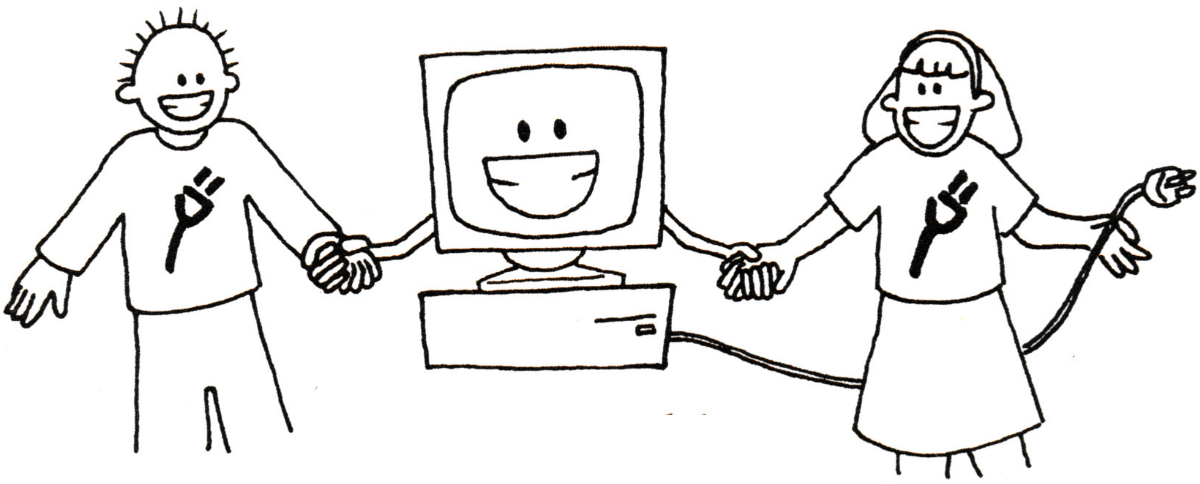
CS UNPLUGGED

Computer Science without a computer

Eine Guideline zur Förderung und Schulung von Schüler_Innen



Inhalte

Vorwort

Eine der größten Materialsammlungen zum informatischen Denken ist CS Unplugged (Computer Science Unplugged), die die Konzepte und die Denkweise des ID durch anregende Spiele und Aufgaben mit Karten, Bindfaden, Wachsstiften und viel Bewegung vermittelt.

CS Unplugged ist frei zugänglich, jedoch waren bis 2019 von den insgesamt 22 Kapiteln leider nur sieben auf Deutsch verfügbar. Deswegen setzt sich das Projekt ADA ein, die vollständige Sammlung auf Deutsch zur freien Nutzung zu stellen. Dies soll unter Beratung des Co-Autors, Prof. Michael Fellows (Uni. Bergen), erfolgen.

ADA stellt zwischen Oktober 2019 und December 2020 die größten Materialsammlungen zum ID für Kinder und Erwachsene schließlich auch dem deutschsprachigen Publikum zur Verfügung.

Unter der Leitung von Prof. Ciabattoni, Prof. Pichler, und Prof. Szeider hat eine Gruppe von Studierenden der TU Wien, Fakultät für Informatik, in Zusammenarbeit mit den Kollegen der ETH Zürich das Buch CS Unplugged in deutscher Sprache zur Verfügung gestellt. Wir möchten uns noch einmal bei der Arbeitsgruppe von Juraj Hromkovic (ETH Zürich) bedanken, die uns die Übersetzung des CS Unplugged zur weiteren Verbesserung zur Verfügung gestellt hat.

Wir möchten uns bei den Kooperationspartners des Projekts bedanken:

- Future Learning Lab Wien (PH Wien)
- eEducation Austria
- Informatik Austria
- Österreichische Computer Gesellschaft (CS Unplugged)
- EIS (Education Innovation Studios Österreich)

Die Sponsoren und finanziellen Unterstützer des Projekts ADA:

- Fakultät für Informatik der TU Wien
- Wirtschaftsagentur Wien (2019 - 2020)
- Wirtschaftskammer Wien (2019)
- Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (2019 2022)

Einführung

Computer sind überall. Wir alle müssen lernen, wie man sie benutzt und viele von uns benutzen sie jeden Tag. Aber wie funktionieren sie? Wie ‚denken' sie? Und wie kann man Software schreiben, die schnell und einfach zu bedienen ist? Informatik ist ein faszinierendes Fachgebiet, das diese Fragen erforscht. Die leichten und lustigen Aktivitäten in diesem Buch, die für SchülerInnen aller Altersstufen entworfen wurden, stellen euch einige der Bausteine vor, wie Computer arbeiten - ohne einen Computer überhaupt zu benutzen!

Dieses Buch kann erfolgreich in Förderungs- und Schulungsprogrammen oder sogar im regulären Klassenunterricht eingesetzt werden. Sie müssen kein Computerexperte oder -expertin sein, um dieses Grundwissen Ihren SchülerInnen zu vermitteln. Das Buch enthält einfach erklärt eine Reihe von Aktivitäten mit Hintergrundinformationen. Antworten auf alle Fragen werden zur Verfügung gestellt und jede Aktivität endet mit einem „Worum geht es in dieser Aktivität?"-Abschnitt, der die Bedeutung der Aktivitäten erklärt.

Viele der Aktivitäten basieren auf Mathematik, z.B. Anwendung von Binärzahlen, Funktionen und Graphen, Modelle, Sortierprobleme und Kryptographie. Andere sind gut auf den technischen Lehrplan angepasst und fokussieren auf Wissen und Verständnis, wie Computer funktionieren. Die SchülerInnen sind aktiv in Kommunikation, Problemlösung, Kreativität und Denkfähigkeit in einem sinnvollen Kontext involviert. Die Aktivitäten bieten auch eine sehr interessante Möglichkeit, das „informatische Denken" zu verstehen, das in den Lehrplänen an Boden gewinnen soll.

Zusätzlich zu diesem Buch stellt das Projekt „Unplugged" viele Online-Ressourcen wie Videos, Bilder und zusätzliches Material unter csunplugged.org frei zur Verfügung. Im Rahmen der Revision dieses Buches 2015, wurde auch eine neue Website erstellt, die einen direkten Zugriff auf Unterlagen, Open-Source Dateien und Links zu weiteren Lehrplänen beinhaltet, um das Verstehen von Informatik und „informatischem Denken" dem Lehrplan der Schulen anzupassen.

Dieses Buch wurde von drei Informatik-Dozenten und zwei Lehrern geschrieben und basiert auf ihre eigene Unterrichtserfahrung, sowie die Erfahrung hunderter Lehrpersonen in den vergangenen zwanzig Jahren. Dabei haben wir festgestellt, dass viele wichtige Konzepte unterrichtet werden können, ohne einen Computer benutzen zu müssen - tatsächlich ist der Computer nur eine Ablenkung vom Lernen. Oft wird Informatik zuerst durch das Programmieren beigebracht, aber nicht jedes Schulkind wird dadurch motiviert und es kann eher ein bedeutendes Hindernis sein, um in die wirklich interessanten Themen der Informatik zu gelangen. Also, schalten Sie Ihren Computer aus und seien Sie bereit zu lernen, was Informatik wirklich ist!

Das Buch ist Dank der Unterstützung von Google, Inc. frei als Download verfügbar. Es steht unter der sogenannten ‚Creative Commons Attribution-Non Commercial-Share Alike'-Lizenz zur Verfügung; das bedeutet, dass das Buch frei kopiert, verteilt und verschickt werden darf. Außerdem darf das Buch auch inhaltlich unter den folgenden Bedingungen neu angeordnet werden: Es enthält den Hinweis auf die Autoren, es darf nicht für kommerzielle Zwecke verwendet werden und unterliegt derselben oder vergleichbarer Lizenz. Mehr Informationen betreffend dieser Lizenz können online unter Sucheingabe „CC BY-NC-SA 3.0" gefunden werden.

Wir unterstützen die Verwendung dieser Unterlagen in pädagogischem Umfeld und laden Sie herzlich ein, Ihre eigenen Kopien des Buches auszudrucken und Arbeitsblätter davon an Ihre SchülerInnen zu verteilen. Auch freuen wir uns auf Anfragen und Anregungen, die Sie an die Autoren richten möchten (siehe csunplugged.org).

Das Buch wurde in viele Sprachen übersetzt. Bitte besuchen Sie die Website betreffend Informationen über die Verfügbarkeit von weiteren Übersetzungen.

Danksagungen

Viele Kinder und Lehrpersonen haben uns geholfen, unsere Ideen zu verfeinern. Die SchülerInnen und LehrerInnen der South Park School und Westburn Primary School (Christchurch, Neuseeland) waren Probanden für viele Aktivitäten. Wir bedanken uns ganz besonders bei Linda Picciotto, Karen Able, Bryon Porteous, Paul Cathro, Tracy Harrold, Simone Tanoa, Lorraine Woodfield und Lynn Atkinson für die Begrüßung in euren Klassen und eure hilfreichen Vorschläge betreffend der Anpassung der Aktivitäten. Gwenda Bensemann hat mehrere Aktivitäten für uns getestet und Änderungen vorgeschlagen. Richard Lynders und Sumant Murugesh haben uns beim Vorgehen im Klassenraum geholfen. Teile des Themas Kryptographie wurden von Ken Noblitz entwickelt. Einige der Aktivitäten wurden unter dem Schirm der Victoria „Mathmania" Gruppe, unter Unterstützung von Kathy Beveridge, geführt. Frühere Versionen der Illustrationen wurden von Malcolm Robinson und Gail Williams erstellt und wir haben auch von den Hinweisen von Hans Knutson profitiert. Matt Powell hat uns auch bei der Entwicklung des Projekts „Unplugged" wertvolle Unterstützung geleistet. Wir bedanken uns bei „Brian Mason Scientific and Technical Trust", einem großzügigen Sponsor in den frühen Stadien der Entstehung dieses Buches.

Besonderer Dank geht an Paul und Ruth Ellen Howard, die viele der Aktivitäten getestet haben und unzählig viele hilfreiche Vorschläge unterbreitet haben. Peter Henderson, Bruce McKenzie, Joan Mitchell, Nancy Walker-Mitchell, Gwen Stark, Tony Smith, Tim A. H. Bell , Mike Hallett und Harold Thimbleby haben uns ebenfalls sehr viele hilfreiche Kommentare gegeben.

Wir verdanken unseren Familien viel für ihre großzügige Unterstützung: Bruce, Fran, Grant, Judith und Pam für ihre Kooperation, und Andrew, Anna, Hannah, Max, Michael und Nikki, die uns oft inspiriert haben und die ersten waren, die Aktivitäten getestet haben.

Besonders dankbar sind wir Google Inc. für das Sponsoring des „Unplugged"-Projekts und der Ermöglichung, diese Edition als kostenlosen Download zur Verfügung zu stellen.

Wir freuen uns auf weitere Kommentare und Anregungen zu den Aktivitäten. Die AutorInnen können über csunplugged.org kontaktiert werden.

Teil I

Daten: Der Rohstoff – Darstellung von Informationen

Daten: Der Rohstoff

Wie können wir Informationen auf Computern speichern?

Das Wort Computer stammt vom lateinischen Begriff ‚computare', was soviel heißt wie ‚rechnen' oder ‚zusammenzählen'. Heute sind die Computer aber viel mehr als nur riesige Rechner; sie können eine ganze Bibliothek sein, uns beim Schreiben helfen, Informationen für uns finden, Musik und sogar Filme abspielen. Aber wie speichern die Computer all diese Informationen? Ob du es glaubst oder nicht, Computer benutzen lediglich zwei Dinge: die Null und die Eins!

Was ist der Unterschied zwischen Daten und Informationen?

Daten sind der Rohstoff: Die Zahlen, mit denen die Computer arbeiten. Ein Computer wandelt seine Daten in Informationen (Worte, Zahlen und Bilder) um, die du und ich verstehen können.

Wie können Zahlen, Buchstaben, Worte und Bilder in Nullen und Einsen umgewandelt werden?

In diesem Kapitel werden wir von den binären Zahlen lernen, wie Computer Bilder zeichnen, wie eine Faxmaschine funktioniert, was der effizienteste Weg ist, um viele Daten zu speichern, wie man Fehler vermeiden kann und wie wir die Menge an Informationen messen, die wir versuchen zu speichern.

Aktivität 1: Punkte zählen – Binärzahlen

Zusammenfassung

Daten sind im Computer als eine Folge von Nullen und Einsen gespeichert und werden auch so übermittelt. Wie können wir Wörter und Zahlen darstellen, indem wir nur diese beiden Symbole verwenden?

Einfügen in den Lehrplan

- Mathematik: Zahlen – Zahlen in einer anderen Basis (hier 2) darstellen.
- Mathematik: Algebra – Zahlenfolgen fortsetzen und eine Regel dafür finden. In diesem Fall handelt es sich um Zweierpotenzen.

Benötigte Vorkenntnisse

- Zählen
- Vervollständigen
- Fortführen

Alter

- 6+

Materialien

Die Lehrperson benötigt:

- Fünf Binärkarten (wie auf Seite 14) für die Demonstration
- A4 Seiten mit Smileys funktionieren gut
- Diskussionsblatt mit Fragen und Aufgaben für die Demonstration (Seite 12)

Jedes Schulkind benötigt:

- Fünf Karten (Kopiervorlage auf Seite 14), zum Ausschneiden
- Arbeitsblatt: Binärzahlen (Seite 13)

Für die erweiterten Aktivitäten braucht jedes Kind:

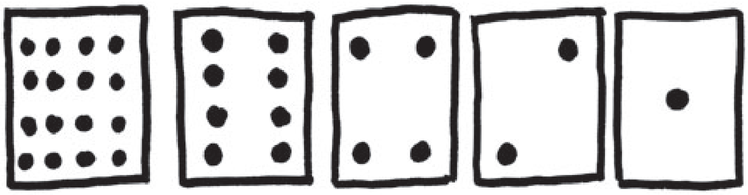
- Arbeitsblatt: Arbeiten mit Binärzahlen (Seite 15)
- Arbeitsblatt: Geheime Nachrichten verschicken (Seite 16)
- Arbeitsblatt: Weiter zählen als 31 (Seite 17)
- Arbeitsblatt: Mehr zum Thema Binärzahlen (Seite 18)

Binärzahlen

Einführung

Bevor das Aufgabenblatt auf Seite 12 verteilt wird, kann es sinnvoll sein das Prinzip vor der ganzen Gruppe zunächst einmal zu demonstrieren.

Für diese Aktivität benötigt die Lehrperson fünf Karten, welche (wie unten dargestellt) auf der einen Seite mit Punkten bedruckt sind, während sie auf der anderen Seite nicht bedruckt sind. Die Lehrperson beginnt damit fünf Kinder nach vorne zu bitten. Die Karten werden an die Kinder in der folgenden Reihenfolge verteilt:



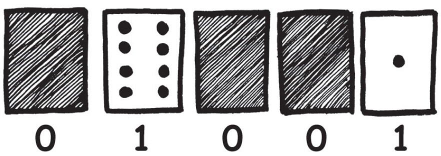
Diskussion

Was fällt euch an der Anzahl der Punkte auf den Karten auf? (Jede Karte enthält jeweils doppelt so viele Punkte wie die vorherige Karte)

Wie viele Punkte müssten also auf der nächsten Karte auf der linken Seite sein, wenn wir noch eine Karte hinzunehmen würden? (32) Und die darauf folgende…? (64)

Wir können diese Karten verwenden um Zahlen darzustellen, indem wir gewisse Karten drehen, sodass deren Punkte sichtbar sind (dies schreiben wir als 1), oder wir lassen sie, sodass keine Punkte sichtbar sind (wir schreiben eine 0). Wir zählen die Anzahl der sichtbaren Punkte. Frage die Kinder, wie man die Zahl 6 darstellen kann (4 Punkte und 2 Punkte), danach 15 (8, 4, 2 und 1 Punkt), danach 21 (16, 4 und 1).

Versuche nun die Klasse von Null hochzählen zu lassen. Der Rest der Klasse soll sorgfältig zuschauen und versuchen das Muster zu erkennen. (Jede Karte wird halb so oft gedreht, wie die Karte auf der rechten Seite). Dies kann man mit mehr als nur einer Gruppe machen.



Fordere die Kinder auf die Zahl 01001 zu bilden. Welche Zahl wird dargestellt? (9). Wie sieht 17 als Binärzahl aus? (10001). Versuche noch einige Beispiele mehr, bis die Kinder das Konzept verstanden haben.

Nun gibt es fünf mögliche Aktivitäten, die folgen können, um das Konzept der Binärzahlen zu verstärken. Die Kinder sollten so viele davon erledigen, wie möglich.

Arbeitsblatt: Binärzahlen

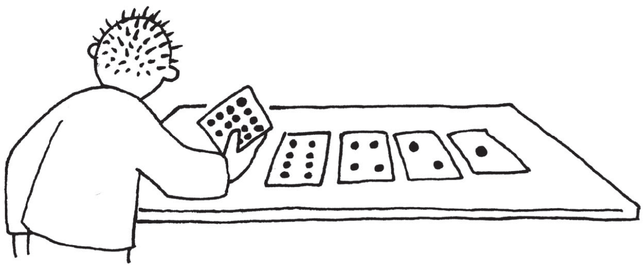
Lernen zu zählen

So, du meinst also, du weißt bereits wie man zählt? Na dann, hier ist eine neue Art zu zählen!

Wusstest du, dass Computer nur Nullen und Einsen kennen? Alles was du auf einem Computer siehst oder von ihm hörst – Wörter, Bilder, Filme, ja sogar Musik, wird mit diesen beiden Zahlen gespeichert. In dieser Aktivität werden wir uns damit befassen, wie man geheime Nachrichten mit Freunden austauscht, genauso wie es der Computer tut.

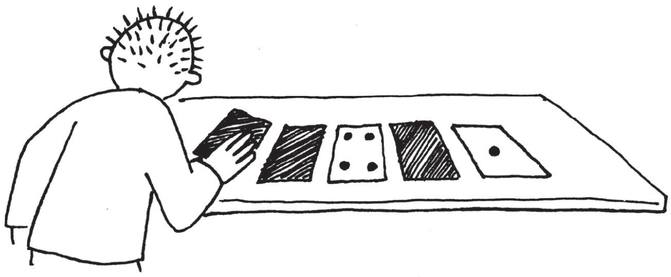
Anleitungen

Nimm das Aufgabenblatt zur Hand und schneide die Karten aus der Vorlage aus. Lege sie danach vor dir auf den Tisch wie dargestellt (die Karte mit 16 Punkten ganz links):



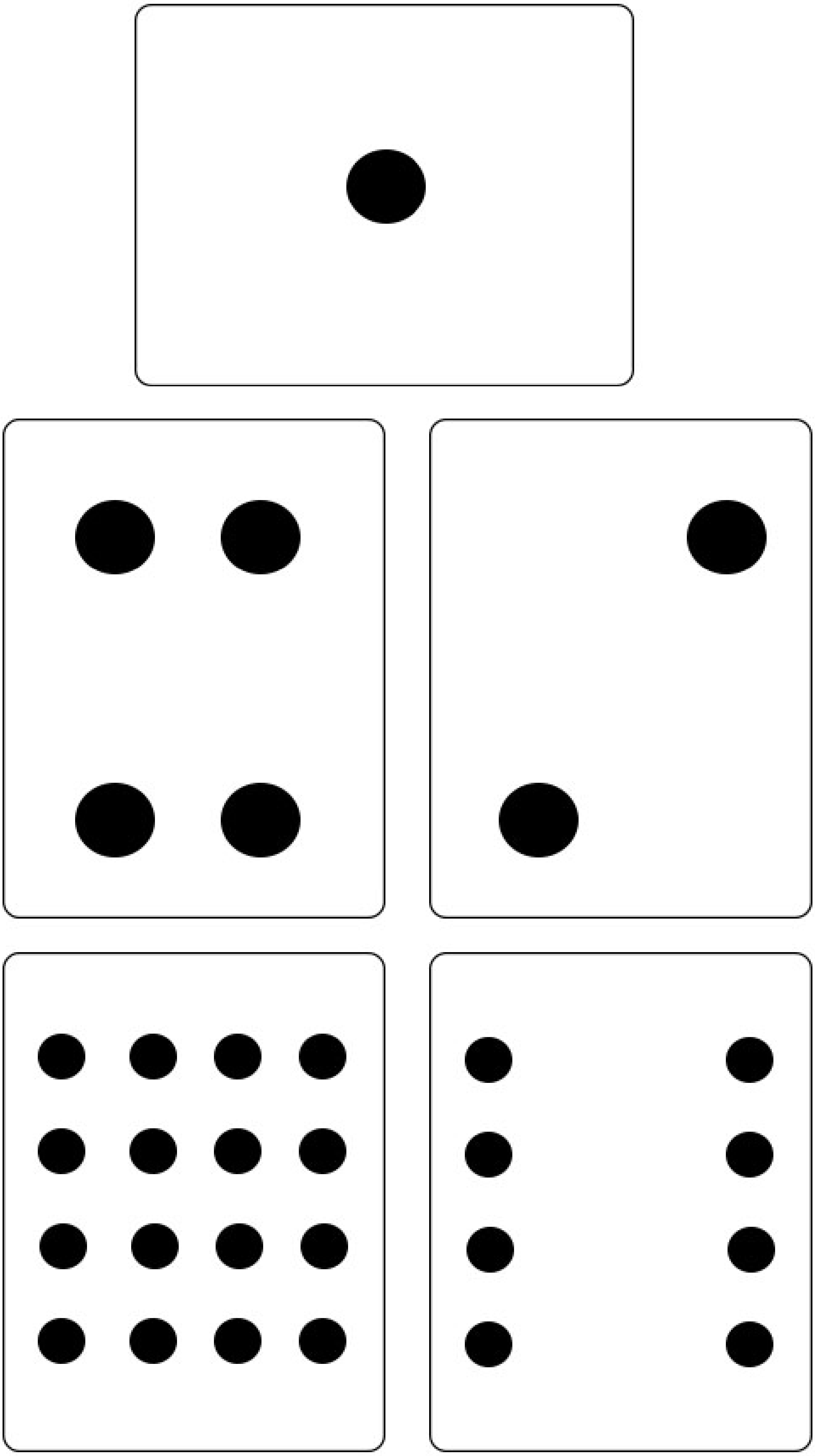
Wichtig: Stelle sicher, dass die Karten genau in derselben Reihenfolge da liegen, wie auf dem Bild. Drehe nun die Karten so um, dass nur noch 5 Punkte sichtbar sind. Behalte dabei die Reihenfolge bei!

Wie stellt man 3, 12 und 19 dar? Gibt es mehrere Möglichkeiten eine Zahl zu bilden? Was ist die größte Zahl, die du auf diese Weise darstellen kannst? Und die kleinste? Gibt es Zahlen zwischen der größten und der kleinsten Zahl, die man nicht erzeugen kann?



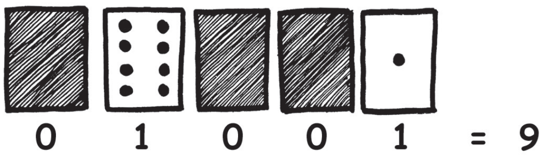
Zusatzaufgabe für ExpertInnen:

Versuche der Reihe nach die Zahlen 1, 2, 3, 4 zu bauen. Finde eine logische und zuverlässige Methode, mit welcher du sagen kannst, welche Karten als nächstes gedreht werden müssen, wenn du hochzählst.



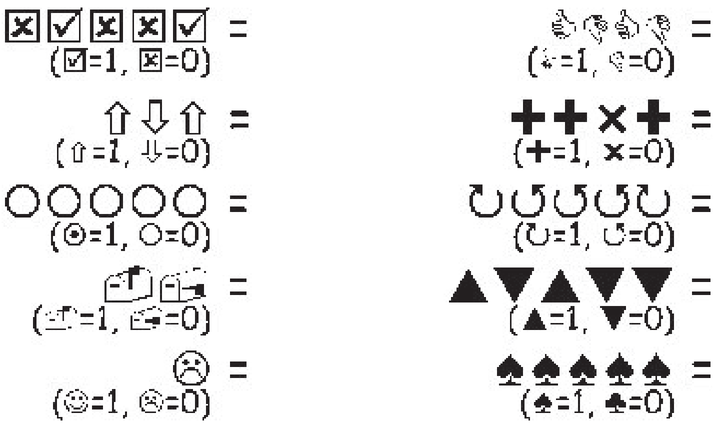
Arbeitsblatt: Arbeiten mit Binärzahlen

Das binäre Zahlensystem verwendet Null und Eins um auszusagen, ob eine Karte nach oben auf dem Tisch liegt (sodass die Punkte sichtbar sind), oder nach unten (dass keine Punkte sichtbar sind). 0 heißt, man sieht keine Punkte. 1 heißt, man sieht welche. Zum Beispiel:



Welche Zahl stellt 10101 dar? Wie steht's mit 11111?

An welchem Tag im Monat wurdest du geboren? Schreibe die Zahl binär auf. Mache dasselbe für das Geburtsdatum deines Banknachbarn / deiner Banknachbarin.



Zugabe für ExpertInnen:

Sagen wir, du hast fünf Schnüre der Länge 1m, 2m, 4m, 8m und 16m. Zeige wie du daraus jede beliebige Länge zwischen 1 und 31 Metern abmessen kannst. Oder überlege dir, wie du bloß mit einer Waage und ein paar Gewichten schwere Gegenstände, wie beispielsweise einen Koffer, wiegen kannst!

Arbeitsblatt: Geheime Nachrichten verschicken

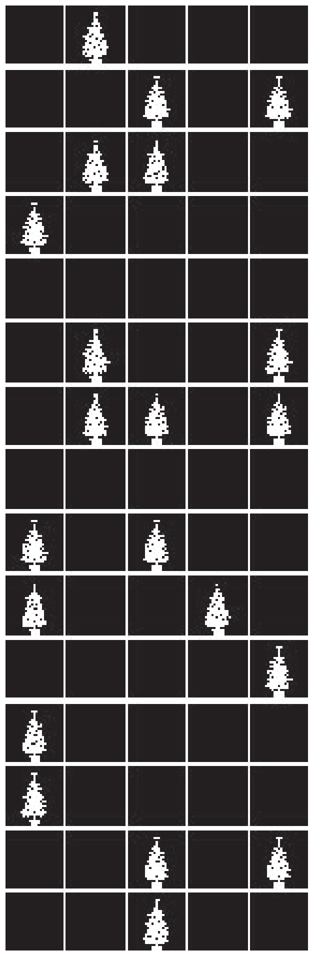
Tom wurde im obersten Stock eines Warenhauses eingeschlossen. Es ist schon bald Weihnachten und er möchte gerne nach Hause zu seiner Familie, wo ihn viele Geschenke erwarten. Was kann er tun?

Er hat bereits versucht anzurufen, sogar um Hilfe geschrien hat er, aber er ist weit und breit der Einzige im Warenhaus; auf diese Weise kann er niemanden erreichen.

Auf der anderen Straßenseite kann er eine Person sehen, die noch am Computer arbeitet, obwohl es bereits langsam dunkel wird. Wie kann er die Aufmerksamkeit dieser Person wecken?

Tom schaut sich um, um zu sehen, was er dazu verwenden könnte. Er hat eine geniale Idee: Er kann das elektrische Licht des Weihnachtsbaumes verwenden, um der Person auf der anderen Straßenseite eine Nachricht zu schicken! Er sucht den Stecker und lässt den Weihnachtsbaum erleuchten und erlöschen.

Tom verwendet einen einfachen Code, von dem er weiß, dass die Person auf der anderen Straßenseite ihn sicher verstehen wird. Findest du heraus, wie die Nachricht lautet, die Tom der Person geschickt hat?



1	2	3	4	5	6	7	8	9	10	11	12	13
a	b	c	d	e	f	g	h	i	j	k	l	m
14	15	16	17	18	19	20	21	22	23	24	25	26
n	o	p	q	r	s	t	u	v	w	x	y	

Arbeitsblatt: Weiter zählen als 31

Schau dir nochmals die Binärkarten an. Wie viele Punkte müsstest du zeichnen, wenn du die nächstgrößere Karte (auf der linken Seite) zeichnen möchtest? Und die danach? Wie lautet die Regel, die du befolgen musst, wenn du neue Karten zeichnen willst? Wie wir gesehen haben, braucht es nur wenige Karten, um schon ziemlich große Zahlen zu erzeugen.

Wenn wir das nochmals genauer betrachten, finden wir einen interessanten Zusammenhang:

1, 2, 4, 8, 16...

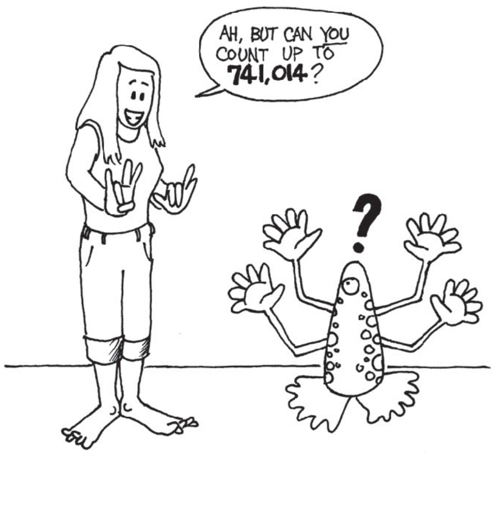
Versuchen wir die Zahlen mal zu addieren: Was ergibt 1+2+4? Wie steht's mit 1+2+4+8?

Hast du dich schon mal daran gestört, dass du nur zehn Finger hast? Früher, als du begonnen hast zu zählen, war das sicher einmal der Fall. Nun ja, wenn wir die Zahlen addieren, können wir viel höhere Zahlen erzeugen, als nur zehn. Und dazu brauchst du nicht einmal ein Alien zu sein. Wenn du das binäre Zahlensystem verwendest und jeden Finger als eine Karte mit 1 bis 16 Punkten betrachtest, kannst du bereits alle Zahlen von 0 bis 31 darstellen. Das sind insgesamt 32 Zahlen (nicht vergessen, die Null ist auch eine Zahl!).

Versuche mit deinen Fingern bis 31 zu zählen, wobei ein Finger immer entweder nach oben gestreckt ist oder nach unten gebeugt, um die Zahlen Null und Eins darzustellen. Oben ist Eins, unten ist Null.

Wenn du nun beide Hände benutzt kommst du sogar bis 1023. Das sind 1024 Zahlen!

Wenn du auch noch sehr bewegliche Zehen hast (und dazu wäre es wohl doch von Vorteil ein Alien zu sein), kämst du sogar noch höher. Mit einer Hand kannst du 32 Zahlen abzählen. Mit zwei Händen sind es 32 × 32 = 1024 Zahlen. Wie weit kann Miss Flexible-Zehen zählen?



Arbeitsblatt: Mehr zum Thema Binärzahlen

1. Eine andere interessante Eigenschaft binärer Zahlen ist das, was mit einer Zahl geschieht, wenn man eine Null rechts anhängt. Wenn wir im Dezimalsystem arbeiten und eine Null rechts an eine Zahl anhängen, wird die ursprüngliche Zahl mit 10 multipliziert. So wird 9 beispielsweise 90 und 30 wird zu 300. Was geschieht aber, wenn wir eine Null rechts an eine Binärzahl heften? Versuchen wir es:

1001	10010
(9)	(?)

Mache noch ein paar andere Experimente um deine Vermutung zu testen. Was ist die Regel? Weshalb ist das so?

2. Jede der Karten, die wir bis jetzt verwendet haben, stellt ein sogenanntes Bit auf dem Computer dar. Der Code, den wir bis jetzt verwendet haben, hat nur fünf Karten (oder Bits) verwendet. Auf dem Computer müssen wir jedoch wissen, ob ein Buchstabe groß- oder kleingeschrieben ist, wir müssen Sonderzeichen und Satzzeichen wie ä,ö,ü und . , : ? oder auch & beachten. Schau dir eine Tastatur an und zähle, wie viele Symbole du erkennen kannst. Wie viele Bits brauchen wir, um alle diese Zeichen darstellen zu können?

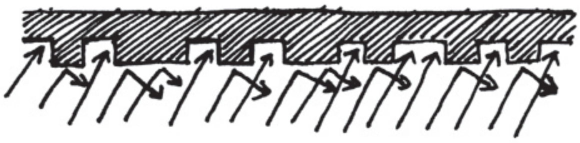
Die meisten Computer brauchen heutzutage eine Darstellung namens ASCII, die auf eben dem Prinzip beruht. Da aber nicht alle Länder die lateinische Schrift verwenden (und deshalb manchmal viel mehr Zeichen verwenden), gibt es auch andere Darstellungen, die dann jedoch mehr Bits benötigen um ein einzelnes Zeichen zu beschreiben.

Worum geht es in dieser Aktivität?

Die Computer von heute verwenden das binäre Zahlensystem um Information darzustellen. Es wird binär genannt, da es zwei verschiedene Nummern verwendet. Manchmal wird es auch als Basis 2 bezeichnet (während wir normalerweise Basis 10 verwenden). Jede Null und jede Eins nennen wir ein Bit. Diese werden im Computer meist durch das Memory repräsentiert, wo ein Transistor angedreht oder abgestellt wird, oder ein Kondensator aufgeladen oder entladen wird.

Wenn Daten via Telefon- oder Fernsehleitung übermittelt werden, erfolgt die Übermittlung meist über hohe und tiefe Töne, die jeweils 0 und 1 darstellen. Auf Disketten und Festplatten werden Bits mittels magnetischer Ausrichtung kleiner Elemente auf der Festplatte dargestellt, die entweder Nord-Süd oder Süd-Nord orientiert sind.

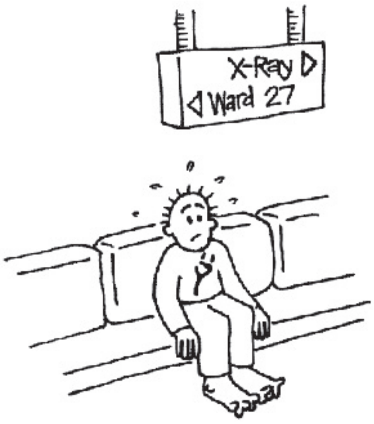
Musik-CDs, CD-ROMs und DVDs speichern Bits optisch – der Teil der Oberfläche, der die Information speichert, ist entweder spiegelnd oder nicht spiegelnd.



Ein einzelnes Bit kann nicht sehr viel repräsentieren, deshalb werden sie oft zusammen, in Gruppengrößen von acht, die Zahlen von 0 bis 255 darstellen, gruppiert. Eine Gruppe von Bits der Größe acht nennt man auch Byte.

Die Geschwindigkeit des Computers hängt davon ab, wie viele Bits er pro Zeiteinheit verarbeiten kann. Ein 32-Bit Computer kann 32-Bit Zahlen in einer Operation verarbeiten. Während ein 16-Bit Computer die Operation auf zwei Operationen aufteilen muss, was ihn langsamer macht.

In einigen der späteren Aktivitäten werden wir sehen, wie andere Arten von Informationen auf einem Computer mit Binärzahlen dargestellt werden können.



Achtung!
Das Verbiegen der Zehen funktioniert nur bei regelmäßigem Training.

Lösungen und Tipps

Binärzahlen (Seite 13)

- Um die Zahl 3 darzustellen, benötigen wir 2 und 1 Punkt(e)
- Um die Zahl 12 darzustellen, benötigen wir 8 und 4 Punkte
- Um die Zahl 19 darzustellen, benötigen wir 16, 2 und 1 Punkt(e)

Die größtmögliche Zahl, die mit den Karten 1,2,4,8 und 16 darstellbar ist, ist die Zahl 31 (wenn sämtliche Karten offen daliegen). Jede Zahl zwischen 1 und 31 lässt sich darstellen und es gibt nur eine korrekte Darstellung pro Zahl.

Expertenfrage: Um hochzuzählen werden von rechts her alle Karten gedreht bis man eine dreht, die nach oben dagelegen ist.

Arbeiten mit Binärzahlen (Seite 15)

10101 = 21, 11111 = 31

Geheime Nachrichten verschicken (Seite 16)

Die Nachricht lautet: HILFE ICH BIN DA

Weiter zählen als 31 (Seite 17)

Jede Karte enthält genau einen Punkt mehr, als alle vorherigen Karten zusammen. (So enthält beispielsweise die vierte Karte 8 Punkte, während die Summe der ersten drei Karten 7 Punkte ergibt.)

Miss Flexible-Zehen kann bis 1024 × 1024 = 1.048.576 zählen (und somit alle Zahlen von 0 bis 1.048.575 mit den Händen und Zehen darstellen!)

Mehr zum Thema Binärzahlen (Seite 18)

Wenn man eine 0 ganz rechts an eine Binärzahl anhängt, verdoppelt sich die Zahl. (All die Stellen, wo die Zahl vorher eine 1 enthalten hat werden verdoppelt, da wir sie um eine Stelle nach rechts verschieben. Daher verdoppelt sich die ganze Zahl. Nebenbemerkung: Wenn wir dasselbe bei Dezimalzahlen machen, multiplizieren wir die Zahl mit 10.)

Ein Computer braucht 7 Bits um alle Buchstaben zu speichern. Die Darstellung mit 7 Bits ermöglicht uns bis zu 128 Buchstaben darzustellen. Normalerweise werden die 7 Bits jedoch als 8-Bit Sequenz (Byte) abgespeichert, wobei ein Bit verschwendet wird.

Aktivität 2: Malen nach Zahlen – Bilddarstellung

Zusammenfassung

Computer speichern Zeichnungen, Fotos und andere Bilder nur durch Verwendung von Zahlen. In dieser Aktivität wird veranschaulicht, wie Computer das machen können.

Einfügen in den Lehrplan

- Mathematik: Geometrie – Formen und Räume
- Technologie: Benutzung von ganzen Zahlen zur Darstellung anderer Datentypen
- Technologie: Verringerung des Raumes durch sich wiederholende Daten

Benötigte Kenntnisse

- Zählen
- Grafisch darstellen

Alter

- 7+

Materialien

- Folie zur Präsentation: Malen nach Zahlen (Seite 23)

Jedes Schulkind benötigt:

- Arbeitsblatt: Male dein eigenes Bild (Seite 25)

Malen nach Zahlen

Einführung

Diskussionsfragen

1. Was machen Faxmaschinen?

2. In welchen Situationen müssen die Computer Bilder speichern? (Ein Zeichenprogramm, ein Spiel mit Grafiken oder ein Multimediasystem)

3. Wie können Computer Bilder speichern, wo sie doch nur Zahlen benutzen können?

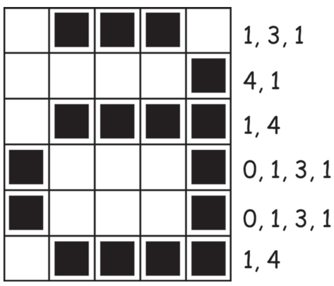
(Sie können die SchülerInnen gerne dazu veranlassen, Faxe als Vorbereitung für diese Aktivität zu senden und/oder zu empfangen)

Demonstration mit Projektion

Computer-Bildschirme sind in ein Raster von kleinen Punkten, die Pixel (picture elements) genannt werden, aufgeteilt.

In einem Schwarz-Weiß-Bild ist jedes Pixel entweder schwarz oder weiß.

Der Buchstabe „a“ wurde oben zur Darstellung der Pixel vergrößert dargestellt. Wenn ein Computer ein Bild speichert, muss lediglich gespeichert werden, welche Punkte schwarz und welche weiß sind.



Das Bild oben zeigt uns, wie ein Bild durch Zahlen dargestellt werden kann. Die erste Zeile besteht aus einem weißen Pixel, dann drei schwarzen und danach einem weißen Pixel. Demzufolge wird die erste Zeile wie folgt dargestellt: 1, 3, 1.

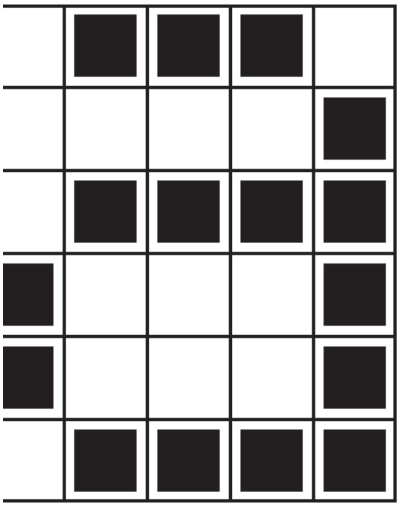
Die erste Zahl bezieht sich immer auf die Anzahl der weißen Pixel. Also beginnt eine Zeile mit einer Null, wenn der erste Pixel schwarz ist.

Das Arbeitsblatt auf Seite 24 zeigt einige Bilder, die die SchülerInnen mit der soeben beschriebenen Methode, entschlüsseln können.

Malen nach Zahlen

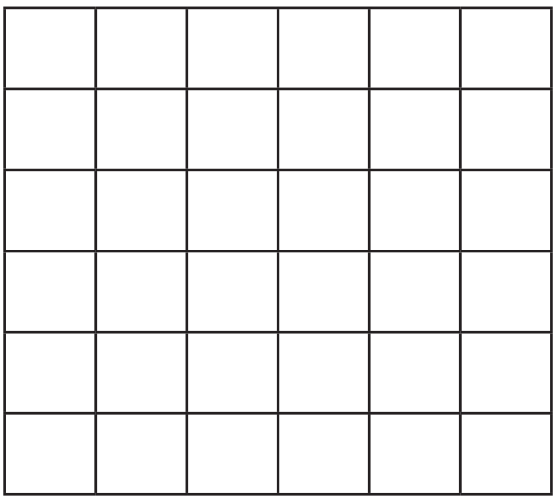
Ein Buchstabe „a“ von einem Computerbildschirm und eine vergrößerte Ansicht, die die Pixel zeigt, die das Bild bilden.

Das gleiche Bild codiert mit Zahlen



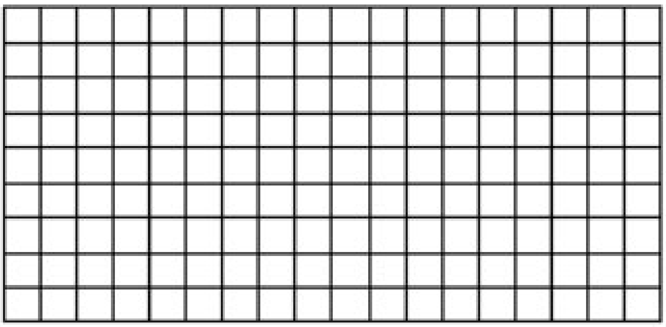
1, 3, 1
4, 1
1, 4
0, 1, 3, 1
0, 1, 3, 1
1, 4

Leeres Raster (für Lehrzwecke)

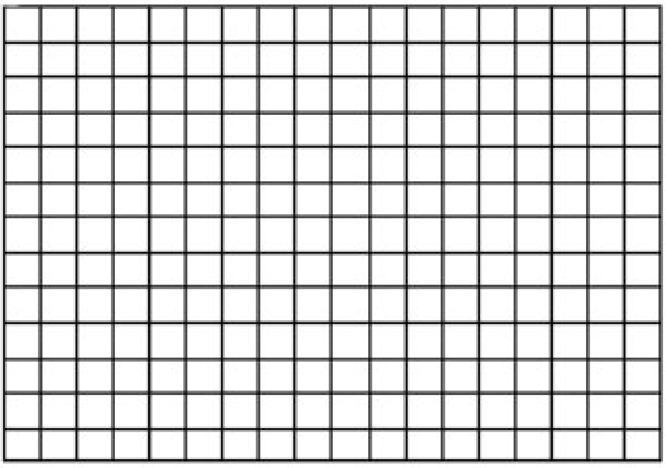


Arbeitsblatt: Kinder Fax

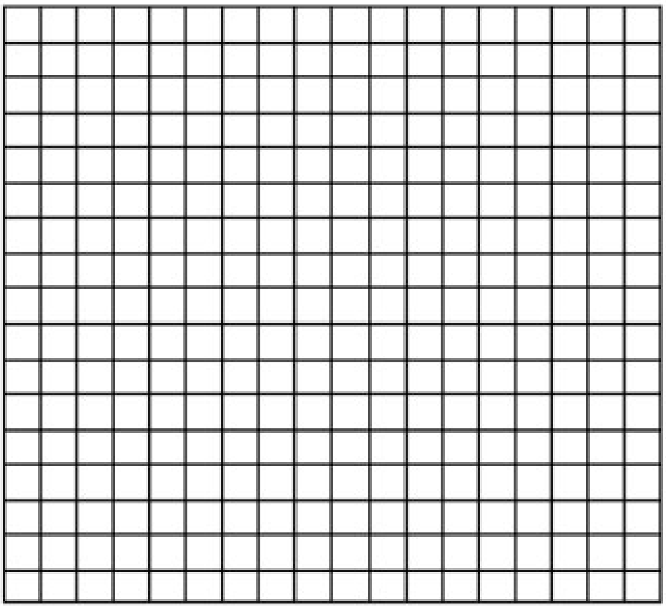
Das erste Bild ist das einfachste und das letzte ist das komplexeste. Es ist leicht, Fehler zu machen und daher eine gute Idee, einen Bleistift mit einem Radiergummi zu verwenden, um zu zeichnen und schnell wieder löschen zu können.



4, 11
4, 9, 2, 1
4, 9, 2, 1
4, 11
4, 9
4, 9
5, 7
0, 17
1, 15



6, 5, 2, 3
4, 2, 5, 2, 3, 1
3, 1, 9, 1, 2, 1
3, 1, 9, 1, 1, 1
2, 1, 11, 1
2, 1, 10, 2
2, 1, 9, 1, 1, 1
2, 1, 8, 1, 2, 1
2, 1, 7, 1, 3, 1
1, 1, 1, 1, 4, 2, 3, 1
0, 1, 2, 1, 2, 2, 5, 1
0, 1, 3, 2, 5, 2
1, 3, 2, 5



6, 2, 2, 2
5, 1, 2, 2, 2, 1
6, 6
4, 2, 6, 2
3, 1, 10, 1
2, 1, 12, 1
2, 1, 3, 1, 4, 1, 3, 1
1, 2, 12, 2
0, 1, 16, 1
0, 1, 6, 1, 2, 1, 6, 1
0, 1, 7, 2, 7, 1
1, 1, 14, 1
2, 1, 12, 1
2, 1, 5, 2, 5, 1
3, 1, 10, 1
4, 2, 6, 2
6, 6

Arbeitsblatt: Male dein eigenes Bild

Nun, da du weißt wie Zahlen Bilder darstellen können, warum nicht versuchen ein eigenes codiertes Bild für einen Freund / eine Freundin zu malen? Zeichne dein Bild auf das Raster und wenn du fertig bist, schreibe die Codenummern neben dem Raster auf der nächsten Seite. Schneide entlang der gepunkteten Linie und gebe das untere Raster einem Freund / einer Freundin zum Malen. (Anmerkung: Du musst nicht das ganze Raster verwenden - lass einfach einige leere Zeilen an der Unterseite, wenn dein Bild nicht das ganze Raster befüllt.)

Arbeitsblatt: Male dein eigenes Bild

Zugabe für ExpertInnen: Wenn du farbige Bilder malen möchtest, kannst du eine Zahl dazu verwenden (z.B. 0 ist schwarz, 1 ist rot, 2 ist grün etc.). Zwei Zahlen werden verwendet, um einen Lauf von Pixeln darzustellen: die erste gibt wie zuvor die Länge des Laufes und die zweite gibt die Farbe an. Versuche ein farbiges Bild für einen Freund / eine Freundin zu machen. Nicht vergessen: Sage deinem Freund / deiner Freundin, welche Nummer für welche Farbe steht!

Variationen und Erweiterungen

1. Versuche mit einem transparenten Blatt Papier auf dem Gitter zu zeichnen, damit das endgültige Bild ohne Raster betrachtet werden kann. Das Bild wird klarer sein.

2. Anstatt das Raster zu färben, könnten die SchülerInnen Quadrate aus klebendem Papier verwenden oder Gegenstände auf ein größeres Raster legen.

Diskussionspunkt

Es gibt gewöhnlich eine Grenze für die Länge eines Laufs von Pixeln, da die Länge als Binärzahl dargestellt wird. Wie würdest du einen Lauf von zwölf schwarzen Pixeln darstellen, wenn du nur Zahlen bis zu sieben verwenden könntest? (Ein guter Weg ist ein Lauf von sieben schwarzen Pixeln, gefolgt von einem Lauf von null weißen und dann ein Lauf von fünf schwarzen Pixeln zu programmieren.)

Worum geht es in dieser Aktivität?

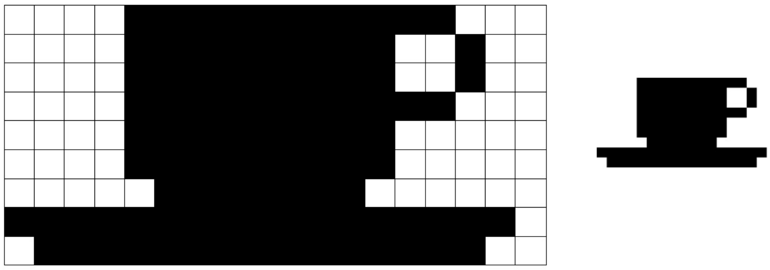
Ein Faxgerät ist eigentlich nur ein einfacher Computer, der eine Schwarz-Weiß-Seite in ca. 1000 × 2000 Pixeln scannt, die mit einem Modem an ein anderes Faxgerät gesendet wird, das die Pixel auf eine Seite druckt. Oftmals haben die Bilder, die über ein Faxgerät geschickt werden, große Blöcke von weißen (z. B. Rändern) oder schwarzen Pixeln (z. B. eine horizontale Linie). Auch Farbbilder enthalten viele Wiederholungsmuster. Um den Speicherplatz einzuschränken, der benötigt wird um solche Bilder zu halten, können Programmierer_Innen eine Vielzahl von Kompressionstechniken verwenden. Die in dieser Aktivität verwendete Methode wird als „Lauflängencodierung“ bezeichnet und ist ein effektiver Weg, um Bilder zu komprimieren. Wenn wir keine Bilder komprimieren würden, würde es viel länger dauern, Bilder zu übertragen und viel mehr Speicherplatz benötigen. Dies würde es unmöglich machen, Faxe zu senden oder Fotos auf eine Website zu stellen. Zum Beispiel werden Faxbilder im Allgemeinen auf etwa ein Siebtel ihrer ursprünglichen Größe komprimiert. Ohne Kompression würde die Übertragung siebenmal so lange dauern!

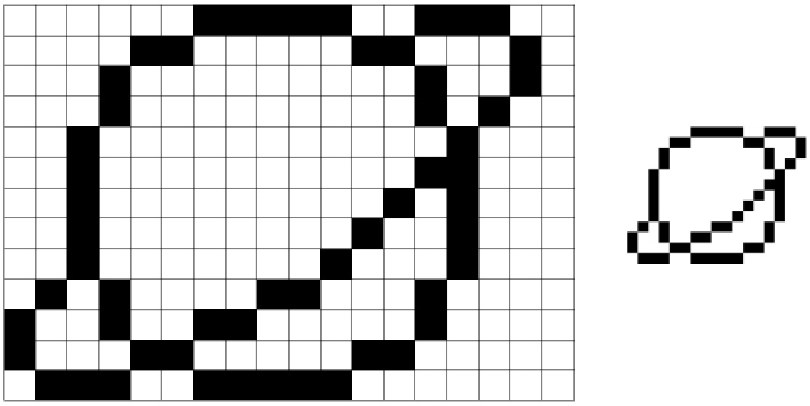
Fotos und Bilder werden oft auf ein Zehntel oder sogar ein Hundertstel ihrer ursprünglichen Größe komprimiert (unter Verwendung von ähnlichen Techniken wie JPEG, GIF und PNG). Dies ermöglicht, dass viele weitere Bilder auf einer Festplatte gespeichert werden können und, dass ihre Betrachtung über das Web nur einen Bruchteil der Zeit in Anspruch nehmen wird.

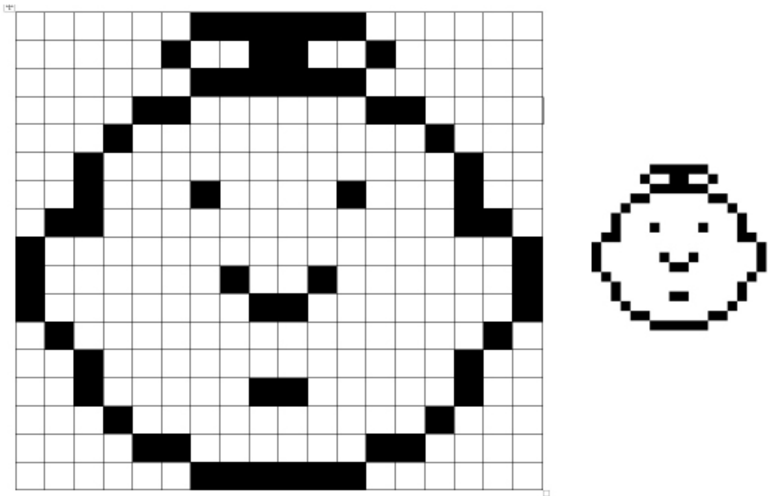
Ein Programmierer kann wählen, welche Kompressionstechnik am besten zu den Bildern passt, die er oder sie versendet.

Lösungen und Tipps

Lösungen für das Kinder Fax Arbeitsblatt:







Aktivität 3: Kannst du das nochmal sagen! – Textkomprimierung

Zusammenfassung

Da Computer nur einen begrenzten Speicherplatz haben, um Informationen zu halten, müssen sie Informationen so effizient wie möglich ablegen. Dies wird als ‚Kompression' bezeichnet. Durch das kodieren von Daten bevor sie gespeichert werden, und dekodieren, wenn sie abgerufen werden, kann der Computer mehr Daten schneller speichern oder durch das Internet senden.

Einfügen in den Lehrplan

- Englisch: Erkennen von Mustern in Worten und Text.
- Technologie: Reduzierung des Speichers, der durch sich wiederholende Daten verwendet wird.

Benötigte Kenntnisse

Kopieren von Text

Alter

9+

Materialien

Präsentationsfolie: Kannst du das nochmal sagen! (Seite 31)

Jedes Schulkind benötigt:

Arbeitsblatt: Kannst du das nochmal sagen! (Seite 33)

Arbeitsblatt: Extras für ExpertInnen (Seite 34)

Arbeitsblatt: Kurz und bündig (Seite 35)

Arbeitsblatt: Extras für echte ExpertInnen (Seite 36)

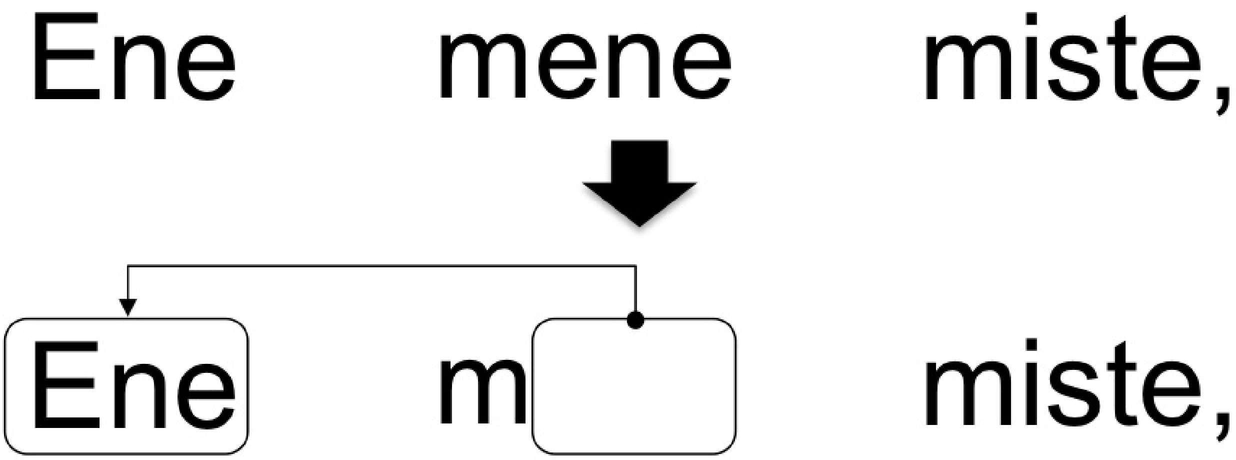
Kannst du das nochmal sagen!

Einführung

Computer müssen sehr viele Daten speichern und versenden. Damit sie nicht zu viel Speicherplatz verbrauchen müssen oder es zu lange dauert, um Informationen über eine Netzwerkverbindung zu senden, komprimieren sie den Text wie im Folgenden beschrieben.

Demonstration und Diskussion

Betrachte die Seite „Ein lustiger Reim“ (Seite 32). Suche nach dem Muster der Buchstaben in diesem Text. Kannst du Gruppen von zwei oder mehr Buchstaben finden, die wiederholt werden, oder sogar ganze Wörter oder Phrasen? (Ersetze diese mit Schachteln wie in der folgenden Abbildung gezeigt wird.)



Kannst du das nochmal sagen!

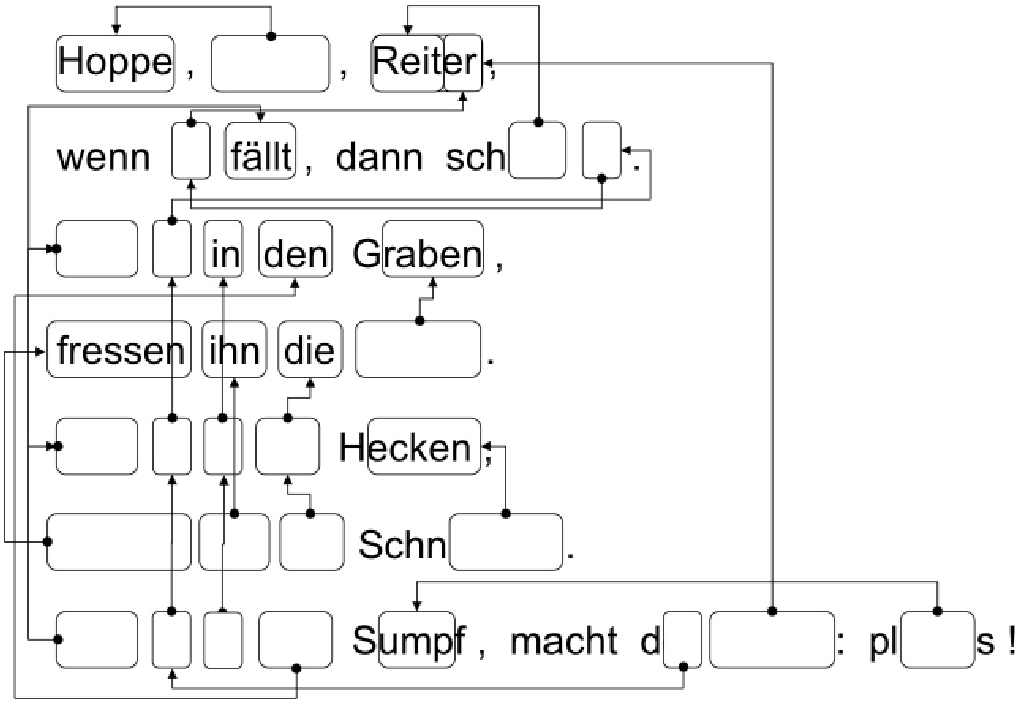
Ein lustiger Reim

Ene mene miste,
es rappelt in der Kiste.

Ene mene meck,
und du bist weg.

Arbeitsblatt: Kannst du das nochmal sagen!

Viele Wörter und Buchstaben fehlen in diesem Text. Kannst du die fehlenden Wörter und Buchstaben korrekt eintragen? Du findest sie in den Feldern, auf die der Pfeil hinzeigt.



Wähle jetzt ein einfaches Gedicht oder ein Kinderlied und entwerfe dein eigenes Puzzle. Achte darauf, dass die Pfeile immer auf einen früheren Teil des Textes zeigen. Das Gedicht sollte von links nach rechts und von oben nach unten, in der gleichen Weise wie wir lesen, dekodiert werden können.

Hinweis: Beachte, wie wenige der ursprünglichen Wörter du behalten musst!

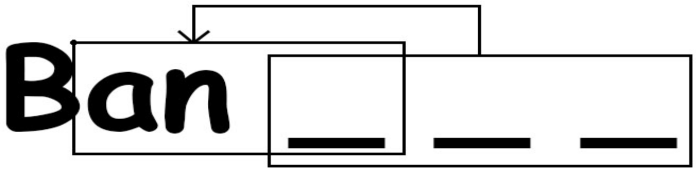
Hier zwei weitere Vorschläge: ‚Heile, heile Segen' oder ‚Bienchen, Bienchen, summ, summ, summ'

Tipp: Versuche die Überlagerung von Pfeilen zu vermeiden. Lass viel Platz für Buchstaben und Wörter, sodass du genug Platz für die Felder hast und die Pfeile darauf zeigen können.

Es ist einfacher das Puzzle zu entwerfen, wenn du zuerst das Gedicht schreibst und dann entscheidest, wo die Felder sein müssen.

Arbeitsblatt: Extras für ExpertInnen

Wie würdest du dieses Rätsel lösen?



Manchmal kann der fehlende Text auf eigene Textteile zeigen. In diesem Fall kann er korrekt dekodiert werden, wenn die Buchstaben von links nach rechts kopiert werden. Dadurch ist jeder Buchstabe verfügbar, bevor er benötigt wird. Dies ist bei Computern nützlich, wenn es einen langen Lauf von bestimmten Schriftzeichen oder Mustern gibt.

Versuche selbst einige zu zeichnen.

Auf Computern werden die Felder und Pfeile durch Zahlen dargestellt. Hier ein Beispiel:

Banana[1]

kann als ‚**Ban(2,3)**' beschrieben werden, wobei **„2"** bedeutet, dass du zwei Buchstaben zurück als Startpunkt für das Kopieren wählen musst und **„3"** ‚drei aufeinanderfolgende Buchstaben' bedeutet:

Ban_ _ _

Bana_ _

Banan_

Banana

Zwei Zahlen werden verwendet um dieses Wort zu kodieren; in der Regel sind nur Gruppen von zwei oder mehr Buchstaben für Komprimierung geeignet. Sonst kann kein Platz gespart werden, da die Größe der Datei steigt, wenn zwei Zahlen verwendet werden, um einen Buchstaben zu kodieren.

Finde eigene Wörter so, wie ein Computer sie komprimieren würde. Können deine Freunde sie dekodieren?

1 'Banana' heißt Banane auf Englisch.

Arbeitsblatt: Kurz und bündig

Wie viele Wörter brauchst du hier wirklich?

Stell dir vor du bist ein Computer, der soviel wie möglich auf deiner Disk speichern möchte. Dazu werden alle Gruppen mit zwei oder mehr Buchstaben gestrichen, die bereits vorgekommen sind; sie werden nicht mehr gebraucht, weil sie durch einen Zeiger ersetzt worden sind. Ziel ist es, so viele Buchstaben wie möglich zu streichen.

Ich kenne eine Frau,
die hat Augen aus Kakao
und eine dicke Leberwurst,
das weiß ich ganz genau!
Ich weiß auch wo sie wohnt,
drei Häuser hinterm Mond.
Und ich weiß auch wie sie heißt:
Zip-zippelip-zippelo- zippeldipap!

Arbeitsblatt: Extras für ‚echte' ExpertInnen

Bereit für eine wirklich schwierige Komprimierung?

