a = 210 mm
90°
b = 297 mm

Mathematik und Kommunikation

Ob beim Telefonieren mit dem Handy, beim Geldabheben am Automaten oder beim Anhören einer CD – in der Kommunikation mit oder mit Hilfe von Maschinen erleichtern uns mathematische Anwendungen, oft unbemerkt, das Leben Tag für Tag. Vor rund 60 Jahren erforschte der amerikanische Mathematiker und Ingenieur Claude Elwood Shannon die wissenschaftliche Verbindung der beiden Disziplinen: Seine berühmte Theorie zur Kommunikation beruht auf Vorarbeiten seines Kollegen Norbert Wiener und ist noch heute maßgeblich, wenn man die Übertragung von Informationen untersuchen will. In dem später so genannten Shannon-Weaver-Modell wird die Information von einem Sender kodiert, auf einem Kanal übertragen, dabei mit einer gewissen Wahrscheinlichkeit – zum Beispiel durch Rauschen – gestört und schließlich vom Empfänger dekodiert.

Doch wie werden Daten dabei am besten verschlüsselt? Und wie können Störfaktoren bei der Übertragung klein gehalten werden? Antworten liefert hier die Kodierungstheorie, ein Teilgebiet der Mathematik, ohne das weder das Tsunami-Frühwarnsystem im Indischen Ozean funktionieren würde noch ein Telefon – ganz zu schweigen von den meisten Multimediaprodukten, die auf der Internationalen Funkausstellung zu sehen sind. Oft muss die Mathematik obendrein Datenmassen komprimieren, um diese zu bändigen. Auch diesen Vorgang ermöglichen die Algorithmen der Kodierungstheorie.

Ein anderes Teilgebiet der Mathematik hilft, die Informationen bei der Übertragung zu schützen. Dafür ist die Theorie der Verschlüsselung zuständig, die Kryptologie. Public-Key-Verfahren etwa – Standardverfahren zur Verschlüsselung – wurden von den Mathematikern Whitfield Diffie, Martin Hellman und Ralph Merkle zu Beginn der 1970er-Jahre erfunden. Einen Schritt weiter gingen 1977/78 die Mathematiker Ron Rivest, Adi Shamir und Leonard Adleman. Sie erdachten den nach den Anfangsbuchstaben ihrer Nachnamen benannten RSA-Algorithmus – das erste konkrete Verschlüsselungsverfahren und heute die Standardverschlüsselung beim Datenverkehr im Internet.

Mathematiker sind zu guter Letzt auch gefragt, wenn es um die so genannte Optimierung geht – etwa die Verteilung von Handyfunkstationen oder -frequenzen.

Am Anfang war der Fehler

Kommunikation ist mehr als nur Reden und Zuhören, Senden und Empfangen – Störungen gehören meist auch dazu. Das gilt für nahezu jede Form der Datenübertragung: vom Satelliten, der Informationen in Richtung Erde sendet, über den Computernutzer, der über WLAN surft, bis zu den Unterwassersonden

a = 210 mm
90°

des Tsunami-Frühwarnsystems, die ihre Daten mehrere Kilometer weit durch das Wasser schicken. Die entscheidende Frage ist hier, wie sich diese Fehler minimieren oder sogar vollständig beheben lassen.

Eine sehr einfache Idee besteht darin, die Daten zu kopieren und mehrmals zu senden. Das Problem: Dieses Verfahren ist nicht besonders effektiv. Wenn man Informationen zur Sicherheit gleich mehrmals übertragen will, dann bläht man die Menge der gesendeten Daten damit unnötig auf. Eine bessere Idee hatten die Mathematiker Irving S. Reed und Gustave Solomon. Sie entwickelten 1960 die Reed-Solomon-Kodierung, die heute unter anderem in DSL-Übertragungen und in DVD-Playern angewendet wird. Reed-Solomon-Codes korrigieren darüber hinaus Fehler in der Datenübertragung zu Satelliten, zum Beispiel beim Voyager-Programm, das an den Grenzen unseres Sonnensystems Daten sammelt. Die Voyager-Daten sind über einen halben Tag unterwegs, bis sie auf der Erde ankommen – viel Zeit, um durch den so genannten Sonnenwind mit seinen aufgeladenen Teilchen oder durch Magnetfelder gestört zu werden.

