Das Einfache im Komplexen finden

Minimalismus in Mathematik und Informatik

Lothar Budach
Universität Potsdam
Institut für Informatik
Am Neuen Palais 10
14415 Potsdam

Tel.: (0331) 977 16 08

Fax.: (0331) 977 17 20

E-mail: lbudach@haiti.cs.uni-potsdam.de

Minimalismus in der Kunst und Wissenschaft
Veranstaltungsreihe zum fünfjährigen Bestehen des interdisziplinären Zentrums für kognitive Studien in Zusammenarbeit mit dem alten Rathaus Potsdam und dem Waschhaus Potsdam e.V.

8. Juni 1999

Prinzip der Einfachheit

Wähle unter allen Erklärungen einer Erscheinung die Einfachste aus.

David Hilbert:
„das Klare und leicht Faßliche zieht uns an, das Verwickelte schreckt uns ab“

Die Erklärung für diese Neigung des Menschen zum Einfachen liefert die Psychologie: George Miller wies 1956 nach, daß die Gedächnisspanne des Kurzzeitgedächnisses etwa

$$\textbf{magical number} := 7 \pm 2$$

chunks beträgt. Dabei ist ein *chunk (Brocken, Klumpen)* eine durch ein einheitliches Symbol adressierbare Gedächnisgruppe. Der spezifische Inhalt der chunks ist irrelevant für die Gedächnisspanne.

Softwarekrise:

Widerspruch zwischen der Komplexität moderner industrieller Softwareprobleme und der intellektuellen Kapazität des Menschen.

Lösung der Softwarekrise:

Suche nach überschaubaren, verständlichen Lösungen.

Die Möglichkeit dazu liegt in der Problemstellung selbst: Komplexe Systeme sind in der Regel strukturiert. Selbst chaotische Systeme weisen eine (rekursive) Struktur auf. Die Aufdeckung bzw. Generierung der Struktur des Systems ist die wichtigste Aufgabe beim Softwaredesign.

Auch sehr komplexe Strukturen können einfach beschrieben werden – Fraktale:

Sehr einfache mathematische Iterationen können hochkomplexe geometrische Strukturen erzeugen

Beispiel: Julia-Mengen

$f : \mathbb{C} \longrightarrow \mathbb{C}$ ein Polynom, etwa die folgende Funktion:

$$x \mapsto f(x) := x^2 + c$$

Zwei Möglichkeiten:

- x ist Fluchtpunkt: $f^n(x)$ verläßt mit wachsendem n jeden Kreis um den Ursprung
- x ist Gefangenenpunkt: es gibt einen Kreis um den Ursprung, der von $f^n(x)$ niemals verlassen wird.

Flucht- und Gefangenenmenge sind nicht leer. Die Grenze zwischen beiden heißt Julia-Menge

Selbst komplizierteste Bewegungen können einfach beschrieben werden

Prinzip der kleinsten Wirkung (Hamiltonsches Prinzip):

Sei $L = L(q_1, q_2, \ldots, q_s, \dot{q}_1, \dot{q}_2, \ldots, \dot{q}_s, t) = L(q, \dot{q}, t)$ die *Lagrange-Funktion* eines mechanischen Systems (Differenz zwischen kinetischer und potentieller Energie des Systems). Die Bewegung des Systems vom Zeitpunkt t_1 zum Zeitpunkt t_2 verläuft in einer solchen Weise, dass die *Aktion* oder *Wirkung*, d.h. das Integral

$$S = \int_{t_1}^{t_2} L(q, \dot{q}, t) dt$$

den kleinstmöglichen Wert annimmt.

Thomas S. Kuhns Theorie des Paradigmenwechsels in der Geschichte der Wissenschaft

Neue wissenschaftliche Fakten zerstören die Einfachheit der Theorie. Die normale Wissenschaft sucht Belege für einfache wissenschaftliche Paradigmen. Jeder, dem Paradigma nicht etsprechende Fakt wird als Störung der Harmonie empfunden. Erst, wenn diese Störungen unerträglich werden, ersetzt ein neue, einfache und alle bekannten Erscheinungen beschreibende Erklärung das alte Paradigma (Wissenschaftliche Revolution).

Mathematik zwingt zur Vereinfachung und nutzt sie als fundamentales methodisches Prinzip

Jacob. T. Schwarz:

„Das Einfache im Komplexen finden, das Endliche im Unendlichen - das scheint mir keine schlechte Beschreibung der Aufgabe und des Wesens der Mathematik zu sein.“

G. W. Leibniz:

„Wenn die Mathematiker nicht alles gesagt haben was sie sollten, so haben sie auch nichts gesagt, was sie nicht sagen sollten. Wenn diejenigen, welche die anderen Wissenschaften gepflegt haben, die Mathematiker wenigstens in diesem Punkte nachgeahmt hätten, würden wir sehr glücklich sein“.

Die Mathematik bedient sich unterschiedlicher Methoden, das Einfache im Komplexen zu erkennen, z.B.:

- Vereinfachung und Idealisierung
- Einfachheit als Kriterium für die Auswahl grundsätzlicher Probleme
- Veranschaulichung
- Verallgemeinerung und Axiomatisierung
- Vollständige Induktion
- Erweiterung durch ideale Elemente
- Einfachheit in der Darstellung
- Abbildung auf einfachere Strukturen
- Unmöglichkeitsbeweise
- Definition einfacher (atomarer) Strukturen und Objekte, aus denen komplexe Strukturen aufgebaut werden können

Vereinfachung und Idealisierung

Beispiel: Punkt

Körper, dessen Ausmaße man vernachlässigen kann. Ein ganzer Planet kann als Punkt betrachtet werden. Ein bewegter Punkt ist durch seine Position $q = (x, z, y)$ und durch seine Geschwindigkeit $\dot{q} = \left(\frac{dx}{dt}, \frac{dy}{dt}, \frac{dz}{dt}\right) = (\dot{x}, \dot{y}, \dot{z})$ charakterisiert.

Vereinfachung und Idealisierung II

Beispiel: Natürliche Zahl

H. Hasse: „Nach Kronecker hat sie der liebe Gott geschaffen, nach Dedekind der menschliche Geist. Das ist je nach Weltanschauung ein unlösbarer Widerspruch oder ein und dasselbe."

Dedekind: Zahl = Abstraktion einer Klasse gleichmächtiger Mengen.
Die gesamte Mathematik kann man letztendlich auf die natürlichen Zahlen reduzieren.

E. Borel:

„Es ist bekannt, daß die Kenntnisse des Menschen die Bezeichnung Wissenschaft in Abhängigkeit davon verdienen, welche Rolle in diesen Kenntnissen die Zahl spielt".

Vereinfachung und Idealisierung III

Komplizierteste Zusammenhänge werden durch einfachste Zeichnungen veranschaulicht.

Komplizierte Theorien gelten als bestätigt, wenn sie sich an einfachen Beispielen bewähren

Komplizierte Algorithmen werden an einfachen Beispielen getestet

Vereinfachung und Idealisierung IV

Kolmogorov-Komplexität:

Komplexität der Beschreibung eines Sachverhaltes S: Größe $C(S)$ eines kleinsten Programms zur Beschreibung von S.

Ein Objekt S der Größe n (Zeichenkette aus n Zeichen oder ein Bild aus n Pixeln) heißt zufällig, falls $C(S) \approx n$ ist.

S heißt einfach, falls $C(S)$ beschränkt ist.

Vereinfachung und Idealisierung V

Rechtfertigung der Einfachheit für Softwaretests:

Ein Softwaresystem, das sich beim Test durch kleine bzw. zufällige Eingabeobjekte als korrekt erwiesen hat, ist korrekt.

Einfachheit als Kriterium für die Auswahl grundsätzlicher Probleme

David Hilbert:

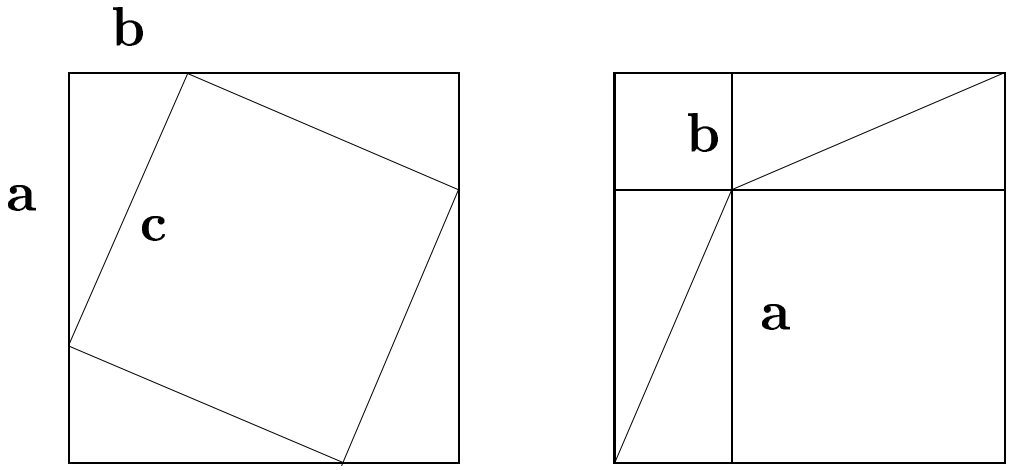
Ein alter französischer Mathematiker hat gesagt: Eine mathematische Theorie ist nicht eher als vollkommen anzusehen, als bis du sie so klar gemacht hast, daß du sie dem ersten Mann erklären könntest, den du auf der Straße triffst. Diese Klarheit und leichte Faßlichkeit, wie sie hier so drastisch für eine mathematische Theorie verlangt wird, möchte ich vielmehr von einem mathematischen Problem fordern, wenn dasselbe vollkommen sein soll.

Veranschaulichung

Durch geeignete Veranschaulichungen werden mathematische Sachverhalte offensichtlich.

Beispiel: Der altindische Beweis des pythgoräischen Lehrsatzes

$$a^2 + b^2 = c^2$$



Verallgemeinerung und Axiomatisierung

Herausarbeiten fundamentaler, zumeist einfach formulierbarer Gemeinsamkeiten unterschiedlicher komplexer Strukturen

David Hilbert

Wenn uns die Beantwortung eines mathematischen Problems nicht gelingen will, so liegt häufig der Grund darin, daß wir noch nicht den allgemeineren Gesichtspunkt erkannt haben, von dem aus das vorgelegte Problem nur als einzelnes Glied einer Kette verwandter Probleme erscheint. Nach Auffinden dieses Gesichtspunktes wird häufig nicht nur das vorgelegte Problem unserer Erforschung zugänglicher, sondern wir gelangen so sogleich in den Besitz einer Methode, die auf die verwandten Probleme anwendbar ist.

Verallgemeinerung und Axiomatisierung II

Pythagoreer, Euklid (etwa 365 v.u.Z.):

Jede natürliche Zahl ist Produkt von Primzahlen

R. Dedekind 1871:

In einer Hauptordnung eines algebraischen Zahlkörpers ist jedes Ideal Produkt von Primidealen

E. Lasker 1905:

In einem Polynomring $k[x_1, x_2, \ldots, x_n]$ ist jedes Ideal Durchschnitt von endlich vielen Primäridealen

Verallgemeinerung durch E. Noether 1919-1921:

In einem kommutativen Ring mit Teilerkettensatz ist jedes Ideal Durchschnitt von Primäridealen.

Verallgemeinerung und Axiomatisierung III

Beweis des Noetherschen Zerlegungssatzes

Sei $\mathfrak{a}$ ein nichtprimäres Ideal. Es gibt Elemente $b, c \notin \mathfrak{a}$ mit $bc \in \mathfrak{a}$ und $b^\rho \notin \mathfrak{a}$ für alle natürlichen Zahlen ρ. Sei $\mathfrak{a}_\rho = \mathfrak{a} : (b^\rho)$. Dann ist

$$\mathfrak{a} \subset \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \cdots \subseteq \mathfrak{a}_\rho \subseteq \cdots .$$

Wegen des Teilerkettensatzes gibt es ein ρ mit $\mathfrak{a}_\rho = \mathfrak{a}_{\rho+1}$. Daraus folgt aber

$$\mathfrak{a} = \mathfrak{a}_\rho \cap (\mathfrak{a} + (b^\rho)),$$

eine Durchschnittsdarstellung von $\mathfrak{a}$ durch echte Oberideale.