Wie viele Buchstaben kannst du hier streichen? Aber denke daran, nur Gruppen mit zwei oder mehreren wiederholten Zeichen dürfen gestrichen werden. Viel Glück!

Die drei Schweinchen

Es war einmal eine alte Schweinemutter, die hatte drei kleine Schweinchen, die aßen und aßen, so viel sie nur konnten. Und als sie so groß waren, dass sie in dem Haus, in dem sie wohnten, keinen Platz mehr finden konnten, sagte die Mutter zu ihnen:
„Ihr könnt jetzt nicht mehr bei mir bleiben, jedes muss ein Haus für sich selber haben."
Und sie schickte sie in die weite Welt hinaus.

Das erste Schweinchen begegnet einem Mann mit einem Bund Stroh.
Es sagt zu ihm:
„Bitte, lieber Mann, gib mir das Stroh, ich will mir ein Haus daraus bauen."
Da sagt der Mann: „Gib mir erst von deinen Borsten, ich will mir eine Bürste daraus machen."

Nun gibt ihm das Schweinchen von seinen Borsten, der Mann gibt ihm das Stroh und hilft ihm das Haus aufbauen.
Vorne hat das Haus eine große Tür und hinten eine kleine Tür.
Dann schaut das Schweinchen sein Strohhaus an und singt:

„Ich hab' ein schönes Haus von Stroh,
ich bin so sicher und so froh.
Und kommt der böse Wolf vorbei,
dann lache ich, hihi, heihei"

Das zweite Schweinchen begegnet einem Mann mit einem Bund Holz.
Es sagt zu ihm: „Bitte, lieber Mann, gib mir das Holz, ich will mir ein Haus daraus bauen."
Der Mann aber sagt: „Gib mir erst von deinen Borsten, ich will mir eine Bürste daraus machen."
Nun gibt ihm das Schweinchen von seinen Borsten, der Mann gibt ihm das Holz und hilft ihm das Haus aufbauen.
Vorne hat das Haus eine große Tür und hinten eine kleine Tür.
Dann schaut das Schweinchen sein Holzhaus an und singt:

„Ich hab' ein schönes Haus von Holz,
ich bin so sicher und so stolz.
Und kommt der böse Wolf vorbei,
dann lache ich, hihi, heihei!"

Das dritte Schweinchen begegnet einem Mann, der zieht einen Karren voll Ziegelsteine.
Es sagt zu ihm: „Bitte, lieber Mann, gib mir von den Ziegelsteinen, ich will mir ein Haus daraus bauen."
Der Mann aber sagt: „Gib mir erst von deinen Borsten, ich will mir eine Bürste daraus machen."
Das Schweinchen gibt ihm, so viel er davon haben will, und der Mann gibt ihm die Ziegelsteine und hilft ihm das Haus aufbauen.

Vorne hat das Haus eine große Tür und hinten eine kleine Tür.
Dann schaut das Schweinchen sein Ziegelhaus an und singt:

„Ich hab' ein schönes Haus von Stein,
es ist so sicher und so fein.

Und kommt der böse Wolf vorbei,
dann lache ich, hihi, heihei"

So lebt nun jedes Schweinchen in seinem eigenen kleinen Haus, und jedes ist glücklich und zufrieden.
Da kommt eines Tages der Wolf aus dem Wald, klopft an die große Tür des kleinen Strohhauses und ruft:

„Liebes, gutes kleines Schwein,
lass mich doch zu dir hinein."

Das Schweinchen aber antwortet:
„Bin ganz allein,
bin ganz allein,
ich lass dich nicht ins Haus herein."

Da sagt der Wolf:
„Ich werde strampeln und trampeln,
ich werde husten und prusten
und dir dein Haus zusammenpusten."

Und der Wolf strampelt und trampelt, er hustet und prustet und pustet das ganze Haus zusammen.
Aber das kleine Schweinchen ist nicht mehr da.
Es ist hinten durch die kleine Tür zum zweiten Schweinchen ins Holzhaus gelaufen.

Da geht der Wolf zum Holzhaus, klopft vorn an die große Tür und ruft:
„Liebes, gutes kleines Schwein,
lass mich doch zu dir hinein."

Das zweite Schweinchen aber antwortet:
„Bin ganz allein, bin ganz allein,
ich lass dich nicht ins Haus herein."

Da sagt der Wolf:
„Ich werde strampeln und trampeln,
ich werde husten und prusten
und dir dein Haus zusammenpusten."

Und der Wolf strampelt und trampelt, er hustet und prustet und pustet das ganze Haus zusammen.
Aber die zwei kleinen Schweinchen sind nicht mehr da, sie sind hinten durch die kleine Tür zum dritten Schweinchen ins Ziegelhaus gelaufen. Da geht der Wolf zum Ziegelhaus, klopft vorn an die große Tür und ruft:

„Liebes, gutes kleines Schwein,
lass mich doch zu dir hinein."

Das dritte Schweinchen aber antwortet:
„Bin ganz allein, bin ganz allein,

ich lass dich nicht ins Haus herein."

Da sagt der Wolf:
„Ich werde strampeln und trampeln,
ich werde husten und prusten
und dir dein Haus zusammenpusten."

Und der Wolf strampelt und trampelt, er hustet und prustet, aber er kann das Haus nicht zusammenpusten.
Da wird er schrecklich zornig und brüllt:

„Wart nur, gleich hab' ich dich!"

und macht sich daran, durch den Kamin ins Haus zu klettern.

Als die drei Schweinchen merken, was der Wolf im Sinne hat, sagt das erste Schweinchen:
„Was sollen wir tun?"

Das zweite Schweinchen:
„Ich will ein großes Feuer im Kamin anmachen."

Und das dritte Schweinchen:
„Ich will einen großen Topf mit Wasser in den Kamin hängen."

Das tun sie auch.

Nicht lange danach - das Feuer prasselt schon lustig und das Wasser ist gerade am Sieden -, da kommt der Wolf den Kamin herunter, und platsch! plumpst er mitten ins heiße Wasser hinein, und schnell geben die Schweinchen noch einen Deckel darauf.

Dann tanzen sie vor Freude um den Kamin herum und singen:
„Der Wolf ist tot,
der Wolf ist tot,
ein Ende hat die große Not."

Dann baute sich das erste Schweinchen ein Ziegelhaus und das zweite auch, und fortan lebten alle drei zufrieden und froh.

Worum geht es in dieser Aktivität?

Die Speicherkapazität von Computern wächst in einem unglaublichen Tempo - in den letzten 25 Jahren ist der Speicherbereich auf einem typischen Computer millionenfach gewachsen - aber wir brauchen ständig noch mehr Speicher auf unseren Computern. Auf Computern können ganze Bücher oder sogar Bibliotheken und jetzt auch Musik und Filme gespeichert werden, wenn es genug ‚Platz' gibt. Große Dateien sind auch ein Problem im Internet, weil sie eine lange Zeit zum Download benötigen. Wir versuchen auch, Computer kleiner zu machen - sogar auf einem Handy oder einer Armbanduhr kann erwartet werden, dass dort viele Informationen gespeichert werden können!

Es gibt indessen eine Lösung für dieses Problem. Anstatt mehr Speicherplatz oder eine schnellere Netzwerkverbindung zu kaufen, können wir die Daten komprimieren, sodass weniger Platz benötigt wird. Dieser Vorgang der Komprimierung und Dekomprimierung der Daten erfolgt normalerweise automatisch auf dem Computer. Alles was wir vielleicht dabei bemerken ist, dass die Festplatte mehr beinhalten kann, oder dass Websites schneller angezeigt werden. Tatsächlich aber kann der Computer mehr verarbeiten.

Viele Methoden der Kompression wurden entwickelt. Die Methode, die in dieser Aktivität verwendet wird – mit dem Prinzip auf frühere Vorkommen von Textstücken zu verweisen – wird oft als „Ziv-Lempel-Codierung" oder „LZ-Codierung" bezeichnet und wurde von zwei israelischen Professoren in den 1970er Jahren entwickelt. Die Codierung kann für jede Sprache verwendet werden und kann leicht die Menge der Daten halbieren. Es wird manchmal auch als 'Zip' auf Personalcomputern bezeichnet, als 'GIF' und 'PNG' für Bilder verwendet und in High-Speed Modems eingesetzt. Bezüglich Modems reduziert es die Datenmenge, die über die Telefonleitung übertragen werden muss, sodass sie viel schneller übertragen wird.

Einige andere Methoden basieren auf der Idee, dass Buchstaben, die häufiger verwendet werden, kürzere Codes als die anderen haben sollten. Der Morsecode verwendet diese Idee.

Lösungen und Tipps

Kannst du das nochmal sagen! (Seite 33)

Hoppe, hoppe, Reiter,

wenn er fällt, dann schreit er.

Fällt er in den Graben,

fressen ihn die Raben.

Fällt er in die Hecken,

fressen ihn die Schnecken.

Fällt er in den Sumpf, macht der Reiter: plumps!

Aktivität 4: Der Zauber, Karten umzublättern –Fehlererkennung & -korrektur

Zusammenfassung

Wenn Daten auf einem Datenträger gespeichert oder von einem Computer zum anderen übertragen werden, nehmen wir in der Regel an, dass sie sich dabei nicht verändern. Aber manchmal passieren Fehler und die Daten werden versehentlich geändert. In dieser Aktivität verwenden wir einen magischen Trick, der zeigt, wie wir erkennen, dass Daten beschädigt wurden und wie wir sie korrigieren können.

Einfügen in den Lehrplan

- Mathematik: Zahlen – Untersuchung von Berechnung und Schätzung.
- Mathematik: Algebra – Untersuchung von Mustern und Beziehungen untereinander, um einen fehlenden Wert zu finden.
- Mathematik: Zeilen und Spalten, Koordinaten
- Technologie: Daten validieren

Benötigte Kenntnisse

- Zählen
- Erkennen von geraden und ungeraden Zahlen

Alter

- 7+

Materialien

- Eine Menge von 36 „Kühlschrankmagneten", die nur auf einer Seite gefärbt sind.
- Eine Metallplatte für die Vorführung (eine Weißwandtafel ist ideal).

Jedes Paar Schüler_Innen braucht:

- 36 gleiche Karten, die nur auf einer Seite gefärbt sind.

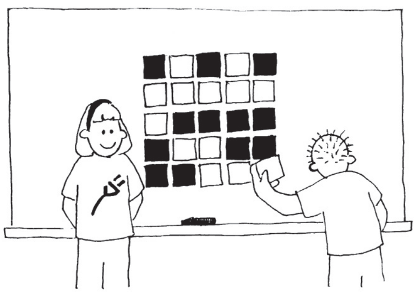
Der „Zaubertrick“

Vorführung

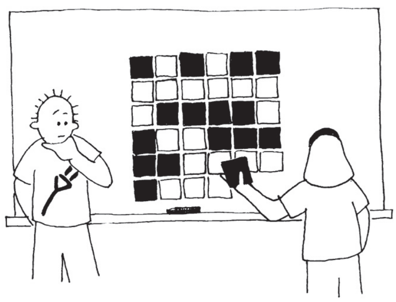
Dies ist deine Chance, ein Zauberer oder eine Zauberin zu sein!

Du brauchst einen Stapel von identischen, zweiseitigen Karten. (Um eigene Karten herzustellen, zerschneide ein großes Kartenblatt, das nur auf einer Seite gefärbt ist). Zur Vorführung ist es am einfachsten flache Magnetkarten zu verwenden, die auf jeder Seite anders gefärbt sind – Kühlschrankmagnete sind dafür ideal, wenn sie auf beiden Seiten magnetisch sind (viele davon sind es nur einseitig, dann klebe sie entsprechend aufeinander und markiere eine Seite mit einem weißen Punkt).

1. Bestimme eine Mitschülerin oder einen Mitschüler, die oder der 25 Karten als ein 5x5 Quadrat nach zufälliger, eigener Wahl an die Tafel heftet.



Nebenbei fügst du eine weitere Zeile und Spalte hinzu, „um die Sache schwieriger zu machen“.



Deine Karten sind aber der Trick dabei. Du musst die zusätzlichen Karten so auswählen, dass in jeder Zeile und Spalte eine gerade Anzahl von farbigen Karten vorhanden ist!

Wähle ein Schulkind, das eine Karte umdrehen soll, während du deine Augen schließt und nicht zur Tafel gerichtet bist. Die Zeile und die Spalte, die die geänderte Karte enthält, hat nun eine ungerade Anzahl von farbigen Karten, und dies hilft die umgedrehte Karte zu identifizieren. Können die SchülerInnen erraten, wie der Trick funktioniert?

Zeige den Trick allen SchülerInnen:

1. Jeweils zu zweit legen die SchülerInnen ihre Karten in einem 5x5 Quadrat aus.

2. Wie viele farbige Karten befinden sich in jeder Zeile und Spalte? Handelt es sich dabei um eine gerade oder ungerade Zahl? Beachte, '0' wird als gerade Zahl betrachtet.

    1. Füge jetzt jeder Reihe eine sechste Karte hinzu, sodass die Anzahl der farbigen Karten immer gerade ist. Die zusätzliche Karte wird als „paritätische" Karte oder „Paritätskarte" be zeichnet.

    2. Füge anschließend ganz unten eine sechste Reihe hinzu, damit die Anzahl der farbigen Karten in jeder Spalte gerade ist.

    3. Drehe jetzt eine Karte. Was fällt bei der betreffenden Zeile und Spalte auf? (Beide haben eine ungerade Anzahl von farbigen Karten.) Paritätskarten werden benutzt, um anzuzeigen, wo ein Fehler aufgetreten ist.

    4. Jetzt wechselt euch ab und führt den Trick aus.

Weitere Aktivitäten:

1. Verwende andere Objekte. Alles, was zwei „Darstellungen" hat, ist geeignet. Zum Beispiel könnt-en Spielkarten, Münzen (Kopf oder Zahl) oder Karten mit 0 oder 1 verwendet werden (um sich auf das binäre System zu beziehen).

2. Was passiert, wenn zwei oder mehr Karten umgedreht werden? (Es ist nicht immer möglich, genau zu wissen, welche beiden Karten umgedreht wurden, obwohl es möglich ist zu sagen, dass etwas geändert wurde. In der Regel kann man das Problem auf eine von zwei Kartenpaar-en reduzieren. Bei vier Kartenumdrehungen ist es allerdings möglich, dass alle Paritätsbits korrekt sind und daher der Fehler unentdeckt bleibt!)

3. Versuche es mit einem größeren Feld, etwa ein 9x9 Quadrat, das mit der zusätzlichen Zeile und Spalte auf 10x10 erweitert wird. (Es wird für jede Feldgröße funktionieren und muss nicht quadratisch sein).

4. Eine weitere interessante Aufgabe ist, die Karte unten rechts zu betrachten. Wenn du sie als korrekten Wert für die Karten der Spalte darüber betrachtest, wird das auch für alle Karten in der Zeile links daneben gelten? (Ja, gilt immer für eine gerade Anzahl von Paritätsbits.)

In dieser Aktivität haben wir gerade Parität mit einer geraden Anzahl von farbigen Karten verwen-det. Können wir das auch für ungerader Parität verwenden? (Es ist möglich, aber die untere rechte Karte funktioniert nur für ihre Zeile und Spalte, wenn die Anzahl der Zeilen und Spalten beide gerade oder ungerade sind. Zum Beispiel funktioniert es bei den Anordnungen 5x9 oder 4x6, aber nicht bei 3x4.)

Ein echtes Beispiel für ExpertInnen!

Die gleiche Prüfmethode wird mit Buchcodes und Barcodes verwendet. Veröffentlichte Bücher haben einen zehn- oder 13-stelligen Code, der normalerweise auf der Rückseite aufgetragen wird. Die letzte Zahl ist eine Prüfziffer, genau wie die Paritätsbits in der Aufgabe.

Wenn du ein Buch unter Angabe der ISBN (International Standard Book Number) bestellst, kann die Website prüfen, dass kein Fehler bei der Eingabe vorgekommen ist. Sie schauen einfach auf die Prüfsumme. Deshalb musst du nicht auf das falsche Buch warten!

Jetzt betrachten wir, wie man die Prüfsumme für einen zehnstelligen Buchcode ausarbeitet:

Multipliziere die erste Zahl mit zehn, die zweite mit neun, die dritte mit acht und so weiter bis zur neunten Zahl; multipliziere diese mit zwei. Alle Werte werden dann addiert.

Zum Beispiel die ISBN 0-13-911991-4 hat folgenden Wert

$$(0 \times 10) + (1 \times 9) + (3 \times 8) + (9 \times 7) + (1 \times 6)$$

$$+ \quad (1 \times 5) + (9 \times 4) + (9 \times 3) + (1 \times 2)$$

$$= \quad 172$$

Das Ergebnis wird jetzt durch 11 geteilt. Was ist der Restwert?

$$172 \div 11 = \quad 15 \text{ Rest } 7$$

Wenn der Restwert Null ist, ist die Prüfsumme Null. Ansonsten subtrahiere den Restwert von 11 zur Berechnung der Prüfsumme.

$$11 - 7 = \quad 4$$

Wie du siehst ist das die letzte Ziffer der oben angegebenen ISBN!

Wäre die letzte Ziffer der ISBN nicht die vier, wüssten wir, dass ein Fehler vorgekommen ist.

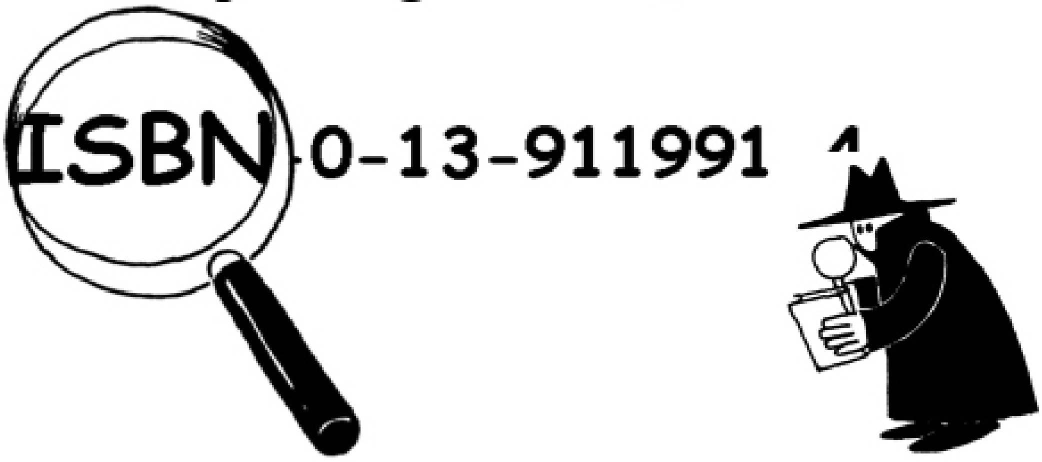
Es ist auch möglich, dass die Prüfsumme 10 vorkommt, die zwei Ziffern benötigen würde. Wenn das passiert, wird das Zeichen X dafür verwendet.

Ein Barcode (UPC) auf einer Schachtel der Firma Weet-Bix™

Ein weiteres Beispiel für die Verwendung von Prüfziffern sind die Barcodes auf Lebensmittelpackungen. Hier wird eine andere Formel verwendet (die gleiche Formel wird für die 13-stellige ISBN angewendet). Wenn ein Strichcode falsch gelesen wird, sollte die letzte Ziffer von ihrem berechneten Wert abweichen. Wenn das vorkommt, ertönt der Scanner und der Verkäufer scannt den Code erneut. Prüfziffern werden auch für Bankkontonummern, Sozialversicherungsnummern, Steuernummern, Ziffern auf Zügen und Fahrzeugen und viele andere Anwendungen verwendet, von denen Personen eine Nummer kopieren und die Sicherheit benötigen, dass sie korrekt eingegeben wurde.

Prüfe dieses Buch!

Detektiv Schnüffler
Buchprüfungs-Service, Inc.



Wir finden und überprüfen ISBN Prüfsummen für eine kleine Gebühr.

Komm zu uns — wir prüfen die echten ISBN-Codes in deinem Klassenzimmer oder deiner Bibliothek.

Sind die Prüfnummern korrekt?

Gelegentlich werden Fehler gemacht. Einige der häufigsten Fehler sind:

- eine Ziffer hat sich geändert;
- zwei benachbarte Ziffern werden miteinander vertauscht;
- eine Ziffer wird in die Zahl eingefügt; und
- eine Ziffer wird von der Zahl entfernt

Kannst du ein Buch mit dem Buchstaben X für eine Prüfsumme von 10 finden? Das sollte nicht zu schwer zu finden sein – mindestens eines von elf Büchern sollte es haben.

Welche Art von Fehler könnte auftreten, der nicht erkannt wird? Kann man eine Ziffer ändern und immer noch die richtige Prüfsumme bekommen? Was, wenn zwei Ziffern vertauscht werden (ein häufiger Schreibfehler)?

Worum geht es in dieser Aktivität?

Stell dir vor du zahlst 10 Euro in dein Bankkonto ein. Der Kassierer tippt den Betrag ein und dieser wird zu einem zentralen Computer gesendet. Angenommen einige Störungen treten auf während der Betrag gesendet wird und der Betrag von 10 Euro wird auf 1.000 Euro geändert. Kein Problem, wenn du der Kunde / die Kundin bist, aber eindeutig ein Problem für die Bank!

Es ist wichtig, Fehler in übermittelten Daten zu erkennen. So muss ein Empfänger (Computer) überprüfen, ob die Daten, die zu ihm kommen, nicht durch irgendeine Art von elektrischer Störung verändert worden sind. Manchmal können die ursprünglichen Daten erneut gesendet werden, wenn ein Fehler übertragen wurde, aber es gibt einige Situationen, wo das nicht möglich ist, etwa wenn eine Festplatte durch Einwirkung von magnetischer oder elektrischer Strahlung, durch Hitze oder durch physischen Schaden beschädigt wurde. Wenn Daten von einer Weltraumsonde empfangen werden, wäre es sehr mühsam auf eine erneute Übertragung zu warten, wenn ein Fehler aufgetreten ist! (Es dauert etwas mehr als eine halbe Stunde, um ein Funksignal vom Planet Jupiter zu bekommen, wenn er der Erde am nächsten ist!)

Wir müssen erkennen können, dass die Daten beschädigt sind (Fehlererkennung) und zudem in der Lage sein, die Originaldaten zu rekonstruieren (Fehlerkorrektur).

Die gleiche Technik wie sie im „Kartentrick"-Spiel verwendet wurde, wird auch auf Computern verwendet. Indem wir die Bits in imaginäre Zeilen und Spalten eintragen und Paritätsbits zu jeder Zeile und Spalte hinzufügen, können wir nicht nur feststellen, ob ein Fehler aufgetreten ist, sondern wo er aufgetreten ist. Das betreffende Bit wird zurückgesetzt und so konnten wir eine Fehlerkorrektur durchführen.

Natürlich verwenden Computer häufig komplexere Fehlerkontrollsysteme, die in der Lage sind, mehrere Fehler zu erkennen und zu korrigieren. Auf jeder Festplatte in einem Computer wird eine große Menge an Speicher für die Anpassung der Korrekturfehler reserviert, sodass es zuverlässig funktioniert, auch wenn einige Teile des Datenträgers ausfallen. Die hierfür verwendeten Systeme stehen in engem Zusammenhang mit dem Paritätsschema.

Lösungen und Tipps

Fehler, die von einer ISBN-10-Prüfsumme nicht erkannt werden, sind diejenigen, bei denen eine Ziffer größer und eine andere kleiner wird, die Summe aber gleich bleibt. Allerdings ist dieser Änderungsvorgang unwahrscheinlich. In anderen Systemen (wie ISBN-13) gibt es noch andere Arten von Fehlern, die möglicherweise nicht erkannt werden, wie z. B. drei aufeinanderfolgende Ziffern, die umgetauscht wurden. Die meisten der häufigsten Fehler (die falsche Eingabe einer Ziffer oder das Tauschen von zwei benachbarten Ziffern) werden aber erkannt.

Teil II

Computer zur Arbeit bringen –Algorithmen

Computer zur Arbeit bringen

Computer arbeiten, indem sie eine Liste von Anweisungen ausführen. Diese Anweisungen ermöglichen es dem Computer, Informationen zu sortieren, zu finden und zu senden. Um diese Dinge so schnell wie möglich zu machen, braucht man gute Methoden, um Dinge in großen Datenmengen zu finden und Informationen über Netzwerke zu senden.

Ein Algorithmus ist ein Satz von Anweisungen zum Abschließen einer Aufgabe. Die Bedeutung eines Algorithmus ist zentral für die Informatik. Algorithmen beschreiben, wie Computer Probleme lösen können. Einige Algorithmen sind schneller als andere und viele der Algorithmen, die entdeckt wurden, haben es möglich gemacht Probleme zu lösen, die zuvor eine unendlich lange Zeitspanne brauchten - zum Beispiel, um Millionen von Ziffern in Pi zu finden, oder alle Websites zu finden, die deinen Namen enthalten, oder den besten Weg herauszufinden, Pakete in einen Container zu packen, oder herauszufinden, ob sehr große (100-stellige) Zahlen Primzahlen sind.

Der Begriff „Algorithmus” stammt aus dem Namen Mohammed ibn Musa Al-Khowarizmi-Mohammed, Sohn von Moses aus Khowarizm - der sich um 800 n. Chr. einem akademischen Zentrum namens „Haus der Weisheit“ in Bagdad angeschlossen hat. Seine Werke übermittelten die hinduistische Kunst zu rechnen an die Araber und dann nach Europa. Als sie im Jahr 1120 ins Lateinische übersetzt wurden, waren die ersten Worte „Dixit Algorismi” - „So sagte Algorismi”.

Aktivität 5: Zwanzig Versuche – Informationstheorie

Zusammenfassung

Wie viele Informationen gibt es in einem 1000-seitigen Buch? Gibt es mehr Informationen in einem 1000-seitigen Telefonbuch oder in einem Ries mit 1000 Blättern leerem Papier oder in Tolkiens 'Herr der Ringe'? Wenn wir dies messen können, können wir abschätzen wie viel Platz benötigt wird, um die Informationen zu speichern. Kannst du zum Beispiel noch den folgenden Satz lesen?

n dsm Stz fhln ll Vkl

Wahrscheinlich kannst du es, weil es in den Vokalen nicht viel „Information" gibt. Diese Aktivität führt zu einer Möglichkeit, Informationsinhalte zu messen.

Einfügen in den Lehrplan

- Mathematik: Zahlen – 'größer als', 'kleiner als' Umfeld.
- Mathematik: Algebra – Muster und Sequenzen
- Englisch: Rechtschreibung, Erkennung von Elementen des Textes

Benötigte Kenntnisse

- Zahlen vergleichen und mit Zahlenbereichen arbeiten
- Schlussfolgerung
- Fragen stellen

Alter

- 10+

Materialien

- Für die erste Aktivität sind keine Materialien erforderlich

Für die weitere Aktivität benötigt jedes Schulkind:

- Arbeitsblatt: Entscheidungsbäume (Seite 55)

Zwanzig Versuche

Diskussion

1. Diskutiere mit den SchülerInnen, was sie denken, was Information ist.

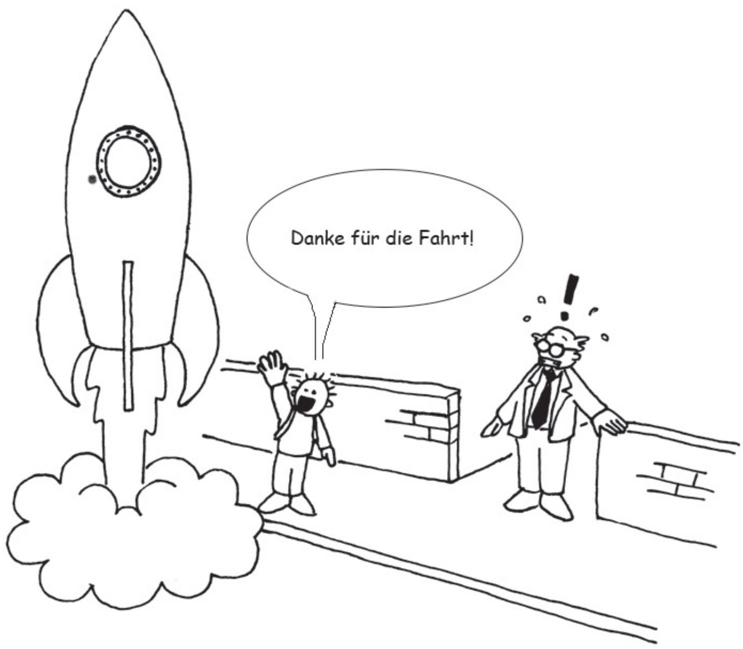
2. Wie könnten wir messen, wie viel Informationen in einem Buch vorhanden wäre? Ist die Anzahl der Seiten oder die Anzahl der Wörter wichtig? Kann ein Buch mehr Informationen beinhalten als ein anderes? Was ist, wenn es ein sehr langweiliges Buch oder ein besonders interessantes ist? Würden 400 Seiten eines Buches mit dem Ausdruck "blah, blah, blah" mehr oder weniger Informationen haben als das Telefonverzeichnis?

3. Erkläre, dass InformatikerInnen Informationen bewerten, abhängig davon wie unerwartet eine Nachricht (oder ein Buch!) ist. Sagt man dir etwas, das du schon weißt – zum Beispiel, wenn ein Freund, der immer zur Schule geht, sagt: „Ich bin heute zur Schule gegangen." – dann gibt man dir keine Informationen, denn es ist nichts Neues dabei. Wenn dein Freund stattdessen sagen würde: „Ich habe heute in einem Hubschrauber eine Fahrt zur Schule gemacht", wäre das sehr überraschend und würde uns viele Informationen mitteilen.

4. Wie kann der ‚Überraschungswert' einer Nachricht gemessen werden?

5. Eine Möglichkeit ist, zu sehen wie schwer es ist, die Informationen zu erraten. Wenn dein Freund sagt: „Rate wie ich heute in die Schule gekommen bin", und er ist zu Fuß gegangen, würdest du wohl sofort das Richtige erraten. Es könnte noch ein paar weitere Vermutungen brauchen, bevor du zu einem Hubschrauber kommen würdest, und noch mehr, wenn er mit einem Raumschiff gereist wäre.

6. Die Menge an Informationen, die Nachrichten enthalten, wird gemessen anhand der Tatsache, wie einfach oder schwer sie zu erraten sind. Das folgende Spiel gibt uns eine Vorstellung davon.



Zwanzig Fragen-Aktivität

Dies ist ein geeignetes Spiel mit 20 Fragen. Die SchülerInnen können einer/m zuvor gewählten Schülerin/Schüler Fragen stellen, die nur mit Ja oder Nein beantwortet werden, bis die Antwort erraten wurde. Jede Frage kann gestellt werden, vorausgesetzt, dass die Antwort streng “Ja” oder “Nein” ist.

Vorschläge:

Ich denke an:

- eine Zahl zwischen 1 und 100
- eine Zahl zwischen 1 und 1000
- eine Zahl zwischen 1 und 1,000,000.
- irgendeine ganze Zahl
- eine Folge von 6 Zahlen nach einem bestimmten Muster (angepasst an die SchülerInnen-Gruppe). Rate die Zahlen von der kleinsten bis zur größten Zahl (z.B. 2, 4, 6, 8, 10)

Zähle die Anzahl der Fragen, die gestellt wurden. Dies ist ein Maß für den Wert der „Information“.

Nachfolgediskussion

Welche Strategien hast du benutzt? Welche waren die besten?

Weise darauf hin, dass es nur 7 Versuche braucht, um eine Zahl zwischen 1 und 100 zu finden, wenn du den Bereich jedes Mal halbierst. Zum Beispiel:

Ist sie kleiner als 50?	**Ja.**
Ist sie kleiner als 25?	**Nein.**
Ist sie kleiner als 37?	**Nein.**
Ist sie kleiner als 43?	**Ja.**
Ist sie kleiner als 40?	**Nein.**
Ist sie kleiner als 41?	**Nein.**
Es muss die 42 sein!	**Ja!**

Interessanterweise dauert es nicht 10 Mal länger, wenn der Zahlenbereich auf 1000 erhöht wird - nur noch drei weitere Fragen werden benötigt. Jedes Mal wenn die Strecke verdoppelt wird, braucht man nur noch eine weitere Frage, um die Antwort zu finden.

Jetzt wäre es für die SchülerInnen zur Vertiefung gut, wenn sie das Spiel ‘Mastermind’ benutzen.

Erweiterung: Wieviel Information befindet sich in einer Nachricht?

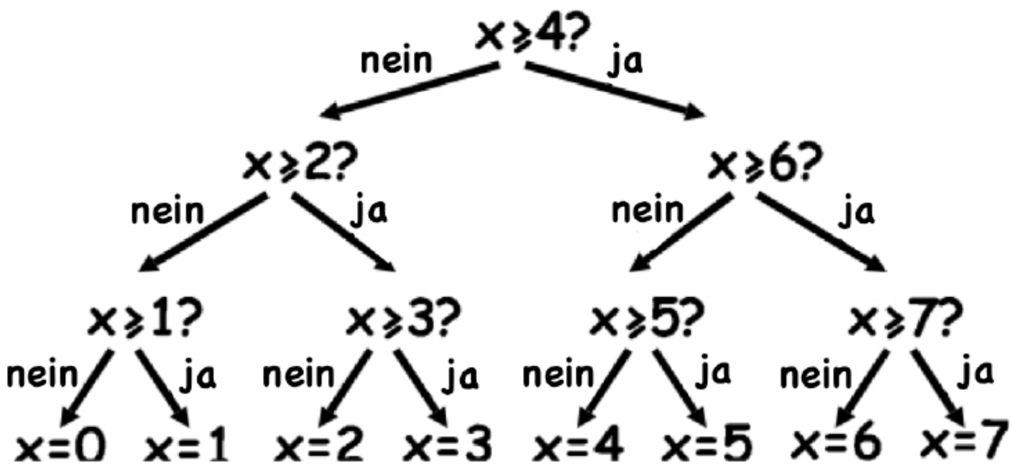
InformatikerInnen benutzen nicht nur das Raten mit Zahlen – sie können auch erraten, welcher Buchstabe eher der nächste in einem Wort oder Satz ist.

Versuche das Ratespiel mit einem kurzen Satz von 4-6 Wörtern. Die Buchstaben müssen in der richtigen Reihenfolge von Anfang bis Ende erraten werden. Bestimme jemanden, der die gefundenen Buchstaben notiert und aufschreibt, wie viele Versuche es gebraucht hat, um jeden Buchstaben zu finden. Alle Fragen mit einer Ja / Nein-Antwort können verwendet werden. Beispiele wären: „Ist es ein t?“ „Ist es ein Vokal?“ „Kommt es vor dem ‘m’ im Alphabet vor?“ Ein Platz zwischen Worten zählt auch als „Buchstabe“ und muss erraten werden. Wechselt euch ab und beobachtet, ob ihr entdecken könnt, welche Teile von Nachrichten am einfachsten herauszufinden sind.

Arbeitsblatt: Entscheidungsbäume

Wenn du die Strategie um die Fragen zu stellen bereits kennst, kannst du eine Nachricht schicken ohne zu fragen.

Hier ist ein Diagramm namens ‘Entscheidungsbaum’ für das Raten einer Zahl zwischen 0 und 7:



Was sind die Ja / Nein-Entscheidungen, um die Zahl 5 zu ‘erraten’?

Wie viele Ja / Nein-Entscheidungen musst du machen, um eine beliebige Zahl zu finden?

Jetzt schauen wir etwas Faszinierendes an. Unterhalb der Zahlen ‘x=0’, ‘x=1’,... in der letzten Zeile des Baumes schreibe die Zahl als binäre Zahl auf (siehe Aktivität 1).

Schau dir den Baum genauer an. Was siehst du, wenn ‘nein=0’ und ‘ja=1’ ist?

In dem Zahlen-Ratespiel versuchen wir Fragen so zu stellen, dass die Reihenfolge der Antworten die Zahl ganz genau so darstellt.

Entwirf einen eigenen Entscheidungsbaum um Zahlen zwischen 0 und 15 zu erraten.

Zugabe für ExpertInnen: Was für einen Baum würdest du benutzen, um das Alter von jemandem zu erraten? Wie sieht ein Baum aus um zu erraten, welcher der nächste Buchstabe in einem Satz ist?

Worum geht es in dieser Aktivität?

Ein berühmter amerikanischer Mathematiker (und Jongleur und Einradfahrer) namens Claude Shannon hat viele Experimente mit diesem Spiel gemacht.

Er maß die Menge an Informationen in Bits - jede Ja / Nein-Antwort entspricht einem 1/0-Bit. Er fand, dass die Menge an „Information", die in einer Nachricht enthalten ist, von dem abhängt, was wir bereits wissen. Manchmal können wir eine Frage stellen, die die Notwendigkeit beseitigt, eine Menge anderer Fragen zu stellen. In diesem Fall ist der Informationsgehalt der Nachricht gering.

Zum Beispiel ist die Information in einem einzigen Wurf einer Münze normalerweise ein Bit: Kopf oder Zahl. Wenn aber die Münze ‘verfälscht’ ist, die den Kopf bei neun von zehn Würfen zeigt, entspricht die Information nicht mehr einem Bit – auch, wenn man’s nicht glauben kann: noch weniger! Wie findest du mit weniger als einer Ja / Nein Frage heraus, wie der Münzwurf war? Einfach – verwende dazu nur Fragen wie „Werden die nächsten zwei Münzwürfe ‚Kopf’ zeigen?“

Für eine Folge von Würfen mit der ‘verfälschten’ Münze, wird die Antwort darauf etwa 80% der Zeit „Ja“ sein. Bei den übrigen 20% der Würfe, wo die Antwort „Nein“ ist, musst du noch zwei weitere Fragen stellen. Im Durchschnitt aber wirst du weniger als eine Frage pro Münzwurf stellen!

Shannon nannte den Informationsgehalt einer Nachricht „Entropie“. Entropie hängt nicht nur von der Anzahl der möglichen Ergebnisse ab (2, im Fall eines Münzwurfs), sondern auch von der Wahrscheinlichkeit, dass es passiert. Unwahrscheinliche Ereignisse oder überraschende Informationen brauchen viel mehr Fragen, um die Botschaft zu erraten, weil sie uns mehr Informationen mitteilen, die wir noch nicht kennen - genau wie die Situation, einen Hubschrauber zur Schule zu nehmen.

Die Entropie einer Botschaft ist für InformatikerInnen sehr wichtig.

Du kannst eine Nachricht nicht komprimieren, um weniger Platz als ihre Entropie zu nehmen, und die besten Kompressionssysteme sind gleichbedeutend mit einem Ratespiel. Da ein Computerprogramm die „Versuche“ macht, kann die Liste der Fragen später wiedergegeben werden; solange die Antworten (Bits) gespeichert sind, können wir die Informationen rekonstruieren! Die besten Kompressionssysteme können Textdateien auf etwa ein Viertel ihrer ursprünglichen Größe reduzieren - eine große Einsparung von Speicherplatz!

Die Rate-Methode kann auch verwendet werden, um eine Computerschnittstelle zu bauen, die prognostiziert, was der Benutzer als nächstes eingeben wird!

Dies kann sehr nützlich sein für körperlich behinderte Menschen, die es schwer haben zu schreiben. Der Computer schlägt ihnen vor was er vermutet und sehr wahrscheinlich ist, als nächstes eingetragen zu werden, und die Benutzer geben nur ein, was sie wollen.

Ein gutes System braucht durchschnittlich nur zwei Ja / Nein-Antworten pro Schriftzeichen und kann von großem Nutzen für jemanden sein, der Schwierigkeiten hat, die feinen Bewegungen zu machen, die benötigt werden, um eine Maus oder eine Tastatur zu steuern. Diese Art von System wird auch in einer anderen Form verwendet, um Text auf einigen Handys einzutippen.

Lösungen und Tipps

Die Antwort auf eine einzelne Ja / Nein-Frage entspricht genau einem Bit an Information - ob es sich um eine einfache Frage wie „Ist es mehr als 50?“ oder eine komplexere wie „Ist es zwischen 20 und 60?“ handelt.

In dem Zahl-Raten-Spiel, wenn die Fragen in einer bestimmten Weise gewählt werden, ist die Reihenfolge der Antworten nur die binäre Darstellung der Zahl. Drei ist ‘011’ in binär und wird durch die Antworten „Nein, Ja, Ja“ im Entscheidungsbaum dargestellt; das ist das gleiche, wie wenn wir ‘Nein’ schreiben für 0 und ‘Ja’ für 1.

Ein Baum, den du für das Alter einer Person verwenden würdest, könnte auf kleinere Zahlen beschränkt sein.

Die Entscheidung über die Buchstaben in einem Satz könnte davon abhängen, was der vorherige Buchstabe war.

Aktivität 6: Das ‚Schiffe versenken' – Suchalgorithmen

Zusammenfassung

Computer werden oft gebraucht, um Informationen in großen Datenmengen zu finden. Dazu müssen schnelle und effiziente Wege für die Durchführung einer Suche beschrieben werden. In dieser Aktivität werden drei unterschiedliche Suchmethoden dargestellt: lineare Suche, binäre Suche und Hashing.

Einfügen in den Lehrplan

- Mathematik: Einführung von Zahlen – Zahlen vergleichen: 'größer als', 'kleiner als' und 'gleich'
- Mathematik: Geometrie – Untersuchen von Formen und Räumen: Koordinaten
- Computer: Algorithmen

Benötigte Kenntnisse

- Logisches Denken

Alter

- 9+

Materialien

Jedes Schulkind benötigt:

- eine Kopie des Spiels ‚Schiffe versenken'

- 1A, 1B für Spiel 1

- 2A, 2B für Spiel 2

- 3A, 3B für Spiel 3

Ein paar Kopien der zusätzlichen Spielblätter 1A', 1B', 2A', 2B', 3A', 3B' können ebenfalls verwendet werden.

Schiffe versenken

Erster Durchlauf

1. Wähle etwa 15 SchülerInnen, die sich vor der Klasse in einer Reihe aufstellen. Jedem der SchülerInnen wird eine Karte mit einer beliebigen Zahl darauf gegeben. Die Zahlen sollen allen anderen SchülerInnen nicht gezeigt werden.
2. Gebe einer anderen Schülerin oder einem anderen Schüler einen Becher mit vier oder fünf Süßigkeiten. Die Süßigkeiten können als Zahlmittel verwendet werden, um eine bestimmte Karte anzusehen. Wird die gesuchte Karte gefunden bevor alle Süßigkeiten verbraucht worden sind, darf das Schulkind den Rest für sich behalten.
3. Wenn gewünscht, die Schritte 1 und 2 wiederholen.
4. Mische die Karten und verteile sie wieder. Jetzt sollen sich die SchülerInnen so aufstellen, dass die Karten aufsteigend verteilt sind. Der Suchvorgang wird erneut durchgeführt.

Da die Zahlen sortiert sind, ist es eine sinnvolle Strategie nur einen Zahlenwert anzugeben, um die Hälfte der SchülerInnen nicht mehr anfragen zu müssen – dazu wird das Schulkind in der Mitte der Reihe aufgefordert, seine Karte vorzuzeigen. Durch Wiederholung dieses Vorgehens sollte die gesuchte Zahl bereits nach Ausgabe von nur drei Süßigkeiten gefunden worden sein. Die Effizienz wird offensichtlich sein.

Aktivität

Die SchülerInnen sollen durch das Spiel ‚Schiffe versenken' das Gefühl dafür bekommen, wie auf einem Computer das Suchen ausgeführt wird. Während des Spiels sollen die SchülerInnen über die Strategien nachdenken, die sie nutzen wollen, um die Schiffe zu finden.

Schiffe versenken – Ein Spiel mit linearer Suche

Folgende Anweisungen den SchülerInnen vorlesen

1. Teilt euch in Zweiergruppen auf. Einer bekommt das Blatt 1A und der (oder die) andere das Blatt 1B. Zeigt eure Blätter aber nicht eurem Partner!
2. Zeichnet beide einen Kreis um ein Schiff eurer Wahl auf der oberen Zeile eures Spielblatts und teilt die jeweilige Zahl eurem Partner mit.
3. Jetzt wechselt euch ab und ratet wo das Schiff eures Partners ist. (Dazu sagst du einen Buchstaben eines Schiffes und dein Partner sagt dir die Zahl des Schiffes für diesen Buchstaben.)
4. Wie viele Schritte hast du gebraucht, um das Schiff deines Partners zu finden? Das ist die Punktzahl des Spiels.

(Die Blätter 1A' und 1B' sind zusätzlich dabei für SchülerInnen, die weiterspielen wollen oder „versehentlich" auf das Blatt des Partners geschaut haben. Die Blätter 2A', 2B' und 3A', 3B' werden bei späteren Spielen gebraucht.)

Anschließende Besprechung

1. Welche Punktzahlen wurden erreicht?
2. Welche mögliche Punktzahl wäre die kleinste und welche die größte?

(Sie liegen natürlich zwischen 1 und 26 unter der Annahme, dass die SchülerInnen keines der Schiffe mehrfach angreifen. Diese Methode wird als ‚lineare Suche' bezeichnet, bei der alle Positionen Schritt für Schritt gewählt werden.)

Schiffe versenken – Ein Spiel mit binärer Suche

Anleitungen

Die Anleitungen für diese Version des Spiels entsprechen der Version des vorherigen Spiels, allerdings sind jetzt die Nummern der Schiffe aufsteigend geordnet. Erkläre das den SchülerInnen bevor sie anfangen.

1. Teilt euch in Zweiergruppen auf. Einer von euch bekommt Blatt 2A und der andere bekommt Blatt 2B. Zeige dein Blatt nicht deinem Partner!
2. Jeder von euch umkreist ein Schiff auf der oberen Zeile eures Spielblatts und sagt die Zahl dem Partner.
3. Nun wechselt euch ab und ratet wo das Schiff eures Partners ist. (Du sagst den Buchstaben eines Schiffes und dein Partner sagt dir die Zahl des Schiffes für diesen Buchstaben.)
4. Wie viele Schritte hast du gebraucht, um das Schiff deines Partners zu finden? Das ist die Punktzahl des Spiels.

Anschließende Besprechung

1. Welche Punktzahlen wurden erreicht?
2. Wie sind die Spieler mit kleiner Punktzahl vorgegangen?
3. Welches Schiff solltest du zuerst wählen? (Das in der Mitte sagt dir, in welcher Hälfte das gesuchte Schiff sein muss.). Welchen Platz würdest du als nächsten wählen? (Auch jetzt ist es wie immer am besten, das mittlere Schiff von den Schiffen zu wählen, bei denen das gesuchte Schiff sein muss.)
4. Wie viele Schritte sind notwendig, wenn du diese Strategie anwendest? (Höchstens fünf.)

Diese Methode nennt man ‚binäre Suche', weil das Problem in zwei Teile zerlegt wird.

Schiffe versenken –
Ein Spiel mit Hashing

Anleitungen

1. Wie bei den letzten Spielen nimmt jeder ein Blatt und sagt seinem Partner die Zahl des gewählten Schiffes.

2. In diesem Spiel findest du heraus, in welcher Spalte (0 bis 9) sich das Schiff befindet. Dazu addierst du zuerst alle Ziffern der Zahl des Schiffes. Die Endziffer der Summe entspricht der Spalte, in der sich das Schiff befindet. Zum Beispiel um den Standort eines Schiffes mit der Zahl 2345 zu bestimmen, addiere die Ziffern 2+3+4+5 und du erhältst 14. Die Endziffer dieser Summe ist 4 - das Schiff muss also in Spalte 4 sein. Wenn du die Spalte weißt, musst du raten, welches der Schiffe in dieser Spalte das gesuchte Schiff ist. Dieses Vorgehen wird ‚Hashing' (deutsch: in Stücke zerlegen) genannt, weil die Ziffern zusammengefasst und einer der Spalten zugeordnet werden.

3. Verwende jetzt die neue Such-Strategie im Spiel. Wenn du das Spiel öfter mit demselben Blatt durchführen möchtest, wähle einfach von verschiedenen Spalten.

(Bitte beachte, dass entgegen den anderen Spielen, die Blätter 3A' und 3B' zusammen benutzt werden müssen, weil das Muster der Schiffe in den Spalten übereinstimmen muss.)

Anschließende Besprechung

1. Sammle und bespreche die Punkte wie vorher.

2. Welche Schiffe sind schnell zu finden? (Die, die allein in ihrer Spalte sind.) Welche Schiffe sind schwerer zu finden? (Die, bei denen sich mehrere Schiffe in derselben Spalte befinden.)

3. Welcher von den drei Suchprozessen ist am schnellsten? Warum?

Was sind die Vorteile jedes der drei Suchverfahren? (Das zweite Verfahren ist schneller als das erste, im ersten Verfahren wird aber die Ordnung der Schiffe nicht gefordert. Das dritte Verfahren ist gewöhnlich schneller als die beiden anderen, kann aber zufällig sehr langsam sein. Im schlimmsten Fall, wenn sich alle Schiffe in derselben Spalte befinden, ist dieses Verfahren so langsam wie das erste.)

Weitere Aktivitäten

1. Lasse die SchülerInnen unter Verwendung der drei Vorlagen ihre eigenen Spiele erstellen. Für das zweite Spiel müssen sie die Zahlen in steigender Ordnung eintragen. Frage sie, wie sie das Hashing-Spiel sehr schwer machen können. (Das Spiel ist am schwersten, wenn alle Schiffe in derselben Spalte sind.) Wie kann man es aber so einfach wie möglich machen? (Man sollte versuchen, in jeder Spalte gleich viele Schiffe einzutragen.)

2. Was würde passieren, wenn das gesuchte Schiff gar nicht vorhanden ist? (In der linearen Suche müssen dafür 26 Schüsse abgegeben werden. In der binären Suche sind zum Beweis fünf Schüsse nötig. Wird Hashing benutzt hängt es davon ab, wie viele Schiffe in der relevanten Spalte sind.)

3. Wie viele Schüsse wären, wenn die binäre Suche verwendet wird, für Hundert Standorte (ungefähr sechs), für Tausend Standorte (ungefähr neun) oder eine Million Standorte (ungefähr neunzehn) notwendig? (Bemerke, dass die Anzahl der Schüsse gegenüber der Anzahl der Schiffe nur langsam zunimmt. Nur ein weiterer Schuss ist jedes Mal notwendig, wenn sich die Anzahl verdoppelt. Es ist also proportional zum Logarithmus der Anzahl der Schiffe.)

Meine Schiffe Anzahl der Schüsse:

9058	7169	3214	5891	4917	2767	4715	674	8088	1790	8949	13	3014
A	B	C	D	E	F	G	H	I	J	K	L	M
8311	7621	3542	9264	450	8562	4191	4932	9462	8423	5063	6221	2244
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Deine Schiffe Anzahl der Schüsse:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

1A

My Ships

Number of Shots Used:

1630	9263	4127	405	4429	7113	3176	4015	7976	88	3465	1571	8625
A	B	C	D	E	F	G	H	I	J	K	L	M
2587	7187	5258	8020	1919	141	4414	3056	9118	717	7021	3076	3336
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Your Ships

Number of Shots Used:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

1B

My Ships

Number of Shots Used:

163	445	622	1410	1704	2169	2680	2713	2734	3972	4208	4871	5031
A	B	C	D	E	F	G	H	I	J	K	L	M
5283	5704	6025	6801	7440	7542	7956	8094	8672	9137	9224	9508	9663
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Your Ships

Number of Shots Used:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

2A

Meine Schiffe

Anzahl der Schüsse:

33	183	730	911	1927	1943	2200	2215	3451	3519	4055	5548	5655
A	B	C	D	E	F	G	H	I	J	K	L	M
5785	5897	5905	6118	6296	6625	6771	6831	7151	7806	8077	9024	9328
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Deine Schiffe

Anzahl der Schüsse:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

2B

Meine Schiffe

Anzahl der Schüsse:

0	1	2	3	4	5	6	7	8	9
A 9047 B 1829	C 3080 D 9994		E 5125 F 1480 G 8212	H 8051 I 1481 J 4712 K 6422	L 7116 M 8944 N 4128	O 6000 P 7432 Q 4110	R 9891 S 1989 T 2050 U 8199	V 4392	W 1062 X 2106 Y 5842 Z 7057

Deine Schiffe

Anzahl der Schüsse:

0	1	2	3	4	5	6	7	8	9
A B C D	E F G	H I J	K	L M N		O P Q	R S T U	V W X	Y Z

3A

Meine Schiffe

Anzahl der Schüsse:

0	1	2	3	4	5	6	7	8	9
A 9308 B 1478 C 8417 D 9434	E 6519 F 2469 G 5105	H 1524 I 8112 J 2000	K 4135	L 9050 M 1265 N 5711		O 4200 P 7153 Q 6028	R 3121 S 9503 T 1114 U 7019	V 2385 W 5832 X 1917	Y 1990 Z 2502

Deine Schiffe

Anzahl der Schüsse:

0	1	2	3	4	5	6	7	8	9
A B	C D		E F G	H I J K	L M N	O P Q	R S T U	V	W X Y Z

3B

Meine Schiffe

Anzahl der Schüsse:

6123	1519	9024	5164	2038	2142	7156	9974	9375	7104	1004	1023	5108
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
1884	3541	5251	4840	3289	3654	2480	5602	8965	4053	2405	2304	1959
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**

Deine Schiffe

Anzahl der Schüsse:

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**

1A′

Meine Schiffe

Anzahl der Schüsse:

2387	9003	3951	5695	1284	4761	7118	1196	1741	3791	3405	3132	6682
A	B	C	D	E	F	G	H	I	J	K	L	M
9493	9864	7359	1250	7036	2916	7562	9299	8910	6713	5173	8617	4222
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Deine Schiffe

Anzahl der Schüsse:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

1B′

Meine Schiffe

Anzahl der Schüsse:

28	326	943	1321	1896	2346	2430	2929	3106	3417	4128	4717	4915
A	B	C	D	E	F	G	H	I	J	K	L	M
5123	5615	6100	7015	7120	7695	7812	8103	8719	9020	9608	9713	9911
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Deine Schiffe

Anzahl der Schüsse:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

2A′

Meine Schiffe

Anzahl der Schüsse:

56	194	306	1024	1510	1807	2500	2812	3011	3902	4178	5902	5915
A	B	C	D	E	F	G	H	I	J	K	L	M
6102	6526	6818	7020	7155	7913	8016	8230	8599	8902	9090	9526	9812
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Deine Schiffe

Anzahl der Schüsse:

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

2B′

Meine Schiffe

Anzahl der Schüsse:

0	1	2	3	4	5	6	7	8	9
A 1982	C 6113		E 9121	H 5009	L 1248	O 2004	R 9369	V 3285	W 9172
B 7841	D 1055		F 1011	I 2651	M 1716	P 5173	S 1321		X 2052
			G 2984	J 1751	N 2148	Q 2806	T 3004		Y 6012
				K 4848			U 7190		Z 7525

Deine Schiffe

Anzahl der Schüsse:

0	1	2	3	4	5	6	7	8	9
A	E	H	K	L		O	R	V	Y
B	F	I		M		P	S	W	Z
C	G	J		N		Q	T	X	
D							U		

3A′

Meine Schiffe

Anzahl der Schüsse:

0	1	2	3	4	5	6	7	8	9
A 8615	E 1361	H 7726	K 3000	L 1814		O 9656	R 6993	V 8208	Y 2917
B 7003	F 7644	I 9003		M 2002		P 4002	S 3121	W 9423	Z 4122
C 1991	G 5600	J 5557		N 8844		Q 1221	T 4300	X 4176	
D 6211							U 1907		

Deine Schiffe

Anzahl der Schüsse:

0	1	2	3	4	5	6	7	8	9
A	C		E	H	L	O	R	V	W
B	D		F	I	M	P	S		X
			G	J	N	Q	T		Y
				K			U		Z

3B′

Worum geht es in dieser Aktivität?

Computer speichern viele Informationen, die sie schnell durchsuchen können müssen. Eines der größten Suchprobleme der Welt steht den Internetsuchmaschinen gegenüber, die Milliarden von Websites in Sekundenbruchteilen durchsuchen müssen. Daten, wie ein Wort, eine Barcodenummer oder der Name eines Autors, nach denen ein Computer suchen muss, werden Suchbegriffe genannt.

Computer können Informationen schnell verarbeiten. Du denkst vielleicht, dass das Suchen immer am Anfang des Speichers beginnt und so lange ausgeführt wird, bis die gesuchte Information gefunden worden ist. So sind wir bei der linearen Suche vorgegangen. Und lineare Suche ist auch bei Computern eine langsame Methode. Stell dir z.B. vor, ein Supermarkt hat 10.000 verschiedene Produkte auf den Regalen verteilt. Wenn der Barcode an der Kasse gescannt wird, muss der Computer 10.000 Zahlen durchsuchen, um die Produktbezeichnung und den Preis zu finden. Selbst wenn es nur eine Tausendstel Sekunde braucht jeden Code zu prüfen, dauert es 10 Sekunden, um die gesamte Liste durchzugehen. Kannst du dir vorstellen wie lange es dauern würde, alle Einkaufswaren einer ganzen Familie zu verarbeiten!

Binäre Suche ist eine bessere Strategie. In dieser Methode sind die Zahlen bereits geordnet. Die Überprüfung des mittleren Wertes der Liste zeigt, welche Hälfte den Suchbegriff enthält. Bezüglich des vorigen Supermarktbeispiels können 10.000 Waren nun in 14 Schritte durchsucht werden, was zwei Hundertstel Sekunden bedeutet – kaum vorstellbar schnell.

Hashing ist die dritte Strategie für Datensuche. Hier wird der Suchbegriff verarbeitet, um genau anzugeben, wo die Informationen gefunden werden können. Wenn z.B. eine Telefonnummer gesucht wird, können alle Ziffern der Nummer addiert und der Rest der Summe geteilt durch 11 verwendet werden. Insofern ist Hashing hier ähnlich wie die Prüfziffer, die in Aktivität 4 betrachtet wurde – nur wenige Daten, deren Werte von den anderen bearbeiteten Daten abhängen. Normalerweise findet der Computer sofort die gesuchten Daten. Es ist sehr unwahrscheinlich, dass mehrere Schlüssel auf denselben Speicherbereich zeigen. Ist das der Fall, durchsucht der Computer alle möglichen Fälle bis der gesuchte Wert gefunden worden ist.

Meistens benutzen ComputerprogrammiererInnen eine Variante der Hashing-Suchstrategie, falls die Daten nicht geordnet gespeichert werden müssen, oder ein zu langsamer Suchablauf inakzeptabel ist.

Aktivität 7: Vom Leichtesten zum Schwersten – Sortieralgorithmen

Zusammenfassung

Häufig verwendet man Computer dazu, Listen von Elementen in eine bestimmte Ordnung zu bringen. So kann man beispielsweise Namen alphabetisch sortieren, Verabredungen nach Datum, oder Zahlen in auf- oder absteigender Reihenfolge sortieren. Wir interessieren uns dafür wie man Elemente sortiert, um Elemente beim Suchen einfacher finden zu können. Zudem ist das Aufspüren spezieller Werte (wie beispielsweise das größte oder kleinste Element) nach dem Sortieren ganz einfach. Wenn man beispielsweise die Noten einer Klasse aufsteigend sortiert, ist es einfach die höchste und die tiefste Note zu finden; diese findet man am Anfang beziehungsweise am Ende der sortierten Liste.

Allerdings erhalten wir die Ordnung nicht gratis; wir zahlen dafür mit Zeit. Es gibt diverse Methoden, die verschieden lange dauern. Sie alle haben den gleichen Effekt: Sie sortieren die Elemente. Da dies jedoch bei den verschiedenen Methoden nicht gleich lange dauert, sind wir daran interessiert, die beste Methode zu finden. Wählt man die falsche, kann es unter Umständen sehr lange dauern bis alle Zahlen korrekt angeordnet sind, und das auch auf einem schnellen Computer. In dieser Aktivität sollen Kinder verschiedene Sortierverfahren kennenlernen und deren Geschwindigkeit vergleichen.

Einfügen in den Lehrplan

- Mathematik: Wiegen, Zählen, Vergleichen.
- Informatik: Algorithmen

Benötigte Kenntnisse

- Wie benutzt man eine Waage
- Was heißt es, Elemente zu ordnen
- Wie vergleicht man Zahlen

Alter

- 8+

Materialien

Jede Gruppe wird folgende Materialien benötigen:

- 8 Behälter, alle gleich groß, aber verschieden schwer
- Eine Waage
- Arbeitsblatt: Gewichte sortieren (Seite 80)
- Arbeitsblatt: Teile und Herrsche (Seite 81)

Vom Leichtesten zum Schwersten

Diskussion

Sortieren gehört zu den Sachen, die von Computern sehr oft ausgeführt werden. Es ist wichtig sich im Klaren zu sein, dass es viele Situationen gibt, in welchen wir daran interessiert sind, eine Menge von Daten zu ordnen. In einem Brainstorming soll die Klasse Situationen zusammentragen, in welchen eine Ordnung hilfreich ist. Eine Klassendiskussion soll darauf folgen mit der Frage, was wäre, wenn in diesen Situationen keine geordneten Daten vorliegen würden (anhand einiger der vorher zusammengetragenen Situationen, in welchen eine Ordnung der Daten nützlich ist).

Normalerweise vergleicht ein Computer jeweils nur zwei Werte miteinander, da zeitweise eine zu große Menge von Daten vorliegt, um sie sich alle merken zu können. Die Aktivität auf den folgenden Seiten verwendet diese Einschränkung und gibt den Kindern so ein Verständnis dafür, wie das Sortieren auf dem Computer funktioniert.

Vorgehen

1. Die Kinder in Gruppen aufteilen.
2. Jede Gruppe erhält:

    i) Die Aufgabenstellung (Seite 80)

    ii) Acht Behälter mit Gewichten

    iii) Eine Waage

3. Die Kinder führen die Aktivität aus.
4. Die Resultate und Erkenntnisse werden in der Klasse besprochen.

Arbeitsblatt: Gewichte sortieren

Ziel: Finde die beste Methode eine Menge von Elementen mit unbekannten Gewichten in aufsteigender Reihenfolge zu sortieren.

Was du dazu brauchst: Sand oder Wasser als Gewichte, 8 identische Büchsen und eine Waage.

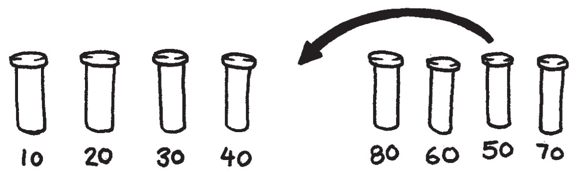
Vorgehen:

1. Fülle jede Büchse mit Wasser oder Sand. Achte darauf, dass sich alle Büchsen dicht verschließen lassen.
2. Mische die Büchsen, sodass du nicht mehr weißt welche Büchse welche ist.
3. Finde die leichteste Büchse. Wie kann man das am einfachsten machen?
   Beachte: Es ist nicht erlaubt die Waage dazu zu verwenden, mehr als zwei Büchsen miteinander zu vergleichen
4. Wähle zufällig drei Gewichte aus und sortiere sie nach aufsteigendem Gewicht (links die leichteste Büchse, rechts die schwerste der drei Büchsen). Wie bist du vorgegangen? Wie oft muss man mit der Waage zwei Gewichte vergleichen, um die drei Büchsen korrekt anzuordnen?
5. Sortiere nun alle Objekte in aufsteigender Reihenfolge, links das leichteste Gewicht, rechts das schwerste Gewicht.

Wenn du fertig bist, kannst du deine Lösung kontrollieren, indem du alle benachbarten Büchsen nochmals vergleichst.