b = 297 mm

Funktionen als Fingerabdruck

Die Reed-Solomon-Kodierung nutzt Funktionen: Zu beliebigen Zahlen wird sehr schnell eine Art mathematischer Fingerabdruck bestimmt. Will man nun jemandem die Zahlen schicken, dann reicht es, ihm lediglich die Funktion zukommen zu lassen – denn damit kann der Empfänger die Zahlenreihe rekonstruieren. Die Datenmenge wird dabei zwar in der Regel kaum kleiner – tatsächlich wächst sie oft sogar geringfügig –, doch die Übertragung der Kennzahlen der Funktion anstelle der Zahlen selbst birgt einen großen Vorteil: Auch wenn die Funktion nicht komplett beim Empfänger ankommt, kann dieser sie aus den Bruchstücken eindeutig rekonstruieren – und damit die Zahlenreihe berechnen, die er eigentlich haben wollte.

Das ist in vielen Anwendungen hilfreich – etwa beim Hören von Musik-CDs. Denn selbst beim Lesen einer auf den ersten Blick kratzerfreien Scheibe können mehr als eine halbe Million Lesefehler auftreten. Wenn deutliche Kratzer dazukommen, dann gehen die Lesefehler in die Millionen. Obendrein treten sie gehäuft in so genannten „Bursts" auf. Gerade damit kommen die Reed-Solomon-Codes jedoch gut zurecht.

WLAN und GSM störungsfrei

Doch es gibt auch andere Fehlerkorrekturen, etwa das Viterbi-Verfahren, das Mitte der 1960er-Jahre der aus Italien stammende Mathematiker Andrew James Viterbi begründet hat. Es basiert auf der Wahrscheinlichkeitstheorie. Zunächst

ergänzt der Sender jedes Bit, das er verschicken will, durch weitere Bits. Die Datenpakete werden auf dem Weg zum Empfänger gestört – doch aufgrund der Ergänzungen kann der Empfänger mit Hilfe von Wahrscheinlichkeitstabellen abschätzen, welche Daten der Sender wohl abgeschickt hat. So ist es ihm möglich, mit einer gewissen Wahrscheinlichkeit auf die tatsächlich gesendete Bitfolge zu schließen.

Diese Fehlerkorrektur wird nicht nur in WLAN-Modems, bei den digitalen Rundfunkformaten DVB-T und DAB sowie beim Telefonieren mit GSM-Handys eingesetzt, sondern auch beim Tsunami-Frühwarnsystem: Hier kommunizieren Sonden, die Wasserdruck und Temperatur in bis zu 6.000 Meter Wassertiefe messen, über Unterwassermodems mit Bojen an der Oberfläche.

Doch nicht nur Viterbis Fehlerkorrektur hilft den Technikern bei der Übertragung von Daten. Mathematik spielt auch eine wichtige Rolle, wenn es darum geht, Daten auf Schallwellen aufzuprägen. Denn die Ingenieure können unter anderem zwischen den beiden folgenden Möglichkeiten wählen: Daten werden entweder als Töne verschickt – ähnlich wie beim Faxgerät – oder als Phasenverschiebungen auf feste Trägerfrequenzen aufgeprägt. Dabei haben die Ingenieure damit zu kämpfen, dass Wasser Schallwellen je nach Druck, Temperatur und Salzgehalt unterschiedlich schnell transportiert. Die korrekte Information lässt sich auch hier wieder dank mathematischer Formeln rekonstruieren.

Komprimierungen für MP3, JPG und HDTV

Mathematische Methoden helfen auch immer dann, wenn es gilt, Datenmengen zu reduzieren. Datenformate wie MP3 für Audiodaten – eine mathematische Entwicklung des Fraunhofer-Instituts für Integrierte Schaltungen (IIS) in Erlangen – und das Format JPG für Bildinformationen haben die Kommunikation in Ton und Bild revolutioniert und die Internetkommunikation in der heutigen Form möglich gemacht.

