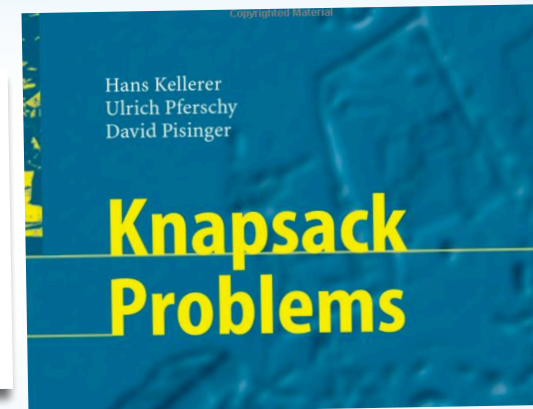




$$\begin{aligned} &\text{maximize} && \sum_{j=1}^n p_j x_j \\ &\text{subject to} && \sum_{j=1}^n w_j x_j \leq c, \\ &&& x_j = 0 \text{ or } 1, \quad j = 1, \dots, n, \end{aligned}$$



# *Algorithmen und Datenstrukturen 2*

*Sommer 2023*

**Prof. Dr. Sándor Fekete**



# Algorithmen und Datenstrukturen 2

Sommersemester 2022

[Startseite](#)

[Veranstaltungen](#)

[Organisation](#) ▾

[Kapitel](#) ▾

[Kontakt](#)

[Archiv](#)

## Startseite

# Algorithmen und Datenstrukturen 2

Die Vorlesung **Algorithmen und Datenstrukturen 2** ist eine Wahlpflichtveranstaltung für Studierende der Informatik, Wirtschaftsinformatik, Informations- und Systemtechnik; außerdem ist sie offen für interessierte Studierende anderer Studiengänge.

Algorithmen sind das methodische Herz der theoretischen und praktischen Informatik; Datenstrukturen ermöglichen die effiziente Umsetzung von Algorithmen und den effizienten Zugriff auf Input- und Outputdaten. In dieser weiterführenden Vorlesung werden die folgenden grundlegenden Begriffe erarbeitet:

## Neuigkeiten

### Letzte Veranstaltungen

[Vorlesung 12](#)

[Übung 6](#)

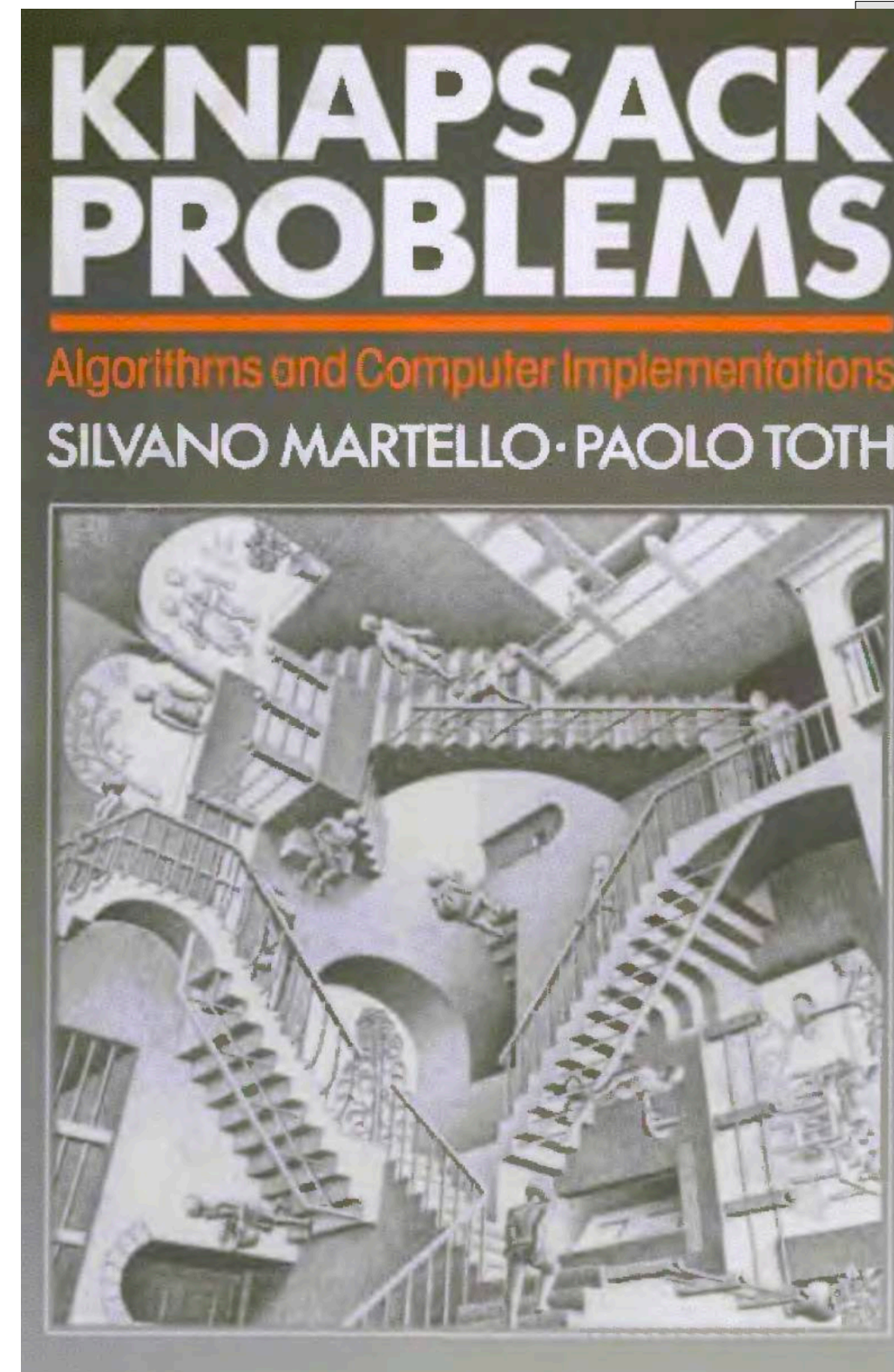
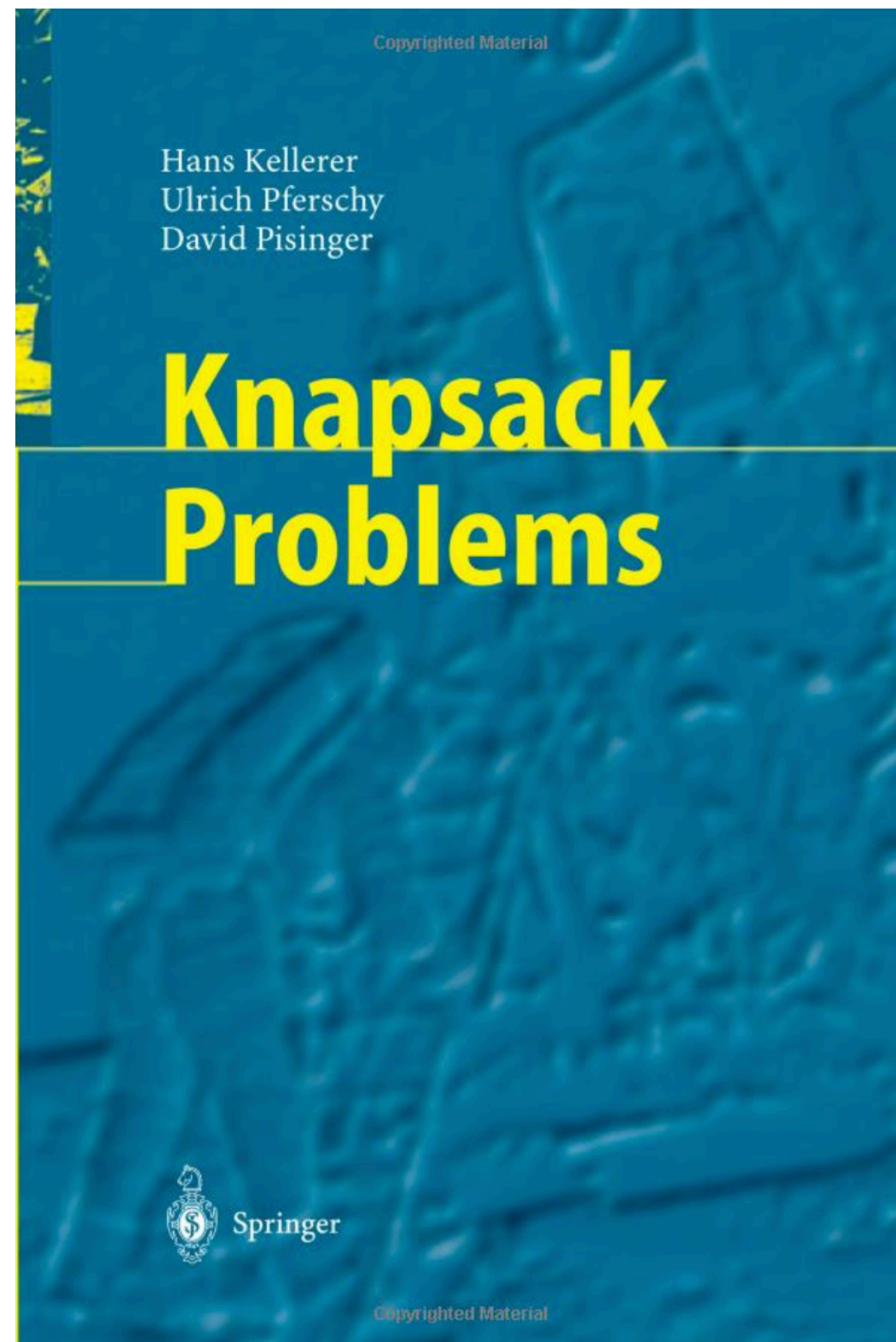
[Vorlesung 11](#)

[Vorlesung 10](#)

## Zeiten

[Vorlesung](#)

# Literatur



KnapsackProblems.pdf (Seite 5 von 306)

Hervorhebung Drehen Markierungen Suchen nach

## Contents

<b>Preface</b>	<b>xi</b>
<b>1 Introduction</b>	<b>1</b>
1.1 What are knapsack problems?	1
1.2 Terminology	2
1.3 Computational complexity	6
1.4 Lower and upper bounds	9
<b>2 0-1 Knapsack problem</b>	<b>13</b>
2.1 Introduction	13
2.2 Relaxations and upper bounds	16
2.2.1 Linear programming relaxation and Dantzig's bound	16
2.2.2 Finding the critical item in $O(n)$ time	17
2.2.3 Lagrangian relaxation	19
2.3 Improved bounds	20
2.3.1 Bounds from additional constraints	20
2.3.2 Bounds from Lagrangian relaxations	23
2.3.3 Bounds from partial enumeration	24
2.4 The greedy algorithm	27

## Algorithmen und Datenstrukturen 2

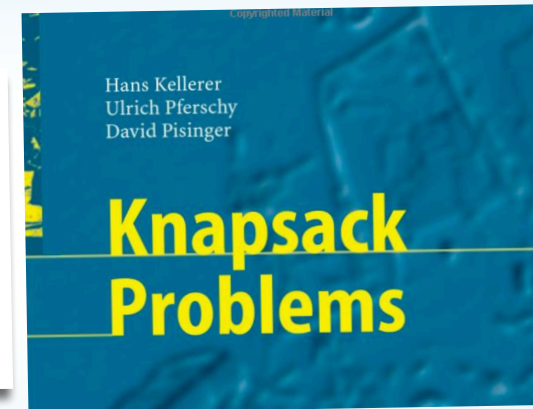
Sándor P. Fekete

L<sup>A</sup>T<sub>E</sub>X Version: Arne Schmidt

21. Juni 2021



$$\begin{aligned} &\text{maximize} && \sum_{j=1}^n p_j x_j \\ &\text{subject to} && \sum_{j=1}^n w_j x_j \leq c, \\ &&& x_j = 0 \text{ or } 1, \quad j = 1, \dots, n, \end{aligned}$$



# *1 Einführung: Knapsack-Probleme*

*Algorithmen und Datenstrukturen 2  
Sommer 2023*

**Prof. Dr. Sándor Fekete**

# Die Zeit läuft!



Knut Donald, erster Studierender der Informatik



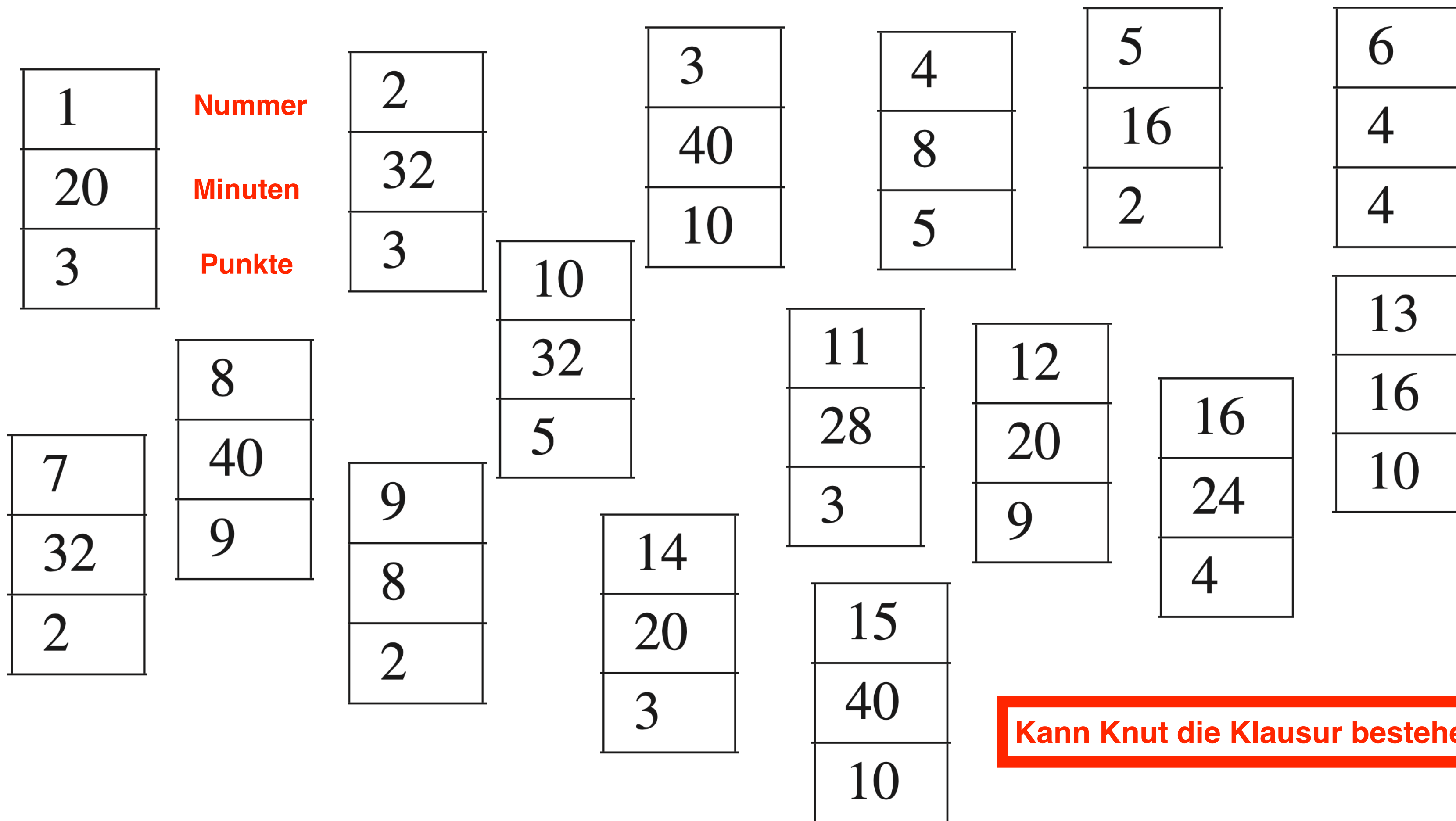
- 150 Minuten
- 20 Aufgaben
- 100 Punkte
- 50 Punkte zum Bestehen
- Die Zeit läuft!