Sortieren durch Auswählen

Eine erste Methode, die wir nun untersuchen werden, heißt Sortieren durch Auswählen. Diese funktioniert folgendermaßen: Zuerst suchen wir unter allen Elementen das Leichteste und platzieren es ganz links. Dann suchen wir wiederum das Leichteste aus denjenigen Elementen, die noch übrig sind. So geht das weiter, bis keine Büchsen mehr übrig sind.



Zähle wie oft du die Waage für einen Vergleich zweier Büchsen verwendet hast.

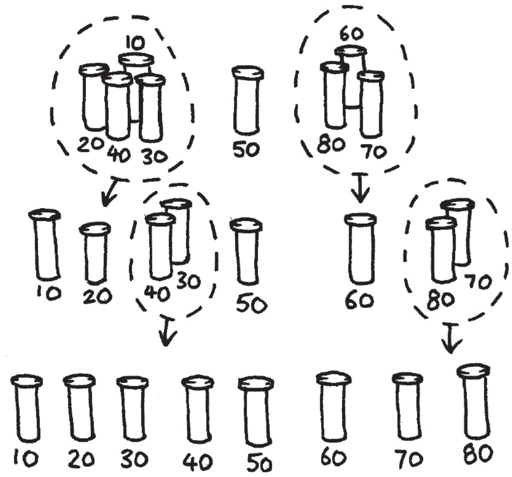
Zugabe für ExpertInnen: Zeige wie man berechnen kann, wie viele Vergleiche man auf diese Weise benötigt, wenn man acht Objekte sortieren will. Wie sieht es für neun Objekte aus? Oder 20?

Arbeitsblatt: Teile und Herrsche

Quicksort

Quicksort ist um einiges schneller als Sortieren durch Auswählen, besonders für große Mengen von Elementen. Es handelt sich sogar um eine der besten Methoden, die heute bekannt sind. Und so funktioniert es:

1. Wähle ein zufälliges Element aus und platziere es auf der einen Seite der Waage.
2. Danach vergleichst du alle anderen Elemente mit dem soeben Gewählten. Diejenigen, die leichter sind als das Element legst du links hin, die anderen rechts, und das Element selbst zum Schluss in die Mitte. (Beachte: Es kann vorkommen, dass sehr viel weniger Elemente auf einer Seite sind, als auf der anderen.)
3. Wiederhole die obigen zwei Anweisungen für die beiden Teile. Das Objekt, welches du zuvor in die Mitte gestellt hast, musst du jedoch nicht mehr wiegen. Es bleibt in der Mitte stehen.
4. Auf die entstehenden Untergruppen wenden wir wiederum die ersten zwei Anweisungen an, bis alle Elemente verarbeitet wurden und es demzufolge keine zwei Elemente zum Vergleichen gibt. Nun sind die Elemente aufsteigend angeordnet.



Wie oft hast du bei dieser Methode die Waage benutzt?

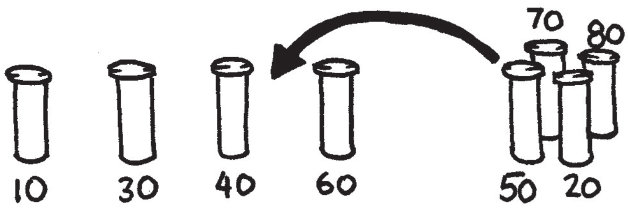
Du solltest festgestellt haben, dass Quicksort effizienter arbeitet als Sortieren durch Auswählen, außer du hast bei jedem Schritt immer das aktuell schwerste Element gewählt. Wenn du jedes Mal zufällig das mittlere Gewicht gewählt hast, hast du 14 Mal die Waage benutzt, was wesentlich besser ist, verglichen zu den 28 Vergleichen bei Sortieren durch Auswählen. Auf jeden Fall kann Quicksort nie schlechter sein als Sortieren durch Auswählen. Möglicherweise kann es aber viel besser sein!

Zugabe für ExpertInnen: Wie viele Vergleiche würde Quicksort brauchen, wenn jedes Mal zufällig das leichteste Element gewählt würde?

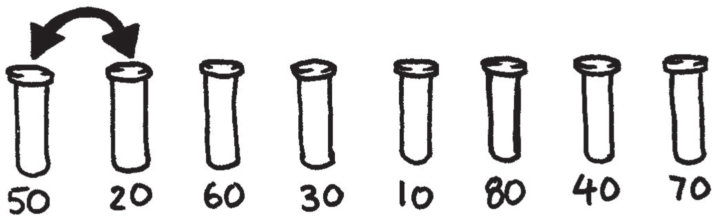
Variationen und Erweiterungen

Es wurden diverse Methoden entwickelt, mit welchen sortiert werden kann. So könnte man die Gewichte auf folgende Weise sortieren:

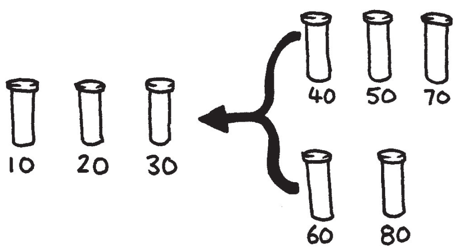
Sortieren durch Einfügen: Diese Methode entnimmt jedes Objekt aus einer unsortierten Menge und ordnet es an der korrekten Stelle in eine bereits sortierte Menge ein. (Siehe das Bild unten). Mit jeder Einfügeoperation wird die Menge der unsortierten Elemente kleiner, bis schließlich alle Elemente aufsteigend sortiert sind.



Bubblesort: Diese Methode sortiert die Elemente, indem sie immer wieder durch die Liste durchgeht und alle benachbarten Elemente tauscht, die falsch herum da stehen. Die Liste ist sortiert, sobald es keine Vertauschungen benachbarter Elemente mehr gibt. Diese Methode ist nicht sonderlich schnell, es gibt jedoch Menschen, die diese Methode einfacher verstehen als die anderen Methoden.



Mergesort: Dies ist eine andere Methode, die das Prinzip ‚Teile und Herrsche' verwendet (wie Quicksort). Zuerst wird die Liste zufällig in zwei Teile der gleichen Größe aufgeteilt (oder fast der gleichen Größe, falls es eine ungerade Anzahl Elemente gibt). Die beiden Hälften werden sortiert und wieder zusammengefügt. Das Zusammenfügen zweier Listen ist einfach: Wir suchen wiederholt das leichteste Element und nehmen es aus der Menge raus, bis keine Elemente mehr übrig sind. In der Abbildung unten steht eine 40g Büchse und eine 60g Büchse zur Auswahl. Wir fügen als nächstes also die 40g Büchse ein. Wie aber erhalten wir zwei sortierte Teile? Einfach, wir wenden Mergesort auf die beiden Teile an! Irgendwann erhalten wir Teile, die nur eine Büchse enthalten. Eine solche Menge ist bereits sortiert.



Worum geht es in dieser Aktivität?

Es ist wesentlich einfacher Informationen in einer geordneten Liste zu finden, als wenn man sie in einer ungeordneten Liste suchen müsste. Telefonbücher, Wörterbücher und Verzeichnisse sind alphabetisch geordnet und das Leben wäre wesentlich weniger bequem, wenn sie es nicht wären. Wenn eine Liste von Zahlen (wie zum Beispiel eine Liste mit Ausgaben) geordnet vorliegt, ist es einfach die Extremen zu sehen, weil sie sich ganz am Anfang oder ganz am Schluss der Liste befinden, während sie in unsortierten Listen überall vorkommen können. Auch doppelte Einträge findet man einfach, da diese in sortierten Listen direkt nebeneinander liegen.

Computer verbringen einen großen Teil der Zeit damit, Dinge zu ordnen. Also ist es für InformatikerInnen von Interesse dies schnell und gut zu machen. Einige der langsameren Methoden, wie beispielsweise Sortieren durch Einfügen, Sortieren durch Auswählen oder Bubblesort, können in gewissen Situationen sehr nützlich sein, doch in den meisten Fällen verwendet man ein schnelles Verfahren, wie zum Beispiel Quicksort.

Quicksort verwendet ein Konzept, das man Rekursion nennt. Das bedeutet, dass wir die Liste immer wieder in kleinere Teile unterteilen und auf diesen kleineren Teilen genau dasselbe tun wie wir es vorher beim größeren Teil gemacht haben. Diesen Ansatz im Speziellen nennt man ‚Teile und Herrsche'. Die Liste wird immer wieder unterteilt, bis wir schließlich fähig sind (wenn die Liste klein genug ist) deren Ordnung zu bestimmen. Im Falle von Quicksort werden die Listen unterteilt bis sie nur noch ein Element enthalten, da es einfach ist eine Menge mit nur einem Element zu sortieren. Das klingt zwar kompliziert, verhilft uns aber in der Praxis dazu, wesentlich schneller zum Ziel zu kommen als mit anderen Methoden.

Lösungen und Tipps

1. Am einfachsten ist es, jedes Element der Reihe nach anzuschauen und sich jeweils zu merken wo sich das momentan leichteste Element befindet, wenn wir aus einer Menge von Elementen das Leichteste bestimmen wollen. Das heißt, wir wählen zwei Elemente und behalten das Leichtere davon auf der Waage. Das andere legen wir weg und nehmen stattdessen ein neues Element hinzu um wieder gleich vorzugehen. Das machen wir, bis alle Elemente verglichen wurden und wir das leichteste Element noch auf der Waage haben.

2. Vergleiche die Gewichte auf der Waage. Wir können drei Elemente ordnen, indem wir die Waage dreimal benutzen (in manchen Fällen reichen sogar zwei). Die Kinder müssen merken, dass Gewichtsvergleiche transitiv sind (wenn also Gewicht a leichter ist als Gewicht b und Gewicht b leichter als Gewicht c, dann ist auch das Gewicht a leichter als das Gewicht c).

Für ExpertInnen:

Hier ein Tipp, wie man die Anzahl Vergleiche von der Methode Sortieren durch Auswählen einfach aufsummieren kann:

Um das Minimum von zwei Objekten zu bestimmen, benötigst du einen Vergleich. Drei Objekte benötigen zwei, vier brauchen drei und so weiter. Um also acht Elemente zu sortieren benötigt Sortieren durch Auswählen sieben Vergleiche um das erste Element zu finden, dann sechs für das nächste, dann fünf, vier, drei zwei und einen Vergleich. Das ergibt:

7 + 6 + 5 + 4 + 3 + 2 + 1 = 28 Vergleiche.

Für n Objekte sind es 1 + 2 + 3 + 4 +... + n – 1 Vergleiche.

Wenn wir dies aufsummieren wollen, können wir die einzelnen Summanden einfach umordnen. Zum Beispiel: Die Summe 1+2+3+...+19 kann man umordnen zu:

(1 + 19) + (2 + 18) + (3 + 17) + (4 + 16) + (5 + 15) +

(6 + 14) + (7 + 13) + (8 + 12) + (9 + 11) + 10

= 9 × 20 + 10

= 190

Allgemein ist die Summe

$$1 + 2 + 3 + 4 \ldots + n - 1 = n(n - 1)/2.$$

Aktivität 8: Schneller fertig sein – Sortiernetzwerk

Zusammenfassung

Obwohl Computer schnell sind, gibt es Grenzen, wie schnell sie Probleme lösen können. Eine Möglichkeit, Dinge zu beschleunigen, ist mehrere Computer zu verwenden um verschiedene Teile eines Problems zu lösen. In dieser Aktivität verwenden wir Sortiernetzwerke, die mehrere Sortiervergleiche gleichzeitig ausführen.

Einfügen in den Lehrplan

- Mathematik: Einführung von Zahlen – Zahlen vergleichen: 'größer als', 'kleiner als'

Benötigte Kenntnisse

- Vergleiche
- Ordnen
- Entwicklung von Algorithmen
- Gemeinsame Problemlösung

Alter

- 7+

Materialien

Gruppenaktivitäten im Freien

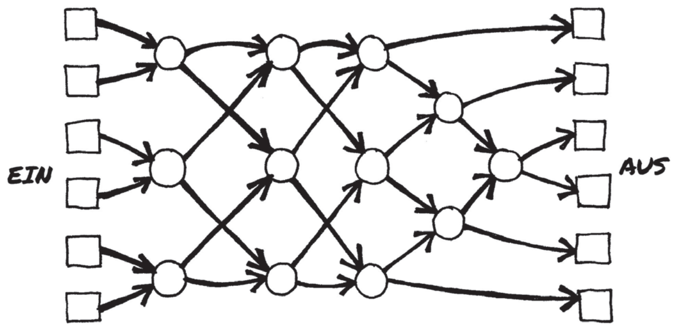
- Kreide
- Zwei Sätze mit je sechs Blättern

  Originalkopie ‚Sortiernetzwerk' (Seite 87) auf Blatt drucken und ausschneiden

- Stoppuhr

Sortiernetzwerke

Vor der Aktivität: Benutze die Kreide und male dieses Netzwerk auf den Boden.

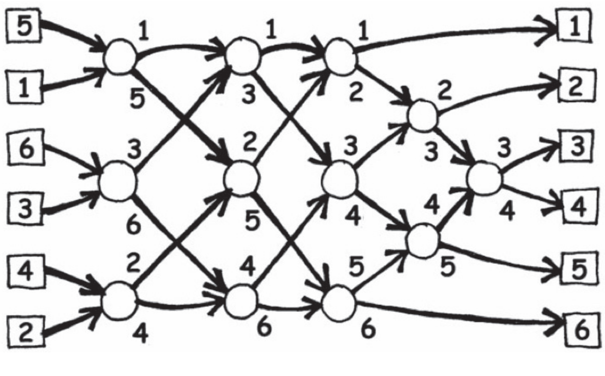


Anleitungen für die SchülerInnen

Diese Aktivität wird euch zeigen, wie Computer unter Verwendung des sogenannten Sortiernetzwerks, zufällig gewählte Zahlen ordnen.

1. Teilt euch in Gruppen mit jeweils sechs Mitgliedern auf. Nur eine Gruppe wird jeweils das Netzwerk verwenden.
2. Jedes Teammitglied wählt ein nummeriertes Blatt.
3. Jedes Teammitglied positioniert sich in einem der Startpunkte (Quadrate) auf der linken Seite – markiert durch"EIN". Eure Zahlen sollen ungeordnet verteilt sein.
4. Geht die markierten Linien entlang und wartet auf jemanden, wenn ihr einen Kreis erreicht habt.
5. Wenn ein anderes Teammitglied in eurem Kreis ankommt, vergleicht eure Blätter. Derjenige von euch mit der kleineren Zahl verlässt den Kreis nach links; der mit der größeren Zahl benutzt die Abzweigung nach rechts.
6. Seid ihr in der richtigen Reihenfolge, wenn ihr an das andere Ende des Feldes ankommt?

Falls ein Team einen Fehler macht, beginnt das Team nochmals von vorn. Prüft, ob ihr die Ausführung der Regel in den Kreisen verstanden habt und bei kleineren Zahlen den linken Weg, sowie bei größeren Zahlen den rechten Weg genommen habt. Hier ein Beispiel:



Originalkopie: Sortiernetzwerk

1	2
3	4
5	6

156	221
289	324
422	499

Variationen

1. Wenn die SchülerInnen mit dieser Aktivität vertraut sind, verwende eine Stoppuhr, um zu messen wie lang jedes Team braucht um durch das Netzwerk zu kommen.

2. Verwende Blätter mit größeren Zahlen (z.B. die dreistelligen Zahlen auf der Originalkopie).

3. Erstelle Blätter mit noch größeren Zahlen, um den Aufwand beim Vergleich zu erhöhen oder benutze Wörter und vergleiche sie alphabetisch.

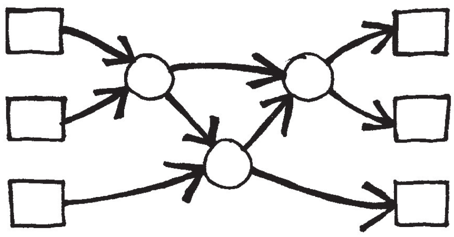
4. Die Aktivität kann auch als Übung mit anderen Objekten verwendet werden, wie z.B. im Bereich Musik, wo Noten auf den Blättern aufgedruckt sind, die von der tiefsten zur höchsten oder von der kürzesten zur längsten Note sortiert werden sollen.

Weitere Aktivitäten

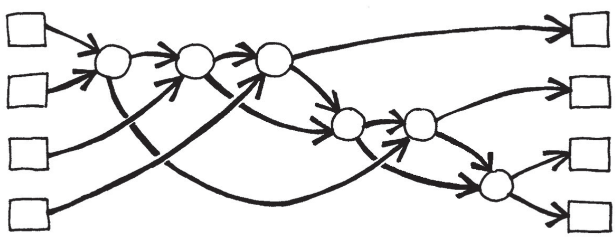
1. Was passiert, wenn die kleinere Zahl nach rechts anstelle von links und umgekehrt verteilt wird? (Die Zahlen werden in umgekehrter Reihenfolge sortiert.)

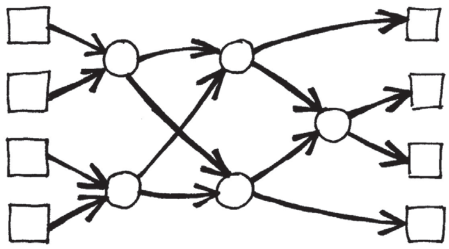
Wird es funktionieren, wenn das Netzwerk umgekehrt benutzt wird? (Es wird nicht unbedingt funktionieren und die SchülerInnen sollten in der Lage sein, ein Beispiel für eine Eingabe zu finden, die in der falschen Reihenfolge herauskommt.)

2. Versuchen Sie kleinere oder größere Netzwerke zu entwerfen. Hier ist ein Beispiel für ein Netzwerk, das drei Zahlen sortiert. Die SchülerInnen sollten selbst solche Beispiele erstellen.



Unten sind zwei verschiedene Netzwerke dargestellt, die jeweils vier Eingaben sortieren. Welches Netzwerk ist schneller?



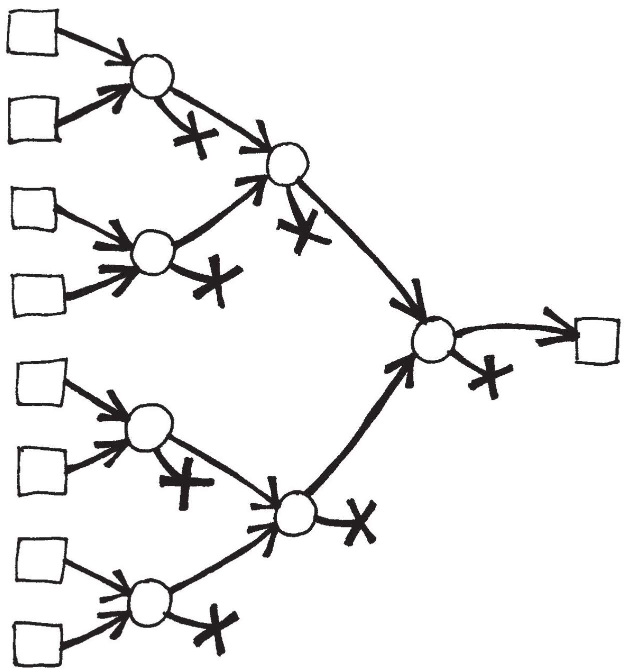


(Das zweite ist schneller. Während beim ersten alle Vergleiche seriell (eins nach dem anderen) ausgeführt werden, wird es im zweiten Fall zum Teil gleichzeitig durchgeführt.)

Das erste Netzwerk ist ein Beispiel für eine serielle Verarbeitung, während im zweiten Fall Parallelverarbeitung verwendet wird, die schneller läuft.

3. Versuchen Sie ein größeres Sortiernetzwerk zu erstellen.

4. Netzwerke können auch verwendet werden, um minimale oder maximale Eingabewerte zu finden. Als Beispiel wird ein Netzwerk mit acht Eingaben gezeigt, dessen einziger Output dem minimalen Eingabewert entspricht (die anderen Eingabewerte werden in Sackgassen des Netzwerks abgelegt.)



5. Welcher Ablaufprozess des täglichen Lebens könnte bzw. könnte nicht durch Parallelverarbeitung beschleunigt werden? Zum Beispiel wäre das Kochen eines Gerichtes viel langsamer, wenn man sich jeweils auf nur eine Beilage konzentriert und so alle Bestandteile des Gerichts erst nach und nach zubereitet werden. Können Aufträge schneller erledigt werden, wenn mehrere Personen angestellt werden? Bei welchen Aufträgen ist das nicht möglich?

Worum geht es in dieser Aktivität?

Da wir Computer immer häufiger verwenden, möchten wir, dass sie Informationen so schnell wie möglich verarbeiten.

Eine Möglichkeit Computer zu beschleunigen ist es, Programme zu schreiben, die weniger Rechenschritte ausführen (das wurde in den Aktivitäten 6 und 7 gezeigt).

Eine andere Möglichkeit, Probleme schneller zu lösen, ist es mehrere Computer zu verwenden, die verschiedene Teile derselben Aufgabe gleichzeitig bearbeiten. Zum Beispiel das Sechs-Zahlen-Sortiernetzwerk: Obwohl insgesamt 12 Vergleiche zur Sortierung notwendig sind, können bis zu drei davon gleichzeitig ausgeführt werden. Das bedeutet, dass insgesamt nur die Zeit für fünf Vergleichsschritte benötigt wird. Dieses Parallelnetzwerk sortiert die Liste mehr als doppelt so schnell wie ein System, das pro Schritt nur einen Vergleich durchführen kann.

Nicht alle Aufgaben können durch Parallelverarbeitung schneller erledigt werden. Als Analogie dazu stellen Sie sich vor, eine Person gräbt einen zehn Meter langen Graben. Wenn zehn Personen jeweils einen Meter des Grabens ausgraben würden, könnte die Aufgabe viel schneller erledigt werden. Jedoch könnte die gleiche Strategie nicht auf einen Graben angewendet werden, der zehn Meter tief sein soll - der zweite Meter ist nicht zugänglich, bis der erste Meter ausgegraben worden ist. ComputerwissenschaftlerInnen sind ständig dabei, die besten Wege zu suchen, um solche Probleme durch Computer mithilfe von Parallelverarbeitung zu lösen.

Aktivität 9: Die Schlammstadt – Minimale Spannbäume

Zusammenfassung

Unsere Gesellschaft ist durch mehrere Netzwerke verbunden: Telefonnetze, Versorgungsnetze, Computernetze und Straßennetze. Für ein bestimmtes Netzwerk gibt es in der Regel eine gewisse Auswahl, wo die Straßen, Kabel oder Funkverbindungen platziert werden können. Wir müssen Wege finden, um Objekte in einem Netzwerk effizient zu verbinden.

Einfügen in den Lehrplan

- Mathematik: Geometrie – Untersuchung von Form und Raum: Bestimmung des kürzesten Weges auf einer Karte

Benötigte Kenntnisse

- Problemlösung

Alter

- 9+

Materialien

Jede Schülerin und jeder Schüler benötigt:

- Arbeitsblatt: Das Schlammstadt-Problem (Seite 93)
- Spielmarken oder Quadrate aus Karton (ungefähr 40 pro SchülerIn)

Die Schlammstadt

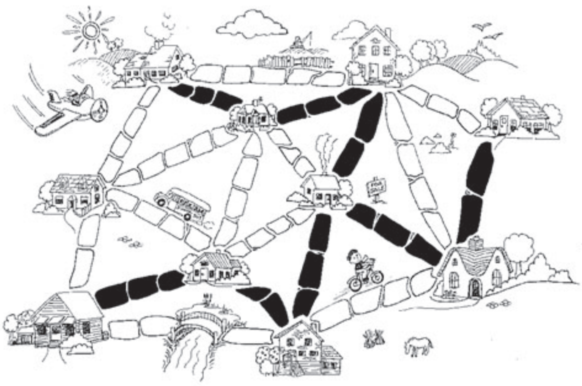
Einführung

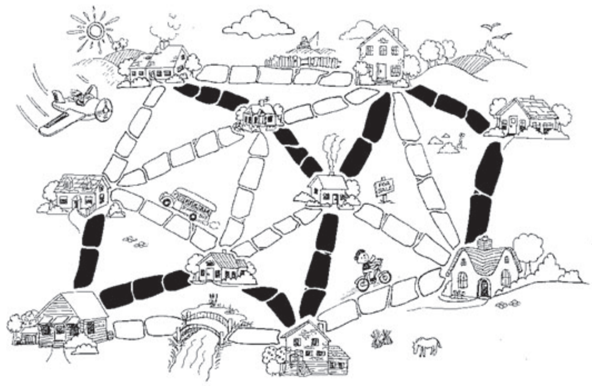
Diese Aktivität zeigt, wie Computer benutzt werden um die beste Lösung für reale Probleme, z.B. das Verlegen von Stromleitungen zwischen Häusern, zu finden. Die SchülerInnen sollen jetzt das Arbeitsblatt auf Seite 93 benutzen, auf dem das Schlammstadt-Problem beschrieben wird.

Anschließende Besprechung

Verteile die Lösungen, die die SchülerInnen gefunden haben. Welche Strategien haben die SchülerInnen verfolgt?

Eine gute Strategie, die beste Lösung zu finden, ist es mit einer leeren Karte anzufangen und schrittweise Spielmarken hinzuzufügen, bis alle Häuser verbunden sind. Dabei werden Wege in zunehmender Reihenfolge ihrer Länge hinzugefügt; Häuser, die bereits über einen Weg verbunden sind, werden nicht erneut beigefügt. Es sind verschiedene Lösungen möglich, wenn die Reihenfolge geändert wird, in der Wege gleicher Länge hinzugefügt werden. Zwei mögliche Lösungen werden im Folgenden dargestellt:





Eine andere Strategie ist es, am Anfang alle Wege zu bepflastern und dann solche Wege wegzunehmen, die nicht gebraucht werden. Das ist jedoch viel aufwendiger!

Wo würdest du Netzwerke in der Realität finden?

InformatikerInnen bezeichnen die Darstellung dieser Netzwerke als „Graphen“. In der Praxis werden Netzwerke durch einen Graphen dargestellt um Probleme zu lösen, wie z.B. das Entwerfen des besten Straßennetzes zwischen Städten oder Flugzeugflüge zu verschiedenen Destinationen in einem Land.

Es gibt noch viele andere Algorithmen, die in Graphen angewendet werden können, wie das Finden des kürzesten Weges zwischen zwei Punkten oder der kürzesten Strecke, die alle Punkte enthält.

Arbeitsblatt: Das Schlammstadt-Problem

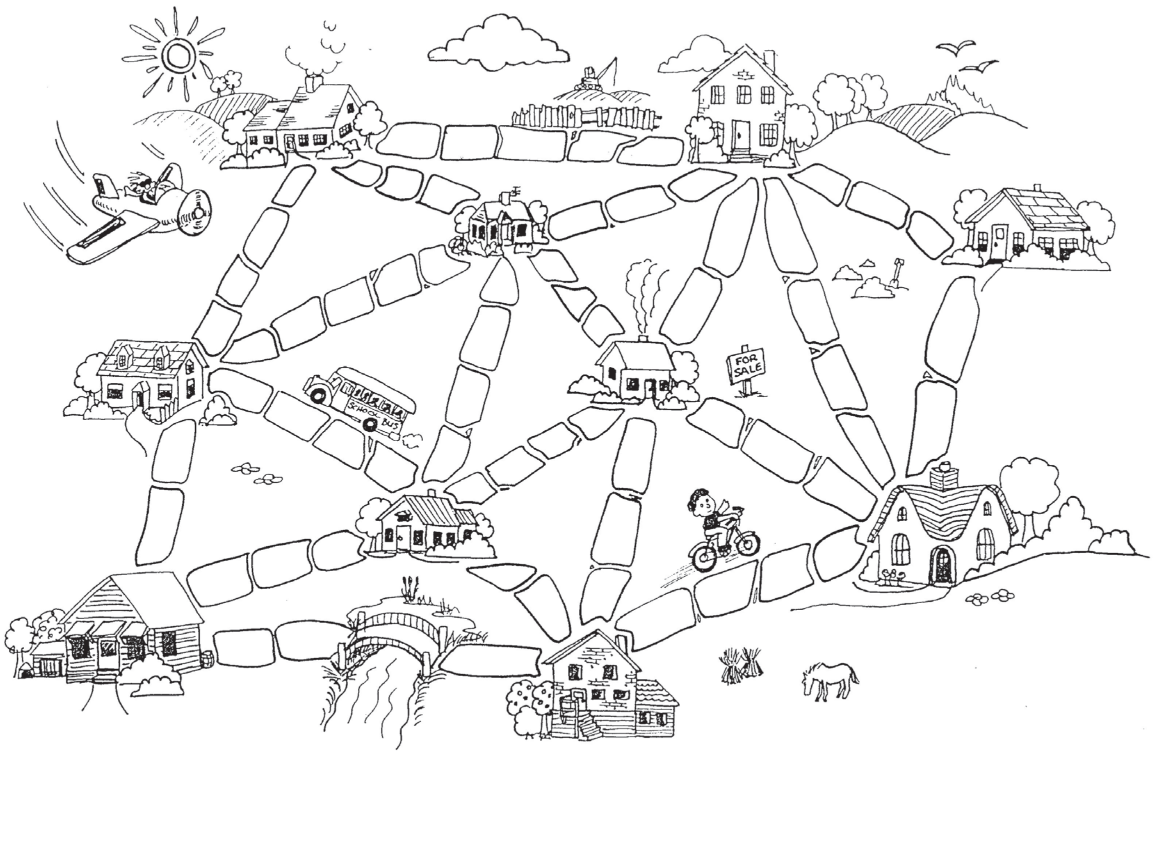
Es gab einmal eine Stadt, in der es keine Straßen gab. Die Stadt zu erkunden war besonders nach Regenfällen schwierig, weil der Boden sehr schlammig wurde - Autos steckten im Schlamm fest und die Leute bekamen dreckige Stiefel. Der Bürgermeister der Stadt entschied, dass einige der Straßen gepflastert werden sollten, aber nicht mehr Geld als nötig dafür ausgegeben werden sollte, weil die Stadt auch vorhatte, ein Schwimmbad zu bauen. Der Bürgermeister gab daher zwei Bedingungen an:

1. Genug Straßen müssen gepflastert werden, sodass es für jeden möglich ist, von seinem Haus aus nur auf gepflasterten Straßen zu jedem anderen Haus gehen zu können und

2. das Pflastern sollte so wenig wie möglich kosten.

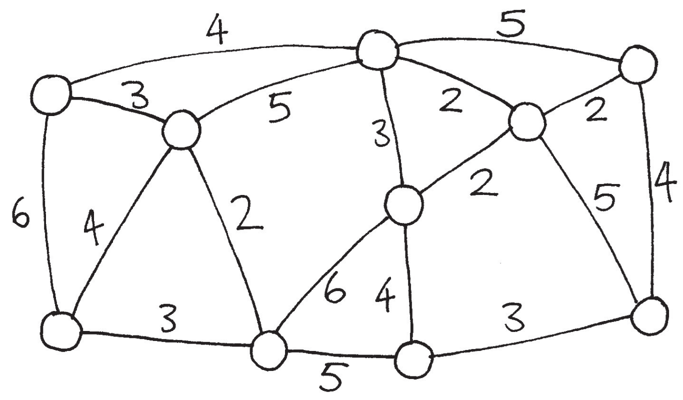
Unten ist der Grundriss der Stadt dargestellt. Die Anzahl der Pflastersteine zwischen jedem Haus stellt die Kosten für die Pflasterung dieser Strecke dar. Finde die beste Route, die alle Häuser verbindet, aber bei der du so wenig Spielmarken (Pflastersteine) wie möglich benutzen musst.

Welche Strategien hast du zur Lösung des Problems benutzt?



Variationen und Erweiterungen

Hier ist eine andere Möglichkeit zur Darstellung von Städten und Straßen:



Die Häuser werden durch Kreise (oder Punkte), die schlammigen Straßen durch Linien und die Länge einer Straße wird durch die Zahl an der entsprechenden Linie dargestellt.

InformatikerInnen und MathematikerInnen benutzen diese grafische Abbildung oft zur Darstellung des Problems; sie nennen es einen Graphen. Das kann verwirren, weil ein „Graph" in der Statistik manchmal als ein Diagramm zur Darstellung numerischer Daten, wie z.B. das Balkendiagramm, verwendet wird. Graphen in der Informatik werden aber nicht so verstanden; die Länge muss nicht maßstäblich gezeichnet werden.

Folge einigen schwierigen Wegen auf den gepflasterten Straßen deines eigenen Graphen und probiere diese Wege auch auf den Graphen deiner Freunde.

Findest du eine Regel um zu beschreiben, wie viele Straßen oder Verbindungen für eine beste Lösung notwendig sind? Ist das abhängig von der Anzahl der Häuser in der Stadt?

Worum geht es in dieser Aktivität?

Angenommen du entwirfst einen Plan, wie die Versorgung von Strom, Gas oder Wasser zu einem neuen Haus sichergestellt werden soll. Ein Netz von Drähten oder Rohren wird benötigt, um alle Häuser mit dem entsprechenden Dienstleistungsunternehmen zu verbinden. Jedes Haus muss mit dem Netzwerk an einer Stelle verbunden sein, aber der Weg, der die Dienstleistung zu dem betroffenen Haus bringt, spielt keine wesentliche Rolle, solange der Anschluss existiert.

Die Aufgabe, ein Netz mit einer minimalen Gesamtlänge zu entwerfen, heißt das *minimale Spannbaum-Problem*.

Minimale Spannbäume sind nicht nur in Gas- und Stromnetzen nützlich; sie helfen auch Probleme in Computernetzwerken, Telefonnetzwerken, Ölpipelines und für Fluglinien zu lösen. Allerdings muss bei einer Entscheidung für eine Reise über die beste Route, vom Anbieter berücksichtigt werden, wie angenehm die Reise für die Reisenden ist und wie viel es kosten wird. Niemand will Stunden in einem Flugzeug verbringen, das einen langen Umweg in ein anderes Land wählt, nur weil es billiger ist. Der Schlammstadt-Algorithmus kann für diese Netzwerke nicht viel genutzt werden, da er hier nur die Gesamtlänge der Straßen oder Flugwege minimiert.

Minimale Spannbäume sind auch als einer der Lösungsschritte anderer Graphenprobleme, wie für das ‘Problem des Handlungsreisenden’ (Travelling Salesman Problem, TSP) nützlich, wo versucht wird den kürzesten Weg zu finden, der jeden Punkt im Netzwerk beinhaltet.

Es gibt effiziente Algorithmen (Methoden) zur Lösung minimaler Spannbaum-Probleme. Eine einfache Methode für eine optimale Lösung ist Kruskals Algorithmus (J.B. Kruskal, publiziert 1956): Beginne mit einem Punkt (Knoten) des Graphen und füge Linien (Kanten) in zunehmender Reihenfolge der Größe hinzu, wenn dadurch ein weiterer Teil des Netzwerks hinzukommt, der noch nicht mit dem Graphen verbunden ist.

Für viele Graphenprobleme, einschließlich TSP, haben InformatikerInnen noch keine schnelle Methode entdeckt, um dadurch die besten möglichen Lösungen zu finden.

Lösungen und Tipps

Variationen und Erweiterungen (Seite 94)

Wie viele Straßen oder Verbindungen sind nötig, wenn es n Häuser in der Stadt gibt? Es stellt sich heraus, dass eine optimale Lösung immer genau n-1 Verbindungen hat, da dies immer ausreichend ist, um die n Häuser miteinander zu verbinden. Beim Hinzufügen eines weiteren Hauses müssten sonst unnötig viele alternative Straßen zwischen den Häusern gebaut werden.

Aktivität 10: Das Orangenspiel – Routing und Stillstand in Netzwerken

Zusammenfassung

Wenn viele Menschen einen Gegenstand benutzen (etwa Autos auf den Straßen oder Nachrichten, die durch das Internet übermittelt werden), kann ein „Stillstand" vorkommen. Eine Art der Zusammenarbeit ist notwendig, um dies zu vermeiden.

Einfügen in den Lehrplan

- Mathematik: Entwicklung von Logik und Argumentation

Benötigte Kenntnisse

- Kooperative Problemlösung
- Logisches Denken

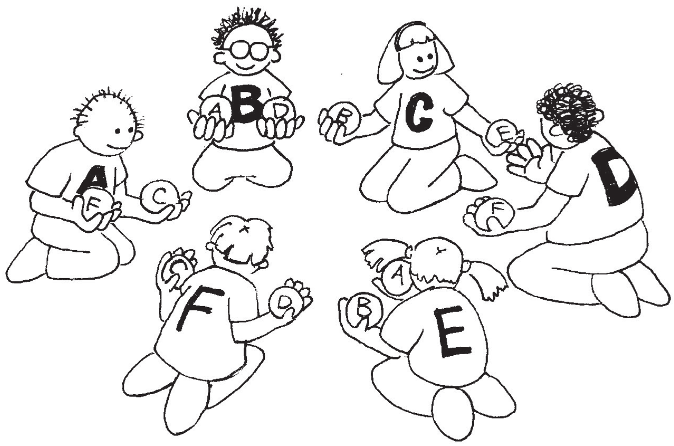
Alter

- 9+

Materialien

Jede Schülerin und jeder Schüler benötigt:

- Zwei Orangen oder Tennisbälle, die mit demselben Buchstaben gekennzeichnet sind, oder zwei Obststücke (am besten künstliche Früchte) für jeden
- Ein Namensschild oder ein Aufkleber mit ihrem Buchstaben darauf oder einen farbigen Hut, ein Abzeichen oder ein T-Shirt, das ihrem Gegenstand (Orange, Tennisball o.ä.) entspricht



Das Orangenspiel

Anleitung

Dies ist ein Spiel hinsichtlich kooperativer Problemlösung. Für alle TeilnehmerInnen ist es das Ziel, am Ende die Orangen mit seinem/ihrem Kennzeichen in den Händen zu halten.

1. Gruppen mit fünf oder mehr SchülerInnen sitzen in einem Kreis.

2. Die SchülerInnen werden mit einem Buchstaben des Alphabets markiert (unter Verwendung von Namensschildern oder Aufklebern) oder jedem Schulkind wird eine Farbe zugeordnet (gekennzeichnet durch einen Hut oder der Farbe der Kleidung). Wenn Buchstaben des Alphabets verwendet werden, erhält jedes Schulkind zwei Orangen mit seinem entsprechenden Buchstaben. Mit einer Ausnahme: eine Schülerin/ein Schüler bekommt nur eine Orange mit ihrem/seinem Buchstaben - damit gibt es in dem Kreis aller SchülerInnen jeweils eine/einen mit einer leeren Hand. Wenn mehrere Früchte verwendet werden, erhält jedes Schulkind zwei Früchte derselben Sorte – z.B. eine Schülerin mit gelbem Hut hält zwei Bananen und ein Schüler mit grünem Hut bekommt zwei grüne Äpfel. Ein Schulkind bekommt nur eine Frucht zugeteilt.

3. Verteile die Orangen oder Früchte beliebig an alle SchülerInnen in dem Kreis. Jeder, außer ein Schulkind, hält zwei Teile in den Händen. (Keiner der SchülerInnen sollte bereits ihre zugeordnete Orange/Frucht in den Händen halten.)

4. Die SchülerInnen verteilen die Orangen/Früchte im Kreis bis jedes Schulkind eine Orange/Frucht mit seinem entsprechenden Buchstaben oder seiner Farbe hat. Folgende beiden Regeln müssen befolgt werden:

   a) in jeder Hand darf nur eine Orange/Frucht gehalten werden.

   b) nur eine Orange/Frucht kann in die leere Hand eines direkten Nachbarn im Kreis gegeben werden. (Ein Schulkind darf nur eine der beiden Orangen an seinen Nachbarn weitergeben.)

Die SchülerInnen finden schnell heraus, dass wenn sie „gierig“ sind (d.h. sie behalten eine ihrer Orangen/Früchte sobald sie sie bekommen haben), die Gruppe vielleicht nicht erfolgreich sein wird. Es ist eventuell notwendig zu betonen, dass das Spiel nicht allein zu gewinnen ist, sondern das Puzzle erst gelöst werden kann, wenn jeder die richtige Orange/Frucht hat.

Anschließende Besprechung

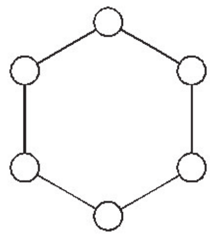
Welche Strategien haben die SchülerInnen benutzt, um das Problem zu lösen?

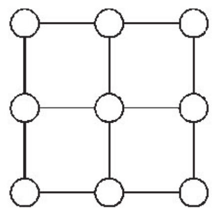
Wo hast du in deinem Leben bereits einen „Stillstand“ erlebt? (Ein Beispiel könnte der Verkehrsstau sein oder, wenn viele Menschen versuchen gleichzeitig durch eine schmale Tür zu gehen.)

Weitere Aktivitäten

Probiere diese Aktivität mit einem kleineren oder größeren Kreis.

- Lass die SchülerInnen neue Regeln vorschlagen.
- Führe die Aktivität ohne Gespräche durch.
- Versuche verschiedene Sitzordnungen – etwa in einer Reihe oder mit mehr als zwei Nachbarn für einige der SchülerInnen. Drei Vorschläge werden hier dargestellt.





Worum geht es in dieser Aktivität?

Routing und Stillstand (deadlock) sind Probleme in vielen Netzwerken, etwa dem Straßen- und Telefonnetz oder in Computersystemen. IngenieurInnen verbringen viel Zeit damit herauszufinden, wie die Probleme gelöst werden können und wie man Netzwerke entwerfen kann, die es ermöglichen, diese Probleme einfacher zu lösen.

Routing, Überlastung und Stillstand können frustrierende Probleme in vielen verschiedenen Netzwerken darstellen. Denken Sie nur an den alltäglichen Berufsverkehr! In New York ist es oft vorgekommen, dass der Verkehr überlastet war und zu einem Stillstand geführt hat: Niemand konnte weiterfahren! Wenn in Unternehmen (wie etwa Banken) die Computer „am Boden" sind, liegt das oft am Stillstand der Datenübertragung. Netzwerke so zu entwerfen, dass Routing einfach und effizient ist und Überlastung minimiert wird, ist ein schwieriges Problem, dem viele EntwicklerInnen gegenüber stehen.

Manchmal möchten mehrere Personen gleichzeitig auf dieselben Daten zugreifen. Wenn Daten (etwa Kontostand von Kunden) aktualisiert werden, müssen diese während des Updates gesperrt sein. Falls das nicht getan wird, könnte jemand anderes dieselben Daten updaten und der Kontostand wird falsch gespeichert. Wenn jedoch diese Verriegelung durch die Sperrung eines anderen Gegenstandes behindert wird, kann es zu einem Deadlock kommen.

Eine der aufregendsten Entwicklungen in der Computerentwicklung ist das Parallelcomputing, wo Hunderte oder Tausende von PC-ähnlichen Prozessoren (in einem Netzwerk) zu einem einzigen leistungsstarken Computer zusammengefasst werden. Viele Probleme, wie das Orangenspiel, müssen ununterbrochen (und viel schneller!) auf diesen Netzwerken ausgeführt werden, damit diese Parallelrechner laufen.

Aktivität 11: Steintafeln – Netzwerk-Kommunikationsprotokolle

Zusammenfassung

Computer kommunizieren über das Internet miteinander, in dem Nachrichten übermittelt werden. Allerdings kann man sich nicht auf das Internet verlassen und manchmal gehen Nachrichten verloren. Es gibt bestimmte Informationsbits, die den Nachrichten beigefügt werden um sicherzustellen, dass sie versendet werden. Diese zusätzliche Information wird in einem Protokoll festgehalten.

Einfügen in den Lehrplan

- Mathematik: Entwicklung von Logik und Argumentation
- Deutsch: Kommunikation, gegenseitiges Zuhören

Benötigte Kenntnisse

- Kooperative Problemlösung
- Logisches Denken

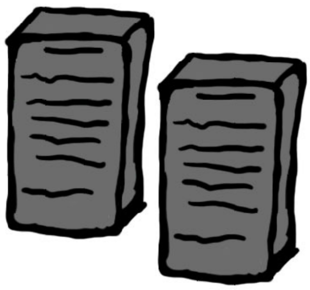
Alter

- 9+

Materialien

Jede Schülerin und jeder Schüler benötigt:

- viele unbeschriebene „Steintafeln“



Jeder Kurier benötigt:

- einen Satz von Aktionskarten für Nachrichten

Jede Lehrperson benötigt:

- einen Zeitmesser (Timer)

Steintafeln

Einführung

In dieser Aktivität beobachten die Schülerinnen und Schüler, wie verschiedene Kommunikationsmethoden erfolgreich ausgeführt werden. Durch das Betrachten von Regeln und Prozeduren werden die SchülerInnen in Kommunikationsprotokolle eingeführt. Bei der Ausführung verschiedener Rollenspiele testen die SchülerInnen ihr eigenes Protokoll in einer unzuverlässigen Umgebung, ähnlich wie etwa TCP/IP bei der Paketlieferung im Internet.

Vorbereitung (30 Minuten)

1. Sammle zuerst die Karten. Drucke dazu die Seite 104 aus und schneide die Karten entsprechend aus. Diese sind die Grundlage des Spiels.

2. Dann entscheide dich für einige Nachrichten, die an SchülerInnen zu senden sind. Es ist wichtig, dass keine Sätze in Deutsch oder in ähnlicher ‚Sprache' (Struktur) ausgehändigt werden. Nachrichten wie „1LHC255HD(RLLS" oder Telefonnummern sind geeignet.

3. Drucke Kopien der Seite 105 aus – jede Seite enthält acht „Steintafeln". Jede Tafel hat nur Platz für sechs Buchstaben oder Ziffern, sodass die ganze Nachricht nicht auf nur eine Tafel passt. Jedes Schulkind benötigt etwa 30 Tafeln, abhängig davon wie lang das Spiel durchgeführt werden soll.

Hinweis: Es gibt drei Typen von Aktionskarten - 'verzögern', 'nicht liefern' und 'liefern'. Das Verhältnis der vorhandenen Kartentypen stellt dabei die Qualität deines Kurierdienstes dar: Mehr Karten vom Typ 'liefern' bedeutet mehr verlässliche Lieferungen, mehr Karten vom Typ 'verzögern' und 'nicht liefern' bedeuten ein weniger verlässliches Netzwerk. Die Karten entsprechen einem Computernetzwerk / Kommunikationskanal.

Ablauf des Spiels

1. Teile deine Klasse in Zweiergruppen auf. Es ist ausschlaggebend, dass sich das Team jeder Zweiergruppe weder sehen noch unterhalten kann. Zwei verschiedene Klassenzimmer wären dazu ideal; sitzend an der gegenseitigen Wand eines Klassenzimmers sollte aber ausreichen.

2. Gebe jeweils einem Schulkind jeder Zweiergruppe eine Nachricht, die an seinen/ihre Partner/in geliefert werden soll.

3. Mische die Aktionskarten und wähle einen Kurier. Der Kurier kannst du sein oder ein Schulkind, wenn die Anzahl der SchülerInnen ungerade ist. Falls es eine große Anzahl an SchülerInnen gibt, werden mehrere Kuriere benötigt.

4. Ein Schulkind schreibt nun auf seine Steintafel und übergibt sie dem Kurier. Auf der Steintafel muss mindestens der Name des Empfängers notiert sein.

5. Der Kurier wählt nun die oberste der Aktionskarten, dreht sie um, liest die Nachricht und verwendet diese, um zu entscheiden, was als nächstes mit der Tafel zu machen ist.

6. Wiederhole die Schritte 4 und 5 für jede Tafel.

Nach ungefähr fünf Minuten voller Chaos und Frustration wird jedes Schulkind feststellen, dass die Namen der Adressaten allein, nicht ausreichend für das Protokoll sind. Unterbrich den Ablauf und diskutiere das mit den SchülerInnen: Welche ist die erste Beobachtung, die sie gemacht haben? Hat es mit der Anordnung zu tun? Vielleicht wäre es am besten, eines dieser sechs Felder zu benutzen, um eine bestimmte Tafel zu wählen (etwa durch Verwendung einer Tafelnummer)? Das aber bedeutet, dass der verfügbare Patz für die tatsächlichen Daten (Nachricht) abnimmt – was bedeutet das in Bezug auf die Anzahl der Tafeln, die wir brauchen werden?

Im anschließenden Verlauf bemerken die SchülerInnen weitere Probleme, die auch besprochen werden sollten. Mögliche Probleme könnten sein, dass eine Tafel fehlt, wobei nicht sicher ist, ob die Tafel überhaupt angekommen ist oder erneut verschickt werden soll. Eine mögliche Lösung wäre es, eine Empfangsbestätigung zu erwarten und erst dann eine weitere Lieferung zu starten – das bedeutet, dass der Empfänger (Schulkind, das die Nachricht bekommen hat) auch über leere Tafeln verfügen muss, um Nachrichten zu senden. Außerdem müssen sich die SchülerInnen darauf einigen, was ihre Antworten auf den sechs Feldern der Tafel bedeuten, bevor sie das Spiel wieder beginnen.

Du brauchst mindestens zwei SchülerInnen für dieses Spiel. Wir aber empfehlen, soviel SchülerInnen wie möglich teilnehmen zu lassen. Wenn du eine große Klasse hast, erwäge es, mehrere Kuriere zu benennen. Noch einmal, besprich Folgendes mit deiner Klasse: Was passiert, wenn du viele Kuriere hast? Was passiert, wenn du nur einen Kurier hast?

Liefere diese Tafel jetzt ab	Liefere diese Nachricht nach der nächsten ab
Liefere diese Tafel jetzt ab	Liefere diese Nachricht nach der nächsten ab
Liefere diese Tafel jetzt ab	Liefere diese Nachricht nach der nächsten ab
Liefere diese Tafel jetzt ab	Liefere diese Nachricht nach der nächsten ab
Liefere diese Tafel jetzt ab	Liefere diese Nachricht nach der nächsten ab

An:

Von:

An:

Von:

An:

Von:

An:

Von:

An:

Von:

An:

Von:

An:

Von:

An:

Von:

Steintafeln

In einer altertümlichen Stadt gibt es eine Gruppe von sehr wichtigen Statthaltern. Diese Statthalter beschließen, was in der Stadt stattfinden wird und treffen sehr wichtige Entscheidungen. Alle von ihnen wohnen verteilt in der Stadt in einem eigenen Haus mit eigener Hausnummer, die nur genau einmal in der Stadt vorkommt.

Die Statthalter kommunizieren oft untereinander und erhalten bzw. müssen Nachrichten an alle Einwohner der Stadt verschicken. Man erkennt den betreffenden Statthalter durch die angegebene Hausnummer und alle von ihnen verfügen über eine Gruppe von Kurieren, deren Aufgabe es ist, die Nachrichten zu liefern.

Die einzige Möglichkeit, Nachrichten zu verschicken, erfolgt durch das Schreiben auf große rechteckige Steintafeln, die von den Kurieren zum Empfänger gebracht werden. Die Steintafeln haben eine beschränkte Größe, auf der nur sechs Informationen eingetragen werden können; jede Information kann nur ein Buchstabe oder eine Ziffer sein. Deshalb werden Nachrichten oft auf mehreren Tafeln verteilt und aufgrund des Gewichtes kann jeweils nur eine Tafel von den Kurieren mitgenommen werden.

Den Kurieren kann es aufgrund ihrer Vergesslichkeit und Trägheit passieren, dass die Nachricht nicht korrekt geliefert wird. Außerdem halten sie oft für eine lange Pause während ihrer Arbeitszeit an und versuchen sogar, aus der Stadt zu flüchten.

Die Statthalter möchten einen Weg finden, ihre Kommunikation verlässlich zu machen. Deshalb möchten sie ein Regelwerk einführen, das alle befolgen sollen. Dadurch können sie feststellen, ob eine Nachricht angekommen ist oder nicht und dass es auch die richtige Nachricht gewesen ist. Die Statthalter haben bereits festgelegt, dass der Empfänger, auf jeder Steintafel eingetragen wird.

Es ist nun eure Aufgabe in euren Gruppen die Regeln zu entwickeln, die die Statthalter benutzen werden um zu kommunizieren.

Worum geht es in dieser Aktivität?

Im Internet werden Daten in Pakete für die Weiterleitung aufgeteilt. Allerdings sind die Kanäle, in denen die Pakete transportiert werden, nicht immer zuverlässlich. Manchmal werden einzelne Pakete beschädigt, gehen verloren oder verlieren ihre Reihenfolge.

Im Text über „Steintafeln“ (Seite 106) stellen die Tafeln Pakete und deren Inhalt Daten dar. Pakete beinhalten beides: Daten- und „Header“-Informationen. Der Umfang der Header-Information beeinflusst wie viel Daten übermittelt werden können – eine Art Gleichgewicht muss eingehalten werden, da die Pakete von endlicher Größe sind.

Die SchülerInnen werden feststellen, dass sie die Daten in einigen ihrer verfügbaren Felder mit Informationen wie Paketnummer und Anzahl von Paketen austauschen müssen. Oder, dass es sich bei diesem Paket um eine Empfangsbestätigung handelt. Aufgrund dieser Informationen, die die Datenfelder aufnehmen, werden insgesamt mehr Pakete benötigt.

Internetprotokolle wie TCP und UDP gleichen diese Faktoren aus, um eine zuverlässige und effiziente Datenübertragung zu ermöglichen.

Diese Aktivität wird von einer Person im Rahmen des Projekts „Computing Science Inside“ übernommen und angepasst (csi.dcs.gla.ac.uk).

Teil III
Sag dem Computer, was er machen soll – Darstellung von Prozeduren

Sag dem Computer, was er machen soll

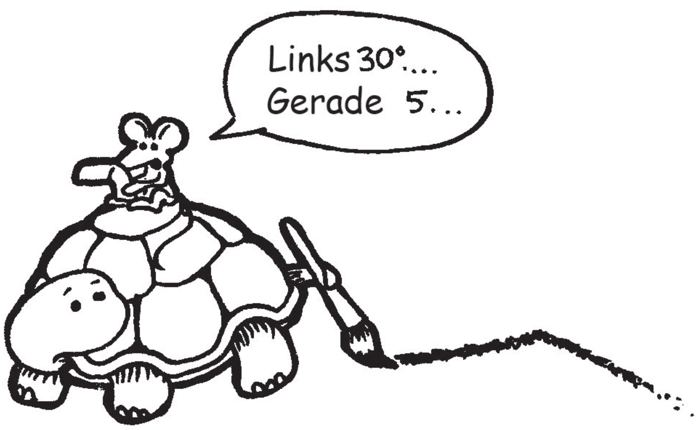
Computer folgen Anweisungen - Millionen von Anweisungen pro Sekunde. Um einem Computer zu sagen, was zu tun ist, musst du ihm nur die richtigen Anweisungen geben. Aber das ist nicht so einfach, wie es klingt!

Wenn wir Anweisungen erhalten, verwenden wir gesunden Menschenverstand, um zu interpretieren, was gemeint ist. Wenn jemand sagt „Geh durch diese Tür", dann heißt das nicht wirklich ‚durch' die Tür gehen – es bedeutet vielmehr, benutze den Eingang durch die Tür und öffne sie zuerst, wenn nötig! Computer sind anders. Wenn sie an mobilen Robotern angebracht sind, musst du vorsichtig sein und Sicherheitsvorkehrungen treffen, um zu vermeiden, dass sie Schaden und Gefahr verursachen, indem sie Anweisungen buchstäblich ausführen – genauso, als wenn du versuchen würdest, ‚durch' eine Tür zu gehen. Der Umgang mit etwas, das Anweisungen genau befolgt ohne „nachzudenken", ist etwas gewöhnungsbedürftig.

Die zwei Aktivitäten in diesem Abschnitt geben uns eine Vorstellung davon, wie es ist mit Maschinen, die ihre Befehle Wort für Wort interpretieren, in einer festen Reihe von Anweisungen zu kommunizieren.

Als erstes wird uns eine „Maschine" erklärt, die Computer verwenden, um Wörter, Zahlen oder Zeichenfolgen zu erkennen, mit denen der Computer arbeiten kann. Diese „Maschinen" werden **endliche Automaten** genannt.

Die zweite Aktivität zeigt uns, wie wir mit Computern kommunizieren können. Ein guter Programmierer bzw. eine gute Programmiererin muss lernen dem Computer zu sagen, was er tun soll, indem er einen festen Satz von Anweisungen verwendet, die wortwörtlich interpretiert werden. Die Liste der Anweisungen ist das Programm. Es gibt viele verschiedene Programmiersprachen, die ein Programmierer / eine Programmiererin wählen kann um diese Anweisungen zu schreiben, aber wir werden eine einfache Sprache verwenden, die ohne einen Computer verwendet werden kann.



Aktivität 12: Schatzsuche – endliche Automaten

Zusammenfassung

Computerprogramme müssen oft eine Folge von Symbolen, wie Buchstaben oder Wörter, in einem Dokument oder sogar den Text eines anderen Computerprogramms verarbeiten. ComputerwissenschaftlerInnen benutzen dafür oft einen endlichen Automaten. Ein endlicher Automat (EA) folgt einer Reihe von Anweisungen, um zu sehen, ob der Computer das Wort oder die Zeichenfolge von Symbolen erkennt. Wir werden mit etwas arbeiten, das einem EA entspricht - Schatzkarten!

Einfügen in den Lehrplan

- Mathematik: Logik und Argumentation entwickeln - Wörter und Symbole verwenden, um Modelle zu beschreiben und umzusetzen
- Sozialwissenschaft
- Englisch

Benötigte Kenntnisse

- Einfache Kartenlesung
- Muster erkennen
- Logik
- Befehle ausführen

Alter

- 9+

Materialien

Du brauchst:

- Einen Satz Inselkarten (die Anweisungen müssen vor denen verborgen bleiben, die versuchen, die Karte zu zeichnen!)

  Kopiere die Kopiervorlage: Inselkarten (ab Seite 113) und schneide sie aus.

  Falte entlang der gepunkteten Linie und klebe jede Karte so, dass auf der Vorderseite der Karte der Name der Insel und auf der Rückseite die Anweisungen stehen.

Jedes Schulkind braucht:

- Arbeitsblatt: Finde deinen Weg zu den Reichtümern auf der Schatzinsel (Seite 116)
- Stift oder Bleistift

Es gibt optionale Erweiterungsaktivitäten, für die jedes Schulkind folgendes benötigt:

- Arbeitsblatt: Schatzinseln (Seite 122)
- Arbeitsblatt: Das mysteriöse Münzenspiel (Seite 123)

Schatzinsel

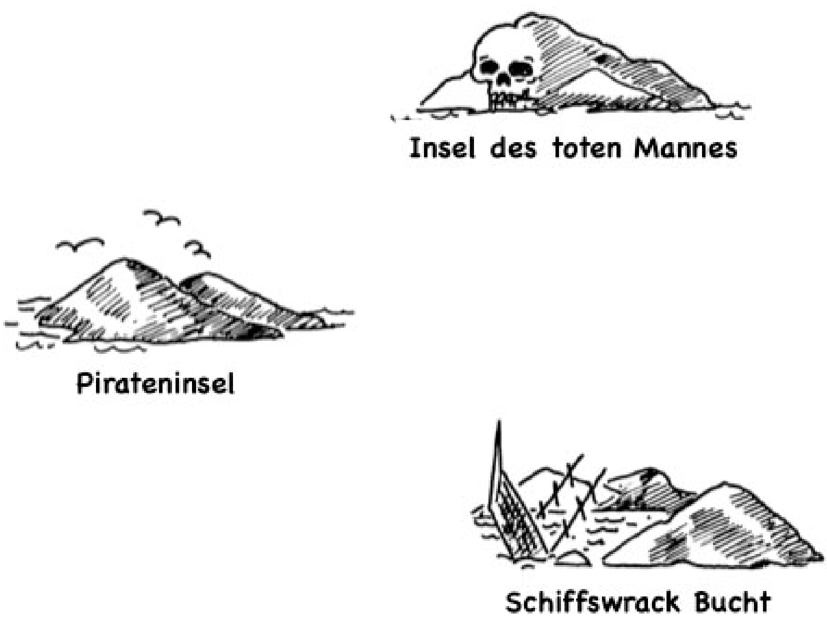
Einführung

Dein Ziel ist es, die Schatzinsel zu finden. Freundliche Piratenschiffe segeln entlang einer festen Reihe von Routen zwischen den Inseln in diesem Teil der Welt und bieten Fahrgästen Fahrten an. Jede Insel hat zwei auslaufende Schiffe A und B, auf denen du reisen kannst. Du sollst die beste Route zur Schatzinsel finden. Auf jeder Insel, die du erreichst, kannst du entweder Schiff A oder B benutzen (aber nicht beide). Die Person auf der Insel wird dir sagen, wohin dein Schiff dich als nächstes bringen wird, aber die Piraten haben keine Karte von allen verfügbaren Inseln. Benutze deine Karte, um zu verfolgen, wohin und auf welchem Schiff du gereist bist.

Beispiel

(Hinweis: Dies ist eine andere Karte als die, die in der tatsächlichen Aktivität verwendet wird.)

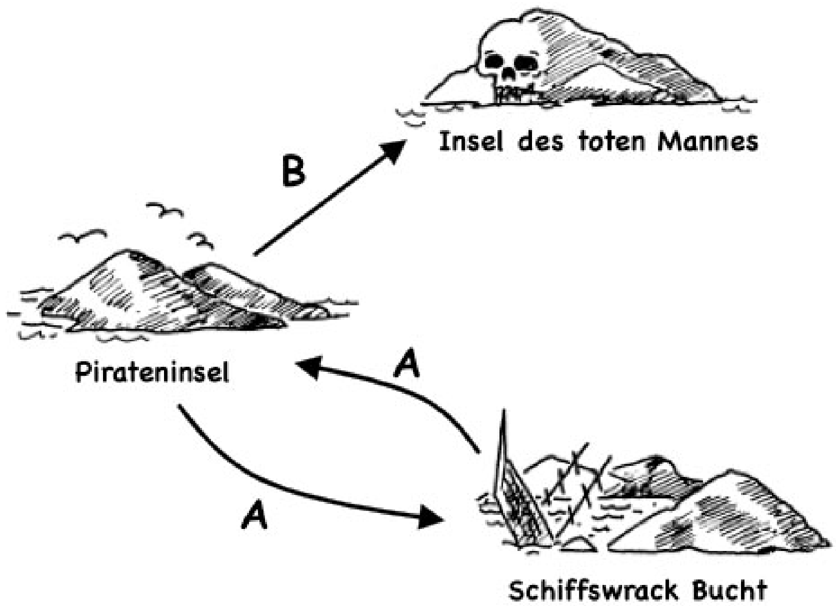
Zeichne auf einer Tafel ein Diagramm von drei Inseln, wie es hier dargestellt ist:



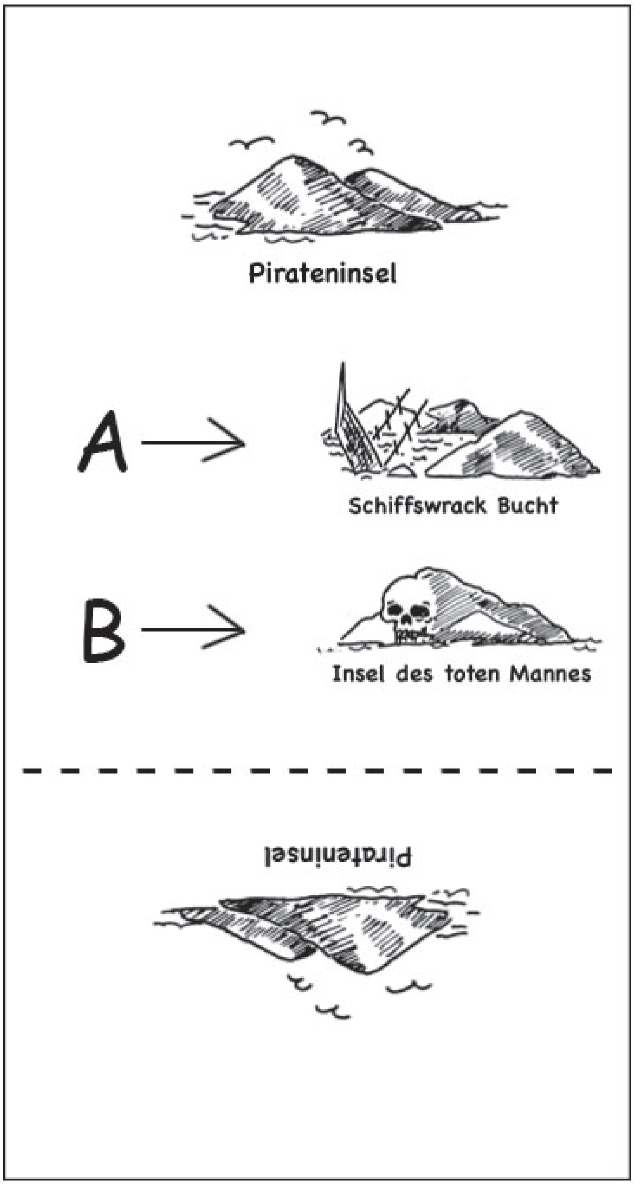
Drucke die drei Karten auf den beiden Seiten 113 und 114 aus und gebe jede Karte einem Schüler oder einer Schülerin. Beachte, dass sich die Routen auf diesen Karten von denen in der Hauptaktivität unterscheiden!