Selbst an Stellen, an denen man es nicht vermutet, werden Daten mit mathematischen Tricks komprimiert. Das kann sogar verlustfrei geschehen, denn es gibt Algorithmen, die es Empfängern ermöglichen, eine exakte Kopie des gesendeten Materials zu „entpacken" – und nicht nur Näherungen. Ein Beispiel ist der Huffman-Code, der in den 50er-Jahren vom amerikanischen Mathematiker David Albert Huffman entwickelt wurde. Dieses Kompressionsverfahren wird bei Faxgeräten oder bei hochauflösendem Fernsehen (HDTV) verwendet. Ein Teil der MP3-Komprimierung beruht ebenfalls darauf.

Die zu übertragenden Zahlen werden beim Huffman-Verfahren nach ihrer Häufigkeit in eine Art Baumstruktur einsortiert. Die Position im Baum liefert den „Namen" der Zahl, unter dem sie vom Sender kodiert und verschickt wird. Der Trick: Jeder der Code-Namen beginnt anders. Daher kann man bei der Übertragung auf „Trenner" zwischen den Buchstaben verzichten und verbraucht so minimal wenige Bits – die Zahlenreihe wird also sehr kurz kodiert.

Packen, Falten, Legen – Mathematik im Handy

Auch das gesprochene Wort im Handy benötigt Komprimierung, denn die digitalen Sprachdaten sind vergleichsweise umfangreich. In der Regel sind es 64 Kilobit, die pro Sekunde übertragen werden müssten – viel zu viel für ein handelsübliches GSM-Handy, dessen Funkkanal in der Regel für gerade einmal 9,6 Kilobit Sprachdaten ausgelegt ist. Zumal zusätzlich auch Informationen zur Identifikation des Telefons und Daten zur Fehlerkorrektur übertragen werden müssen.

Die digitalen Sprachdaten werden daher in kleine Abschnitte zerlegt und durch Filter geschickt, um zum Beispiel Sprachpausen zu registrieren und Vokale künstlich zu verkürzen. Anschließend werden die Daten in einer komplizierten Kodierung mit unterschiedlichen Verfahren gepackt, gleichsam gefaltet und in Zeitscheiben zerlegt, weil sich so mehrere Nutzer eine Empfangsantenne teilen können.

Beim Empfänger geht das Rechnen dann weiter: Falls zum Beispiel – trotz Tricks wie dem so genannten Frequenzhopping – ein Sprach-Datenpaket nicht mehr wiederherzustellen ist, dann schätzt das Empfängerhandy mit Hilfe von Wahrscheinlichkeitsrechnung, wie die Information gelautet haben könnte. Der Effekt: Die Lücken werden mit Hilfe von Mathematik so geschlossen, dass man sie kaum wahrnimmt.

Mehr Sicherheit am Geldautomaten

Nicht nur Störungen sind bei der Kommunikation unerwünscht, sondern in der Regel auch Mithörer oder -leser – besonders bei Finanztransaktionen oder im militärischen und diplomatischen Bereich. Informationen müssen daher verschlüsselt werden. Zuweilen dienen Schlüssel aber auch als eine Art Ausweis, der zum Beispiel sicherstellt, dass nur der Kontoinhaber am Geldautomaten Geld von seinem Konto abheben kann.

Ein Schlüssel der ersten Art wird zum Beispiel beim Handy genutzt: Hier werden vor der Übertragung alle teilnehmerbezogenen Daten mit Hilfe einer Binärzahl aus 64 Nullen und Einsen für Dritte unlesbar gemacht. Ein Schlüssel der zweiten

Art ist die PIN für die EC-Karte. Sie wird unter anderem mit dem DES-Verfahren erzeugt. DES steht für „Data Encryption Standard", eine Verschlüsselungsmethode, die von IBM und der US-amerikanischen „National Security Association" entwickelt wurde. Hierbei werden Kontonummern und andere Zahlen mit Hilfe eines 56 Bit langen Schlüssels, den nur die Bank kennt, durcheinandergewürfelt und komprimiert. Möchte ein Kunde Geld abheben, wird die eingegebene PIN vom Geldautomaten an die Bank übertragen. Dort wird mit Hilfe des geheimen Bankschlüssels und der Kontodaten die PIN berechnet und mit der eingegebenen Zahl verglichen – und nur, wenn beide übereinstimmen, gibt der Automat das Geld frei.