Verallgemeinerung und Axiomatisierung IV

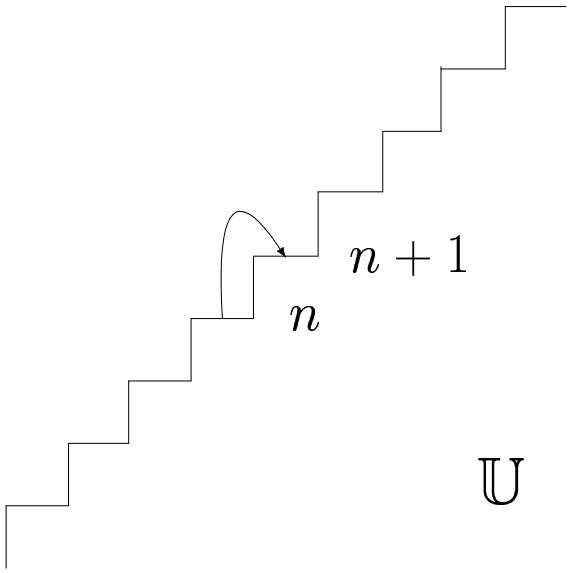
- Also ist jedes nichtprimäre Ideal Durchschnitt echter Oberideale.
- Sei $\mathfrak{A}$ die Menge aller Ideale, die nicht Durchschnitt von Primäridealen sind. Ist $\mathfrak{a} \in \mathfrak{A}$, so ist $\mathfrak{a}$ Durchschnitt echter Oberideale, von denen natürlich wenigstens eines in $\mathfrak{A}$ ist. Also ist jedes Element von $\mathfrak{A}$ in einem größeren Element von $\mathfrak{A}$ enthalten. Das geht wegen des Teilerkettensatzes nicht. $\Rightarrow \mathfrak{A} = \emptyset$.

Vollständige Induktion

Die Vollständige Induktion basiert auf dem folgenden Sachverhalt (5. Peanosches Axiom)

Sei $\mathbb{U}$ eine Teilmenge der natürlichen Zahlen $\mathbb{N}$.

- $0 \in \mathbb{U}$
- $n \in \mathbb{U} \Rightarrow n + 1 \in \mathbb{U}$



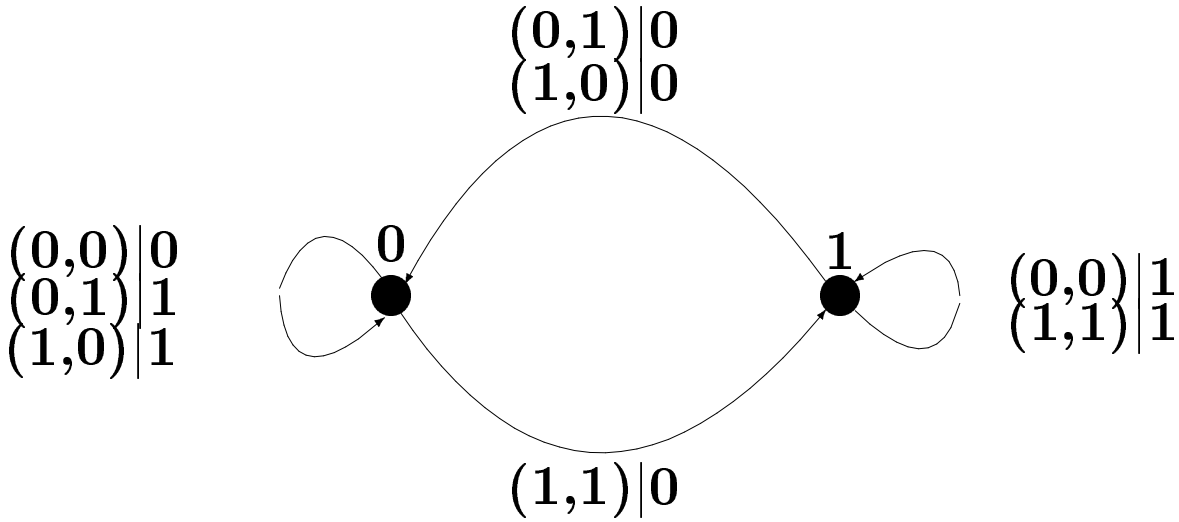
Dann ist $\mathbb{U} = \mathbb{N}$

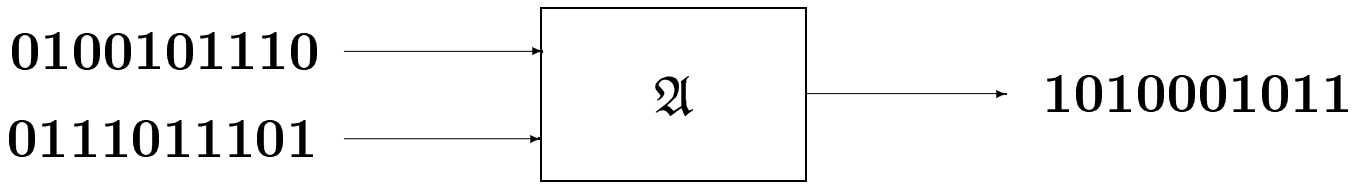
Vollständige Induktion II

Endlicher Automat:

λ	0	1
(0,0)	0	1
(0,1)	1	0
(1,0)	1	0
(1,1)	0	1

δ	0	1
(0,0)	0	0
(0,1)	0	1
(1,0)	0	1
(1,1)	1	1





$$2\ \delta(i,(a_0,b_0)) + \lambda(i,(a_0,b_0)) = i + a_0 + b_0$$

Vollständige Induktion III

$\mathfrak{A}$ realisiert die Addition zweier binär kodierter Zahlen.

Beweis

Wir betrachten die Automaten $\mathfrak{A}_i, i = 0, 1$, die beide mit $\mathfrak{A}$ übereinstimmen und sich nur um den initialen Zustand i unterscheiden. Sei $\mathfrak{A}_i(\alpha, \beta)$ die Ausgabe von $\mathfrak{A}_i$ bei Eingabe von α und β.

Sei $\mathbb{N}_n$ die Menge aller $(n+1)$-stelligen Zahlen, die mit einer Null beginnen.

Sei $\alpha = a_{n+1}a_n \ldots a_0$, $\beta = b_{n+1}b_n \ldots b_0 \in \mathbb{N}_{n+1}$.

$\alpha' := a_{n+1}a_n \ldots a_1$, $\beta := b_{n+1}b_n \ldots b_1 \in \mathbb{N}_n$.

Es gilt

$$\begin{aligned}
&\alpha = 2\alpha' + a_0 \\
&\beta = 2\beta' + b_0 \\
&\mathfrak{A}_i(\alpha, \beta) = 2\ \mathfrak{A}_{\delta(i,(a_0,b_0))}(\alpha', \beta') + \lambda(a_0, b_0)
\end{aligned}$$

Vollständige Induktion IV

$$\mathbb{U} := \{n \in \mathbb{N} \mid \mathfrak{A}_i(\alpha, \beta) = \alpha + \beta + i \text{für } i = 0, 1:\}$$

- $0 \in \mathbb{U}$.
- $n \in \mathbb{U} \Rightarrow n + 1 \in \mathbb{U}$, da

$$\begin{array}{ll} \mathfrak{A}_i(\alpha, \beta) & = \\ 2\ \mathfrak{A}_{\delta(i,(a_0,b_0))}(\alpha', \beta') + \lambda(i, (a_0, b_0)) & = \\ 2\ (\alpha' + \beta' + \delta(i, (a_0, b_0)) + \lambda(i, (a_0, b_0)) & = \\ 2\ (\alpha' + \beta') + i + a_0 + b_0 & = \\ \alpha + \beta + i & \end{array}$$

Erweiterung durch ideale Elemente

Durch die Erweiterung der reellen Zahlen durch die Zahl $i = \sqrt{-1}$ vereinfachen sich viele Zusammenhänge:

Die Funktionen

$$\begin{aligned} \sin(x) &= x - \tfrac{x^3}{3!} + \tfrac{x^5}{5!} - + \cdots \\ \cos(x) &= 1 - \tfrac{x^2}{2!} + \tfrac{x^4}{4!} - + \cdots \\ e^x &= 1 + x + \tfrac{x^2}{2!} + \tfrac{x^3}{3!} + \tfrac{x^4}{4!} + \tfrac{x^5}{5!} + \cdots \end{aligned}$$

haben als reelle Funktionen wenig Gemeinsamkeiten. Betrachtet man sie als komplexe Funktionen, so erhält man:

$$\begin{aligned} i\sin\ x &= & i\ x & & -i\ \tfrac{x^3}{3!} & & +i\ \tfrac{x^5}{5!} & -+\ \cdots \\ \cos\ x &= 1 & & -\ \tfrac{x^2}{2!} & & +\ \tfrac{x^4}{4!} & & -+\ \cdots \\ e^{ix} &= 1 & +i\ x & +i^2\ \tfrac{x^2}{2!} & +i^3\ \tfrac{x^3}{3!} & +i^4\ \tfrac{x^4}{4!} & +i^5\ \tfrac{x^5}{5!} & +\ \cdots \end{aligned}$$

Da $i^2 = -1$ ist, ergeben sich die Eulerschen Formeln:

$$\begin{aligned} e^{ix} &= \cos\ x + i\sin\ x \\ \cos\ x &= \tfrac{e^{ix}+e^{-ix}}{2} \\ \sin\ x &= \tfrac{e^{ix}-e^{-ix}}{2i} \end{aligned}$$

Erweiterung durch ideale Elemente II

Aus den Potenzgesetzen folgen die Additionstheoreme

$$a^x a^y = a^{x+y} \Rightarrow$$

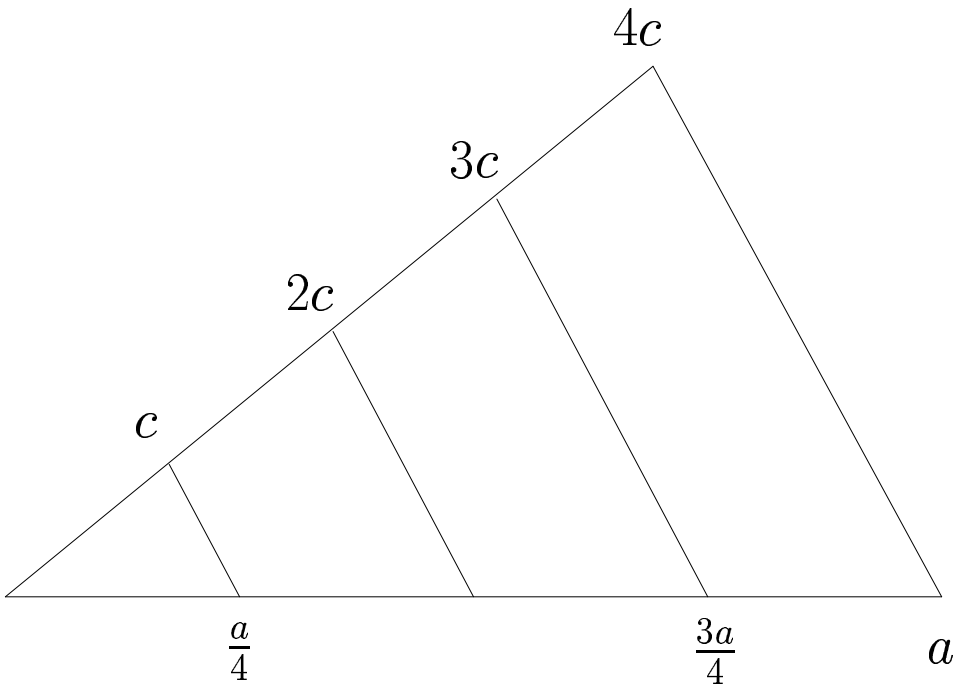
$$\begin{aligned}\cos\,(x+y) &= e^{i(x+y)} + e^{-i(x+y)} \big/\, 2 \\ &= e^{ix}e^{iy} + e^{-ix}e^{-iy} \big/\, 2\end{aligned}$$

$$\begin{aligned}&= \tfrac{1}{2}(\ \ (\cos x + i\sin x)(\cos y + i\sin y) \\ &\quad +\ (\cos x - i\sin x)(\cos y - i\sin y)) \\ &= \tfrac{1}{2}(\ \ \cos x\cos y - \sin x\sin y + i\sin x\cos y + i\cos x\sin y \\ &\quad +\ \cos x\cos y - \sin x\sin y - i\sin x\cos y - i\cos x\sin y)\end{aligned}$$

$$\cos\,(x+y) = \cos\ x\cos\ y - \sin\ x\sin\ y$$

Einfachheit in der Darstellung

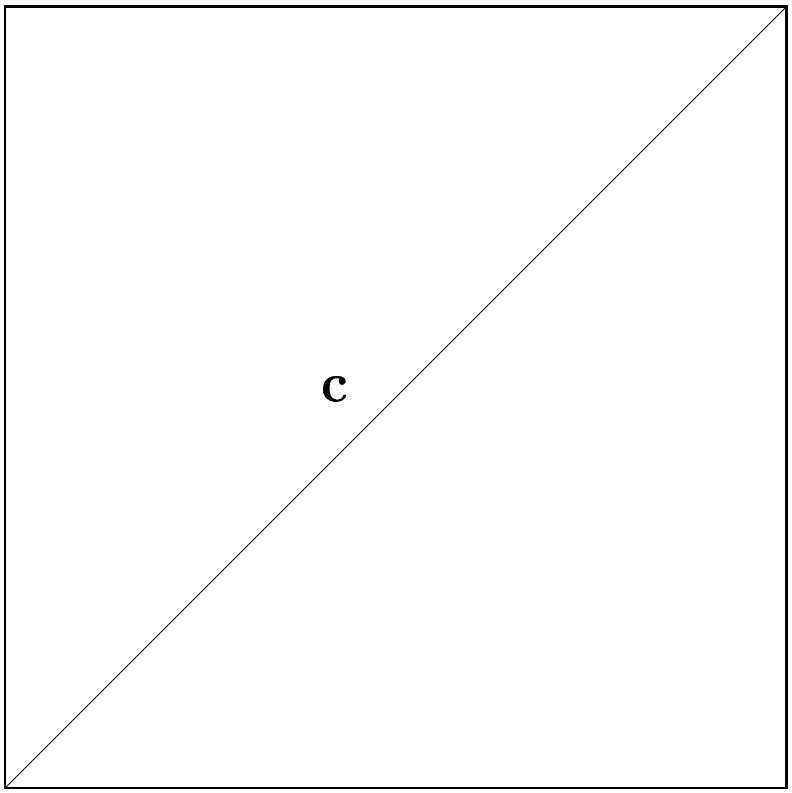
Kommensurabilität: Geometrische Darstellung rationaler Zahlen



Hippasos von Metapontum (etwa 420 v.u.Z.) bewies, daß es nicht kommensurable Strecken gibt. Es heißt, das Pythagoras ihn dafür zum Tode verurteilte. Er kam als ein Gottloser im Meere um.