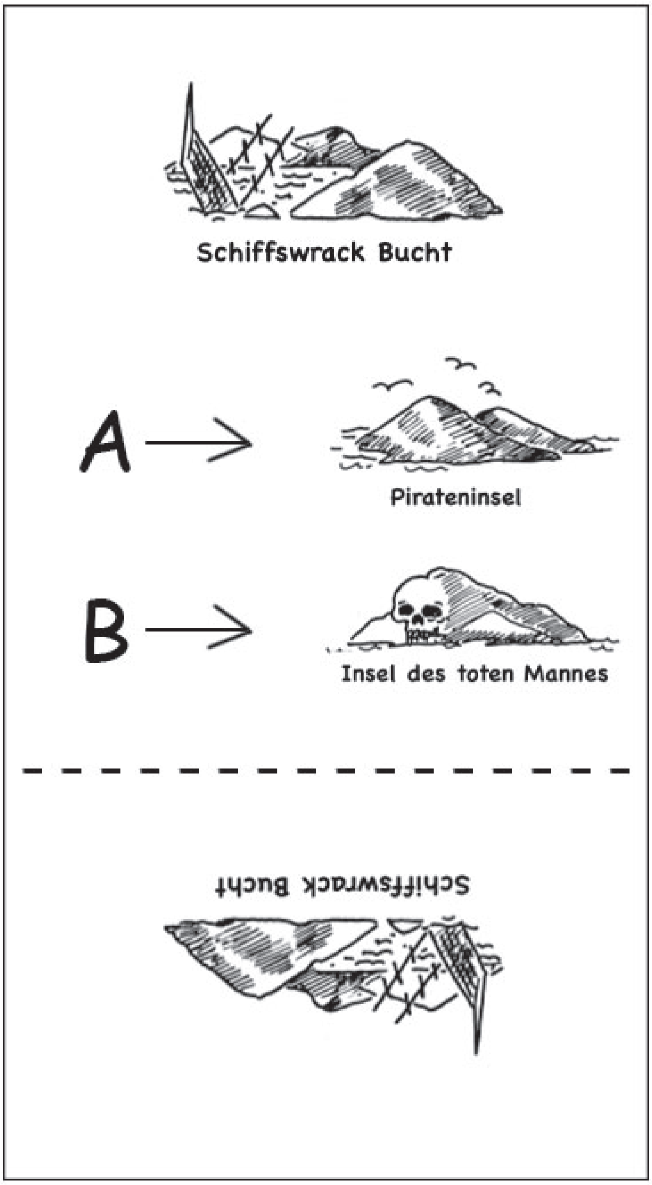
Beginne bei der Pirateninsel und frage nach dem Schiff A. Der Schüler oder die Schülerin sollte dich zur Schiffswrack Bucht bringen. Markiere die Route auf der Karte. Danach frage sie in der Schiffswrack Bucht wieder nach dem Schiff A. Du wirst zurück auf die Pirateninsel geleitet. Benutze jetzt das Schiff B. Markiere dies auf der Karte. Diese Route führt dich zur Insel des toten Mannes, wo du feststecken wirst und nicht weiterfahren kannst!

Deine Karte sollte letztendlich wie folgt aussehen:



Karten für das Beispiel



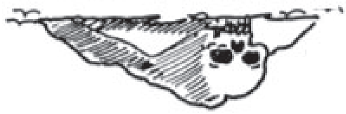


Karten für das Beispiel

Insel des toten Mannes

Kein Schiff
verlässt die Insel
des toten Mannes !

Insel des toten Mannes

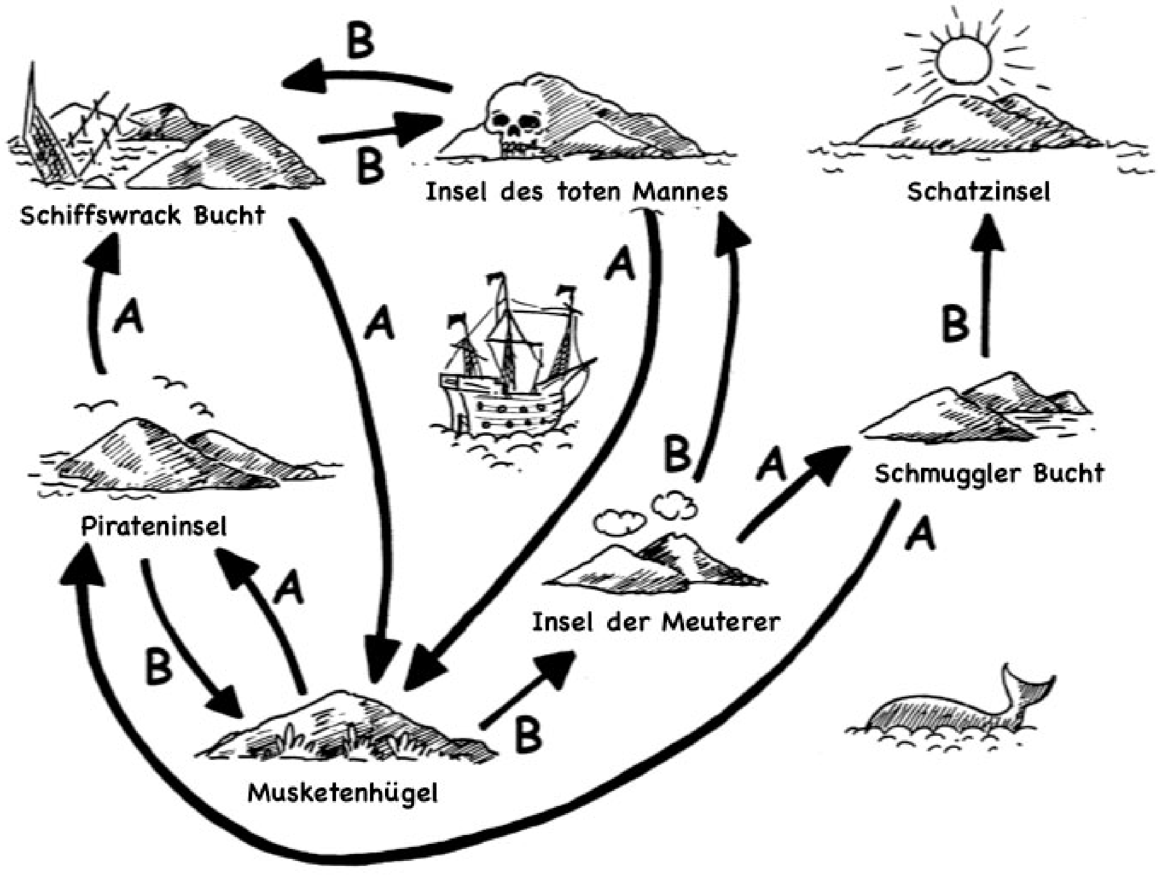


Aktivität

Wähle sieben SchülerInnen als „Inseln". Die SchülerInnen werden Karten halten, die ihre Insel beschreiben und deren geheime Anweisungen sich auf der Rückseite befinden. Sie sollen sich rein zufällig im Raum oder auf dem Spielplatz aufstellen. Die anderen SchülerInnen erhalten eine leere Karte und sollen eine Route von der Pirateninsel zur Schatzinsel nehmen, die sie sorgfältig auf ihren Karten markieren. (Es empfiehlt sich, die SchülerInnen nacheinander abzuschicken, damit sie nicht im Voraus von den Routen erfahren.)

Für die Schnellen: Sie sollen versuchen, mehr als eine Route zu finden.

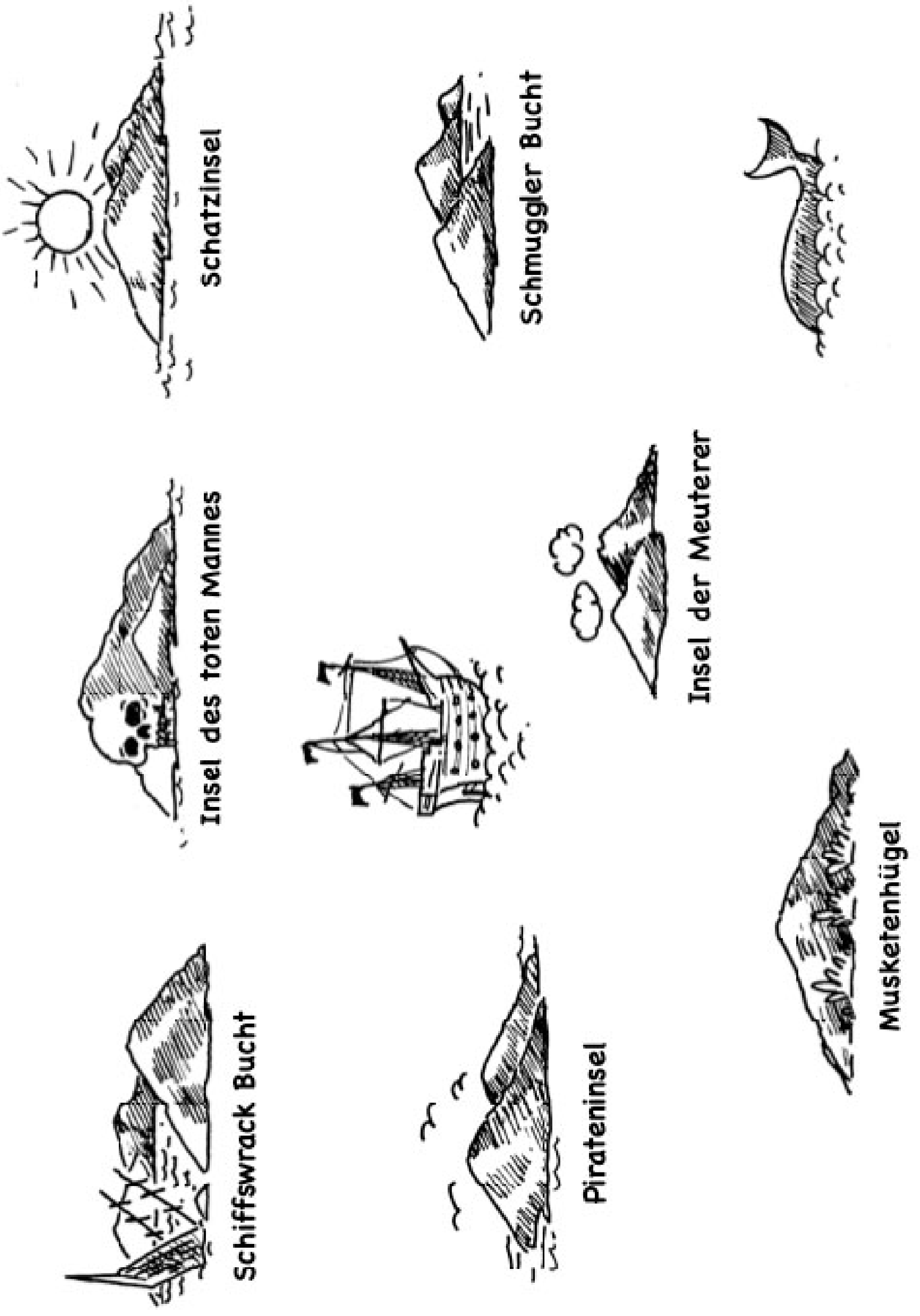
Die vollständige Karte sieht so aus:



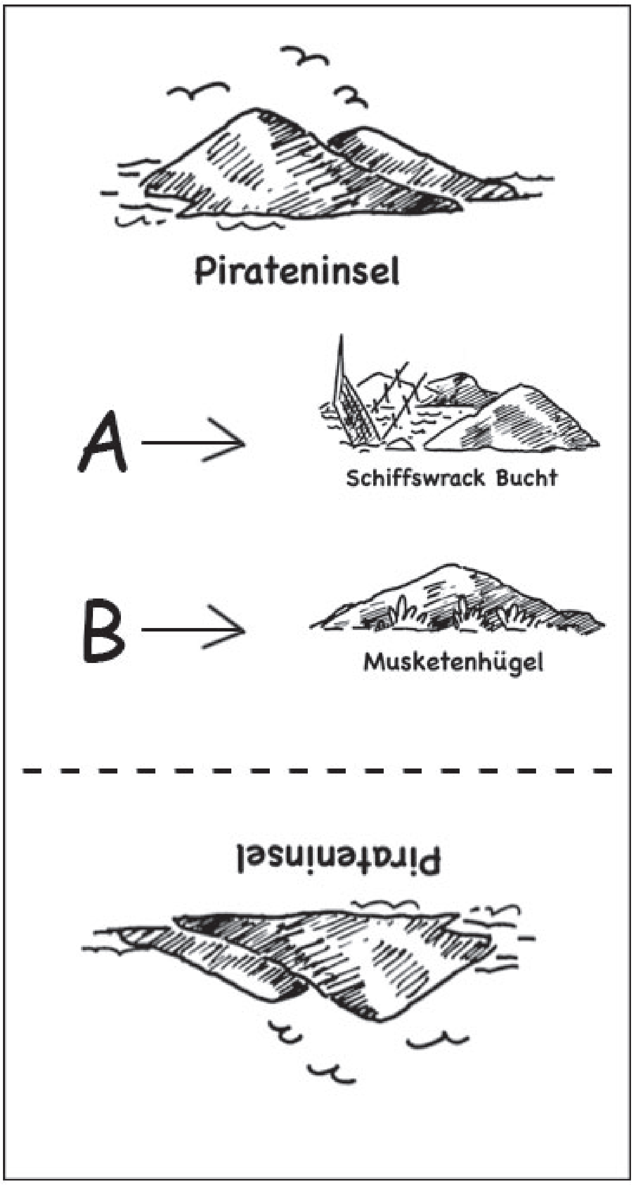
Nachfolgediskussion

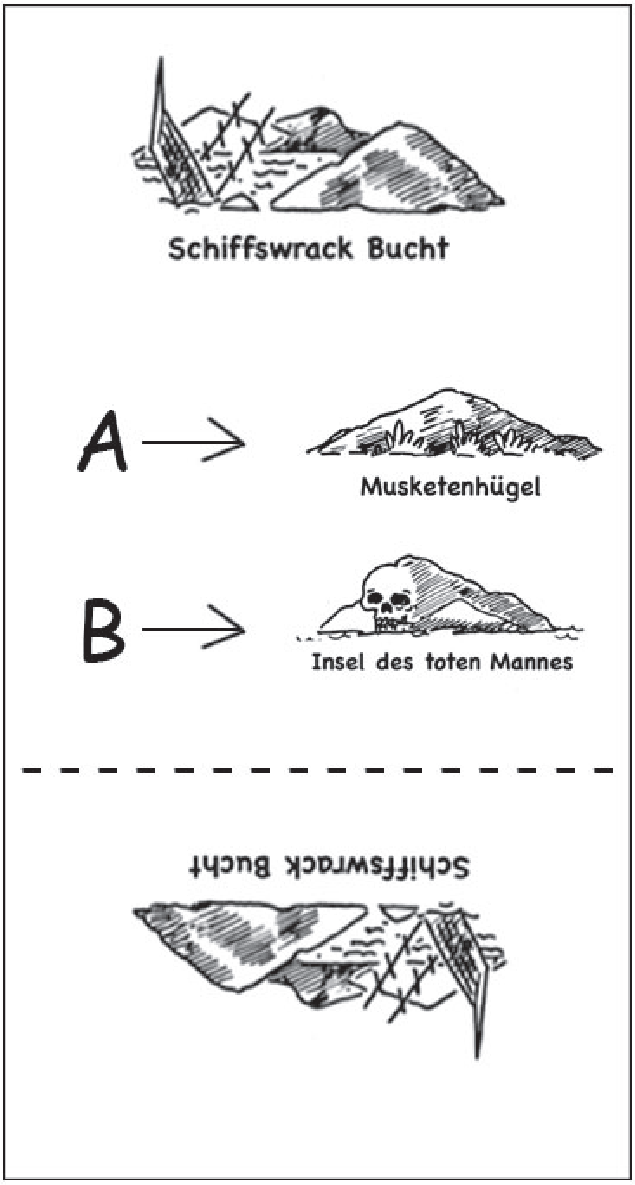
Welche ist die schnellste Route? Welche wäre eine sehr langsame Route? Einige Routen können Schleifen enthalten. Kannst du dazu ein Beispiel finden? (Beispiel: BBBABAB und BBBABBABAB führen beide zur Schatzinsel.)

Arbeitsblatt: Finde deinen Weg zu den Reichtümern auf der Schatzinsel

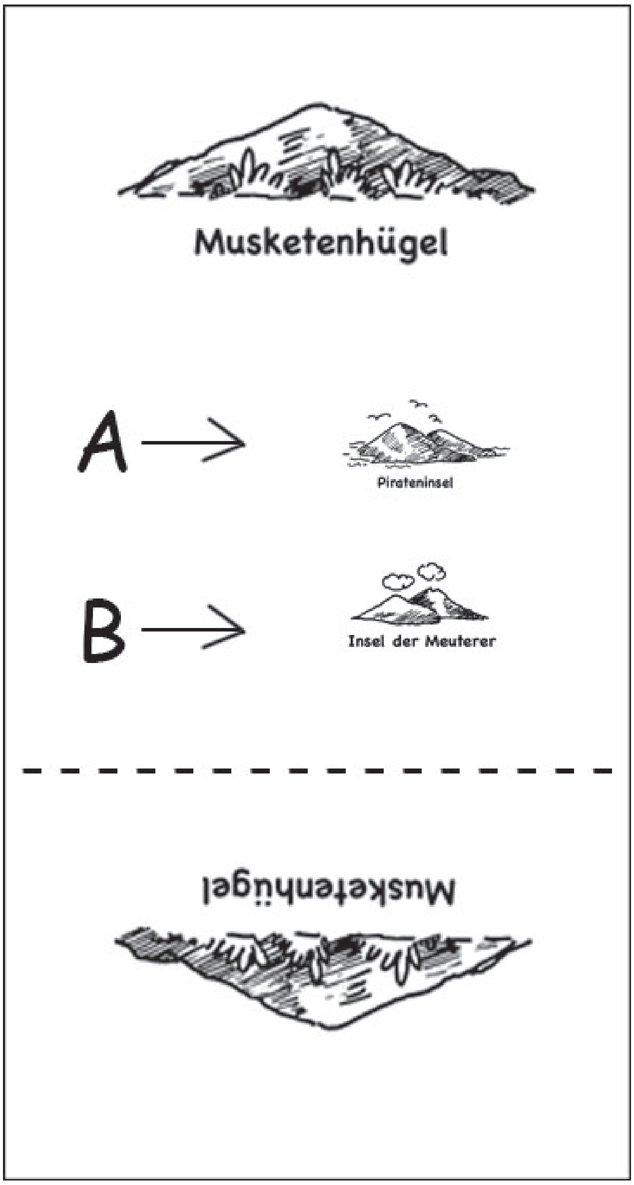


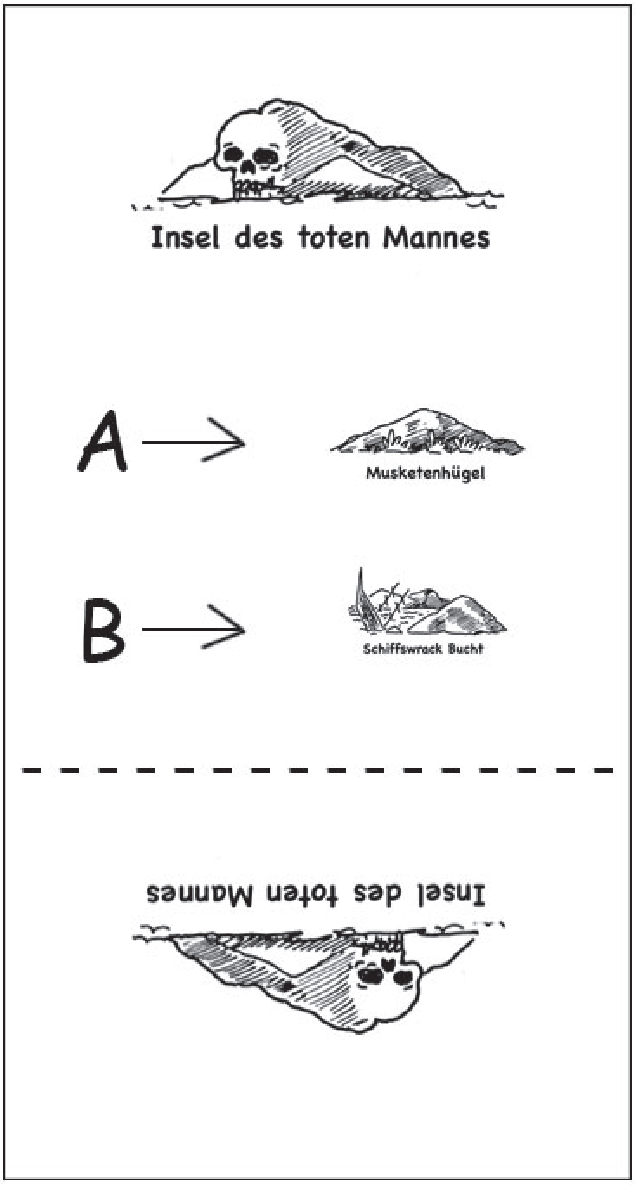
Kopiervorlage: Inselkarten (1/4)



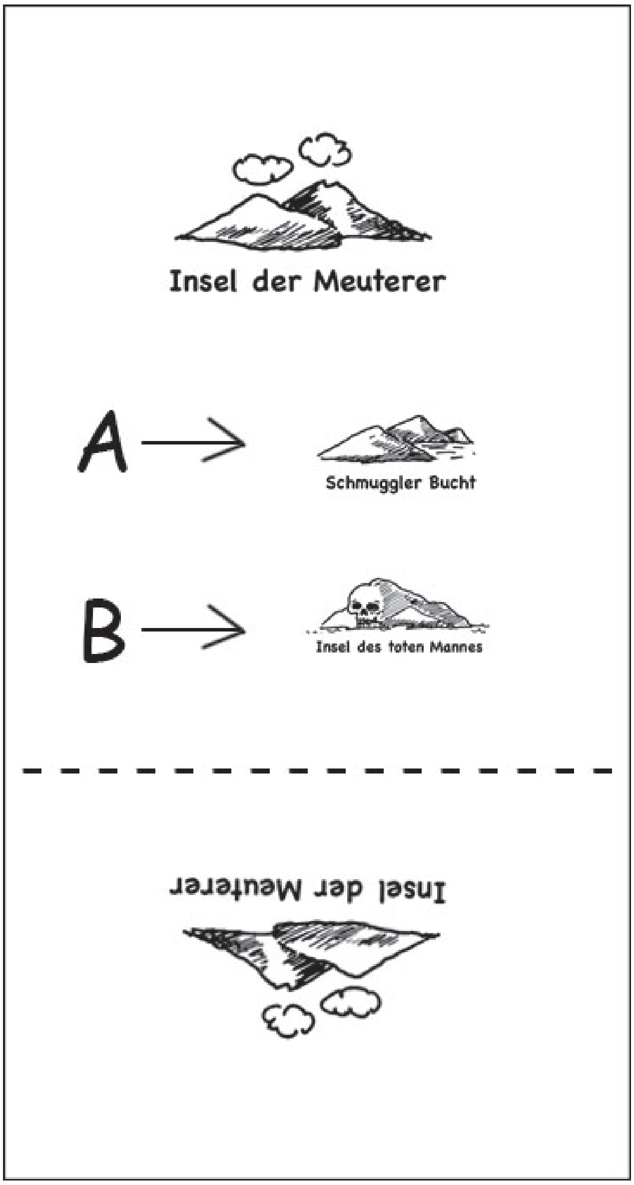


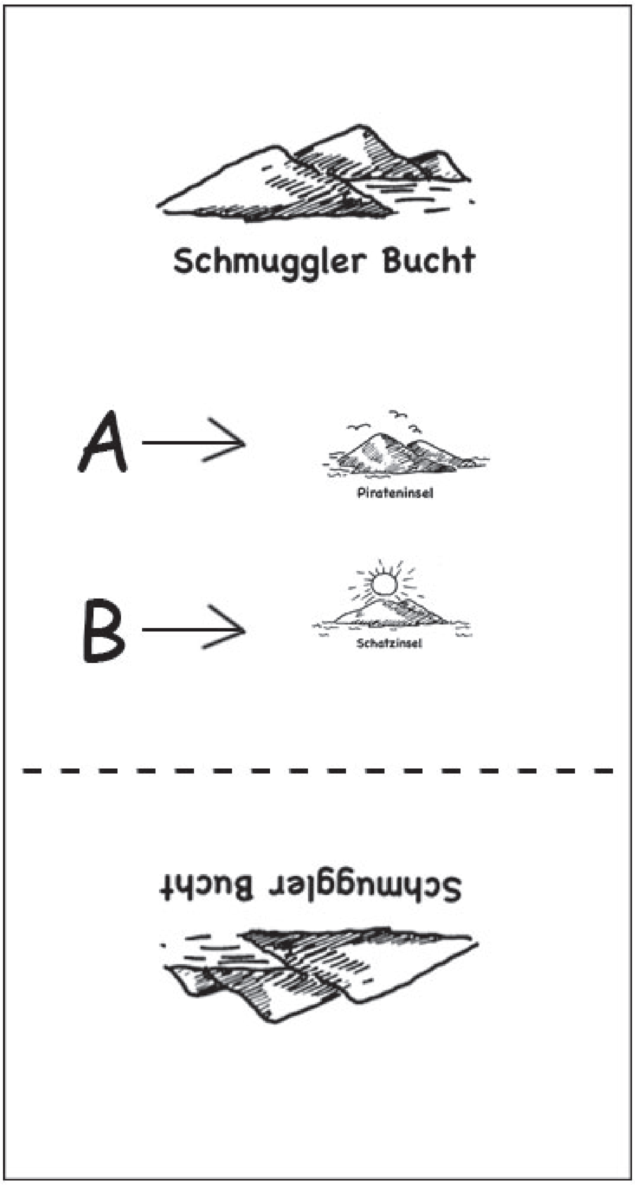
Kopiervorlage: Inselkarten (2/4)





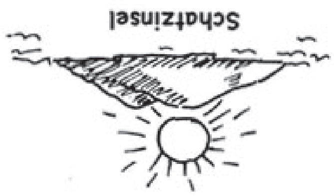
Kopiervorlage: Inselkarten (3/4)





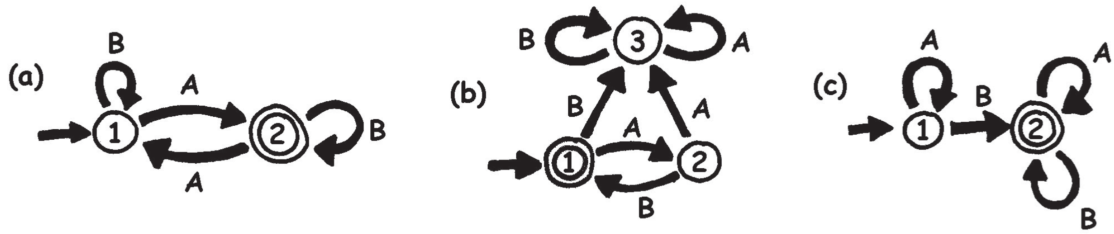
Kopiervorlage: Inselkarten (4/4)

Gratulation!



Endliche Automaten

Das ist eine andere Möglichkeit, die Karten darzustellen:



Die Inseln werden als nummerierte Kreise und die letzte Insel (die Schatzinsel als Ziel) als Doppelkreis dargestellt. Auf welchen Routen können wir reisen, um zur letzten Insel zu gelangen? (Es ist gut es auszuprobieren, indem Beispiele betrachtet werden, z.B. führt "A" in den Doppelkreiszustand? "AA"? "ABA"? "AABA"? Was ist das allgemeine Muster?)

Lösungen:

In Abbildung (a) wird der Doppelkreis (Insel 2) nur erreicht, wenn auf dem Weg dorthin eine ungerade Anzahl von A's vorkommen (z.B. AB, BABAA oder AAABABA).

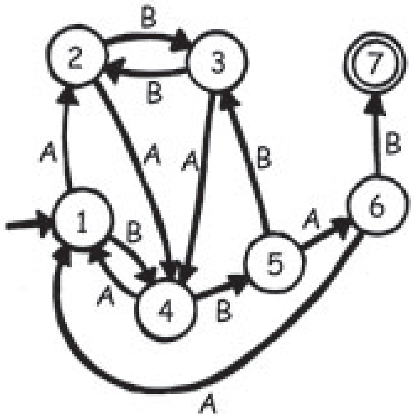
In Abbildung (b) gelangt man nur durch eine alternierende Folge von A's und B's (z.B. AB, ABAB, ABABAB, ...) zum Doppelkreis.

Abbildung (c) zeigt, dass auf dem Weg zum Ziel, B mindestens einmal besucht werden muss (die einzigen ungültigen Folgen sind A, AA, AAA, AAAA, ...).

Arbeitsblatt: Schatzinseln

Kannst du den vergrabenen Schatz gut verstecken? Wie schwer kannst du es machen, dass der Schatz gefunden wird? Es ist Zeit, eine eigene Karte zu erstellen!

1. Hier ist eine kompliziertere Version derselben Idee, eine Karte darzustellen. Diese Karte ist die gleiche wie für die vorherigen Beispiele. InformatikerInnen nutzen diese schnelle und einfache Möglichkeit, Routen für ihre Muster zu entwerfen.

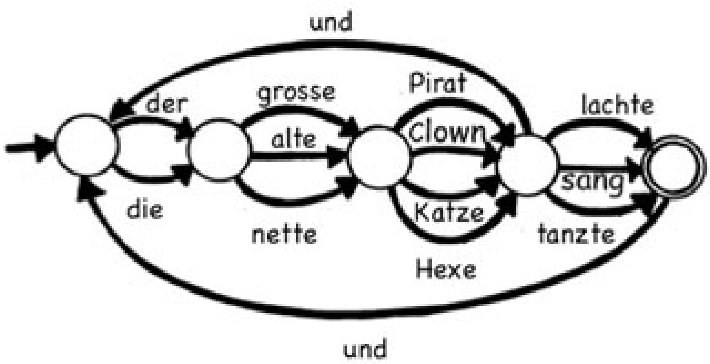


Zeichne deinen eigenen Grundplan so, dass du deutlich sehen kannst, auf welchen Routen deine Piratenschiffe reisen und erstelle dann deine eigenen leeren Karten und Inselkarten. Was ist die effizienteste Folge von Routen, um deine Schatzinsel zu erreichen?

2. Wie gut können deine Freunde deiner Karte folgen? Gib ihnen eine Folge von A's und B's und beobachte, ob sie das Ziel auch korrekt erreichen.

Basierend auf dieser Vorstellung von endlichen Automaten kannst du eine Vielzahl von Spielen und Puzzles erstellen.

3. Hier kannst du Sätze erstellen, indem du zufällige Pfade auf der Karte wählst und die gefundenen Wörter notierst.



Versuche es nun selbst. Vielleicht kannst du sogar eine lustige Geschichte erfinden!

Arbeitsblatt: Das mysteriöse Münzenspiel

Einige Freunde luden ein Spiel aus dem Internet herunter, in dem ein Roboter eine Münze warf und sie raten mussten, ob es Kopf oder Zahl werden würde. Zuerst sah das Spiel sehr einfach aus. Zumindest hätten sie ja eine 50:50 Chance zu gewinnen, dachten sie! Nach einer Weile wurden sie jedoch misstrauisch. Es schien ein Muster in den Münzwürfen zu sein. Wurde das Spiel manipuliert? Sicher nicht! Sie entschieden sich, es zu untersuchen. Joe schrieb die Ergebnisse ihrer nächsten Spielversuche auf und fand heraus:

(k = Kopf, z = Zahl)

k k z k k z k k k z z k k k k z z k z z z k k k k k z k k k z z z k k k z z z k k k k k k z z k z z z z z k z z k z z z k
k k z z k k k z k k k k k k k k k z z k k k z z z z k k k k k z z z z z z z

Kannst du ein vorhersehbares Muster finden?

Es gibt eine sehr einfache „Karte", die die Reihenfolge der Münzwürfe beschreibt. Versuche es herauszufinden.

(Hinweis: Es braucht nur 4 „Inseln")

Worum geht es in dieser Aktivität?

Endliche Automaten werden in der Informatik verwendet, um einem Computer bei der Verarbeitung einer Folge von Zeichen oder Ereignissen zu helfen.

Ein einfaches Beispiel ist, wenn du eine Telefonnummer wählst und eine Nachricht erhältst, die sagt „Drücken Sie 1 für diese … Drücken Sie 2 für das … Drücken Sie 3, um mit einer Serviceperson zu sprechen." Die Tastendrücke sind Eingaben für einen endlichen Automaten am anderen Ende des Telefons. Der Dialog kann ziemlich einfach oder sehr komplex sein. Manchmal wird man im Kreis herumgeführt, weil es im endlichen Automaten eine seltsame Schleife gibt. Wenn dies auftritt, ist dies ein Fehler im Design des Systems - und es kann für den Anrufer extrem frustrierend sein!

Ein anderes Beispiel ist, wenn du Geld von einem Bankautomaten erhältst. Das Programm im Computer der Maschine führt dich durch eine Abfolge von Ereignissen. Innerhalb des Programms werden alle möglichen Sequenzen als endlicher Automat gespeichert. Jede Taste, die du drückst, bringt den Automaten in einen anderen Zustand. In einigen Ländern haben Computer verschiedene Anweisungen wie „100€ Bargeld herausgeben" oder „einen Beleg drucken" oder „die Geldkarte auswerfen".

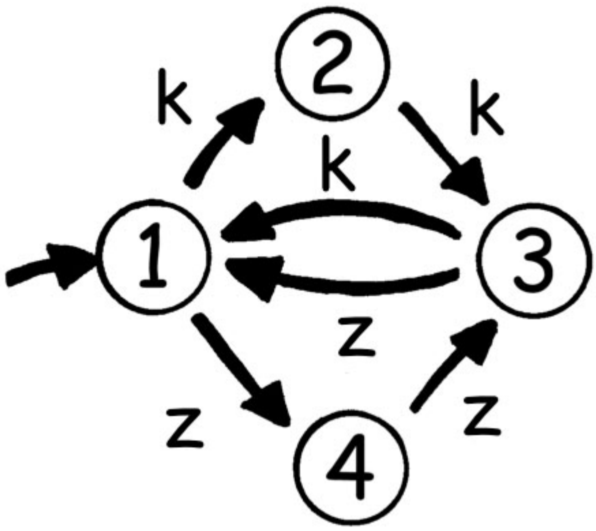
Einige Computerprogramme befassen sich tatsächlich mit deutschen Sätzen, die Karten, wie die auf Seite 113, verwenden. Sie können sowohl Sätze selbst erzeugen, als auch Sätze verarbeiten, die der Benutzer eingibt. In den 1960er Jahren schrieb ein Informatiker ein berühmtes Programm namens „Eliza" (nach Eliza Doolittle), das Gespräche mit Menschen führte. Das Programm gab vor, Psychotherapeut zu sein und brachte führende Ausdrücke wie „Erzähl mir von deiner Familie" und „Mach weiter" hervor. Obwohl es nichts „verstand" war es ausreichend plausibel - und seine menschlichen Benutzer waren ausreichend leichtgläubig, sodass einige Leute wirklich glaubten, sie würden mit einem menschlichen Psychotherapeuten sprechen.

Obwohl Computer die natürliche Sprache nicht wirklich gut verstehen, können sie künstliche Sprachen leicht verarbeiten. Eine wichtige Art der künstlichen Sprache ist die Programmiersprache. Computer benutzen Automaten mit endlichen Zuständen, um Programme einzulesen und in Form elementarer Computeranweisungen zu übersetzen, die dann direkt vom Computer „ausgeführt" werden können.

Lösungen und Tipps

Das mysteriöse Münzenspiel (Seite 123)

Das mysteriöse Münzenspiel benutzt die folgende Karte für den Münzwurf:



Wenn du sie befolgst, wirst du sehen, dass die ersten beiden Münzwürfe von Punkt 1 jeweils das gleiche Ergebnis haben.

Aktivität 13: Marschbefehle – Programmiersprachen

Zusammenfassung

Computer werden normalerweise mithilfe einer „Sprache“ programmiert, bei der es sich um ein eingeschränktes Vokabular von Anweisungen handelt, die ausgeführt werden können. Eines der frustrierendsten Dinge beim Programmieren ist, dass Computer immer den Anweisungen folgen, auch wenn sie ein verrücktes Ergebnis liefern. Diese Aktivität vermittelt den SchülerInnen einige Erfahrungen mit diesem Aspekt der Programmierung.

Einfügen in den Lehrplan

- Deutsch: Zwischenmenschliches Zuhören

Benötigte Kenntnisse

- Anweisungen angeben und ausführen

Alter

- 7+

Materialien

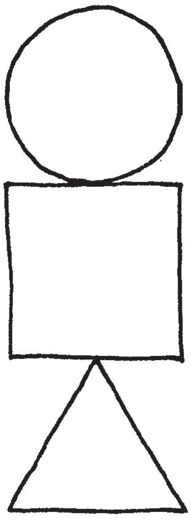
Du brauchst:

- Karten mit Bildern, wie auf der nächsten Seite dargestellt.

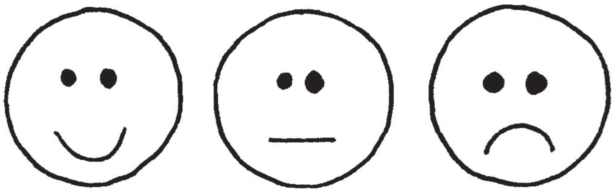
Jedes Schulkind braucht:

- Stift, Papier und Lineal

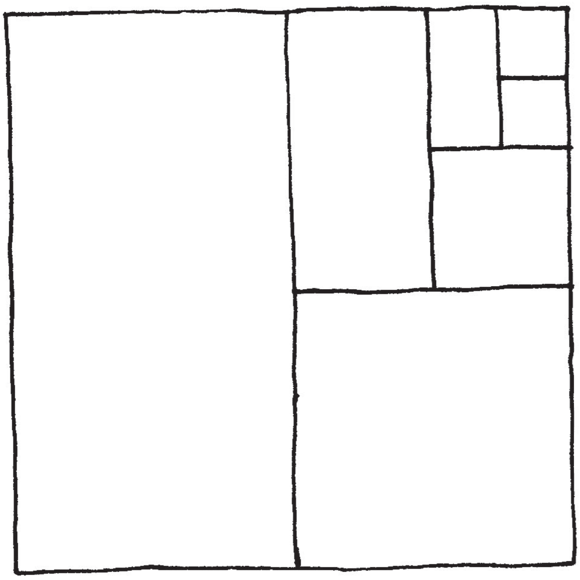
A



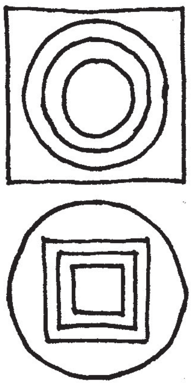
B



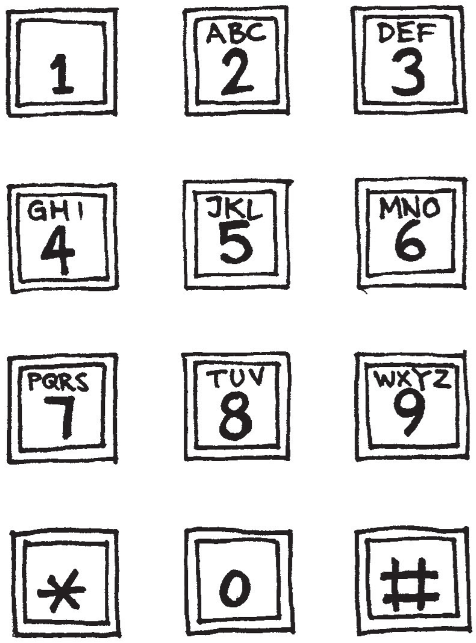
D



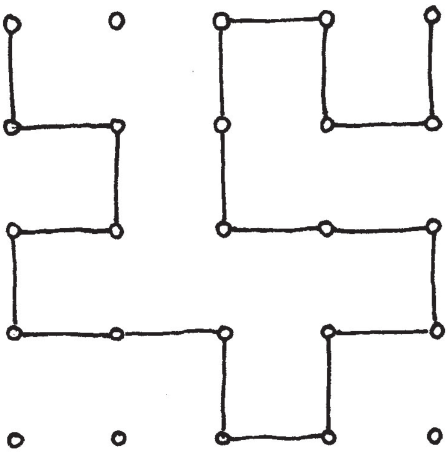
C



F



E



Marschbefehle

Einführung

Bespreche mit den SchülerInnen, ob es gut wäre, wenn Menschen im Allgemeinen Anweisungen genau befolgen würden. Was würde beispielsweise passieren, wenn sie auf eine geschlossene Tür zeigen und sagen: „Gehen Sie durch diese Tür?“

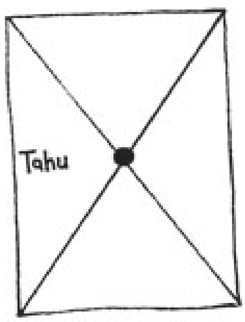
Computer arbeiten, indem sie Anweisungslisten befolgen und genau das tun, was die Anweisungen sagen - auch wenn es keinen Sinn ergibt!

Vorführungsbeispiel

Überprüfe, ob die SchülerInnen das Bild aus den folgenden Anweisungen zeichnen können.

1. Zeichne einen Punkt in der Mitte deines Papierblattes.
2. Zeichne mit dem Lineal eine gerade Linie von links oben durch den von dir gezeichneten Punkt nach rechts unten.
3. Zeichne mit dem Lineal eine gerade Linie von links unten durch den von dir gezeichneten Punkt nach rechts oben.
4. Schreibe deinen Namen in das Dreieck in der Mitte auf der linken Seite des Blattes.

Das Ergebnis sollte etwa so aussehen:



Aktivitäten

Wähle eine Schülerin oder einen Schüler und gebe ihr/ihm ein Bild (Beispiele dazu auf Seite 127). Anschließend beschreibt die Schülerin/der Schüler das Bild vor der Klasse und alle anderen SchülerInnen zeichnen es auf. Die SchülerInnen können auch Fragen stellen, wenn ihnen die Beschreibung nicht klar ist. Ziel ist es zu sehen, wie schnell und genau die Übung absolviert werden kann.

Wiederhole die Übung, aber dieses Mal dürfen die SchülerInnen keine Fragen stellen. Es ist am besten, für diese Übung ein einfacheres Bild zu verwenden, da sich die SchülerInnen sehr schnell verirren können.

Führe nun die Übung so durch, dass sich der/die SchülerIn mit dem Bild hinter einem Bildschirm verbirgt und auch keine Fragen entgegennimmt, sodass die einzige Kommunikation in Form von Anweisungen erfolgt.

Weise die SchülerInnen darauf hin, dass diese Form der Kommunikation am ehesten die ist, die ComputerprogrammiererInnen beim Schreiben von Programmen erfahren; sie geben dem Computer eine Reihe von Anweisungen und erfahren die Wirkung der Anweisungen erst danach.

Lasse die SchülerInnen ein Bild zeichnen und ihre eigenen Anweisungen dazu notieren. Probiere es paarweise oder mit der ganzen Klasse aus.

Variationen

1. Beschreibe Anweisungen zur Konstruktion eines Papierfliegers
2. Schreibe Anweisungen, wie man einen geheimen Ort im Umfeld der Schule findet und verwende Befehle wie „Gehe x Meter vorwärts“, „nach links drehen“ (90 Grad) und „nach rechts drehen“ (90 Grad).

   Die SchülerInnen sollen ihre Anweisungen testen und anpassen, bis sie das gewünschte Ergebnis haben.
3. ‚Blindes Spiel’ - Verbinde einem Schulkind die Augen und lasse es von den anderen Schüler_Innen im Raum herumführen.

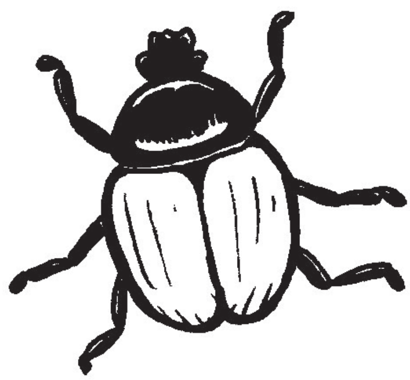
Worum geht es in dieser Aktivität?

Computer arbeiten, indem sie einer Liste von Anweisungen folgen, die als Programm bezeichnet wird, und für die Ausführung einer bestimmten Aufgabe geschrieben wurde. Programme werden in Sprachen geschrieben, die speziell eine begrenzte Anzahl von Anweisungen enthalten und dadurch den Computern sagen, was zu tun ist. Einige Sprachen sind für gewisse Zwecke besser geeignet als andere.

Unabhängig von der Sprache, die sie verwenden, müssen ProgrammiererInnen in der Lage sein, exakt festzulegen, was der Computer tun soll. Im Gegensatz zu Menschen wird ein Computer Anweisungen auf jeden Buchstaben genau ausführen; selbst wenn sie absurd sind.

Es ist wichtig, dass Programme gut geschrieben sind. Selbst ein kleiner Fehler kann viele Probleme verursachen. Stelle dir vor welche dramatischen Folgen ein Fehler im Programm eines Computers bei einer Raumfähre, einem Atomkraftwerk oder den Signalen auf einer Bahn haben kann! Fehler werden gemeinhin als „Bugs“, deutsch: Käfer, bezeichnet. Das kommt daher, weil so ein Käfer aus einem elektrischen Relais eines elektronischen Rechners der frühen 1940er Jahre entfernt („debugged“) werden musste.

Je komplexer das Programm ist, desto mehr Fehler sind wahrscheinlich. Dies wurde zu einem wichtigen Thema, als die USA am Programm der Strategischen Verteidigungsinitiative („Star Wars“) arbeiteten; einem computergesteuerten System, das für nukleare Angriffe ein undurchdringliches Feld bedeuten sollte. Einige ComputerwissenschaftlerInnen behaupteten, dass es wegen der Komplexität und inhärenten Unzuverlässigkeit der Software nie funktionieren könnte. Software muss sorgfältig getestet werden, um so viele Fehler wie möglich zu finden und es wäre nicht möglich dieses System zu testen, da man in den Vereinigten Staaten Raketen abfeuern müsste, um sicher zu gehen, dass diese auch funktionieren!



Teil IV
Wirklich schwere Probleme – Hartnäckigkeit

Hartnäckigkeit

Gibt es Probleme, die selbst für Computer zu schwer sind? Ja. Wir werden in Aktivität 20 sehen, dass es einfach nicht möglich ist, mit einem ins Gespräch zu kommen - etwas, was Computer nicht können, nicht weil sie nicht sprechen können, sondern weil sie keine sinnvollen Dinge verstehen oder denken können. Aber das ist nicht die Art von ‚harten' Problemen, über die wir hier sprechen - es ist nicht so, dass Computer keine Gespräche durchführen können, es ist eher so, dass wir selbst nicht wissen, wie es bei uns funktioniert und so können wir dem Computer nicht sagen, was zu tun ist. Aber in diesem Abschnitt gehen wir auf Probleme ein, bei denen es einfach ist, dem Computer zu sagen, was er tun soll - indem wir ein Programm schreiben - aber der Computer nicht tun kann, was wir wollen, weil es viel zu lange dauern wird: vielleicht Millionen von Jahren. Es reicht nicht, einen schnelleren Computer zu kaufen: Selbst wenn er hundert Mal schneller wäre, würde es immer noch Millionen von Jahre dauern; sogar eine Million mal schneller würde Hunderte von Jahre brauchen. Das nennt man ein hartes Problem - eines, das viel länger dauert, als die Lebensdauer des schnellsten Computers, der für eine Lösung gedacht ist!

Die Aktivitäten in Teil II über Algorithmen haben mögliche Wege gezeigt, um Computerprogramme effizienter zu machen. In diesem Abschnitt befassen wir uns mit Probleme, für die es keine effizienten Lösungen gibt, also Probleme, für die Computer Millionen von Jahren für eine Lösung brauchen. Und wir werden auf das wohl größte Geheimnis der Informatik stoßen: dass niemand weiß, ob es einen effizienteren Weg zur Lösung dieser Probleme gibt! Es mag sein, dass noch niemand einen guten Weg gefunden hat, oder es kann sein, dass es gar keinen guten Weg gibt. Wir wissen es nicht. Und das ist nicht alles. Es gibt Tausende von Probleme, die, obwohl sie völlig anders aussehen, in dem Sinne äquivalent sind, dass, wenn eine effiziente Methode gefunden wird, um ein Problem zu lösen, sie in eine effiziente Methode umgewandelt werden kann, um alle Probleme zu lösen. In den folgenden Aktivitäten lernst du diese Probleme kennen.

Für Lehrpersonen

In diesem Abschnitt gibt es drei Aktivitäten. Die erste besteht darin, Karten zu färben und zu zählen, wie viele Farben benötigt werden, um benachbarte Länder voneinander zu unterscheiden. Die zweite erfordert die Fähigkeit, eine einfache Straßenkarte zu verwenden um Eiswagen an Straßenecken so zu platzieren, dass niemand zu weit gehen muss, um ein Eis zu bekommen. Die dritte ist eine Aktivität im Freien, wo mithilfe von Seil und Stöpseln untersucht wird, wie ein kurzes Netzwerk durch eine Reihe von Punkten erstellt werden kann.

Die Aktivitäten vermitteln einen praktischen Eindruck vom Begriff der Komplexität - wie Probleme, die sehr einfach zu erklären sind, sich als unglaublich schwierig herausstellen können. Diese Probleme sind nicht unverständlich. Es sind praktische Fragen, die in alltäglichen Aktivitäten wie Kartierung, Zeitplanung und Straßenbau entstehen. Die rechnerische Untermauerung stützt sich auf einen Begriff namens „NP-Vollständigkeit", der im Abschnitt „Worum geht es in dieser Aktivität?" am Ende jeder Aktivität erklärt wird. Obwohl die Aktivitäten selbst in beliebiger Reihenfolge angegangen werden können, sollen diese Abschnitte in der Reihenfolge gelesen werden, in der sie erscheinen. Wenn Sie das Ende erreicht haben, werden Sie die wichtigste offene Frage der modernen Informatik fest im Griff haben.

Die Fachbezeichnung für diesen Teil ist „hartnäckig", weil Probleme, die schwer zu lösen sind, als hartnäckig bezeichnet werden. Das Wort stammt aus dem lateinischen Wort ‚tractare', das ‚zu zeichnen' oder ‚zu ziehen' bedeutet. Heute verstehen wir darunter, dass etwas ‚machbar', d.h. leicht zu behandeln, biegsam oder fügsam ist. Hartnäckige Probleme sind solche, mit denen man nicht so leicht umgehen kann, weil es zu lange dauern würde, um eine Antwort zu finden. Auch wenn es vielleicht etwas esoterisch klingt, so ist doch die ‚Hartnäckigkeit' von großem praktischen Interesse, denn ein Durchbruch in diesem Bereich würde für viele verschiedene Forschungsrichtungen große Auswirkungen haben. Zum Beispiel beruhen die meisten kryptographischen Codes auf der Hartnäckigkeit einiger Probleme und ein Krimineller /eine Kriminelle, der es geschafft hat eine effiziente Lösung zu finden, könnte seinen großen Tag damit haben, Geheimnisse zu entschlüsseln und sie zu verkaufen, oder einfach gefälschte Banktransaktionen auszuführen. Wir werden diese Dinge in Teil V „Kryptographie" betrachten.

Aktivität 14: Der arme Kartograph – Färbung von Bildern

Zusammenfassung

Viele Optimierungsprobleme beinhalten Situationen, in denen bestimmte Ereignisse nicht gleichzeitig auftreten können oder bestimmte Elemente einer Gruppe von Objekten nicht benachbart sein können. Zum Beispiel wird jeder, der versucht hat, Stunden oder Treffen zu planen, auf das Problem gestoßen sein, die Beschränkungen für alle beteiligten Personen zu erfüllen. Viele dieser Schwierigkeiten erweisen sich als Problem der Karteneinfärbung, bei dem Farben für Länder auf einer Karte so gewählt werden müssen, dass angrenzende Länder unterschiedliche Farben haben. Bei dieser Aktivität geht es um dieses Problem.

Einfügen in den Lehrplan

- Mathematik: Zahlen – Erforschen von Zahlen mit anderen Basen. Darstellung von binären Zahlen.
- Mathematik: Algebra – Fortsetzung sequenzieller Muster und Beschreibung einer Regel für dieses Muster. Muster und Beziehungen in Zweierpotenzen.

Benötigte Kenntnisse

- Problemlösung.
- Logisches Denken.
- Algorithmische Verfahren und Komplexität.
- Vermittlung von Einsichten.

Alter

- 7+

Materialien

- Ein Whiteboard oder eine ähnliche Schreiboberfläche.

Alle SchülerInnen brauchen:

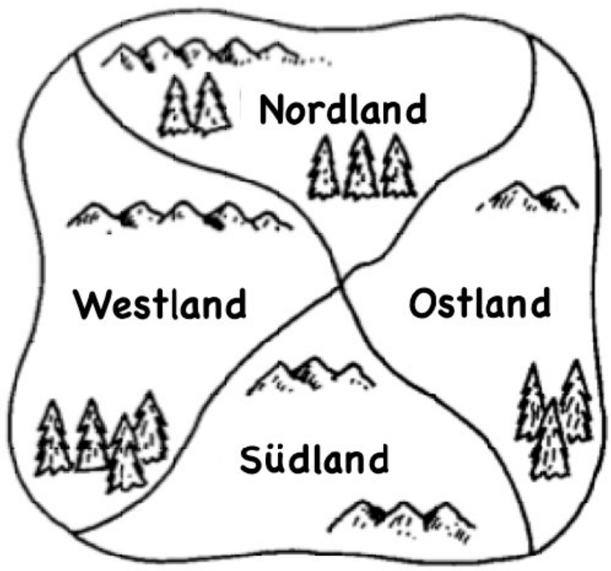
- eine Kopie einer oder mehrerer Arbeitsblätter,
- bewegliche kleine farbige Marker (z. B. Spielsteine oder Pokerchips) und
- vier Stifte in verschiedenen Farben (Buntstifte, Filzstifte etc.)

Färbung von Bildern

Einführung

Diese Aktivität dreht sich um eine Geschichte, in der die SchülerInnen gebeten werden einem Kartographen oder Kartenmacher, der die Länder auf einer Karte einfärbt, zu helfen. Es spielt keine Rolle, welche Farbe ein Land hat, solange es sich von allen angrenzenden Ländern unterscheidet.

Diese Karte zeigt beispielsweise vier Länder. Wenn wir Nordland rot färben, dann können Westland und Ostland nicht rot sein, da ihre Grenzen zu Nordland schwer zu sehen wären. Wir können Westland grün färben, und es ist auch okay wenn wir Ostland grün färben, weil es keine Grenze mit Westland teilt. (Wenn sich zwei Länder nur an einem einzigen Punkt treffen, zählen sie nicht als gemeinsame Grenze und können daher dieselbe Farbe verwenden.)



Südland kann auch rot gefärbt sein und so benötigen wir nur zwei Farben für die ganze Karte.

In unserer Geschichte ist der Kartograph arm und kann sich nicht viele Buntstifte leisten, deshalb ist es die Idee so wenig Farben wie möglich zu verwenden.

Diskussion

Beschreibe das Problem, an dem die Schüler_Innen arbeiten sollen, und zeige den Farbgebungsprozess an einer Tafel.

Verteile eine Kopie des ersten Arbeitsblattes. Diese Karte kann mit nur zwei Farben korrekt eingefärbt werden. Obwohl das Einschränken der Anzahl der Farben auf nur zwei als besonders schwierig erscheint, ist die Aufgabe ziemlich einfach im Vergleich zu Karten, die mehrere Farben erfordern, da es kaum eine Wahl gibt, welche Farbe jedes Land haben kann.

Lass die SchülerInnen versuchen die Karte mit nur zwei Farben zu färben. Dabei entdecken sie möglicherweise die „Muss"-Regel: Sobald ein Land eingefärbt ist, muss jedes angrenzende Land die entgegengesetzte Farbe haben. Diese Regel wird wiederholt angewendet, bis alle Länder eingefärbt sind. Ideal ist es, wenn die SchülerInnen diese Regel selbst entdecken, da es ihnen einen besseren Einblick in den Prozess geben wird.

Wenn die SchülerInnen jede Übung absolviert haben, kann ihnen das nächste Blatt zum Ausprobieren gegeben werden.

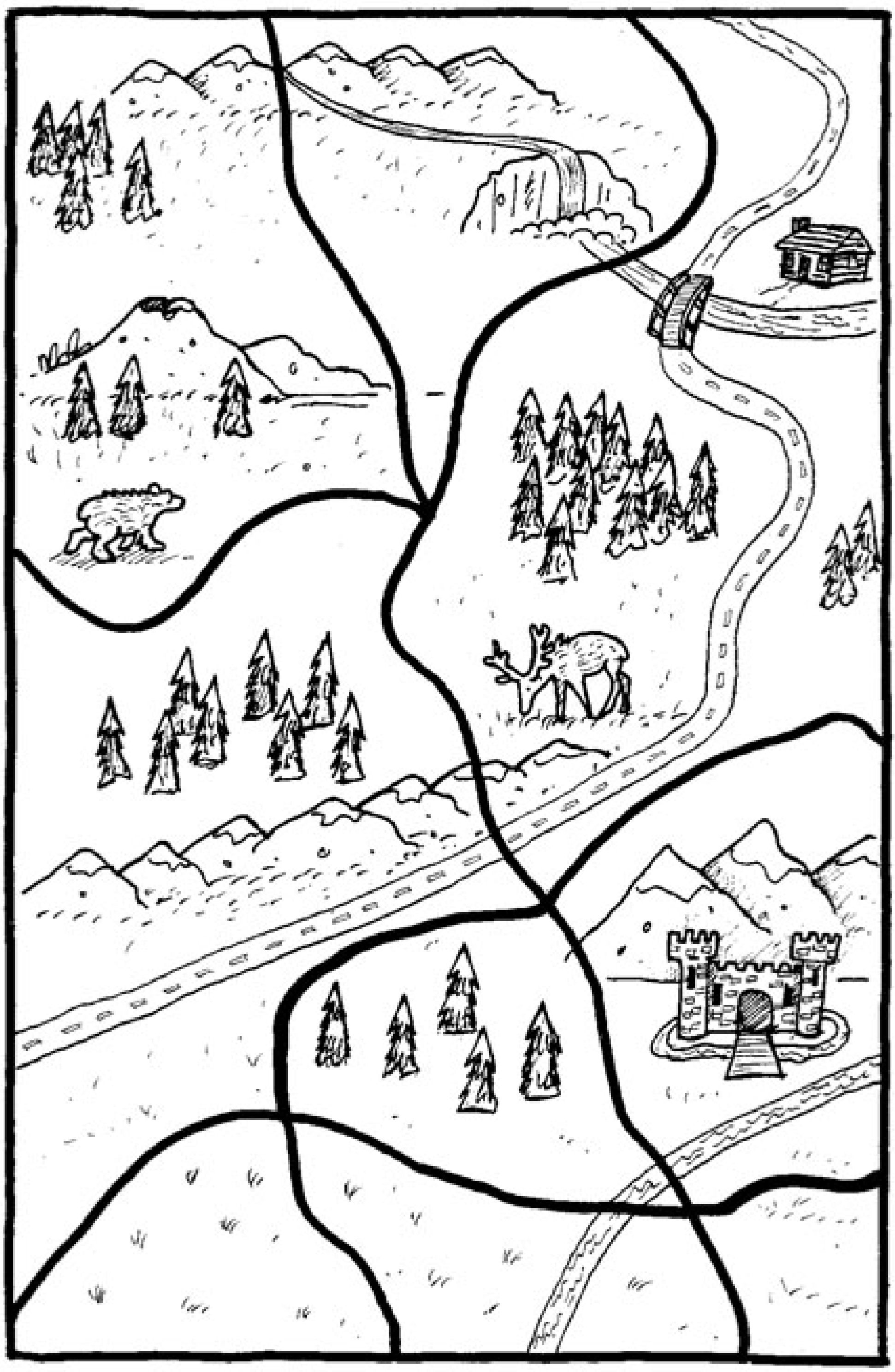
Die SchülerInnen können auch feststellen, dass es besser ist Platzhalter, wie z. B. farbige Spielsteine, zu verwenden anstatt die Länder sofort zu färben, da dies es ihnen leichter macht, ihren Entscheid zu ändern.

Bitte ältere Schulkinder dir zu erklären, woher sie wissen, dass sie die Mindestanzahl von Farben gefunden haben. Zum Beispiel sind mindestens drei Farben für diese Karte erforderlich, da sie eine Gruppe von drei Ländern (die größten drei) enthält, von denen jedes an die anderen zwei grenzt.

Wenn ein Schulkind alle Blätter vorzeitig fertigstellt, bitte es eine eigene Karte zu entwerfen, die fünf verschiedene Farben erfordert. Es wurde bewiesen, dass jede Karte mit nur vier Farben gefärbt werden kann, sodass diese Aufgabe ihn oder sie für einige Zeit beschäftigen wird! Nach unserer Erfahrung werden die SchülerInnen schnell Karten finden, von denen sie glauben, dass sie fünf Farben erfordern, aber natürlich ist es immer möglich eine vierfarbige Lösung für ihre Karten zu finden.