# 30 Minuten später:



- 6 sichere Punkte
- 10 hoffnungslose Punkte
- Noch 44 Punkte zum Bestehen
- Restliche Aufgaben...

# Restliche Aufgaben



**Kann Knut die Klausur bestehen?**



# Sortieren?

nach Wert  $\left(\frac{z_i}{p_i}\right)$  sortieren:

$i$	6	4	13	12	9	3	15	8	16	10	1	14	5	11	2	7
$z_i$	4	8	16	20	8	40	40	40	24	32	20	20	16	28	32	32
$p_i$	4	5	10	9	2	10	10	9	4	5	3	3	2	3	3	2

$$\sum_{i=1}^n z_i x_i = 120$$

$$\sum_{i=1}^n p_i x_i = 44$$

**Knut kann die Klausur bestehen!**

# Optimierungsvariante

**Problem 1.2'** (MAXIMUM KNAPSACK).

**Gegeben:**

- $n$  Objekte  $1, \dots, n$  mit jeweils Größe  $z_i$  Gewinn  $p_i$
- Größenschranke  $Z$

**Gesucht:**

*Eine Menge*

$$S \subseteq \{1, \dots, n\}$$

*mit*

$$\sum_{i \in S} z_i \leq Z$$

*und*

$$\sum_{i \in S} p_i = \text{Maximal}$$

# Teilaufgaben?!

## Problem 1.3 ( FRACTIONAL KNAPSACK).

### Gegeben:

- $n$  Objekte  $1, \dots, n$  mit jeweils Größe  $z_i > 0$  Gewinn  $p_i > 0$
- Größenschranke  $Z$

### Gesucht:

Für jedes Objekt ein Wert

$$x_i \in [0, 1]$$

sodass

$$\sum_{i=1}^n z_i x_i \leq Z$$

und

$$\sum_{i=1}^n p_i x_i = \text{Maximal}$$

# Teilaufgaben?!

nach Wert  $\left(\frac{z_i}{p_i}\right)$  sortieren:

$i$	6	4	13	12	9	3	15	8	16	10	1	14	5	11	2	7
$z_i$	4	8	16	20	8	40	24	40	24	32	20	20	16	28	32	32
$p_i$	4	5	10	9	2	10	6	9	4	5	3	3	2	3	3	2

$$\sum_{i=1}^n z_i x_i = 120$$

$$\sum_{i=1}^n p_i x_i = 46$$

$$x_{15} = 0,6$$

# Algorithmus

## Algorithmus 1.4. (*Greedy-Algorithmus*)

---

**Eingabe:**  $z_1, \dots, z_n, Z, p_1, \dots, p_n$

**Ausgabe:**  $x_1, \dots, x_n \in [0, 1]$

mit

$$\sum_{i=1}^n z_i x_i \leq Z$$

und

$$\sum_{i=1}^n p_i x_i = \text{Maximal}$$

1: *Sortiere*  $\{1, \dots, n\}$  nach  $\frac{z_i}{p_i}$  *aufsteigend*;

*Dies ergibt die Permutation*  $\pi(1), \dots, \pi(n)$ .

*Setze*  $j = 1$ .

2: **while**  $(\sum_{i=1}^j z_{\pi(i)} \leq Z)$  **do**

3:      $x_{\pi(j)} := 1$

4:      $j := j + 1$

5: *Setze*  $x_{\pi(j)} := \frac{Z - \sum_{i=1}^{j-1} z_{\pi(i)}}{z_{\pi(j)}}$

6: **return**

---

# Das klappt immer!

**Satz 1.5.** Algorithmus 1.4 liefert eine optimale Lösung für Problem 1.3.

**Beweis:**

O.B.d.A. sei  $\sum_{i=1}^n z_{\pi(i)} > Z$  - sonst nimmt man einfach alles.

- (1) Wir bekommen eine zulässige Lösung.
- (2) Wir bekommen eine optimale Lösung.

# (1) Zulässigkeit

Setze  $j = 1$ .  
 2: **while**  $(\sum_{i=1}^j z_{\pi(i)} \leq Z)$  **do**  
 3:      $x_{\pi(j)} := 1$   
 4:      $j := j + 1$   
 5: Setze  $x_{\pi(j)} := \frac{Z - \sum_{i=1}^{j-1} z_{\pi(i)}}{z_{\pi(j)}}$   
 6: **return**

$i$	6	4	13	12	9	3	15	8	16	10	1	14	5	11	2	7
$z_i$	4	8	16	20	8	40	24	40	24	32	20	20	16	28	32	32
$p_i$	4	5	10	9	2	10	6	9	4	5	3	3	2	3	3	2

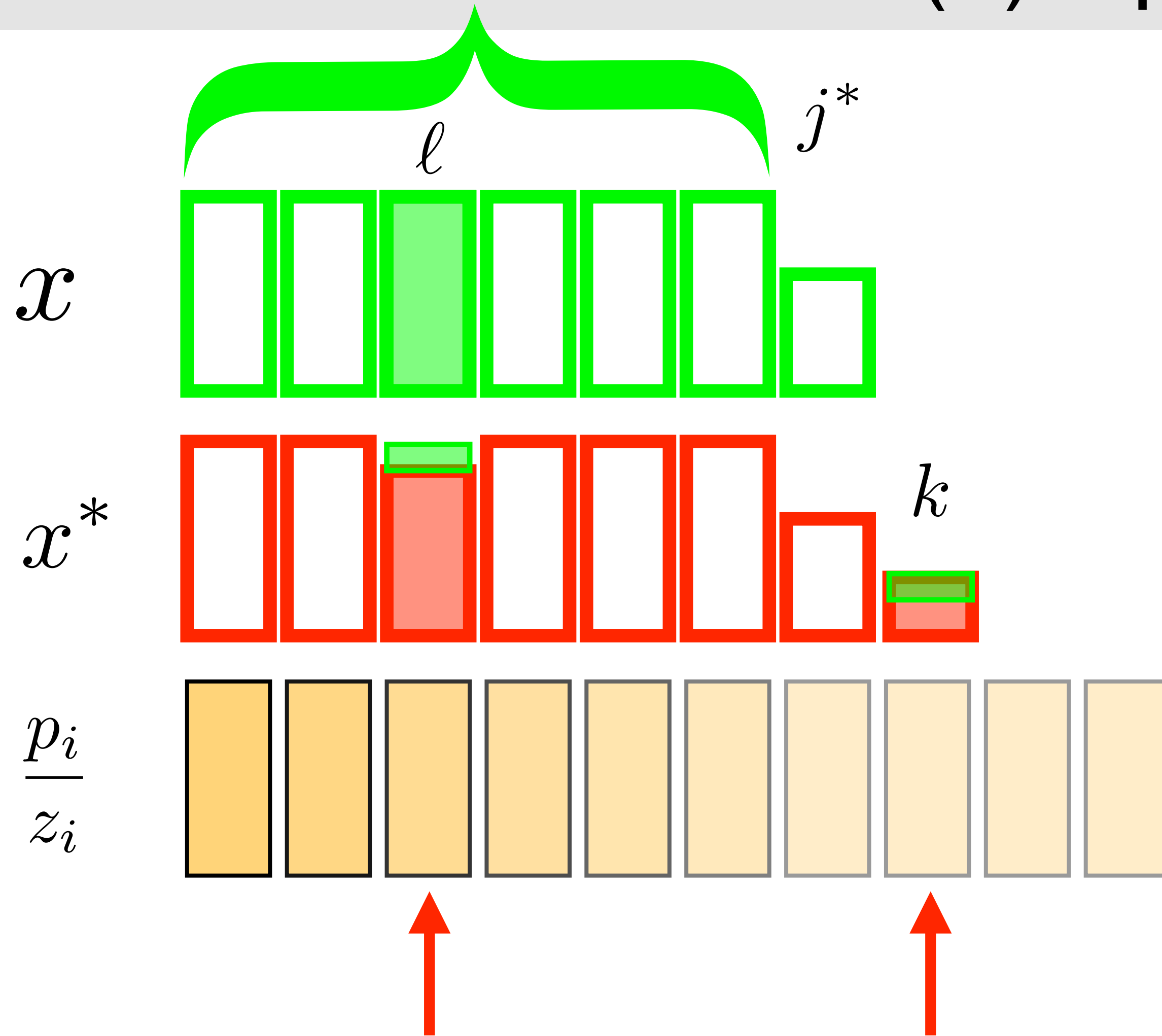
$\sum_{i=1}^n z_i x_i = 120$   
 $\sum_{i=1}^n p_i x_i = 46$   
 $x_{15} = 0,6$

Sei  $j^*$  der letzte Index, für den die **while**-Bedingung getestet wird.

Dann ist  $\sum_{i=1}^{j^*-1} z_{\pi(i)} \leq Z$  und  $\sum_{i=1}^{j^*} z_{\pi(i)} > Z$

Also ist  $x_{\pi(1)}, \dots, x_{\pi(j^*-1)} = 1$  und  $x_{\pi(j^*)} \in [0, 1[$  und  $\sum_{i=1}^{j^*} x_{\pi(i)} z_{\pi(i)} = Z$

## (2) Optimalität



$$\sum_{i=1}^n x_i p_i < \sum_{i=1}^n x_i^* p_i$$

$$p_i > 0 :$$

$$\implies \exists k \in \{1, \dots, n\} : x_{\pi(k)} < x_{\pi(k)}^*$$

$$\implies \exists k \in \{j^*, \dots, n\} : x_{\pi(k)} < x_{\pi(k)}^*$$

$$\implies \exists l \in \{1, \dots, j^*\} : x_{\pi(l)} > x_{\pi(l)}^*$$

$x^*$  nicht optimal!



# Verallgemeinerung: Mehrfachverwendung

**Problem 1.6 (INTEGER KNAPSACK).**

**Gegeben:**

- $n$  Objekte  $1, \dots, n$  mit jeweils Größe  $z_i$  Gewinn  $p_i$
- Größenschranke  $Z$

**Gesucht:**

*Für jedes Objekt ein Wert*

$$x_i \in \mathbb{N}$$

*mit*

$$\sum_{i=1}^n z_i x_i \leq Z$$

*und*

$$\sum_{i=1}^n p_i x_i = \text{Maximal}$$

# Spezialfall: Alle Gewinndichten gleich

## Problem 1.7.

### Gegeben:

- $n$  Objekte  $1, \dots, n$  mit jeweils Größe  $z_i$
- Größenschranke  $Z$

### Gesucht:

Eine Menge

$$S \subseteq \{1, \dots, n\}$$

mit

$$\sum_{i \in S} z_i \leq Z$$

und

$$\sum_{i \in S} z_i = \textit{Maximal}$$

# Spezialfall des Spezialfalls: Größenschränke treffen

**Problem 1.8** (SUBSET SUM).

**Gegeben:**

- $n$  Objekte  $1, \dots, n$  mit jeweils Größe  $z_i$
- Zielgröße  $Z$

**Gesucht:**

*Eine Menge*

$$S \subseteq \{1, \dots, n\}$$

*mit*

$$\sum_{i \in S} z_i = Z$$

# Spezialfall<sup>3</sup>: Partition

**Problem 1.9** (PARTITION).

**Gegeben:**

- $n$  Objekte  $1, \dots, n$  mit jeweils Größe  $z_i$

**Gesucht:**

*Eine Menge*

$$S \subseteq \{1, \dots, n\}$$

*mit*

$$\sum_{i \in S} z_i = \sum_{i \notin S} z_i$$

# Beispiel

## Beispiel 1.10.

Partition für  $\{z_1, \dots, z_9\} = \{7, 13, 17, 20, 29, 31, 31, 35, 57\}$

Gesamtsumme: 240

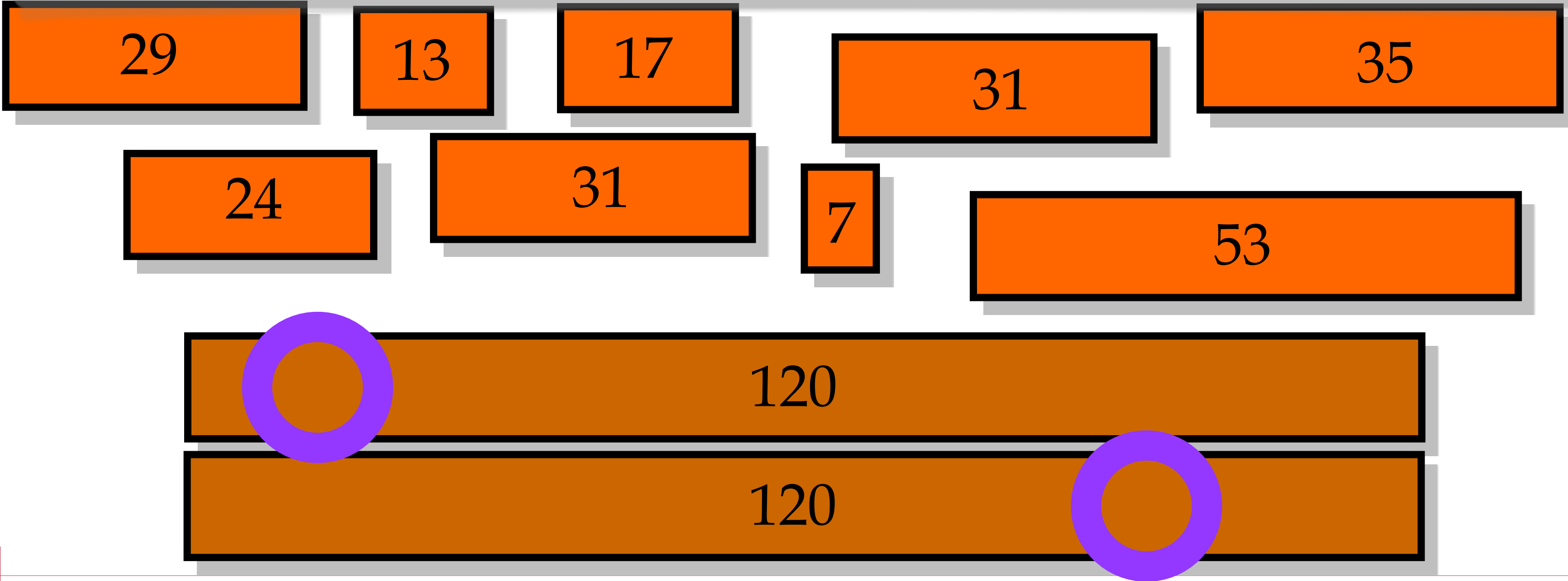
Finde Aufteilung in zwei gleiche Teilmengen!

