

Digitalisierung und Programmierung

Vorlesungsskript

Prof. Dr. Nicolas Meseth

21. Februar 2025

Inhaltsverzeichnis

| | |
|------------------------------------------------------------------------------------|-----------|
| 1. Bevor es losgeht | 6 |
| Bevor es losgeht | 7 |
| 1.1. Warum dieses Buch? | 7 |
| 1.2. Wen möchte ich wie ansprechen? | 7 |
| 1.3. Wie ist das Buch aufgebaut? | 8 |
| 1.4. Wie sollte man dieses Buch lesen? | 9 |
| 2. Das LiFi-Projekt | 10 |
| 2.1. Worum geht es im LiFi-Projekt? | 10 |
| 2.2. Was sind die Ziele? | 10 |
| 2.2.1. Informationen aus der Umwelt erfassen | 10 |
| 2.2.2. Informationen für automatisierte Entscheidungen nutzen | 11 |
| 2.2.3. Informationen über Licht kommunizieren und empfangen | 11 |
| 2.3. Wie gehen wir vor? | 11 |
| 3. Setup für das LiFi-Projekt | 12 |
| 3.1. Welche Hardware benötigen wir? | 12 |
| 3.2. Welche Software müssen wir installieren? | 12 |
| I. Probleme | 13 |
| 4. Problemlösung | 14 |
| 4.1. Das Eingabe-Verarbeitung-Ausgabe-Modell | 14 |
| 4.1.1. Taschenrechner | 16 |
| 4.1.2. Pflanzen zählen | 17 |
| 4.1.3. Schach spielen | 18 |
| 4.1.4. Mit Computern chatten | 20 |
| 4.2. Die Lösung des Problems | 21 |
| 4.3. Problemlösungsstrategien | 22 |
| 4.3.1. Problemzerlegung (<i>Problem Decomposition</i>) | 22 |
| 4.3.2. Teile und Herrsche (<i>Divide and Conquer</i>) | 23 |
| 4.3.3. Verteile und Parallelisiere (<i>Distribute and Parallelize</i>) | 24 |
| 4.4. Warum nutzen wir Computer? | 27 |

| | |
|--------------------------------------------------------------|---------------|
| 5. Algorithmen | 28 |
| 5.1. Zusammenfassung | 28 |
| 5.2. Was ist ein Algorithmus? | 28 |
| 5.2.1. Herkunft des Begriffs | 28 |
| 5.2.2. Algorithmen und Programme | 29 |
| 5.3. Kategorien | 29 |
| 5.3.1. Mathematische Algorithmen | 30 |
| 5.3.2. Suchalgorithmen | 32 |
| 5.3.3. Sortieralgorithmen | 32 |
| 5.3.4. Optimierungsalgorithmen | 32 |
| 5.3.5. Graphenalgorithmen | 32 |
| 5.3.6. Stochastische Algorithmen | 32 |
| 5.3.7. Maschinelle Lernalgorithmen | 32 |
| 5.4. Iteration und Rekursion | 32 |
| II. Repräsentation | 33 |
| 6. Informationen | 34 |
| 6.1. Information in der Informatik | 34 |
| 6.1.1. Zahlenraten | 35 |
| 6.1.2. Bit für Bit | 35 |
| 6.1.3. Unsicherheit | 38 |
| 6.1.4. Information | 39 |
| 6.1.5. Unwahrscheinliche Antworten | 40 |
| 6.1.6. Mehr als zwei Antworten | 42 |
| 6.2. Daten repräsentieren Information | 42 |
| 7. Bits | 43 |
| 7.1. Ist das Bit die kleinste Informationseinheit? | 43 |
| 7.2. Was ist ein Byte | 43 |
| 8. Codesysteme | 44 |
| 8.1. ASCII-Code | 44 |
| 8.2. Verallgemeinerung von Codesystemen | 44 |
| 8.3. Unicode | 44 |
| 8.4. RGB-Code | 44 |
| 8.5. Code vs Codec | 44 |
| 9. Datenstrukturen | 45 |
| 9.1. Listen | 45 |
| 9.2. Mengen | 45 |
| 9.3. Graphen | 45 |

| | |
|-----------------------------------------------------------------------------------|-----------|
| 9.4. Bäume | 45 |
| 9.5. Warteschlangen | 45 |
| III. Verarbeitung | 46 |
| 10. Analog vs. Digital | 47 |
| 10.1. Was ist der Unterschied zwischen der analogen und digitalen Welt? | 47 |
| 10.1.1. Endlich viele Möglichkeiten vs. Unendlichkeit | 47 |
| 10.1.2. Diskrete und kontinuierliche Werte | 47 |
| 11. Speicher | 48 |
| 11.1. Substratunabhängigkeit | 48 |
| 12. Logik und Arithmetik | 49 |
| 12.1. Schalter | 49 |
| 12.1.1. Relais, Vakuumröhren und Transistoren | 49 |
| 12.2. Logikgatter | 49 |
| 12.3. Binäre Addition | 49 |
| 12.4. Binäre Subtraktion | 49 |
| 12.5. Substratunabhängigkeit | 49 |
| 13. Computer | 50 |
| 13.1. Komponenten eines Computers | 50 |
| IV. Kommunikation | 51 |
| 14. Signale | 52 |
| 14.1. Was ist ein Signal? | 52 |
| 14.1.1. Der Kern ist die Veränderung | 52 |
| 14.1.2. Häufig elektrisch | 52 |
| 14.2. Wie können wir Signale erzeugen? | 53 |
| 14.2.1. Von digital zu analog | 53 |
| 14.2.2. Die LED | 53 |
| 14.3. Wie können wir Signale empfangen? | 53 |
| 14.3.1. Von analog zu digital | 53 |
| 14.3.2. Der Farbsensor | 53 |
| 14.4. Welche Bedeutung hat ein Signal? | 53 |
| 15. Protokolle | 54 |
| 15.1. Peer-To-Peer | 54 |
| 15.2. Handshake | 54 |
| 15.3. TCP/IP & HTTPs | 54 |

| | |
|----------------------------------------------|-----------|
| 16. Verschlüsselung | 55 |
| 16.1. Verschlüsselung | 55 |
| 16.1.1. Symmetrisch | 55 |
| 16.1.2. Asymmetrisch | 55 |
| 16.2. Digitale Signaturen | 55 |
| 17. Kompression | 56 |
| 17.1. Verlustfreie Kompression | 56 |
| 17.2. Verlustbehaftete Kompression | 56 |
| Literaturverzeichnis | 57 |

1. Bevor es losgeht

Bevor es losgeht

1.1. Warum dieses Buch?

Dieses Buch entstand aus der Erkenntnis, dass viele klassische Lehrbücher der Informatik für Anfänger oft zu technisch und abstrakt sind. In meiner langjährigen Lehrtätigkeit habe ich beobachtet, dass Studierende besonders dann erfolgreich lernen, wenn sie die Konzepte der Informatik in einem praktischen Kontext erleben können. Deshalb habe ich mich entschieden, einen praxisorientierten Ansatz zu wählen, der theoretische Grundlagen mit einem konkreten Projekt verbindet.

1.2. Wen möchte ich wie ansprechen?

Ich richte dieses Buch an Menschen ohne Vorkenntnisse in den Bereichen Digitalisierung, Computertechnik oder Programmierung. Ich gehe nicht davon aus, dass die Leserinnen und Leser eine besondere Motivation mitbringen, sich mit diesen Themen zu beschäftigen. Wenn doch, umso besser. Diese beiden Annahmen – fehlende Vorkenntnisse und Motivation – treffen auf den Großteil meiner Studierenden zu, für die ich dieses Buch in erster Linie geschrieben habe.

Mein Ziel ist es, sowohl die Kenntnisse als auch die Begeisterung für die Informatik zu steigern – zumindest bei einigen, die dieses Buch zur Hand nehmen (müssen). Um dies zu erreichen, habe ich mich entschieden, einen anderen Weg einzuschlagen als klassische Informatik-Lehrbücher:

- Ich verwende bewusst eine **einfache Sprache**. Das heißt nicht, dass wir keine Fachbegriffe einführen werden. Wir erklären die Sachverhalte aber zunächst in einer für alle Studierenden verständlichen Sprache und führen Fachbegriffe schrittweise ein.
- Neben der Sprache knüpfe ich bei den Beispielen gezielt an bestehendes Wissen an. Ich verwende **Beispiele und Analogien aus dem Alltag**, um Ideen und Konzepte der Informatik zu veranschaulichen. Das mag nicht immer perfekt gelingen – aber wenn es gelingt, hilft es meiner Erfahrung nach dabei, neue Themen besser zu verstehen.
- Mein Fokus liegt auf dem **Verständnis** der Konzepte statt auf technischen Details. Ich verzichte bewusst auf zu viel Tiefe zugunsten eines zugänglichen Buches, das einen guten Überblick vermittelt und echtes Verständnis ermöglicht. Wer anschließend Lust auf mehr Tiefe hat, bekommt von mir in jedem Kapitel Leseempfehlungen an die Hand.

- Ich bin überzeugt, dass konkrete Projekte das Interesse und Verständnis am besten fördern. Dieses Buch verbindet das **LiFi-Projekt** mit den theoretischen Grundlagen der Informatik und führt Schritt für Schritt an algorithmisches Denken und Programmierung heran. Das Ergebnis ist ein fertiges Produkt, für das die Leserinnen und Leser alle erlernten Kenntnisse praktisch anwenden mussten – ganz nach dem Prinzip „Learning by Doing“.
- Mir ist bewusst, dass viele der jüngeren Generation das Lesen eines Buches als Herausforderung empfinden. Dennoch halte ich Bücher für unverzichtbar, um komplexe Themengebiete zu erschließen. Um den Leseprozess zu erleichtern, stelle ich ergänzende **Videos und Audioaufnahmen** bereit, die in den Kapiteln verlinkt und über QR-Codes zugänglich sind.

1.3. Wie ist das Buch aufgebaut?

Dieses Buch befasst sich mit der Frage, wie wir Computer zum Lösen von Problemen einsetzen können. Das Schaubild in Abbildung 1.1 visualisiert die wichtigsten Themenblöcke.

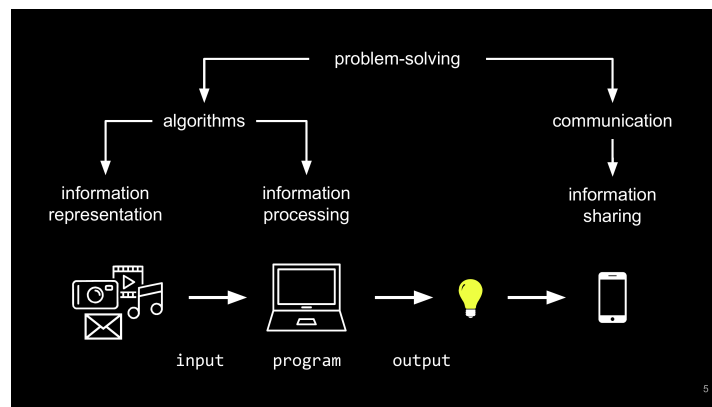


Abbildung 1.1.: Überblick über die Themenblöcke dieses Buches.

Ich orientiere mich übergeordnet an dem Thema des Problemlösens (*problem-solving*), das sich in zwei Bereiche gliedert:

1. **Algorithmen** (*algorithms*) bilden den Kern des Problemlösens und der Informatik. Sie beschreiben die notwendigen Schritte zur Lösung eines Problems.
2. **Kommunikation** (*communication*) umfasst das Teilen von Informationen in Computernetzwerken. Mit der weiten Verbreitung des Internets ist dieser Aspekt zentral für die moderne Computernutzung geworden. Lösungen, die ein Computer erzeugt, können heute unmittelbar über Netzwerke weltweit geteilt werden.

Im Bereich der Algorithmen beschäftigen wir uns zunächst damit, wie wir Probleme für Computer verständlich und lösbar beschreiben können. Eine zentrale Rolle spielt dabei die **Informationsrepräsentation** (*information representation*): Wie können wir Zahlen, Texte, Bilder, Videos, Audioaufnahmen und andere wichtige Inhalte so darstellen, dass ein Computer damit arbeiten kann?