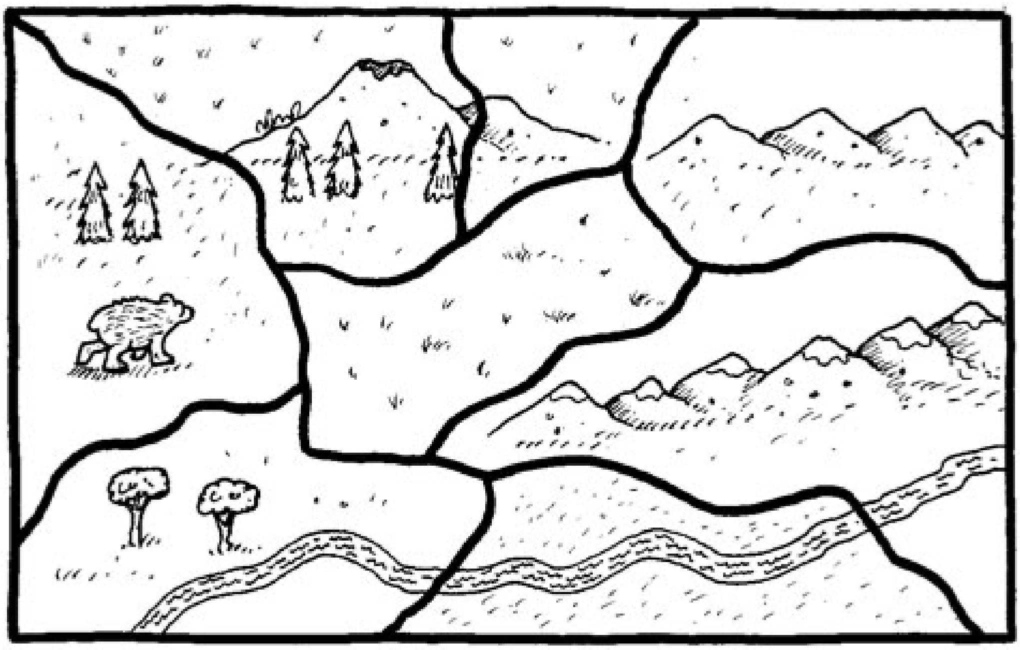
Arbeitsblatt: Bild einfärben 1

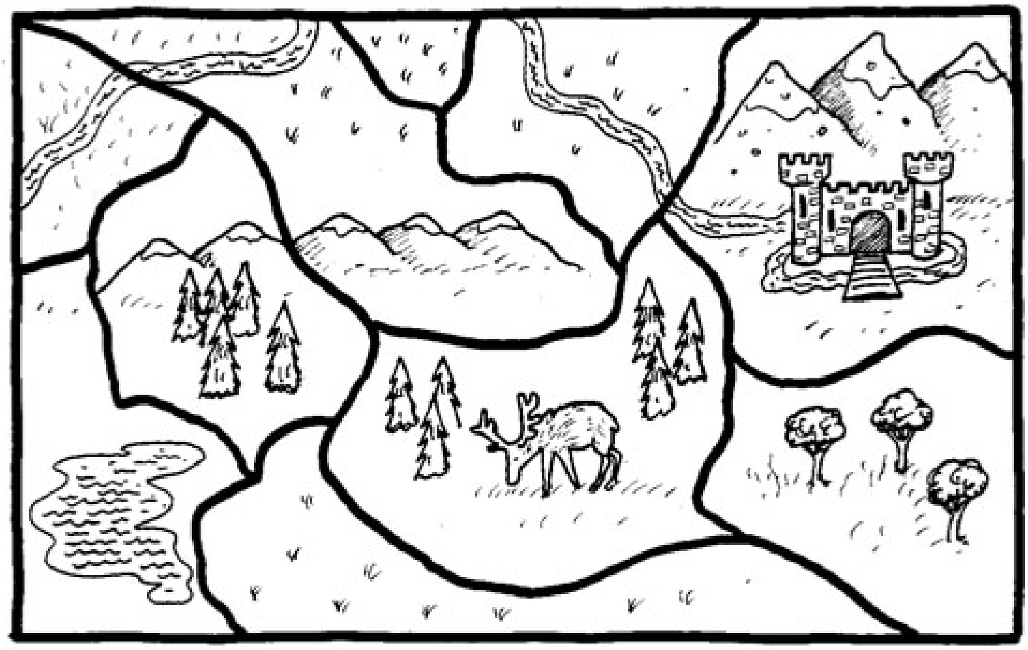
Färbe die Länder auf dieser Karte mit so wenigen Farben wie möglich, aber stelle sicher, dass keine zwei angrenzenden Länder die gleiche Farbe haben!



Arbeitsblatt: Bild einfärben 2

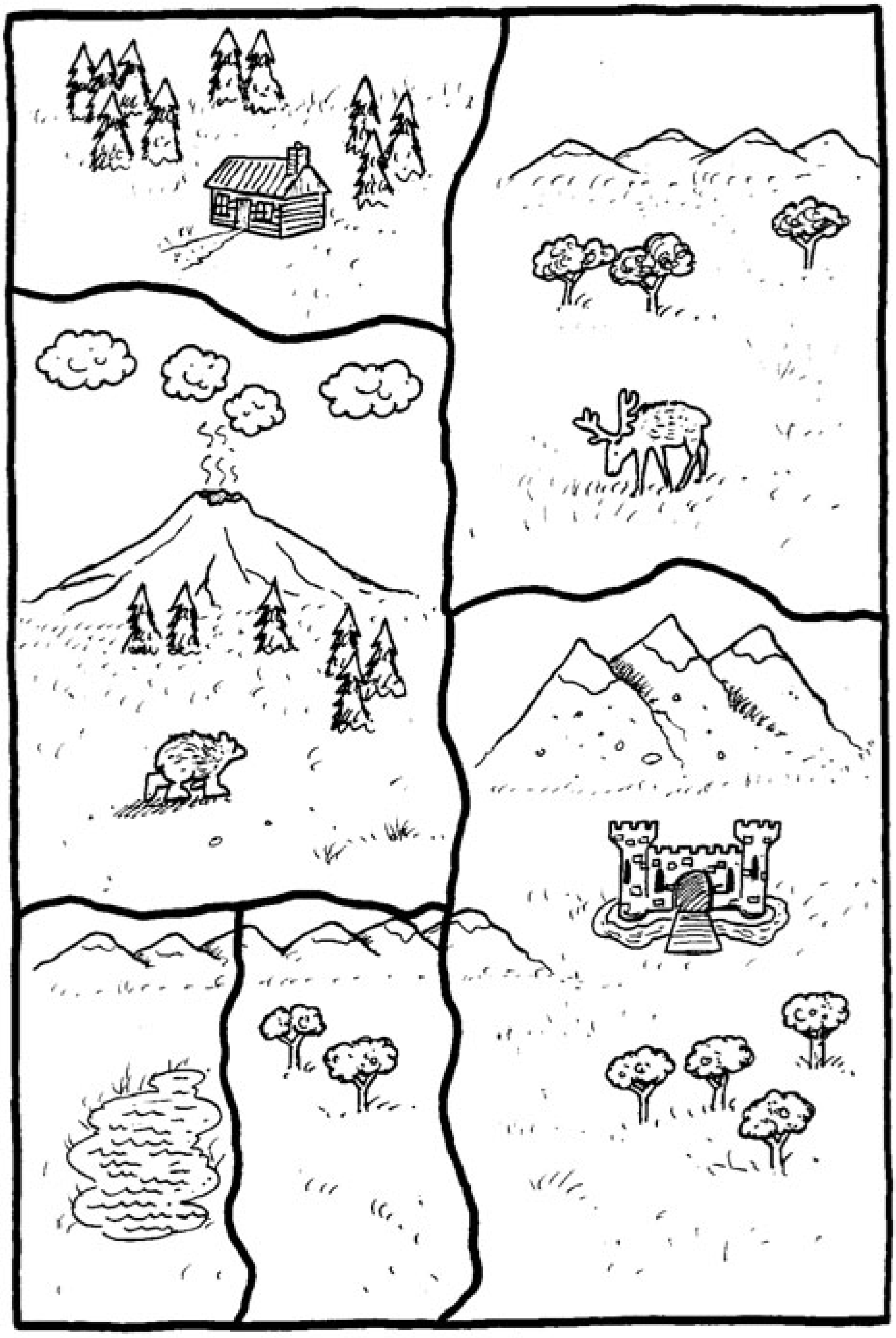
Färbe die Länder auf dieser Karte mit so wenigen Farben wie möglich, aber stellen sicher, dass keine zwei angrenzenden Länder die gleiche Farbe haben!





Arbeitsblatt: Bild einfärben 3

Färbe die Länder auf dieser Karte mit so wenigen Farben wie möglich, aber stelle sicher, dass keine zwei angrenzenden Länder die gleiche Farbe haben!

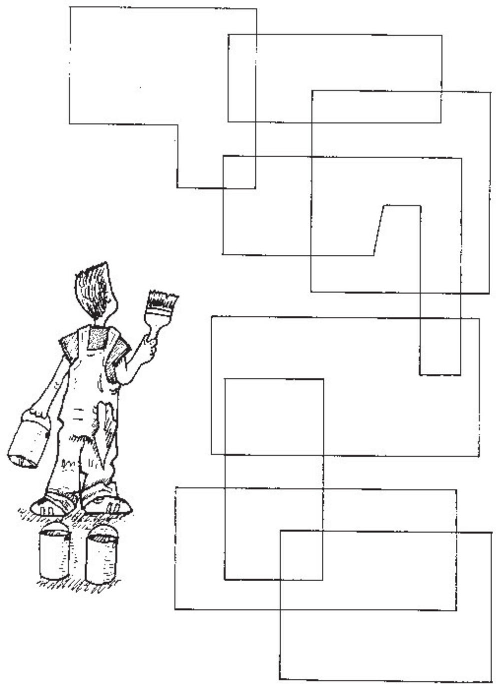


Arbeitsblatt: Bild einfärben 4

Färbe die Länder auf dieser Karte mit so wenigen Farben wie möglich, aber stelle sicher, dass keine zwei angrenzenden Länder die gleiche Farbe haben!

Variationen und Erweiterungen

Wie hier gezeigt, gibt es eine einfache Möglichkeit Karten zu erstellen, die nur zwei Farben benötigen. Diese Karte wurde gezeichnet, indem geschlossene Kurven (Linien, deren Anfang sich mit ihrem Ende verbindet) überlagert wurden.



Du kannst eine beliebige Anzahl dieser Kurven in beliebiger Form übereinander zeichnen, und erhältst immer eine Karte, die mit zwei Farben gefärbt werden kann. Die SchülerInnen können mit der Erstellung dieser Art von Karte experimentieren.

Vier Farben reichen immer aus, um eine Karte auf einem Blatt Papier oder auf einer Kugel (also einem Globus) zu zeichnen. Man könnte sich fragen (wozu Wissenschaftler_Innen ja bezahlt werden), wie viele Farben für Karten benötigt werden, die auf schrägen Oberflächen gezeichnet sind, wie zum Beispiel der Torus (die Form eines Donuts).

In diesem Fall braucht man fünf Farben, und fünf sind immer genug. Die SchülerInnen möchten vielleicht damit experimentieren.

Es gibt viele andere kurzweilige Varianten des Kartenfärbungsproblems, die in Richtungen führen, in denen vieles noch unbekannt ist.

Wenn ich zum Beispiel eine Karte auf einem Blatt Papier selbst male, weiß ich, dass vier Farben ausreichen, wenn ich clever arbeite. Aber angenommen, dass ich anstatt alleine zu arbeiten, mit einem inkompetenten (oder sogar gegnerisch gestimmten) Partner arbeite und wir wechseln uns ab, wenn wir die Farbe für Länder wählen. Angenommen, ich arbeite clever, während mein Partner nur „korrekt" arbeitet, wenn wir Länder auf der Karte färben. Wie viele Buntstifte müssen auf dem Tisch liegen, damit ich in meiner Klugheit die korrekten, aber nicht sehr schlauen (oder sogar subversiven) Schritte meines Partners wiedergutmachen kann?

Die maximale Anzahl ist nicht bekannt! 1992 wurde bewiesen, dass 33 Buntstifte immer genug sein werden und 2008 wurde durch einen Beweis gezeigt, dass 17 ausreichen würden, aber wir wissen immer noch nicht, dass diese vielen Schritte tatsächlich jemals benötigt werden. (Expert_Innen vermuten, dass weniger als 10 Farben ausreichen.)

Die SchülerInnen mögen es diese Situation auszuleben, die als Zwei-Personen-Spiel gespielt werden kann, indem sie versuchen, die Anzahl der Farben zu maximieren, die ihr Gegner braucht.

In einer anderen Variante der Karteneinfärbung, die als Empire-Färbung bekannt ist, beginnen wir mit zwei verschiedenen Karten auf zwei Blättern Papier mit der gleichen Anzahl an Ländern. Jedes Land auf einer der Karten (z. B. die Erde) wird mit genau einem Land auf der anderen Karte gepaart (das könnten Kolonien auf dem Mond sein).

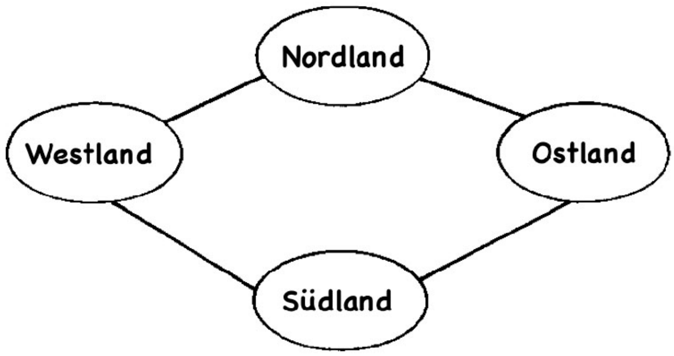
Zusätzlich zu den üblichen Farbanforderungen verschiedener Farben für Länder, die eine Grenze teilen (für beide Karten), fügen wir die Anforderung hinzu, dass jedes Erdland genauso wie seine Kolonie auf dem Mond gefärbt sein muss. Wie viele Farben brauchen wir für dieses Problem? Die Antwort ist derzeit unbekannt.

Worum geht es in dieser Aktivität?

Das Problem mit der Karteneinfärbung, das wir in dieser Übung untersucht haben, besteht im Wesentlichen darin, die Mindestanzahl von Farben zu finden, die zum Ausmalen einer bestimmten Karte erforderlich sind - zwei, drei oder vier. Die Vermutung, dass jede Karte nur mit vier Farben gefärbt werden kann, wurde 1852 formuliert, aber erst 1976 bewiesen. Die Informatik ist voll ungelöster Probleme und zu wissen, dass das Vier-Farben-Theorem nach mehr als 120 Jahren Aufmerksamkeit von ForscherInnen bewiesen wurde, ist eine Ermutigung für diejenigen, die an anderen Problemen arbeiten, deren Lösung seit Jahrzehnten nicht gelungen ist.

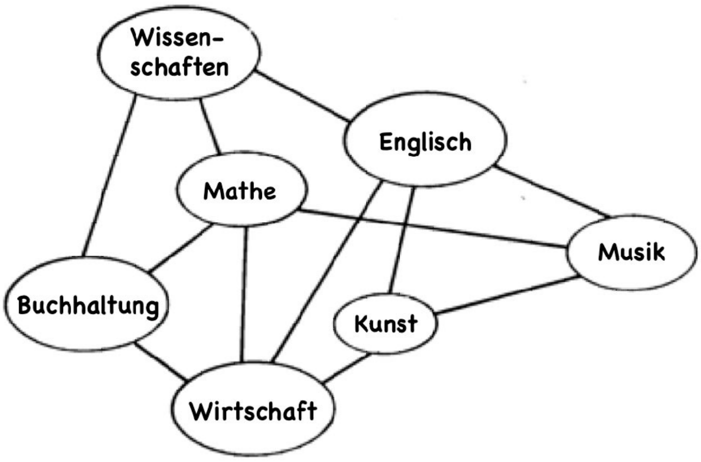
Kartenfärbung gehört zu einer allgemeinen Klasse von Problemen, in der Graphentheorie bekannt als „Färbung". In der Informatik ist ein Graph eine abstrakte Darstellung von Beziehungen, wie hier gezeigt wird.

Wie in Aktivität 9 über die Schlammstadt erwähnt, wird der Begriff ‚Graph' in der Mathematik in einer anderen Bedeutung verwendet, um ein Diagramm zu bezeichnen, das numerische Daten wie ein Balkendiagramm anzeigt. Aber die Graphen, die InformatikerInnen benutzen, stehen damit nicht in Zusammenhang. In der Informatik werden Graphen mit Kreisen oder großen Punkten gezeichnet, die technisch „Knoten" genannt werden, um Objekte zu bezeichnen, wobei Linien zwischen ihnen eine Art von Beziehung zwischen den Objekten anzeigen.



Der obige Graph stellt die Karte am Anfang dieser Aktivität dar. Die Knoten repräsentieren die Länder und eine Linie zwischen zwei Knoten zeigt an, dass diese beiden Länder eine gemeinsame Grenze haben. In der Graphentheorie bedeutet die Farbregel, dass keinem Nachbarknoten die gleiche Farbe zugewiesen werden soll. Anders als bei einer Karte gibt es keine Begrenzung für die Anzahl der Farben, die ein allgemeiner Graph benötigen könnte, da viele verschiedene Beschränkungen als Verbindungslinien eingezeichnet werden können, während die zweidimensionale Natur von Karten die möglichen Anordnungen einschränkt. Das „Graphenfärbung-Problem" besteht darin, die minimale Anzahl von Farben zu finden, die für einen bestimmten Graphen benötigt werden.

Die Knoten in dem Graphen rechts beziehen sich auf Schulfächer.



Eine Linie zwischen zwei Fächern zeigt an, dass mindestens ein Schulkind beide Fächer belegt und daher nicht für denselben Zeitraum geplant werden sollte. Unter Verwendung dieser Darstellung entspricht das Problem, einen funktionsfähigen Stundenplan unter Verwendung der minimalen Anzahl von Perioden zu finden, dem Färbungsproblem, bei dem die verschiedenen Farben unterschiedlichen Zeitbereichen entsprechen.

Algorithmen zur Graphenfärbung sind von großem Interesse in der Informatik und werden für viele reale Probleme verwendet, obwohl sie wahrscheinlich nie zum Einfärben von Karten verwendet werden - unser armer Kartograph ist nur eine Fiktion!
Es gibt buchstäblich Tausende andere Probleme, die auf Graphentheorie basieren. Einige werden an anderer Stelle in diesem Buch beschrieben, wie der minimal spannende Baum von Aktivität 9 und die Dominating Sets von Aktivität 15. Graphen sind eine sehr allgemeine Art der Darstellung von Daten und können verwendet werden, um alle Arten von Situationen darzustellen, wie zum Beispiel eine Karte aus Straßen und Kreuzungen, Verbindungen zwischen Atomen in einem Molekül, Pfade, die Nachrichten über ein Computernetzwerk aufnehmen können, Verbindungen zwischen Komponenten auf einer Leiterplatine und Beziehungen zwischen den Aufgaben, die zur Durchführung eines großen Projekts erforderlich sind. Aus diesem Grund haben Probleme mit Graphendarstellungen die InformatikerInnen seit langem fasziniert.

Viele dieser Probleme sind konzeptionell nicht schwierig, aber sehr schwierig, weil sie lange brauchen, um gelöst zu werden. Zum Beispiel könnte ein Computer zur Bestimmung der effizientesten Lösung für ein Graphenfärbungsproblem von mäßiger Größe - wie zum Beispiel die Suche nach dem besten Weg, eine Schule mit dreißig Lehrern und 800 Schülern zu planen - Jahre oder sogar Jahrhunderte dauern, obwohl er den bekanntesten Algorithmus verwendet. Das Problem wäre irrelevant zu dem Zeitpunkt, bei dem die Lösung gefunden wurde, und zwar unter der Annahme, dass der Computer nicht kaputt geht oder abgenutzt wird, bevor er damit fertig ist! Solche Probleme werden nur in der Praxis gelöst, weil wir uns mit suboptimalen, aber immer noch sehr guten Lösungen zufrieden geben. Wenn wir darauf bestehen würden, die gefundene Lösung als die beste zu garantieren, wäre das Problem völlig unlösbar.

Die Menge an Computerzeit, die zur Lösung von Farbproblemen benötigt wird, steigt exponentiell mit der Größe des Graphen. Betrachten wir das Problem mit der Karteneinfärbung. Es kann gelöst werden, indem man alle möglichen Wege ausprobiert, um die Karte zu färben. Wir wissen, dass höchstens vier Farben benötigt werden, daher müssen wir jede Kombination der Zuordnung der vier Farben zu den Ländern bewerten. Da es n Länder gibt, gibt es 4n Kombinationen.

Diese Zahl wächst sehr schnell: Jedes Land, das hinzugefügt wird, multipliziert die Anzahl der Kombinationen mit vier und vervierfacht somit die Lösungszeit. Selbst wenn ein Computer erfunden würde, der das Problem für beispielsweise fünfzig Länder in nur einer Stunde lösen könnte, würde das Hinzufügen eines weiteren Landes vier Stunden erfordern, und wir müssten nur zehn weitere Länder hinzufügen, damit der Computer ein Jahr braucht um die Lösung zu finden. Diese Art von Problem wird nicht verschwinden, auch wenn wir immer schnellere Computer erfinden!

Die Färbung von Graphen ist ein gutes Beispiel für ein Problem, dessen Lösungszeit exponentiell zunimmt. Für sehr einfache Fälle des Problems, wie die kleine Anzahl von Karten, die in dieser Aktivität verwendet werden, ist es ziemlich einfach, die optimale Lösung zu finden, aber sobald die Anzahl der Länder über zehn steigt, wird das Problem sehr schwierig um von Hand zur Lösung zu kommen und mit 100 oder mehr Ländern kann sogar ein Computer viele Jahre brauchen, um alle möglichen Möglichkeiten auszuprobieren, um die optimale Lösung der Kartenfärbung zu finden.

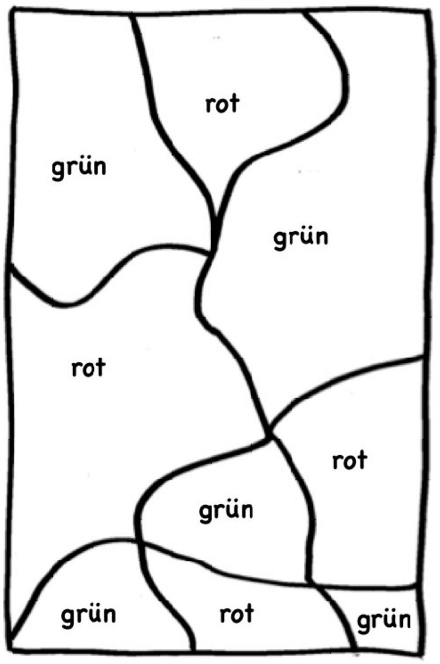
Viele Probleme im wirklichen Leben sind von dieser Art, müssen aber trotzdem gelöst werden. InformatikerInnen verwenden auch Methoden, die gute, aber nicht perfekte Antworten geben. Diese heuristischen Techniken sind oft sehr nahe am Optimum, sehr schnell zu berechnen und geben Antworten, die für alle praktischen Zwecke nahe genug am Ziel sind. Schulen können es tolerieren, ein Klassenzimmer mehr zu benutzen als notwendig, wenn der Zeitplan perfekt wäre. Und vielleicht könnte sich der arme Kartograph eine zusätzliche Farbe leisten, obwohl es nicht unbedingt notwendig ist.

Niemand hat bewiesen, dass es keinen effizienten Weg gibt, um diese Art von Problemen auf herkömmlichen Computern zu lösen, ebenso hat bisher niemand das Gegenteil bewiesen und ComputerwissenschaftlerInnen sind skeptisch, dass jemals eine effiziente Methode gefunden werden kann. Wir werden in den nächsten beiden Aktivitäten mehr über diese Art von Problem erfahren.

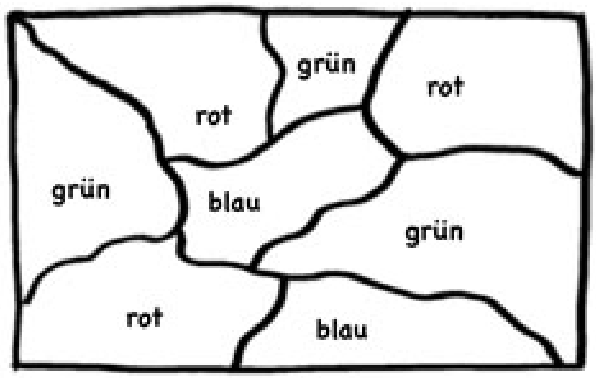
Weiterführende Literatur

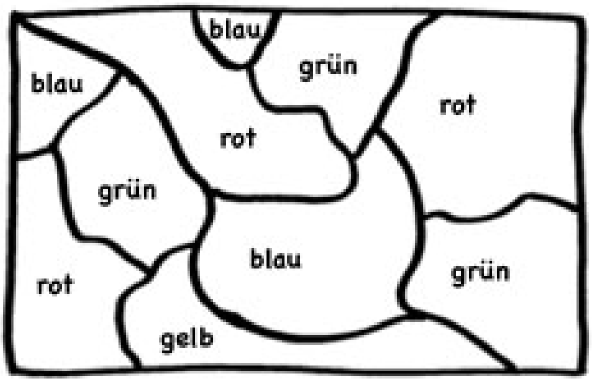
Harel diskutiert das Vier-Farben-Theorem einschließlich dessen Geschichte in *Algorithmics*. Weitere Aspekte des Kartenfärbungsproblems werden in D*ies ist MEGA-Mathematik!* von Casey und Fellows besprochen. Kubale’s 2004 erschienenes Buch *Graph Colorings* enthält eine Geschichte des Problems. Es gibt auch viele Internetseiten, die dieses Thema behandeln.

Lösungen und Tipps

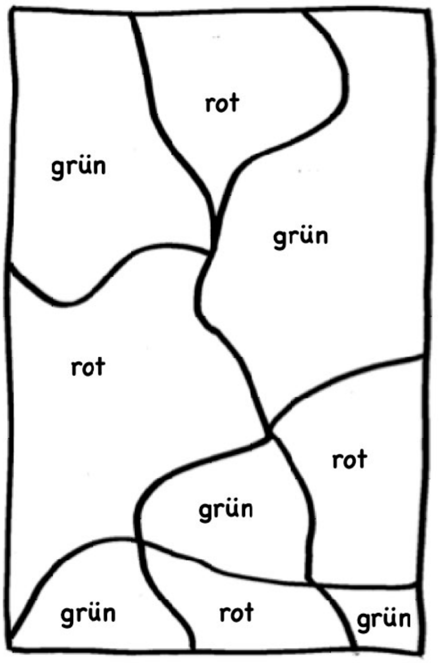


Dies ist die einzige mögliche Lösung der Aufgabe auf dem Arbeitsblatt 1 (natürlich ist die Auswahl der Farben Sache der SchülerInnen, aber nur zwei verschiedene Farben werden benötigt).

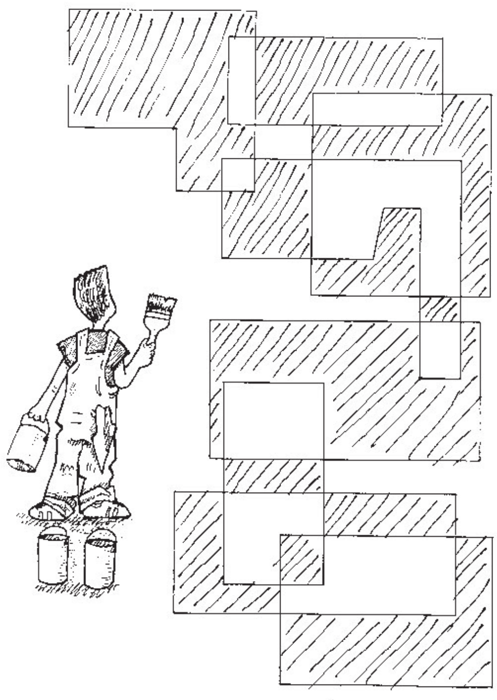




Die obere Karte von Arbeitsblatt 2 kann mit drei Farben korrekt eingefärbt werden, während die untere Karte vier benötigt. Hier sind zwei mögliche Lösungen.



Die Karte auf dem Arbeitsblatt 3 ist eine einfache 3-Farben Karte. Eine mögliche Lösung wird hier dargestellt.



Die Lösung für Arbeitsblatt 4, unter Verwendung von nur zwei Farben (schattiert und weiß).

Aktivität 15: Die Touristenstadt – Absorptionsmengen

Zusammenfassung

Viele reale Situationen können in der Form eines Netzwerkes oder „Graphen“ dargestellt werden, wie es in der Aktivität 14 verwendet wird. Netzwerke bieten viele Möglichkeiten für die Entwicklung von praktischen, nützlichen Algorithmen. In dieser Aktivität möchten wir einige der Knotenpunkte oder „Knoten“ so markieren, dass alle anderen Knoten höchstens einen Schritt von einem der markierten entfernt sind. Die Frage ist, mit wie wenigen markierten Knoten können wir auskommen? Dies stellt sich als ein überraschend schwieriges Problem heraus.

Einfügen in den Lehrplan

- Mathematik – Position und Orientierung
- Mathematik – Logisches Denken

Benötigte Kenntnisse

- Karten
- Beziehungen
- Puzzle lösen
- Iterative Zielsuche

Alter

- 7+

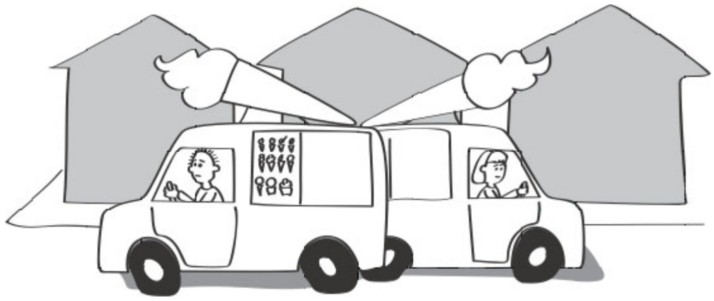
Materialien

Jede Gruppe wird Folgendes brauchen:

- eine Kopie des Arbeitsblattes Eiswagen und
- mehrere Spielsteine oder Jetons in zwei verschiedenen Farben.

Du wirst Folgendes brauchen:

- eine Projektion des Arbeitsblatts Eiswagen Lösung auf einer Weißwandtafel oder zeichne es auf die Weißwandtafel.



Absorptionsmengen

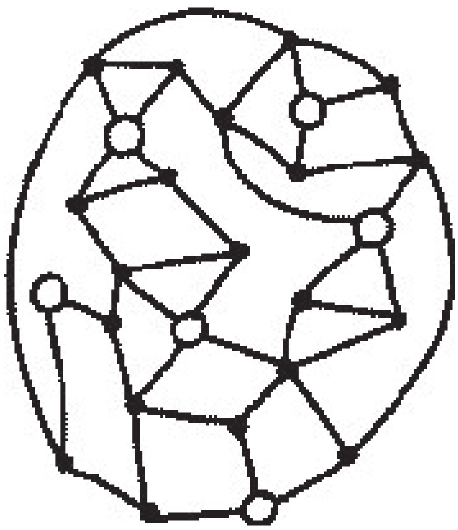
Einführung

Auf dem Arbeitsblatt Eiswagen befindet sich eine Karte der Touristenstadt. Die Linien sind Straßen und die Punkte sind Straßenecken. Die Stadt liegt in einem sehr heißen Land und in der Sommersaison parken Eiswagen an Straßenecken und verkaufen Eis an Touristen. Wir wollen die Wagen so platzieren, dass jeder einen erreichen kann, indem er bis zum Ende seiner Straße und dann höchstens einen Block weiter gehen muss.

(Es ist einfacher sich Menschen vorzustellen, die an den Kreuzungen leben, als entlang der Straßen; dann müssen sie in der Lage sein Eis zu bekommen, indem sie höchstens einen Block entlang gehen.)

Die Frage ist, wie viele Eiswagen werden benötigt und an welchen Kreuzungen sollen sie platziert werden?

Diskussion



1. Teile die SchülerInnen in kleine Gruppen auf, gebe jeder Gruppe die Karte der Touristenstadt und einige Jetons und erkläre das Vorgehen.
2. Zeige den SchülerInnen, wie man einen Jeton an einer Kreuzung platziert, um einen Eiswagen zu markieren, und platziere dann andersfarbige Jetons an den Kreuzungen eine Straße weiter. Menschen, die an diesen Kreuzungen (oder entlang der Straßen, die in sie hineinführen) leben, werden von diesem Eiswagen bedient.
3. Lass die SchülerInnen mit verschiedenen Positionen für die Eiswagen experimentieren. Wenn sie Positionen finden, die allen Häusern dienen, erinnere die SchülerInnen daran, dass Eiswagen teuer sind und es das Ziel ist, so wenige wie möglich zu nutzen.

Es ist offensichtlich, dass die Bedingungen erfüllt werden können, wenn genügend Eiswagen an allen Kreuzungen vorhanden sind - die interessante Frage ist, mit wie wenigen davon man auskommen kann.

4. Die Mindestanzahl von Eiswagen für die Touristenstadt ist sechs und eine Lösung wird hier gezeigt. Aber es ist sehr schwierig, diese Lösung zu finden! Sage der Klasse nach einiger Zeit, dass sechs Eiswagen ausreichen und fordere sie auf, sie entsprechend zu platzieren.

Das ist immer noch ein schwieriges Problem: Viele Gruppen werden sicher irgendwann aufgeben. Selbst eine Lösung mit acht oder neun Eiswagen ist schwierig zu finden.

5. Die Karte der Touristenstadt wurde erstellt, indem man mit den sechs Kartenteilen der unteren Hälfte des Arbeitsblattes Eiswagen Lösung begann (Seite 151), von denen jedes offensichtlich nur einen Eiswagen benötigt und diese dann mit vielen Straßen verbindet, um die Lösung zu verschleiern.

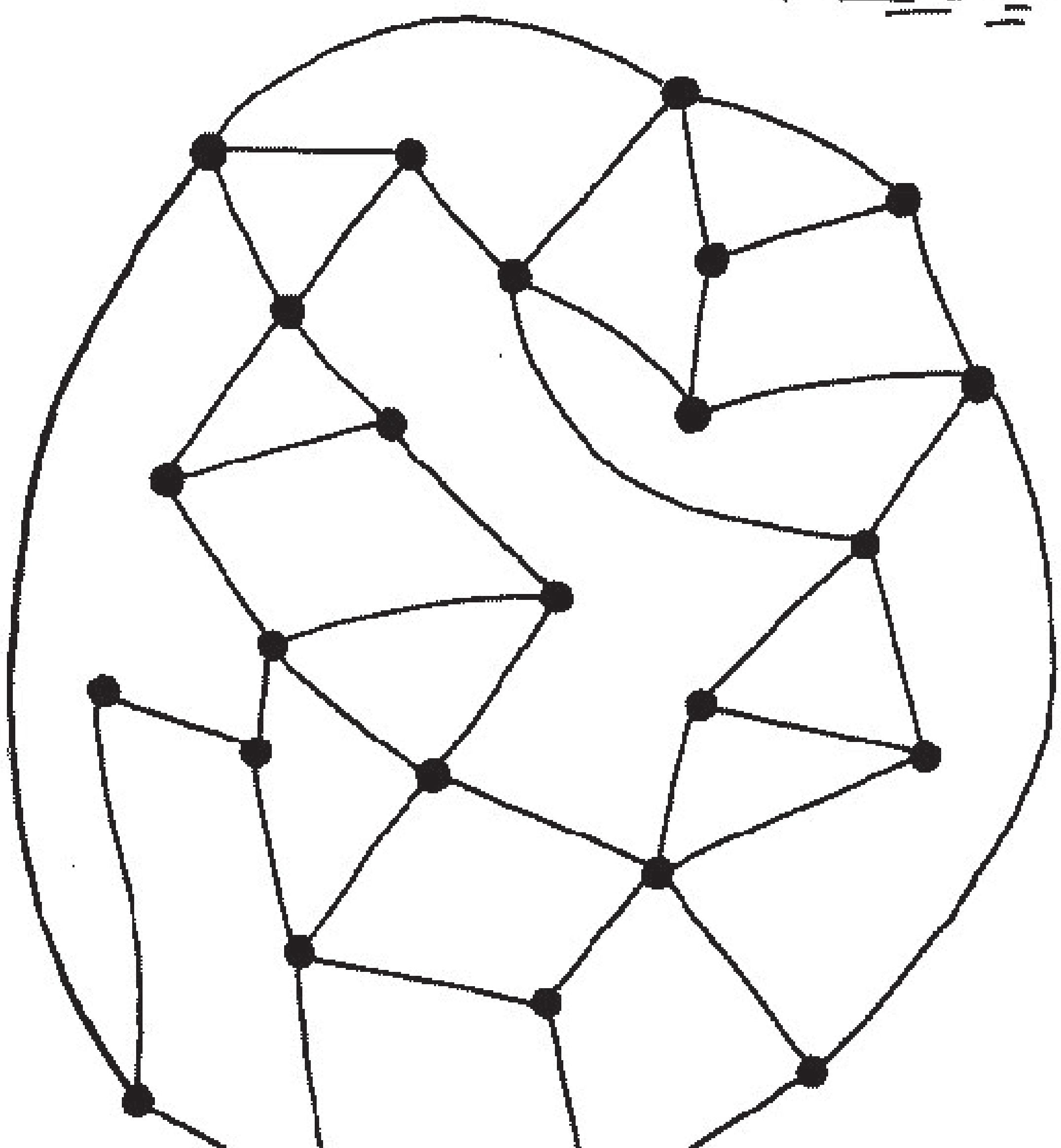
Die Hauptsache ist, keine Verbindungen zwischen den Lösungskreuzungen (den ungefüllten Punkten) herzustellen, sondern nur zwischen den zusätzlichen (den gefüllten) Punkten. Zeige der Klasse diese Technik auf dem Brett oder mit einem Projektor.

6. Lass die SchülerInnen mit dieser Strategie ihre eigenen schwierigen Karten erstellen. Vielleicht möchten sie diese dann mit ihren Freunden und Eltern ausprobieren - du wirst feststellen, dass die SchülerInnen Rätsel erstellen können, die sie selbst lösen können, andere jedoch nicht!

Dies sind Beispiele für eine sogenannte „Einweg-Funktion“: Es ist einfach, ein Puzzle zu entwickeln, das nur schwer zu lösen ist - es sei denn, du bist derjenige, der es erstellt hat. Einwegfunktionen spielen eine entscheidende Rolle in der Kryptographie (siehe Aktivitäten 17 und 18).

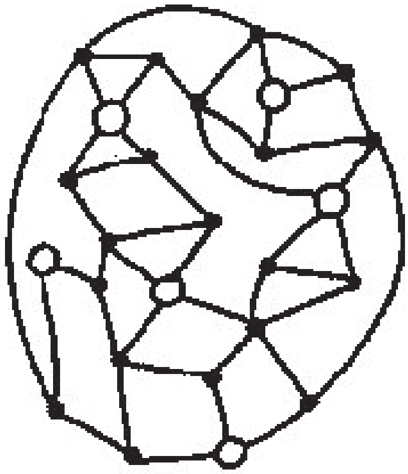
Arbeitsblatt: Eiswagen

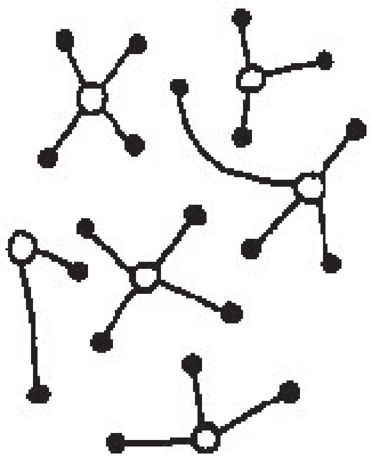
Finde heraus, wie du die Eiswagen an den Straßenkreuzungen platzieren kannst, sodass jede andere Kreuzung mit einem Eiswagen verbunden ist.



Arbeitsblatt: Eiswagen Lösung

Zeige dies der Klasse, um zu erklären, wie das Puzzle aufgebaut wurde.





Variationen und Erweiterungen

Es gibt viele mögliche Situationen, in denen man mit einem solchen Problem in der Stadtplanung konfrontiert werden könnte: das Aufstellen von Briefkästen, Brunnen, Feuerwachen und so weiter. Im wirklichen Leben wird die Planung aber nicht auf einem so einfachen Trick basieren. Wenn du ein Problem wie dieses wirklich lösen musst, wie würdest du das machen?

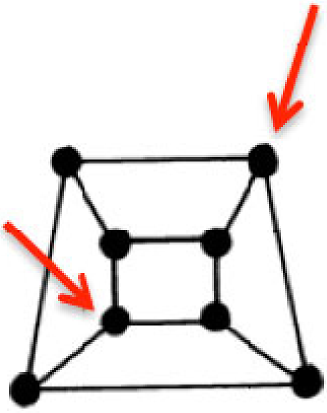
Es gibt einen sehr einfachen Weg: Betrachte alle Möglichkeiten Eiswagen zu platzieren und überprüfe, welche die beste ist. Mit den 26 Straßenecken in der Touristenstadt gibt es 26 Möglichkeiten, um nur einen Lieferwagen zu platzieren. Es ist einfach alle 26 Möglichkeiten zu überprüfen und es ist offensichtlich, dass keine davon die gewünschte Bedingung erfüllt. Mit zwei Eiswagen gibt es 26 Plätze, um den ersten aufzustellen und je nachdem, welcher Platz für den ersten Eiswagen bereits gewählt wurde, sind noch 25 Plätze frei, um den zweiten Eiswagen zu platzieren (natürlich würde man nicht beide Eiswagen an der gleichen Kreuzung platzieren): Demnach sind 26 × 25 = 650 Möglichkeiten zu überprüfen. Auch hier ist jeder Check einfach, obwohl es sehr mühsam wäre, sie alle durchzuführen. Eigentlich musst du nur die Hälfte (325) überprüfen, da es egal ist, um welchen Eiswagen es sich handelt: D.h. wenn du Eiswagen 1 an der Kreuzung A und Eiswagen 2 an der Kreuzung B überprüft hast, brauchst du nicht auch den Fall überprüfen, wenn Eiswagen 1 an Kreuzung B steht und Eiswagen 2 bei Kreuzung A. Weiter kannst du es mit drei Eiswagen (2600 Möglichkeiten), vier Eiswagen (14950 Möglichkeiten) und so weiter prüfen. Selbstverständlich sind 26 Eiswagen genug, da es nur 26 Kreuzungen gibt und es keinen Sinn hat, mehr als einen Eiswagen am selben Ort zu haben. Eine andere Möglichkeit die Anzahl der Möglichkeiten zu bewerten, ist die Gesamtzahl der Konfigurationen mit 26 Kreuzungen und einer beliebigen Anzahl von Eiswagen. Da es für jede Straßenecke zwei Möglichkeiten gibt – entweder steht dort ein Eiswagen oder nicht - beträgt die Anzahl der Anordnungen 226, was 67.108.864 entspricht.

Dieses Vorgehen das Problem zu lösen, wird als „Brute-Force"-Algorithmus bezeichnet und braucht sehr viel Zeit. Es ist ein weit verbreitetes Missverständnis, dass Computer so schnell sind, dass sie jedes Problem schnell lösen können, egal wie viel Arbeit es beinhaltet. Das stimmt aber nicht. Wie lang der Brute-Force-Algorithmus braucht, hängt davon ab wie schnell überprüft werden kann, ob eine bestimmte Anordnung eine Lösung ist. Um dies zu überprüfen, muss jede Kreuzung getestet werden, um die Entfernung zum nächstgelegenen Eiswagen zu finden. Angenommen eine ganze Anordnung kann in einer Sekunde getestet werden. Wie lange dauert es, alle 226 Möglichkeiten für die Touristenstadt zu überprüfen?

(*Antwort: 226 entspricht ungefähr 67 Millionen; ein Tag hat 86.400 Sekunden, also entsprechen 226 Sekunden ungefähr 777 Tagen, respektive ungefähr zwei Jahre.) Und angenommen, statt einer Sekunde dauert es nur eine tausendstel Sekunde, um jede einzelne Anordnung zu überprüfen. Dann würde der Computer etwa zwei Jahre brauchen für eine Stadt, die 36 Kreuzungen hat, denn 236 ist etwa 1000 mal 226. Selbst wenn der Computer eine Million mal schneller wäre, sodass pro Sekunde eine Million Anordnungen überprüft werden könnten, würde es zwei Jahre dauern, bis er eine Stadt mit 46 Kreuzungen durchsucht hat. Und das sind keine sehr großen Städte! (Wie viele Kreuzungen gibt es in deiner Stadt?*)

Da der Brute-Force-Algorithmus so langsam ist, gibt es andere Möglichkeiten das Problem zu lösen?

Tja, wir könnten den ‚gierigen' Ansatz versuchen, der in der Schlammstadt so erfolgreich war (Aktivität 9). Wir müssen darüber nachdenken, wie man gierig auf Eiscreme wird - ich meine, wie man den gierigen Ansatz auf das Eiswagenproblem anwendet.



Eine Möglichkeit ist es, den ersten Eiswagen an der Kreuzung zu platzieren, die die größte Anzahl von Straßen verbindet, die zweite Wahl ist die nächste noch nicht gewählte Kreuzung, die die größte Anzahl von Straßen verbindet, und so weiter. Dies führt jedoch nicht unbedingt zu einem Minimum an Stellplätzen für Eiswagen – tatsächlich ist die am meisten vernetzte Kreuzung in der Touristenstadt, die über fünf Straßen verfügt, kein guter Ort um dort einen Eiswagen hin zu stellen (bitte prüfe das mit der Klasse).

Schauen wir uns ein einfacheres Problem an. Statt eine minimale Anordnung zu suchen nimm einmal an, dass man dir eine Anordnung gegeben hat und du gefragt wurdest, ob diese minimal ist oder nicht. In einigen Fällen ist das einfach. Zum Beispiel zeigt dieses Diagramm eine schlichte Karte, deren Lösung ziemlich einfach ist. Wenn du dir die Straßen als Würfelränder vorstellst, ist es klar, dass zwei Eiswagen an diagonal gegenüberliegenden Würfelecken ausreichen (siehe die roten Pfeile).

Außerdem sollte dir klar sein, dass es nicht möglich ist, das Problem mit weniger als zwei Eiswagen zu lösen. Es ist viel schwieriger, wenn auch nicht unmöglich, sich davon zu überzeugen, dass die Touristenstadt nicht von weniger als sechs Eiswagen bedient werden kann. Das heißt, dass es im Allgemeinen extrem schwierig zu beweisen ist, dass eine bestimmte Anordnung von Eiswagen minimal ist.

Worum geht es in dieser Aktivität?

Eines der interessanten Dinge an der Eiswagen-Problematik ist, dass niemand weiß, ob es einen Algorithmus gibt um eine minimale Anzahl von Orten zu finden, der wesentlich schneller ist als die Brute-Force-Methode!

Die Zeit, die die Brute-Force-Methode braucht, wächst exponentiell mit der Anzahl der Kreuzungen - man spricht von einem exponentiellen Algorithmus oder Exponentialzeitalgorithmus. Ein Polynomialzeitalgorithmus (oder auch: polynomieller Algorithmus) ist einer, dessen Laufzeit mit dem Quadrat oder der dritten Potenz oder irgendeiner anderen Potenz der Anzahl von Kreuzungen wächst. Ein Polynomialzeitalgorithmus wird für ausreichend große Straßenkarten - sogar (sagen wir) für einen Algorithmus mit Laufzeit der siebzehnten Potenz - immer schneller sein, da eine exponentiell wachsende Funktion jede polynomiell wachsende Funktion überwiegt, sobald ihr Argument groß genug wird. (Probiere es an folgendem Beispiel aus: wenn n größer ist als 117, dann ist n17 kleiner als 2n).

Gibt es einen Polynomialzeitalgorithmus, um die minimale Anzahl von Standorten zu finden? - Niemand weiß es, obwohl man sehr bemüht ist, einen zu finden. Das gleiche gilt für die scheinbar einfachere Aufgabe zu überprüfen, ob eine bestimmte Menge von Standorten minimal ist: Der Brute-Force-Algorithmus, der alle Möglichkeiten für kleinere Mengen von Standorten ausprobiert, ist exponentiell abhängig von der Anzahl der Kreuzungen, und polynomielle Algorithmen wurden bisher nicht entdeckt oder es konnte auch nicht bewiesen werden, dass diese gar nicht existieren.

Erinnert dich das an die Färbung der Karte (Aktivität 13)?

Das sollte es. Die Eiswagen-Frage, die offiziell als Bestimmung minimaler Absorptionsmengen bezeichnet wird, ist eines von vielen Tausend Problemen, für die nicht bekannt ist, ob Polynomialzeitalgorithmen in Bereichen von logischen über puzzle-typische Anordnungsprobleme bis hin zur Kartenfärbung existieren, um optimale Routen auf Karten zu finden und Prozesse zu planen. Erstaunlicherweise haben sich alle diese Probleme in dem Sinne als äquivalent erwiesen, dass wenn ein Polynomialzeitalgorithmus für eines von ihnen gefunden wird, dieser für alle anderen in einen Polynomialzeitalgorithmus umgewandelt werden kann - man könnte sagen, es gibt nur ein gemeinsames Gewinnen oder Verlieren.

Solche Probleme werden NP-vollständig genannt. ‚NP' bedeutet: „nicht-deterministisch in Polynomialzeit". Dieser Jargon bedeutet, dass das Problem in einer angemessenen Zeit gelöst werden könnte, wenn man einen Computer hätte, der eine beliebig große Anzahl von Lösungen auf einmal überprüfen könnte (das ist der nicht-deterministische Teil).

Du könntest meinen, dass dies eine ziemlich unrealistische Annahme ist, und das ist auch tatsächlich so. Es ist nicht möglich, einen solchen Computer zu bauen, da dieser beliebig groß sein müsste! Das Konzept einer solchen Maschine ist jedoch im Prinzip wichtig, da NP-vollständige Probleme anscheinend nicht in einer vernünftigen Zeitspanne ohne einen nicht-deterministischen Computer gelöst werden können.

Darüber hinaus wird diese Gruppe von Problemen als vollständig bezeichnet, weil obwohl die Probleme sehr unterschiedlich erscheinen - zum Beispiel, Kartenfäbung ist sehr unterschiedlich verglichen mit der Platzierung der Eiswagen – sich herausstellt, dass, wenn eine effiziente Lösung für ein Problem gefunden wird, die Methode auch angepasst werden kann, um jedes Problem dieser Gruppe zu lösen. Das ist es auch, was wir oben unter ‚gemeinsames Gewinnen oder Verlieren' zum Ausdruck gebracht haben.

Es gibt Tausende von NP-vollständigen Problemen und ForscherInnen haben sie auf der Suche nach effizienten Lösungen für mehrere Jahrzehnte bisher ohne Erfolg verfolgt. Wenn für nur eines von ihnen eine effiziente Lösung gefunden worden wäre, hätten wir effiziente Lösungen für alle Probleme. Aus diesem Grund wird stark vermutet, dass es keine effiziente Lösung gibt. Aber zu beweisen, dass die Probleme notwendigerweise exponentielle Zeit benötigen, ist heute die herausragendste offene Frage in der theoretischen Informatik - möglicherweise in der gesamten Mathematik.

Weiterführende Literatur

Harels Buch *Algorithmics* stellt mehrere NP-vollständige Probleme vor und diskutiert die Frage, ob polynomielle Algorithmen existieren. In Dewdneys *Turing Omnibus* wird auch NP-Vollständigkeit diskutiert. Das Standardwerk im Bereich Computerwissenschaften zu diesem Thema ist Garey & Johnsons *Computer and Intractivability*, in dem mehrere hundert NP-vollständige Probleme, zusammen mit Techniken zum Nachweis der NP-Vollständigkeit, vorgestellt werden. Allerdings ist es ziemlich schwerfällig und eignet sich wirklich nur für InformatikspezialistInnen.

Aktivität 16: Eisstraßen – Steinerbäume

Zusammenfassung

Manchmal löst eine kleine, scheinbar unbedeutende Änderung in der Beschreibung eines Problems einen großen Unterschied aus, der schwerer zu lösen ist. In dieser Aktivität geht es ähnlich wie beim Problem in der Schlammstadt (Aktivität 9) zu, wo es darum geht kurze Wege durch Netzwerke zu finden. Der Unterschied in dieser Aktivität besteht darin, dass hier neue Punkte in das Netzwerk eingefügt werden dürfen, wenn dies die Pfadlänge reduziert. Das Ergebnis ist ein weitaus schwierigeres Problem, das nicht mit der Schlammstadt zusammenhängt, sondern algorithmisch dem Puzzle des Kartographen (Aktivität 13) und der Touristenstadt (Aktivität 15) entspricht.

Einfügen in den Lehrplan

- Mathematik – Position und Orientierung
- Mathematik – Logisches Denken

Benötigte Kenntnisse

- Räumliche Veranschauung
- Geometrisches Denken
- Algorithmische Verfahren und Komplexität

Alter

- 7+

Materialien

Jede Gruppe wird Folgendes brauchen:

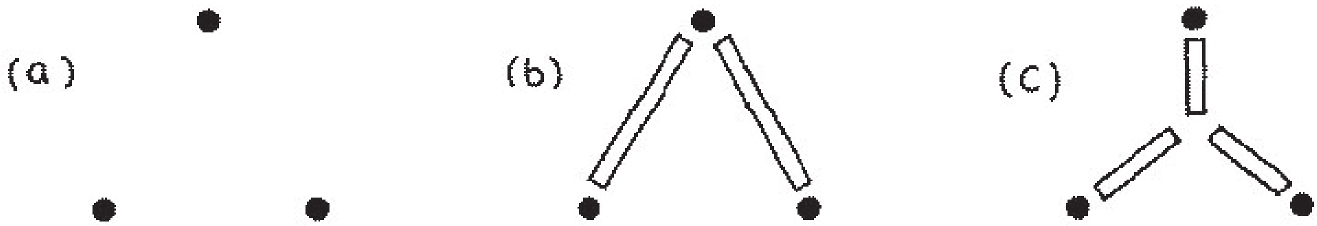
- fünf oder sechs Pflöcke für den Boden (Zeltpflöcke sind gut; es kann auch ein Kleiderbügel verwendet werden, der in Stücke geschnitten ist, die dann umgebogen werden),
- mehrere Meter Schnur oder Gummiband,
- ein Lineal oder ein Maßband und
- ein Stift und Papier für Notizen.

Eisstraßen

Einführung

Die vorherige Aktivität, Touristenstadt, fand in einem sehr heißen Land statt; das ist jetzt genau das Gegenteil. Im gefrorenen Norden Kanadas machen (so die Geschichte) im Winter auf den riesigen gefrorenen Seen, Schneepflüge Straßen, um Bohrstellen zu verbinden, sodass die Besatzungen sich gegenseitig besuchen können. Draußen in der Kälte soll nur ein Minimum an Straßenbauarbeiten gemacht werden und deine Aufgabe ist es nun herauszufinden, wo man die Straßen bauen soll. Es gibt keine Beschränkungen: Autobahnen können überall durch den Schnee führen - die Seen sind gefroren und bedeckt. Es ist alles flach.

Die Straßen sollten natürlich als gerade Strecken erstellt werden, da das Einführen von Kurven die Länge nur unnötig vergrößern würde. Auch wenn es nicht so einfach ist wie eine Direktverbindung aller Standorte mit geraden Straßen, kann das Hinzufügen von Kreuzungen in der gefrorenen Eiswüste manchmal doch die gesamte Straßenlänge reduzieren - und es ist die Gesamtlänge wichtig, nicht die Reisezeit von einem Ort zum anderen.

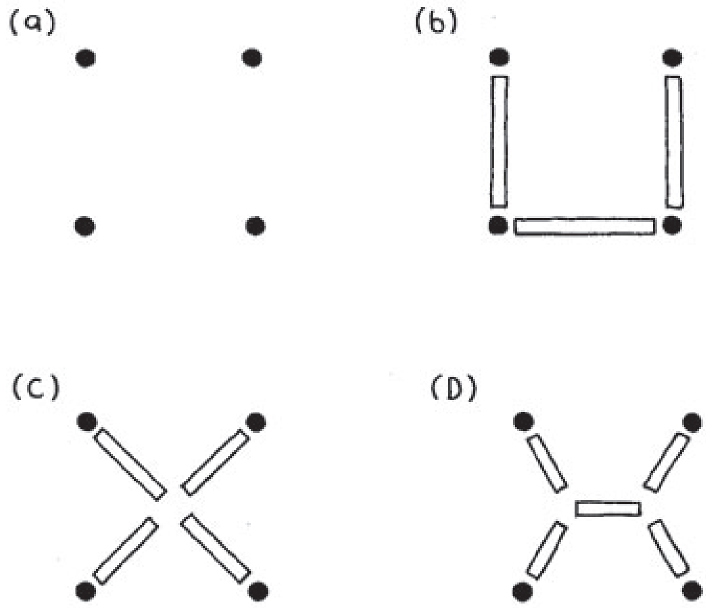


Diese Abbildung zeigt (a) drei Bohrstandorte.

Das Verbinden eines von ihnen mit jedem der anderen (wie in (b)) würde ein akzeptables Straßennetz ergeben. Eine andere Möglichkeit besteht darin, eine Kreuzung irgendwo in der Mitte des Dreiecks zu erstellen und sie mit den drei Orten zu verbinden (c). Und wenn du die Gesamtlänge der freigeräumten Straße misst, ist dies in der Tat eine bessere Lösung. Die zusätzliche Straßenkreuzung wird nach dem Schweizer Mathematiker Jacob Steiner (1796-1863) als „Steiner"-Punkt bezeichnet, der das Problem darstellte und als Erster bemerkte, dass die Gesamtlänge durch Einführung neuer Punkte reduziert werden kann. Man kann sich einen Steiner-Punkt als neue, fiktive Bohrstelle vorstellen.

Diskussion

Beschreibe das Problem, an dem die SchülerInnen arbeiten werden. Zeige den SchülerInnen anhand des obigen Beispiels, dass das Hinzufügen einer neuen Bohrstelle zu den bereits exitierenden drei Standorten, manchmal die Lösung verbessert, indem der Straßenbau reduziert wird.



1. Die SchülerInnen benutzen vier in einem Quadrat angeordnete Punkte, wie in (a) dargestellt. Geht nach draußen und lass jede Gruppe vier Pflöcke im Gras auf einem Quadrat von etwa 1 Meter mal 1 Meter platzieren.

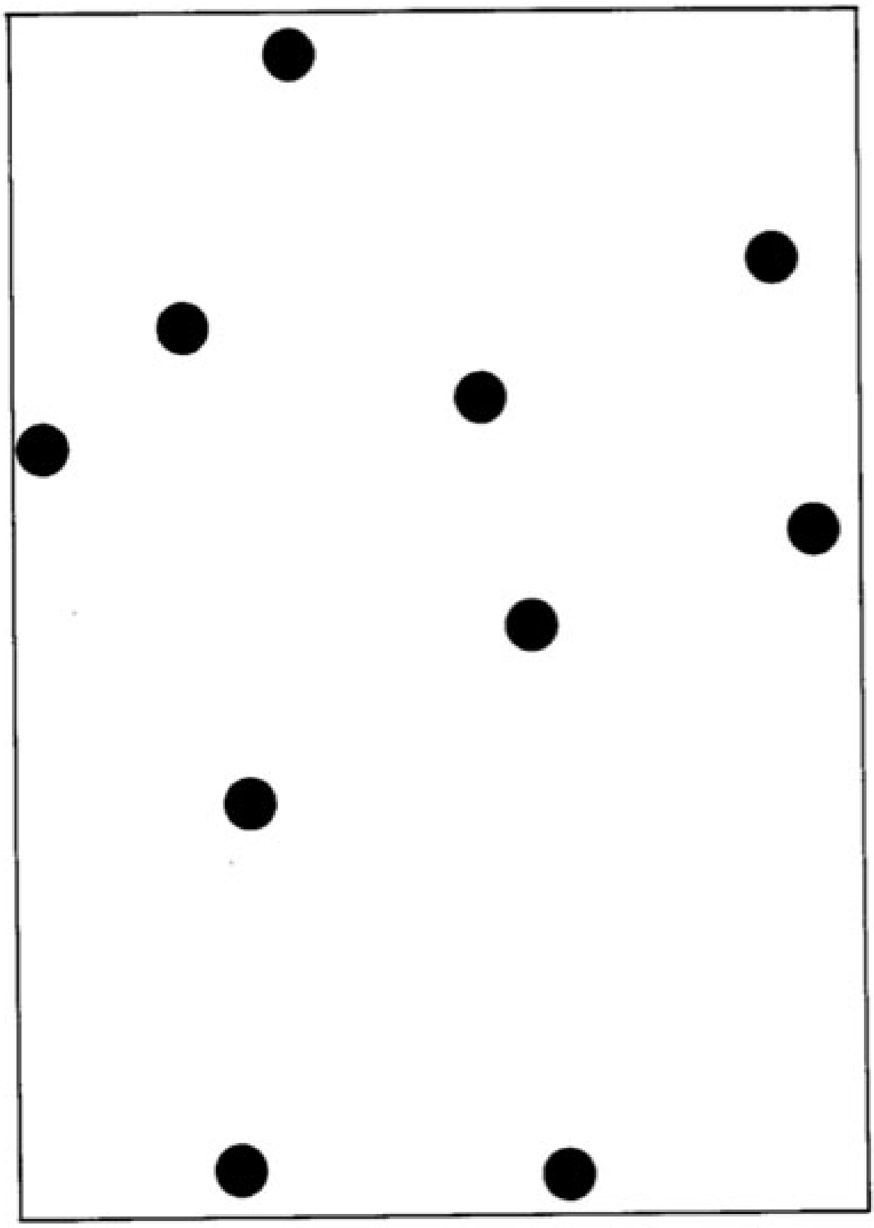
2. Lass die SchülerInnen experimentieren, indem sie die Stifte mit Schnur oder Gummiband verbinden und die erforderliche Mindestgesamtlänge messen und aufzeichnen. Jetzt sollten sie noch keine Steiner-Punkte verwenden. (Das Minimum wird erreicht durch Verbinden von drei Seiten des Quadrats, wie in (b) gezeigt; die Gesamtlänge beträgt 3 Meter.)

3. Beobachte jetzt, ob die SchülerInnen es mit einem Steiner-Punkt besser machen können. (Der beste Platz ist in der Mitte der Fläche, (c). Dann ist die Gesamtlänge $2\sqrt{2} = 2{,}83$ Meter.) Schlage vor, dass es zwei Steiner-Punkte noch besser machen könnten. (Das gelingt, indem die SchülerInnen die zwei Punkte, wie in (d) dargestellt, setzen und einen 120 Grad Winkel zwischen den ankommenden Straßen bilden. Die Gesamtlänge ist dann $1 + \sqrt{3} = 2{,}73$ Meter.)