Einfachheit in der Darstellung II

$\sqrt{2}$ ist irrational



Pythagoräischer Lehrsatz: $d^2 = 2a$, d.h. $d = \sqrt{2}a$.

Euklid im 10. Buch seiner *Elemente*: a ist zu d inkommensurabel.

Einfachheit in der Darstellung III

Sei $d = pe,\ a = qe \Rightarrow pe = \sqrt{2}a = \sqrt{2}qe$

$p = \sqrt{2}q$, $\sqrt{2} = \frac{p}{q}$ (p und q natürliche Zahlen).

Annahme (stets möglich): p und q teilerfremd.

$p^2 = 2q^2$, $2|p^2 \Rightarrow 2|p \Rightarrow p = 2r$
$p^2 = 4r^2 = 2q^2 \Rightarrow 2r^2 = q^2 \Rightarrow 2|q^2$
$2|q$, $q = 2s$.

Schlußfolgerung: p und q haben den gemeinsamen Teiler 2

Widerspruch!

Nur dadurch zu erklären, daß die Voraussetzung
$p = \sqrt{2}q$, $p, q \in \mathbb{N}$ falsch war.

Einfachheit in der Darstellung IV

$\sqrt{2}$ ist ein unendlicher, nichtperiodischer Dezimalbruch.

$$\begin{aligned}\sqrt{2} = 1,41421\ &35623\ 73095\ 04880\ 16887\\ &24209\ \ 69807\ 85696\ 71875\ 37694\\ &80731\ \ 76679\ 73799\ 07324\ 78462\\ &10703\ \ 88503\ 87534\ 32764\ 15727\ \ldots\end{aligned}$$

Eine rationale Zahl ist ein endlicher oder periodischer Dezimalbruch

Einfachheit in der Darstellung V

Kettenbruchentwicklung einer rationalen Zahl:

$$\begin{aligned}
\frac{65}{19} &= 3 + \frac{8}{19} = 3 + \frac{1}{\frac{19}{8}} \\
&= 3 + \frac{1}{2 + \frac{3}{8}} = 3 + \frac{1}{2 + \frac{1}{\frac{8}{3}}} \\
&= 3 + \frac{1}{2 + \frac{1}{2 + \frac{2}{3}}} = 3 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\frac{3}{2}}}} \\
&= 3 + \frac{1}{2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2}}}} = 3 + [2, 2, 1]
\end{aligned}$$

Einfachheit in der Darstellung VI

Auch $\sqrt{2}$ kann man als Kettenbruch entwickeln: $\sqrt{2}-1$ ist Wurzel des Polynoms x^2+2x-1. Aus $x^2+2x-1=0$ ergibt sich: $x\,(x+2)=1$, d.h. $x=\frac{1}{2+x}$. Folglich:

$$x=\frac{1}{2+x}=\frac{1}{2+\frac{1}{2+x}}=$$
$$=\frac{1}{2+\frac{1}{2+\frac{1}{2+x}}}=\frac{1}{2+\frac{1}{2+\frac{1}{2+\frac{1}{2+x}}}}$$

Damit ergibt sich:

$$\sqrt{2}=1+\frac{1}{2+\frac{1}{2+\frac{1}{2+\frac{1}{2+\cdots}}}}=1+[2,2,2,2,\cdots].$$

$\sqrt{2}$ ist ein periodischer Kettenbruch.

Abbildung auf einfachere Strukturen

Schon die Griechen konnten quadratische Gleichungen

$$x^2 + px + q = 0$$

lösen. Schreibt man eine solche Gleichung in der Form

$$x^2 + 2\frac{p}{2}x + \left(\frac{p}{2}\right) + \left(q - \left(\frac{p}{2}\right)^2\right) = 0,$$

so erkennt man, daß sie zur Gleichung

$$\left(x + \frac{p}{2}\right)^2 = \left(\frac{p}{2}\right)^2 - q$$

äquivalent ist und daher die Lösungen

$$x_{1,2} = -\frac{p}{2} \stackrel{+}{-} \sqrt{\left(\frac{p}{2}\right)^2 - q}$$

besitzt.

Gibt es derartige Lösungsformeln auch für Gleichungen höheren Grades?

Abbildung auf einfachere Strukturen II

In der Renaissance konnten auch Lösungen der Gleichungen dritten und vierten Grades gefunden werden, in denen nur die vier rationalen Rechenoperationen und die Bildung von Radikalen (Wurzeloperationen) Verwendung fanden. (Sc. del Ferro (1465-1526), N. Tartaglia(1500-1557), G. Cardano (1501-1576), L. Ferrari (1522-1565), J. Hudde (1628-1704),E. W. von Tschirnhaus (1651-1708), L. Euler (1707-1783), E. Bezout (1730-1783)).

$$x^3 + ax^2 + bx + c = 0$$

$$\begin{aligned} x_1 &= w + w',\ x_2 = \bar{\rho}w + \rho w',\ x_3 = \rho w', \\ w &= \sqrt{-\tfrac{q}{2} + \sqrt{\left(\tfrac{q}{2}\right)^2 + \left(\tfrac{p}{3}\right)^3}}, \\ w' &= \sqrt{-\tfrac{q}{2} - \sqrt{\left(\tfrac{q}{2}\right)^2 + \left(\tfrac{p}{3}\right)^3}}, \\ \text{und} \quad & \rho,\ \bar{\rho} \text{ sind die dritten Einheitswurzeln:} \\ \rho &= \tfrac{-1+\sqrt{-3}}{2},\ \bar{\rho} = \tfrac{-1-\sqrt{-3}}{2}. \end{aligned}$$

Abbildung auf einfachere Strukturen III

Gibt es auch Lösungsformeln für Gleichungen höheren als vierten Grades?

Galoissche Theorie

Jedem irreduziblen Polynom ordnet man seinen Zerfällungskörper K zu. Das sind alle Zahlen, die sich mittels der rationalen Operationen Addition, Subtraktion, Multiplikation und Division aus der 1 und aus allen Nullstellen des Polynoms bilden lassen.

Ein Automorphismus ist eine Abbildung, die alle rationalen Grundoperationen erhält. Die Menge aller Automorphismen von K, die einen Unterkörper k (d.h. eine Teilmenge von K, aus der die rationalen operationen nicht herausführen) elementweise festlassen, bildet eine Gruppe $\mathbf{Gal}(K|k)$. Diese Gruppe wurde von E. GALOIS eingeführt und wird nach ihm als **Galoissche Gruppe** von K über k bezeichnet.

Abbildung auf einfachere Strukturen IV

$$k \subseteq E \subseteq K$$

K Zerfällungskörper eines irreduziblen Polynoms,
E Zwischenkörper.

$$E \mapsto H = \mathbf{Gal}(K|E) \subseteq \mathbf{Gal}(K|k)$$

$\mathbf{Gal}(K|E) :=$ alle Automorphismen φ, für die $\varphi(a) = a$ für alle $a \in E$ ist.
Ist H eine beliebige Untergruppe von G.

$$H \mapsto K^H$$

$K^H :=$ alle $a \in K$, für die $\varphi(a) = a$ für alle $\varphi \in H$ ist.

Abbildung auf einfachere Strukturen V

Hauptsatz der Galoisschen Theorie

Untergruppen von $G = \mathbf{Gal}(K|k)$
und Körper E mit $k \subseteq E \subseteq K$
entsprechen sich eineindeutig. Dabei gilt:

$$\begin{aligned} E_1 \subseteq E_2 &\implies \mathbf{Gal}(K|E_2) \subseteq \mathbf{Gal}(K|E_1) \\ H_1 \subseteq H_2 &\implies K^{H_2} \subseteq K^{H_1}, \end{aligned}$$

d. h. bei dieser Entsprechung kehren sich die Inklusionsbeziehungen um.

$$\begin{aligned} E &= K^{\mathbf{Gal}(K|E)}, \\ H &= \mathbf{Gal}(K|K^H). \end{aligned}$$

Abbildung auf einfachere Strukturen VI

Satz 0.1 *Ist K der Zerfällungskörper eines Primpolynoms $f(x)$, so gibt es genau dann für $f(x) = 0$ eine Lösungsformel (genauer: $f(x) = 0$ ist genau dann durch Radikale auflösbar), wenn die Galoisgruppe $\mathbf{Gal}(K|k)$ auflösbar ist.*

Abbildung auf einfachere Strukturen VII

Satz 0.2 *Die alternierenden Gruppen A_n sind für $n > 4$ einfache Gruppen, d.h. sie besitzen außer sich selbst und der Einheitsgruppe $E = \{\epsilon\}$ keine weiteren Normalteiler. Demzufolge ist S_n für $n > 4$ nicht auflösbar.*

Demzufolge gibt es keine Lösungsformel für Gleichungen höheren als vierten Grades.

Abbildung auf einfachere Strukturen in der Informatik

Hierarchie als Prinzip zur Reduktion komplexer Zusammenhänge auf einfachere

- Basisdatentypen
- Namensräume
- das Modulprinzip
- **Teilen und Herrschen** (divide et impera, divide and conquer): Abstraktionsprinzip des Verbergens von Information (*information hiding, Geheimhaltungsprinzip*)
- **Separierung der Sichten** (separation of concerns), Abstraktionsprinzip des Weglassens von Information (*information neglection*)

Abbildung auf einfachere Strukturen in der Informatik II

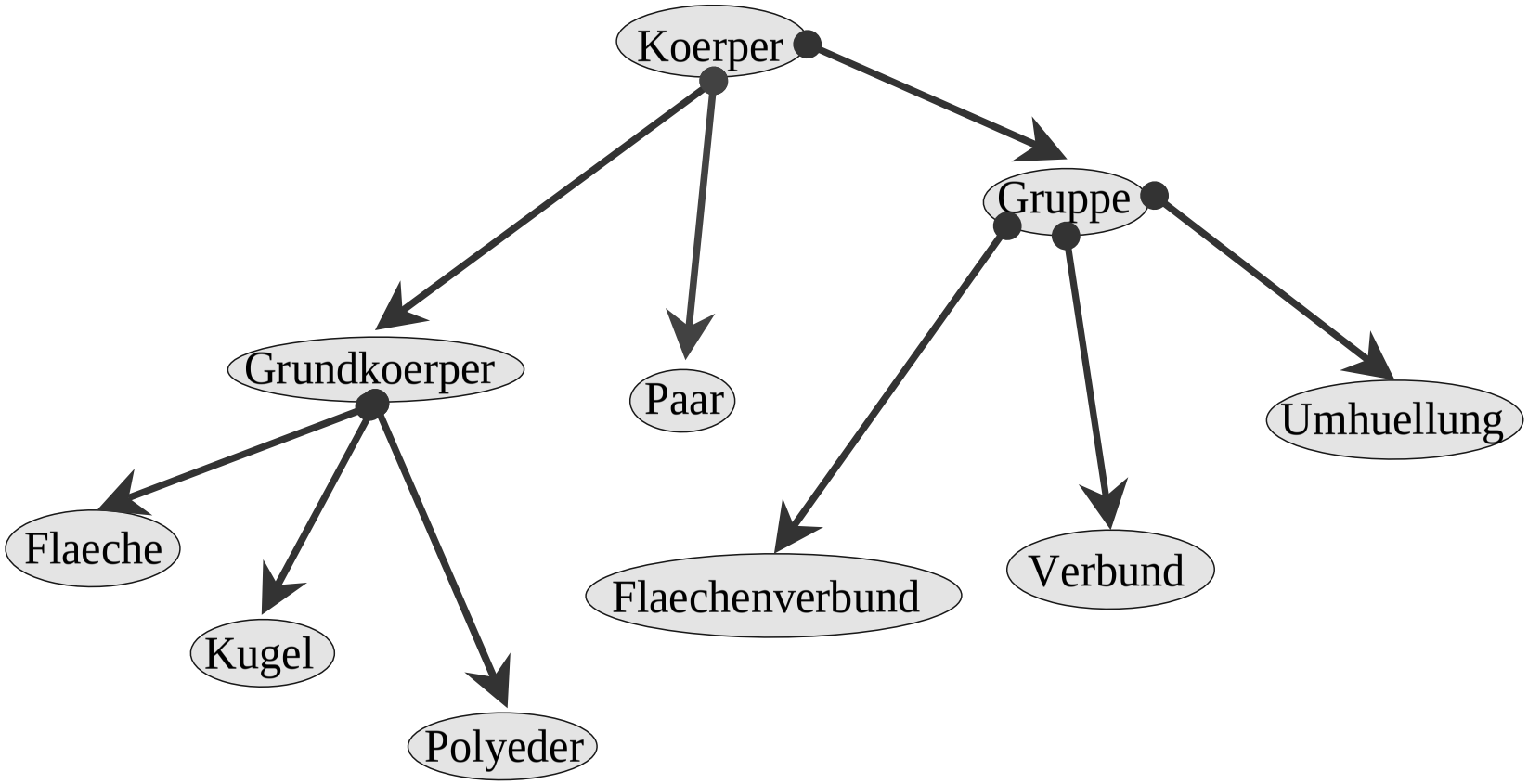
Graphen als einfaches Beschreibungsmittel komplexer Zusammenhänge Quadrupel $\Gamma = (V, E, H, o, t)$ mit