Nachdem wir das verstanden haben, widmen wir uns der **Informationsverarbeitung** (*information processing*) – also der Frage, wie Eingabeinformationen so verarbeitet werden können, dass eine Lösung entsteht. Dies ist die Kernaufgabe der Algorithmen, und wir untersuchen, wie ein Algorithmus sowohl für Menschen als auch für Computer verständlich dargestellt werden kann. Dabei lernen wir die Programmiersprache Python kennen, die als moderne Programmiersprache Algorithmen in ausführbare **Programme** (*programs*) übersetzt. Anhand einfacher Beispiele wie der Addition zweier Zahlen verstehen wir zudem, wie die Ausführung von Programmierbefehlen im Rechner auf der Ebene der Bits funktioniert.

Bei der Kommunikation stellen wir uns die Frage, wie **das Teilen von Informationen** (*information sharing*) über unterschiedliche Medien wie Kabel, Luft oder Licht funktioniert. Wir lernen dabei etwas über das Senden und Empfangen von Signalen, über Protokolle – also Vereinbarungen zur Informationsübermittlung – sowie über die Frage, wie wir unsere Kommunikation effizient und gleichzeitig sicher gestalten können.

1.4. Wie sollte man dieses Buch lesen?

Das Buch ist für eine lineare Lektüre von vorne nach hinten konzipiert. An der Hochschule Osnabrück behandeln wir in der zugehörigen Veranstaltung pro Woche ein Kapitel – gelegentlich auch zwei, abhängig von der Verteilung der Feiertage im Semester. Die Kapitel hängen zusammen und bauen teilweise aufeinander auf.

Wie beschrieben orientiert sich dieses Buch an der Durchführung eines Projekts – dem LiFi-Projekt. Das Projekt bildet den Ausgangspunkt jedes Kapitels, und für jedes Thema wird der praktische Bezug zum Projekt hergestellt. Was genau das LiFi-Projekt beinhaltet, schauen wir uns im nächsten Kapitel an.

2. Das LiFi-Projekt

2.1. Worum geht es im LiFi-Projekt?

LiFi ist eine Technologie, die die Übertragung von Informationen mithilfe von Licht ermöglicht. Sie nutzt das sichtbare Lichtspektrum, um ein Signal zu erzeugen, das von einem Fotodetektor empfangen werden kann, welcher das von einer LED ausgestrahlte Licht erfasst. Durch die Veränderung der Lichteigenschaften über die Zeit, wie etwa der Wellenlänge oder der Helligkeit, können wir Daten kodieren und übertragen. LiFi bietet großes Potenzial für den Einsatz in Umgebungen, in denen Hochfrequenzsignale Mikroorganismen oder andere empfindliche elektronische Geräte stören könnten. Darüber hinaus könnte LiFi im Gegensatz zu Bluetooth oder WiFi in Robotern eingesetzt werden, die unter Wasser arbeiten.

Als Teil eines interdisziplinären F&E-Teams in einem Hightech-Unternehmen, das Roboter für Lebensmittel- und Landwirtschaftsanwendungen entwickelt, besteht deine Aufgabe darin, ein LiFi-Kommunikationsgerät zu entwickeln, das in die nächste Robotergeneration des Unternehmens integriert werden kann. Das Gerät hat zwei Hauptkomponenten: eine kleine LED, die in etwa 16 Millionen Farben des RGB-Farbsystems leuchten kann, und einen Farbsensor, der die Intensität der drei RGB-Farbkanäle sowie die Helligkeit des Lichts messen kann. Diese Komponenten werden von einem Master Brick gesteuert, der für die reibungslose Kommunikation zwischen dem Roboter und seinen Peripheriegeräten verantwortlich ist.

[BILD]

2.2. Was sind die Ziele?

Das LiFi-Projekt stellt ein klassisches Ingenieursproblem dar: die Kombination von Hardware und Software zur Lösung einer praktischen Aufgabe. Die zentralen inhaltlichen Fragen dieses Projekts lauten:

2.2.1. Informationen aus der Umwelt erfassen

- **Wie können physikalische Größen digital erfasst werden?** (*Informationen, Bits, Analog vs. Digital, Codesysteme*)

2.2.2. Informationen für automatisierte Entscheidungen nutzen

- Wie können Algorithmen Entscheidungen auf Basis von Eingabedaten treffen? (*Algorithmen*)

2.2.3. Informationen über Licht kommunizieren und empfangen

- Wie kann Licht Informationen darstellen? (*Information Representation*)
- Wie können mithilfe einer LED und eines Farbsensors Informationen übertragen? (*Information Communication*)
- Welches Protokoll eignet sich am besten für die LED-basierte Datenübertragung?
- Wie verlässlich ist die Datenübertragung? (*Protokolle*)
- Welche maximale Übertragungsdistanz ist möglich? (*Signale*)
- Welche Umgebungsbedingungen sind für eine erfolgreiche Übertragung erforderlich? (*Signale*)
- Wie lässt sich die Datenübertragung sicher gestalten? (*Algorithmen, Verschlüsselung*)
- Welche Datenübertragungsrate können wir erreichen? (*Algorithmen, Kompression*)

Eine wesentliche Einschränkung besteht darin, dass wir diese Fragen nur mit der verfügbaren Hardware beantworten können: einer LED und einem Farbsensor.

Am Ende dieses Projekts wirst du nicht nur das Ingenieursproblem gelöst haben, sondern auch Antworten auf alle genannten Fragen gefunden haben. Als zusätzlicher Bonus erwirbst du dabei tiefere Einblicke in die digitale Welt und grundlegende Programmierkenntnisse.

2.3. Wie gehen wir vor?

3. Setup für das LiFi-Projekt

3.1. Welche Hardware benötigen wir?

3.2. Welche Software müssen wir installieren?

Teil I.

Probleme

4. Problemlösung

Das LiFi-Projekt stellt eine komplexe Herausforderung dar. Beim Lesen der Ziele und Fragestellungen in Kapitel 2 kann man sich überfordert fühlen. Die zentrale Frage lautet: Wie nähern wir uns dieser Aufgabe systematisch an?

Ein bewährter Ansatz für komplexe Situationen ist die Vereinfachung. Auch wenn wir das Problem selbst nicht vereinfachen können, können wir es durch eine strukturierte Herangehensweise besser verstehen und handhabbarer machen. Die Verwendung von Modellen ist dafür ein geeigneter Weg.

Modelle zielen darauf ab, die wesentlichen Aspekte der realen Welt hervorzuheben und unwichtige Details auszublenden. Da dies zunächst abstrakt klingen mag, werden wir es anhand eines Modells veranschaulichen, das uns durch das gesamte Buch begleiten wird: das Eingabe-Verarbeitung-Ausgabe-Modell, kurz EVA-Modell.

4.1. Das Eingabe-Verarbeitung-Ausgabe-Modell

Das Eingabe-Verarbeitung-Ausgabe-Modell (EVA-Modell, s. Abbildung 4.1) ist ein wichtiges Modell in der Informatik. Es erklärt die Arbeitsweise von Computern auf vereinfachte Weise und beinhaltet nur die nötigsten Elemente. Konkret zeigt das Modell, wie Computer Probleme lösen und welche drei Elemente wir dabei betrachten müssen: Computer benötigen **(1) Eingabedaten**, die sie durch einen definierten **(2) Verarbeitungsprozess** in gewünschte **(3) Ausgabedaten** umwandeln.

Das EVA-Modell beschreibt ein Problem und dessen Lösung durch drei Komponenten: die Eingabe (*Input*), die der Computer erhält, die Verarbeitung (*Computation*), die er mit diesen Daten durchführt, und die Ausgabe (*Output*), die er als Ergebnis liefert. Wenn wir diese drei Komponenten beschreiben können, haben wir die für den Computer relevanten Aspekte des Problems erfasst – alles andere ist unwichtig.

Wenden wir das EVA-Modell auf das LiFi-Projekt an. Das LiFi-Gerät soll verschiedene Daten erfassen: Lichtsignale von einem anderen LiFi-Gerät und die Temperatur des eigenen Sensors. Basierend auf diesen Daten trifft es eine Entscheidung. Anschließend kommuniziert es diese Entscheidung zusammen mit den erfassten Temperaturdaten über Lichtsignale an das nächste

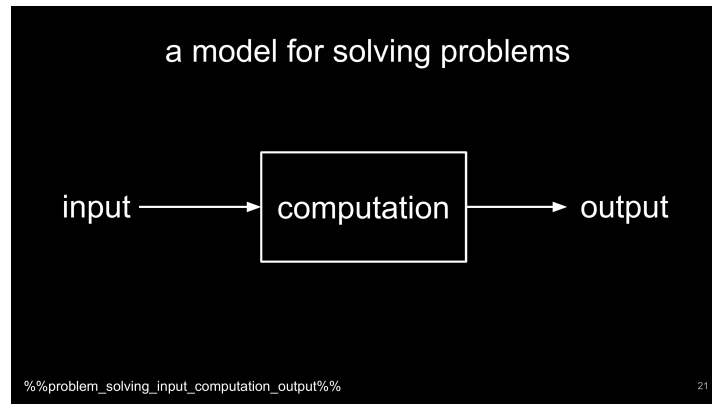


Abbildung 4.1.: Das EVA-Modell besteht aus der Eingabe, der Berechnung und der Ausgabe.

Gerät. Zwar ist jeder dieser Teilschritte für sich genommen komplex und erfordert eine eigene Lösung. Dennoch können wir das EVA-Modell nutzen, um das LiFi-Projekt als Ganzes darzustellen, indem wir von den Details der einzelnen Schritte abstrahieren:

[BILD LIFI-PROJEKT IM EVA MODELL]

Was haben wir nun dadurch gewonnen, dass wir das EVA-Modell angewendet haben? Wir können uns nun auf die einzelnen Elemente konzentrieren und diese getrennt voneinander betrachten. Damit zerlegen wir das große, überfordernde Problem in kleinere Teile und machen es dadurch besser beherrschbar.

Bei den Eingaben müssen wir uns fragen, wie diese konkret aussehen und erfasst werden. Dabei geht es vor allem darum, in welcher Form die Eingaben dem Computer vorliegen müssen, damit er sie verarbeiten kann. Wie werden Lichtsignale im Computer dargestellt? Wie wird die physikalische Größe der Umgebungstemperatur in eine computerverständliche Form umgewandelt, und wie sieht diese aus? Es geht also um die **Repräsentation von Informationen**.

Sobald wir die Darstellung der Eingaben geklärt haben, können wir diese als Grundlage für die Verarbeitung nutzen. Wie muss ein Programm aussehen, das auf Basis der Eingabedaten die richtige Entscheidung trifft? Welche Schritte sind notwendig? Welche Prüfungen muss das Programm durchführen? Bei diesem Schritt geht es folglich um die **Verarbeitung von Informationen**.

Schließlich müssen wir die Form der Ausgabe festlegen. Wie soll das Verarbeitungsergebnis konkret aussehen? Da wir für die Kommunikation wieder Lichtsignale verwenden, geht es auch bei der Ausgabe um die **Repräsentation von Informationen**.

Wir können die Perspektive auf eine LiFi-Gerät-übergreifende Sicht erweitern. Dann kommt neben der Repräsentation von Informationen ein weiterer Aspekt hinzu: Die **Kommunikation von Informationen**. Wie übertragen wir die Informationen, die das erste LiFi-Gerät erzeugt zum nächsten?

Vielleicht ist dir aufgefallen, dass die Struktur des gesamten Buches an den gerade identifizierten, übergeordneten Problemstellungen ausgerichtet ist. Wir befinden uns gerade im ersten Teil und sprechen darüber, wie wir Probleme im Computer darstellen. Im zweiten Teil des Buches lernen wir, wie Computer ganz unterschiedliche Informationen repräsentieren können, damit sie für die Lösung des Problems verwendet werden können. Im dritten Teil beschäftigen wir uns damit, wie Computer Informationen verarbeiten. Der vierte und letzte Teil führt uns in wichtige Konzepte der Kommunikation mithilfe von Computern und Netzwerken ein.