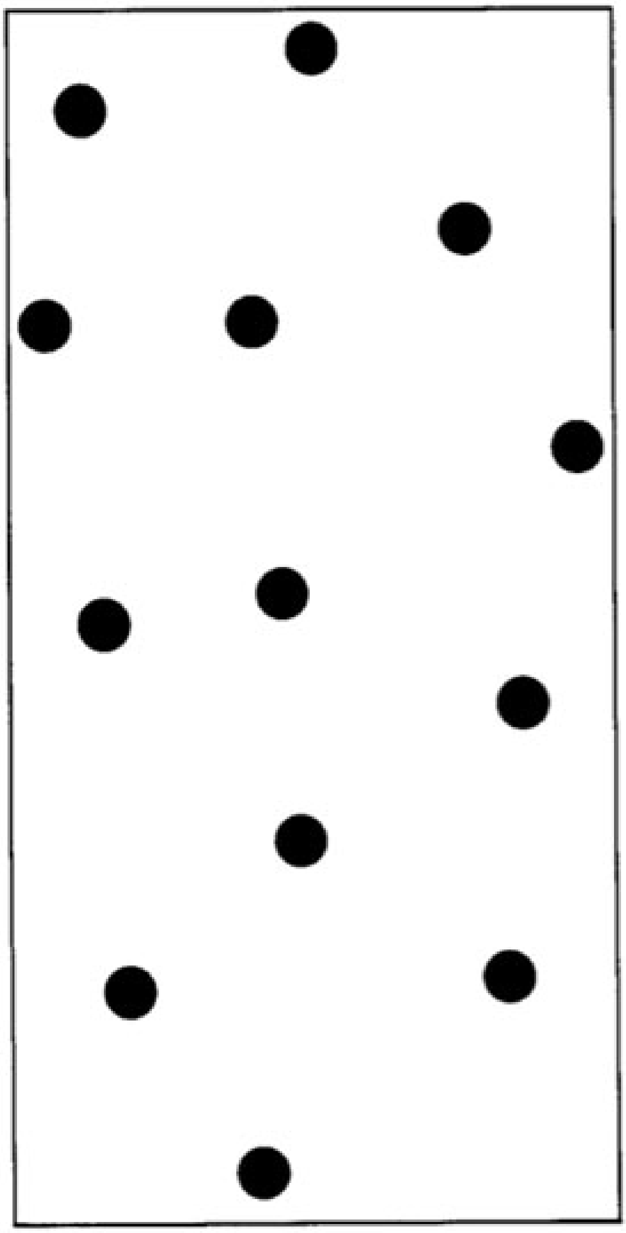
4. Können die SchülerInnen das mit drei Steiner-Punkten noch verbessern? (Nein - zwei Punkte sind am besten und durch die Verwendung von mehr als zwei Punkten wird kein Vorteil erzielt.)

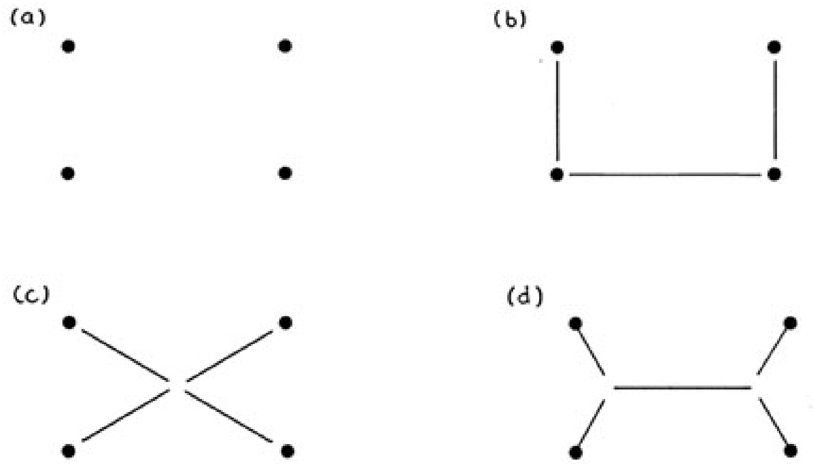
5. Bespreche mit den SchülerInnen, warum diese Probleme schwierig erscheinen. (Es ist, weil die SchülerInnen nicht wissen, wo sie die Steiner-Punkte positionieren sollen, und es gibt viele Möglichkeiten es auszuprobieren.)

Arbeitsblatt: Steinerbaum - Beispiel 1



Arbeitsblatt: Steinerbaum - Beispiel 2





Variationen und Erweiterungen

1. Ein interessantes Experiment für Gruppen, die die ursprüngliche Aktivität früh beenden, ist das Arbeiten mit einem Rechteck von etwa 1 mal 2 Metern (a).

Die SchülerInnen werden feststellen, dass das Hinzufügen eines Steiner-Punktes die Situation verschlimmern kann, aber zwei ergeben die bessere Lösung.
(Die Länge beträgt 4 Meter für (b), $2\sqrt{5} = 4{,}47$ Meter für (c) und $2 + \sqrt{3} = 3{,}73$ Meter für (d).)

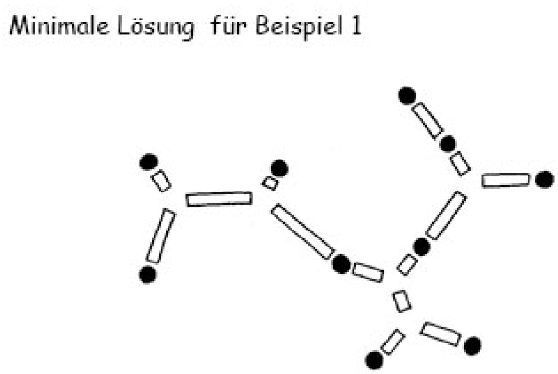
Verfolge, ob die SchülerInnen herausfinden können, warum die Ein-Punkt-Konfiguration für Rechtecke viel schlechter ist als für Quadrate.
(Es ist so, weil wenn das Quadrat in ein Rechteck gestreckt wird, die Dehnung in (b) und (d) nur einmal hinzugefügt wird, aber beide Diagonalen in (c) zunehmen.)

2. Ältere SchülerInnen können ein größeres Problem bearbeiten.

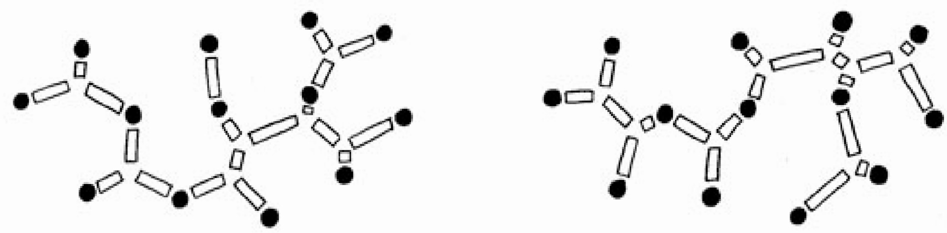
In den Arbeitsblättern sind zwei Layouts von Punkten zum Verbinden zu Eisstraßen angegeben. Die SchülerInnen können mit verschiedenen Lösungen experimentieren, indem Sie entweder neue Kopien des Arbeitsblatts verwenden oder mit einem löschbaren Stift auf einer Folie über dem Blatt schreiben.

Alternativ dazu können die Karten auch mit Stöpseln am Boden befestigt werden. Informiere die Klasse, wenn du feststellst, dass sie einen neuen Rekord für die kürzeste Distanz aufgestellt hat.

(Die Abbildung auf der rechten Seite zeigt die minimale Lösung für das erste Beispiel und unten (auf der anderen Seite) gibt es zwei mögliche Lösungen für das zweite, deren Gesamtlänge sehr ähnlich ist.)



Zwei mögliche Steinerbäume für Beispiel 2



Die Tatsache, dass es zwei ähnliche Lösungen gibt zeigt, warum solche Probleme so schwer sind - es gibt sehr viele Möglichkeiten, wo man die Steiner-Punkte platzieren kann!

3. Ein Leitungsnetzwerk wie dieses bietet eine weitere Möglichkeit, das Problem zu erweitern:

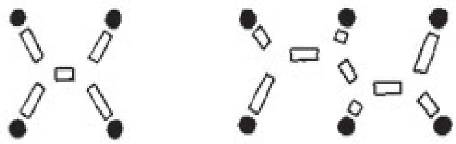
Unten rechts werden einige minimale Steinerbäume für Leiternetzwerke gezeigt.

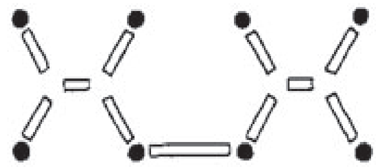
Der für eine Zweisprossenleiter ist genau der gleiche wie für ein Quadrat. Für eine Leiter mit drei Sprossen ist die Lösung jedoch ganz anders – wie du feststellen wirst, wenn du versuchst, es wieder aus der Erinnerung zu holen!.

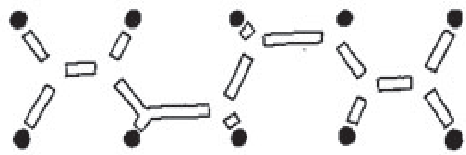
Die Lösung für vier Sprossen ist wie für zwei miteinander verbundene Sprossenleitern, während sie für fünf Sprossen eher eine Erweiterung der Lösung für drei Sprossen ist.

Allgemein hängt die Form des minimalen Steinerbaums für eine Leiter davon ab, ob sie eine gerade oder ungerade Anzahl von Sprossen aufweist. Ist die Anzahl gerade, ist es, als ob mehrere Zwei-Sprossen-Leitern zusammengefügt werden.

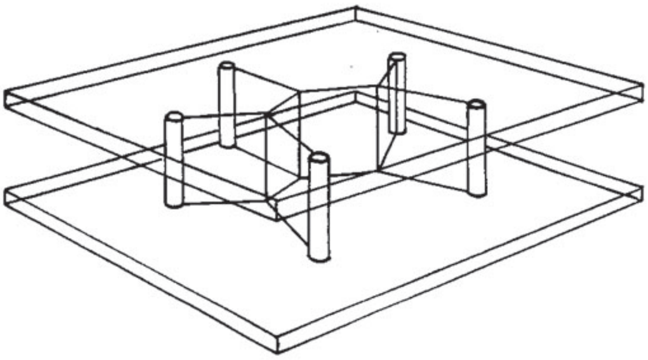
Ansonsten ist es wie eine Wiederholung der Drei-Sprossen-Lösung. Aber diese Dinge grundsätzlich zu beweisen, ist nicht einfach.







4. Eine weitere interessante Darstellung besteht darin, Seifenblasenmodelle von Steinerbäumen zu konstruieren. Du kannst das machen, indem du zwei Lagen aus durchsichtigem Kunststoff nimmst und dazwischen Stifte einsetzt, um die zu überspannenden Punkte darzustellen, wie hier gezeigt wird. Nun tauche das Ganze in eine Seifenlösung ein. Wenn du es heraushebst, wirst du feststellen, dass ein Seifenfilm die Stifte in einem schönen Steinerbaum-Netzwerk verbindet.



5. Leider ist es aber nicht unbedingt ein minimaler Steinerbaum. Der Seifenfilm wird aufgestellt, so dass die Gesamtlänge minimiert wird, d.h. das Minimum ist nur lokal, nicht notwendigerweise global. Es kann nämlich völlig unterschiedliche Wege geben, die Steiner-Punkte auf eine kleinere Gesamtlänge zu positionieren. Zum Beispiel kannst du dir sicher vorstellen, dass der Seifenfilm wie die erste Möglichkeit von Beispiel 2 aussieht (s.Bild ‚Zwei mögliche Steinerbäume für Beispiel 2' auf Seite 162), wenn er zum ersten Mal aus der Flüssigkeit gezogen wird, und beim zweiten Versuch wie das andere Bild rechts daneben.

Worum geht es in dieser Aktivität?

Die Netzwerke, an denen wir gearbeitet haben, sind minimale Steinerbäume. Sie werden „Bäume“ genannt, weil sie keine Zyklen haben, genau so wie die Zweige auf einem echten Baum auseinander wachsen, sich aber (normalerweise) nicht wieder vereinigen und wieder zusammenwachsen. Sie werden „Steiner“-Bäume genannt, weil neue Punkte, Steiner-Punkte, zu den ursprünglichen Standorten hinzugefügt werden können, die die Bäume verbinden. Und sie werden „minimal“ genannt, weil sie die kürzeste Länge eines Baumes haben, der all diese Punkte verbindet. In der Schlammstadt (Aktivität 9) haben wir gelernt, dass ein Netzwerk, das eine Anzahl von Punkten verbindet, die die Gesamtlänge minimiert, ein minimal aufspannender Baum genannt wird: Steinerbäume sind genauso, außer dass neue Punkte eingeführt werden können.

Es ist interessant, dass es zwar einen sehr effizienten Algorithmus zum Aufspüren minimaler Spannbäume gibt (Aktivität 14) - ein gieriger, der die beiden nächsten, bisher nicht verbundenen Punkte wiederholt verbindet - es aber keine allgemein effiziente Lösung für das minimale Steiner-Problem gibt. Steinerbäume sind viel komplexer, weil du entscheiden musst, wo du die Extrapunkte einsetzen möchtest. Tatsächlich ist es eher überraschend, dass der schwierige Teil des Steinerbaum-Problems nicht darin besteht, die genaue Position der Steiner-Punkte zu bestimmen, sondern grob zu entscheiden, wo sie platziert werden sollen: zum Beispiel den Unterschied zwischen den zwei Lösungen zu Beispiel 2. Sobald du weißt, in welche Regionen die neuen Punkte eingefügt werden sollen, ist die Feinabstimmung auf die optimale Position relativ einfach. Seifenfilme machen das sehr effektiv, genauso wie Computer.

Minimale Steinerbäume zu finden ist Teil einer Geschichte, die das Einsparen von viel Geld im Telefongeschäft bewirkt hat. Vor 1967, als Firmenkunden in den USA große private Telefonnetze betrieben, mieteten sie die Leitungen von einer Telefongesellschaft. Der Betrag, den sie in Rechnung stellten, wurde nicht auf der Grundlage berechnet, wie die Drähte tatsächlich verwendet worden sind, sondern auf der Grundlage der kürzesten Netzverbindung, die möglich war. Der Grund war, dass der Kunde nicht extra bezahlen musste, nur weil die Telefongesellschaft eine Rundum-Route verwendete. Ursprünglich arbeitete der Algorithmus, der die Kosten berechnete, durch das Bestimmen des minimalen aufspannenden Baums. Um 1967 wurde jedoch von einem Kunden - einer Fluggesellschaft mit drei großen Netzknoten - bemerkt, dass die Gesamtlänge des Netzwerks reduziert würde, wenn sie einen vierten Netzknoten als Zwischenpunkt anfordern würden. Die Telefongesellschaft musste die Gebühren auf das reduzieren, was sie gewesen wären, wenn es am Steiner-Punkt eine Telefonzentrale gegeben hätte! Obwohl der minimale Steinerbaum bei typischen Einstellungen nur 5% oder 10% kürzer ist als der minimale Spannbaum, kann dies eine lohnende Einsparung sein, wenn große Geldbeträge betroffen sind. Das Steinerbaum-Problem wird manchmal als „kürzestes Netzwerkproblem“ bezeichnet, da das kürzeste Netzwerk, das eine Gruppe von Punkten verbindet, gefunden wird.

Wenn du die beiden vorhergehenden Aktivitäten, das Puzzle und die Touristenstadt des Kartographen, bereits bearbeitet hast, wirst du nicht überrascht sein zu hören, dass das minimale Steinerbaum-Problem NP-vollständig ist. Mit steigender Anzahl der Standorte erhöht sich auch die Anzahl der möglichen Standorte für Steiner-Punkte und der Versuch, alle Möglichkeiten zu nutzen erfordert eine exponentiell wachsende Suche. Dies ist ein weiteres der Tausenden von Problemen, für die es einfach nicht bekannt ist, ob die exponentielle Suche das Beste ist, was gemacht werden kann, oder ob es einen noch nicht entdeckten polynomiellen Algorithmus gibt. Es ist jedoch bekannt dass, wenn ein Polynomialzeitalgorithmus für dieses Problem gefunden wird, dieser in einen Polynomzeitalgorithmus für die Graphfärbung umgewandelt werden kann, um minimale Absorptionsmengen zu finden - und das gilt auch für alle anderen NP-vollständigen Probleme.

Wir haben am Ende der vorherigen Aktivität erklärt, dass „NP“ im Begriff NP-vollständig für „nicht-deterministisches Polynom“ steht und „complete“ bedeutet, dass wenn ein polynomieller Algorithmus für eines der NP-vollständigen Probleme existiert, dann können auch alle anderen NP-vollständigen Probleme zu polynomiellen Algorithmen umgewandelt werden. Die Menge der Probleme, die in polynomieller Zeit lösbar sind, wird „P“ bezeichnet. Die entscheidende Frage ist also, ob es für NP-vollständige Probleme polynomielle Algorithmen gibt - mit anderen Worten, ist P = NP? Die Antwort auf diese Frage ist nicht bekannt, und es ist eines der großen Geheimnisse der modernen Informatik.

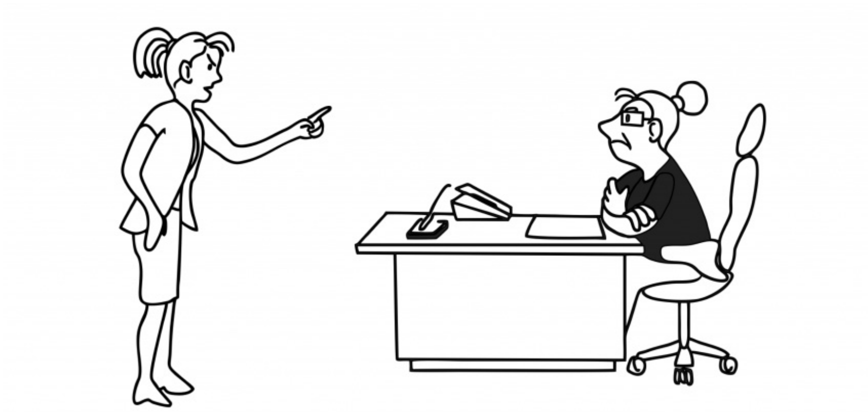
Probleme, für die polynomielle Algorithmen existieren - auch wenn diese Algorithmen sehr langsam sind - werden als „machbar“ bezeichnet. Probleme, für die polynomielle Algorithmen nicht existieren, werden als „hartnäckig“ bezeichnet, denn unabhängig davon wie schnell dein Computer ist oder wie viele Computer du gleichzeitig verwendest, bedeutet ein kleiner Anstieg der Problemgröße, dass sie in der Praxis nicht gelöst werden können. Es ist nicht bekannt, ob die NP-vollständigen Probleme – zu denen auch das Puzzle des Kartographen, die Touristenstadt und die Eisstraßen gehören – „machbar“ sind oder nicht. Aber die meisten ComputerwissenschaftlerInnen sind pessimistisch und vermuten, dass ein polynomialer Algorithmus für NP-vollständige Probleme niemals gefunden werden kann. Daher wird der Beweis, dass ein Problem NP-vollständig ist als starker Beweis dafür angesehen, dass das Problem von Natur aus unlösbar ist.

Was kannst du tun, wenn dein Chef / deine Chefin dich auffordert einen effizienten Algorithmus zu entwickeln, der die optimale Lösung für ein Problem ermöglicht und du findest keinen?

– Beispiel dazu ist der Fall, wo eine Fluggesellschaft auf die Tatsache stieß, dass die Netzwerkkosten durch Einführung von Steiner-Punkten reduziert werden konnten. Es wäre schon vorab großartig, wenn du beweisen könntest, dass es keinen effizienten Algorithmus gibt um die optimale Lösung zu finden. Aber es ist sehr schwierig, negative Ergebnisse wie diese in der Informatik zu beweisen, denn wer weiß schon, welche/r schlaue ProgrammiererIn in der Zukunft einen obskuren Trick findet, der das Problem löst. Es ist also unwahrscheinlich, dass du in der Lage bist, kategorisch zu sagen, dass kein effizienter Algorithmus existiert - dass das Problem demnach unlösbar ist.

Wenn du aber zeigen kannst, dass dein Problem NP-vollständig ist, dann ist es stark anzunehmen, dass Tausende von Menschen in Forschungslaboratorien an ähnlichen Problemen gearbeitet haben, die deinem eigenen Problem entsprechen, und es auch nicht geschafft haben, eine effiziente Lösung zu finden. Das bringt vielleicht keinen Bonus, aber es bringt dich aus dem Schneider!

“Ich kann keinen effizienten Algorithmus finden, ich denke, ich bin einfach zu dumm.”



“Ich kann keinen effizienten Algorithmus finden, weil kein solcher Algorithmus möglich ist.”

“Ich kann keinen effizienten Algorithmus finden, aber all diese berühmten Leute auch nicht.” *

* Die zeitgenössische Version des Cartoons wurde von Prof. Stefan Szeider erstellt. Mehr: https://www.ac.tuwien.ac.at/people/szeider/cartoon/

Natürlich müssen solche Probleme im wirklichen Leben noch gelöst werden und dann wenden sich die Leute der Heuristik zu - Algorithmen, die nicht garantieren die bestmögliche Lösung zu geben, aber eine Lösung geben, die sehr nahe an der optimalen Lösung liegt. Heuristische Algorithmen können sehr schnell sein, und der Verlust nicht die bestmögliche Lösung zu finden, kann ziemlich klein sein, sodass sie gut genug sind, um die Aufgabe zu erledigen. Es ist einfach frustrierend zu wissen, dass es einen etwas besseren Zeitplan oder einen etwas besseren Entwurf für ein Netzwerk oder für Straßen geben könnte.

Weiterführende Literatur

Der Cartoon basiert auf einem aus Gareys und Johnsons Buch “Computers and Intractivability”.

Berühmt ist eine Karikatur, die einen Forscher darstellt, der seinem Chef Bericht erstattet und begründet, warum er eine bestimmte Aufgabe nicht erfüllen konnte. Mit diesem Szenario veranschaulicht die Karikatur, wie die Methode der NP-Vollständigkeit verwendet werden kann, um ein berühmtes Dilemma der Informatik zu lösen, in dem man für buchstäblich Tausende von grundlegenden Rechenproblemen weder einen effizienten Algorithmus angeben noch beweisen kann, dass es einen solchen Algorithmus nicht gibt. Der in dieser Sammlung verwendete Cartoon wurde von Stefan Szeider angepasst und unter der Creative-Commons-Lizenz 4.0 veröffentlicht.

Die Spalte “Computer recreations” im Scientific American, Juni 1984, enthält eine kurze Beschreibung, wie man Steinerbäume mit Seifenblasen herstellt, zusammen mit interessanten Beschreibungen anderer analoger Geräte zur Problemlösung, einschließlich eines ‚Spaghetti-Computers' zum Sortieren, eines Fadenspiels mit Leinen, um den kürzesten Pfad in einem Graphen zu finden und einer Licht- und Spiegelvorrichtung zum Ermitteln, ob eine Zahl eine Primzahl ist oder nicht. Diese erscheinen auch in einem Abschnitt über analoge Computer in Dewdneys „Turing Omnibus“.

Teil V
Geheimnisse teilen und Verbrechen bekämpfen – Kryptographie

Geheimnisse teilen und Verbrechen bekämpfen

Du hast von Spionen und Geheimagenten gehört, die versteckte Codes oder magische, unsichtbare Schriften verwenden, um Nachrichten auszutauschen. So hat auch das Thema „Kryptographie” begonnen - als die Kunst, Geheimcodes zu schreiben und zu entschlüsseln. Während des Zweiten Weltkrieges bauten die Engländer spezielle elektronische Code-Entschlüsselungsmaschinen und benutzten sie, um militärische Codes zu knacken. Und dann kamen Computer und änderten alles, und die Kryptographie trat in eine neue Ära ein. Enorm viele Mengen an Berechnungen, die vorher unvorstellbar gewesen waren, konnten eingesetzt werden um Codes zu knacken. Als Leute anfingen Computersysteme miteinander zu teilen, gab es für geheime Passwörter neue Verwendungen. Als Computer in Netzwerken verbunden wurden, gab es neue Gründe, Informationen vor solchen Leuten zu schützen, die sie einfach gerne erhalten hätten. Als elektronische Post eingeführt wurde, wurde es wichtig Nachrichten so zu signieren, dass man wusste, dass eine Person wirklich die ist, die sie sagt, dass sie ist. Heute, wo Menschen Online-Banking benutzen und Waren mit Computern ein- und verkaufen können, brauchen wir sichere Verbindungen um Bestellungen aufzugeben und Zahlungen in Computernetzwerken auszuführen. Und die wachsende Bedrohung durch Terroristen, die Computersystem angreifen, macht Computersicherheit immer wichtiger.

Am Computer lässt dich Kryptographie wahrscheinlich denken, dass dadurch geheime Passwörter gespeichert und die Buchstaben von Nachrichten durcheinander gebracht werden, sodass der Feind sie nicht lesen kann. In Realität ist das ganz anders. Moderne Computersysteme speichern keine geheimen Passwörter, denn wenn sie es tun würden, könnte jeder, der Zugang zu ihnen hat, die gesamte Sicherheit des Systems durchbrechen. Das wäre katastrophal: So könnten gefälschte Banküberweisungen gemacht werden, Nachrichten gesendet werden, die vorgeben, jemand anderes zu sein, geheime Akten von jedermann gelesen werden, Armeen befehligt werden, Regierungen gestürzt werden. Heutzutage werden Passwörter mit den „Einwegfunktionen” behandelt, über die wir in Aktivität 14 gesprochen haben. Die Verschlüsselung bringt nicht nur die Buchstaben der Nachrichten in Unordnung: Sie benutzt Techniken, die wirklich harte Probleme beinhalten - wie die „hartnäckigen” Probleme, die in Teil IV eingeführt wurden.

Mit Kryptographie kannst du Dinge tun, die du für unmöglich hältst. In diesem Abschnitt findest du eine einfache Methode, um das Durchschnittsalter der Personen in einer Gruppe zu berechnen, ohne dass jemand anderes wissen lassen muss, wie alt er ist. Du wirst verstehen, wie zwei Menschen, die einander nicht vertrauen, eine Münze werfen und sich auf das Ergebnis einigen können, obwohl sie in verschiedenen Städten sind und beide nicht die geworfene Münze sehen können. Außerdem wirst du einen Weg finden, geheime Nachrichten zu verschlüsseln, die nur von einer Person entschlüsselt werden können, obwohl jeder weiß, wie man sie verschlüsselt.

Für LehrerInnen

Die folgenden Aktivitäten bieten praktische Erfahrungen mit modernen kryptographischen Techniken, die sich sehr von dem unterscheiden, was die meisten Leute meinen, wenn sie an Geheimhaltung und Computer denken.

Es gibt zwei Schlüsselideen. Die erste ist die Vorstellung eines „Protokolls”, das eine formale Aussage über eine Transaktion ist. Protokolle erinnern vielleicht an Diplomaten oder Umgangsformen - aber Computer benutzen sie auch! Scheinbar schwierige Aufgaben können durch überraschend einfache Protokolle gelöst werden. Aktivität 16, die nur wenige Minuten dauert, zeigt wie eine Gruppe von Menschen, die zusammen arbeiten, ihr Durchschnittsalter (oder ihr Einkommen) leicht berechnen kann, ohne dass jemand das Alter (oder Einkommen) einer anderen Person ermittelt. Die zweite Schlüsselidee ist eine Rolle, die die rechnerische Komplexität - Hartnäckigkeit - bei der Interaktion mit anderen Computern spielen kann. Aktivität 17 zeigt, wie sich zwei Personen, die einander nicht unbedingt vertrauen, auf das Ergebnis eines Münzwurfs einigen können, wenn sie nur per Telefon miteinander verbunden sind. (Diese Übung führt nebenbei auch die Idee von Booleschen Logikschaltungen ein und wie man mit ihnen arbeitet.) Aktivität 18 zeigt, wie Menschen mit Hilfe von Computertechniken Nachrichten sicher verschlüsseln können, obwohl das Verfahren zur Durchführung der Verschlüsselung öffentlich bekannt ist.

Einige dieser Aktivitäten - besonders die letzte - sind harte Arbeit. Sie müssen ihre Klasse motivieren, indem sie den SchülerInnen ein Gefühl des Staunens vermitteln, dass solche Dinge überhaupt möglich sind, da die Aktivitäten wirklich Dinge ausführen, die die meisten Menschen für unmöglich halten. Es ist wichtig, dieses Gefühl des Staunens zu schaffen, es zu kommunizieren und häufiger stehen zu bleiben, um es während der gesamten Aktivität am Leben zu erhalten, sodass die SchülerInnen den (erstaunlichen!) Wald vor (vielleicht ziemlich ermüdenden) Bäumen nicht sehen. Diese Aktivitäten gehören zu den anspruchsvollsten und technisch kompliziertesten im Buch. Wenn sich herausstellt, dass sie zu schwierig sind, fahren Sie bitte mit Teil VI fort, der einen völlig anderen, nicht technischen Inhalt hat.

Für die technisch Gesinnten

Da Computer in unser tägliches Leben eingreifen, ist die Anwendung der Kryptographie möglicherweise eher tendenziell. Die meisten Menschen wissen einfach nicht, zu was moderne kryptographische Protokolle fähig sind. Das Ergebnis ist, dass wenn große Institutionen - sowohl staatliche als auch kommerzielle - Systeme einrichten, die persönliche Informationen beinhalten, es eher Technokraten sind, die die entscheidenden Entscheidungen darüber treffen, wie mit den Dingen umzugehen ist, was gesammelt werden soll, was verfügbar sein soll und für wen. Wenn die Menschen die Möglichkeiten der modernen Technologie besser verstehen würden, könnten sie sich aktiver an solchen Entscheidungen beteiligen und die Gesellschaft könnte eine andere Informationsinfrastruktur haben.

Dieses Wissen über Protokolle zum Verstecken von Informationen, Verschlüsselungsprotokolle und Verschlüsselung mit öffentlichen Schlüsseln wird im Allgemeinen als ziemlich fortgeschritten angesehen. Die Ideen selbst sind nicht schwierig. Es sind die technischen Aspekte und nicht die zugrundeliegenden Konzepte, die schwer zu verstehen sind. In praktischen Situationen, die den elektronischen Handel betreffen, sind die technischen Details in Computersoftware eingebaut, wodurch die neuen Verschlüsselungstechnologien sehr einfach zu verwenden sind. Es ist aber auch wichtig die Ideen zu verstehen, auf denen sie basieren, um einen Einblick zu bekommen, was getan werden kann.

Kryptographische Systeme sind für die Regierungen von großem Interesse, nicht nur, weil sie die öffentliche Kommunikation sichern wollen, sondern auch wegen der Bedenken, dass verschlüsselte Kommunikation von Personen genutzt werden könnte, die an illegalen Aktivitäten wie Drogenhandel und Terrorismus beteiligt sind. Wenn solche Personen eine Verschlüsselung verwenden, wird das Abhören unbrauchbar, wenn keine Entschlüsselungsmethode verfügbar ist. Diese Bedenken haben viele Debatten zwischen Menschen, die sich mit der Strafverfolgung befassen, die die Stärke kryptographischer Systeme einschränken wollen und den Befürwortern der individuellen Handlungs- und Gedankenfreiheit, die sich unbehaglich fühlen, wenn die Regierung Zugang zur privaten Kommunikationen hat, verursacht. Für eine Weile hat die US-Regierung die Verwendung einiger kryptographischer Methoden eingeschränkt, indem sie sie als Munition wie Bomben und Waffen ansieht. Jeder kann mit den richtigen Informationen und einigen technischen Fähigkeiten ein sicheres Kommunikationssystem aufbauen, aber sie sind gefährlich, wenn sie in falsche Hände geraten. Zu einem Zeitpunkt gab es eine umfassende Debatte über den „Clipper Chip", ein System, das ein zusätzliches Passwort hat, das als Schlüsselhinterlegung bezeichnet wird und von einer Regierungsbehörde gehalten wird, die es ermöglicht, jede vom Chip verschlüsselte Nachricht zu entschlüsseln. Das FBI und das US-Justizministerium wollten, dass dieser Chip in großem Umfang für die Kommunikation verwendet wird, aber dies hat wegen der Bedrohung der Privatsphäre erhebliche Widerstände hervorgerufen. Alle Arten von kryptographischen Systemen sind technisch machbar, aber sie sind nicht unbedingt politisch akzeptierbar!

Kryptographische Ideen betreffen viele Anwendungsbereiche, nicht nur die Absicht, Nachrichten geheim zu halten. Wie zum Beispiel die Bestätigung, dass Nachrichten wirklich von den Leuten gesendet wurden, die sagten, dass sie sie gesendet haben - das ist „Authentifizierung" und ohne sie ist elektronischer Handel nicht möglich. Es gibt auch die Möglichkeit, das Volk per Computer abstimmen zu lassen, ohne dass jemand anderes herausfinden kann, für wen jeder einzelne gewählt hat - selbst nicht diejenigen, die das Computersystem betreiben. Gleichzeitig kann man verhindern, dass die WählerInnen mehr als einmal abstimmen. Und man kann sogar Karten über das Telefon spielen - das klingt albern, bis man versteht, dass der Ablauf von Geschäftsabschlüssen viel mit Poker zu tun hat.

Diese Dinge scheinen unmöglich zu sein. Wie könntest du anfangen einen Kartenstapel über das Telefon zu mischen, wenn du mit der Person am anderen Ende im Wettbewerb stehst und ihr deshalb nicht trauen kannst? Wie kannst du möglicherweise feststellen, dass jemand eine Nachricht abgefangen, geändert und dann als Original weitergegeben hat? Aber wenn du diese Dinge nicht tun kannst, können keine Geschäfte elektronisch abgewickelt werden. Es muss verhindert werden, dass technisch gesinnte Kriminelle Genehmigungen für Bankeinzahlungen fälschen, indem sie die Telefonleitung zwischen einem Kassenterminal und der Bank abfangen. Es muss verhindert werden, dass Geschäftskonkurrenten durch falsche Bestellungen oder falsche Verträge Schaden anrichten. Mit modernen kryptographischen Techniken können solche Wunder getan werden und diese Aktivitäten zeigen wie das geht.

Es gibt viele interessante Bücher über Codes und Codes knacken. *Codebreakers: the inside story of Bletchley Park*, herausgegeben von Hinsley und Stripp, berichtet aus erster Hand darüber, wie einige der ersten Computer während des Zweiten Weltkriegs benutzt wurden, um Codes zu knacken; wodurch der Krieg erheblich verkürzt und viele Menschenleben gerettet wurden.

Aktivität 17: Geheimnisse teilen – Protokolle zum Verstecken von Informationen

Zusammenfassung

Kryptographische Techniken ermöglichen es uns, Informationen mit anderen zu teilen und dennoch ein überraschend hohes Maß an Privatsphäre zu bewahren. Diese Aktivität veranschaulicht eine Situation, in der Informationen geteilt werden, und dennoch wird nichts davon preisgegeben: Eine Gruppe von SchülerInnen wird ihr Durchschnittsalter berechnen, ohne dass jemand anderes ihnen sein/ihr respektives Alter offenlegen muss.

Einfügen in den Lehrplan

- Mathematik – Summe und Durchschnitt

Benötigte Kenntnisse

- Durchschnittswert berechnen
- Zufallszahlen
- Zusammenarbeitende Aufgaben

Alter

- 7+

Materialien

Jede Gruppe benötigt:

- ein kleines Blatt Papier und
- einen Stift

Geheimnisse teilen

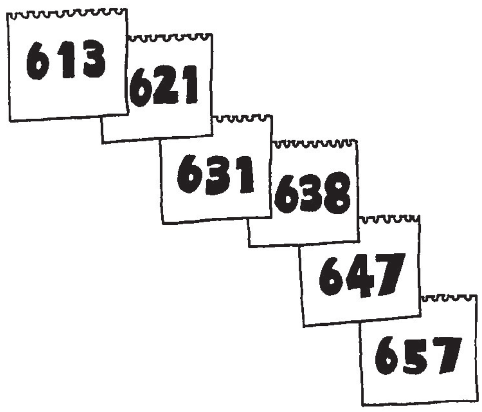
Einführung

Bei dieser Aktivität wird das Durchschnittsalter einer Gruppe von SchülerInnen ermittelt, ohne dass jemand sein Alter angeben muss. Alternativ dazu könnte man auch das durchschnittliche Einkommen (Zulage) der SchülerInnen in der Gruppe oder ähnliche persönliche Details bestimmen. Die Berechnung dieser Werte funktioniert besonders gut mit Erwachsenen, da ältere Menschen genauer auf Details wie Alter und Einkommen reagieren können.

Du brauchst mindestens drei SchülerInnen in der Gruppe.

Diskussion

1. Erkläre der Gruppe, dass du ihr Durchschnittsalter herausfinden möchtest, ohne jemanden zu fragen, wie alt er oder sie ist. Frage die SchülerInnen nach Vorschlägen, wie dies geschehen könnte oder ob sie tatsächlich glauben, dass dies möglich ist.
2. Wähle etwa sechs bis zehn SchülerInnen aus, mit denen du arbeiten möchtest. Gebe dem ersten Schulkind den Block und den Stift und bitte es, eine zufällig gewählte dreistellige Nummer auf dem obersten Blatt Papier aufzuschreiben. In diesem Beispiel wurde 613 als Zufallszahl ausgewählt.



3. Lass das erste Schulkind die erste Seite abreißen, dann soll es der Zufallszahl von der ersten Seite sein Alter hinzuaddieren und das Ergebnis auf das zweite Blatt des Blockes schreiben. Das Alter des ersten Schulkindes ist 8, also zeigt das zweite Blatt die Zahl 621. Die erste abgerissene Seite wird behalten (und wird niemandem gezeigt).
4. Der Block wird dann an das zweite Schulkind weitergegeben, das sein Alter zu der Zahl oben addiert, die Seite abreißt und die Summe auf die nächste Seite schreibt. In unserem Beispiel ist das zweite Schulkind 10 Jahre alt.

5. Setze diesen Prozess fort, wobei jedes Schulkind die oberste Seite jeweils abreißt und sein Alter zu der Zahl hinzufügt, bis alle SchülerInnen den Block bekommen haben.

6. Gib den Block dem ersten Schulkind zurück. Lass das Schulkind nun die ursprüngliche Zufallszahl von der Zahl auf dem Block abziehen. In unserem Beispiel hatten fünf Schüler den Block und die letzte Zahl 657 war die Endzahl. Dann wird die ursprüngliche Zahl 613 davon subtrahiert und es ergibt sich die Zahl 44. Diese Zahl ist die Summe des Alters aller SchülerInnen und der Durchschnitt kann geteilt durch die Anzahl der Schüler berechnet werden; somit ist das Durchschnittsalter unserer Beispielgruppe 8,8 Jahre.

7. Weise die Schüler darauf hin, dass niemand das genaue Alter einer Person berechnen kann, wenn alle ihr Stück Papier zerreißen, es sei denn, zwei von den SchülerInnen entscheiden sich zur Mitarbeit und behalten das Papier.

Variationen und Erweiterungen

Dieses System könnte angepasst werden, um eine geheime Wahl zu ermöglichen, indem jede Person eine 1 dazu addiert, wenn sie ‚Ja' wählt, und eine 0, wenn sie ‚Nein' wählt. Wenn jemand mehr als 1 (oder weniger als 0) hinzu addiert, wäre die Abstimmung natürlich unfair und es würde Gefahr laufen Verdacht zu erregen, wenn alle mit ‚Ja' stimmen würden, da die Anzahl der Ja-Stimmen größer wäre als die Anzahl der Wählerinnen und Wähler.

Worum geht es in dieser Aktivität?

Computer speichern viele persönliche Informationen über uns: unsere Bankbilanz, unsere sozialen Netzwerke, wie viel Steuern wir schuldig sind, wie lange wir einen Führerschein besitzen, unsere Kredite, Untersuchungsergebnisse, Krankenakten und so weiter. Datenschutz ist sehr wichtig! Aber wir müssen in der Lage sein, einige dieser Informationen mit anderen Menschen zu teilen. Wenn wir zum Beispiel Waren in einem Geschäft mit einer Bankkarte bezahlen, wissen wir, dass das Geschäft überprüfen muss, ob wir die Mittel zur Verfügung haben.

Oft liefern wir aber mehr Informationen als nötig. Zum Beispiel wenn wir eine elektronische Transaktion in einem Geschäft durchführen, wird im Wesentlichen angezeigt, wo wir ein Konto haben, was unsere Kontonummer ist und wie unser Name ist. Außerdem erfährt die Bank, wo wir unsere Einkäufe erledigt haben. Banken können ein Profil von jemandem erstellen, indem sie beispielsweise überwachen, wo sie tanken oder Lebensmittel kaufen, wie viel sie jeden Tag für diese Gegenstände ausgeben und wann welche Orte besucht wurden. Wenn wir bar bezahlt hätten, wäre keine dieser Informationen bekannt geworden. Die meisten Menschen machen sich aber nicht allzu viele Sorgen darüber, dass diese Informationen weitergegeben werden. Aber es besteht die Gefahr, dass Daten missbraucht werden, sei es für gezieltes Marketing (z. B. das Senden von Reisewerbung an Personen, die viel für Flugtickets ausgeben), Diskriminierung (zum Beispiel einen besseren Service für jemanden anbieten, dessen Bank in der Regel nur vermögende Kunden aufnimmt) oder gar zu erpressen (zum Beispiel mit der Drohung Details einer unangenehmen Transaktion preiszugeben). Nicht zuletzt könnten die Menschen die Art und Weise ändern, in der sie einkaufen, wenn sie glauben, dass jemand sie überwacht.

Dieser Verlust der Privatsphäre wird weitgehend akzeptiert, doch existieren auch kryptographische Protokolle, die es uns ermöglichen, elektronische Finanztransaktionen mit dem gleichen Maß an Privatsphäre zu betreiben, wie wir es mit Bargeld bekommen würden. Es kann schwer sein zu glauben, dass Geld von Ihrem Bankkonto auf ein Konto eines Geschäfts übertragen werden kann, ohne dass jemand weiß, woher das Geld kommt oder wohin es geht. Diese Aktivität lässt eine solche Transaktion ein wenig plausibler erscheinen: Beide Situationen beinhalten einen begrenzten Informationsaustausch, und dies kann durch ein ausgeklügeltes Protokoll ermöglicht werden.

Weiterführende Literatur

Eine klassische Veröffentlichung, die diese Themen beleuchtet, schrieb David Chaum mit dem provokanten Titel “Security without identification: transaction systems to make Big Brother obsolete”. Das Werk ist gut lesbar und enthält einfache Beispiele für Protokolle zum Verstecken von Informationen, darunter wie vollständig private Transaktionen mit „elektronischem Bargeld“ durchgeführt werden können. Es ist zu finden in *Communications of the ACM*, Oktober 1985.

Aktivität 18: Der peruanische Münzwurf – Kryptographische Protokolle

Zusammenfassung

Diese Aktivität zeigt, wie man eine einfache, aber dennoch scheinbar unmögliche Aufgabe, bewältigt - eine faire Zufallsauswahl zu treffen, indem man eine Münze zwischen zwei Personen fallen lässt, die sich nicht unbedingt gegenseitig vertrauen und nur durch ein Telefon verbunden sind.

Einfügen in den Lehrplan

- Mathematik – logisches Denken
- Mathematik – Boolesche Logik

Alter

- 9+

Benötigte Kenntnisse

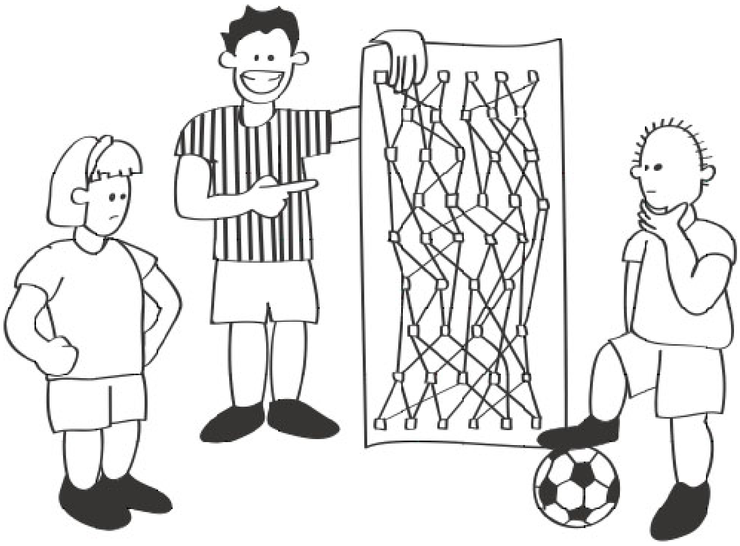
- Boolesche Logik
- Funktionen
- Puzzle lösen

Materialien

Jede Gruppe braucht:

- eine Kopie des reproduzierbaren Blattes Der peruanische Münzwurf
- etwa zwei Dutzend kleine Knöpfe oder Spielsteine in zwei verschiedenen Farben

Der peruanische Münzwurf



Einführung

Diese Aktivität wurde ursprünglich entwickelt, als einer der Autoren (MRF) mit Studenten in Peru arbeitete, daher der Name. Sie können die Geschichte an die örtlichen Gegebenheiten anpassen.

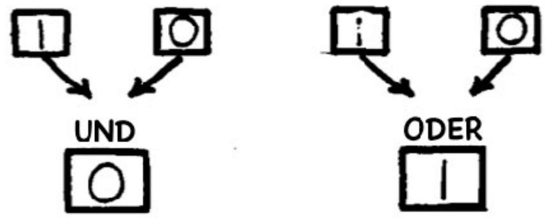
Die Fußballmannschaften von Lima und Cuzco müssen entscheiden, wer die Heimmannschaft für das Meisterschaftsspiel wird. Der einfachste Weg wäre, eine Münze zu werfen. Aber die Städte sind weit voneinander entfernt, und Alicia, die Lima vertritt, und Benito, der Cuzco repräsentiert, können nicht die Zeit verschwenden und das Geld ausgeben, um zusammen eine Münze zu werfen. Können sie das telefonisch tun? Alicia könnte die Münze umdrehen und Benito könnte Kopf oder Zahl nennen. Aber das wird nicht funktionieren, denn wenn Benito ‚Kopf' sagt, kann Alicia einfach „Entschuldigung, es war Zahl" sagen und Benito wäre nicht klüger. Alicia ist von Natur aus nicht betrügerisch, aber das ist schließlich ein wichtiger Wettbewerb und die Versuchung ist furchtbar stark. Selbst wenn Alicia ehrlich wäre, würde Benito glauben, dass er verloren hätte?

Die SchülerInnen werden mehr aus dieser Aktivität herausholen, wenn sie die binäre Zahlendarstellung gelernt haben (Punkte zählen), das Konzept der Parität (siehe „Der Zauber, Karten umzudrehen") und das Beispiel der Einwegfunktionen in der Aktivität „Touristenstadt" gesehen haben.

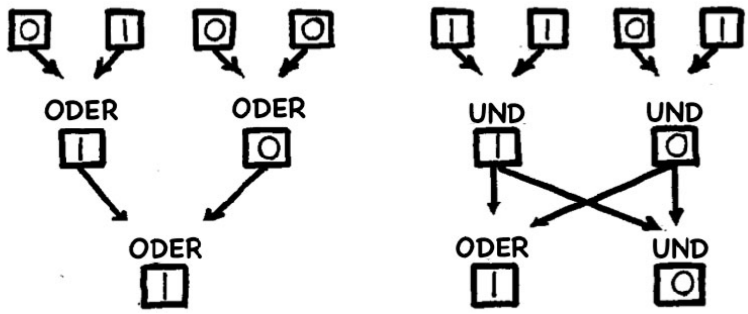
Diskussion

Die Regeln der UND- und ODER-Gatter sind einfach. Jedes „Tor“ hat zwei Eingänge und einen Ausgang. Jeder der Eingänge kann entweder eine ‚0’ oder eine ‚1’ sein, was als falsch bzw. wahr interpretiert werden kann. Die Ausgabe eines UND-Gatters ist nur dann ‚1’ (wahr), wenn beide Eingaben ‚1’ (wahr) sind; andernfalls ist sie stets ‚0’ (falsch).

Zum Beispiel hat das UND-Gatter an seinen Eingängen (oben) eine ‚1’ und eine ‚0’, sodass der Ausgang (das Quadrat an der Unterseite) eine ‚0’ ist. Der Ausgang eines ODER-Gatters ist ‚1’ (wahr), wenn einer (oder beide) der Eingaben ‚1’ (wahr) ist. Eine ‚0’ (falsch) wird nur dann ausgegeben, wenn beide Eingänge ‚0’ sind. Somit ist der Ausgang des ODER-Gatters eine ‚1’ für die Eingänge ‚0’ und ‚1’.



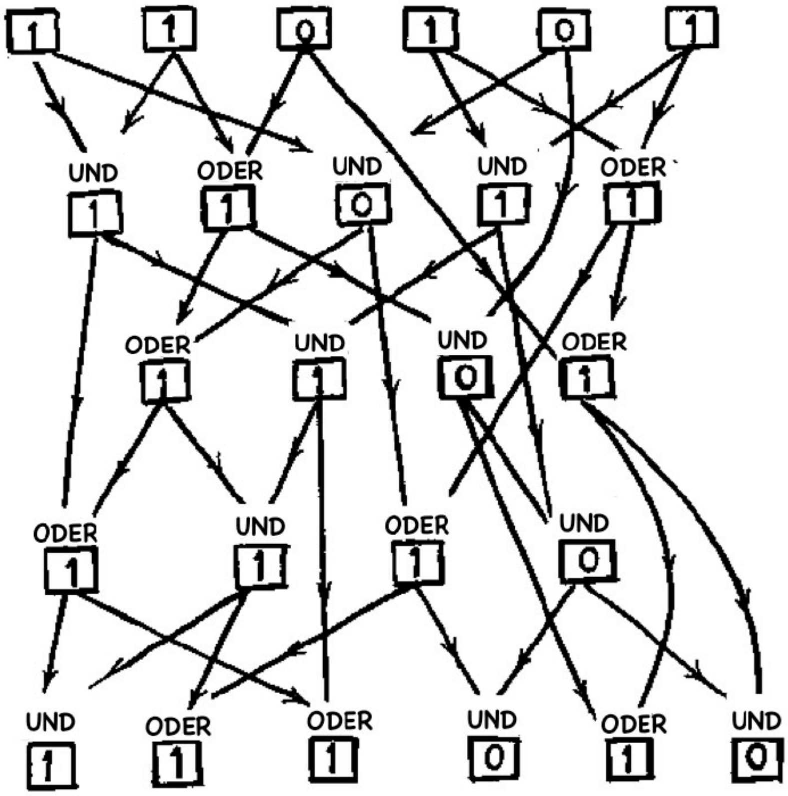
Der Ausgang eines Gatters kann mit dem Eingang eines anderen (oder mehrerer anderer) verbunden sein, um einen komplizierteren Effekt zu erzeugen.



Zum Beispiel sind in dem linken Schaltkreis die Ausgänge von zwei ODER-Gattern mit den Eingängen eines dritten ODER-Gatters verbunden, mit dem Effekt, dass, wenn einer der vier Eingänge eine Eins ist, der Ausgang eine Eins ist.

In dem rechten Schaltkreis fließen die Ausgänge jedes der oberen zwei UND-Gatter in die unteren zwei Gatter, sodass der gesamte Schaltkreis zwei Werte an seinem Ausgang aufweist.

Für den peruanischen Münzwurf benötigen wir noch komplexere Schaltkreise. Der Schaltkreis auf dem Arbeitsblatt hat sechs Eingänge und sechs Ausgänge. Hier ist ein Beispiel für einen bestimmten Satz von Eingabewerten



Die Art, wie diese Schaltung verwendet werden kann um eine Münze per Telefon umzudrehen, ist wie folgt: Alicia wählt eine zufällige Eingabe für den Schaltkreis aus, bestehend aus sechs Binärziffern (Nullen oder Einsen), die sie geheim hält. Sie sendet die sechs Eingabe-Bits durch den Schaltkreis und sendet Benito die sechs Bits der Ausgabe. Sobald Benito die Ausgabe hat, muss er versuchen zu erraten, ob Alicias Eingabe eine gerade oder ungerade Anzahl von Einsen hat - mit anderen Worten, er muss die Parität von Alicias Eingabe erraten. Wenn der Schaltkreis komplex genug ist, wird Benito die Antwort nicht erraten können und seine Wahl wird eine zufällige Vermutung sein (eigentlich könnte er sogar einfach eine Münze werfen!). Benito gewinnt - und das Playoff ist in Cuzco - wenn seine Vermutung richtig ist; Alicia gewinnt - und das Playoff ist in Lima - wenn Benito falsch rät. Sobald Benito seine Vermutung Alicia mitgeteilt hat, gibt Alicia ihren geheimen Input preis, damit Benito prüfen kann, dass der gegebene Input die richtige Ausgabe erzeugt.

1. Teile die SchülerInnen in kleine Gruppen auf; gebe jeder Gruppe den Schaltkreis und einige Spielsteine und erkläre den Ablauf. Die Situation wird wahrscheinlich für die SchülerInnen interessanter sein, wenn sie sich vorstellen sollen, dass einer ihrer Spielleiter den Wurf mit einer rivalisierenden Schulklasse organisiert. Lege eine Konvention für die Farben der Spielsteine fest - Rot ist ‚0', Blau ist ‚1' oder so ähnlich - und lass die SchülerInnen es als Hinweis oben auf dem Blatt notieren, damit sie sich daran erinnern können.

2. Zeige den SchülerInnen, wie die Spielsteine an den Eingängen platziert werden sollen um die Ziffern anzuzeigen, die Alicia ausgewählt hat. Dann erkläre die Regeln von UND-Gattern und ODER-Gattern, die unten auf dem Blatt zusammengefasst sind (überlege dir, die SchülerInnen dazu zu bringen, diese einzufärben).

3. Zeige den SchülerInnen, wie der Schaltkreis durchlaufen wird, indem du Spielsteine an den Knoten platzierst, um die entsprechende Ausgabe darzustellen. Dies muss genau durchgeführt werden und erfordert Sorgfalt. Die Tabelle (die nicht an die SchülerInnen ausgegeben werden sollte) zeigt die Ausgabe für jeden möglichen Input zur eigenen Referenz im Zweifelsfall.

Input	000000	000001	000010	000011	000100	000101	000110	000111
Ouput	000000	010010	000000	010010	010010	010010	010010	010010
Input	001000	001001	001010	001011	001100	001101	001110	001111
Ouput	001010	011010	001010	011010	011010	011010	011010	011111
Input	010000	010001	010010	010011	010100	010101	010110	010111
Ouput	001000	011010	001010	011010	011010	011010	011010	011111
Input	011000	011001	011010	011011	011100	011101	011110	011111
Ouput	001010	011010	001010	011010	011010	011010	011010	011111
Input	100000	100001	100010	100011	100100	100101	100110	100111
Ouput	000000	010010	011000	011010	010010	010010	011010	011010
Input	101000	101001	101010	101011	101100	101101	101110	101111
Ouput	001010	011010	011010	011010	011010	011010	011010	011111
Input	110000	110001	110010	110011	110100	110101	110110	110111
Ouput	001000	011010	011010	011010	011010	111010	011010	111111
Input	111000	111001	111010	111011	111100	111101	111110	111111
Ouput	001010	011010	011010	011010	011010	111010	011010	111111

4. Jetzt sollte jede Gruppe eine ‚Alicia' und einen ‚Benito' wählen. Die Gruppe kann sich aufteilen und jeweils eine Hälfte wird Alicia bzw. Benito zugeteilt. Alicia wählt nun eine zufällige Eingabe für den Schaltkreis, ermittelt die Ausgabe und teilt das Ergebnis Benito mit. Benito schätzt die Parität der Eingabe (ob sie eine ungerade oder gerade Anzahl von Einsen enthält). Es sollte während des Ablaufs offensichtlich werden, dass Benitos Vermutung im Wesentlichen zufällig ist. Alicia erzählt dann allen, was ihre Eingabe war, und Benito gewinnt, wenn er die richtige Parität erraten hat. Benito kann bestätigen, dass Alicia ihre gewählte Eingabe nicht verändert hat, indem er überprüft, ob diese die richtige Ausgabe durch den Schaltkreis liefert.

Der Münzwurf ist hiermit abgeschlossen.

Benito kann schummeln, wenn er bei einer Ausgabe den Input findet, der ihn produziert hat. Daher liegt es in Alicias Interesse, dafür zu sorgen, dass die Funktion des Schaltkreises wie eine Einbahnstraße ist (haben wir ja in Aktivität 14 diskutiert), um zu verhindern, dass Benito betrügt. Eine Einwegfunktion ist eine, für die die Ausgabe einfach zu berechnen ist, wenn man weiß, was die Eingabe ist. Aber die Eingabe ist für eine gegebene Ausgabe sehr schwierig zu berechnen.

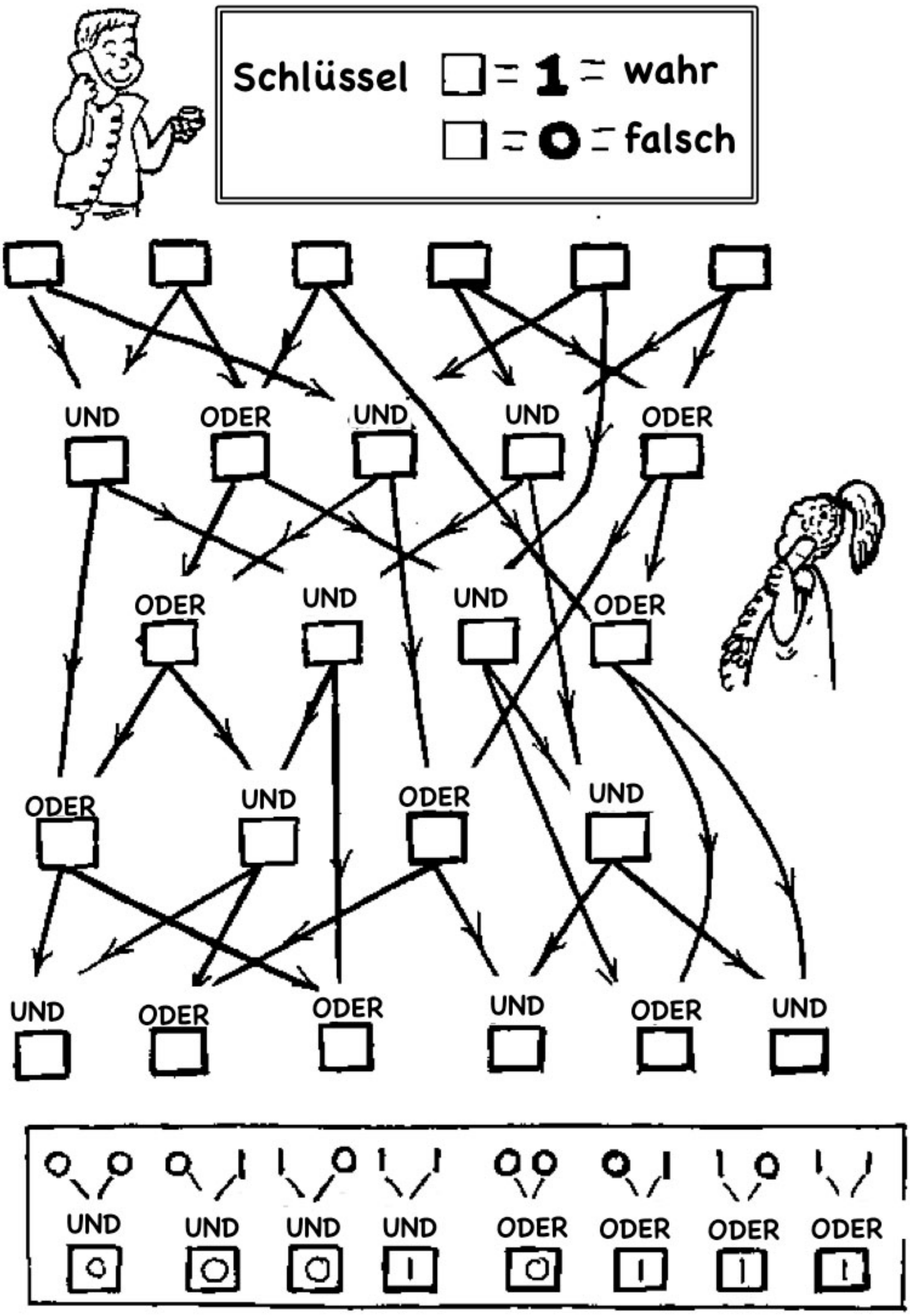
Alicia kann schummeln, wenn sie zwei Eingänge mit entgegengesetzter Parität findet, die dieselbe Ausgabe erzeugen. Dann kann Alicia (was auch immer Benito vermutet) den Input enthüllen, der zeigt, dass er falsch liegt. Es liegt also im Interesse von Benito dafür zu sorgen, dass der Schaltkreis trotz verschiedener Eingaben nicht zur selben Ausgabe führt.

5. Probiert, ob die SchülerInnen einen Weg finden können, wie Alicia oder Benito schummeln können. In der ersten Zeile der Tabelle siehst du, dass mehrere, verschiedene Eingaben die Ausgabe 010010 erzeugen, z. B. 000001, 000011, 000101 usw. Wenn also Alicia 010010 als Ausgabe angibt, kann sie als Eingabe 000001 wählen, wenn Benito rät, dass die Parität gerade ist, und 000011, wenn er vermutet, dass sie ungerade ist.

Mit diesem Schaltkreis ist es für Benito schwer zu betrügen. Aber wenn die Ausgabe 011000 ist, dann muss die Eingabe 100010 gewesen sein - es gibt keine andere Möglichkeit (das siehst du, wenn du in der Tabelle nachschaust). Also, wenn dies die Zahl ist, die Alicia zufällig gewählt hat, kann Benito gerade Parität erraten und sicher sein, dass es richtig ist. Ein computerbasiertes System verwendet viel mehr Bits, sodass es zu viele Möglichkeiten gibt (jedes zusätzliche Bit verdoppelt die Anzahl der Möglichkeiten).

6. Bitte jetzt die Schülergruppen ihre eigenen Schaltkreise für dieses Spiel zu entwickeln. Beobachte, ob sie einen Schaltkreis finden können, der es Alicia leicht macht zu schummeln, und einen anderen, der es Benito leicht macht zu schummeln. Es gibt keinen Grund, warum der Schaltkreis sechs Eingänge haben muss, und er kann sogar unterschiedliche Anzahlen von Eingängen und Ausgängen haben.

Arbeitsblatt: der peruanische Münzwurf



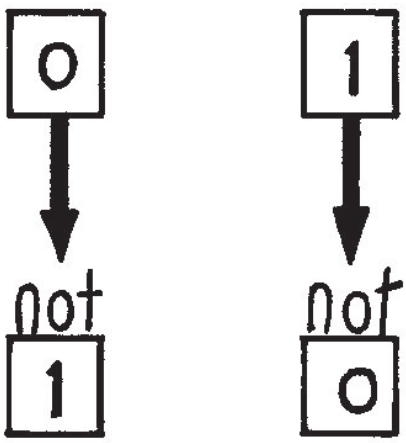
Wähle einige Eingaben für diesen Schaltkreis und ermittle, was die Ausgaben sind.

Variationen und Erweiterungen

1. Ein offensichtliches Problem in der Praxis ist die Zusammenarbeit, die benötigt wird um einen Schaltkreis zu bauen, der für Alicia und Benito akzeptabel ist. Dies könnte die Aktivität für die Kinder unterhaltsam machen, aber es wird wahrscheinlich dazu führen, dass das Verfahren in der Praxis nicht funktioniert - besonders nicht am Telefon! Es gibt jedoch eine einfache Alternative, bei der Alicia und Benito ihre Schaltkreise unabhängig voneinander konstruieren und öffentlich zugänglich machen können. Dann sendet Alicia ihre geheime Eingabe durch beide Schaltkreise und verbindet die beiden Ausgänge miteinander, indem sie die entsprechenden Bits vergleicht und die letzte Ausgabe zu einer Eins macht, wenn sie gleich sind und andernfalls zu Null setzt. In dieser Situation kann keiner der Teilnehmer schummeln, wenn der andere dies nicht tut, denn wenn nur eine der Schaltungen eine Einwegfunktion ist, dann ist die Kombination beider auch eine Einwegfunktion.