- V: Knoten
- E: Kanten
- $o, t : E \longrightarrow V$; $o(e)$ ist der Anfang, $t(e)$ ist das Ende der Kante e

Erstaunlicherweise lassen sich Elemente aller bekannten konkreten mathematischen Strukturen durch Graphen modellieren

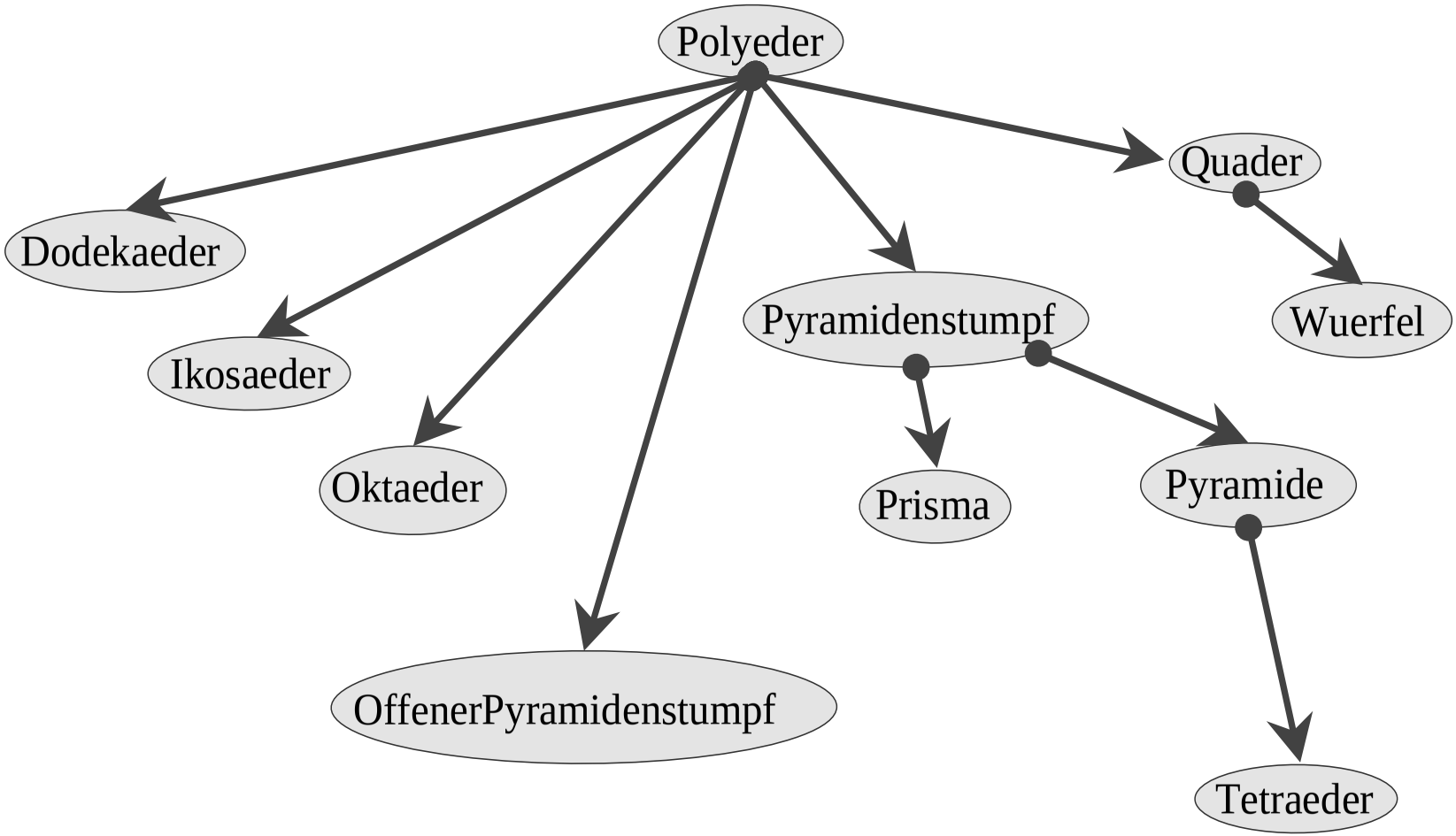
Die Klassenhierarchie der geometrischen Objekte

I

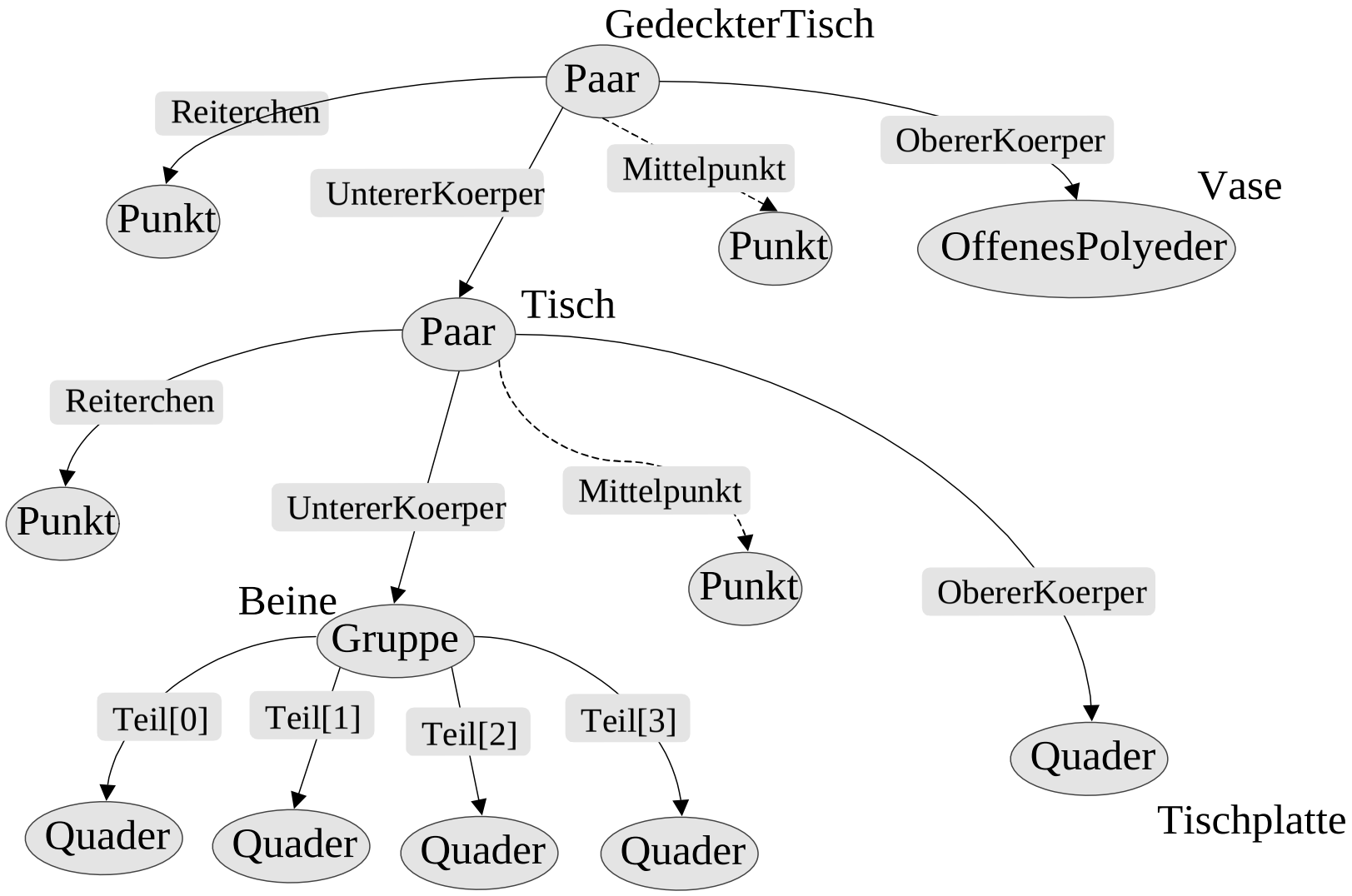


Die Klassenhierarchie der geometrischen Objekte

II



Konstruktion eines Körpers



Unmöglichkeitsbeweise

Um zu zeigen, daß ein *Etwas*, das bestimmten Anforderungen genügt, nicht existiert, wird dieses *Etwas*, falls es existieren würde, möglichst einfach beschrieben, um dann zu zeigen, daß etwas **so einfaches** den beschriebenen Anforderungen nicht genügen kann.

Beispiele:

- Das zehnte Hilbertsche Problem und die Entwicklung des Algorithmenbegriffs
- untere Schranken als terra incognita der Informatik
- Das Labyrinthproblem

Unmöglichkeitsbeweise II

SHANNONs kybernetische Maus:

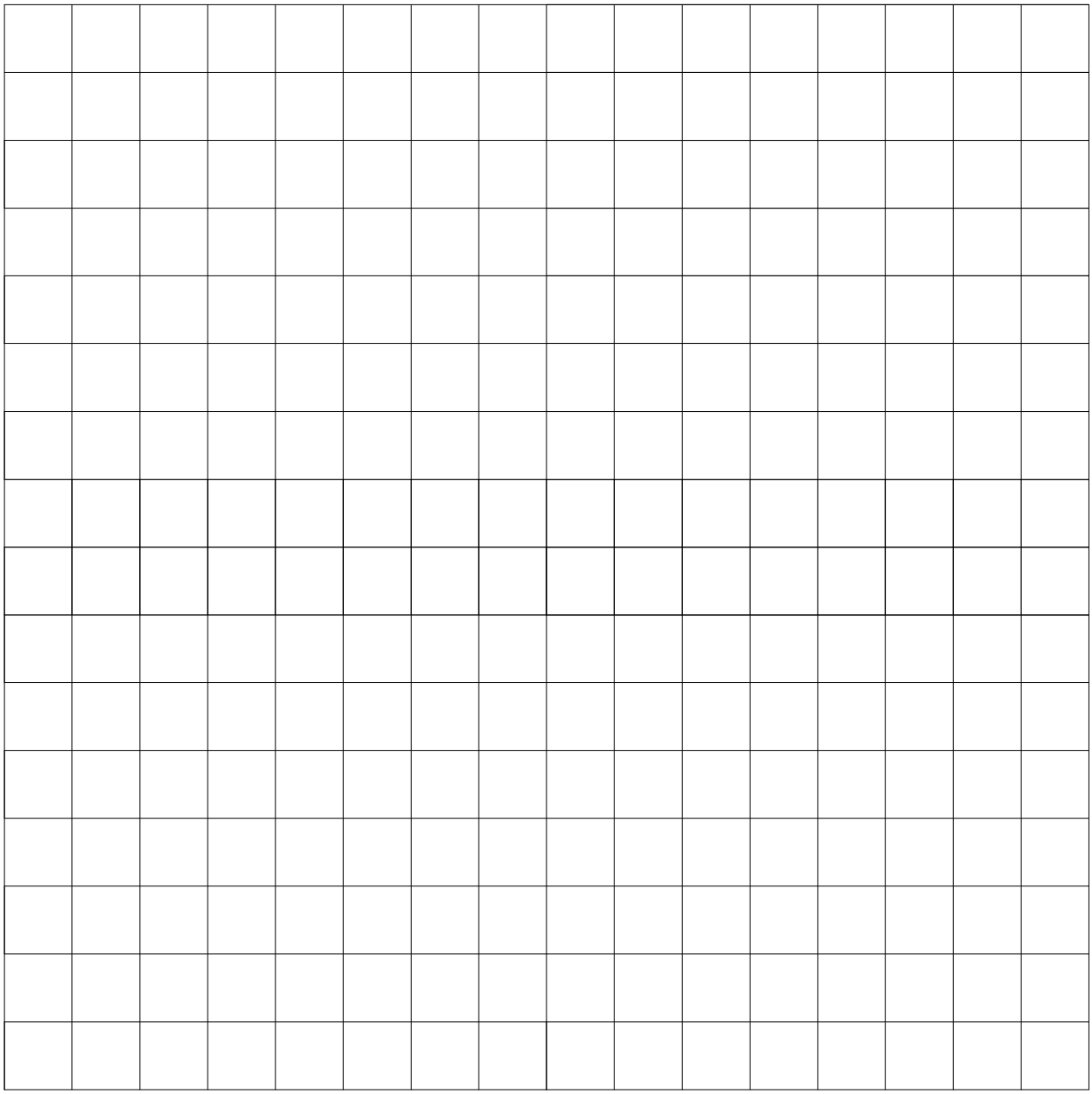
$\mathfrak{A} = (Y, X, S, \delta, \lambda, s_0)$

- $X = \{n, s, o, w\}$
- $Y = 2^X =$ alle Teilmengen von X
- S ist die endliche Menge der Zustände der Maus
- $\delta : S \times Y \longrightarrow S$
- $\lambda : S \times Y \longrightarrow X$
- $s_0 \in S$ ist der Startzustand
- Eine Bedingung: Für alle $s \in S$ gilt: $\lambda(s, y) \in y$ – die Maus geht nicht durch Wände hindurch.