4.1.1. Taschenrechner

Am Beispiel eines Taschenrechner lässt sich das EVA-Modell gut darstellen. Wir können uns bildlich vorstellen, wie ein Mensch die Eingabe tätigt und danach das Ergebnis abliest. Es ist wichtig zu verstehen, dass Eingabe und Ausgabe sehr unterschiedliche Formen annehmen können und keinesfalls nur über eine Tastatur erfolgen müssen.

Das Beispiel des Taschenrechners wird in Abbildung 4.2 anhand einer einfachen Addition zweier Zahlen konkreter verdeutlicht. Als Eingabe werden zwei Zahlen benötigt, die Berechnung erfolgt durch eine Addition, dargestellt durch das Plusymbol. Die Ausgabe ist das Ergebnis – die Summe.

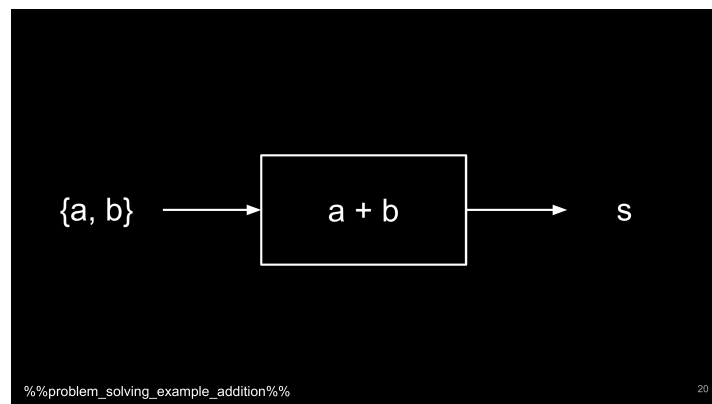


Abbildung 4.2.: Das EVA-Modell für die Addition zweier Zahlen.

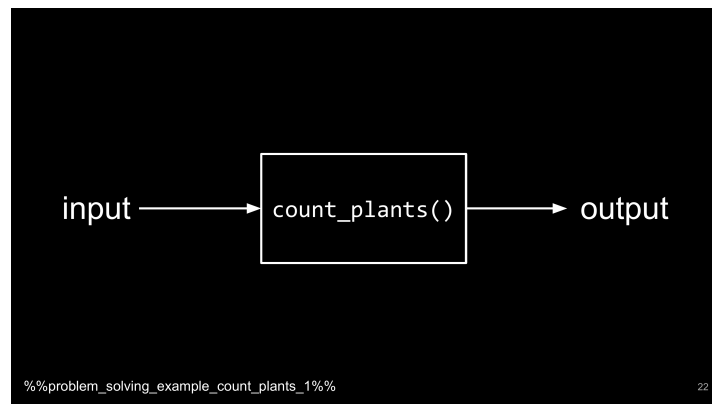
Dieses einfache Beispiel zeigt, dass wir verstehen müssen, wie Computer die drei Bestandteile des EVA-Modells umsetzen. Beim Taschenrechner sind Ein- und Ausgabe jeweils Zahlen. Diese Daten speichert der Computer in seinem Arbeitsspeicher. Dabei ist wichtig zu wissen, dass Computer auf der untersten Ebene ausschließlich Nullen und Einsen speichern. Wir müssen also verstehen, wie Computer Zahlen mithilfe dieser Binärzahlen darstellen können.

Was passiert bei der Berechnung in der Mitte des Modells? Eine Addition mag uns einfach erscheinen, doch auch hier müssen wir beachten, dass Computer mit Binärzahlen arbeiten. Es stellt sich also die Frage: Wie funktioniert eine Addition, wenn die Zahlen als Folge von

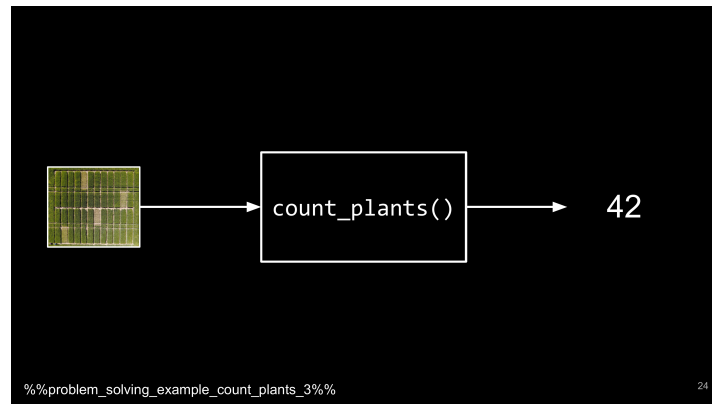
Nullen und Einsen dargestellt sind? Auf die beiden Fragen zur **Repräsentation und der Verarbeitung von Informationen** im binären System werden wir im Laufe des Buches Antworten bekommen.

4.1.2. Pflanzen zählen

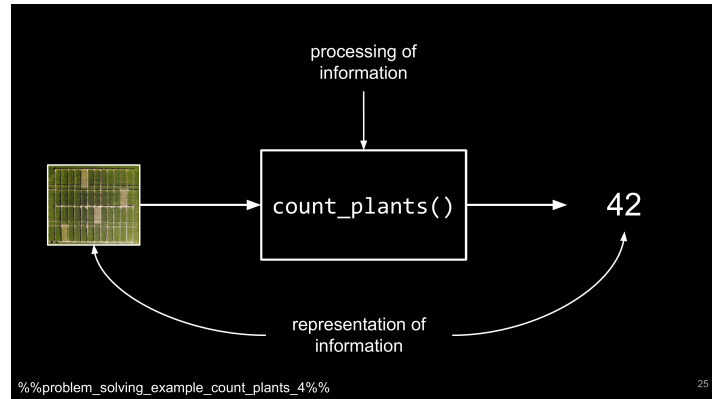
Betrachten wir ein weiteres Beispiel: Stell dir vor, du möchtest einen Computer nutzen, um Maispflanzen auf einer Drohnenaufnahme eines Ackers zu zählen. Diese Aufgabe ist für Menschen zwar einfach zu verstehen, wäre aber sehr zeitaufwändig auszuführen. Moderne Algorithmen ermöglichen es Computern, Objekte auf Bildern präzise zu lokalisieren und zu zählen. Nehmen wir an, wir haben für dieses Problem bereits eine Lösung entwickelt und ein Programm namens `count_plants` erstellt. Nun stellt sich die Frage: Wie sehen die Eingabe und die Ausgabe für dieses Problem aus? Was benötigt das Programm von uns, und was liefert es als Ergebnis?



Die erwartete **Ausgabe** lässt sich einfach beschreiben: Das Ergebnis der Zählung ist eine ganze Zahl. Die **Eingabe** für dieses Problem ist - anders als beim Taschenrechner - kein Tastendruck, sondern ein Bild. Damit der Computer das Bild verarbeiten kann, muss es dem Computer in digitaler Form bereitgestellt werden. Was das genau bedeutet, lernen wir in einem späteren Kapitel. Hier genügt es uns zu verstehen, *dass* wir das Bild digital abbilden müssen.

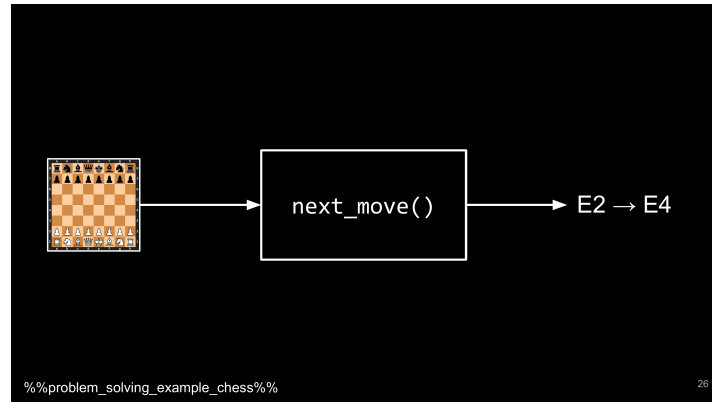


Wie gelangt das Bild in den Computer? Dies ist im Modell nicht näher definiert und für die Problembeschreibung auch nicht wesentlich. Das Bild muss lediglich irgendwie in den Arbeitsspeicher des Programms `count_plants` gelangen. Dies kann auf verschiedene Arten geschehen: Es kann von der Festplatte gelesen werden, über eine drahtlose Verbindung wie Bluetooth direkt übertragen und verarbeitet werden, oder das Programm `count_plants` läuft direkt auf der Drohne und greift unmittelbar auf deren Kamera zu. Die technische Umsetzung ist für unser Modell zunächst irrelevant. In einem späteren Kapitel werden wir uns damit befassen, wie Informationen genau übertragen und gespeichert werden. Genauso werden wir lernen, wie die benötigten Informationen für die Ein- und Ausgabe eines Programms in digitaler Form dargestellt werden können.



4.1.3. Schach spielen

Ein weiteres Beispiel zur Verdeutlichung des EVA-Modells ist das Schachspiel. Das Problem lässt sich einfach beschreiben: Der Computer soll auf Grundlage einer bestehenden Spielsituation den bestmöglichen nächsten Zug vorschlagen. Dieser Zug soll die Gewinnchancen maximieren.



Betrachten wir zunächst die Eingabe für dieses Problem: Wir können dem Computer nicht einfach ein physisches Schachbrett zeigen, sondern müssen überlegen, wie sich ein Schachbrett und die Position der Figuren in digitaler Form darstellen lassen. Dabei kann es durchaus mehrere Möglichkeiten geben, die uns ans Ziel führen.

Ein Schachbrett lässt sich etwa als Liste von 64 Feldern darstellen, die von oben links nach unten rechts durchnummeriert sind. Für jedes Feld speichern wir, ob es leer ist oder welche Figur darauf steht. Die Figuren werden durch Buchstaben dargestellt – zum Beispiel “R” für den Turm (Englisch: Rook) oder “N” für den Springer (Englisch: Knight). Für die Farben Schwarz und Weiß verwenden wir einfach 0 und 1. Diese Darstellungsform reduziert unser Problem auf Listen, Zahlen und Buchstaben in digitaler Form. Für Computer ist das eine leicht zu verarbeitende Struktur, wie wir später noch sehen werden. Ein Beispiel für eine solche Kodierung zeigt Abbildung 4.3.

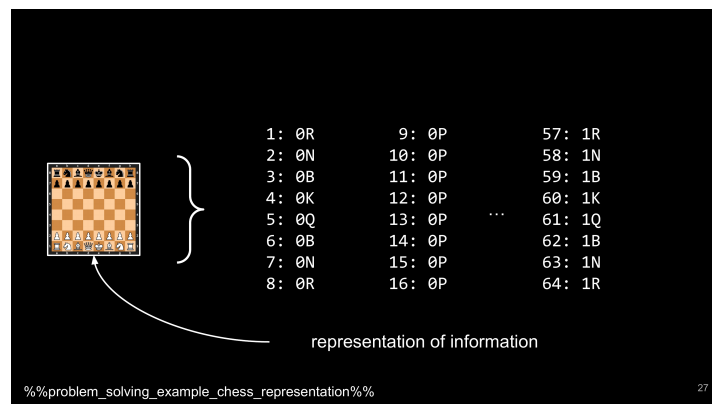


Abbildung 4.3.: Beispiel für die Darstellung von Schachfiguren als Zahlen und Buchstaben.

Die Ausgabe, also der nächste Zug, lässt sich ebenfalls durch Zahlen und Buchstaben darstellen. Eine weit verbreitete Notation gibt zunächst die Koordinate des Ausgangsfelds an, von dem eine Figur gezogen werden soll, gefolgt von der Koordinate des Zielfelds. Ein Beispiel wäre

der Zug von “E2 nach E4”. Statt “E2” und “E4” könnten wir ebenso die entsprechende Zahl zwischen 1 und 64 aus unserer Liste verwenden, um mit dem obigen Schema konsistent zu bleiben. Der Zug hieße dann “53 nach 37”.