Die nächsten beiden Varianten betreffen nicht kryptographische Protokolle oder das Problem des Münzwerfens an sich, sondern eher das Konzept von Schaltkreisen, die aus UND und ODER-Gattern aufgebaut sind. Es werden einige wichtige Begriffe der Grundlagen erklärt, die sich nicht nur der Computerschaltkreise, sondern auch der Logik selbst beziehen. Diese Art von Logik nennt man Boolesche Algebra, benannt nach dem Mathematiker George Boole (1815-64).

2. Die SchülerInnen mögen bemerkt haben, dass die Nur-Null-Eingabe 000000, es dazu gebracht hat, die Nur-Null-Ausgabe zu erzeugen, und ebenso wird durch den Nur-Eins-Input 111111 der Nur-Eins-Output erzeugt. (Es kann andere Eingaben geben, die diese Ausgaben ebenfalls erzeugen; tatsächlich gibt es für den Beispielschaltkreis-000010 nur Nullen, während 110111 nur Einsen erzeugt.)

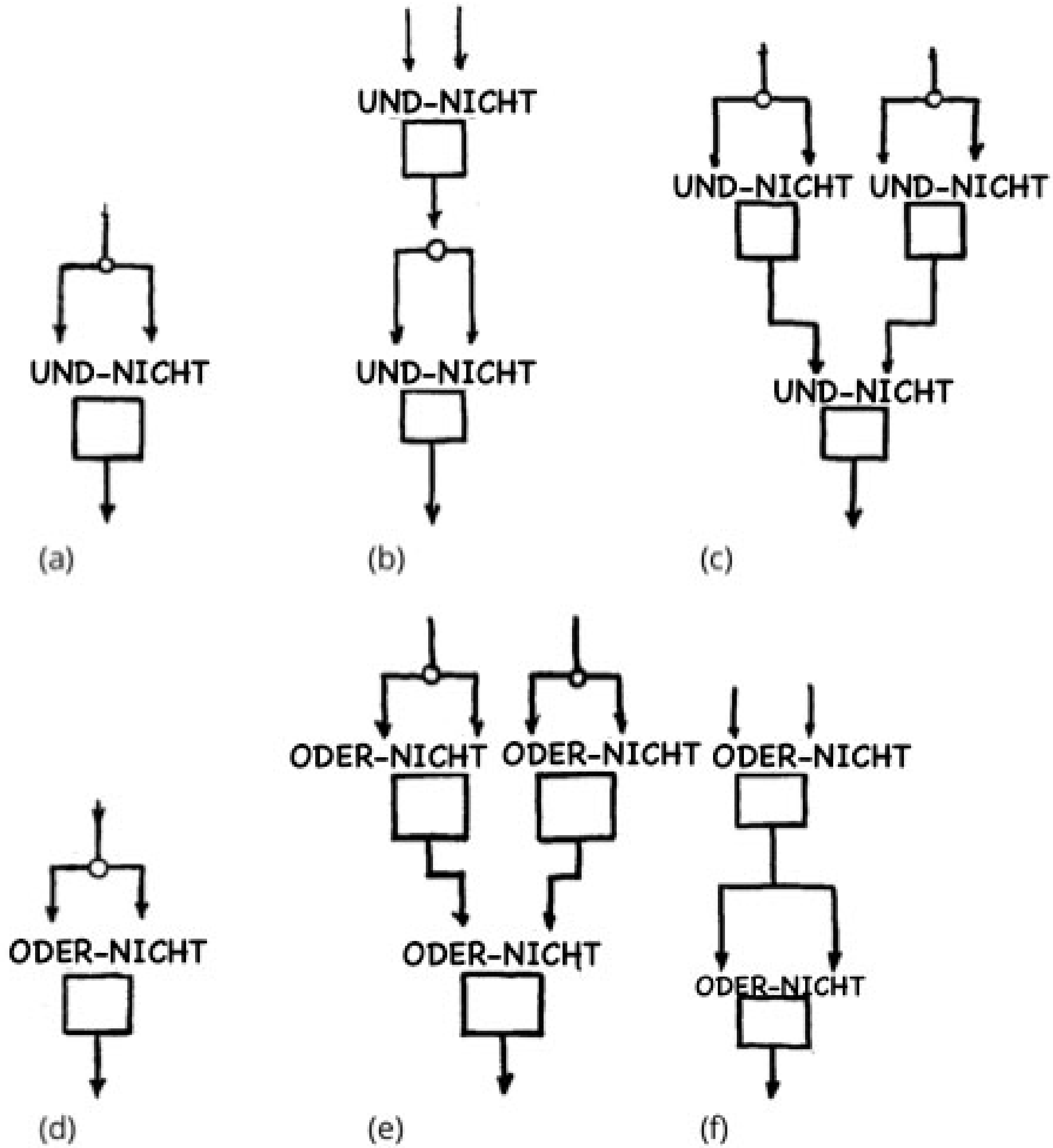


Dies folgt aus der Tatsache, dass die Schaltkreise nur aus UND- und ODER-Gattern bestehen. Durch Hinzufügen eines NICHT-Gatters, das nur eine Eingabe benötigt und die Umkehrung als Ausgabe erzeugt (d. h. 0 •1 und 1 ⊠ 0), können die SchülerInnen Schaltkreise konstruieren, die diese Eigenschaft nicht haben.

3. Zwei andere wichtige Arten von Gattern sind UND-NICHT und ODER-NICHT (normalerweise abgekürzt als NAND und NOR), die gleich sind wie UND und ODER, die Ausgabe aber von einem NICHT umgekehrt wird.

Zum Beispiel ist ‚a UND-NICHT b' dasselbe wie ‚NICHT (a UND b)'. Sie ermöglichen keine funktionell unterschiedlichen Schaltkreise, da deren Auswirkung immer mit dem entsprechenden UND- / ODER-Gatter, gefolgt von NICHT, erreicht werden kann. Interessant ist aber, dass alle anderen Gatter-Typen aus UND-NICHT-Gattern und ODER-NICHT-Gattern bestehen können.

Nachdem UND-NICHT und ODER-NICHT den SchülerInnen vorgestellt wurden, fordere sie auf herauszufinden, ob eines dieser Gatter aus anderen miteinander verbundenen Gattern hergestellt werden kann. Dazu als weiteren Schritt, ob solche Gatter auch aus nur einem Typ von miteinander verbundenen Gattern hergestellt werden kann. Die folgende Abbildung zeigt, wie die drei grundlegenden Gatter NICHT, UND und ODER aus UND-NICHT-Gattern in der oberen Reihe und ODER-NICHT-Gattern in der unteren Reihe konstruiert werden können.


UND-NICHT
UND-NICHT
UND-NICHT
UND-NICHT
UND-NICHT
UND-NICHT
(a)
(b)
(c)
ODER-NICHT
ODER-NICHT
ODER-NICHT
ODER-NICHT
ODER-NICHT
ODER-NICHT
(d)
(e)
(f)

Worum geht es in dieser Aktivität?

In den letzten Jahren hat der Umfang des Handels über Computernetze stark zugenommen und es ist wichtig einen sicheren Austausch von elektronischen Zahlungen, vertraulichen Transaktionen und rechtsverbindlichen Dokumenten zu garantieren. Beim Thema Kryptographie geht es darum, auf sichere und private Weise zu kommunizieren. Vor einigen Jahrzehnten entdeckten InformatikerInnen die kontraintuitive Eigenschaft, dass durch Verfahren eine Geheimhaltung gewährleistet werden kann, die sicherstellt, dass bestimmte Informationen öffentlich zugänglich gemacht werden können. Das Ergebnis ist das sogenannte „Public-Key-Kryptosystem“ (siehe Aktivität 19), das heute weit verbreitet als der sicherste Weg zum Informationsaustausch verwendet wird. Beispielsweise hast du möglicherweise Einstellungen wie SSL (Secure Sockets Layer) oder TLS (Transport Layer Security) in deinem Webbrowser gesehen. Diese Systeme basieren auf öffentlichen Schlüsselsystemen, mit denen dein Webbrowser eine sichere Verbindung zu einer Website wie einer Bank aufbauen kann, selbst wenn jemand alle gesendeten Daten abhört.

Bei der Kryptographie geht es nicht nur darum, die Dinge geheim zu halten, sondern um Informationsaustausch zu kontrollieren, d.h. einschränken, was andere über dich herausfinden können und um Vertrauen zwischen geografisch getrennten Personen herzustellen. Formale Regeln oder „Protokolle“ für kryptographische Transaktionen wurden entwickelt, um solche scheinbar unmöglichen Dinge, wie fälschungssichere digitale Signaturen, zu ermöglichen und anderen zu sagen, dass man das ‚Geheimnis' besitzt (etwa ein Passwort) ohne es tatsächlich enthüllen zu müssen. Ein Münzwurf per Telefon ist ein einfaches, aber analoges Problem, das auf den ersten Blick unmöglich erscheint.

In einer realen Situation würden Alicia und Benito selbst keine Schaltkreise entwerfen, sondern sich ein Computerprogramm anschaffen, das die Arbeit intern erledigt. Wahrscheinlich würde sich keiner für die Innereien der Software interessieren. Aber beide möchten sich darauf verlassen können, dass kein anderer in der Lage ist, das Ergebnis der Vorgangs zu beeinflussen, egal wie gute Computerkenntnisse er oder sie hat und wie intensiv es versucht wird.

Im Prinzip müssten alle Streitigkeiten durch einen neutralen Richter gelöst werden. Der Richter sollte den Schaltkreis, Alicias ursprüngliche Binärzahl, die Ausgabe, die sie ursprünglich Benito schickte, und die Vermutung erhalten, die Benito im Gegenzug geschickt hat. Sobald der Austausch abgeschlossen ist, handelt es sich um öffentliche Informationen, sodass beide Teilnehmer zustimmen müssen, dass dies dem Ergebnis zugrunde liegt. Der Richter wird in der Lage sein, Alicias ursprüngliche Zahl in dem Schaltkreis einzugeben und zu überprüfen, ob die Ausgabe wie erwartet ist. Dadurch kann gezeigt werden, ob die Entscheidung fair getroffen wurde. Es erübrigt sich zu erwähnen, dass es unwahrscheinlich ist, dass ein Streit entsteht, da es ein klares Vorgehen gibt um zu überprüfen, dass die Regeln befolgt wurden. Vergleiche das mit der Situation, in der Alicia eine Münze wirft und Benito Kopf oder Zahl sagt - kein Richter würde diesen Fall annehmen!

Ein Schaltkreis, der so klein ist wie der gezeigte, wäre in der Praxis nicht sehr nützlich, da es leicht ist einen Tisch zu benutzen und darauf zu schummeln. Die Verwendung von zweiunddreißig Binärziffern in der Eingabe würde einen besseren Schutz bieten. Aber auch das garantiert nicht, dass es schwer ist zu schummeln - das hängt von dem jeweiligen Schaltkreis ab. Andere Methoden könnten verwendet werden, wie die in Aktivität 15 („Touristenstadt“) eingeführte Einwegfunktion. Die in der Praxis verwendeten Methoden hängen häufig vom Faktorisieren großer Zahlen ab, von dem bekannt ist, dass es ein schweres Problem ist (obwohl, wie wir am Ende der nächsten Aktivität erfahren werden, es nicht NP-vollständig ist). Es ist leicht zu überprüfen, ob eine Zahl ein Faktor einer anderen ist, aber das Finden der Faktoren einer großen Zahl ist sehr zeitaufwendig. Dies macht es für Alicia und Benito (und den Richter) komplizierter sich von Hand durchzuarbeiten, obwohl dies, wie oben erwähnt, in der Praxis durch handelsübliche Software gemacht wird.

Digitale Signaturen basieren auf ähnlicher Grundlage. Indem Alicia die Ausgabe des Schaltkreises für den bestimmten geheimen Input, den sie gewählt hat, öffentlich macht, ist sie effektiv in der Lage zu beweisen, dass sie diejenige ist, welche die Ausgabe erzeugt hat, denn mit einer korrekten Einwegfunktion kann niemand anderes mit einer Eingabe kommen, die funktioniert. Niemand kann sich als Alicia ausgeben! Um eine gültige digitale Signatur zu erstellen ist ein komplexeres Protokoll erforderlich, das sicherstellt, dass Alicia eine bestimmte Nachricht signieren kann und, dass andere überprüfen können, ob Alicia die Unterzeichnerin ist, selbst wenn sie dies nicht behauptet. Das Prinzip ist das gleiche.

Eine andere Anwendung ist das Pokern über das Telefon in einer Umgebung, in der es keinen Schiedsrichter gibt, der die Karten austeilt und beide Hände der Spielenden aufzeichnet. Alles muss von den Spielenden selbst ausgeführt werden, wobei im Streitfall ein Schiedsrichter am Ende des Spiels hinzugezogen werden muss. Ähnliche Situationen ergeben sich tatsächlich bei Vertragsverhandlungen. Offensichtlich müssen SpielerInnen ihre Karten während des Spiels geheim halten. Aber sie müssen ehrlich sein - sie dürfen nicht behaupten ein Ass zu haben, es sei denn, sie haben tatsächlich ein Ass! Dies kann überprüft werden, indem man wartet, bis das Spiel vorbei ist und dann jedem Spielenden erlaubt, die ursprünglichen Karten der anderen MitspielerInnen und die Abfolge der Züge zu überprüfen. Ein anderes Problem ist es, wie man die Karten austeilen kann, obwohl man die Hände jedes Spielenden bis nach dem Spiel versteckt hält. Überraschenderweise ist es möglich, dies unter Verwendung eines kryptographischen Protokolls zu erreichen, das dem Münzwurf nicht unähnlich ist.

Kryptographische Protokolle sind bei elektronischen Transaktionen extrem wichtig, sei es um den Besitzer einer Debitkarte zu identifizieren, die Verwendung eines Mobiltelefons für einen Anruf zu autorisieren oder den Absender einer E-Mail zu authentifizieren. Die Fähigkeit, diese Dinge zuverlässig zu tun, ist entscheidend für den Erfolg des elektronischen Handels.

Weiterführende Literatur

Harels Buch *Algorithmics* behandelt digitale Signaturen und zugehörige kryptographische Protokolle. Es beschreibt auch, wie man Poker über das Telefon spielt; eine Idee, die erstmals 1981 in einem Kapitel namens „Mental Poker“ in dem Buch *The Mathematical Gardener* erwähnt wurde (herausgegeben von D.A. Klarner). *Cryptography and Data Security* von Dorothy Denning ist ein exzellenter Artikel über Kryptographie. Dewdneys Buch *Turing Omnibus* enthält einen Abschnitt über Boolesche Logik, der die Bausteine beschreibt, die für die Schaltkreise in dieser Aktivität verwendet werden.

Aktivität 19: Kid Krypto – Public-Key Verschlüsselung

Zusammenfassung

Verschlüsselung ist der Vorgang zur Informationssicherheit. Und der Schlüssel zur modernen Verschlüsselung ist, dass ein Absender, der nur öffentliche Kanäle verwendet, seine Nachricht so sperren kann, dass sie nur vom beabsichtigten Empfänger freigeschaltet werden kann (privat natürlich!).

Es ist, als ob jeder ein Vorhängeschloss kauft, seinen Namen darauf schreibt und sie alle auf den gleichen Tisch legt, damit andere sie benutzen können. Jeder behält natürlich seinen Schlüssel - die Vorhängeschlösser können einfach durch das Draufdrücken (Klicken) verschlossen werden. Wenn ich jemandem eine sichere Nachricht senden möchte, lege ich sie in eine Schachtel, hebe dein Vorhängeschloss auf, sperre die Schachtel und schicke es ab. Selbst wenn es in die falschen Hände gerät, kann niemand anderes es öffnen. Dadurch ist keine vorherige Kommunikation erforderlich, um geheime Codes festzulegen.

Diese Aktivität zeigt, wie dies digital durchgeführt werden kann. Und in der digitalen Welt funktioniert es so: Anstatt ein Vorhängeschloss zu benutzen, kopiere ich es und benutze die Kopie, wobei ich das Originalschloss auf dem Tisch liegen lasse. Wenn ich eine Kopie eines physischen Vorhängeschlosses machen würde, könnte ich das nur tun, indem ich es auseinander nehme. Dabei würde ich unweigerlich sehen, wie es funktioniert. Aber in der digitalen Welt wird ermöglicht Schlösser zu kopieren, ohne den verwendeten Schlüssel entdecken zu können!

Klingt unmöglich? Lies einfach weiter.

Einfügen in den Lehrplan

- Technologie – Public-Key Verschlüsselung; Geheimcode

Benötigte Kenntnisse

- Puzzle lösen

Alter

- 11+

Materialien

Die SchülerInnen sind in Gruppen von etwa vier Beteiligten unterteilt und innerhalb dieser Gruppen bilden sie zwei Untergruppen. Jede Untergruppe erhält eine Kopie der zwei Karten auf dem Arbeitsblatt Kid Krypto Karten.

Zusätzlich braucht jede Gruppe:

- eine Kopie des Arbeitsblatts Kid Krypto Verschlüsselung auf einer durchsichtigen Folie und
- einen Stift, um auf der Folie schreiben zu können

Kid Krypto

Einführung

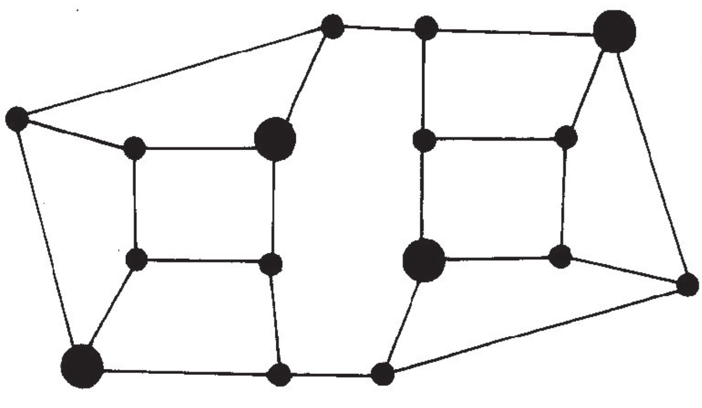
Dies ist die technisch anspruchsvollste Aktivität in diesem Buch. Sie lohnt sich und erfordert sorgfältige Arbeit und anhaltende Konzentration, um erfolgreich abgeschlossen zu werden. Die SchülerInnen sollten bereits das Beispiel der Einweg-Funktionen in der Aktivität „Touristenstadt" studiert haben, und es ist hilfreich, wenn sie die anderen Aktivitäten in diesem Abschnitt („Geheimnisse teilen" und „Der peruanische Münzwurf") durchgeführt haben. Die Aktivität verwendet auch Ideen, die die Aktivitäten „Punkte zählen" und „Zwanzig Versuche" abdecken.

Amy plant, Bill eine geheime Nachricht zu schicken. Normalerweise denken wir bei geheimen Nachrichten an einen oder mehrere Sätze, aber in der folgenden Übung wird Amy nur ein Zeichen senden - tatsächlich wird sie eine Zahl senden, die ein Zeichen darstellt. Obwohl dies wie eine sehr einfache simple Nachricht erscheinen mag, bedenke, dass du eine ganze Reihe solcher „Nachrichten" senden könntest, um einen Satz zu bilden und in der Praxis würde die Arbeit von einem Computer erledigt werden. Und manchmal sind sogar kleine Nachrichten wichtig - eine der berühmtesten Nachrichten in der Geschichte, die von Paul Revere übertragen wurde, hatte nur zwei mögliche Werte. Wir werden sehen, wie man Amys Nummer in eine verschlüsselte Nachricht einbetten kann, indem man Bills öffentliches Schloss verwendet, sodass, wenn jemand sie abfängt, es nicht möglich ist, sie zu entschlüsseln. Das kann nur Bill, denn nur er hat den Schlüssel für das Schloss.

Wir werden Nachrichten mit Karten sperren. Nicht wie bei der Schatzinselkarte, wo X die zu erreichende Stelle markiert, sondern Straßenkarten wie die von der Touristenstadt-Aktivität, wo die Linien Straßen darstellen und die Punkte Straßenkreuzungen sind. Jede Karte hat eine öffentliche Version - das Schloss - und eine private Version - den Schlüssel.

Diskussion

Auf dem Arbeitsblatt Kid Krypto Verschlüsselung ist Bills öffentliche Karte dargestellt. Sie ist nicht geheim: Bill legt sie auf einen Tisch (oder macht sie per Internet verfügbar) für alle sichtbar oder schickt sie jedem als Nachricht per Post. Amy hat wie jeder andere eine Kopie davon. Das Bild rechts zeigt Bills private Karte. Sie ist gleich wie die öffentliche Karte, mit der Ausnahme, dass einige der Kreuzungen vergrößert dargestellt sind – diese Karte behält er sicher für sich allein.

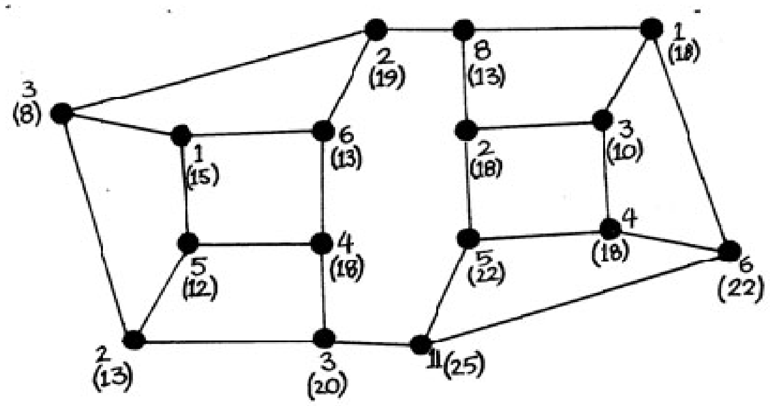


Diese Aktivität wird am besten von einer Klasse durchgeführt, weil hinsichtlich der Lösung eine Menge Arbeit erfordert wird. Obwohl es nicht schwierig ist, muss dies genau durchgeführt werden, da Fehler viel Ärger verursachen können. Es ist wichtig, dass die SchülerInnen erkennen, wie erstaunlich es ist, dass diese Art von Verschlüsselung überhaupt möglich ist - es scheint unmöglich (oder?) - weil sie diese Motivation brauchen, um sie durch die erforderlichen Anstrengungen zu führen.

Ein Punkt, den wir für die SchülerInnen sehr motivierend finden ist, dass sie mit dieser Methode geheime Notizen im Unterricht weitergeben können, und selbst wenn die Lehrerperson weiß, wie die Notiz verschlüsselt wurde, wird er oder sie diese nicht entschlüsseln können.

1. Zeige Bills öffentliche Karte (Arbeitsblatt Kid Krypto Verschlüsselung). Bestimme welche Zahl Amy senden wird. Platziere nun Zufallszahlen an jeder Kreuzung auf der Karte, sodass die Summe der Zufallszahlen die Zahl ergibt, die Amy senden möchte.

Das Bild rechts gibt ein Beispiel für solche Zufallszahlen; es sind die oberen (nicht eingeklammerten) Zahlen neben jeder Kreuzung. Amy hat gewählt, die Zahl 66 zu senden, also addieren sich alle nicht eingeklammerten Zahlen zu 66. Falls nötig, können auch negative Zahlen verwendet werden, um die Summe auf den gewünschten Wert herunter zu bringen.



2. Als nächstes muss Amy berechnen, was an Bill gesendet werden soll. Schickt sie die Karte mit den Zahlen ist das nicht gut, denn wenn die Karte in falsche Hände gerät, kann jeder sie addieren und die Nachricht bestimmen.

Stattdessen wählt sie eine beliebige Kreuzung, betrachtet diese und ihre drei Nachbarn - insgesamt vier Kreuzungen – und addiert die vier Zahlen. Sie schreibt diese Summe an der Kreuzung in Klammern (oder mit einem anderen Farbstift) nieder. Zum Beispiel ist die Kreuzung ganz rechts auf der Beispielkarte mit drei anderen verbunden, die mit 1, 4, 11 bezeichnet sind; sie selbst ist mit 6 bezeichnet. Als Summe ergibt sich aus den vier Zahlen der Wert 22. Amy wiederholt das auch für alle anderen Kreuzungen auf der Karte. Als Resultat sind alle Werte in Klammern für jeden Punkt eingetragen.

3. Amy schickt die Karte an Bill zurück, auf der nur die eingeklammerten Zahlen an jeder Kreuzung eingetragen sind.

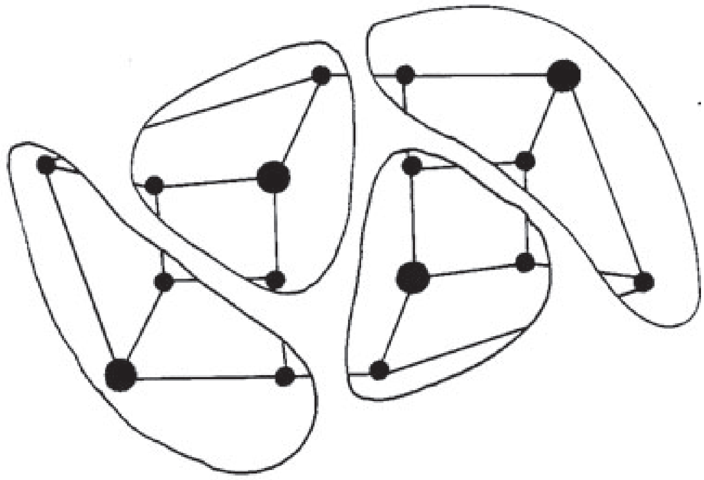
Lösche die ursprünglichen Zahlen und die Zählungen und lasse nur die Zahlen übrig, die Amy sendet; oder schreibe eine neue Karte mit genau diesen Zahlen auf. Probiere, ob einer der SchülerInnen einen Weg findet, die ursprüngliche Nachricht zu ermitteln. Sie werden es nicht können.

4. Nur jemand mit Bills privatem Schlüssel kann die Nachricht entschlüsseln, um die Information zu finden, die Amy ursprünglich senden wollte. Markiere auf der verschlüsselten Nachricht die speziellen vergrößerten Knoten von Bills privater Karte.

Um die Nachricht zu entschlüsseln, betrachtet Bill nur die geheimen Kreuzungen und summiert die Zahlen auf ihnen. In dem Beispiel sind diese Kreuzungen mit 13, 13, 22, 18 bezeichnet, was zu Amys ursprünglicher Nachricht 66 führt.

5. Wie funktioniert das? Nun, die Karte ist eine besondere. Angenommen Bill würde eine der markierten Kreuzungen wählen, einen Kreis um die Kreuzungen eine Straße entfernt von ihm zeichnen und die Prozedur für jede markierte Kreuzung wiederholen. Dies würde die Karte in vier nicht überlappende Bereiche teilen, wie hier dargestellt.

Zeige den SchülerInnen diese Bereiche, indem du die Linien auf der Karte zeichnest.



Die Gruppe von Kreuzungen in jedem separaten Bereich ergibt genau die Summe, die der markierten Kreuzung entspricht, sodass die Summe der vier übertragenen Zahlen von diesen markierten Kreuzungen die Summe aller ursprünglichen Zahlen in der ursprünglichen Karte ist; das entspricht genau der geheimen Nachricht!

Puh! Es scheint eine Menge Arbeit zu sein, einen Brief zu schreiben Und es ist eine Menge Arbeit, einen Brief zu verschicken - die Verschlüsselung ist nicht einfach. Aber schau, was erreicht wurde: Vollständige Geheimhaltung mit einem öffentlichen Schlüssel, ohne vorherige Absprache zwischen den TeilnehmerInnen. Du könntest deinen Schlüssel auf einem Anschlagbrett veröffentlichen und jeder könnte dir eine geheime Nachricht senden, doch niemand könnte sie ohne den privaten Schlüssel entschlüsseln. Und im täglichen Leben wird die gesamte Berechnung von einem Softwarepaket durchgeführt, das normalerweise bereits im Webbrowser integriert ist. Es ist also nur der Computer, der hart arbeiten muss.

Ganz bestimmt ist deine Klasse stolz, dass sie jetzt zu einer ausgewählten Gruppe von Leuten gehört, die ein Beispiel der Public Key-Verschlüsselung von Hand durchgeführt hat - InformatikerInnen würden dies rein fachlich als eine fast unmögliche Aufgabe betrachten und nur wenige Menschen haben es auch jemals so getan!

Was ist mit dem Abhören? Bills Karte ist wie die in der *Aktivität Touristenstadt (Aktivität 14)*, wo die markierten Kreuzungen eine optimale Möglichkeit darstellen, Eiswagen an Straßenecken zu platzieren, ohne dass jemand mehr als einen Block laufen muss. Wir haben, wie in der Touristenstadt, gesehen, dass es für Bill leicht ist, eine solche Karte zu erstellen, indem er mit den markierten Punkten beginnt, die auf seiner privaten Karte dargestellt werden, und es ist sehr schwierig für jeden anderen, den optimalen Weg zu finden, um die Eiswagen zu platzieren - mit Ausnahme einer Brut-Force-Methode. Die Brut-Force-Methode besteht darin, jede mögliche Anordnung mit einem Eiswagen zu testen, dann jede Anordnung mit zwei Eiswagen und so weiter, bis man auf eine Lösung stößt. Niemand weiß, ob es eine bessere Methode für eine allgemeine Karte gibt - und du kannst sicher sein, dass viele Leute versucht haben, eine zu finden!

Vorausgesetzt dass Bill eine hinreichend komplizierte Karte mit etwa fünfzig oder hundert Kreuzungen verwendet, dann scheint es, als ob niemand den Code knacken kann - selbst die klügsten MathematikerInnen haben sich bislang bemüht und versagt. (Aber es gibt einen Vorbehalt: Siehe unten, unter *Worum geht es in dieser Aktivität?*)

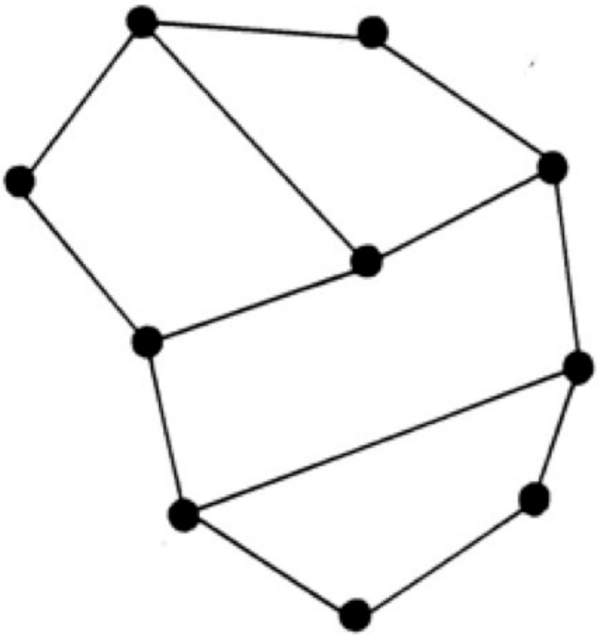
6. Nachdem du das Beispiel mit der ganzen Klasse durchgearbeitet hast, teile die SchülerInnen in vier Gruppen. Gebe einem Paar jeder Gruppe die öffentliche Karte vom *Arbeitsblatt Kid Krypto Karten*. Jedes Paar sollte eine „Nachricht“ (irgendeine ganze Zahl) auswählen, sie mit dem öffentlichen Schlüssel verschlüsseln und die resultierende Karte einer anderen Gruppe geben. Die andere Gruppe kann nun versuchen sie zu entschlüsseln. Es ist unwahrscheinlich, dass sie erfolgreich sein wird bis sie die private Karte erhalten (oder ausgearbeitet!) hat. Anschließend verteile die private Karte und beobachte, ob die SchülerInnen sie jetzt richtig entschlüsseln können.

7. Jetzt soll jedes Paar seine eigene Karte entwerfen, die private Version geheim halten und die öffentliche Version einem anderen Paar geben - oder sogar auf die Wandtafel schreiben. Das Prinzip für das Entwerfen von Karten ist das gleiche wie es in der Touristenstadt-Aktivität dargestellt wurde; weitere Straßen können hinzugefügt werden, um die Lösung zu verschleiern. Vorsicht, dass keine zusätzlichen Straßen den „speziellen“ Kreuzungen hinzugefügt werden. Das würde z.B. eine Kreuzung schaffen, von der aus zwei Eiswagen in einem Schritt erreicht werden könnten, was für die Situation in der Touristenstadt gut ist, aber beim Verschlüsseln Chaos verursachen würde. Das liegt daran, dass sich die Karte hinsichtlich der speziellen Kreuzungen nicht mehr in nicht-überlappende Teile zerlegen lässt, wie sie in der privaten Karte dargestellt ist; dies ist aber wichtig, damit der Trick auch funktioniert.

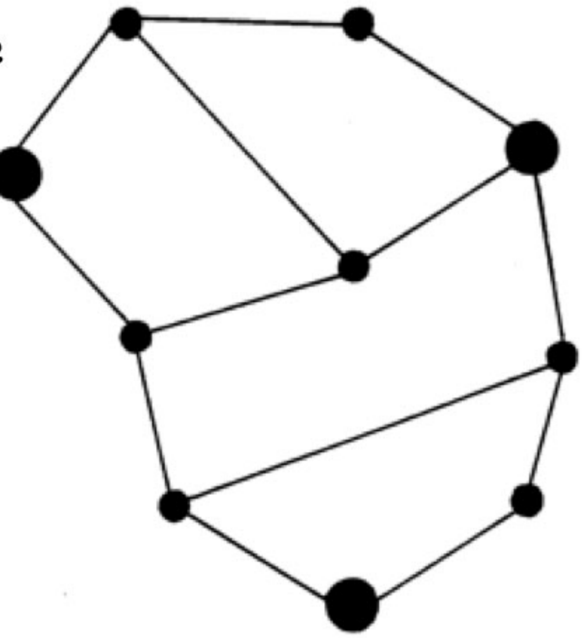
Arbeitsblatt: Kid Krypto Karten

Verwende diese Karten um Nachrichten wie im Text beschrieben zu ver- und entschlüsseln.

Öffentliche Karte

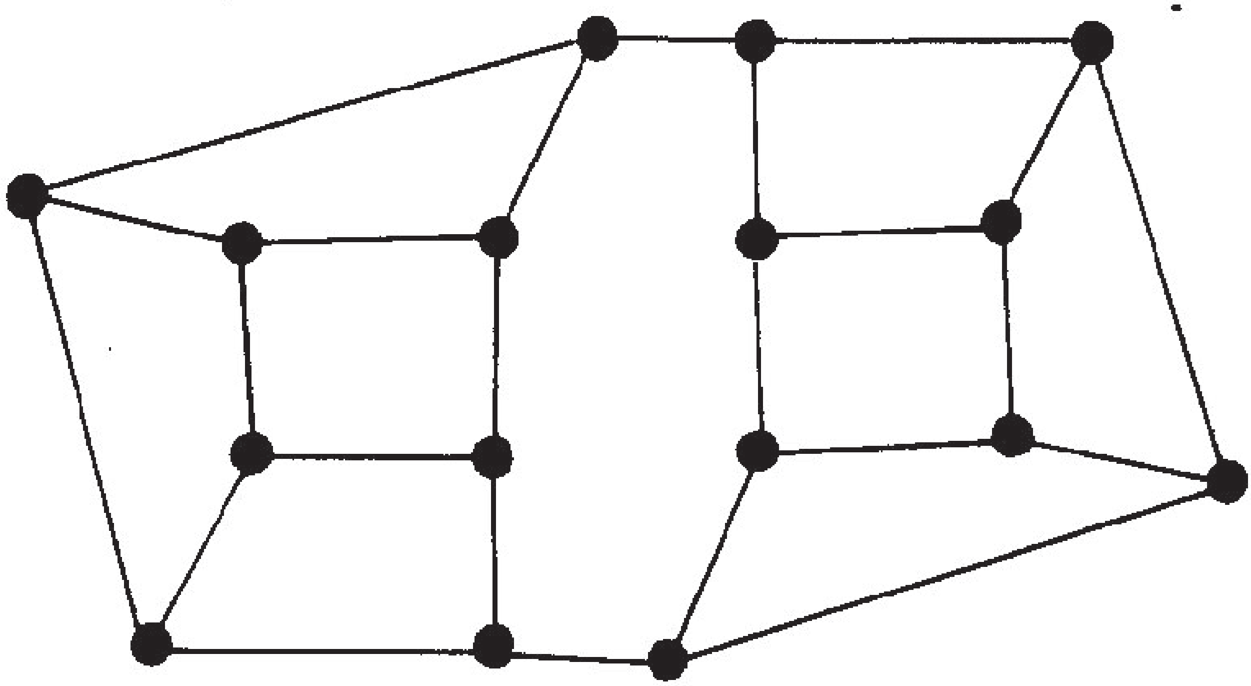


Private Karte



Arbeitsblatt: Kid Krypto Verschlüsselung

Zeige der Klasse diese Karte und verwende sie zur Demonstration der Verschlüsselung einer Nachricht.



Worum geht es in dieser Aktivität?

Es ist klar, dass du auch geheime Nachrichten über Computernetzwerke senden möchtest, die niemand außer dem beabsichtigten Empfänger /der beabsichtigten Empfängerin entschlüsseln kann, egal wie clever oder wie schwer es versucht wird. Und natürlich gibt es viele Möglichkeiten dies zu tun, falls Sender und Empfänger einen geheimen Schlüssel benutzen. Aber das clevere an der Public-Key-Verschlüsselung ist, dass Amy eine sichere Nachricht ohne irgendeine geheime vorherige Absprache, an Bill senden kann und er einfach sein „Schloss“ von einem öffentlichen Ort wie einer Website abholt.

Geheimhaltung ist nur eine Seite der Kryptographie. Eine andere ist die Authentifizierung: Wenn Amy eine Nachricht von Bill erhält, woher weiß sie dann, dass sie wirklich von ihm kommt und nicht von einem Betrüger? Angenommen sie erhält eine E-Mail von ihm, in der steht: „Liebling, ich sitze hier fest ohne Geld. Bitte überweise 100 Euro auf mein Bankkonto, Nummer 0241-45-784329 – Dein Schatz, Bill.“ Wie kann sie wissen, ob sie wirklich von Bill kommt? Einige Public-Key-Kryptosysteme können auch dafür verwendet werden. So wie Amy eine geheime Nachricht an Bill sendet, indem sie sie mit seinem öffentlichen Schlüssel verschlüsselt, kann er ihr eine Nachricht schicken, die nur er erzeugen kann, indem er sie mit seinem privaten Schlüssel verschlüsselt. Wenn Amy sie mit Bills öffentlichem Schlüssel entschlüsseln kann, muss sie von ihm kommen. Natürlich könnte auch jeder andere sie entschlüsseln, da der Schlüssel öffentlich ist, aber wenn die Nachricht nur für Amy bestimmt ist, kann Bill sie dann ein zweites Mal mit Amys öffentlichem Schlüssel verschlüsseln. Diese duale Codierung bietet sowohl Geheimhaltung, als auch Authentifizierung mit demselben Grundschema öffentlicher und privater Schlüssel.

Jetzt ist es an der Zeit zu gestehen, dass das in dieser Aktivität dargestellte Schema eines Verschlüsselungssystems mit öffentlichem Schlüssel dem in der Industrie sehr ähnlich ist. Allerdings ist es kein sicheres Verfahren - selbst wenn eine ziemlich große Karte verwendet wird.

Obwohl es keinen Weg gibt, den minimalen Weg zu finden, um einen Eiswagen auf einer willkürlichen Karte zu platzieren und demzufolge das Schema auch sicher ist, gibt es eine ganz andere Methode, es anzugreifen. Es ist unwahrscheinlich, dass die SchülerInnen (zumindest vor der Sekundarstufe) auf die Idee kommen. Aber sie sollten zumindest wissen, dass eine Methode existiert. Man könnte sagen, das Schema, das wir uns angesehen haben, ist schulisch aber nicht mathematisch sicher. Bitte ignoriere den nächsten Absatz, wenn Mathematik nicht so dein Fach ist!

Nummeriere die Kreuzungen auf der Karte mit 1, 2, 3, … Bezeichne die ursprünglichen Zahlen der Kreuzungen als b1, b2, b3, …, und die Zahlen, die übermittelt werden als t1, t2, t3, …. Angenommen Kreuzung 1 ist mit den Kreuzungen 2, 3 und 4 verbunden, dann ist die Zahl, die für die Kreuzung 1 übermittelt wird

$t1 = b1+b2+b3+b4$.

Natürlich gibt es für jede Kreuzung ähnliche Gleichungen—tatsächlich gibt es so viel Gleichungen wie die Anzahl der Unbekannten b1, b2, b3, …. Eine lauschende Person kennt die öffentliche Karte und die übermittelten Zahlen t1, t2, t3, … und kann deshalb die Gleichungen aufschreiben und mit einem Gleichungslösungsprogramm zu einer Lösung kommen. Sobald die ursprünglichen Zahlen erhalten wurden, entspricht die Nachricht einfach ihrer Summe - es ist tatsächlich nicht notwendig, die Entschlüsselungskarte zu finden.

Der erforderliche Rechenaufwand zur Lösung der Gleichungen unter Verwendung des Gauß'schen Eliminationsverfahren ist proportional zur dritten Potenz der Anzahl der Gleichungen, aber da diese Gleichungen dünn besetzt sind - die meisten Koeffizienten sind Null - gibt es noch effizientere Techniken. Vergleiche das mit dem exponentiellen Rechenaufwand, der - soweit bekannt - der beste ist, um die Entschlüsselungskarte zu erstellen.

Wir hoffen, du fühlst dich nicht überfordert! Tatsächlich sind die Prozesse, die in echten Kryptosystemen mit öffentlichem Schlüssel enthalten sind, praktisch identisch mit dem, was wir gesehen haben, abgesehen davon, dass die Techniken, die sie zum Verschlüsseln verwenden, verschieden - und auch nicht per Hand ausführbar sind. Die ursprüngliche Public-Key-Methode und immer noch eine der sichersten, basiert auf der Schwierigkeit große Zahlen zu faktorisieren.

Welche sind die Faktoren der 100-stelligen Zahl?

9,412,343,607,359,262,946,971,172,136,294,514,357,528,981,378,983,082,541,347,532,211,942, 640,121,301,590,698,634,089, 611,468,911,681? Verbringe nicht allzu viel Zeit mit dieser Frage!

86,759,222,313,428,390,812,218,077,095,850,708,048, 977 und 108,488,104,853,637,470,612,96 1,399,842,972,948,409,834,611,525,790,577,216,753 sind die gesuchten Faktoren. Es gibt keine anderen Faktoren – beide sind Primzahlen. Sie zu finden ist eine ziemlich aufwendige Aufgabe: Tatsächlich ist es ein mehrmonatiges Projekt für einen Supercomputer.

In einem echten Public-Key-Kryptosystem könnte Bill nun die 100-stellige Zahl als seinen öffentlichen Schlüssel und die beiden Faktoren als privaten Schlüssel verwenden. Es wäre nicht schwer, solche Schlüssel zu finden: Dazu brauchst du nur eine Möglichkeit große Primzahlen zu berechnen. Finde zwei Primzahlen, die groß genug sind (das ist nicht so schwer), multipliziere sie, und - tada, da ist dein öffentlicher Schlüssel. Das Multiplizieren großer Zahlen ist für einen Computer keine große Sache. Mit dem öffentlichen Schlüssel kann niemand deinen privaten Schlüssel finden, es sei denn er hat mehrere Monate Zugriff auf einen Supercomputer. Und wenn dir das nicht reicht, verwende 200-stellige Primzahlen anstelle von 100-stelligen - das wird die Faktorisierung um Jahre verlangsamen! Die Hauptsache ist, dass die Kosten für das Knacken des Schlüssels höher sind als der Wert der Informationen, die er freischalten würde. In der Praxis sind 512-Bit- oder größere Schlüssel zum Einrichten sicherer Verbindungen üblich, was ungefähr 155 Dezimalziffern oder mehr entspricht.

Wir haben noch immer keinen Weg gefunden, eine Nachricht unter Verwendung eines öffentlichen Schlüssels auf Primzahl-Basis so zu verschlüsseln, dass sie ohne den privaten Schlüssel nicht entschlüsselt werden kann. Um das zu tun, ist das Leben nicht ganz so einfach, wie wir es oben beschrieben haben. Es sind nicht die beiden Primzahlen, die als privater Schlüssel verwendet werden und ihr Produkt, das als öffentlicher Schlüssel verwendet wird, sondern Zahlen, die von ihnen abgeleitet sind. Aber der Effekt ist der gleiche: Du kannst den Code knacken, indem du die Zahl faktorisierst. Wie auch immer, es ist nicht schwer, diese Schwierigkeiten zu überwinden und das Schema zu einem geeigneten Verschlüsselungs- und Entschlüsselungsalgorithmus zu machen, darauf wollen wir aber jetzt nicht weiter eingehen. Diese Aktivität hat bereits genug Arbeit geleistet!

Wie sicher ist ein auf Primzahlen basiertes System? Nun, die Faktorisierung großer Zahlen ist ein Problem, das seit mehreren Jahrhunderten die Aufmerksamkeit der größten MathematikerInnen der Welt auf sich gezogen hat, und während Methoden entdeckt wurden, die wesentlich besser sind als die Brut-Force-Methode (d.h. es mit allen möglichen Faktoren auszuprobieren) ist man bisher nicht zu einem sehr schnellen (d.h. polynomiellen) Algorithmus gekommen. (Niemand hat bewiesen, dass ein solcher Algorithmus auch unmöglich ist.) Somit scheint das Schema nicht nur für SchülerInnen sicher zu sein, sondern auch für MathematikerInnen. Aber Achtung: Wir müssen vorsichtig sein. So wie sich herausstellte, dass es eine Möglichkeit gibt Bills Code zu knacken, ohne das Problem der Touristenstadt zu lösen, könnte es einen Weg geben, die Primzahlcodes zu knacken, ohne große Zahlen zu faktorisieren. Die Menschen haben das soweit sorgfältig überprüft und es scheint in Ordnung zu sein.

Ein weiterer Vorbehalt ist, dass ein Eindringling, wenn es nur ein paar mögliche Nachrichten gibt, jede von ihnen nacheinander mit dem öffentlichen Schlüssel verschlüsselt und die tatsächliche Nachricht mit allen möglichen Resultaten vergleicht. Amys Methode verhindert das, da es viele Möglichkeiten gibt die gleiche Nachricht zu verschlüsseln, abhängig davon, welche Zahlen ausgewählt und zum Codewert addiert wurden. In der Praxis sind kryptographische Systeme so konzipiert, dass es zu viele mögliche Nachrichten gibt, um es sogar mit Hilfe eines sehr schnellen Computers auszuprobieren.

Es ist nicht bekannt, ob eine schnelle Methode zur Lösung des Problems der Primfaktorzerlegung existiert. Niemand hat es geschafft eine zu entwickeln, aber es ist auch nicht bewiesen, dass eine schnelle Methode unmöglich ist. Wenn ein schneller Algorithmus zur Lösung dieses Problems gefunden wird, werden viele derzeit verwendete kryptographische Systeme unsicher werden. In Teil IV betrachteten wir NP-vollständige Probleme, die alle zusammen stehen oder fallen. Das bedeutet: Wenn eines von ihnen effizient lösbar ist, dann sind auch alle anderen lösbar. Da sehr viel (erfolgloser) Aufwand betrieben wurde, um schnelle Algorithmen für diese Probleme zu finden, schienen sie ausgezeichnete Kandidaten zum Entwurf sicherer Kryptosysteme zu sein. Leider gibt es Schwierigkeiten mit diesem Vorgehen und bis jetzt waren die EntwicklerInnen von Kryptosystemen gezwungen, sich auf Probleme (wie Primfaktorzerlegung) zu verlassen, die in der Tat einfacher zu lösen sind als die NP-vollständigen Probleme - vielleicht sogar sehr viel einfacher. Die Antworten auf die Fragen, die sich daraus ergeben, sind der Industrie viele Millionen Euro wert und gelten als entscheidend für die nationale Sicherheit. Kryptographie ist heute ein sehr aktives Forschungsgebiet in der Informatik.

Weiterführende Literatur

Harels Buch *Algorithmics* behandelt Public-Key-Kryptographie; es wird erläutert, wie große Primzahlen verwendet werden, um ein sicheres öffentliches Schlüsselsystem zu erstellen. Als Standardliteratur zum Thema Kryptographie zählt *Cryptography and Data Security* von Dorothy Denning; ein mehr praxisorientiertes Buch heißt *Applied Cryptography* von Bruce Schneier. Das Buch *Turing Omnibus* von Dewdney beschreibt ein weiteres System zur Anwendung von Public Key-Kryptographie.

Teil VI

Das menschliche Gesicht von Computern – Interaktion mit Computern

Das menschliche Gesicht von Computern

Warum sind Computer so schwer zu verstehen? Viele Menschen haben erlebt, wie schwierig Computer zu bedienen sind und dass sie scheinbar nie das tun, was sie wirklich tun sollen, einfach ‚falsch' laufen und absurde Fehler machen. Computer scheinen für Magier und Magierinnen gemacht zu sein, nicht für ‚normale' Menschen. Aber sie sollten für alle Menschen gemacht werden, denn Computer sind alltägliche Werkzeuge, die uns helfen besser zu lernen, zu arbeiten und zu spielen.

Der Bereich eines Computersystems, mit dem man interagiert, wird als „Benutzerschnittstelle" bezeichnet. Das ist das Wichtigste! Obwohl du bestimmt weißt, welche Aufgabe das Programm eigentlich ausführt und wie die Benutzeroberfläche aussieht, ist ein Programm überhaupt nicht ansprechend, wenn du damit nicht interagieren kannst und es auch nicht macht, was du willst. Benutzerschnittstellen sind sehr schwierig zu entwerfen und zu erstellen, und es wird vermutet, dass beim Schreiben von Programmen viel mehr Aufwand in die Erstellung von Schnittstellen fließt, als in irgendeinen anderen Teil des Programms. Manche Software verfügt über hervorragende Benutzeroberflächen, d.h. Schnittstellen, die keine komplizierten Anweisungen benötigen und fast unsichtbar sind, wenn man die Anwendung benutzt. Aber unzählige Softwareprodukte, die ansonsten sehr gut sind, erweisen sich als Flops, weil sie unübliche Benutzeroberflächen haben. Ganze Branchen sind um clevere Schnittstellen-Ideen herum entstanden, wie Textverarbeitung oder Smartphones, die den Zugang zu Rechenfunktionen fördern, die von grundlegender Bedeutung sind.

Aber warum müssen wir überhaupt Benutzerschnittstellen haben? Warum können wir nicht einfach so mit unseren Computern reden wie mit unseren Freunden? Gute Frage. Vielleicht werden wir es eines Tages tun; vielleicht aber auch nicht. Aber sicher noch nicht jetzt: Es gibt gewaltige, praktische Einschränkungen, wie „intelligente" Computer heute sein könnten. Die folgenden Aktivitäten werden dir helfen, die Probleme des Benutzeroberflächen-Designs zu verstehen, klarer über die Einschränkungen von Computern nachzudenken und dich vor dem irreführenden Tamtam zu hüten, der häufig zur Förderung von Computer-Produkten verwendet wird.

Für Lehrpersonen

Auf dem Computer geht es weniger um Kalkulation als vielmehr um Kommunikation. Das Rechnen an sich hat keinen inneren Wert; es lohnt sich nur, wenn die Ergebnisse irgendwie außerhalb des Computers der Welt mitgeteilt werden und dort einen Einfluss haben. Überraschend bedeutet das vielleicht, dass es in der Informatik weniger um Computer geht als vielmehr um Menschen - am Ende ist ein Computer nutzlos, wenn er den Menschen nicht irgendwie hilft. Alle Ideen, die wir uns angeschaut haben, um Computer schnell und effizient arbeiten zu lassen, werden nur benötigt, weil Menschen Computer brauchen, um schnell zu reagieren und wirtschaftlich zu sein.

Die Schnittstelle ist, wie Mensch und Computer kommunizieren. Bei vielen Aktivitäten in diesem Buch geht es um Kommunikation. Die Darstellung von Daten (Teil I) zeigt, wie verschiedene Arten von Informationen an einen Computer oder zwischen Computern übertragen werden können. Bei der Repräsentation von Prozessen (Teil III) geht es darum mit Prozessen an einen Computer zu kommunizieren, um ihm mitzuteilen, wie bestimmte Aufgaben zu erledigen sind - „Programmierung" bedeutet schließlich nur, mit einem Computer in seiner eigenen Sprache zu sprechen! Bei der Kryptographie (Teil V) geht es darum, wie man geheim kommuniziert oder Teile von Geheimnissen kommuniziert, ohne alles zu enthüllen.

Bei den folgenden Aktivitäten geht es darum, wie Menschen mit Computern kommunizieren. Während alle Teile des Buches von Beginn an auf gut verstandenen, technischen Ideen basieren, ist es für diesen Teil nicht mehr so. Das macht es zum einen einfacher, weil keine speziellen Kenntnisse von den SchülerInnen verlangt werden, und zum anderen schwieriger, da ein bestimmter Reifegrad benötigt wird, um zu verstehen, worum es in den Aktivitäten geht und sie mit einem breiteren Kontext in Beziehung zu setzen. Diese Aktivitäten enthalten viel detailliertere Erklärungen als die meisten anderen, da es notwendig ist, Ihnen als Lehrperson genügend Hintergrundmaterial zu geben, um in der Lage zu sein, Folgerungen in der Gruppendiskussion herauszuarbeiten.

In diesem Abschnitt gibt es zwei Aktivitäten. Die erste betrifft den Bereich, der als „Mensch-Computer-Interaktion" bekannt ist und üblicherweise als HCI abgekürzt wird. Um diese Aktivität zu „trennen" (Englisch: to unplug), d.h. ohne von vorherigem Wissen über ein bestimmtes Beispiel eines Computersystems abhängig zu sein, haben wir uns eine Designübung ausgedacht, die nicht wirklich Computer betrifft, sondern grundlegende Prinzipien einführt, die bei der Gestaltung von Mensch-Computer-Interaktionen verwendet werden. Da Mensch-Computer-Design kulturabhängig ist, gibt es in dieser Aktivität keine notwendigerweise „richtigen" Antworten, was manche SchülerInnen frustrieren könnte. Die zweite Aktivität betrifft das Gebiet, das als „künstliche Intelligenz" oder AI bekannt ist. Es beinhaltet ein Ratespiel, das SchülerInnen dazu anregt darüber nachzudenken, was Computer können und was nicht.

Für die technisch Gesinnten

Mensch-Computer-Interaktion ist zu einem der aktuellsten Forschungsgebiete in der Informatik geworden, da die Menschen erkannt haben, wie sehr der Erfolg eines Softwareprodukts von seiner Benutzerschnittstelle abhängt. Das Thema stützt sich auf eine breite Palette von Disziplinen außerhalb der Informatik, wie Psychologie, Kognitionswissenschaft, Linguistik, Soziologie - auch Anthropologie. Nur wenige InformatikerInnen haben in diesen Bereichen eine Ausbildung, und HCI ist ein wichtiger Wachstumsbereich für Menschen, die sich für die „sanftere" Seite des Themas interessieren.

Künstliche Intelligenz (AI) ist ein Thema, das häufig zu Streit führt. In diesem Buch haben wir versucht, einen Mittelweg zwischen AI-Anhängern, die glauben, dass intelligente Maschinen bereits in unmittelbarer Nähe vorkommen, und AI-Skeptikern zu steuern, die glauben, dass Maschinen prinzipiell nicht intelligent sein können. Unser Ziel ist es, die SchülerInnen zu ermutigen, selbständig über solche Probleme nachzudenken und eine ausgewogene Sichtweise zu fördern.

Die Aktivitäten hier beziehen sich auf zwei sehr gut lesbare Bücher, die wir Ihnen sehr empfehlen, wenn Sie diese Themen weiter verfolgen möchten: *The design of everyday things* von Don Norman und *Artificial intelligence: the very idea* von John Haugeland.

Computer beinhalten eine andere wichtige Art der Kommunikation, die in diesem Buch nicht behandelt wird: Kommunikation zwischen Menschen, die ein Computersystem aufbauen. SchülerInnen, die etwas über Computer lernen und ihren Weg in den Arbeitsmarkt finden - vielleicht mit einem Universitätsabschluss in Informatik - sind immer wieder überrascht, wie viel zwischenmenschliche Kommunikation ihr Job mit sich bringt. Computerprogramme sind die komplexesten Objekte, die je von Menschen konstruiert wurden, mit Millionen oder vielleicht Milliarden ineinander verschlungenen Bauteilen, und Programmierprojekte werden von eng verbundenen Teams durchgeführt, die zusammenarbeiten und einen großen Teil ihrer Zeit mit Kommunikation verbringen. Sobald das Produkt fertig ist, folgt die Aufgabe, mit den Kunden über Benutzerhandbücher, Kurse, „Hilfe"-Fernsprechanlagen, Online-Support und dergleichen zu kommunizieren - ganz zu schweigen von dem Problem der Kommunikation mit potenziellen Kunden durch Präsentationen, Ausstellungen und Werbung. Wir haben noch keinen Weg gefunden, um den zwischenmenschlichen Kommunikationsaspekt der Informatik für SchülerInnen realistisch zu „trennen" (to unplug it), sodass in diesem Buch nicht darauf eingegangen wird. Aber es ist etwas, wozu die Computerprofis, die einen Klassenraum besuchen, in der Lage sind, nämlich Dinge aus eigener Erfahrung zu beschreiben und Diskussionen anzuregen.

Aktivität 20: Die Schokoladenfabrik – menschliche Schnittstellengestaltung

Zusammenfassung

Ziel dieser Aktivität ist es, das Bewusstsein für die Gestaltung von Benutzeroberflächen zwischen Mensch und Maschine zu fördern. Weil wir in einer Welt leben, in der schlechte Gestaltungen (Designs) weit verbreitet sind, haben wir uns daran gewöhnt, Probleme mit den Artefakten, mit denen wir interagieren, zu akzeptieren und uns selbst die Schuld zu geben („menschlicher Fehler“, „unzureichendes Training“, „zu kompliziert für mich“), anstatt die Probleme auf fehlerhaftes Design zurückzuführen. Das Problem wird durch Computer stark erhöht, weil sie keinen offensichtlichen Zweck haben - tatsächlich sind sie Mehrzweckgeräte - und ihr Aussehen gibt keine Hinweise darauf, wozu sie dienen oder wie sie zu bedienen sind.

Einfügen in den Lehrplan

- Technologie – Verstehen, dass Technologie eine gezielte Intervention durch Design ist

Benötigte Kenntnisse

- Design
- Logisches Denken
- Bekanntheit von Gebrauchsgegenständen

Alter

- 7+

Materialien

Jede Gruppe der SchülerInnen braucht:

- eine Kopie des Arbeitsblatts Wie öffnet man Türen?, Herdplatten und
- eine Kopie der Bilder vom Arbeitsblatt Icons (entweder dargestellt mithilfe eines Beamers/ Projektors unter Verwendung von Folien oder ausgedruckten Karten, die der Klasse gezeigt werden können) und
- eine oder mehrere von den sechs Karten auf dem Arbeitsblatt Icon Karten. Zerschneide das Arbeitsblatt in sechs einzelne Karten und verteile die Karten den Gruppen.

Die Schokoladenfabrik

Einführung

Die große Schokoladenfabrik wird von einer Rasse elfenähnlicher Wesen namens Oompa Loompas geführt . Die Oompa Loompas haben eine schrecklich schlechte Erinnerung und keine Schriftsprache. Deshalb fällt es ihnen schwer sich zu erinnern was sie tun müssen, um die Schokoladenfabrik zu betreiben und oft laufen Dinge schief. Aus diesem Grund wird eine neue Fabrik entworfen, die sehr einfach zu bedienen sein soll.

Diskussion

1. Erkläre den SchülerInnen die Geschichte und teile sie in kleine Gruppen auf.

2. Das erste Problem, mit dem die Oompa Loompas[1] konfrontiert sind, besteht darin mit dampfenden Eimern voll flüssiger Schokolade durch die Türen zu kommen. Sie können sich nicht daran erinnern, ob sie die Türen drücken, ziehen oder zur Seite schieben sollen um sie zu öffnen. Folglich stoßen sie aneinander und verschütten überall klebrige Schokolade. Die SchülerInnen sollten das Arbeitsblatt Wie öffnet man Türen? ausfüllen. Mehr als eine Schachtel ist in jedem Fall geeignet. Für einige der Türen (einschließlich der ersten) ist es nicht offensichtlich wie man sie öffnet und die SchülerInnen sollten aufschreiben, was sie zuerst versuchen würden. Sobald alle ihre Arbeitsblätter ausgefüllt haben, lass alle SchülerInnen über die Vorteile jedes Türtyps sprechen, insbesondere im Hinblick darauf, wie einfach sie sagen können wie sie funktioniert und wie geeignet die Tür ist, wenn man einen Eimer mit heißer Schokolade trägt. Danach sollten sie entscheiden, welche Art von Türen und Griffe in der Fabrik verwendet werden sollen.

3. Führe nach dieser Aktivität eine Gruppendiskussion. Die folgende Tabelle enthält eine kurze Erläuterung für jeden Türtyp auf dem Arbeitsblatt. Richtige Türen geben anhand ihrer Rahmen und Scharniere Hinweise daraufhin, wie sie sich öffnen und ob sich Türen nach innen oder außen öffnen. Betrachtet die Arten von Türgriffen, die in eurer Schule verwendet werden und besprecht, ob sie angemessen sind (sie können ziemlich ungeeignet sein!). Gibt es eine Tür, die euch oft durcheinander bringt? Warum? Öffnen die Türen im Korridor normalerweise nach innen oder außen? Und warum? (Antwort: Sie öffnen sich so, dass du, wenn du herausgehst, den Leuten, die den Gang entlang laufen, nicht die Tür zuschmeißen wirst. In manchen Situationen öffnet sich eine Tür auch nach außen, um die Evakuierung im Notfall zu erleichtern.)

1 Mit Entschuldigung an Roald Dahl. Du kennst die Oompa Loompas sicher, wenn du seine wunderbare Geschichte „Charlie und die Schokoladenfabrik“ gelesen hast. Wenn nicht, egal: Die Geschichte ist für diese Aktivität nicht relevant.

Einfache Tür	Man kann nicht sehen wie man diese öffnet, nur dass sie keinen Griff hat und man drücken muss anstatt zu ziehen.	**Tür mit Aufschrift**	Das Label ist wie eine kleine Bedienungsanleitung. Aber sollte eine Tür eine Bedienungsanleitung benötigen? Und die Oompa Loompas können nicht lesen.
Tür mit Scharniere	Zumindest kannst du sehen nach welcher Seite die Tür sich öffnen lässt.	**Tür mit Riegel**	Klar, dass du den Riegel schieben musst, aber auf welche Seite?
Tür mit Griff	Griffe wie diese sind normalerweise zum Ziehen oder Schieben geeignet.	**Tür mit Knauf**	Der Knauf zeigt an, dass du auf ihn zugreifen sollst, aber nicht, ob man drücken, ziehen oder drehen soll; schieben kann man ihn wahrscheinlich nicht.
Tür mit Täfelung	Klar, dass du die Tür schieben musst. Was könntest du noch tun?	**Glastür**	Der kleine vertikale Balken auf dies er Seite signalisiert "ziehen"; der längere horizontale Balken auf der anderen Seite sagt "drücken".
Schiebetür	Diese kann nur hin- und hergeschoben werden.		