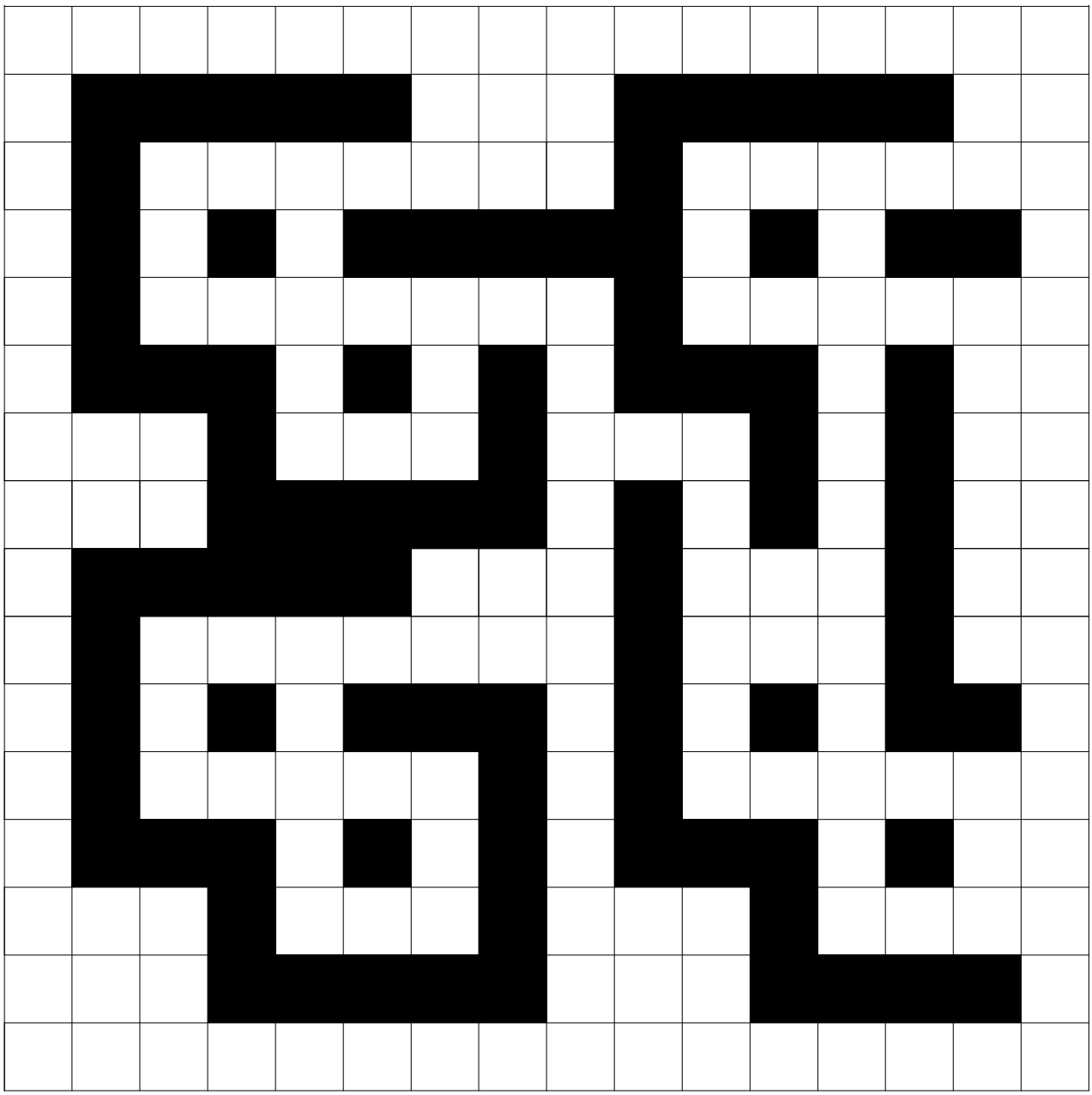
Unmöglichkeitsbeweise III

Es gibt keine Maus, die in der Lage ist, aus allen Labyrinthen auszubrechen.
(Eine Maus bricht aus einem Labyrinth aus, falls sie sich beliebig weit von ihrem Startpunkt entfernt.

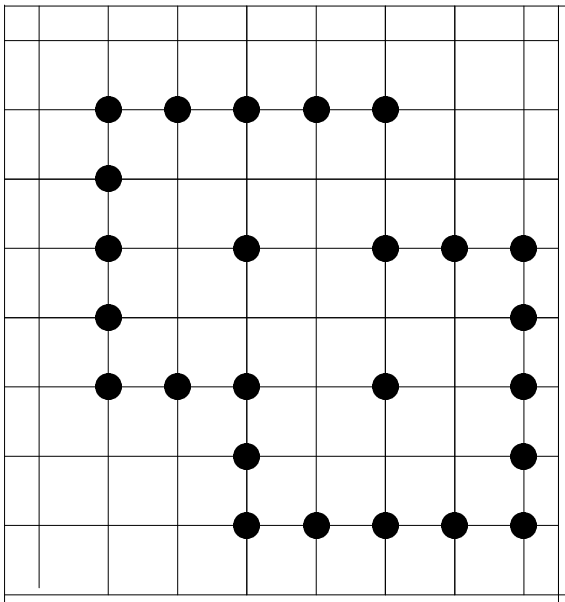
Ein leeres Schachbrett



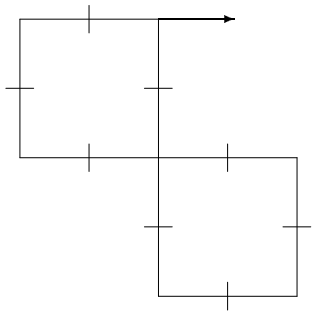
Labyrinth als verallgemeinertes Schachbrett



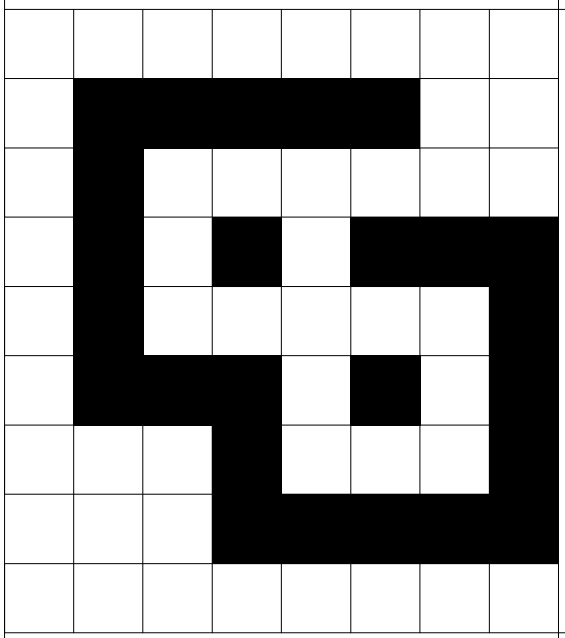
Verschiedene Darstellungen eines Labyrinths