4.1.4. Mit Computern chatten

Als drittes Beispiel betrachten wir die Verwendung von Chatprogrammen wie ChatGPT. Seit seiner Veröffentlichung im November 2022 hat es die Welt stark verändert und einen regelrechten KI-Hype ausgelöst. Ein großes Sprachmodell wie GPT-4, das hinter dem heutigen ChatGPT steckt, ist eine komplexe Software, die wir in diesem Buch nicht vollständig ergründen können. Das Schöne an Modellen wie dem EVA-Modell ist jedoch, dass sie komplexe Sachverhalte vereinfachen können – so auch bei Sprachmodellen. Das Problem, das Sprachmodelle lösen, lässt sich wie alle Probleme in unserem EVA-Modell einfach darstellen.

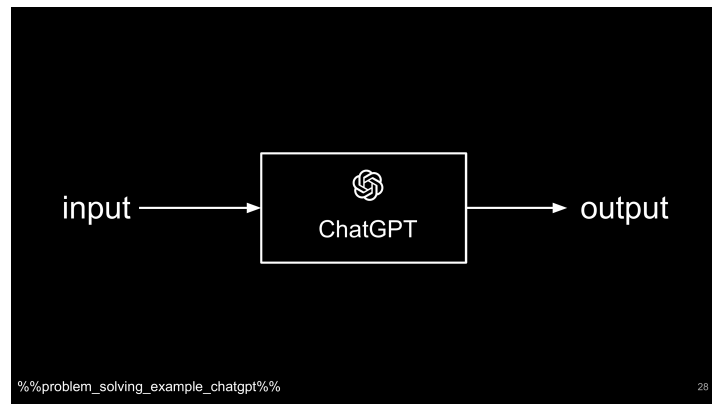


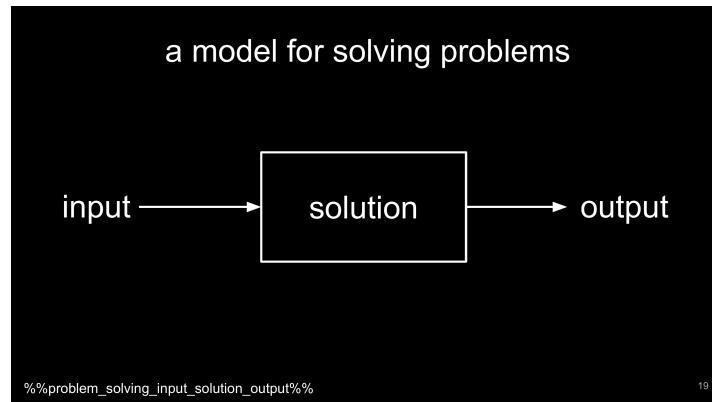
Abbildung 4.4.: ChatGPT im EVA-Modell.

Dabei betrachten wir das Sprachmodell – oder ChatGPT – als Blackbox, ohne die internen Prozesse genauer zu definieren. Für unser Modell genügt es zu verstehen, dass wir eine Eingabe in Form einer Nachricht an ChatGPT benötigen und als Ausgabe eine Antwort erhalten. Auch hier stellt sich die Frage, wie wir beides digital repräsentieren können, damit ChatGPT damit arbeiten kann.

Klassischerweise bestehen sowohl Eingabe als auch Ausgabe einfach aus Texten – allerdings beherrschen moderne Sprachmodelle auch andere Eingabeformen wie Bilder oder gesprochene Sprache über ein Mikrofon. Wir sprechen dann von multimodalen KI-Modellen. Bei Bildern stehen wir vor demselben Repräsentationsproblem wie bei unserer Drohnenaufnahme. Bei der Sprache stellt sich neben der Repräsentation von Audioinhalten die Frage, wie wir gesprochene Worte überhaupt in eine digitale Form überführen können. Auch dazu erfahren wir im späteren Verlauf des Buches mehr.

4.2. Die Lösung des Problems

Anhand des EVA-Modells wird deutlich, dass wir dem Computer Informationen in Form von digitalen Daten bereitstellen müssen, mit denen er arbeiten kann. Was aber genau soll er damit machen? Hier kommt der mittlere Kasten des Modells ins Spiel – die eigentliche Lösung des Problems.



In der Informatik nennen wir die Beschreibung zur Lösung eines Problems einen **Algorithmus**. Ein Algorithmus ist eine Schritt-für-Schritt-Anleitung zur Problemlösung und ist zunächst unabhängig von Computern. Das bedeutet, wir können die Lösung eines Problems ohne Bezug zu einem Computer beschreiben und nennen das einen Algorithmus.

Stellt euch dazu zum Beispiel eine IKEA-Aufbauanleitung vor. Sie beschreibt in sequenziellen Schritten, was zu tun ist, um das fertige Möbelstück zu bekommen. Die Eingabe besteht aus den mitgelieferten Teilen, Schrauben und dem benötigten Werkzeug für den Zusammenbau. Die Ausgabe ist das fertige Regal (oder ein anderes Möbelstück) – und das alles ganz ohne Computer.

Oder nehmt das Kochrezept eure Lieblingsessens. Auch ein Kochrezept ist ein Algorithmus: Die Eingabe besteht aus den Zutaten und Küchenutensilien, die Verarbeitung erfolgt durch die Schritt-für-Schritt-Anleitung, und die Ausgabe ist das fertige Gericht. Wie bei der IKEA-Anleitung ist der Algorithmus unabhängig von einem Computer – er beschreibt lediglich die Lösung des Problems “Wie koche ich dieses Gericht?”.

Zu Beginn des Kapitels haben wir festgestellt, dass Computer aufgrund ihrer Geschwindigkeit und Fehlerfreiheit besonders gut zur Problemlösung geeignet sind – insbesondere bei häufig wiederkehrenden Problemen. Die beiden genannten Beispiele, das IKEA-Regal und das Kochrezept, eignen sich allerdings nicht für eine direkte Umsetzung durch Computer. Der Grund liegt in den analogen Eingaben (Baumaterial, Kochzutaten) und Ausgaben (Möbelstück, fertige Mahlzeit). Diese kann ein Computer nicht unmittelbar verarbeiten. Dafür wären Roboter nötig, die mit der physischen Welt interagieren können. Eine solche Automatisierung lohnt sich

heute nur bei Aufgaben, die sehr häufig auftreten und ansonsten mit hohen Kosten verbunden sind – wie etwa in der Automobilindustrie, wo computergesteuerte Roboter in der Produktion zum Einsatz kommen.

Nehmen wir an, dass Haushaltsroboter in Zukunft erschwinglich werden und uns beim Kochen unseres Lieblingsgerichts helfen können. Wie vermitteln wir dann dem Roboter – im Grunde ein Computer mit Armen und Beinen – den Algorithmus für unser Rezept? Die Lösung liegt in der Programmierung: Wir erstellen ein **Programm** in einer computerverständlichen Sprache. Dieses Programm wandelt die Anweisungen aus unserem Kochbuch in Befehle um, die der Computer verstehen und ausführen kann. Genau genommen besteht ein Programm ebenfalls nur aus Informationen, und wir müssen herausfinden, wie wir diese Informationen digital darstellen können. Die Lösung besteht in der Verwendung einer **Programmiersprache** wie Python, die wir später kennenlernen werden.

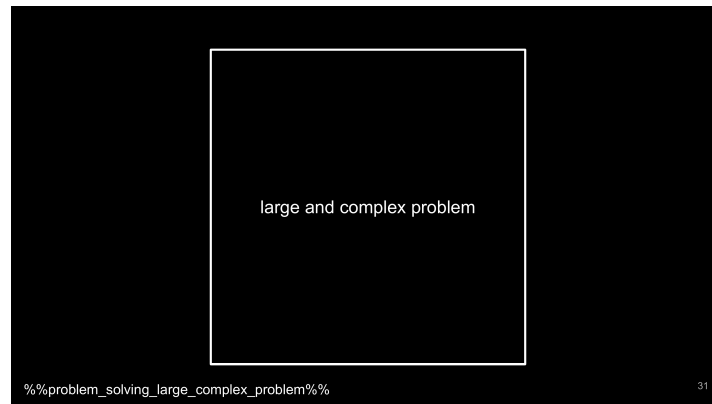
4.3. Problemlösungsstrategien

Die konkrete Lösung und der zugehörige Algorithmus sehen für jedes Problem unterschiedlich aus. Das Erkennen von Pflanzen folgt einer anderen Logik als die Entscheidung, welche Schachfigur als nächstes gezogen werden soll. Dennoch gibt es universelle Lösungsstrategien, die auf viele Probleme anwendbar sind, um sie möglichst effizient zu lösen. Im Folgenden betrachten wir drei dieser Strategien.

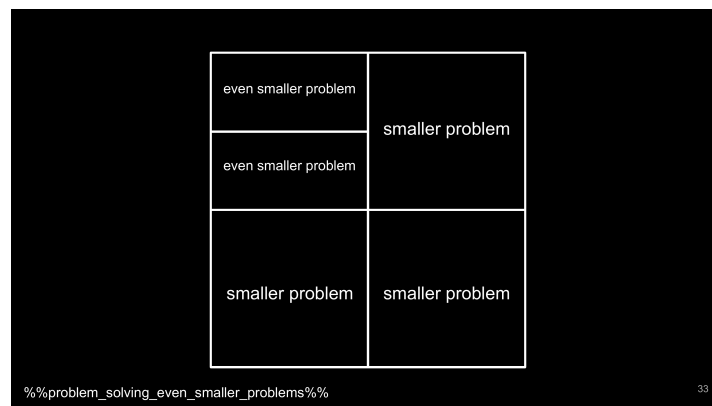
4.3.1. Problemzerlegung (*Problem Decomposition*)

Eine universelle Strategie zur Lösung komplexer Probleme ist die Zerlegung in kleinere Schritte oder Teilprobleme. Jedes dieser Teilprobleme ist unterschiedlich und erfordert einen spezifischen Lösungsansatz. Nehmen wir als Beispiel das Zählen von Pflanzen auf einer Drohnenaufnahme. Dieses komplexe Problem lässt sich, ausgehend von der Eingabe – dem digitalen Bild – in drei Teilprobleme zerlegen:

1. Pflanzen auf dem Bild lokalisieren
2. Lokalisierte Pflanzen klassifizieren: Maispflanze oder nicht?
3. Identifizierte Maispflanzen zählen



Jedes dieser Teilprobleme erfordert einen eigenen Algorithmus. Dabei ist es möglich, die Teilprobleme noch weiter zu zerlegen, um sie besser bearbeiten zu können.



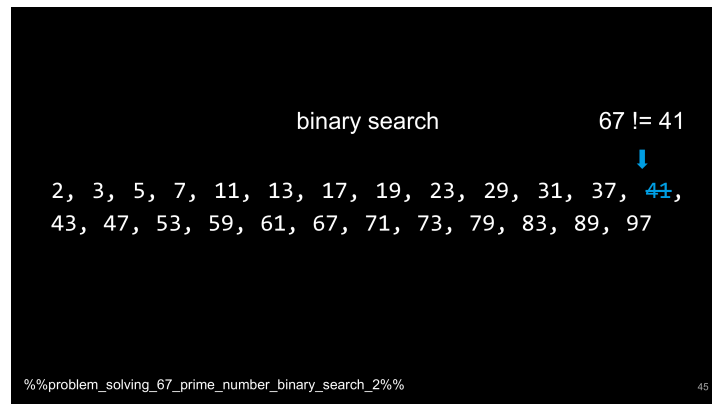
Die Identifizierung sinnvoller Teilprobleme erfordert ein ausgeprägtes analytisches Denkvermögen. Dies ist besonders wichtig im Umgang mit Computern. Wie wir beim Erlernen der Programmierung sehen werden, ist die Zerlegung eines Problems in kleine, lösbare Schritte der Schlüssel zur Beherrschung seiner Komplexität.