4. Das Schlüsselkonzept hier wird als der Angebotscharakter (Affordanz) eines Objekts bezeichnet, dessen sichtbare Merkmale - sowohl fundamentale als auch wahrgenommene - andeuten, wie das Objekt verwendet werden soll. Affordanzen sind die Arten von Operationen, die das Objekt erlaubt oder „anbietet".

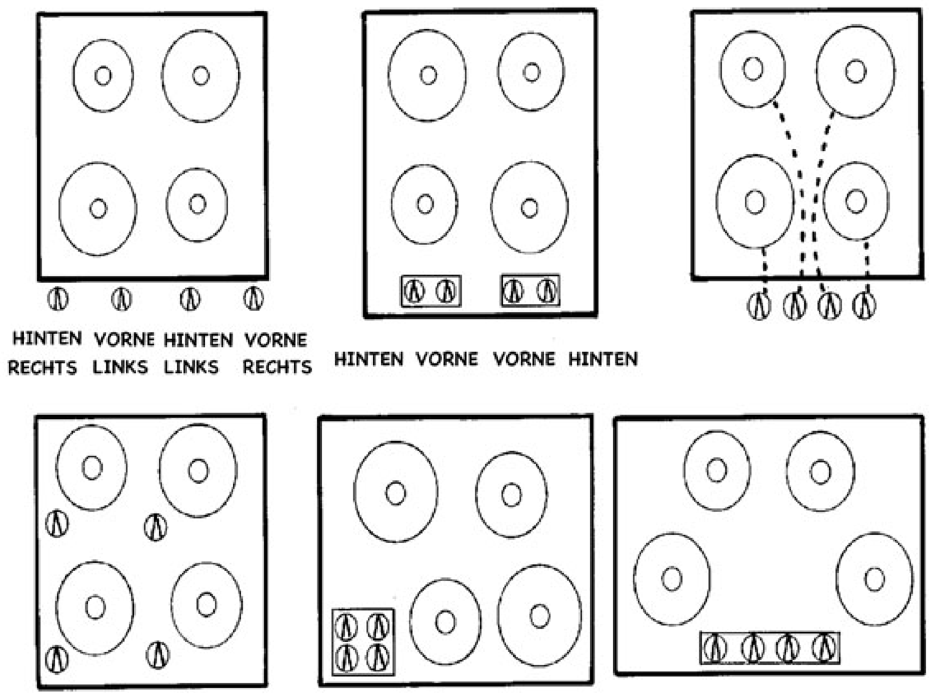
Zum Beispiel ist es (meistens) aufgrund ihrer Erscheinung klar, dass sich Stühle zum Sitzen, Tische zum Aufstellen von Gegenständen, Knöpfe zum Drehen, Schlitze zum Einfügen von Dingen und Tasten zum Draufdrücken anbieten. Bei einer Computerschnittstelle sind die Affordanzen die Formen von Schaltflächen, Textfeldern, Menüs usw., die dem Benutzer einen Hinweis geben, wie sie verwendet werden sollten. Wenn ein Knopf anders aussieht, werden die Leute nicht merken, dass sie ihn drücken können. Dies mag verständlich sein, aber diese Probleme sind auf digitalen Geräten allgegenwärtig.

Türen sind sehr einfache Objekte. Komplexe Dinge müssen eher erklärt werden, was aber bei einfachen Objekten nicht notwendig sein sollte. Wenn einfache Objekte Bilder, Beschriftungen oder Anweisungen benötigen, ist das Design missglückt.

5. Die Töpfe, die verschiedene Arten von Schokolade enthalten, müssen bei unterschiedlichen Temperaturen gekocht werden. In der alten Schokoladenfabrik wurden Herdplatten verwendet, wie auf dem Arbeitsblatt Herdplatten dargestellt. Der linke Knopf steuerte die hintere linke Platte, der nächste Knopf die vordere linke Platte, der nächste die vordere rechte Platte und der rechte Knopf die Kochplatte hinten rechts. Die Oompa Loompas machten immer Fehler, kochten die Schokolade mit der falschen Temperatur und verbrannten sich ihre Ärmel, wenn sie über die Herdplatten griffen, um die Schalter anzupassen.

6. Die SchülerInnen sollen nachdenken, wie die Schalter an ihren Herden zuhause angeordnet sind und sich eine bessere Anordnung für die neue Fabrik einfallen lassen.

Nächster Schritt dieser Aktivität ist eine Gruppendiskussion. Das folgende Bild zeigt einige mögliche Anordnungen.



Alle, außer der unten links, haben die Bedienelemente an der Vorderseite, um nicht über die Herdplatten greifen zu müssen. In dem Design oben links gibt es viele mögliche Zuordnungen der Herdplattenschalter (tatsächlich 24 Möglichkeiten), sodass acht Wörter zur Kennzeichnung benötigt werden. Die „paarweise" Anordnung mit nur vier möglichen Zuordnungen (zwei auf der linken und zwei auf der rechten Seite) in der oberen Mitte ist besser; hier sind nur vier Beschriftungen nötig.

Das Design oben rechts gibt die Beziehung zwischen Schalter und Platte eher schematisch als sprachlich an (was gut ist für die Oompa Loompas!). Die unteren drei Designs benötigen keine Etiketten. Der linke hat einen Schalter für jede Herdplatte, was umständlich und gefährlich ist. Bei den anderen beiden handelt es sich um eine geringfügige Verlagerung der Herdplatten, aber aus verschiedenen Gründen: In der mittleren werden sie verschoben, um Platz für die Schalter zu lassen, während sie in der rechten Darstellung neu angeordnet werden, um die Zuordnung zu verdeutlichen.

Das Schlüsselkonzept hier ist die Zuordnung (Mapping) von Schaltern auf ihre Ergebnisse in der realen Welt. Natural Mapping, das physikalische Analogien und kulturelle Standards nutzt, führt zu einem unmittelbaren Verständnis. Natürliche Zuordnung (Natural Mapping)[2], die physikalische Analogien und kulturelle Standards nutzt, führt zu einem unmittelbaren Verständnis. Die räumlichen Zuordnungen in der unteren Zeile des Bildes sind gute Beispiele - sie sind leicht erlernbar und werden immer in Erinnerung behalten. Willkürliche Zuordnungen, wie in der oberen Zeile dargestellt, müssen beschriftet, erklärt und gespeichert werden.

7. Die Fabrik ist voll von Förderbändern, die Töpfe mit halb hergestellter Schokolade zu den verschiedenen Stadien der Fertigstellung transportieren. Diese Förderbänder werden von Oompa Loompas auf Anweisung eines zentralen Kontrollraums manuell gesteuert.

Die Leute im Kontrollraum müssen in der Lage sein, dem Oompa Loompa mitzuteilen, dass er das Förderband anhalten, verlangsamen oder neu starten soll.

In der alten Fabrik wurde dies mit einem Sprachsystem gemacht: Die Stimme des Kontrollraumpersonals kam durch die Steuerung des Förderbands aus einem Lautsprecher. Aber die Fabrik war laut und es war schwer etwas zu hören. Die Gruppen sollten ein Schema entwerfen, das visuelle Signale verwendet.

Eine Möglichkeit besteht darin Lichter anzuzünden, um Stop!, Langsamer Fahren! und Einschalten! anzuzeigen. Die SchülerInnen werden wahrscheinlich herausfinden, dass das wie eine Ampel funktionieren soll, indem sie Rot für *Stop!,* Gelb für *Langsamer Fahren!* und Grün für *Einschalten!* verwenden. Sie sollten auch wie Ampeln angeordnet sein, mit rot an der Spitze und grün an der Unterseite.

Aber zuerst verrate der Klasse, dass im Oompa Loompa-Land Ampeln anders funktionieren als sie für uns tun: Gelb bedeutet zu stoppen, rot bedeutet zu gehen und Lichter werden grün, um die Menschen zu warnen, dass sie bald ein Stopplicht haben werden. Wie wirkt sich das auf die Dinge aus? (Antwort: Die Fabrik sollte den üblichen Regeln für Ampeln der Oompa Loompa folgen - wir sollten nicht versuchen unsere eigenen durchzusetzen.)

2 Die eigentliche Funktion natürlicher Zuordnungen besteht darin, die Notwendigkeit von Informationen aus dem Gedächtnis eines Menschen zu reduzieren, um eine Aufgabe auszuführen.

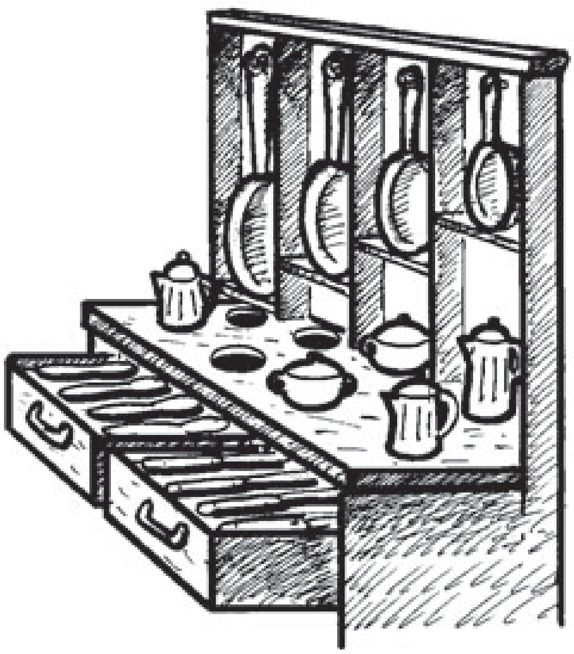
Die Schlüsselkonzepte hier, sind die der Übertragungseffekte - die Menschen übertragen Lernen und Erwartungen früherer Objekte in neue, aber ähnliche Situationen und Stereotypen der Bevölkerung - verschiedene Bevölkerungsgruppen lernen bestimmte Verhaltensweisen und erwarten, dass die Dinge in einer bestimmten Weise funktionieren.

Obwohl das Ampelbeispiel vielleicht weit hergeholt erscheint (obwohl im Oompa Loompa-Land nichts weit hergeholt ist), gibt es viele Beispiele in unserer eigenen Welt: In Amerika sind Lichtschalter eingeschaltet, wenn sie oben sind und ausgeschaltet, wenn sie unten sind. In Großbritannien ist das Gegenteil der Fall; Taschenrechner-Tastaturen und TouchTone-Telefone sind verschieden angeordnet. Und Zahlenformate (Dezimalpunkt oder Komma) und Datumsformate (Tag / Monat / Jahr oder Monat / Tag / Jahr) unterscheiden sich auf der ganzen Welt.

8. Wenn eine Schicht der Oompa Loompas in der Schokoladenfabrik beendet ist, müssen sie Töpfe, Pfannen, Krüge, Löffel und Rührer für die nächste Schicht waschen und wegräumen. Es gibt einen Schrank mit Regalen, auf die sie die Gegenstände legen können; aber die nächste Schicht hat immer Schwierigkeiten herauszufinden, wohin die Gegenstände weggeräumt wurden. Oompa Loompas sind sehr schlecht darin, sich an Dinge zu erinnern und haben Probleme mit Regeln wie „Lege die Töpfe immer auf das mittlere Regal“ oder „Stell die Krüge nach links“.

Die Schulkindergruppen sollen versuchen eine bessere Lösung zu finden.

Das Bild unten auf der linken Seite zeigt eine gute Anordnung (die manchmal - aber aus ganz anderen Gründen - auf Yachten und anderen Orten verwendet wird, wo es notwendig ist zu verhindern, dass die Gegenstände herumrutschen).



Das Schlüsselkonzept hier ist *sichtbare Einschränkungen* zu verwenden, um klar zu machen, wo die Gegenstände abgelegt werden sollen. Aus der Größe und Form jedes Loches, für das das Utensil bestimmt ist, wird klar: Der Designer hat die Beschränkungen sichtbar gemacht und die physikalischen Eigenschaften der Objekte verwendet, um zu vermeiden, dass man sich auf willkürliche Konventionen verlassen muss.

9. Im Hauptkontrollraum der Schokoladenfabrik befinden sich viele Knöpfe, Hebel und Schalter, um die einzelnen Maschinen zu bedienen. Diese müssen etikettiert werden, aber weil die Oompa Loompas nicht lesen können, müssen die Etiketten bildhaft – ikonisch - statt sprachlich sein.

Um den SchülerInnen ein Gefühl für Symbole (Icons) zu geben, zeigt das Arbeitsblatt Icons einige Beispiele. Die SchülerInnen sollen herausfinden, was die Icons bedeuten könnten (beispielsweise könnte der in eine Mailbox eingehende Brief das Senden einer Nachricht darstellen). Es gibt keine „richtigen" Antworten in dieser Übung. Die Idee besteht einfach darin, mögliche Bedeutungen zu identifizieren.

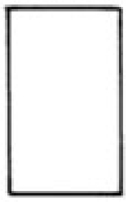
10. Lasst uns jetzt Icons für die Schokoladenfabrik entwerfen. Die Karten auf dem Arbeitsblatt Icon-Karten spezifizieren jeweils eine Ansammlung verwandter Funktionen (Funktionscluster); jede Gruppe von SchülerInnen erhält eine oder mehrere Karten, ohne dass die anderen Gruppen wissen, welche es ist oder sind.

Für die Funktionscluster soll ein Control Panel entworfen werden, das für jede der fünf oder sechs Operationen individuelle Icons enthält. Die Gruppen zeigen ihre Arbeit dann den anderen SchülerInnen, ohne zu sagen, was die einzelnen Operationen bedeuten und verfolgen, ob die anderen erraten können, was die Icons bedeuten. Ermutige die SchülerInnen zum Gebrauch von Fantasie, Farbe und einfachen, klaren Icons.

Arbeitsblatt: Wie öffnet man Türen?

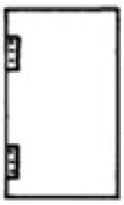
Fülle das Arbeitsblatt aus um zu zeigen, wie du dir die einzelnen Türtypen vorstellst.

Einfache Tür



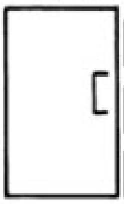
☐ stossen ☐ linke Seite
☐ ziehen ☐ rechte Seite
☐ schieben

Tür mit Scharniere



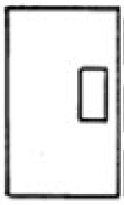
☐ stossen ☐ linke Seite
☐ ziehen ☐ rechte Seite
☐ schieben

Tür mit Griff



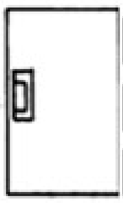
☐ stossen ☐ linke Seite
☐ ziehen ☐ rechte Seite
☐ schieben

Tür mit Täfelung



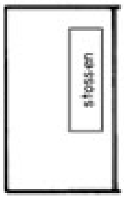
☐ stossen ☐ linke Seite
☐ ziehen ☐ rechte Seite
☐ schieben

Schiebetür



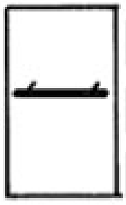
☐ stossen ☐ linke Seite
☐ ziehen ☐ rechte Seite
☐ schieben

Tür mit Aufschrift



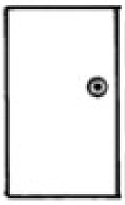
☐ stossen ☐ linke Seite
☐ ziehen ☐ rechte Seite
☐ schieben

Tür mit Riegel



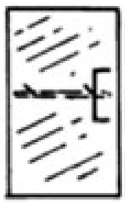
☐ stossen ☐ linke Seite
☐ ziehen ☐ rechte Seite
☐ schieben

Tür mit Knauf



☐ stossen ☐ linke Seite
☐ ziehen ☐ rechte Seite
☐ schieben

Glastür

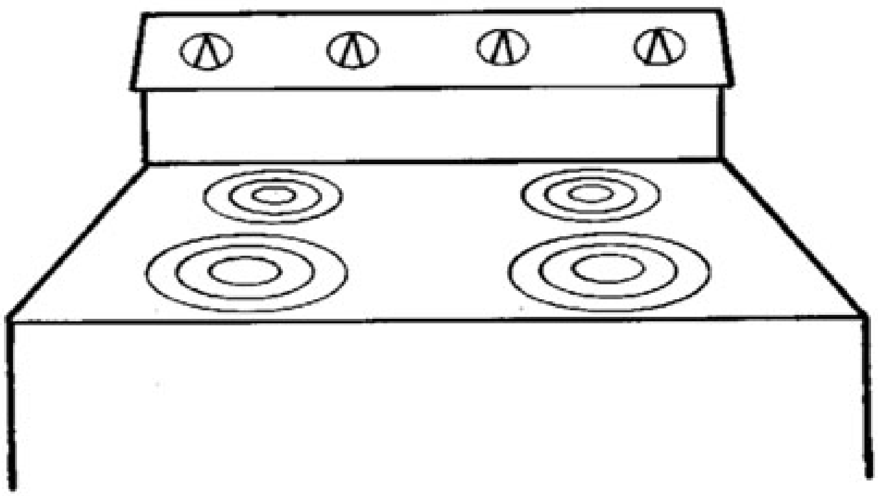


☐ stossen ☐ linke Seite
☐ ziehen ☐ rechte Seite
☐ schieben

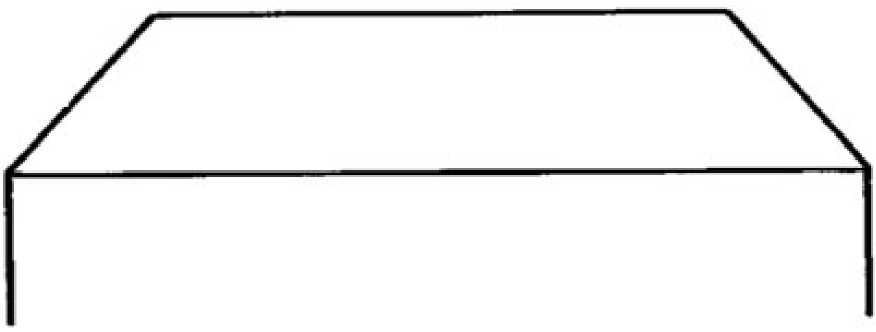
Arbeitsblatt: Herdplatten

Gestalte den Herd neu, so dass die Schalter einfach zu bedienen sind. Front- oder Rückplatten können auf Wunsch hinzugefügt werden.

ALT



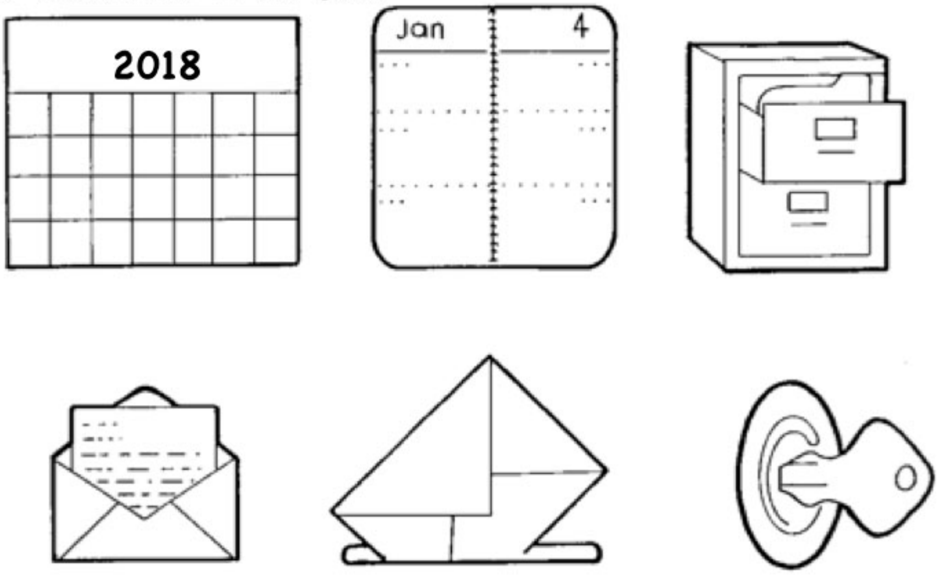
NEU



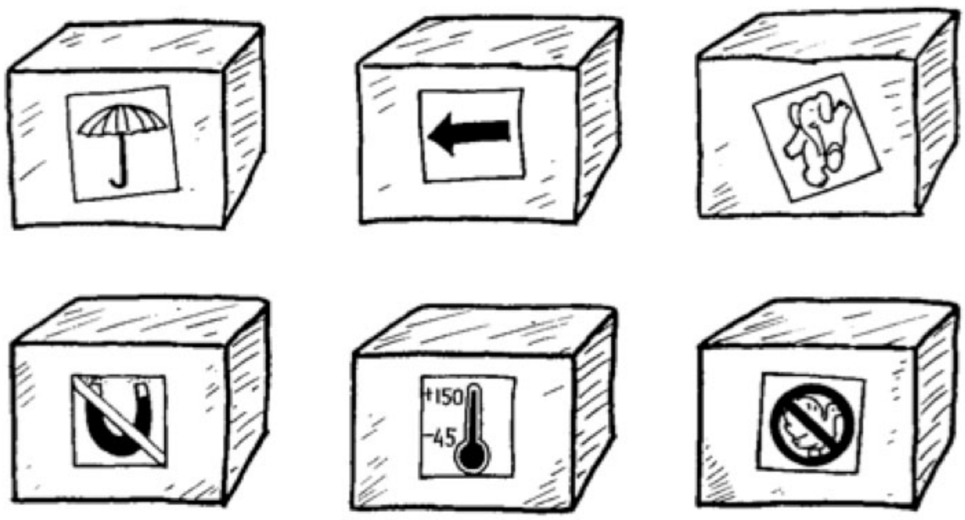
Arbeitsblatt: Icons

Was denkst du, was jedes Symbol (Icon) bedeutet?

In einem Büro...



Auf einem Paket...



Arbeitsblatt: Icon Karten

Schneide die Karten aus und gib jeder Gruppe eine. Lasse jede Gruppe Icons (Symbole) entwerfen, um ein Control Panel zur Darstellung der Anweisung zu erstellen.

Zutaten
Füge hinzu
- Kakao
- Milch
- Zucker
- Zucker als Zusatz
- Butter

Sonderbeilagen
Füge hinzu
- Nüsse
- Karamell
- Ingwer
- Rosinen
- Kokosnuss

Zubereitung
- Beginne das Mischen
- Stoppe das Mischen
- Beginne das Erhitzen
- Stoppe das Erhitzen
- Gieße in die Form
- Stemple ein Muster (viele verschiedene!)

Degustation
- Probiere es
- Wunderbar! Spitzenklasse!
- Ok - ganz normal!
- Igitt! Gekochte Schokolade!
- Igitt, igitt! Werf´s weg

Größeneinteilung
- Kleine Tafel
- Mittlere Tafel
- Große Tafel
- Riesige Tafel
- Wahl der Tafelgröße (in Quadratzentimeter)
- Mache Schokoladenstücke

Verpackung
- In Folie einwickeln
- In Papier einwickeln
- In eine Tasche tun
- In eine Box tun
- Förderband starten
- Förderband stoppen

Variationen und Erweiterungen

Können die SchülerInnen die Zeit auf einer digitalen Armbanduhr oder einem Mikrowellenherd einstellen? Die Zuordnung der Kochplatten auf dem Herd war einfach, da vier Schalter für vier Kochplatten vorhanden waren. Schwieriger wird es, wenn die Anzahl der Aktionen die Anzahl der Steuerelemente übersteigt. Die Tasten an Armbanduhren oder Mikrowellen sind oft äußerst komplex, nicht wegen der Anzahl der Knöpfe (oft sind es nur ein paar), sondern wegen der Anzahl der Zustände, in die das Gerät sich setzen kann. („Sie werden einen Ingenieurabschluss vom MIT benötigen, um das zu schaffen", sagte jemand zu dem führenden Benutzerschnittstellenpsychologen Don Norman, als er seine neue Armbanduhr ansah. Don hat einen Ingenieurabschluss vom MIT und kann die Uhr nach ein paar Stunden Zeit durchschauen. Aber warum sollte es Stunden dauern?)

SchülerInnen sollten nach Orten Ausschau halten, an denen Menschen durch digitale Geräte - Mobiltelefone, Videorekorder, Computer, Fernbedienungen - verwirrt oder frustriert werden – dabei bieten all diese Geräte Möglichkeiten für frustrierte Benutzer! Die SchülerInnen sollten sich fragen: Was ist mit dem Gerät, dass die Benutzer verwirrt sind, und wie hätte es besser gestaltet werden können?

Worum geht es in dieser Aktivität?

Bei der Mensch-Maschine-Interaktion geht es darum, Computersysteme so zu gestalten, zu evaluieren und zu implementieren, dass Menschen ihre Aktivitäten produktiv und sicher ausführen können. Früher gab es Computer für SpezialistInnen und von den BenutzerInnen konnte erwartet werden, dass sie gut ausgebildet und in ihrem Gebrauch besonders geschult waren. Später haben die Leute gedacht, es sei völlig normal, ein „Dummies“-Buch zu kaufen, um herauszufinden, wie sie ihren Computer benutzen können. Aber jetzt sind Computer alltägliche Werkzeuge, die wir alle benutzen müssen, und viel mehr Aufmerksamkeit muss der menschlichen Schnittstelle geschenkt werden.

Viele Katastrophen, von denen einige Lebensverluste mit sich brachten, sind auf unzureichende Schnittstellen zurückzuführen: Flugzeugabstürze und sogar Abschüsse von zivilen Flugzeugen, Autobahnunfälle aufgrund von Fehlern beim Umschalten von ferngesteuerten Autobahnschildern, Atomkraftwerkkatastrophen. In einem kleineren Maßstab erleben die meisten Menschen Frustration - oft extreme Frustration (ein Polizist hat einmal Kugeln in seinen Computerbildschirm gefeuert) - mit Computern und anderen High-Tech-Geräten jeden Tag am Arbeitsplatz. Und es sind nicht nur Computer: Was ist mit diesen eingeschweißten Paketen, die man nur öffnen konnte, wenn man scharfe Krallen oder einen Hakenschnabel hatte; Türen, bei denen man sich beim Öffnen am Handgelenk verletzt; Milchkartons, bei denen man sich immer wieder beim Öffnen bespritzt; Aufzüge, wo man nicht sehen kann, wie man den Knopf drücken soll; Home-Entertainment-Systeme, wo die Werbung behauptet, dass man damit alles tun kann, die es aber fast unmöglich machen, überhaupt etwas zu tun?

Wir gewöhnen uns an „menschliches Versagen“ und verstehen uns selbst als irgendwie unangemessen; Menschen beschuldigen sich oft selbst, wenn etwas schief läuft. Aber viele sogenannte menschliche Fehler sind tatsächlich Konstruktionsfehler. Die Menschen sind beschränkt hinsichtlich der Menge an Informationen, die sie verarbeiten können und Designer müssen das berücksichtigen. Schlechtes Design kann nicht durch ein detailliertes und kompliziertes Benutzerhandbuch korrigiert werden, von dem erwartet wird, dass Menschen es intensiv studieren und sich für immer daran erinnern. Auch Menschen machen Fehler und Design muss dies berücksichtigen.

Die Schnittstellenauswertung ist ein wesentlicher Bestandteil des Designprozesses. Diese Aktivität beinhaltete eine Auswertung, als die SchülerInnen ihre Icon Entwürfe mit anderen verglichen. Eine gründlichere Auswertung würde das Design mit echten Oompa Loompas (welche Icons möglicherweise unterschiedlich wahrnehmen) in einem sorgfältig kontrollierten psychologischen Experiment testen.

Obwohl die Probleme, die durch die Technologie verursacht werden, Zielscheibe von Spott sind, ist das Design der menschlichen Schnittstelle keineswegs ein Spaß. Mangelhafte Schnittstellen führen zu Problemen, die von der Unzufriedenheit einzelner Mitarbeiter bis hin zu Börsenkatastrophen, vom Verlust des Selbstwertgefühls bis hin zum Verlust von Leben reichen.

Weiterführende Literatur

Don Normans Buch T*he design of everyday things* ist ein erfreulicher und befreiender Bericht über die unzähligen Designprobleme alltäglicher Produkte. Jeff Johnsons Buch *Designing with the mind in mind* ist ein nachdenklicher Einblick, wie Menschen denken und wie Schnittstellen gestaltet werden sollten, um den Faktor Mensch zu berücksichtigen.

Aktivität 21: Gespräche mit Computern – der Turing-Test

Zusammenfassung

Diese Aktivität zielt darauf ab, Diskussionen über die Frage anzuregen, ob Computer „Intelligenz“ zeigen können oder in Zukunft wahrscheinlich können werden. Basierend auf der Ansicht eines wegweisenden Informatikers, wie man künstliche Intelligenz erkennt: Wenn sie jemals auftaucht, vermittelt sie etwas von dem, was derzeit machbar ist und wie leicht es ist, durch sorgfältig ausgewählte Demonstrationen von „Intelligenz“ in die Irre geführt zu werden.

Einfügen in den Lehrplan

- Technologie – Technologische Systeme. Verstehen, dass technologische Systeme durch symbolische Sprachwerkzeuge repräsentiert werden und die Rolle, die die Black Box in technologischen Systemen spielt

Benötigte Kenntnisse

- Befragung
- Logisches Denken

Alter

- 7+

Materialien

- Eine Kopie des Arbeitsblatts Turing-Testfragen, die jedes Schulkind sehen kann (entweder eine für jedes Schülerpaar oder eine Kopie auf einem Projektor/Overhead-Projektor darstellen) und
- eine Kopie des Arbeitsblatts Turing-Test Antworten.

Gespräche mit Computern

Diskussion

Diese Aktivität hat die Form eines Spiels, in dem die SchülerInnen versuchen müssen zwischen einem Menschen und einem Computer zu unterscheiden, indem sie Fragen stellen und die Antworten analysieren. Das Spiel wird wie folgt gespielt.

Es gibt vier DarstellerInnen: wir nennen sie Vreni, Viktor, Mathias und Conny (der erste Buchstabe der Namen wird helfen, sich an ihre Rollen zu erinnern). Die Lehrperson koordiniert den Ablauf, der Rest der Klasse bildet das Publikum. Vreni und Viktor sind Vermittler, Mathias und Conny werden Fragen beantworten. Mathias wird die Antworten wie ein Mensch geben, während Conny vorgibt, ein Computer zu sein. Das Ziel der Klasse ist es herauszufinden, welcher von beiden sich als Computer ausgibt und welcher ein Mensch ist. Vreni und Viktor sind da, um faires Spiel zu gewährleisten: Sie leiten Fragen an Mathias und Conny weiter, lassen aber sonst niemanden wissen, wer was ist. Mathias und Conny sind in getrennten Räumen und haben keinen Kontakt zueinander und zum Publikum.

Und so läuft es ab. Vreni übergibt Mathias eine Frage aus der Klasse und Viktor übergibt Conny dieselbe Frage (obwohl die Klasse nicht weiß, wer die Nachrichten an wen weitergibt). Vreni und Viktor kommen mit den Antworten zurück. Die Aufgabe, Vermittler zu sein, besteht darin sicherzustellen, dass das Publikum nicht sieht wie Mathias und Conny die Fragen beantworten.

Bevor die Klasse mit dieser Aktivität beginnt, wähle die Personen aus, die diese Rollen spielen sollen und informiere sie darüber, was sie tun sollen. Vreni und Viktor müssen Fragen aus der Klasse an Mathias und Conny stellen und ihre Antworten an die Klasse zurückgeben. Es ist wichtig, dass sie nicht bekannt geben mit wem sie es zu tun haben, zum Beispiel indem sie sagen: „Sie sagte, die Antwort ist…“. Mathias muss seine eigenen kurzen, genauen und ehrlichen Antworten auf die Fragen geben, die ihm gestellt werden. Conny beantwortet die Fragen, indem sie sie von dem Turing-Test-Antwortbogen wählt. Wo die Antworten kursiv und unterstrichen geschrieben sind, muss sich Conny selbst eine Antwort ausdenken.

Vreni und Viktor sollten Stift und Papier haben, weil einige der Antworten schwer zu merken sein werden.

1. Bevor das Spiel beginnt, hole dir die Meinung der SchülerInnen, ob Computer bereits intelligent sind oder ob sie es eines Tages sein werden. Frage die SchülerInnen nach Ideen und wie sie entscheiden würden, ob ein Computer intelligent ist.

2. Führe die SchülerInnen in den Test für Intelligenz ein, indem du versuchst, den Unterschied zwischen einem Menschen und einem Computer zu erklären, indem man Fragen stellt und die Antworten vergleicht. Der Computer besteht den Test immer, wenn die Klasse den Unterschied nicht zuverlässig erkennen kann. Erkläre den SchülerInnen, dass Vreni und Viktor ihre Fragen an zwei Personen richten werden, von denen eine seine eigenen (menschlichen) Antworten geben wird, während die andere Antworten geben wird, die ein Computer geben könnte. Ihre Aufgabe ist es herauszufinden, wer die Antworten des Computers gibt.

3. Zeige die Liste der möglichen Fragen auf dem *Arbeitsblatt Turing-Testfragen*. Dieses kann entweder kopiert und verteilt oder auf einem Projektor gezeigt werden.

Lass die SchülerInnen auswählen, welche Frage sie zuerst stellen möchten. Sobald eine Frage ausgewählt wurde, bringe sie dazu dir zu erklären, warum sie diese für eine gute Frage halten, den Computer vom Menschen zu unterscheiden. Diese Aufgabe ist der wichtigste Teil der Übung, weil sie die SchülerInnen dazu zwingt darüber nachzudenken, wie ein intelligenter Mensch beantworten könnte, aber ein Computer es nicht kann.

Vreni und Viktor leiten dann die Frage weiter und kehren mit einer Antwort zurück. Die Klasse soll dann besprechen, welche Antwort wahrscheinlich von einem Computer kommt.

Wiederhole das mit weiteren Fragen, vorzugsweise bis die Klasse sicher ist, dass sie herausgefunden hat, wer der Computer ist.

Wenn sie schnell herausfinden, wer der Computer ist, kann das Spiel fortgesetzt werden, indem Vreni und Viktor eine Münze werfen, um zu entscheiden, ob sie ihre Rollen tauschen werden und die Klasse dadurch nicht mehr weiß, wer von ihnen welche Rolle hat.

Die Antworten, die Conny abliest, sind nicht unähnlich zu denen, die einige „intelligente" Computerprogramme erzeugen können. Einige der Antworten werden wahrscheinlich schnell vom Computer zurück gegeben.

Zum Beispiel wird wahrscheinlich niemand die Quadratwurzel von 2 bis auf zwanzig Dezimalstellen aufsagen und die meisten Leute (einschließlich der SchülerInnen in der Klasse) sind nicht in der Lage, diese Frage überhaupt zu beantworten. Einige Fragen werden den Computer verraten, wenn die Antworten zusammengesetzt werden.

Zum Beispiel klingen die Antworten auf die Fragen „Willst du…" von sich aus plausibel, aber wenn du sie öfter verwendest, wird es offensichtlich sein, dass eine einfache Formel verwendet wird, um die Antworten aus den Fragen zu generieren.

Einige der Antworten deuten darauf hin, dass die Frage falsch verstanden wurde, obwohl die Klasse vermuten könnte, dass der Fragesteller/die Fragestellerin den Fehler begangen haben könnte.

Viele der Antworten sind sehr langweilig, aber korrekt und eine Folgefrage würde wahrscheinlich zeigen, dass der Computer das Thema nicht wirklich versteht. Die Antwort „Ich weiß nicht“ ist relativ sicher für den Computer und könnte ihn sogar menschlicher erscheinen lassen - wir können auch erwarten, dass die SchülerInnen auf einige der Fragen mit „Ich weiß nicht“ antworten, etwa bei der Frage nach der Quadratwurzel von 2. Wenn jedoch ein Computer diese Antwort zu oft oder auf eine sehr einfache Frage gibt, dann würde dies wiederum seine Identität offenbaren.

Da das Ziel des Computers darin besteht, die FragestellerIn zu überzeugen, dass sie es mit einer Person zu tun haben, sind einige der Antworten absichtlich irreführend - wie etwa verzögerte und falsche Antworten auf Rechenaufgaben.

Fragen und Antworten dazu sollten viel Diskussionsstoff liefern.

Arbeitsblatt: Turing-Testfragen

Wähle Fragen/Aufgaben aus dieser Liste, die du an den versteckten Menschen und “Computer” schicken möchtest.

1. Wie heißt Bart Simpsons jüngere Schwester?
2. Was weißt du von Michael Ende?
3. Bist du ein Computer?
4. Was ist die nächste Zahl in der Reihenfolge 3, 6, 9, 12, 15?
5. Was hältst du von Atomwaffen?
6. Was ist 2 x 78?
7. Was ist die Quadratwurzel von zwei?
8. Addiere 34957 und 70764.
9. Magst du die Schule?
10. Möchtest du gern tanzen?
11. Welchen Tag haben wir heute?
12. Welche Uhrzeit ist es?
13. Wieviele Tage hat der Monat Februar in einem Schaltjahr?
14. Wieviele Tage hat eine Woche?
15. Für welches Land hat die Flagge einen roten Kreis mit weißen Hintergrund?
16. Möchtest du gern Bücher lesen?
17. Was isst du am liebsten?

Arbeitsblatt: Turing-Test Antworten

Wähle Antworten aus dieser Liste, die du als „Computer“ schicken möchtest. Wo die Antworten kursiv und unterstrichen geschrieben sind, musst du dir selbst eine Antwort ausdenken.

1. Wie heißt Bart Simpsons jüngere Schwester?

Ich weiß es nicht mehr.

2. Was weißt du von Michael Ende?

Er hat tolle Bücher geschrieben.

3. Bist du ein Computer?

Bist du ein Computer?

4. Was ist die nächste Zahl in der Reihenfolge 3, 6, 9, 12, 15?

18

5. Was hältst du von Atomwaffen?

Atomwaffen sind sehr gefährlich und sollten nicht benutzt werden.

6. 17. Was ist 2 x 78?

166 (das ist absichtlich falsch!)

7. Was ist die Quadratwurzel von 2?

1.41421356237309504878

8. Addiere 34957 und 70764.

(warte etwa 20 Sekunden, bevor du die Antwort gibst!)

105621

9. Magst du die Schule?

Ja, ich mag die Schule.

10. Möchtest du gerne tanzen?

Ja, ich tanze gerne.

11. Welchen Tag haben wir heute?

(nenne den richtigen Wochentag)

12. Welche Zeit ist es?

(nenne die richtige Zeit)

13. Wieviele Tage hat der Monat Februar in einem Schaltjahr?

2000 und 2004 waren Schaltjahre (das ist absichtlich falsch!)

14. Wieviele Tage hat eine Woche?

Sieben

15. Welches Land hat eine Flagge mit einem roten Kreis auf weißem Hintergrund?

Das weiß ich nicht.

16. Möchtest du gerne Bücher lesen?

Ja, ich lese gern Bücher.

17. Was isst du am liebsten?

Danke, ich bin nicht hungrig.

Variationen und Erweiterungen

Das Spiel kann auch mit nur drei SchülerInnen gespielt werden, wenn Vreni auch die Rolle von Viktor und Conny übernimmt. Vreni stellt Mathias die Frage, notiert seine Antwort und notiert die Antwort aus dem Arbeitsblatt Turing-Test Antworten. Sie gibt die zwei Antworten zurück und verwendet die Buchstaben A und B, um zu identifizieren, von wem die Antwort kam.

Um zu überlegen, ob ein Computer einen Menschen bei der Befragung simulieren kann, überlege dir mit der Klasse, welches Wissen benötigt wird, damit jede der Fragen mittels Turing-Test Antworten beantwortet werden kann. Die SchülerInnen können andere Fragen vorschlagen, die sie gerne gestellt hätten, und sollten die Art von Antworten besprechen, die sie erwarten würden. Dies erfordert einiges an Vorstellungskraft, da es unmöglich ist vorauszusagen, wie das Gespräch verlaufen wird.

Frage:	Bitte schreibe mir ein Sonett zum Thema Forth Bridge[1].
Antwort:	Ohne mich! Ich kann nicht Gedichte schreiben.
Frage:	Addiere 34957 und 70764.
Antwort:	(ca. 30 Sekunden Pause) ... 105621
Frage:	Spielst du Schach?
Antwort:	Ja
Frage:	Mein König ist auf dem Platz K1 und ich habe keine anderen Figuren. Du hast nur deinen König auf dem K6-Feld und einen Turm auf dem R1-Feld. Du bist dran.
Antwort:	(ca. 15 Sekunden Pause) ... Turm auf R8 – Schachmatt.

Zur Veranschaulichung sind hier zwei Beispielgespräche.

Als erstes werden „faktische“ Fragen verwendet, die ein Computer möglicherweise richtig beantworten kann, während Letzteres zeigt, wie weitreichend die Diskussion sein könnte, und die Art von breitem Wissen demonstriert, auf das ein Computer zurückgreifen müsste.

1 f Die Forth Bridge ist eine zweigleisige Eisenbahnbrücke über den Firth of Forth, dem weit ins Land reichenden Mündungstrichter des Flusses Forth in Schottland , sowie Weltkulturerbe (s. Wikipedia)

Frage:	In der ersten Zeile des Sonetts heißt es: „Soll ich dich mit einem Sommertag vergleichen“; würde „ein Frühlingstag“ nicht genauso gut oder besser sein?
Antwort:	Es wird nicht so gescannt.
Frage:	Wie wäre es mit „einem Wintertag“? Das kann doch gut gescannt werden.
Antwort:	Ja, aber niemand möchte mit einem Wintertag verglichen werden.
Frage:	Würden Sie sagen, Mr. Pickwick hat Sie an Weihnachten erinnert?
Antwort:	In gewisser Weise.
Frage:	Aber Weihnachten ist ein Wintertag, und ich glaube nicht, dass Mr. Pickwick sich um den Vergleich kümmern würde.
Antwort:	Ich glaube nicht, dass du es ernst meinst. Unter Wintertag versteht man eher einen typischen Wintertag als einen besonderen wie Weihnachten.

Es gibt ein System namens „Eliza“, das im Internet weit verbreitet ist (es ist eine Art „Chatbot“, ein System, mit dem man Gespräche eintippen kann).

Eliza simuliert eine Sitzung mit einem Psychotherapeuten und kann mit einigen einfachen Regeln bemerkenswert intelligente Konversation erzeugen. Einige Beispielsitzungen mit Eliza werden unten besprochen. D

Die SchülerInnen können Eliza oder andere Chatbots ausprobieren, obwohl sie darauf hingewiesen werden müssen, dass bei einigen davon Sprachen und Themen installiert sind, die für die SchülerInnen nicht geeignet sind.

Worum geht es in dieser Aktivität?

Seit Jahrhunderten streiten sich PhilosophInnen darüber, ob eine Maschine menschliche Intelligenz simulieren könnte, und umgekehrt, ob das menschliche Gehirn nichts anderes ist als eine Maschine, die ein besseres Computerprogramm ausführt. Diese Frage hat die Menschen stark geteilt. Manche finden die Idee absurd, wahnsinnig oder sogar blasphemisch, während andere glauben, dass künstliche Intelligenz unvermeidlich ist und wir letztendlich Maschinen entwickeln werden, die genauso intelligent sind wie wir. (Wie zahlreiche Science-Fiction-Autoren gezeigt haben, werden Maschinen, selbst wenn sie letztendlich unsere eigene Intelligenz übertreffen, in der Lage sein, sogar klügere Maschinen zu konstruieren.) Künstliche Intelligenz (KI)-ForscherInnen wurden dafür kritisiert, dass sie ihre hochgesteckten Ziele dazu nutzen, Forschungsgelder von Regierungen zu bekommen um autonome Kriegsmaschinen zu bauen, während die ForscherInnen selbst die Proteste als technikfeindliche Gegenreaktion zurückweisen und eindeutig auf die Vorteile für die Gesellschaft hinweisen, wenn es nur ein bisschen mehr Intelligenz gäbe. Eine ausgewogenere Sichtweise ist, dass künstliche Intelligenz weder absurd noch unvermeidlich ist: Während keines der gegenwärtigen Computerprogramme „Intelligenz“ in einem weiten Sinne aufweist, ist es eine experimentelle, noch nicht beantwortete Frage, ob sie dazu auch in der Lage sind.

Die KI-Debatte hängt von der Definition von Intelligenz ab. Viele Definitionen wurden vorgeschlagen und diskutiert. Ein interessanter Ansatz zur Schaffung von Intelligenz wurde in den späten 1940er Jahren von Alan Turing, einem bedeutenden britischen Mathematiker, Kriegsgegner und Langstreckenläufer, als eine Art „Gedankenexperiment“ vorgeschlagen. Turings Ansatz war operativ - anstatt Intelligenz zu definieren, beschrieb er eine Situation, in der ein Computer sie demonstrieren konnte. Sein Szenario war ähnlich der oben beschriebenen Aktivität, die Essenz bestand darin einen Fragesteller zu haben, der sowohl mit einer Person als auch mit einem Computer über eine Fernschreiberverbindung (die neueste Technologie der 1940er Jahre!) interagierte. Wenn der Fragesteller nicht zuverlässig voneinander unterscheiden konnte, hätte der Computer Turings Test für Intelligenz bestanden. Die Verwendung eines Fernschreibers vermied das Problem, dass der Computer durch physische Eigenschaften oder Tonfall verraten wurde. Man kann sich vorstellen, die Übung so zu erweitern, dass die Maschine eine Person in Aussehen, Klang, Berührung, vielleicht sogar Geruch nachahmen muss - aber diese physischen Attribute scheinen für die Intelligenz kaum relevant zu sein.

Turings Originaltest war ein bisschen anders als unserer. Er schlug als vorläufige Übung ein Szenario vor, in dem ein Mann und eine Frau verhört wurden und der Fragesteller ihre Geschlechter bestimmen musste. Das Ziel des Mannes bestand darin, den Fragenden davon zu überzeugen, dass er die Frau war, und die Frau sollte den Fragenden davon überzeugen, dass sie sie selbst war. Dann stellte sich Turing einen Computer vor - da dies nur als Gedankenexperiment vorgeschlagen wurde - der eine der Parteien ersetzte, um zu sehen, ob er bei diesem „Nachahmungsspiel“ genauso erfolgreich sein konnte wie ein Mensch. Wir haben das Setup für diese Klassenaktivität geändert, weil die Art von Fragen, die die SchülerInnen stellen könnten um das Geschlecht zu bestimmen, wahrscheinlich nicht angemessen wäre. Außerdem fördert die Übung die klischeehafte Zuordnung der Geschlechterrollen - ganz zu schweigen von Irreführungen.

Intelligenz nachzuahmen ist eine schwierige Aufgabe. Wenn die Rollen vertauscht würden und eine Person sich als Computer ausgeben wollte, würde sie das sicher nicht tun können: Sie würde durch ihre langsame (und wahrscheinlich ungenaue) Antwort auf Fragen wie „Was ist 123456 × 789012?" verraten.

Es ist jedoch überraschend einfach für einen Computer, eine 'dünne Schicht' an Konversationsfähigkeit zu erlangen. Das berühmte Programm Eliza (bereits erwähnt), das in den frühen 60er Jahren entwickelt wurde, simulierte einen nicht-direktiven Psychotherapeuten im Dialog mit dem Benutzer. Unten ist ein Beispiel für eine Konversation mit diesem System. Etwas, das sich einer natürlichen Konversation nähert, kann von Maschinen erzeugt werden, wie z.B.:

- Erzeugen von vorgefertigten Antworten (z. B. Kannst du da an ein bestimmtes Beispiel denken? als Antwort auf etwas, das anfängt wie Sie sind immer ...; Es tut mir leid zu hören, dass ... als Antwort auf Er sagt ...);
- Aussagen des Nutzers widerspiegeln (z. B. Dein Freund hat dich hierher kommen lassen als Antwort auf Mein Freund hat mich hierher kommen lassen);
- Schlüsselworte erkennen (Erzähle mir mehr über deine Familie als Antwort auf ... Mutter ...);
- einige Standardausdrücke (Was würde es für dich bedeuten, wenn ...);
- Dinge, die aus früheren Teilen der Konversation übernommen wurden (Hat das etwas damit zu tun, dass ...).

Natürlich bedeutet dies nicht, dass der Turing-Test bestanden wurde, da die Person keine Fragen stellt, um festzustellen, ob der Befragte eine Maschine ist oder nicht: Wenn es so wäre, würde es nicht lange dauern, bis es geklärt worden wäre.

Person:	Menschen sind alle gleich.
Computer:	Auf welche Weise?
Person:	Sie nerven uns immer wegen irgendwas.
Computer:	Kannst du an ein bestimmtes Beispiel denken?
Person:	Nun, mein Freund hat mich hierher kommen lassen.
Computer:	Dein Freund hat dich hierher kommen lassen.
Person:	Er sagt, ich bin die meiste Zeit deprimiert.
Computer:	Es tut mir leid zu hören, dass du deprimiert bist.
Person:	Das stimmt. Ich bin unglücklich.
Computer:	Denkst du, dass dein Kommen zu mir dir helfen wird, nicht unglücklich zu sein?
Person:	Ich brauche Hilfe, das scheint mir sicher.

Computer:	Was würde es für dich bedeuten, wenn du Hilfe bekommst?
Person:	Vielleicht könnte ich lernen, mit meiner Mutter auszukommen.
Computer:	Erzähl mir mehr über deine Familie. ...
Computer:	Was fällt dir sonst noch ein, wenn du an deinen Vater denkst?
Person:	Tyrann!
Computer:	Hat das etwas damit zu tun, dass dein Freund dir gesagt hat, dass du hierher kommen sollst? ...

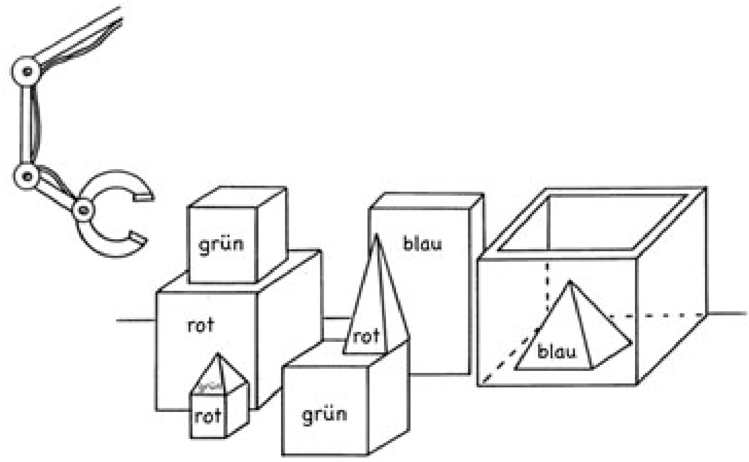
Ein weithin zitierter Vorfall, der vielleicht apokryph ist, aber nun in der Geschichte der künstlichen Intelligenz zu finden ist, ereignete sich als ein Vizepräsident (VP) für Computerverkäufe angeblich auf ein Terminal stieß, das normalerweise direkt mit dem Haus einer bestimmten Person verbunden war, aber diesmal das

„Psychotherapeuten"-Programm ausführte. Das Gespräch zeigt, was passiert ist. Weil der Vizepräsident offensichtlich Kontakt aufnehmen konnte, ist es klar, dass die Situation ihn prädisponiert hat zu glauben, dass er mit einer Person sprach. Hätte er etwas anderes vermutet, hätte er es bald bemerkt!

Ein anderes System, das in der Lage zu sein scheint, intelligente Gespräche zu führen, ist ein Programm namens „SHRDLU", das in den späten 60er Jahren entwickelt wurde und die Anweisungen annahm, Blöcke auf einem Tisch zu versetzen. Tatsächlich wurden die Blöcke und der Tisch simuliert und in Form eines Bildes auf einem Computerbildschirm dargestellt, obwohl es nicht zu schwierig gewesen wäre, die Dinge von einem echten Roboter durchführen zu lassen (zumindest im Prinzip). Das Bild zeigt die Mikrowelt des Roboters.

VP:	Denkst du, dass ich heute morgen den Computer benutzen kann?
Terminal:	Warum fragst du?
VP :	Ich könnte vielleicht zusätzliche Telekommunikationsverkäufe machen.
Terminal :	Warum bist du dir nicht sicher?
VP :	Meine potenziellen Kunden haben noch nie eine Vorführung des Systems gesehen.
Terminal :	Bedeutet das sehr viel für dich?
VP :	Natürlich tut es das.
Terminal :	Sie scheinen sehr positiv darüber zu sein.
VP :	Das ist lächerlich.
Terminal :	Was meinst du damit?

VP :	Gibt es einen Grund, warum ich den Computer jetzt nicht benutzen kann?
Terminal :	Erzähl mir mehr über deine potenziellen Kunden.
VP :	Bitte ruf mich an unter 491-1850
VP vergisst, einen Punkt einzugeben ... der Computer antwortet nicht ... VP wird so wütend, dass er die Person zu Hause anruft.	
VP:	Warum bist du so rotzfrech zu mir?
Person:	Was meinst du damit, warum ich rotzfrech zu dir bin?



SHRDLU konnte überraschend fließende Gespräche führen, wie im folgenden Dialog gezeigt wird. Dies zeigt unter anderem, wie es Befehlen gehorchen, Anweisungen vereindeutigen, den Bezug von Pronomen erarbeiten und neue Begriffe („Kirchturm“) verstehen kann.

Person:	Hebe einen großen roten Block auf.
Roboter:	Ok.
Das System antwortet mit “OK”, wenn es einen Befehl ausführt. Um den roten Block aufzuheben, musste er ihn abräumen, indem er einen Platz für den grünen Block fand und den grünen Block wegbewegte	
Person:	Fasse die Pyramide.
Roboter:	Ich weiß nicht, welche Pyramide du meinst.
Es gibt drei Pyramiden in der Szene, also macht das Programm nichts.	
Person:	Finde einen Block, der größer ist als der, den du in der Hand hältst, und lege ihn in die Schachtel.
Das System muss herausfinden, was mit “Eins” und “Es” gemeint ist, und anhand der Schlussfolgerung entscheiden, welchen Block es hält.	

Roboter:	Mit “Es” nehme ich an, du meinst den Block, der größer ist als der, den ich halte.

Gedruckt um uns auf dem Laufenden zu halten.

Roboter:	Ok.

Die Hand muss den roten Block ablegen, um den größeren blauen Block aufzunehmen.

Person:	Was enthält die Box?
Roboter:	Die blaue Pyramide und den blauen Block.
Person:	Wovon wird die Pyramide abgestützt?

Vorher antwortete das System auf “die Pyramide”, indem es sagte: “Ich weiß nicht, welche Pyramide du meinst.” Jetzt weiß es, dass es das eben Erwähnte bedeuten muss.

Roboter:	Die Box.
Person:	Hat ein Kirchturm ...
Roboter:	Entschuldigung, ich kenne das Wort „Kirchturm“ nicht.

Das System unterbricht sofort, wenn es ein Wort findet, das es nicht interpretieren kann.

Person:	Ein „Kirchturm“ ist ein Stapel, der zwei grüne Würfel und eine Pyramide enthält.

Die Anführungszeichen zeigen an, dass wir ein neues Wort definieren.

Roboter:	Ich verstehe.
Person:	Gibts dort Kirchtürme?
Roboter:	Nein.

Die neue Definition dient zur Beschreibung, um Kirchtürme zu erkennen.

Person:	Baue einen.
Roboter:	Ok.

Die in der Definition gegebene Beschreibung reicht aus, um einen Plan zum Aufbau neuer Objekte, sowie deren Erkennung abzuleiten. Das Wort “eins” bedeutet “ein Kirchturm”, und der Plan wird ausgeführt.

Das System ist jedoch sehr zerbrechlich und die Illusion, die es erzeugt, wird leicht zerstört.

Hier ist eine Fortsetzung der Konversation - die nicht wirklich vom Programm generiert wurde, aber sich bestimmt so hätte ergeben können. Obwohl es möglich war, den neuen Begriff „Kirchturm“ im letzten Gespräch zu definieren, kann nur eine sehr begrenzte Art von Begriffen beschrieben werden, da der Roboter eine extrem eingeschränkte „Intelligenz“ hat.

Person:	Tausche den großen roten Block gegen eine Wasserpistole aus.
Roboter:	Entschuldigung, ich kenne das Wort „Tausche“ nicht.
Person:	Ein „Tausch“ ist ein freier Wechsel von Eigentum.
Roboter:	Entschuldigung, ich kenne das Wort „frei“ nicht.
Person:	Eine „freie“ Handlung wird freiwillig und ohne Zwang ausgeführt.
Roboter:	Tut mir leid, ich kenne das Wort „Handlung“ nicht.
Person:	„Handlungen“ sind das, was Leute absichtlich und nicht zufällig tun.
Roboter:	Entschuldigung, ich kenne das Wort „Leute“ nicht.
Person:	Entschuldigung, ich dachte du wärst schlauer als du bist.
Roboter:	Entschuldigung, ich kenne das Wort „Entschuldigung“ nicht.

Letzten Endes muss der Roboter zugeben, dass er nicht einmal die Wörter versteht, die er selbst benutzt (Entschuldigung, ich kenne das Wort „Entschuldigung“ nicht)!

Betrachte nun eine alternative, völlig imaginäre Fortsetzung der Konversation, die möglicherweise von einem Schüler oder einer Schülerin erstellt wurde. Obwohl winzig, zeigt dieses Fragment eine Fülle von Weltwissen.

Person:	Tausche den großen roten Block gegen eine Wasserpistole aus.
Roboter:	Ich habe schon eine Wasserpistole, aber ich gebe dir zwei Blöcke und eine Pyramide für deinen schleimigen alten Frosch.

- Der „Roboter“ weiß, dass eine Wasserpistole weniger wertvoll ist, wenn man bereits eine besitzt.
- Außerdem erwartet er, dass die Person das auch weiß, da er sich nicht darum bemüht zu erklären, dass dies ein Grund für die Ablehnung des Angebots ist.
- Dennoch sieht er, dass die Person unbedingt einen Block will und bereit ist, sich von etwas Wichtigem zu trennen.
- Er sieht auch ein, dass - im Gegensatz zu Wasserpistolen - Blöcke in der Quantität wertvoller sind.
- Er versucht, die Person zu besänftigen, indem er den Frosch erniedrigt.
- Das bedeutet, dass er bereit ist zu feilschen.

Sicher ist dieser Grad an Kunstfertigkeit noch weit weg von den heutigen Computern!

Die Geschichte unten wurde von einem anderen Computerprogramm (Ende der 80er Jahre) generiert. Obwohl es durch seine Spärlichkeit und Kürze sofort als computergeneriert erkannt wird, ist es nicht schwer sich vorzustellen, wie es durch das Hinzufügen aller Arten von Details verfeinert werden könnte.

Interessant sind nicht die oberflächlichen Aspekte der Geschichte, sondern die Handlung, die sie verkörpert. Diese ist zwar weit entfernt von jeder vom Menschen erzeugten Handlung, aber sie scheint einige menschliche Konfliktelemente zu beinhalten. Heutzutage gibt es eine Reihe von Systemen zum automatischen Erstellen von Stories (Geschichten), obwohl die Herausforderung bei der Bewertung darin besteht zu bestimmen, wie viel Material nur Standardmuster mit zu füllenden Lücken ist, und wie umfangreich die Handlung ist, die wie oben kreativ aufgebaut wurde.

Es war einmal eine Küstenseeschwalbe namens Truman. Truman war obdachlos. Truman brauchte ein Nest. Er flog zum Ufer. Truman suchte nach einigen Zweigen. Truman fand keine Zweige. Er flog in die Tundra. Er traf einen Eisbären namens Horace. Truman fragte Horace, wo es Zweige gäbe. Horace verbarg die Zweige. Horace erzählte Truman, dass einige Zweige auf dem Eisberg waren. Truman flog zum Eisberg. Er suchte nach einigen Zweigen. Er fand keine Zweige. Horace suchte nach etwas Fleisch. Er hat etwas Fleisch gefunden. Er aß Truman. Truman ist gestorben.

Es gibt einen jährlichen Wettbewerb für den Loebner-Preis, bei dem Computerprogramme darum kämpfen, den Turing-Test zu bestehen, indem sie sich bei der Jury als Mensch vorgeben. Seit 2012 hat noch kein Computer die Gold- oder Silberpreise gewonnen, bei denen die Jurymitglieder ständig getäuscht worden sind, aber jedes Jahr wird ein Bronze-Preis für das 'menschlichste' der bewerteten Programme vergeben. Im ersten Jahr des Wettbewerbs (1991) gelang es einem Programm einen Bronze-Preis zu gewinnen, der unter anderem Tippfehler menschlich erscheinen ließ!

Es wurde kein künstliches Intelligenzsystem geschaffen, das den Turing-Test fast vollständig besteht. Selbst wenn man dies täte, haben viele PhilosophInnen behauptet, dass der Test nicht wirklich misst, was die meisten Menschen unter Intelligenz verstehen. Was er testet, ist die Verhaltensäquivalenz: Er soll herausfinden, ob ein bestimmtes Computerprogramm die Symptome des Intellekts aufweist, die möglicherweise nicht mit der wirklichen Intelligenz vergleichbar sind. Kannst du menschlich intelligent sein ohne dir darüber bewusst zu sein, dich selbst zu kennen, selbstbewusst zu sein, fähig zu sein, Selbstbewusstsein zu fühlen, Liebe zu erfahren, … lebendig zu sein?

Künstliche Intelligenz wird uns wahrscheinlich für viele weitere Jahrzehnte beschäftigen.

Weiterführende Literatur

Artificial intelligence: the very idea von dem Philosophen John Haugeland ist ein äußerst lesenswertes Buch über die Debatte betreffend künstliche Intelligenz, und ist die Quelle einiger der Illustrationen in dieser Aktivität (insbesondere der SHRDLU-Gespräche und der Diskussion darüber).

Der ursprüngliche Turing-Test wurde in einem Artikel mit dem Titel "Computing Machinery and Intelligence" von Alan Turing beschrieben, der 1950 in der philosophischen Zeitschrift Mind erschien und in dem von Feigenbaum und Feldman herausgegebenen Buch Computers and thought nachgedruckt wurde. Der Artikel enthielt die ersten beiden Gespräche.

Das Psychotherapeutenprogramm wurde in "ELIZA - A computer program for the study of natural language communication between man and machine " von J. Weizenbaum beschrieben, das 1966 in der Computerzeitschrift Communications of the Association for Computing Machinery veröffentlicht wurde.

Das Roboterprogramm 'blocks-world' wird in der Dissertation von Terry Winograd beschrieben, die als Buch mit dem Titel Understanding natural language (Academic Press, New York, 1972) veröffentlicht wurde.

Das Programm, das die Geschichte von Truman und Horace hervorgebracht hat, ist in "A planning mechanism for generating story text" von Tony Smith und Ian Witten beschrieben, das 1990 in den Proceedings of the 10th International Conference on Computing and the Humanities veröffentlicht wurde.

Contributors: Agata Ciabattoni, Stefan Szeider, Reinhard Pichler
Language editor: Elisa Di Cristo
Editor: Mihaela Rozman

Publisher: Projekt ADA - Algorithmen Denken Anders
Vienna Center for Logic and Algorithms
Institute for Logic and Computation
Technische Universität Wien

Image credits: CS UNPLUGGED; UNDER DESIGNATION * VCLA

Vienna Center for
Logic and Algorithms

FAKULTÄT
FÜR !NFORMATIK

Faculty of Informatics

Vienna Center for Logic and Algorithms
Institute for Logic and Computation
Technische Universität Wien
Favoritenstraße 9-11
A-1040 Vienna
Phone: +43 (0) 1 58801 184806
E-mail: office@vcla.at
Web: http://www.vcla.at
Facebook: @vclaTUwien
Twitter: @vclaTUwien
Web: http://www.vcla.at