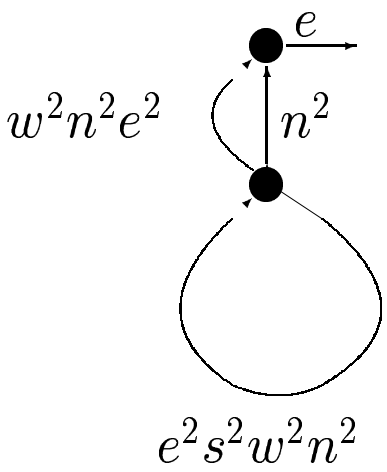
Gitter



Reduziertes Gitter

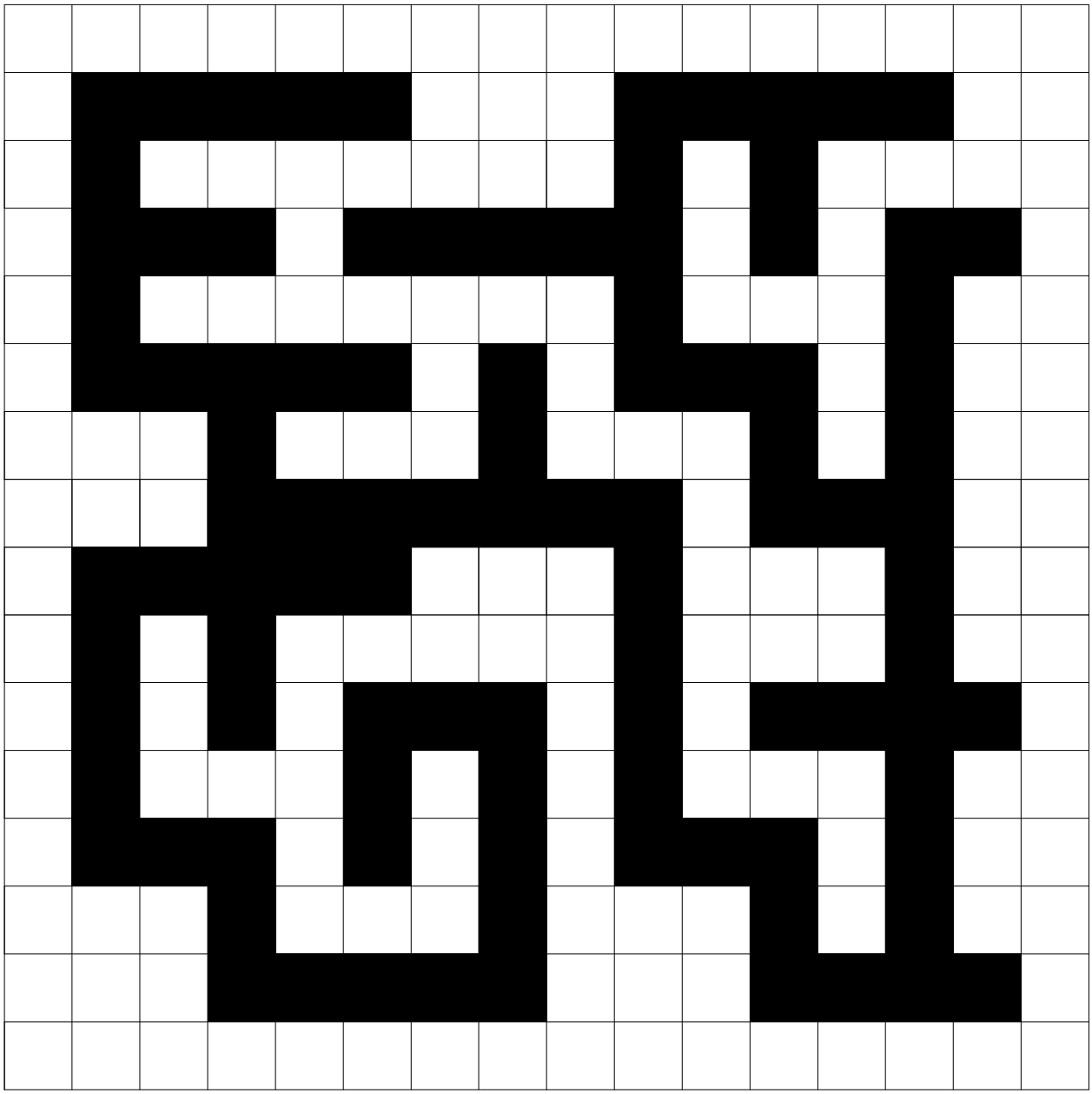


Labyrinth

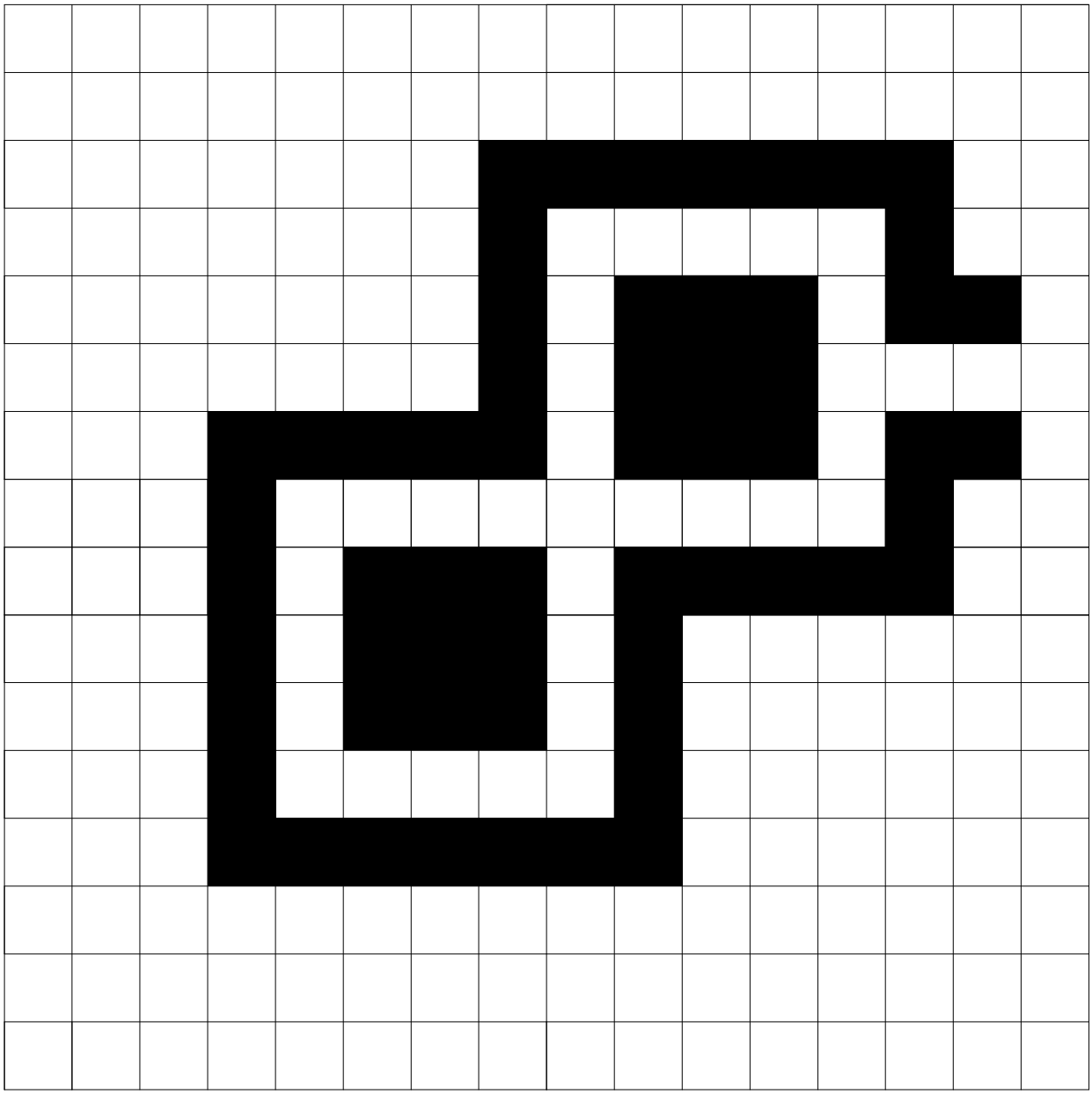


Prälabyrinth

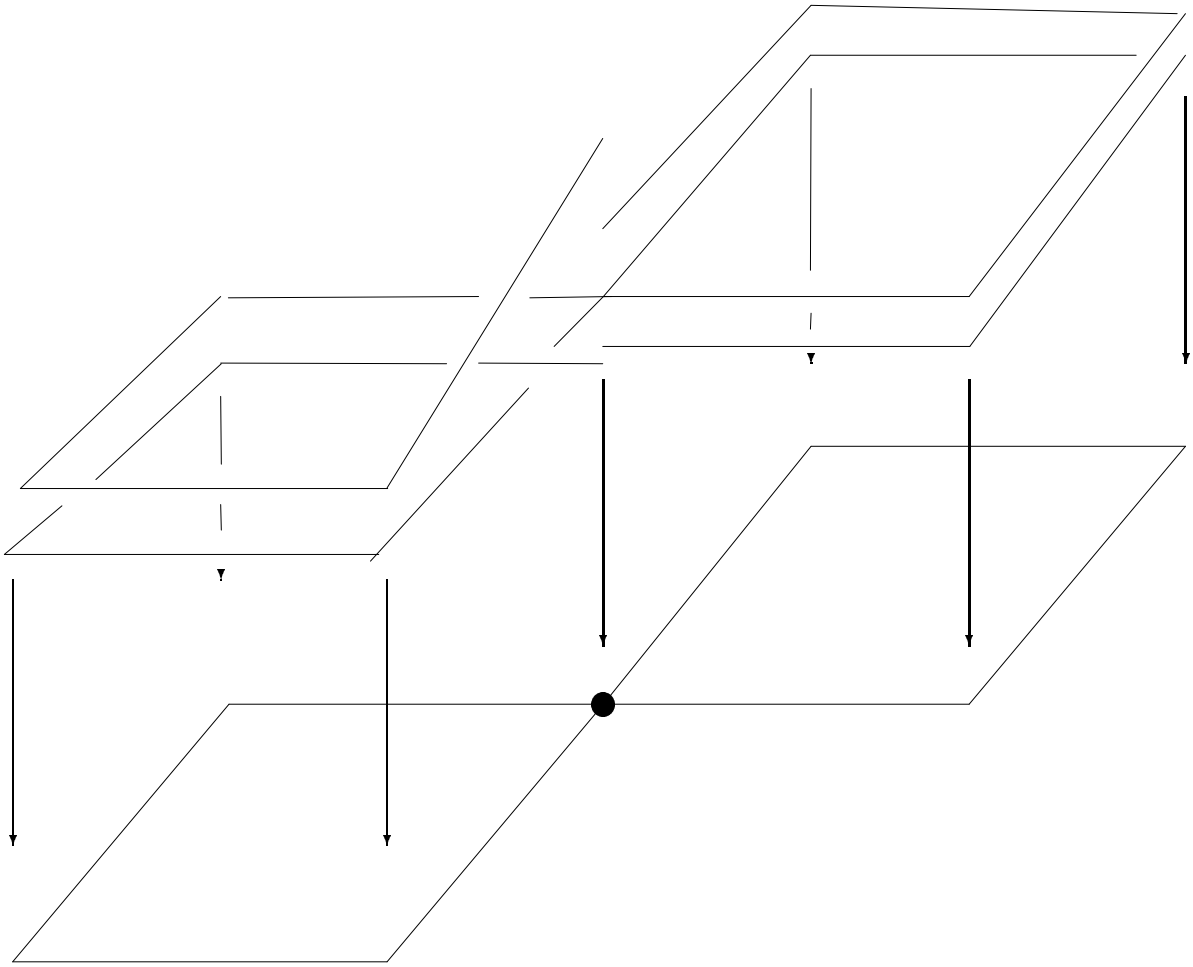
Labyrinth mit nur einer Mauer



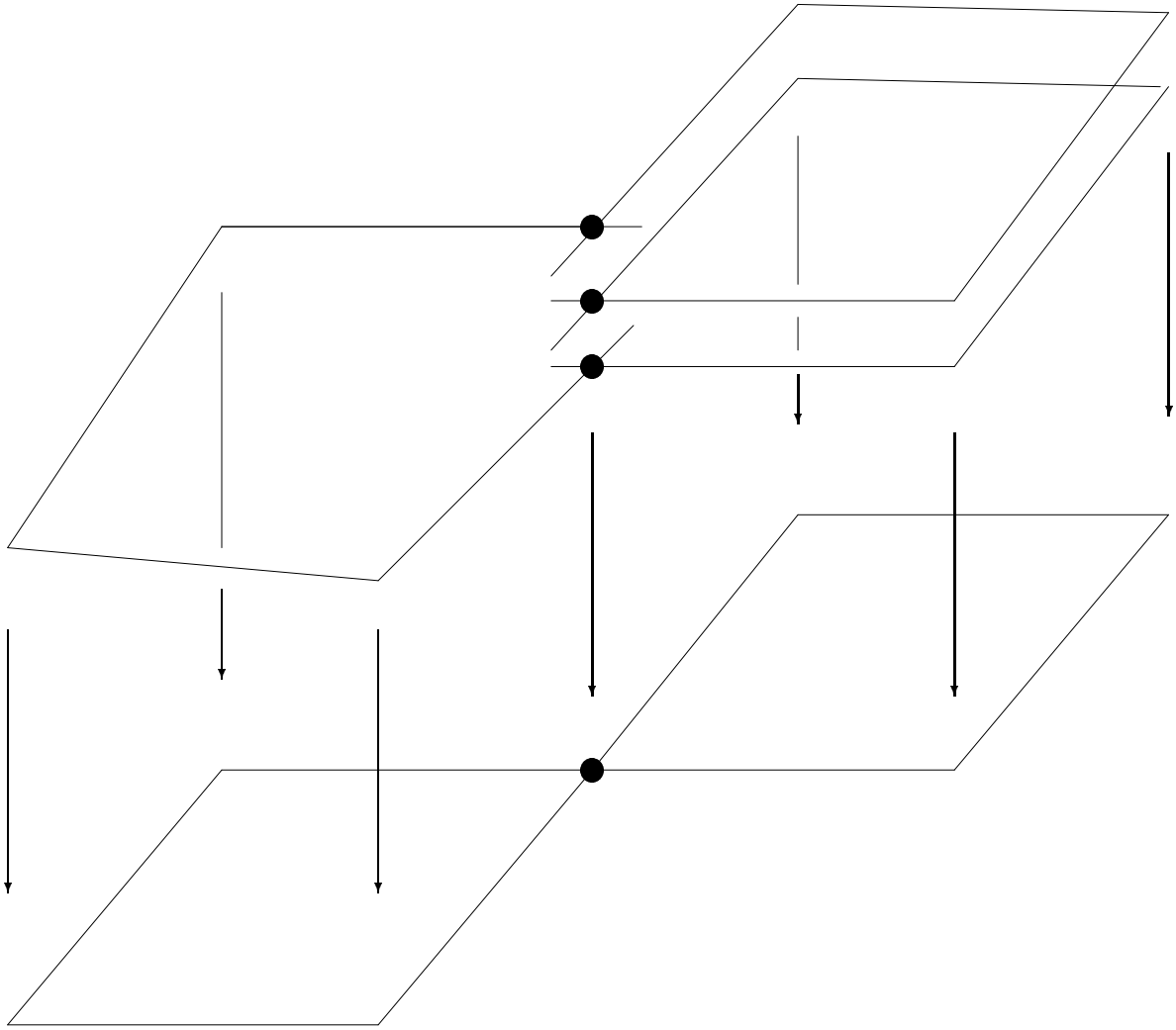
Labyrinth mit drei Mauern



Der Faden der Ariadne

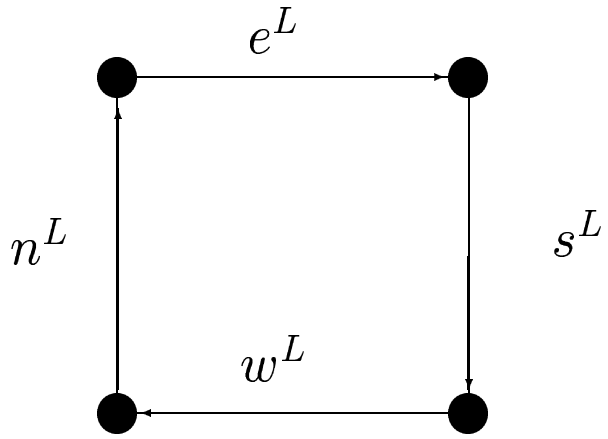


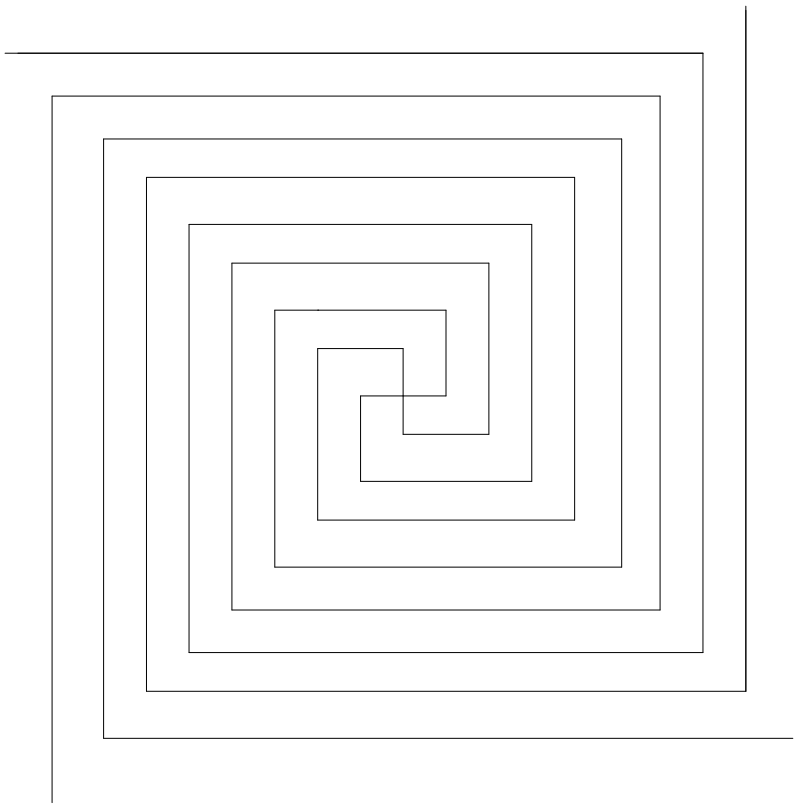
Eine Katakombe als Falle

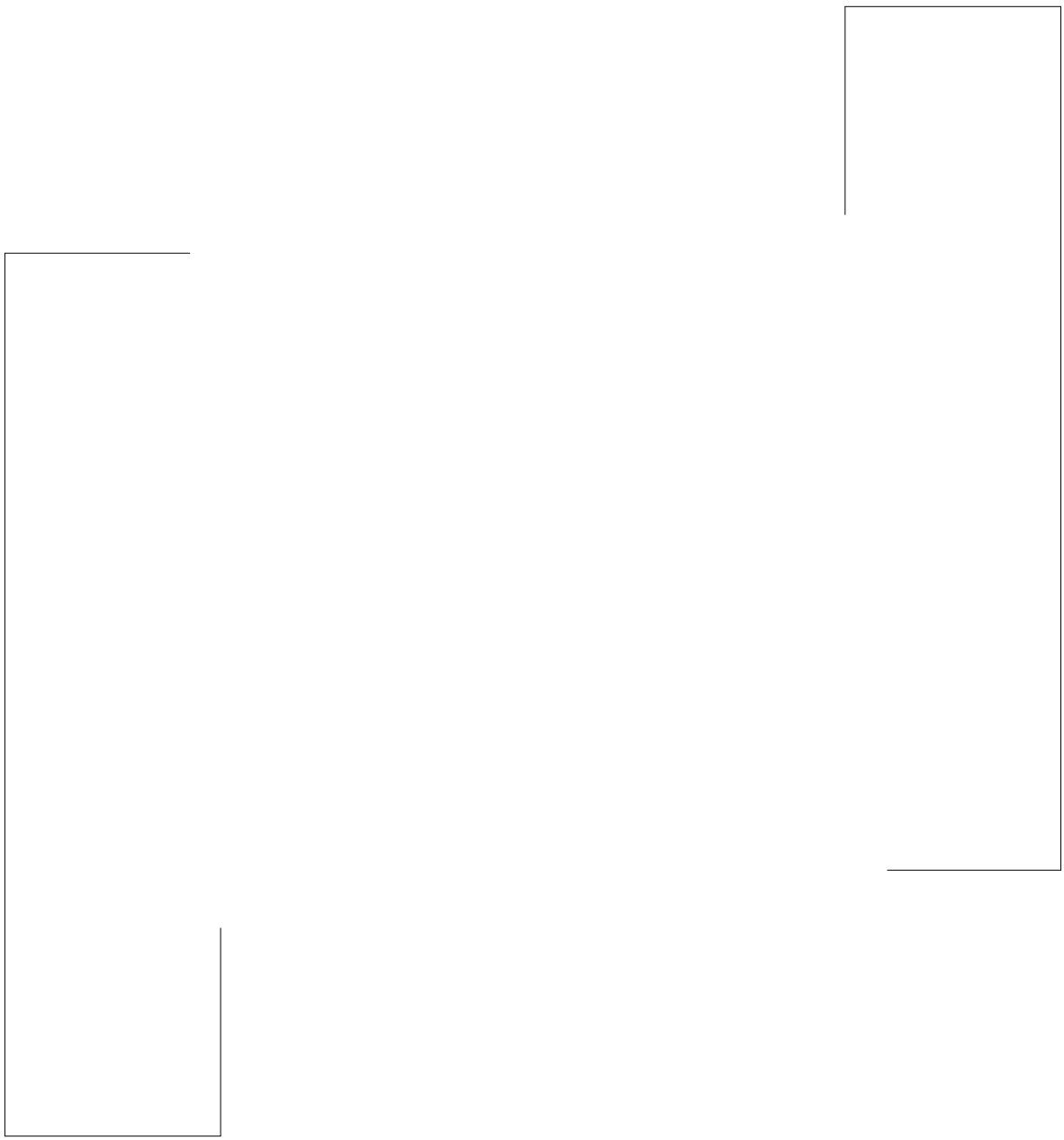


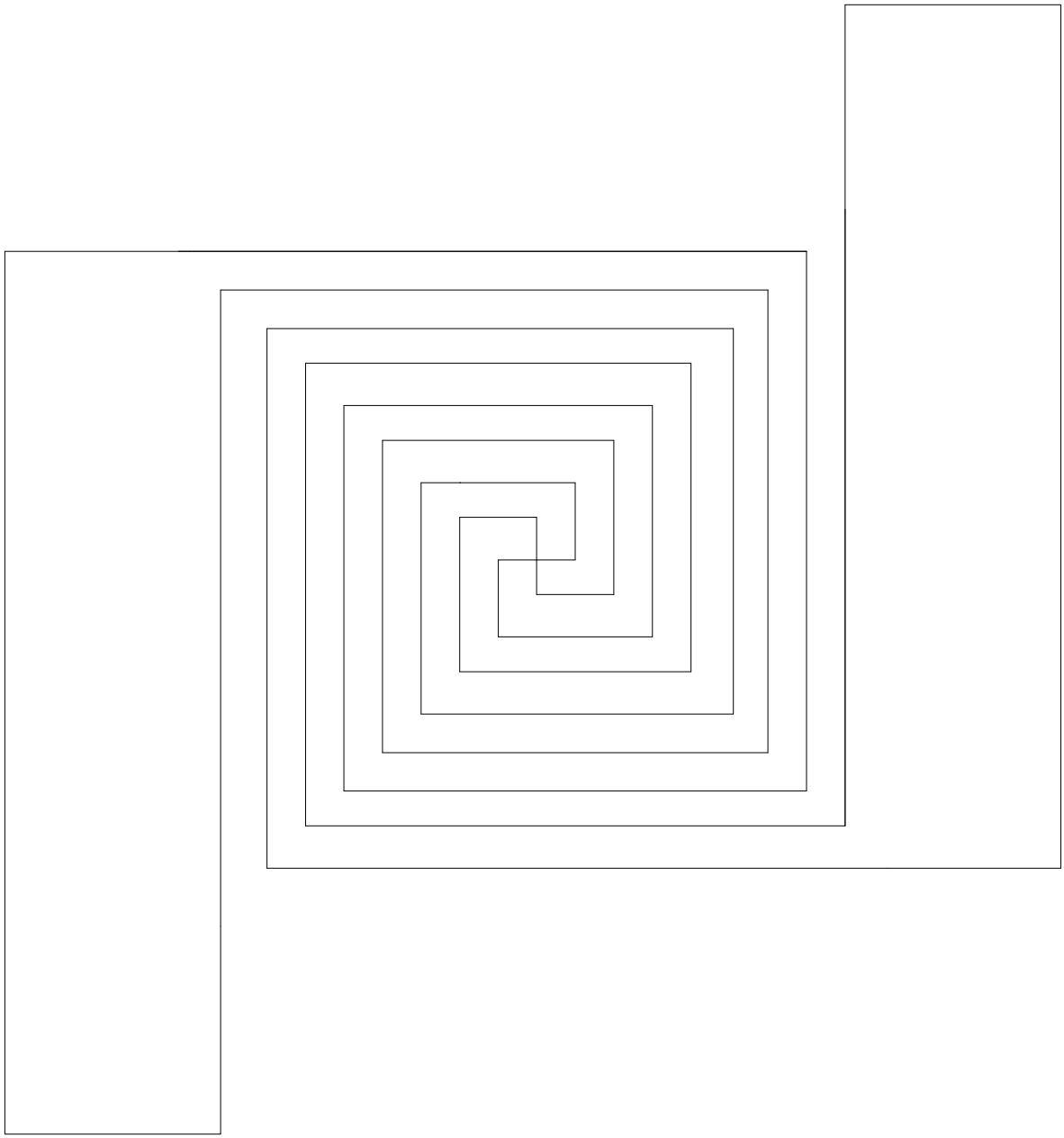
Testlabyrinthe

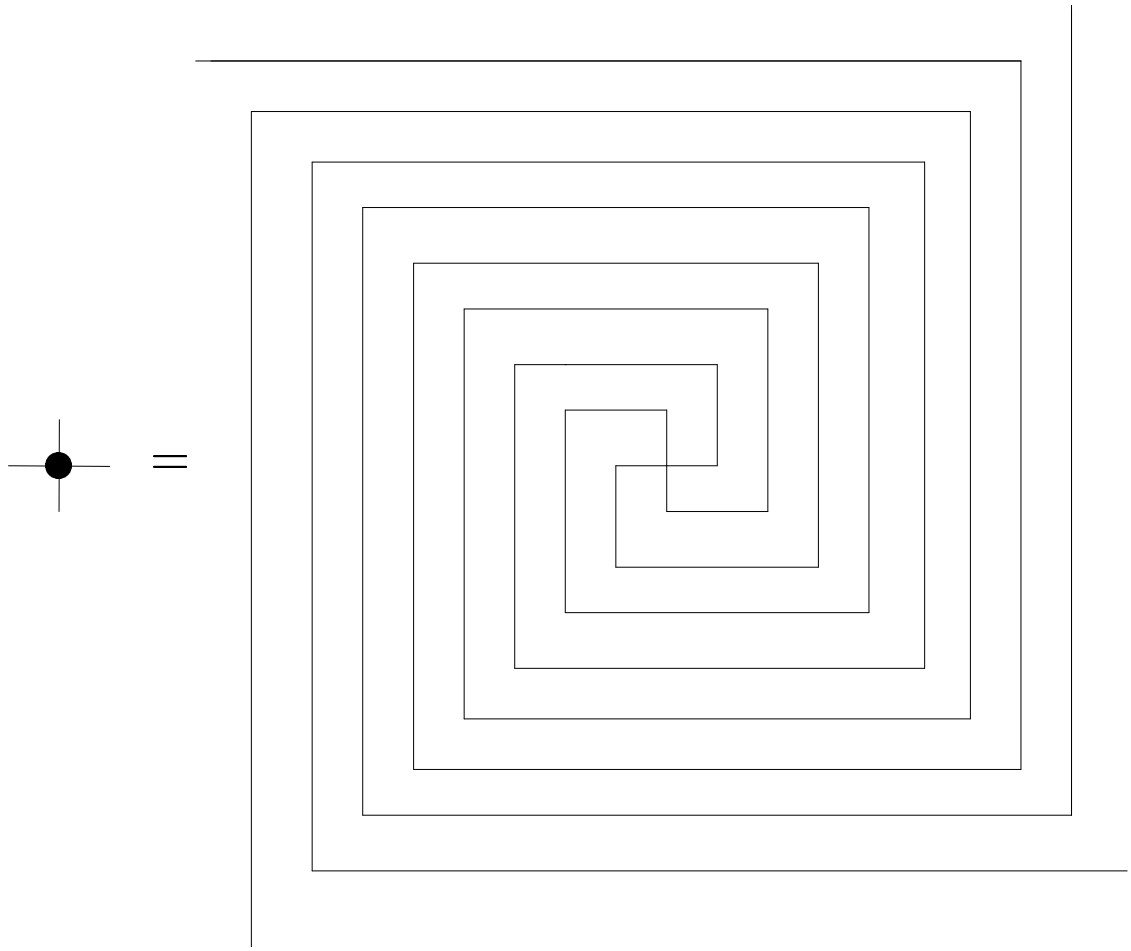
e n





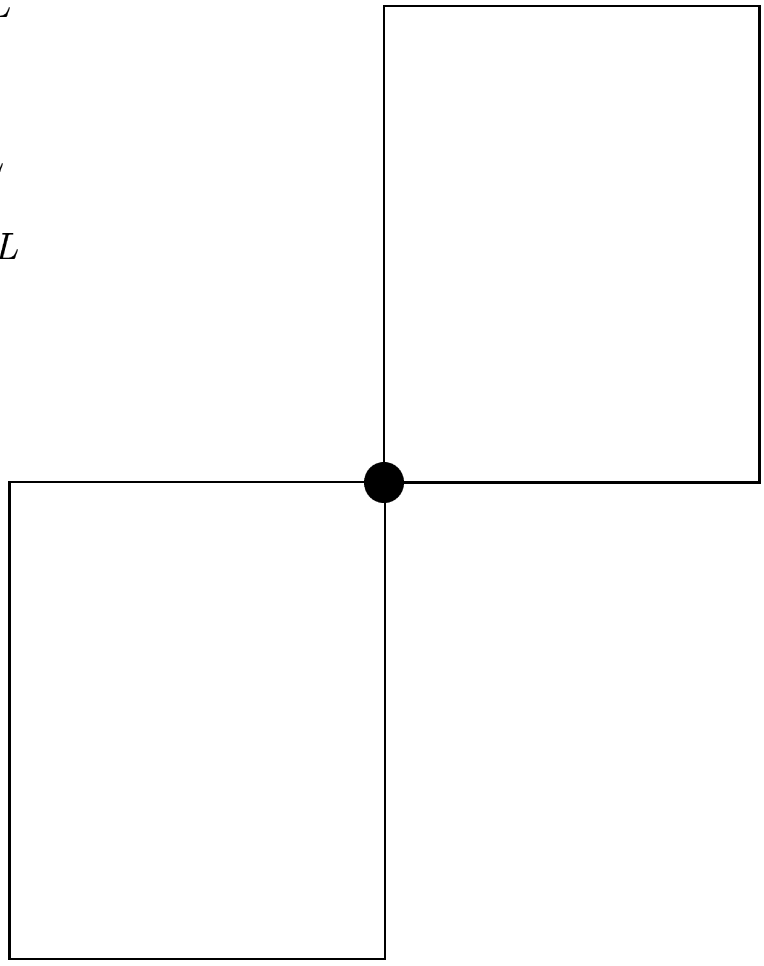






Der entscheidende Test

$$N := n^L$$
$$S := s^L$$
$$E := e^L$$
$$W := w^L$$

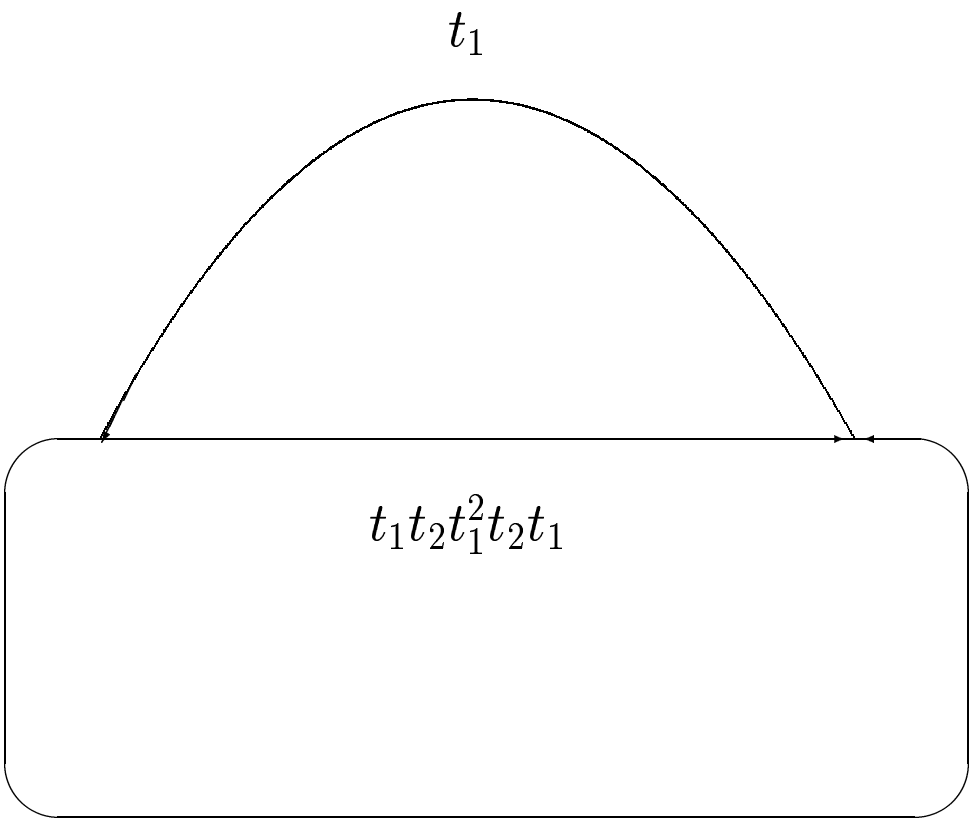


Das Ergebnis dieses Testes sei:

$$(ENWS)^2WSEN,\ E := e^L,\ N := n^L, \ldots$$

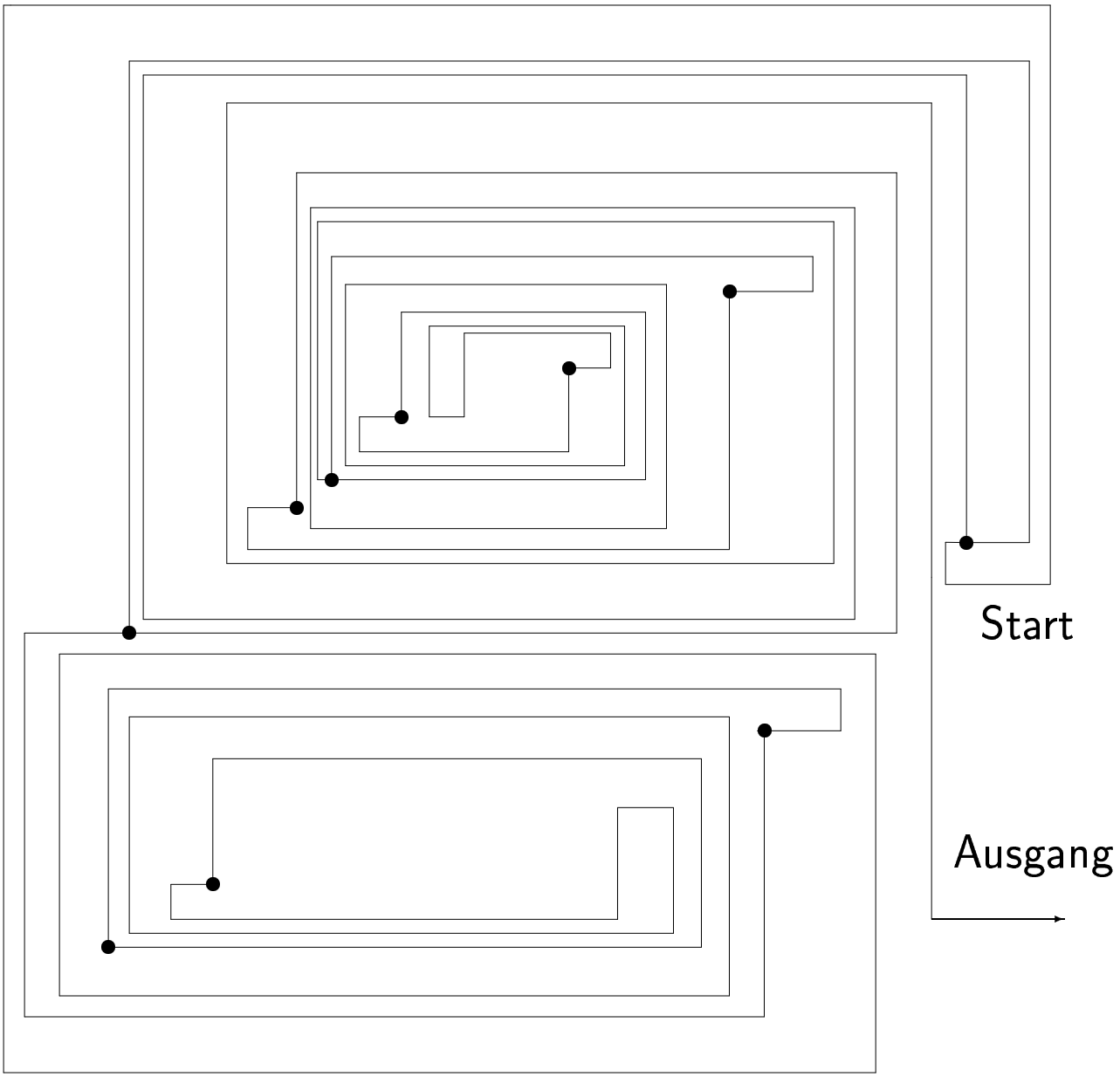
Die Falle

Sei $t_1 := s_e ENWS s_n^{-1}$, $t_2 := (s_e)^{-1} WSEN s_n$.



$t_2 T_1^2 t_2$

Eine Falle



Entwurf von Algorithmen: Anwendung von Alltagserfahrungen

- Rekursion: Teile und herrsche
- Depth first search und Backtracking: Weitergehen, solange es möglich ist. Ansonsten Rückzug auf letzte Position und Suche in einer neuen Richtung.
- Parallelität und Arbeitsorganisation

Komplexität von Algorithmen, effiziente Algorithmen