4.3.2. Teile und Herrsche (*Divide and Conquer*)

Die "Teile und Herrsche"-Strategie ist ein Ansatz zur Lösung komplexer Probleme, bei dem wir das Hauptproblem schrittweise in immer kleinere Teilprobleme zerlegen, bis diese einfach zu lösen sind. Dabei gehen wir rekursiv vor: Wir teilen das ursprüngliche Problem in kleinere Teile, diese kleineren Probleme wiederum in noch kleinere Teile und so weiter. Die Rekursion endet, wenn die Probleme so klein sind, dass sie sich nicht weiter aufteilen lassen und die Lösung direkt ersichtlich ist.

Anders als bei der Problemzerlegung sind die Teilprobleme beim Divide and Conquer-Ansatz dadurch gleichartig und stellen nur kleinere Instanzen des ursprünglichen Problems dar. Die einzelnen Lösungen für jedes Teilproblem werden dann schrittweise wieder zusammengeführt, um die Gesamtlösung zu erhalten. Ein klassisches Beispiel ist die Sortierung einer langen Liste von Zahlen: Wir teilen die Liste immer wieder in der Mitte, bis nur noch einzelne Zahlen übrig sind, und fügen diese dann in sortierter Reihenfolge wieder zusammen.

Ein anderes Beispiel ist die binäre Suche in einer sortierten Liste. Hier betrachten wir das Element in der Mitte der Liste und vergleichen es mit dem gesuchten Element. Da die Liste sortiert ist, können wir entscheiden, in welchem Teil der Liste wir weitersuchen müssen. Im zweiten Schritt suchen wir nur in diesem Teil weiter und haben damit das Problem halbiert. Die Natur des Problems bleibt dabei gleich, und wir können erneut genauso verfahren – so lange, bis wir nur noch ein Element übrig haben, das entweder das gesuchte Element ist oder nicht.



4.3.3. Verteile und Parallelisiere (*Distribute and Parallelize*)

Manche Probleme lassen sich effizienter lösen, wenn mehrere Personen gleichzeitig daran arbeiten. Anstatt eine einzelne Person mit der gesamten Aufgabe zu betrauen, verteilen wir die Arbeit auf mehrere Schultern und arbeiten parallel an der Lösung. Allerdings eignet sich nicht jedes Problem für diesen Ansatz.

Ein gutes Beispiel ist das Aufräumen eines Zimmers: Eine einzelne Person müsste nacheinander verschiedene Bereiche aufräumen, während mehrere Personen gleichzeitig unterschiedliche Ecken des Raums in Angriff nehmen können. Je größer das Zimmer, desto mehr Personen werden benötigt, um es in der gleichen Zeit aufzuräumen. Ein Gegenbeispiel, bei dem diese Strategie nicht funktioniert, ist das Lösen einer mathematischen Gleichung. Hier müssen die einzelnen Rechenschritte aufeinander aufbauen, weshalb das Problem nicht gleichzeitig an mehrere Personen übergeben werden kann, die unabhängig daran arbeiten.

Die Strategie des Verteilens und Parallelisierens – im Englischen *Distribute and Parallelize* – funktioniert nach einem klaren Prinzip: Wir zerlegen ein großes Problem in Teile, die unabhängig voneinander gelöst werden können. Diese Teile weisen wir dann verschiedenen Ressourcen zu – zum Beispiel mehreren Personen oder Computern. Jede Ressource arbeitet an ihrem Teilproblem und erzeugt ein eigenes Ergebnis. Dabei gehen wir davon aus, dass sich alle Teilergebnisse am Ende zu einer Gesamtlösung zusammenfügen lassen. Ähnlich wie beim Divide and Conquer-Ansatz sind die Teilprobleme meist gleichartig.

Um dieses Konzept greifbar zu machen, schauen wir uns ein konkretes Beispiel an, das wir mit dem EVA-Modell analysieren: das Zählen aller Wörter in einem Buch.

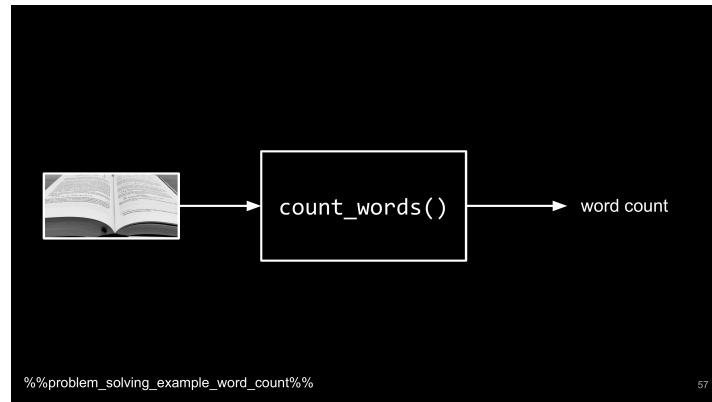


Abbildung 4.5.: Das Wörterzählen-Problem im EVA-Modell

Je nach Umfang des Buches kann dies eine mühsame Aufgabe sein, besonders für Menschen. Ein Computer bewältigt ein einzelnes Buch dank seiner hohen Verarbeitungsgeschwindigkeit problemlos. Allerdings lässt sich das Problem beliebig erweitern – etwa wenn wir statt eines Buches alle Texte im Internet oder sämtliche Wikipedia-Artikel analysieren möchten. In solchen Fällen wird die Aufgabe auch für Computer aufwendig und zeitintensiv. Eine Lösung besteht darin, mehrere Computer parallel einzusetzen.

In [Abbildung 4.6](#) sehen wir beispielhaft die Verteilung der Buchseiten auf vier Studenten. Jeder erhält einen gleichen Anteil, wodurch sich die Bearbeitungszeit im Optimalfall auf ein Viertel reduziert. Bei Computern können wir analog vorgehen und mehrere Rechner gleichzeitig mit Teilen der Seiten betrauen. Diese Rechner werden in einem Netzwerk verbunden und von einem zentralen Computer gesteuert, der die Teilergebnisse am Ende zusammenführt. Ein solches System nennen wir Rechencluster, bestehend aus Arbeitern – den *Worker Nodes* – sowie einer Steuereinheit, die in solchen Systemen als *Driver* oder *Name Node* bezeichnet wird.

Durch die Verteilung und parallele Ausführung kann das EVA-Modell wie in [Abbildung 4.7](#) angepasst und detaillierter dargestellt werden. Statt eines einzelnen Prozesses `count_words` laufen nun n parallele Prozesse, die jeweils einen Teil des Buches durchsuchen. Die Aufteilung

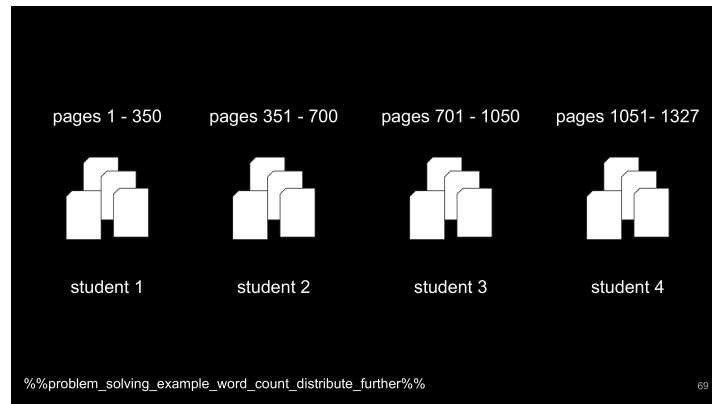


Abbildung 4.6.: Verteiltes Wörterzählen

erfolgt zu Beginn durch den `split`-Prozess, während das Zusammenführen der Teilergebnisse – in diesem Fall das Addieren der Teilsummen – durch den `merge`-Schritt erfolgt.

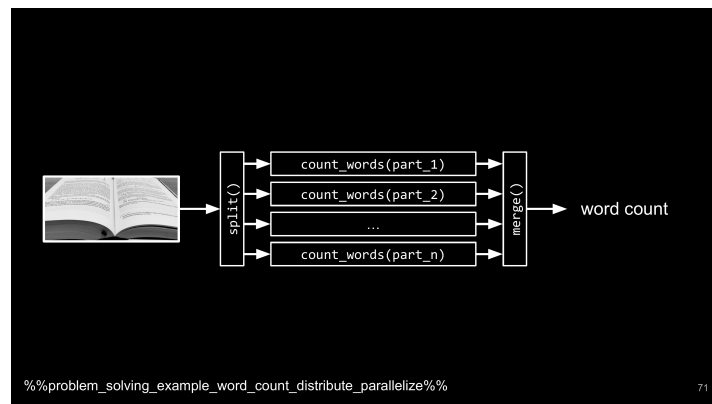


Abbildung 4.7.: Das parallelisierte Wörterzählen im EVA-Modell

In diesem Kapitel haben wir uns mit dem EVA-Modell auseinandergesetzt - einem fundamentalen Konzept für die computergestützte Problemlösung. Dieses Modell bietet uns einen strukturierten Rahmen, der aus drei wesentlichen Komponenten besteht:

- Eingabe (E): Die zu verarbeitenden Daten oder Informationen
- Verarbeitung (V): Der Kern der Problemlösung durch Algorithmen
- Ausgabe (A): Das Ergebnis der Verarbeitung in nutzbarer Form

Die Verarbeitung als zentrales Element des Modells ist dabei der Ort, an dem die eigentliche Problemlösung stattfindet. Hier kommen Algorithmen zum Einsatz - präzise Handlungsanweisungen, die Schritt für Schritt zur Lösung führen. Die genaue Natur dieser Algorithmen, ihre

charakteristischen Eigenschaften und wie wir sie entwickeln können, werden wir im nächsten Kapitel detailliert betrachten.

4.4. Warum nutzen wir Computer?

Der wichtigste Grund für die Nutzung von Computern ist das Lösen von Problemen. Ob wir eine Route mit Google Maps planen, Online-Bestellungen bei DHL verfolgen oder eine KI wie ChatGPT um eine Empfehlung bitten – überall lösen Computer Probleme. Warum? Weil Computer zwei Eigenschaften besitzen, die für viele Probleme und deren Lösung vorteilhaft sind:

1. Computer machen keine Fehler. Wenn wir einem Computer einen Lösungsweg beibringen, wendet er ihn fehlerfrei auf neue Probleme an.
2. Computer sind unglaublich schnell. Ob einfache Schritte, komplexe Berechnungen oder die Verarbeitung großer Datenmengen – Computer lösen Probleme in einem Bruchteil der Zeit, die wir Menschen benötigen würden.

Diese beiden Eigenschaften ermöglichen es uns, mit Computern besonders solche Probleme effizient zu lösen, die wiederkehrend und in großer Zahl auftreten. Wir sprechen dann von **Automatisierung**.

In diesem Kapitel lernen wir, wie Computer Probleme strukturieren und lösen. Um den Begriff des Problems besser zu verstehen und seine Bedeutung im Kontext von Computern einzugrenzen, führen wir zunächst ein einfaches Modell ein.

5. Algorithmen

5.1. Zusammenfassung

Willkommen zum Kapitel über Algorithmen - ein fundamentales Konzept der Informatik und der digitalen Problemlösung. In diesem Abschnitt werden wir uns mit den grundlegenden Aspekten von Algorithmen befassen und dabei zentrale Fragen beantworten:

- Was ist ein Algorithmus und wie grenzt er sich von einem Computerprogramm ab?
- Welche verschiedenen Kategorien von Algorithmen existieren und durch welche praktischen Beispiele lassen sie sich veranschaulichen?
- Wie können wir Algorithmen systematisch und präzise formulieren?
- Nach welchen Kriterien bewerten wir die Effizienz und Eignung verschiedener Algorithmen für spezifische Problemstellungen?