# Ein Bild hilft

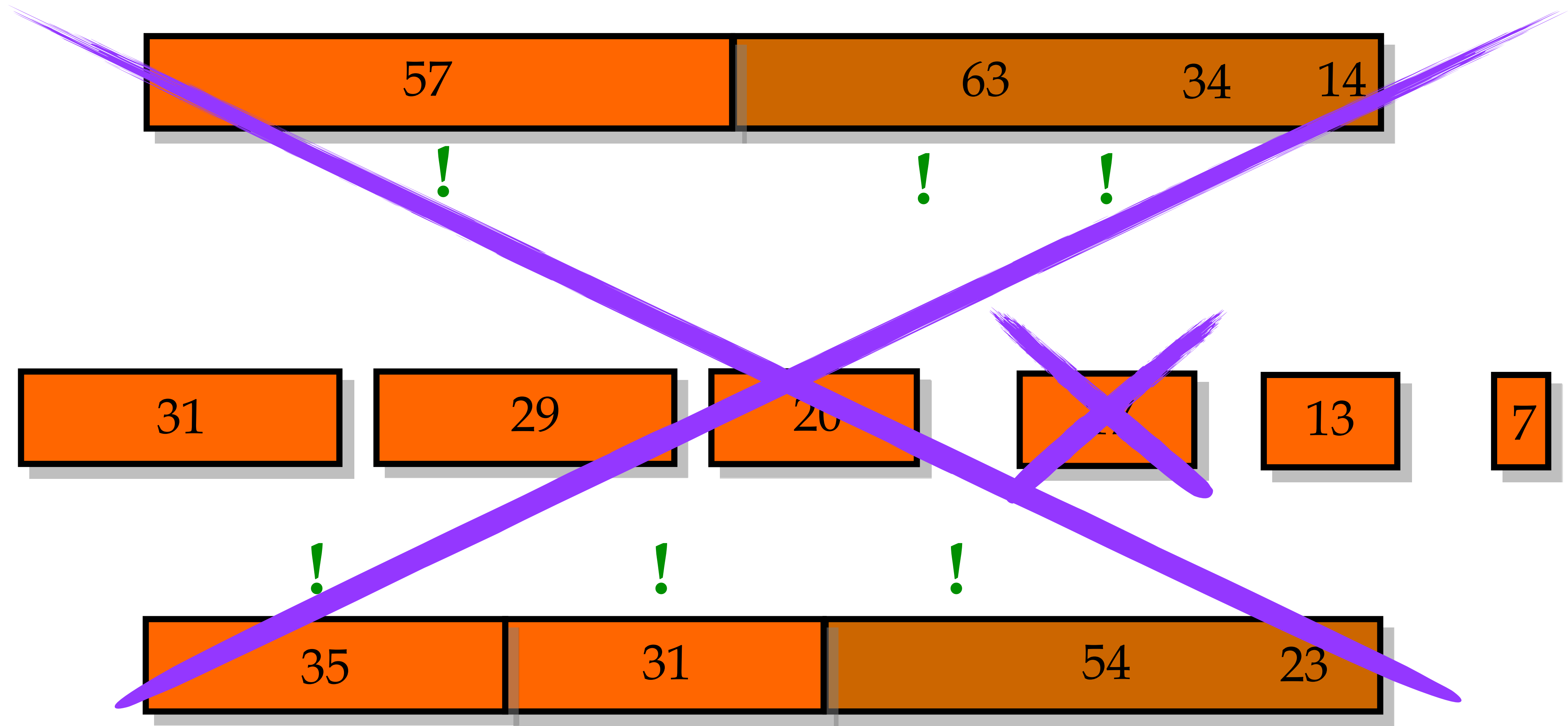
## Beispiel 1.10.

Partition für  $\{z_1, \dots, z_9\} = \{7, 13, 17, 20, 29, 31, 31, 35, 57\}$

Gesamtsumme: 240

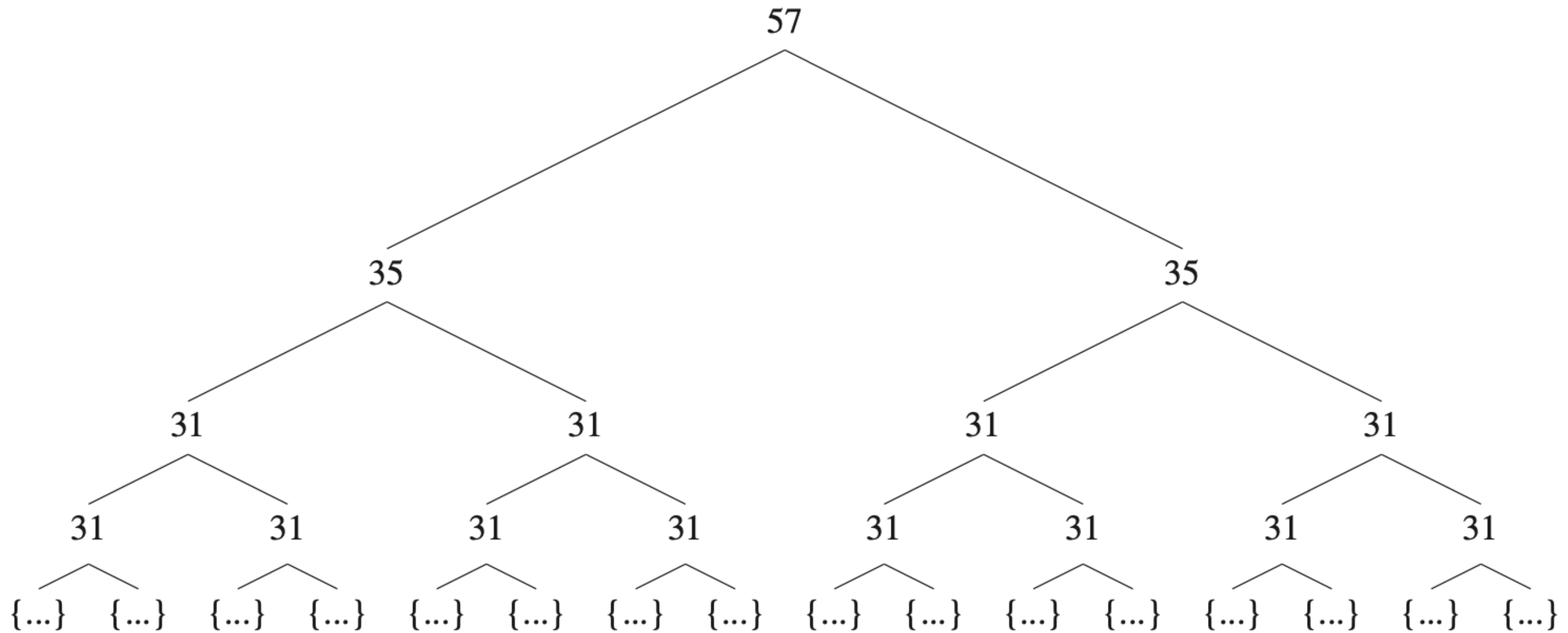


# Keine Lösung?!



# Enumerationsprinzip

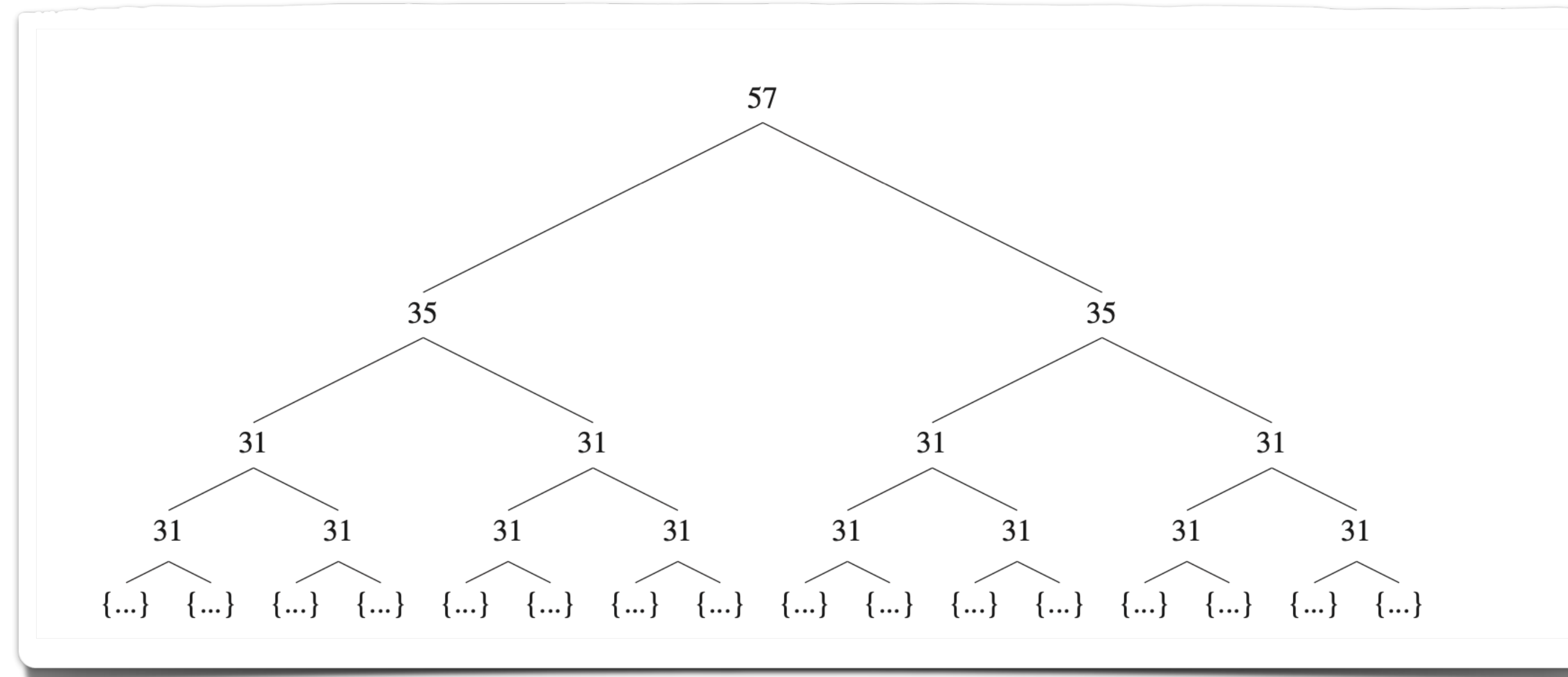
120



120



# Enumerationsprinzip



- Exponentiell viele Fälle!
- Wie geht das systematisch?
- Wo kann man Arbeit sparen?