Erkennung traktabler Probleme; Nachweis einer extrem hohen Zeit- oder Speicherkomplexität führt auf die Notwendigkeit der Suche nach Heuristiken

Interpretationen bekannter mathematischer Modelle führen zu neuen algorithmischen Prinzipien.

1872 Ludwig Boltzmann: "Weitere Studien über das Wärmegleichgewicht unter Gasmolekülen"
Theorie des thermodynamischen Gleichgewichts von Gasen
Makrosystem bestehend aus sehr vielen (N mit $N \gg 0$) Mikrosystemen, die $E_1, E_2, \ldots$ als mögliche Energiewerte haben.
Wir sagen, dass sich eines dieser Mikrosysteme im Zustand k befindet, wenn seine Energie gleich E_k ist.

Seien $N_1, N_2, \ldots$ die Zahl der Mikrosysteme im Zustand $1, 2, \ldots$.

L. Boltzmann: im thermodynamischen Gleichgewicht gilt:

$$\frac{N_k}{N} \approx \frac{e^{-\frac{E_k}{T}}}{\sum_{i=1}^{n} e^{-\frac{E_i}{T}}}$$

wobei T die Temperatur des Systems ist.

1953 **N. Metropolis, A.W. und M.N. Rosenbluth, A.H. und E. Teller** simulierten in Los Alamos ein System von 224 Teilchen

Grundstruktur des Programms: Sei x ein Punkt im Phasenraum des Systems.
Wiederhole sehr oft die folgende Prozedur:

1. Wähle einen Punkt y in der Nachbarschaft von x;
2. Berechne die Energien $E(x)$ und $E(y)$ und bilde ihre Differenz
$$\Delta(x) := E(y) - E(x);$$
3. Falls $\Delta(x) \leq 0$, so ersetze x durch y;
4. Falls $\Delta(x) > 0$ ist, wähle eine zufällige Zahl ξ im Intervall $[0, 1]$; falls $\xi < e^{-\frac{\Delta(x)}{T}}$, so ersetze x durch y;