5.2. Was ist ein Algorithmus?

5.2.1. Herkunft des Begriffs

Der Begriff “**Algorithmus**” [stammt vom Namen des persischen Mathematikers Muhammad al-Khwarizmi](#), der um das Jahr 780 n. Chr. geboren wurde. Al-Khwarizmi war ein bedeutender Gelehrter am Hofe des Kalifen al-Mamun und verfasste dort Schriften, die den Gebrauch der indischen Zahlzeichen erklärten. Diese Schriften wurden im 12. Jahrhundert ins Lateinische übersetzt, wobei der Titel “Algoritmi de numero Indorum” verwendet wurde. Im Laufe der Zeit wurde der Name al-Khwarizmi zur Bezeichnung für die von ihm beschriebenen Rechenverfahren und entwickelte sich schließlich zum modernen Begriff “Algorithmus”.

Heute bezeichnet ein **Algorithmus** eine präzise Abfolge von Anweisungen, die ein bestimmtes Problem lösen oder eine Aufgabe erfüllen sollen. Im Alltag begegnen uns Algorithmen ständig, oft, ohne dass wir es merken: beim Kochen, bei der Wegbeschreibung oder beim Aufbau eines IKEA-Regals.

5.2.2. Algorithmen und Programme

Ein wichtiger Aspekt von Algorithmen ist ihre Universalität: Sie sind nicht an Computer gebunden. Ein Algorithmus ist im Kern eine strukturierte Anleitung zur Problemlösung, unabhängig davon, wer oder was diese Anleitung ausführt. Diese Flexibilität zeigt sich besonders deutlich in unserem Alltag, wo wir ständig algorithmische Anleitungen befolgen - sei es beim Aufbau eines Möbelstücks oder beim Kochen nach einem Rezept. Bei diesen Tätigkeiten führen wir Menschen die algorithmischen Schritte aus, ganz ohne Beteiligung eines Computers:

- **Kochen:** Ein Rezept ist ein Algorithmus für die Zubereitung eines Gerichts.

Comment

- **Wegbeschreibung:** Eine Schritt-für-Schritt-Anleitung, um von Punkt A nach Punkt B zu gelangen.
- **Bastelanleitung:** Die Anweisungen, um ein Modellflugzeug zusammenzubauen.

Viele Algorithmen können von Computern ausgeführt werden. Dafür ist jedoch eine Übersetzung in eine maschinenverständliche Form notwendig. Diese Übersetzung erfolgt durch das Programmieren, wobei wir den Algorithmus in einer Programmiersprache formulieren. Um die Beziehung zwischen Algorithmen und Computerprogrammen besser zu verstehen, ist es hilfreich, drei zentrale Begriffe zu unterscheiden:

- **Algorithmus:** Die abstrakte Beschreibung einer Lösungsmethode in Form einer präzisen, endlichen Sequenz von individuellen Anweisungen. Ein Algorithmus ist unabhängig von der konkreten Umsetzung und kann sowohl von Menschen als auch von Maschinen ausgeführt werden.
- **Programm:** Die konkrete Implementation eines oder mehrerer Algorithmen in einer Programmiersprache. Das Programm übersetzt die abstrakten Anweisungen des Algorithmus in eine Form, die ein Computer verstehen und ausführen kann.
- **Prozess:** Die tatsächliche Ausführung eines Programms durch einen Computer. Dabei werden die programmierten Anweisungen Schritt für Schritt abgearbeitet, um das gewünschte Ergebnis zu erzielen.

5.3. Kategorien

Algorithmen können nach ihrer Funktion und ihrem Anwendungsbereich in verschiedene Kategorien eingeteilt werden. Jede Kategorie repräsentiert einen spezifischen Problemlösungsansatz:

- **Mathematische Algorithmen:** Berechnen oder approximieren Werte

- **Suchalgorithmen:** Finden bestimmte Elemente in einer Datenmenge
- **Sortieralgorithmen:** Ordnen Daten nach bestimmten Kriterien
- **Optimierungsalgorithmen:** Finden die bestmögliche Lösung für ein Problem
- **Graphenalgorithmen:** Arbeiten mit vernetzten Strukturen
- **Stochastische Algorithmen:** Verwenden Zufallselemente, um ein Problem zu lösen
- **Maschinelle Lernalgorithmen:** Erkennen Muster und treffen Vorhersagen

Diese Kategorien sind weder vollständig noch strikt voneinander getrennt. Viele Algorithmen lassen sich mehreren Kategorien zuordnen. Ein anschauliches Beispiel hierfür ist der **Dijkstra-Algorithmus**, der die kürzeste Route zwischen zwei Punkten findet. Er ist sowohl ein Graphenalgorithmus, da er auf vernetzten Strukturen arbeitet, als auch ein Optimierungsalgorithmus, da er die optimale (kürzeste) Route ermittelt.

Im folgenden beleuchten wir ein oder mehr Beispiele für jeder der genannten Klassen.

5.3.1. Mathematische Algorithmen

5.3.1.1. Größter gemeinsamer Teiler (GGT)

Der Algorithmus zur Berechnung des größten gemeinsamen Teilers (GGT) ist ein klassisches Beispiel für einen eleganten mathematischen Algorithmus. Er wurde vom griechischen Mathematiker Euklid um 300 v. Chr. in seinem Werk “Die Elemente” beschrieben und demonstriert eindrucksvoll die zeitlose Natur algorithmischen Denkens.

Das Verfahren basiert auf einem einfachen, aber genialen Prinzip: Der GGT zweier Zahlen ist identisch mit dem GGT der kleineren Zahl und der Differenz beider Zahlen. Zum Beispiel haben die Zahlen 48 und 18 den gleichen GGT wie 18 und 30 (48-18). Durch wiederholtes Anwenden dieser Regel wird der GGT systematisch ermittelt. Die Eleganz dieses Verfahrens liegt in seiner Einfachheit und mathematischen Präzision - Eigenschaften, die auch heute noch moderne Algorithmen auszeichnen.

Der Block unten zeigt die Schritte des Euklidschen Algorithmus für das obige Zahlenbeispiel.

```

Loop 1:
a = 18, b = 48
a < b → swap: a = 48, b = 18
a = 48 - 18 = 30

Loop 2:
a = 30, b = 18
a >= b → no swap

```

$a = 30 - 18 = 12$

Loop 3:

$a = 12, b = 18$

$a < b \rightarrow \text{swap: } a = 18, b = 12$

$a = 18 - 12 = 6$

Loop 4:

$a = 6, b = 12$

$a < b \rightarrow \text{swap: } a = 12, b = 6$

$a = 12 - 6 = 6$

Loop 5:

$a = 6, b = 6$

$a \geq b \rightarrow \text{no swap}$

$a = 6 - 6 = 0$

result: $b = 6$

5.3.1.2. Babylonisches Wurzelziehen

5.3.2. Suchalgorithmen

5.3.2.1. Lineare Suche

5.3.2.2. Binäre Suche

5.3.2.3. Suche in Bäumen

5.3.3. Sortieralgorithmen

5.3.4. Optimierungsalgorithmen

5.3.4.1. Dijkstra-Algorithmus

5.3.5. Graphenalgorithmen

5.3.6. Stochastische Algorithmen

5.3.6.1.

5.3.7. Maschinelle Lernalgorithmen

5.4. Iteration und Rekursion

Teil II.

Repräsentation

6. Informationen



Zu diesem Kapitel gibt es ein Video auf YouTube. Scanne einfach den QR-Code oder klicke in der digitalen Version des Buches auf den QR-Code.

6.1. Information in der Informatik

Hast du dich jemals gefragt, was eigentlich Information genau ist? Jeder hat eine intuitive Vorstellung davon, was wir mit Information meinen. Aber was ist die genaue Definition? Und wie ist der Begriff *Information* im Zusammenhang mit digitalen Computern gemeint?

Hier schon einmal eine Definition, die wir in diesem Kapitel anhand von einigen Beispielen genauer verstehen wollen.

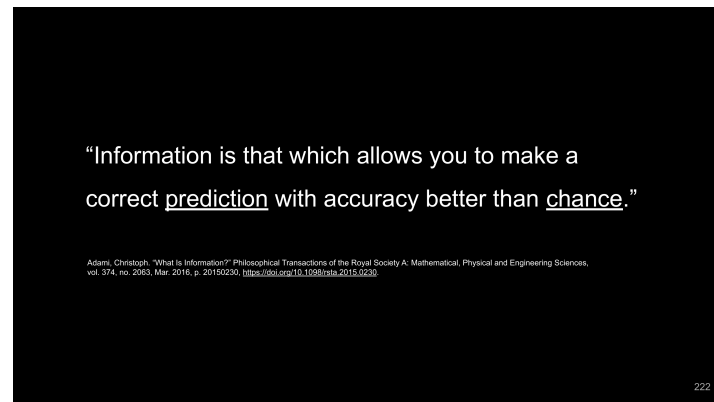


Abbildung 6.1.: Lauter dieser Definition erhöht Information unsere Treffsicherheit bei Vorhersagen.

6.1.1. Zahlenraten

Um der Information auf die Spur zu kommen beginnen wir mit einem Gedankenexperiment. Stell dir vor, wir spielen ein Zahlenratespiel. Ich denke an eine Zahl zwischen 1 und 16, und dein Ziel ist es, sie zu erraten. Der Haken ist, dass du nur einen Versuch hast, die richtige Zahl zu erraten, aber du kannst die Möglichkeiten vorher durch Fragen der Form “Ist die Zahl größer als X?” eingrenzen. Für jede Frage werde ich dir mit “ja” oder “nein” antworten und damit die verbleibenden Optionen reduzieren.

Mit jeder Antwort, die du erhältst, wächst dein Wissen über meine Zahl, was bedeutet, dass deine **Unsicherheit** bezüglich der gesuchten Zahl abnimmt. Du kannst einige mögliche Zahlen ausschließen, wenn du eine neue Antwort erhältst.

Wir halten zunächst fest, dass das Eingrenzen der verbleibenden Möglichkeiten die Unsicherheit reduziert. Wir untersuchen nun, wie diese Idee die Grundlage der Informationstheorie bildet. Durch die Reduzierung der Unsicherheit sammeln wir mit jedem Versuch mehr **Information**. Aber wie viel Information erhältst du mit jeder Antwort? Und wie können wir das messen?

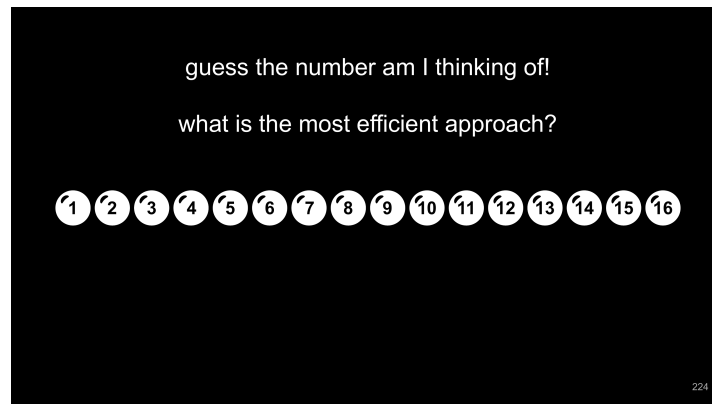


Abbildung 6.2.: Ich denke an eine Zahl zwischen 1 und 16. Deine Aufgabe ist es, die Zahl mit so wenig Fragen wie möglich zu erraten.

6.1.2. Bit für Bit

In der Informatik kann Information definiert werden als “das, was es ermöglicht, eine korrekte Vorhersage mit besserer Genauigkeit als der Zufall zu treffen” [CITE]. Einfacher ausgedrückt bedeutet dies, die Unsicherheit durch Eingrenzung der möglichen Optionen zu reduzieren.

Vor diesem Hintergrund wollen wir unser Zahlenratespiel noch einmal genauer betrachten. Wie oben beschrieben, versuchst du meine Zahl zu erraten, und jede Antwort, die du von mir erhältst, grenzt den Bereich der möglichen Zahlen ein. Diese Reduzierung der Unsicherheit kann mit einer Einheit namens **Bit** gemessen werden. Ein Bit, was für **binary digit** (Binärziffer)

steht, ist die grundlegende Einheit der Information. Es zeigt eine Halbierung der Unsicherheit an. Einfacher ausgedrückt: Wenn eine neue Antwort nur noch halb so viele Optionen wie zuvor übrig lässt, liefert sie uns genau ein Bit an Information.