# Alltagsanwendung: xkcd #287

MY HOBBY:  
EMBEDDING NP-COMPLETE PROBLEMS IN RESTAURANT ORDERS

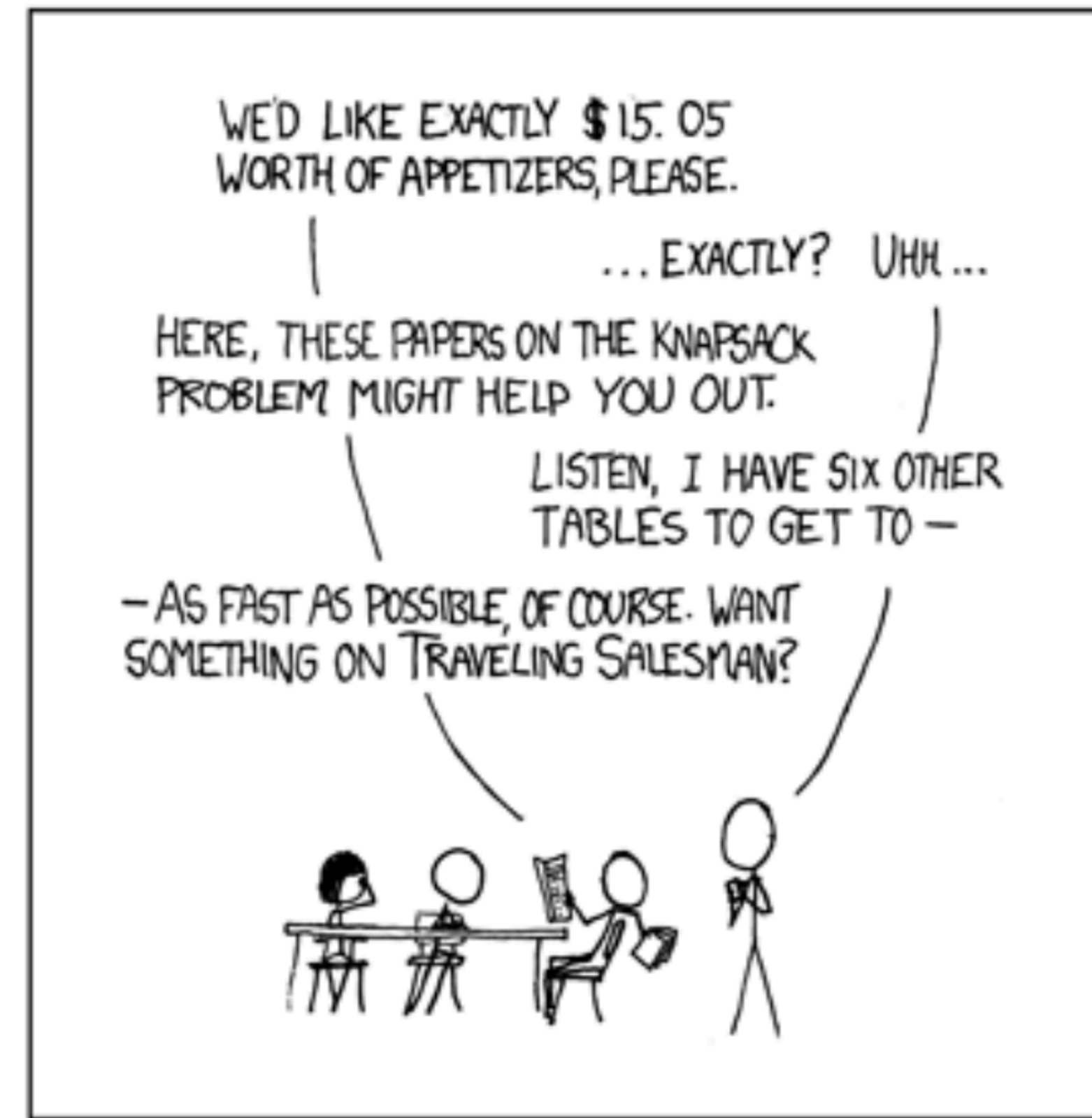
CHOTCHKIES RESTAURANT

APPETIZERS

MIXED FRUIT	2.15
FRENCH FRIES	2.75
SIDE SALAD	3.35
HOT WINGS	3.55
MOZZARELLA STICKS	4.20
SAMPLER PLATE	5.80

SANDWICHES

BARBECUE	6.55
----------	------





$$P(x, i) = \begin{cases} P(x, i-1), \\ \max\{P(x, i-1), \\ P(x, i-2) + 13\} \end{cases}$$

$x \backslash i$	0	1	2	3	3	5
0	1	0	0	0	0	0
1	1	0	0	0	0	0
2	1	0	0	0	0	+13
3						

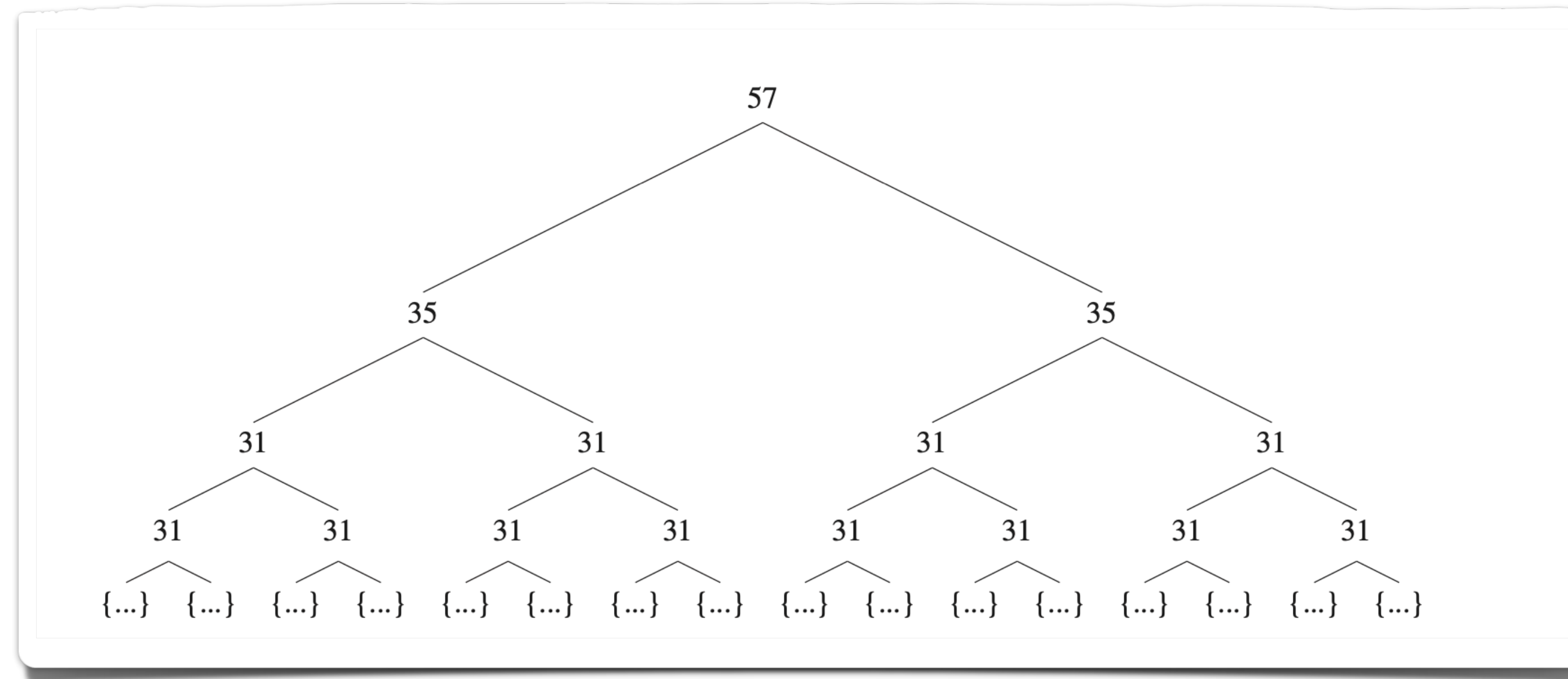
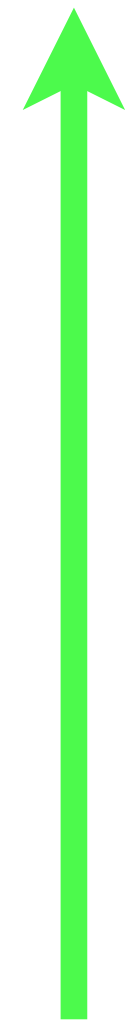
## 2 Dynamic Programming

*Algorithmen und Datenstrukturen 2  
Sommer 2022*

**Prof. Dr. Sándor Fekete**

# Ideen

Dynamic  
Programming



- Bestimme erreichbare Zahlen
- Vorwärts: Nimm Zahlen hinzu

- Zeige Unerreichbarkeit von Zahlen
- Rückwärts: Schließe Zahlen aus

# Dynamic Programming für Anfänger

- Wieviel ist das?

$$1+1+1+1+1+1+1+1+1+1+1+1+1 = 13$$

- Und das?

$$1+1+1+1+1+1+1+1+1+1+1+1+1+1 = 13+1 = 14$$

- Dynamic Programming:
  - Nicht von vorn lösen
  - Zwischenergebnisse merken

# Beispiel

## Beispiel 2.1

$$\{z_1, \dots, z_9\} = \{7, 13, 17, 20, 29, 31, 31, 35, 57\}$$

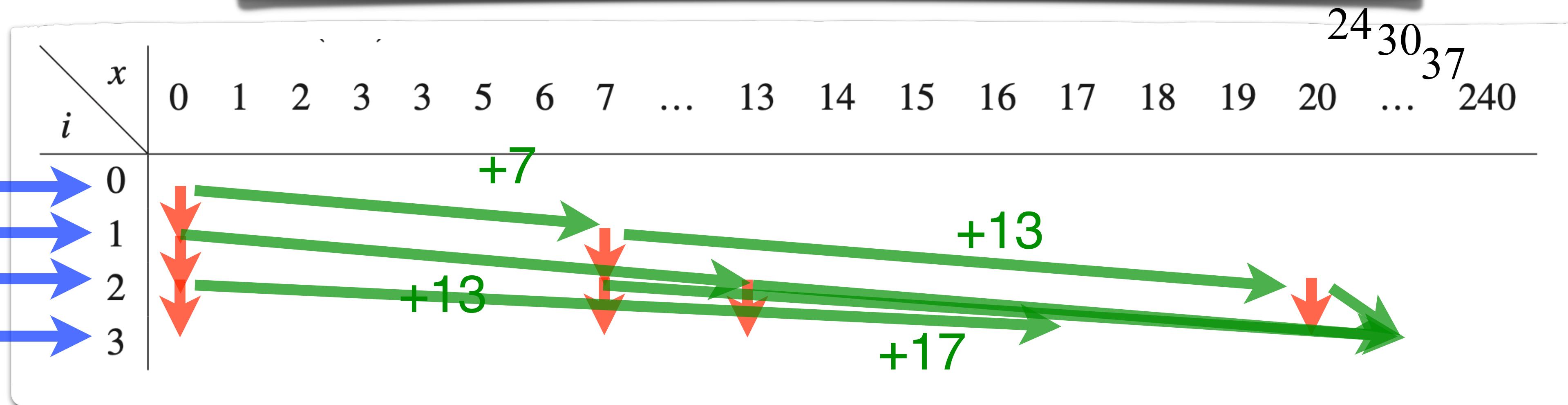
Bestimme alle Zahlen, die als Teilsummen erreichbar sind!

- Bestimme erreichbare Zahlen
- Vorwärts: Nimm Zahlen hinzu

# Beispiel

$$\{z_1, \dots, z_9\} = \{7, 13, 17, 20, 29, 31, 31, 35, 57\}$$

$$\mathcal{P}(x, i) = \begin{cases} 1, & \text{falls } x \text{ mit } z_1, \dots, z_i \text{ erzeugt werden kann} \\ 0, & \text{sonst} \end{cases}$$



# Allgemeiner

$$\mathcal{S}(x, i) = \begin{cases} 1, & \text{falls } x \text{ mit } z_1, \dots, z_i \text{ erzeugt werden kann} \\ 0, & \text{sonst} \end{cases}$$

$$\mathcal{S}(x, 0) = 0, \text{ für alle } x \in \{1, \dots, Z\}; \mathcal{S}(0, 0) = 1$$

$x \backslash i$	0	1	2	3	3	5	6	7	...	13	14	15	16	17	18	19	20	...	240
0	1	0	0	0	0	0	0	0	...	0	0	0	0	0	0	0	0	...	0
1	1	0	0	0	0	0	0	1	...	0	0	0	+13	0	0	0	0	...	0
2	1	0	0	0	+13	0	1	...	1	0	0	0	0	0	0	0	1	...	0
3																			

$$\mathcal{S}(x, i-1) = 1 \Rightarrow \mathcal{S}(x, i) = 1$$

$$\mathcal{S}(x - z_i, i-1) = 1 \Rightarrow \mathcal{S}(x, i) = 1$$



# Algorithmus

**Algorithmus 2.2** . (Dynamic Programming für SUBSET SUM).

**Eingabe:** Zahlen  $z_1, \dots, z_n$  mit  $\sum_{i=1}^n z_i = Z$

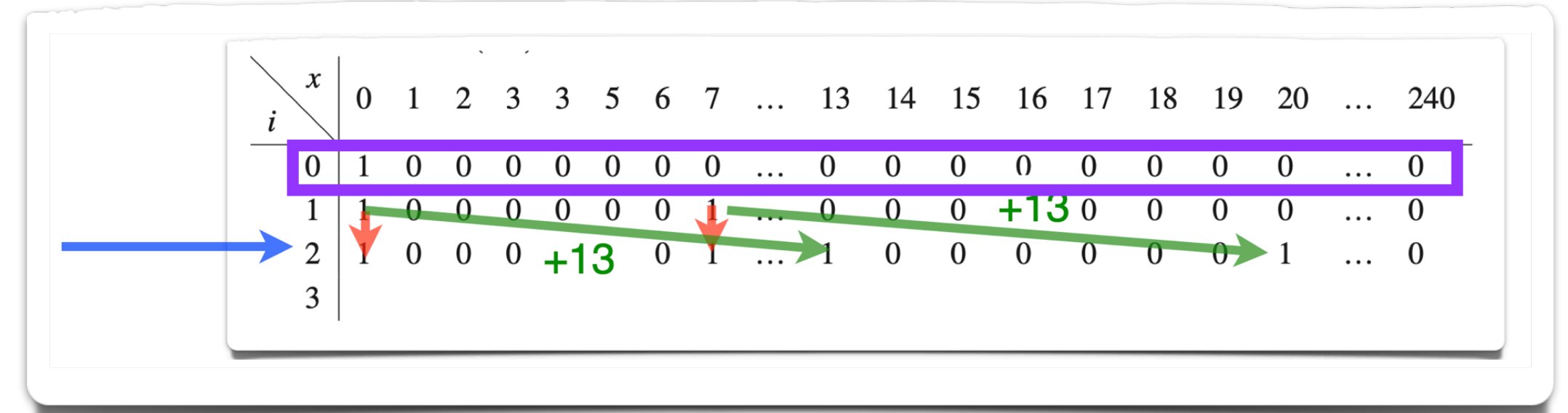
**Ausgabe:** Boolesche Funktion  $\mathcal{S} : \{0, \dots, Z\} \times \{0, \dots, n\} \rightarrow \{0, 1\}$

mit  $\mathcal{S}(x, i) = \begin{cases} 1, & \text{falls } x \text{ mit } z_1, \dots, z_i \text{ erzeugt werden kann} \\ 0, & \text{sonst} \end{cases}$

1:  $\mathcal{S}(0, 0) := 1$   
 2: **for** ( $x=1$ ) **to**  $Z$  **do**  
 3:      $\mathcal{S}(x, 0) := 0;$

4: **for** ( $i = 1$ ) **to**  $n$  **do**  
 5:     **for** ( $x = 0$ ) **to**  $z_i - 1$  **do**  
 6:          $\mathcal{S}(x, i) := \mathcal{S}(x, i - 1);$   
 7:     **for** ( $x = z_i$ ) **to**  $Z$  **do**  
 8:         **if** ( $\mathcal{S}(x, i - 1) = 1$  **OR** ( $\mathcal{S}((x - z_i), i - 1) = 1$ )) **then**  
 9:              $\mathcal{S}(x, i) := 1;$   
 10:         **else**  
 11:              $\mathcal{S}(x, i) := 0;$

12: **return**



# Korrektheit

**Satz 2.3** Algorithmus 2.2 löst das Problem SUBSET SUM. Die Laufzeit ist  $O(Z \cdot n)$ .

**Beweis.** Induktion über die Anzahl der Elemente  $n$ .

**Induktionsanfang:** Initialisierung korrekt für  $n=0$ .

**Induktionssannahme:**  $\mathcal{S}(x, i-1)$  korrekt für alle  $i$ .

**Induktionsschritt:** Erzeugung von  $x$  mit  $z_1, \dots, z_i$ .

(I)  $z_i$  wird nicht verwendet  $\Rightarrow x$  kann mit  $z_1, \dots, z_{i-1}$  erzeugt werden.