30 Jahre später: V. Cerny, S. Kirkpatrick, C. D. Gelatt und M. P. Venchi: dieses Progamm, in leicht modifizierter Form, kann auch für viele andere Zwecke genutzt werden. Man ersetze die Energie durch die Kosten und führe eine hypothetische Temperatur ein, die man langsam senkt. Man läßt also den Kristall langsam aus der Schmelze wachsen. Der Kristall entspricht dann dem Optimum.

Sei x eine Konfiguration des Optimierungsproblems und seien die Kosten von x durch die Funktion (Zielfunktion) $E(x)$ beschrieben.
Bei konstanter Temperatur Programmschleife:

1. Wähle eine Konfiguration y in der Nachbarschaft von x;
2. berechne die Kosten $E(x)$ und $E(y)$ und bilde ihre Differenz $\Delta(x) := E(y) - E(x)$;
3. falls $\Delta(x) \leq 0$, so ersetze x durch y;
4. falls $\Delta(x) > 0$ ist, wähle eine zufällige Zahl ξ im Intervall $[0, 1]$; falls $\xi < e^{-\frac{\Delta(x)}{T}}$, so ersetze x durch y;

Danach senke man langsam die Temperatur und beginne erneut mit obiger Programmschleife.

Mögliche Weiterungen

- Diktatortheorem: Es gibt keine einfachen demokratischen Entscheidungsverfahren; jede demokratische Pareto-Entscheidung erzwingt einen Diktator
- Chiffrierung
- Parallelität und Primzahltest
- Datenkompression
- Spektrum: Mathematik in der Praxis
- Faraktale
- VLSI-Schaltkreisentwurf: RELACS