Allerdings werden nicht alle Fragen und deren Antworten genau ein Bit Information liefern. Wenn zum Beispiel deine erste Frage im Ratespiel lautet: “Ist deine Zahl größer als 12?” und die Antwort “nein” ist, bleiben die Zahlen 1 bis 12 übrig. Das bedeutet, du hast noch 12 Optionen von ursprünglich 16, was die Unsicherheit nicht halbiert. Es werden nur 4 statt der nötigen 8 Möglichkeiten entfernt. Lautet die Antwort dagegen “ja”, so kannst du insgesamt 12 Möglichkeiten streichen, was mehr als der Hälfte entspricht und der Informationsgehalt der Antwort wäre größer als ein Bit.

Um genau ein Bit Information zu erhalten, solltest du darauf abzielen, mit jeder Frage genau die Hälfte der möglichen Zahlen auszuschließen. Wenn du zum Beispiel fragst “Ist deine Zahl größer als 8?”, stellst du sicher, dass du - egal ob die Antwort “ja” oder “nein” ist - in beiden Fällen 8 mögliche Zahlen übrig behältst. Ist die Antwort “ja”, bleiben die Zahlen 9 bis 16 übrig. Ist die Antwort “nein”, bleiben die Zahlen 1 bis 8. In beiden Szenarien wird deine Unsicherheit um die Hälfte reduziert, also um ein Bit.

Indem du deine Fragen sorgfältig so wählst, dass sie die verbleibenden Optionen jedes Mal halbieren, reduzierst du deine Unsicherheit Bit für Bit und machst es dir leichter und schneller, die richtige Zahl zu finden.

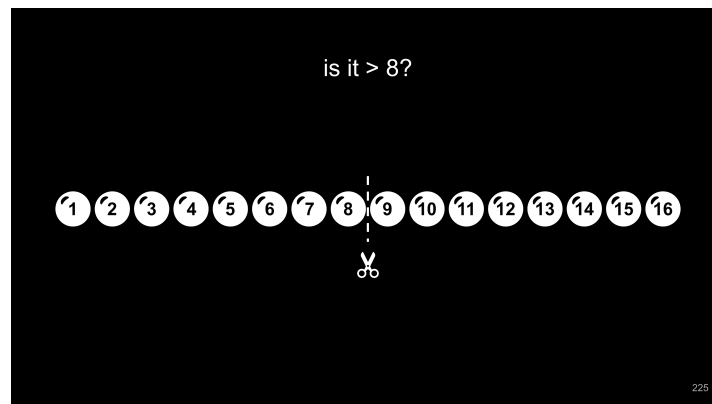


Abbildung 6.3.: Deine Fragen sollten die Anzahl der Möglichkeiten halbieren.

Angenommen, die Antwort auf deine erste Frage “Ist deine Zahl größer als 8?” war “nein”. Was sollte deine nächste Frage sein, um die Unsicherheit weiterhin effektiv zu reduzieren? Die beste Strategie ist es zu fragen: “Ist sie größer als 4?”. Diese Vorgehensweise stellt sicher, dass dir immer nur vier mögliche Zahlen bleiben: entweder 1 bis 4, wenn die Antwort “nein” ist, oder 5 bis 8, wenn die Antwort “ja” ist. Erneut halbiert dies die verbleibenden Optionen und liefert genau ein Bit an Information.

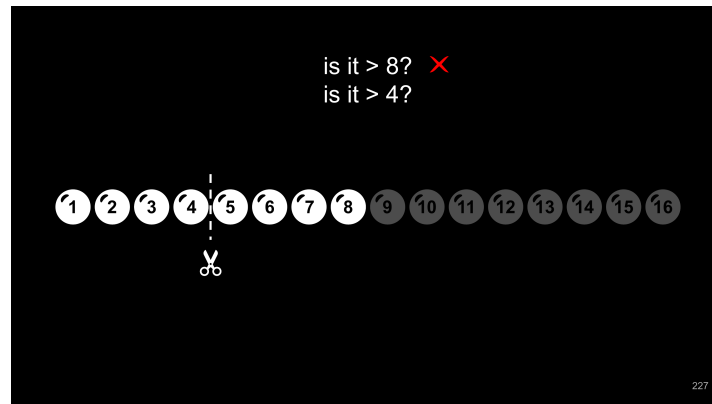


Abbildung 6.4.: Nach zwei Fragen bleiben noch 4 Möglichkeiten, wenn die Fragen gut gewählt wurden.

Lass uns mit dieser Methode fortfahren. Angenommen, deine zweite Frage “Ist sie größer als 4?” erhält ein “nein” als Antwort. Deine neue Auswahl an Zahlen ist auf 1, 2, 3 und 4 begrenzt. Um die Unsicherheit weiter zu reduzieren, wäre die nächste logische Frage: “Ist sie größer als 2?” Dies lässt dir entweder die Zahlen 1 und 2 oder 3 und 4, abhängig von der Antwort.

Indem du weiterhin Fragen stellst, die systematisch die verbleibenden Optionen halbieren, kannst du sehen, wie wir schrittweise die Unsicherheit Bit für Bit reduzieren. Schließlich wirst du nach nur vier Fragen die Zahl auf genau eine eingrenzen, da keine anderen Möglichkeiten mehr übrig sind. Das bedeutet, du hast die Unsicherheit auf null reduziert.

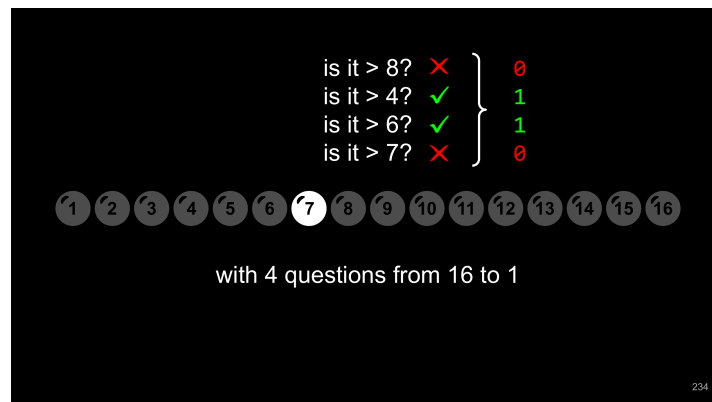


Abbildung 6.5.: Wir benötigen vier Ja/Nein-Fragen, um die Optionen von 16 auf eine einzige zu reduzieren.

6.1.3. Unsicherheit

Wir haben gerade gelernt, dass wir mit jeder Ja/Nein-Frage, die die Hälfte der Möglichkeiten eliminiert, ein Bit an Information gewinnen. Aber wie können wir dieses Konzept der Reduktion von Unsicherheit mathematisch quantifizieren? Wir gehen das Schritt für Schritt durch.

Stell dir vor, du bist am Anfang unseres Zahlenratespiels. Es gibt 16 mögliche Zahlen, an die ich denken könnte, daher ist deine Wahrscheinlichkeit, beim ersten Versuch die richtige Zahl zu erraten, ziemlich gering:

$$P_{correct} = \frac{1}{16}$$

Das entspricht einer Wahrscheinlichkeit von nur 0,0625 - definitiv nicht zu deinen Gunsten. Angenommen, du stellst eine Frage, die die Möglichkeiten auf die Hälfte reduziert. Jetzt verbessert sich deine Chance, richtig zu raten:

$$P_{correct} = \frac{1}{8}$$

Mit jeder weiteren Frage verdoppelt sich diese Wahrscheinlichkeit, während sich deine Unsicherheit halbiert. Ist Wahrscheinlichkeit die beste Methode, um Unsicherheit zu messen? Wenn wir möchten, dass unser Maß für Unsicherheit abnimmt, während wir mehr Informationen sammeln, ist es sinnvoll, den Kehrwert der Wahrscheinlichkeit zu verwenden. Das entspräche der Anzahl an Möglichkeiten, die noch im Rennen sind.

Zu Beginn gibt es 16 Möglichkeiten, also begänne die Unsicherheit bei 16. Nach der ersten Frage fiel sie auf 8, dann auf 4, 2 und schließlich 1. Allerdings würde dieses Maß uns selbst dann, wenn nur noch eine Option übrig ist, eine gewisse Unsicherheit, nämlich 1, anzeigen, was nicht ganz unserem intuitiven Verständnis entspricht. Wenn wir sicher sind, dann sollte die Unsicherheit 0 sein.

Claude Shannon, der Vater der Informationstheorie, schlug einen anderen Ansatz vor. Er empfahl, die Unsicherheit mithilfe des Logarithmus zur Basis 2 der Anzahl der Möglichkeiten zu messen:

$$H = \log_2(N)$$

Diese Methode hat mehrere Vorteile. Erstens ist die Unsicherheit gleich null, wenn es nur eine mögliche Antwort gibt ($N=1$), was mit unserer Intuition übereinstimmt:

$$\log_2(1) = 0$$

Ein weiterer Vorteil ist die Einfachheit der Berechnungen, besonders wenn es um mehrere unabhängige Unsicherheiten geht. Nehmen wir an, das Spiel ändert sich: Jetzt denke ich an zwei unabhängige Zahlen zwischen 1 und 16. Bevor du irgendwelche Fragen stellst, beträgt deine Unsicherheit für jede Zahl:

$$\log_2(16) = 4 \text{ bits}$$

Die Gesamtunsicherheit für beide Zahlen ist einfach die Summe ihrer individuellen Unsicherheiten:

$$\log_2(16) + \log_2(16) = 8 \text{ bits}$$

Wenn wir stattdessen Wahrscheinlichkeiten verwenden, müssten wir die Chancen multiplizieren, um die Wahrscheinlichkeit zu finden, beide Zahlen korrekt zu erraten:

$$P_{\text{correct,correct}} = \frac{1}{16} \times \frac{1}{16} = \frac{1}{256}$$

Mit beiden Zahlen gibt es 256 Möglichkeiten. Mit Shannons Methode erhalten wir das gleiche Ergebnis:

$$\log_2(256) = 8 \text{ bits}$$

Wie du siehst, vereinfacht die Verwendung von Logarithmen unsere Berechnungen, besonders wenn es um mehrere Quellen der Unsicherheit geht. Diese Klarheit und Einfachheit sind der Grund, warum Shannons Ansatz fundamental für die Informationstheorie geworden ist.

6.1.4. Information

Um den Begriff *Information* aus dem Begriff der *Unsicherheit* herzuleiten, betrachten wir zwei Zustände: Die ursprüngliche Unsicherheit vor einer Frage, die wir als H_0 bezeichnen, und die reduzierte Unsicherheit nach der Antwort, die wir H_1 nennen. Die Menge an Information I , die wir durch die Antwort gewinnen, entspricht der Differenz dieser beiden Unsicherheiten:

$$I = H_0 - H_1$$

Information ist also die Reduzierung von Unsicherheit. Mit der obigen Formel können wir die Information I präzise quantifizieren. Dies ermöglicht uns zu berechnen, wie viel Information wir durch jede Frage gewinnen. Betrachten wir ein konkretes Beispiel aus unserem Zahlenratespiel: Angenommen, deine erste Frage ist “Ist deine Zahl größer als 12?” und die Antwort lautet

“nein”. Dann bleiben die Zahlen 1 bis 12 als Möglichkeiten übrig. Die gewonnene Information berechnet sich wie folgt:

$$I = \log_2(16) - \log_2(12) \approx 4 - 3.585 \approx 0.415 \text{ bits}$$

In diesem Fall lieferte die Antwort etwa 0,415 Bits an Information – also weniger als ein Bit. Das ist folgerichtig, da die Antwort weniger als die Hälfte der Möglichkeiten eliminiert hat.

Wie sähe es aus, wenn die Antwort “ja” gewesen wäre? In diesem Fall blieben nur die Zahlen 13, 14, 15 und 16 übrig, also vier mögliche Optionen:

$$I = \log_2(16) - \log_2(4) = 4 - 2 = 2 \text{ bits}$$

Diese Antwort lieferte mehr als ein Bit, nämlich 2 Bits. Wie lässt sich dieser Unterschied erklären?