(II)  $z_i$  wird verwendet  $\Rightarrow x - z_i$  kann mit  $z_1, \dots, z_{i-1}$  erzeugt werden.

$x \backslash i$	0	1	2	3	3	5	6	7	...	13	14	15	16	17	18	19	20	...	240
0	1	0	0	0	0	0	0	0	...	0	0	0	0	0	0	0	0	...	0
1	1	0	0	0	0	0	0	1	...	0	0	0	+13	0	0	0	0	...	0
2	1	0	0	0	+13	0	1	...	1	0	0	0	0	0	0	0	0	...	1
3																			

# Laufzeit

**Algorithmus 2.2** . (Dynamic Programming für SUBSET SUM).

**Eingabe:** Zahlen  $z_1, \dots, z_n$  mit  $\sum_{i=1}^n z_i = Z$

**Ausgabe:** Boolesche Funktion  $\mathcal{S} : \{0, \dots, Z\} \times \{0, \dots, n\} \rightarrow \{0, 1\}$

mit  $\mathcal{S}(x, i) = \begin{cases} 1, & \text{falls } x \text{ mit } z_1, \dots, z_i \text{ erzeugt werden kann} \\ 0, & \text{sonst} \end{cases}$

1:  $\mathcal{S}(0, 0) := 1$

2: **for** ( $x=1$ ) **to**  $Z$  **do**

3:      $\mathcal{S}(x, 0) := 0;$

4: **for** ( $i = 1$ ) **to**  $n$  **do**

5:     **for** ( $x = 0$ ) **to**  $z_i - 1$  **do**

6:          $\mathcal{S}(x, i) := \mathcal{S}(x, i - 1);$

7:     **for** ( $x = z_i$ ) **to**  $Z$  **do**

8:         **if** ( $(\mathcal{S}(x, i - 1) = 1)$  **OR**  $(\mathcal{S}((x - z_i), i - 1) = 1)$ ) **then**

9:              $\mathcal{S}(x, i) := 1;$

10:         **else**

11:              $\mathcal{S}(x, i) := 0;$

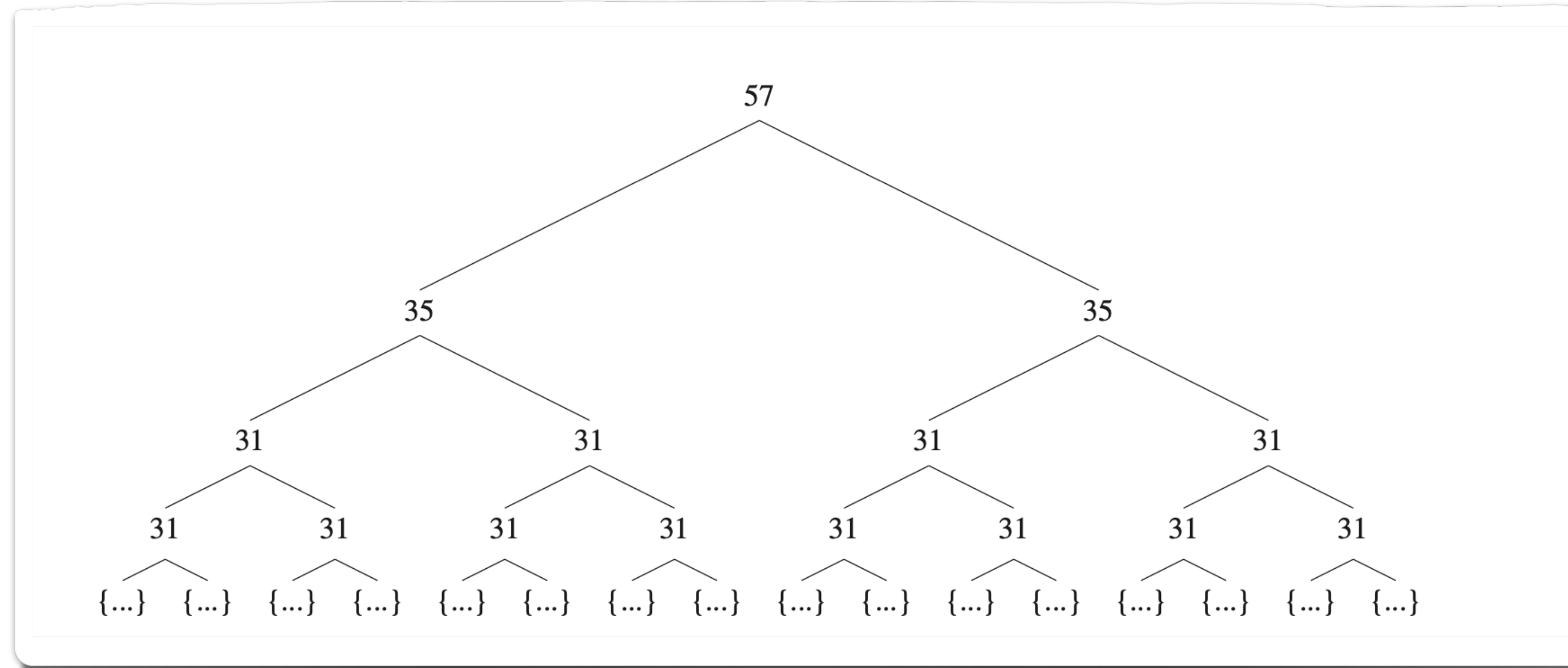
12: **return**

$O(nZ)$

# Effizienz?!

Dynamic  
Programming

$O(nZ)$



$2^n$

- Exponentiell viele Fälle!
- Wo sparen wir Arbeit?

$Z$  klein im Vergleich zu  $2^n$  : viele Duplikate gespart  
 $Z$  groß im Vergleich zu  $2^n$  : viel unnötige Arbeit

# Fragen

- Wie lässt sich das Prinzip verallgemeinern?
- Wie geht das für Knapsack?
- Wie geht das für andere Probleme?



$$P(x, i) = \begin{cases} P(x, i-1), \\ \max\{P(x, i-1), \dots\} \end{cases}$$

$x \backslash i$	0	1	2	3	3	5
0	1	0	0	0	0	0
1	1	0	0	0	0	0
2	1	0	0	0	0	+13
3						

## 2.2 Dynamic Programming für Knapsack

Algorithmen und Datenstrukturen 2  
Sommer 2023

Prof. Dr. Sándor Fekete

# Fragen

- Wie lässt sich das Prinzip verallgemeinern?
- Wie geht das für Knapsack?
- Wie geht das für andere Probleme?

# Knapsack

- Objekte  $1, \dots, n$
- Kosten  $z_1, \dots, z_n$
- Nutzen  $p_1, \dots, p_n$



# Von Subset Sum zu Knapsack

$$\mathcal{S}(x, i) = \begin{cases} 1, & \text{falls } x \text{ mit } z_1, \dots, z_i \text{ erzeugt werden kann} \\ 0, & \text{sonst} \end{cases}$$

$i \backslash x$	0	1	2	3	3	5	6	7	...	13	14	15	16	17	18	19	20	...	240
0	1	0	0	0	0	0	0	0	...	0	0	0	0	0	0	0	0	...	0
1	1	0	0	0	0	0	0	1	...	0	0	0	0	0	0	0	0	...	0
2	1	0	0	0	0	0	0	1	...	1	0	0	0	0	0	0	1	...	0
3	1	0	0	0	0	0	0	1	...	1	0	0	0	1	0	0	1	...	0

$P(x, i)$

der höchste Nutzen

der sich mit den Objekten

$1, \dots, i$  erzielen lässt

wenn die Kosten auf  $x$  begrenzt sind

# Beispiel: Knapsack

## Beispiel 2.4 (Knapsackproblem).

Sei  $Z = 9$  und seien folgende sieben Objekte gegeben:

$i$	1	2	3	4	5	6	7
$z_i$	2	3	6	7	5	9	4
$p_i$	6	5	8	9	6	7	3

# Dynamic Programming für Knapsack

$$P(x, i)$$

der höchste Nutzen

der sich mit den Objekten  $1, \dots, i$  erzielen lässt

wenn die Kosten auf  $x$  begrenzt sind

$i$	1	2	3	4	5	6	7
$z_i$	2	3	6	7	5	9	4
$p_i$	6	5	8	9	6	7	3

1. Objekt  $i$  ist zu teuer für Kostenschranke  $x$ , falls  $z_i > x$

2. Objekt  $i$  ist nicht zu teuer, bringt aber keine Verbesserung

3. Objekt  $i$  ist nicht zu teuer und bringt eine Verbesserung

$x \backslash i$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	0	6	6	6	6	6	6	6	6
2	0	0	6	6	6	11	11	11	11	11
3	0	0	6	6	6	11	11	11	14	14
4	0	0	6	6	6	11	11	11	14	15
5	0	0	6	6	6	11	11	12	14	15
6	0	0	6	6	6	11	11	12	14	15
7	0	0	6	6	6	11	11	12	14	15

# Systematisch!

## „Bellman-Rekursion“

$$P(x, i) = \begin{cases} P(x, i-1), & \text{falls } z_i > x \\ \max\{P(x, i-1), P(x - z_i, i-1) + p_i\} & \text{sonst} \end{cases}$$

1. Objekt  $i$  ist zu teuer für Kostenschranke  $x$ , falls  $z_i > x$

2. Objekt  $i$  ist nicht zu teuer, bringt aber keine Verbesserung

3. Objekt  $i$  ist nicht zu teuer und bringt eine Verbesserung

$i \backslash x$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	0	6	6	6	6	6	6	6	6
2	0	0	6	6	6	11	11	11	11	11
3	0	0	6	6	6	11	11	11	14	14
4	0	0	6	6	6	11	11	11	14	15
5	0	0	6	6	6	11	11	12	14	15
6	0	0	6	6	6	11	11	12	14	15
7	0	0	6	6	6	11	11	12	14	15

# Historie



Richard Bellman (1920-1984)

## DYNAMIC PROGRAMMING

BY

RICHARD BELLMAN

1957

PRINCETON UNIVERSITY PRESS  
PRINCETON, NEW JERSEY

### Preface

The purpose of this work is to provide an introduction to the mathematical theory of multi-stage decision processes. Since these constitute a somewhat formidable set of terms we have coined the term “dynamic programming” to describe the subject matter. Actually, as we shall see, the distinction involves more than nomenclature. Rather, it involves a certain conceptual framework which furnishes us a new and versatile mathematical tool for the treatment of many novel and interesting problems both in this new discipline and in various parts of classical analysis. Before expanding upon this theme, let us present a brief discussion of what is meant by a multi-stage decision process.

The functional equations which arise in this way are of a novel type, completely different from any of the functional equations encountered in classical analysis. The particular one we shall employ for purposes of discussion in this chapter is

$$(1) \quad f(x) = \text{Max}_{0 \leq y \leq x} [g(y) + h(x - y) + f(ay + b(x - y))].$$

where  $g$  and  $h$  are known functions and  $a$  and  $b$  are known constants, satisfying the condition  $0 \leq a, b < 1$ .

# Algorithmus

## Algorithmus 2.5 (Dynamic Programming für Knapsack)

**Eingabe:**  $z_1, \dots, z_n, Z, p_1, \dots, p_n$

**Ausgabe:** Funktion  $P : \{1, \dots, Z\} \times \{1, \dots, n\} \rightarrow \mathbb{R}; (x, i) \mapsto P(x, i)$

mit  $P(x, i) = \max \sum_{j=1}^i p_j y_j$  mit  $\sum_{j=1}^i z_j y_j \leq x$ , für  $y_j \in \{0, 1\}$

1: **for** ( $x = 0$ ) to  $Z$  **do**  
 2:      $P(x, 0) := 0$

3: **for** ( $i = 1$ ) to  $n$  **do**

4:     **for** ( $x = 0$ ) to  $(z_i - 1)$  **do**  
 5:          $P(x, i) := P(x, i - 1)$

6:     **for** ( $x = z_i$ ) to  $Z$  **do**

7:         **if** ( $(P(x - z_i, i - 1) + p_i) > P(x, i - 1)$ ) **then**  
 8:              $P(x, i) := P(x - z_i, i - 1) + p_i$

9:         **else**

0:              $P(x, i) := P(x, i - 1)$

$i \backslash x$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	0	6	6	6	6	6	6	6	6
2	0	0	6	6	6	11	11	11	11	11
3	0	0	6	6	6	11	11	11	14	14
4	0	0	6	6	6	11	11	11	14	15
5	0	0	6	6	6	11	11	12	14	15
6	0	0	6	6	6	11	11	12	14	15
7	0	0	6	6	6	11	11	12	14	15

# Korrektheit und Laufzeit

**Satz 2.6** Algorithmus 2.5 berechnet besten Lösungswert für das Rucksackproblem in einer Laufzeit  $O(nZ)$ .

**Algorithmus 2.5** (Dynamic Programming für Knapsack)

**Eingabe:**  $z_1, \dots, z_n, Z, p_1, \dots, p_n$   
**Ausgabe:** Funktion  $P : \{1, \dots, Z\} \times \{1, \dots, n\} \rightarrow \mathbb{R}; (x, i) \mapsto P(x, i)$   
 mit  $P(x, i) = \max \sum_{j=1}^i p_j y_j$  mit  $\sum_{j=1}^i z_j y_j \leq x$ , für  $y_j \in \{0, 1\}$

```

1: for (x = 0) to Z do
2:   P(x, 0) := 0
3: for (i = 1) to n do
4:   for (x = 0) to (z_i - 1) do
5:     P(x, i) := P(x, i - 1)
6:   for (x = z_i) to Z do
7:     if ((P(x - z_i, i - 1) + p_i) > P(x, i - 1)) then
8:       P(x, i) := P(x - z_i, i - 1) + p_i
9:     else
0:       P(x, i) := P(x, i - 1)
    
```