Ein anderes Verfahren, das bis zum Jahr 2000 unter Patentschutz stand, dient heute unter anderem der Verschlüsselung des Datenverkehrs im Internet: das Verschlüsselungsverfahren RSA.

Die Idee ist einfach: Salz und Zucker zusammenzuschütten, ist ein Kinderspiel, aber die Kristalle hinterher wieder auseinanderzusortieren, ist eine langwierige Arbeit. Auf die Mathematik übertragen bedeutet das: Die Erfinder des RSA-Algorithmus verwendeten zum Verschlüsseln eine Operation, die man leicht in eine Richtung durchführen kann, aber nur sehr schwer in die umgekehrte: die Primfaktorzerlegung. Ein Beispiel: Die Primzahlen 3, 31 und 1.381 sind schnell miteinander multipliziert, das Ergebnis ist 128.433. Aber in welche Primfaktoren zerfällt die Zahl 1.221.162? Noch immer gibt es kein effektives Verfahren, das die Primfaktoren großer Zahlen mit einigen hundert Dezimalstellen schnell bestimmt.

Wird nun ein Text mit Hilfe von RSA verschlüsselt, werden zwei große Primzahlen gesucht und als für alle zugänglicher Schlüssel veröffentlicht. In diesen Code geht das Produkt dieser beiden Primzahlen ein. Zum Entschlüsseln des Textes wird jedoch wiederum ein privater Schlüssel benötigt, in dem die Informationen über die beiden Primfaktoren enthalten sind – diese bleiben natürlich geheim.

Derartige Verschlüsselungstechniken beruhen zum Teil auf über 150 Jahre altem mathematischem Wissen. Es geht auf den Mathematiker Evariste Galois zurück, einen französischen Revolutionär, der unter abenteuerlichen Bedingungen seine ersten Ideen zur Gruppentheorie aufschrieb.

Chiffren und Algorithmen auf dem Prüfstand

Mathematiker interessieren sich auch für die Frage, *wie sicher* eine Chiffriermethode ist. Bei RSA ergibt sich entsprechend die Fragestellung, wie schnell man Zahlen in Faktoren zerlegen kann. Damit beschäftigt sich zum Beispiel das Team um Jens Franke und Thorsten Kleinjung an der Universität

Bonn, die derzeitigen Weltrekordhalter in Fragen der Faktorisierung. Mit Hilfe ausgefeilter Tricks und Algorithmen faktorisierten sie in monatelanger Arbeit zum Beispiel die Zahl 2^{1039}-1, eine Zahl mit 139 Dezimalstellen. Ihr derzeit bestes Ergebnis ist aber eine Zahl mit 200 Stellen, deren zwei Primfaktoren sie 2005 nach mehreren Jahren Arbeit berechnen konnten.

Andere Forscher kümmern sich um die Frage, wie sicher der DES-Algorithmus für die Nutzung von EC-Karten ist. Im März 2007 etwa verkündete ein Team um Christof Paar und Manfred Schimmler an den Universitäten Kiel und Bochum, mit einer speziellen Rechnerarchitektur könne man den DES-Schlüssel innerhalb von sechseinhalb Tagen knacken. Das Team hatte dazu eigens einen speziellen kleinen Rechner gebaut, den es „Copacobana" nannte (die Abkürzung steht für „Cost-Optimized Parallel Code Breaker"). Copacobana arbeitet mit „brute force", das heißt, der Rechner probiert einfach alle möglichen 2^{56} Schlüssel aus. Hierfür arbeiten die 120 Prozessoren von Copacobana parallel – jeder Prozessor testet pro Sekunde 400 Schlüssel.