6.1.5. Unwahrscheinliche Antworten

Die Menge an Information hängt von der Wahrscheinlichkeit der jeweiligen Antwort ab. Bei einer Frage, die die Möglichkeiten halbiert, hat jede Antwort “Ja” oder “Nein” auf die Frage “Ist die Zahl größer als X?” eine Wahrscheinlichkeit von genau 50%. Diese gleichmäßige Verteilung vereinfacht die Berechnung und liefert genau ein Bit an Information.

Bei der Frage “Ist deine Zahl größer als 12?” sind die beiden Antworten “Ja” und “Nein” allerdings nicht gleich wahrscheinlich. Es gibt zwölf mögliche Zahlen, die ein “Nein” ergeben und nur vier, die ein “Ja” ergeben, was Wahrscheinlichkeiten von 75% für “Nein” und 25% für “Ja” bedeutet. Da die “Ja”-Antwort weniger wahrscheinlich ist, ist sie überraschender – und liefert deshalb mehr Information. Wie wir berechnet haben, gibt uns ein “Ja” 2 Bits an Information, während ein “Nein” nur 0,415 Bits liefert.

Dieser Zusammenhang ist ein Kernprinzip der Informationstheorie: Je unwahrscheinlicher ein Ereignis ist, desto mehr Information enthält sein Auftreten. Umgekehrt liefert eine sehr wahrscheinliche Antwort, wie das “Nein” im obigen Beispiel, weniger Information, da sie weniger überraschend ist.

Warum zielen wir darauf ab, Fragen zu stellen, die die Möglichkeiten gleichmäßig halbieren? Man könnte auch wild raten in der Hoffnung, durch eine unwahrscheinlichere Antwort mehr Informationen zu bekommen – auch wenn man seltener richtig liegt. Die Antwort ist einfach: Eine Frage, die den Raum der Möglichkeiten halbiert, maximiert unseren *erwarteten* Informationsgewinn. Zwar können wir mit einer riskanten Frage wie “Ist die Zahl größer 15?” unser Glück herausfordern und im Erfolgsfall die Unsicherheit stark verringern. Dies ist jedoch keine nachhaltige Strategie. Wenn wir das Spiel nicht nur einmal, sondern 10, 100 oder 1000 Mal spielen, nähern wir uns im Mittel dem Erwartungswert für die gewonnene Information

$E[I]$. Und dieser Erwartungswert favorisiert eindeutig Fragen, die die Hälfte der Möglichkeiten eliminieren.

Um dies zu verdeutlichen, berechnen wir zunächst den Erwartungswert für die extreme Frage “Ist die Zahl größer 15?”:

$$E[I] = \left(\frac{1}{16} \times 4\right) + \left(\frac{15}{16} \times 0.09311\right) = 0.3373$$

Der Erwartungswert berechnet sich durch den mit der Wahrscheinlichkeit gewichteten Informationsgewinn für jede mögliche Antwort. Bei der Frage “Ist die Zahl größer als 15?” gibt es ein “Ja” nur dann, wenn die Zahl 16 ist. Von den sechzehn möglichen Zahlen erzeugt also nur eine diese Antwort. Die Wahrscheinlichkeit beträgt somit $\frac{1}{16}$. In diesem Fall reduziert sich unsere Unsicherheit sofort auf Null, da nur noch eine einzige Möglichkeit übrig bleibt. Die ursprüngliche Unsicherheit betrug 4 Bits:

$$H_0 = \log_2(16) = 4 \text{ bits}$$

Und wenn die Unsicherheit nach der Antwort “Ja” auf Null reduziert wird:

$$H_1 = \log_2(1) = 0 \text{ bits}$$

Daraus ergibt sich ein Informationsgehalt von 4 Bits:

$$I = H_0 - H_1 = 4 - 0 = 4 \text{ bits}$$

Dies erklärt den ersten Teil der Erwartungswertgleichung. Der zweite Teil folgt demselben Prinzip, allerdings mit einem wichtigen Unterschied: Die Wahrscheinlichkeit für die Antwort “Nein” ist mit $\frac{15}{16}$ deutlich höher. Gleichzeitig verbleibt eine große Restunsicherheit H_1 , da wir lediglich eine einzige Zahl ausschließen konnten:

$$H_1 = \log_2(15) \approx 3.9069 \text{ bits}$$

Die gewonnene Information ist somit sehr klein:

$$I = 4 - 3.9069 \approx 0.0931 \text{ bits}$$

Anhand der Erwartungswertformel konnten wir zeigen, dass eine extreme Frage, die mit viel Glück direkt zum Ziel führt, in unserem Ratespiel einen erwarteten Informationsgehalt von etwa einem Drittel Bit (0,3373) hat. Prüfen wir nun, ob der Erwartungswert für Fragen, die die Hälfte der Möglichkeiten eliminieren, tatsächlich höher ist:

$$E[I] = (0.5 \times 1) + (0.5 \times 1) = 0.5 + 0.5 = 1 \text{ bit}$$

Wie erwartet beträgt der Erwartungswert genau 1 Bit, da bei jeder Antwort – ob “Ja” oder “Nein” – jeweils die Hälfte der Optionen eliminiert wird.

6.1.6. Mehr als zwei Antworten

Bisher haben wir in unserem Zahlenratespiel nur Fragen mit zwei Antwortmöglichkeiten betrachtet. Informationen, also Antworten auf Fragen, können jedoch vielfältiger sein. Wie berechnen wir die Information, wenn es mehr als zwei Antwortmöglichkeiten gibt?

Als Beispiel betrachten wir eine Urne mit farbigen Kugeln in drei Farben: Rot, Grün und Blau. Aus dieser Urne ziehen wir zwei Kugeln, wobei wir nach jedem Zug die gezogene Kugel zurück in die Urne legen. Dieses statistische Experiment bezeichnet man als “Ziehen mit Zurücklegen”.

6.2. Daten repräsentieren Information

7. Bits



Zu diesem Kapitel gibt es ein Video auf YouTube. Scanne einfach den QR-Code oder klicke in der digitalen Version des Buches auf den QR-Code.

7.1. Ist das Bit die kleinste Informationseinheit?

7.2. Was ist ein Byte

8. Codesysteme

8.1. ASCII-Code

8.2. Verallgemeinerung von Codesystemen

8.3. Unicode

8.4. RGB-Code

8.5. Code vs Codec

Der Begriff *Codec* leitet sich von den zwei Wörtern **enc**oder und **dec**oder ab. Die beiden Begriffe werden zwar ähnlich geschrieben, unterscheiden sich aber in ihrer Bedeutung. Ein Codec beschreibt ein Vorgehen oder einen Algorithmus, um Daten vor dem Senden nach einem definierten Verfahren zu kodieren und nach dem Empfang wieder zu dekodieren. Dies ist besonders sinnvoll, um Informationen effizienter zu übertragen und weniger Bandbreite zu beanspruchen. Zudem können Daten verschlüsselt und die Kommunikation dadurch sicherer gemacht werden. Wir lernen einige Methoden für beide Anwendungsfälle in einem späteren Kapitel kennen. Im Gegensatz dazu beschreibt ein Code ein System, das einer Reihe von Symbolen eine bestimmte Bedeutung zuordnet, wie wir in diesem Abschnitt gesehen haben.

9. Datenstrukturen

9.1. Listen

9.2. Mengen

9.3. Graphen

9.4. Bäume

9.5. Warteschlangen

Teil III.

Verarbeitung

10. Analog vs. Digital



Zu diesem Kapitel gibt es ein Video auf YouTube. Scanne einfach den QR-Code oder klicke in der digitalen Version des Buches auf den QR-Code.

10.1. Was ist der Unterschied zwischen der analogen und digitalen Welt?

10.1.1. Endlich viele Möglichkeiten vs. Unendlichkeit

10.1.2. Diskrete und kontinuierliche Werte

11. Speicher

11.1. Substratunabhängigkeit

12. Logik und Arithmetik

12.1. Schalter

12.1.1. Relais, Vakuumröhren und Transistoren

12.2. Logikgatter

12.3. Binäre Addition

12.4. Binäre Subtraktion

12.5. Substratunabhängigkeit

13. Computer

13.1. Komponenten eines Computers

- von Neumann-Architektur

Teil IV.

Kommunikation

14. Signale

14.1. Was ist ein Signal?

“A signal is a function that conveys information about the behavior of a system or attributes of some phenomenon”.

Ein Signal ist eine physikalische Größe, die Informationen trägt. Stellen wir uns vor, du stehst an einer Straßenecke und winkst einem Freund auf der anderen Seite zu. Deine Handbewegung ist ein **optisches Signal**, das die Information „Komm her!“ überträgt. Signale können auch Schallwellen (wie deine Stimme), elektrische Impulse (in Kabeln) oder Licht (in Glasfasern) sein

14.1.1. Der Kern ist die Veränderung

Eine statische physikalische Größe kann keine Informationen übertragen. Dies haben wir bereits im Kapitel Kapitel 6 kennengelernt. Erst die Veränderung einer physikalischen Größe über die Zeit ermöglicht es, Informationen zu kodieren und zu übertragen. Ein einfaches Beispiel ist das An- und Ausschalten einer Lampe, wobei die Veränderung der Helligkeit das Signal darstellt. Die zeitliche Abfolge dieser Veränderungen kann dann als Nachricht interpretiert werden, wie etwa beim Morsecode.

14.1.2. Häufig elektrisch

Ein Signal muss nicht unbedingt eine elektrische Größe wie Spannung (gemessen in Volt) sein. Signale können auch mechanische Größen (Druck, Beschleunigung), optische Größen (Helligkeit, Farbe) oder akustische Größen (Schallwellen) sein. Das Entscheidende ist, dass sich das Signal als messbare Größe über die Zeit verändert und dadurch Informationen transportiert.

Für die Verarbeitung mit Computern müssen wir alle Signale in elektrische Signale umwandeln. Von dort aus ist es dann ein kleiner Schritt zum digitalen Signal, das nur die Werte Null oder Eins annehmen kann. Dafür nutzen wir sogenannte **Analog-to-Digital-Converter (ADC)**.

14.2. Wie können wir Signale erzeugen?

14.2.1. Von digital zu analog

14.2.2. Die LED

14.3. Wie können wir Signale empfangen?

14.3.1. Von analog zu digital

14.3.2. Der Farbsensor

14.4. Welche Bedeutung hat ein Signal?

Ein Signal ist zunächst nur eine messbare Abfolge von Veränderungen einer physikalischen Größe über die Zeit. Die Bedeutung, die wir diesen Veränderungen – oder der Modulation – zuschreiben, bestimmen wir selbst.

15. Protokolle

15.1. Peer-To-Peer

15.2. Handshake

15.3. TCP/IP & HTTPs

- How can we communicate between two computers?
 - Protocols / Handshake
 - Netzwerk / Internet / P2P-Communication

16. Verschlüsselung

16.1. Verschlüsselung

16.1.1. Symmetrisch

- Symmetric encryption with Caesar Cipher

16.1.2. Asymmetrisch

- Assymetric with RSA Toy

16.2. Digitale Signaturen

- Digital signatures

17. Kompression

17.1. Verlustfreie Kompression

- Huffman

17.2. Verlustbehaftete Kompression

- JPEG

Literaturverzeichnis

- Adami, Christoph. 2016. „What is Information;“ *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374 (2063): 20150230. <https://doi.org/10.1098/rsta.2015.0230>.
- Brookshear, J. Glenn, und Dennis Brylow. 2020. *Computer science: an overview*. 13th edition, global edition. NY, NY: Pearson.
- Petzold, Charles. 2022. *Code: the hidden language of computer hardware and software*. 2. Aufl. Hoboken: Microsoft Press.
- Scott, John C. 2009. *But how do it know?: the basic principles of computers for everyone*. Oldsmar, FL: John C. Scott.

Index

Dijkstra-Algorithmus, [30](#)