$O(nZ)$  {

x \ i	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	0	6	6	6	6	6	6	6	6
2	0	0	6	6	6	11	11	11	11	11
3	0	0	6	6	6	11	11	11	14	14
4	0	0	6	6	6	11	11	11	14	15
5	0	0	6	6	6	11	11	12	14	15
6	0	0	6	6	6	11	11	12	14	15
7	0	0	6	6	6	11	11	12	14	15

## Induktion!

- Objekt  $i$  ist zu teuer für Kostenschranke  $x$ , falls  $z_i > x$
- Objekt  $i$  ist nicht zu teuer, bringt aber keine Verbesserung
- Objekt  $i$  ist nicht zu teuer und bringt eine Verbesserung

# Sparsamer?!

## Limitierender Faktor bei Dynamic Programming?

- Laufzeit?
- Speicherplatz!

$$O(nZ)$$

Idee:

- Nicht ganze Tabelle speichern
- Nur die relevante Zeile

$i \backslash x$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	0	6	6	6	6	6	6	6	6
2	0	0	6	6	6	11	11	11	11	11
3	0	0	6	6	6	11	11	11	14	14
4	0	0	6	6	6	11	11	11	14	15
5	0	0	6	6	6	11	11	12	14	15
6	0	0	6	6	6	11	11	12	14	15
7	0	0	6	6	6	11	11	12	14	15



# Sparsamer!

Ideen:

- Nur die jeweils letzte Zeile wird benötigt

- Updates von rechts nach links, damit nur erledigte Werte überschrieben werden

$i \backslash x$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	0	6	6	6	6	6	6	6	6
2	0	0	6	6	6	11	11	11	11	11
3	0	0	6	6	6	11	11	11	14	14
4	0	0	6	6	6	11	11	11	14	15
5	0	0	6	6	6	11	11	12	14	15
6	0	0	6	6	6	11	11	12	14	15
7	0	0	6	6	6	11	11	12	14	15

# Algorithmus (sparsamer)

**Algorithmus 2.7** (*Dynamic Programming für Knapsack - sparsamer*)

**Eingabe:**  $z_1, \dots, z_n, Z, p_1, \dots, p_n$

**Ausgabe:** Funktion  $P : \{1, \dots, Z\} \times \{1, \dots, n\} \rightarrow \mathbb{R}; (x, i) \mapsto P(x, i)$

mit  $P(x, i) = \max \sum_{j=1}^i p_j y_j$  mit  $\sum_{j=1}^i z_j y_j \leq x$ , für  $y_j \in \{0, 1\}$

1: **for** ( $x = 0$ ) to  $Z$  **do**

2:      $P(x, 0) := 0$

3: **for** ( $i = 1$ ) to  $n$  **do**

4:     **for** ( $x = Z$ ) **downto**  $z_i$  **do**

5:         **if** ( $(P(x - z_i) + p_i) > P(x)$ ) **then**

6:              $P(x, i) := P(x - z_i) + p_i$

7: **return**  $p^* := P(Z)$

# Korrektheit und Laufzeit

**Satz 2.8** *Algorithmus 2.7* berechnet besten Lösungswert für das Rucksackproblem in einer Laufzeit  $O(nZ)$ .

**Algorithmus 2.5** (Dynamic Programming für Knapsack)

**Eingabe:**  $z_1, \dots, z_n, Z, p_1, \dots, p_n$

**Ausgabe:** Funktion  $P : \{1, \dots, Z\} \times \{1, \dots, n\} \rightarrow \mathbb{R}; (x, i) \mapsto P(x, i)$

mit  $P(x, i) = \max \sum_{j=1}^i p_j y_j$  mit  $\sum_{j=1}^i z_j y_j \leq x$ , für  $y_j \in \{0, 1\}$

1: **for** ( $x = 0$ ) **to**  $Z$  **do**

2:  $P(x, 0) := 0$

3: **for** ( $i = 1$ ) **to**  $n$  **do**

4: **for** ( $x = 0$ ) **to**  $(z_i - 1)$  **do**

5:  $P(x, i) := P(x, i - 1)$

6: **for** ( $x = z_i$ ) **to**  $Z$  **do**

7: **if**  $((P(x - z_i, i - 1) + p_i) > P(x, i - 1))$  **then**

8:  $P(x, i) := P(x - z_i, i - 1) + p_i$

9: **else**

0:  $P(x, i) := P(x, i - 1)$

**Algorithmus 2.7** (Dynamic Programming für Knapsack - sparsamer)

**Eingabe:**  $z_1, \dots, z_n, Z, p_1, \dots, p_n$

**Ausgabe:** Funktion  $P : \{1, \dots, Z\} \times \{1, \dots, n\} \rightarrow \mathbb{R}; (x, i) \mapsto P(x, i)$

mit  $P(x, i) = \max \sum_{j=1}^i p_j y_j$  mit  $\sum_{j=1}^i z_j y_j \leq x$ , für  $y_j \in \{0, 1\}$

1: **for** ( $x = 0$ ) **to**  $Z$  **do**

2:  $P(x, 0) := 0$

3: **for** ( $i = 1$ ) **to**  $n$  **do**

4: **for** ( $x = Z$ ) **downto**  $z_i$  **do**

5: **if**  $((P(x - z_i) + p_i) > P(x))$  **then**

6:  $P(x, i) := P(x - z_i) + p_i$

7: **return**  $p^* := P(Z)$

$O(nZ)$



$$P(x, i) = \begin{cases} P(x, i-1), \\ \max\{P(x, i-1), \dots\} \end{cases}$$

$x \backslash i$	0	1	2	3	3	5
0	1	0	0	0	0	0
1	1	0	0	0	0	0
2	1	0	0	0	0	+13
3						

## 2.3 Andere Beispiele für Dynamic Programming

*Algorithmen und Datenstrukturen 2  
Sommer 2023*

**Prof. Dr. Sándor Fekete**

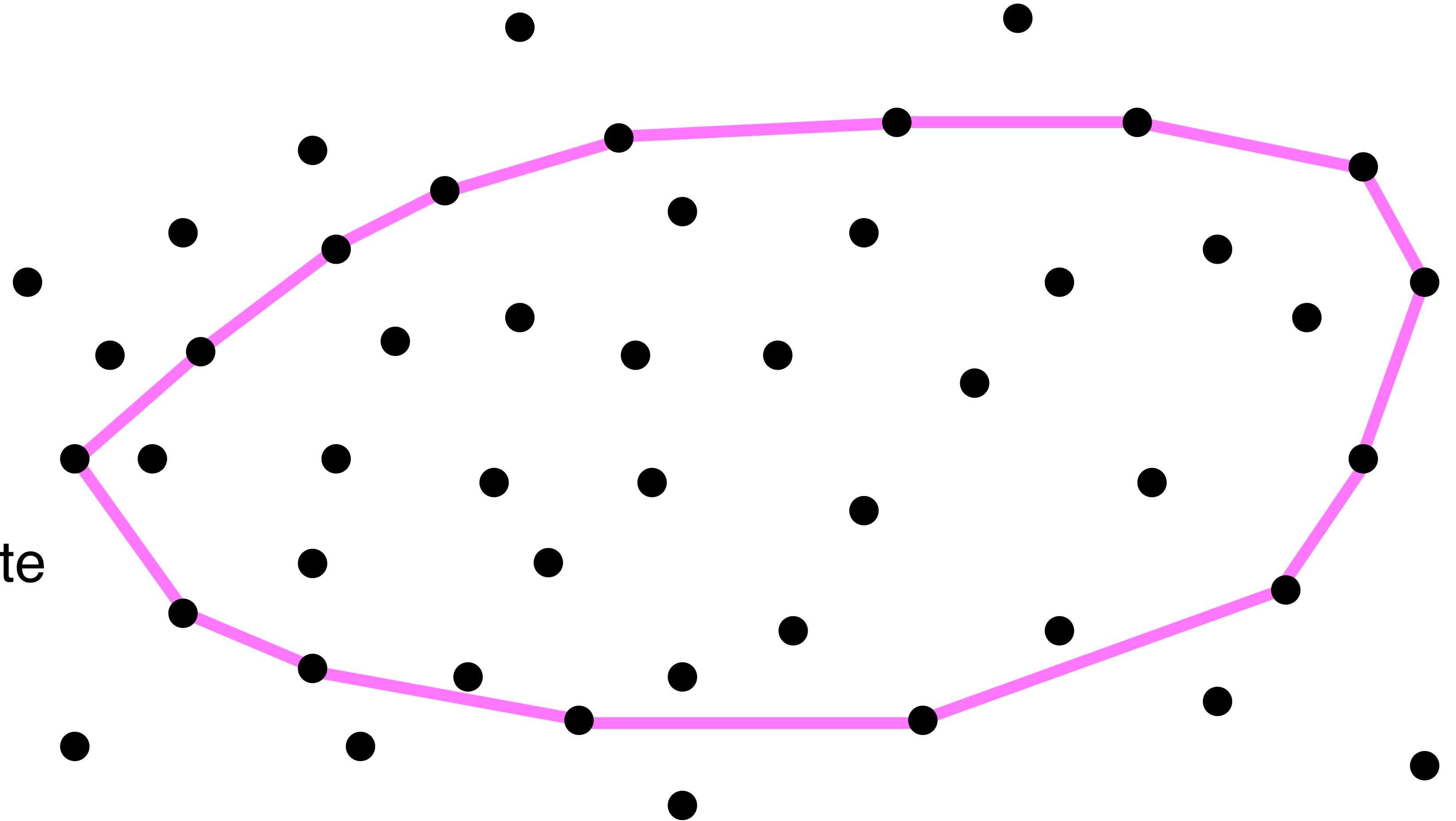
# Längste konvexe Kette

**Gegeben:**

Punktmenge

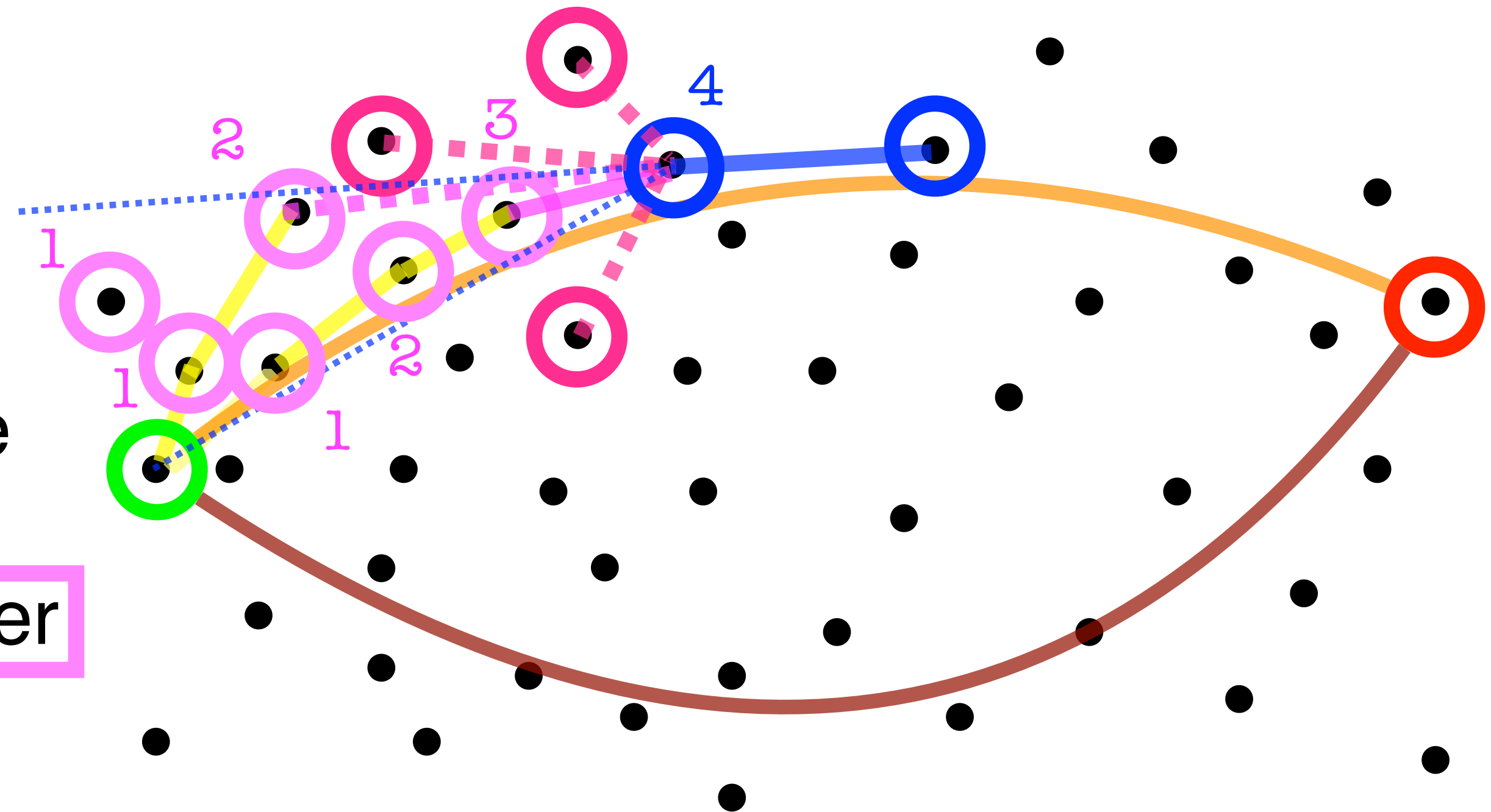
**Gesucht:**

Längste konvexe Kette



# Idee

1. Enumeriere Startpunkt
- 1.1 Enumeriere Endpunkt
- 1.1.1. Betrachte obere und untere Kette
- 1.1.1.1 Für jedes Punktepaar:
- 1.1.1.1.1 Ermittle besten Vorgänger



# Optimale Triangulation

## Gegeben:

„Einfaches“ Polygon  
(mit zusammenhängendem Rand)