Optimierung für die Kommunikation von morgen

Mathematiker ermöglichen aber auch auf ganz andere Weise, dass die zwischenmenschliche Kommunikation störungsfrei verläuft. Mobilfunkanbieter etwa sind daran interessiert, die knappen und teuren Mobilfunkfrequenzen möglichst effektiv nutzen zu können. Das Problem hierbei: Sendemasten, die mit derselben Frequenz Daten übertragen, können sich gegenseitig stören. Durch eine optimale Aufstellung der Masten kann man diese Störungen verringern – und braucht dabei auch weiterhin nur wenige Frequenzen zu verwenden. Zudem ist der Betrieb hierarchisch gegliedert: Sendemasten werden in Gruppen verwaltet, mehrere dieser Gruppen werden zusammen jeweils einer Vermittlungszentrale zugeordnet, welche die Telefongespräche weiterleitet. Wissenschaftler untersuchen hierbei, wie man diese Aufteilung möglichst ökonomisch gestaltet, sodass zum Beispiel nur kurze Verbindungen und wenige Vermittlungszentralen nötig sind.

Mit Fragen der Optimierung beschäftigen sich auch die Mathematiker am Zuse-Institut in Berlin. Durch geschickte Frequenzzuweisung ist es ihnen gelungen, bei einem Mobilfunkanbieter Störungen deutlich zu verringern.
Ein anderes Projekt verfolgt der Professor für Mobilfunkkommunikation und Leibniz-Preisträger 2008, Holger Boche, am Heinrich-Hertz-Institut des Berliner Fraunhofer-Instituts für Nachrichtentechnik und zeitgleich an der Technischen Universität Berlin. Boche beschäftigt sich als Mathematiker unter anderem damit, wie man in innovativen Mehrantennensystemen die Ressourcen optimal auf alle Nutzer verteilt. Ziel des Projekts ist es, die Effektivität des Mobilfunknetzes bis 2010 deutlich zu steigern – denn der Bedarf wird bis dahin nach vorsichtigen

Schätzungen ungefähr um den Faktor 10 anwachsen. Für die moderne Breitband-Mobilkommunikation ist das eine spannende und zugleich herausfordernde Aufgabe. Dank der Mathematik ist diese auch lösbar.

Ansprechpartner

Verlustfreie Kompression
Prof. Dr. Thomas Borys
PH Karlsruhe
0721/925-4277
Thomas.Borys@ph-karlsruhe.de

Kompression von Ton- und Bilddaten
Marc Briele
Fraunhofer-Institut für Integrierte Schaltungen
09131/776-0
marc.briele@iis.fraunhofer.de

Verschlüsselungsverfahren
Prof. Dr. Albrecht Beutelspacher
0641/99-32080
albrecht.beutelspacher@math.uni-giessen.de

Prof. Dr.-Ing. Christof Paar
Ruhr-Universität Bochum
0234/32-29944
cpaar@crypto.ruhr-uni-bochum.de

Prof. Dr. Manfred Schimmler
Christian-Albrechts-Universität Kiel
0431/880-4480
masch@informatik.uni-kiel.de

Faktorisierung
Professor Dr. Jens Franke
Mathematisches Institut der Universität Bonn
0228/73-2952
franke@math.uni-bonn.de

Mobilfunkkommunikation
Prof. Dr.-Ing. Dr. Holger Boche
holger.boche@mk.tu-berlin.de
030/314-28459

Dr. Andreas Eisenblätter
Zuse-Institut Berlin
eisenblaetter@zib.de
030/84185-284

Komprimierungsverfahren
Dr. Bernhard Grill
Fraunhofer-Institut für Integrierte Schaltungen IIS
09131/776-0
amm-info@iis.fraunhofer.de

Mehr erfahren Sie auch unter: www.jahr-der-mathematik.de

Der Abdruck ist honorarfrei. Ein Belegexemplar wird erbeten.
Für weitere Informationen wenden Sie sich bitte an:

Redaktionsbüro Jahr der Mathematik

Steffi Würzig
Friedrichstr. 78
10117 Berlin
T. 030/70 01 86-797
F. 030/70 01 86-909
wuerzig@jahr-der-mathematik.de
www.jahr-der-mathematik.de

Julia Kranz
Friedrichstr. 78
10117 Berlin
T. 030/70 01 86-741
F. 030/70 01 86-810
kranz@jahr-der-mathematik.de
www.jahr-der-mathematik.de

Wissenschaftsjahr 2008
Mathematik
Alles, was zählt