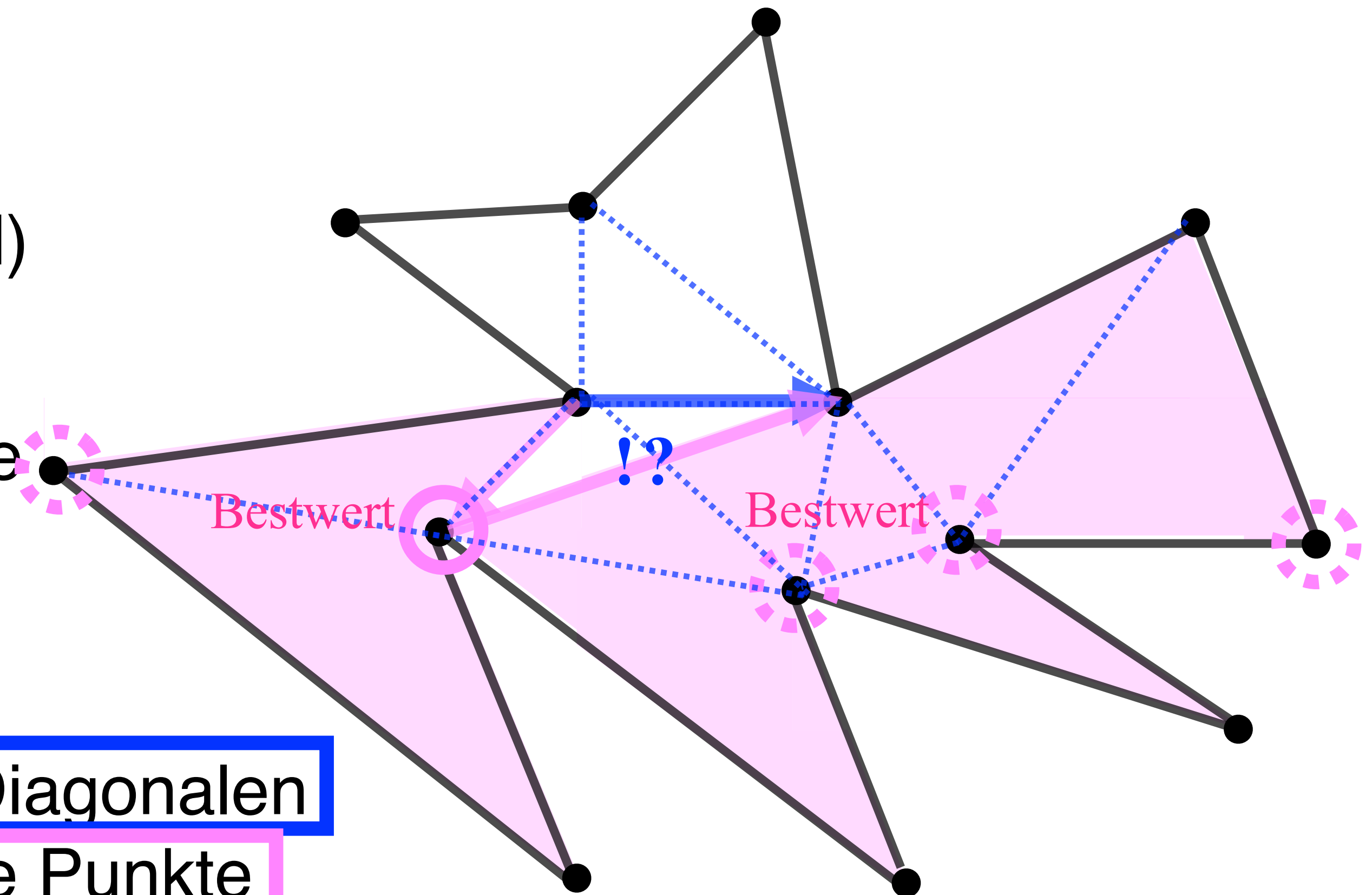
## Gesucht:

Optimale Unterteilung in Dreiecke  
durch „Diagonalen“

## Idee:

1. Berechne für alle (gerichtete) Diagonalen

1.1. Optimiere über möglich dritte Punkte



# Andere geometrische Probleme

CCCG 2014, Halifax, Nova Scotia, August 11–13, 2014

## On the Chromatic Art Gallery Problem

Sándor P. Fekete\*    Stephan Friedrichs\*    Michael Hemmer\*    Joseph B. M. Mitchell†  
 Christiane Schmidt\*

### Abstract

For a polygonal region  $P$  with  $n$  vertices, a *guard cover*  $S$  is a set of points in  $P$ , such that any point in  $P$  can be seen from a point in  $S$ . In a *colored guard cover*, every element in a guard cover is assigned a color, such that no two guards with the same color have overlapping visibility regions. The Chromatic Art Gallery Problem (CAGP) asks for the minimum number of colors for which a colored guard cover exists.

We discuss the CAGP for the case of only two colors. We show that it is already *NP*-hard to decide whether two colors suffice for covering a polygon with holes, even when arbitrary guard positions are allowed. For simple polygons with a discrete set of possible guard locations, we give a polynomial-time algorithm for deciding whether a two-colorable guard set exists. This algo-

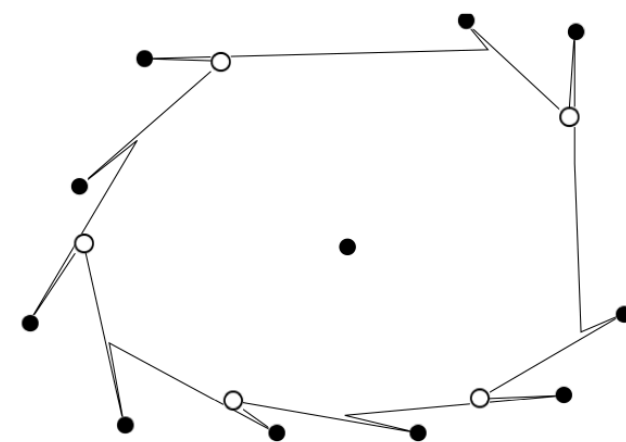


Figure 1: An example polygon with  $n = 20$  vertices. A minimum-cardinality guard cover with  $n/4$  guards (shown in white) requires  $n/4$  colors, while a minimum-color guard cover (shown in black) has  $n/2 + 1$  guards and requires only 3 colors.

**Theorem 4.1** For a simple polygon  $P$  with  $n$  vertices and  $\ell$  discrete guard locations  $L$ , it can be decided in polynomial time whether there is a 2-colorable guard set.

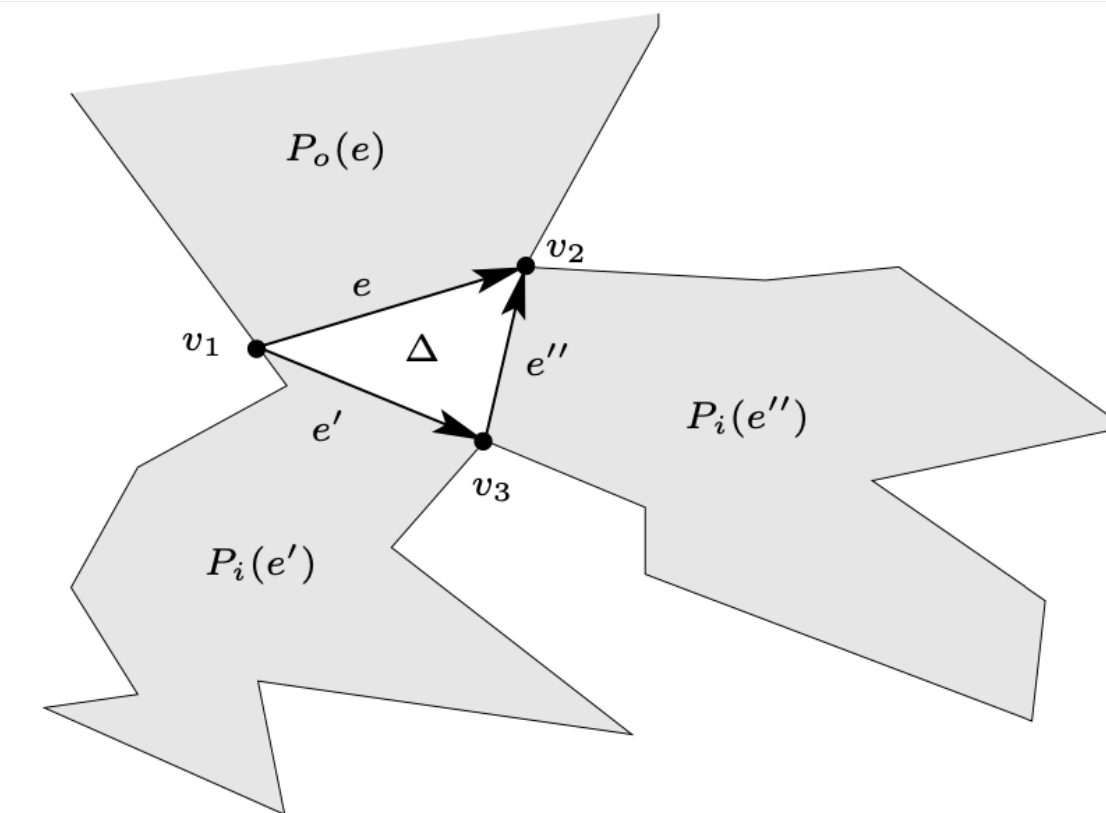


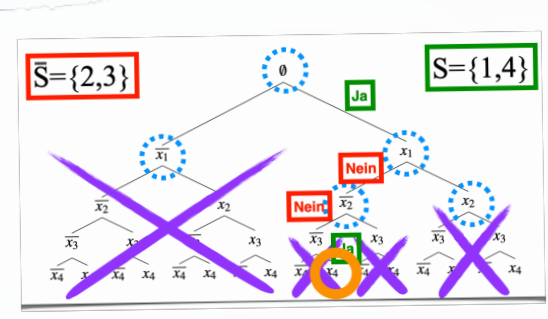
Figure 7: Solving a subproblem  $(e, \Gamma)$  by combining solutions for subproblems  $(e', \Gamma')$  and  $(e'', \Gamma'')$ .





$$\sum_{i=1}^n x_i z_i \leq Z$$

$x_i \in [0, 1]$



## 3 Branch-and-Bound

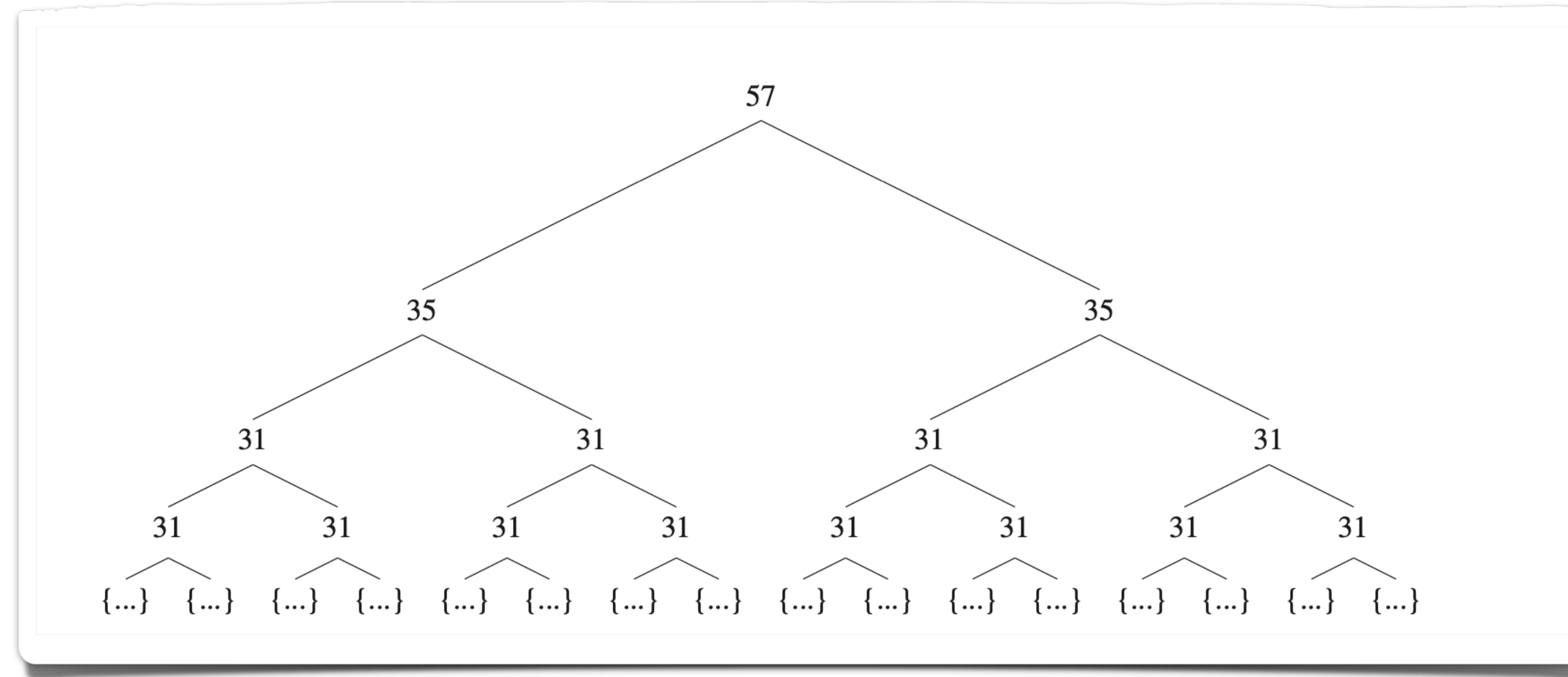
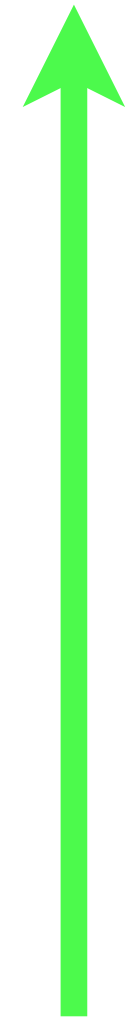
*Algorithmen und Datenstrukturen 2*  
*Sommer 2023*

**Prof. Dr. Sándor Fekete**

# 3.1 Motivation

# Enumerationsprinzip

Dynamic  
Programming

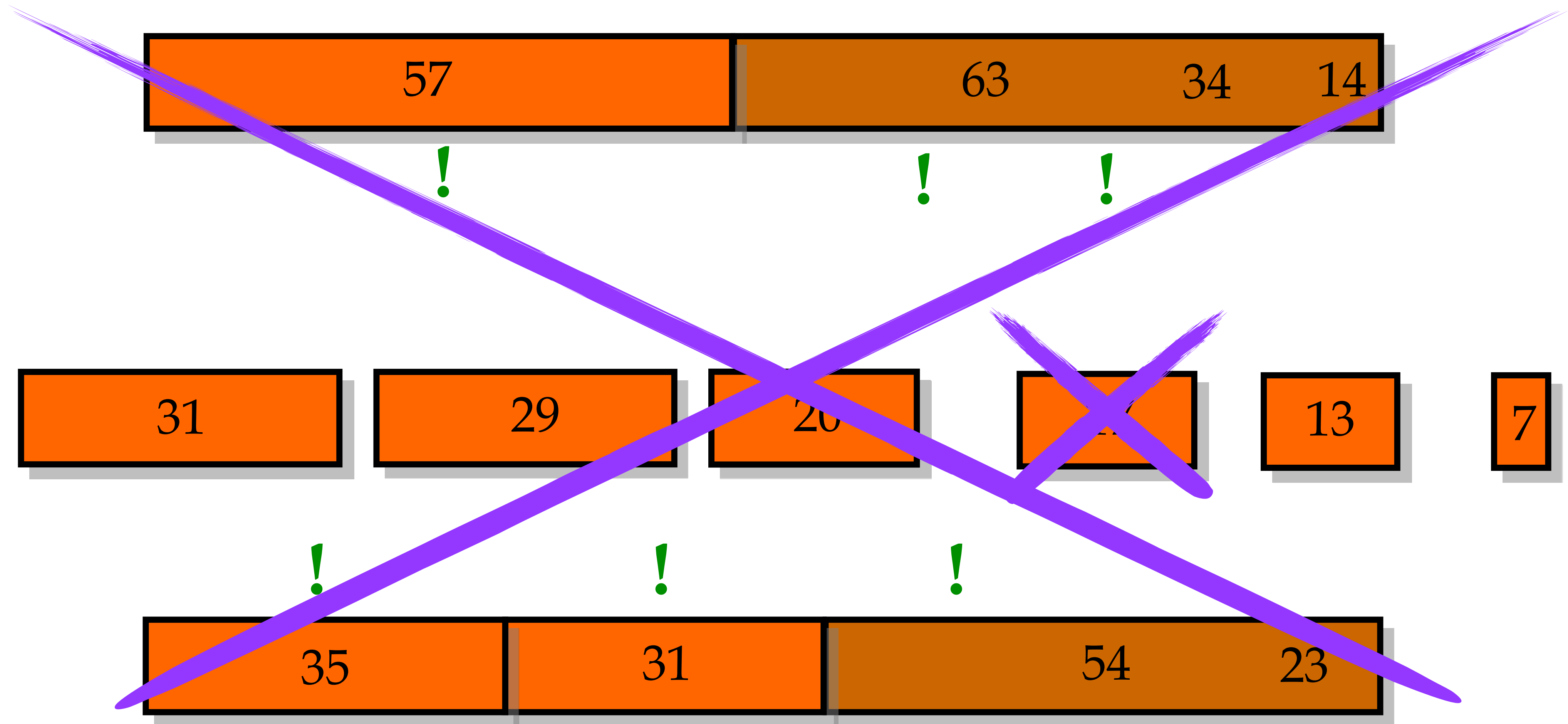


Branch and  
Bound



- Exponentiell viele Fälle!
- Wie geht das systematisch?
- Wo kann man Arbeit sparen?

# Zur Erinnerung: Subset Sum



# Dynamic Programming

**Satz 2.6** Algorithmus 2.5 berechnet besten Lösungswert für das Rucksackproblem in einer Laufzeit  $O(nZ)$ .

**Algorithmus 2.5** (Dynamic Programming für Knapsack)

**Eingabe:**  $z_1, \dots, z_n, Z, p_1, \dots, p_n$   
**Ausgabe:** Funktion  $P : \{1, \dots, Z\} \times \{1, \dots, n\} \rightarrow \mathbb{R}; (x, i) \mapsto P(x, i)$   
 mit  $P(x, i) = \max \sum_{j=1}^i p_j y_j$  mit  $\sum_{j=1}^i z_j y_j \leq x$ , für  $y_j \in \{0, 1\}$

```

1: for (x = 0) to Z do
2:   P(x, 0) := 0
3: for (i = 1) to n do
4:   for (x = 0) to (z_i - 1) do
5:     P(x, i) := P(x, i - 1)
6:   for (x = z_i) to Z do
7:     if ((P(x - z_i, i - 1) + p_i) > P(x, i - 1)) then
8:       P(x, i) := P(x - z_i, i - 1) + p_i
9:     else
0:       P(x, i) := P(x, i - 1)
    
```

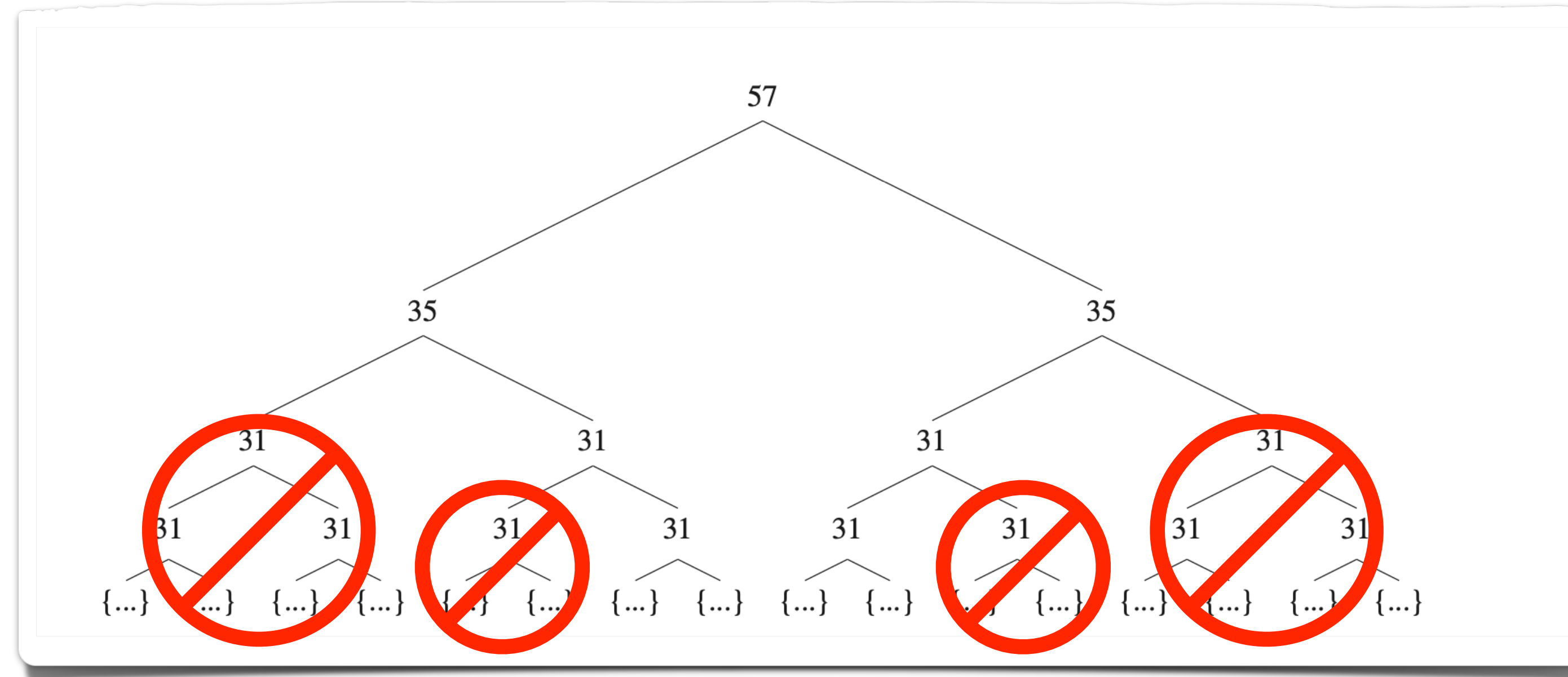
$O(nZ)$  {

$x \backslash i$	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	0	6	6	6	6	6	6	6	6
2	0	0	6	6	6	11	11	11	11	11
3	0	0	6	6	6	11	11	11	14	14
4	0	0	6	6	6	11	11	11	14	15
5	0	0	6	6	6	11	11	12	14	15
6	0	0	6	6	6	11	11	12	14	15
7	0	0	6	6	6	11	11	12	14	15

## Induktion!

- 1. Objekt  $i$  ist zu teuer für Kostenschranke  $x$ , falls  $z_i > x$
- 2. Objekt  $i$  ist nicht zu teuer, bringt aber keine Verbesserung
- 3. Objekt  $i$  ist nicht zu teuer und bringt eine Verbesserung

# Branch-and-Bound



Branch and Bound

- Beschneide Enumerationsbaum
- Verfolge Mindest- und Maximalwerte

# Historie

1960

## ECONOMETRICA

VOLUME 28

July, 1960

NUMBER 3

### AN AUTOMATIC METHOD OF SOLVING DISCRETE PROGRAMMING PROBLEMS

BY A. H. LAND AND A. G. DOIG

In the classical linear programming problem the behaviour of continuous, nonnegative variables subject to a system of linear inequalities is investigated. One possible generalization of this problem is to relax the continuity condition on the variables. This paper presents a simple numerical algorithm for the solution of programming problems in which some or all of the variables can take only discrete values. The algorithm requires no special techniques beyond those used in ordinary linear programming, and lends itself to automatic computing. Its use is illustrated on two numerical examples.

#### 1. INTRODUCTION

THERE IS A growing literature [1, 3, 5, 6] about optimization problems which could be formulated as linear programming problems with additional constraints that some or all of the variables may take only integral values. This form of linear programming arises whenever there are indivisibilities. It is not meaningful, for instance, to schedule 3-7/10 flights between two cities, or to undertake only 1/4 of the necessary setting up operation for running a job through a machine shop. Yet it is basic to linear programming that the variables are free to take on any positive value,<sup>1</sup> and this sort of answer is very likely to turn up.

In some cases, notably those which can be expressed as transport problems, the linear programming solution will itself yield discrete values of the variables. In other cases the percentage change in the maximand<sup>2</sup> from common sense rounding of the variables is sufficiently small to be neglected. But there remain many problems where the discrete variable constraints are significant and costly.

Until recently there was no general automatic routine for solving such problems, as opposed to procedures for proving the optimality of conjectured solutions, and the work reported here is intended to fill the gap. About the time of its completion an alternative method was proposed by Gomory [5] and subsequently extended by Beale [1]. Gomory's method

<sup>1</sup> Or more generally, any value within a bounded interval.

<sup>2</sup> We shall speak throughout of maximisation, but of course an exactly analogous argument applies to minimisation.

497



Ailsa H. Land

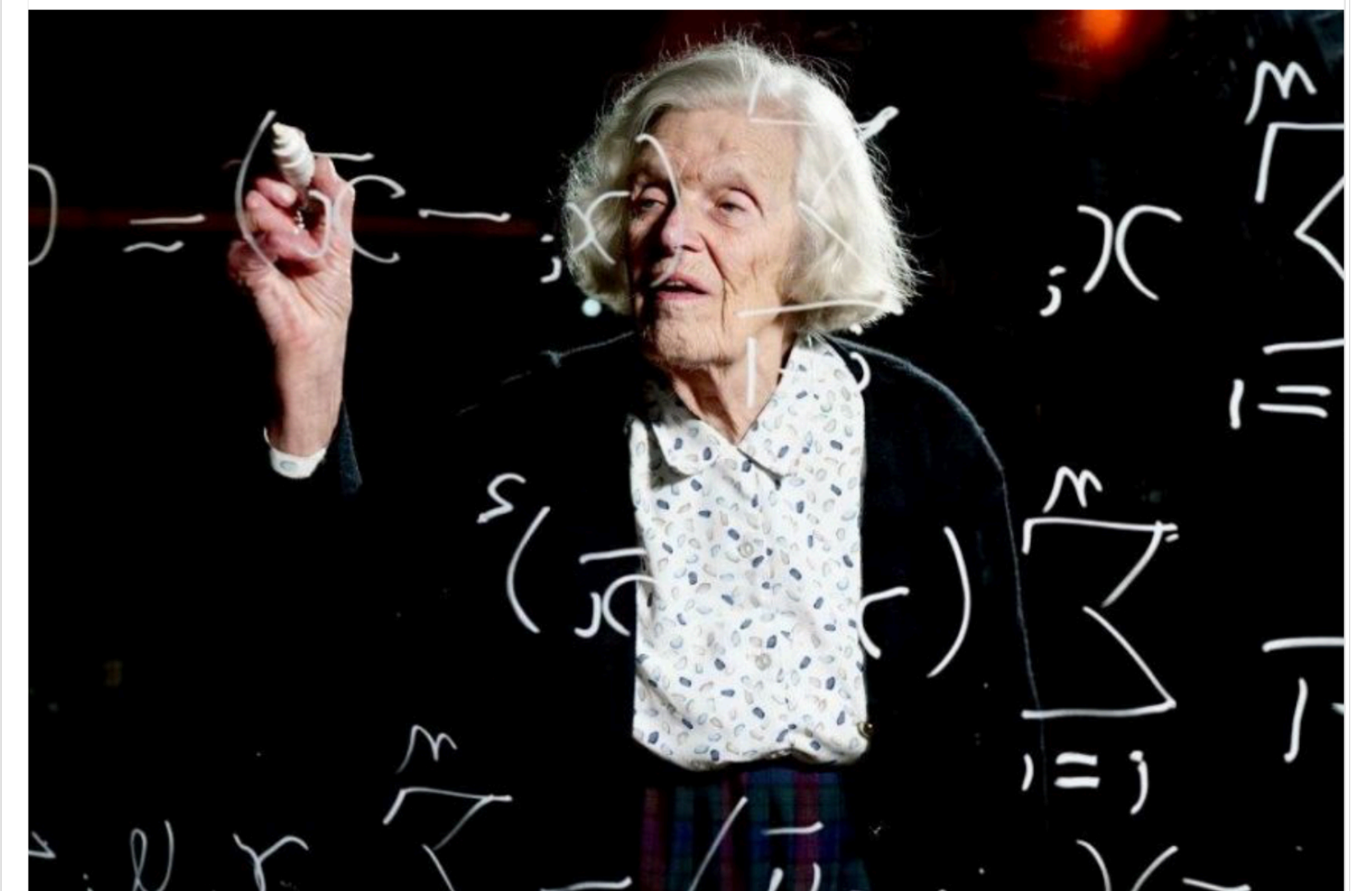


Alison Doig

## 'I've always loved numbers': Meet the ground-breaking grandmother of Australian mathematics

7.30 / By Lauren Day

Posted 8 Oct 2018, updated 10 Oct 2018



Alison Grant Harcourt AO

In June 2019, Harcourt was made an Officer of the Order of Australia

# 3.2 Methodik



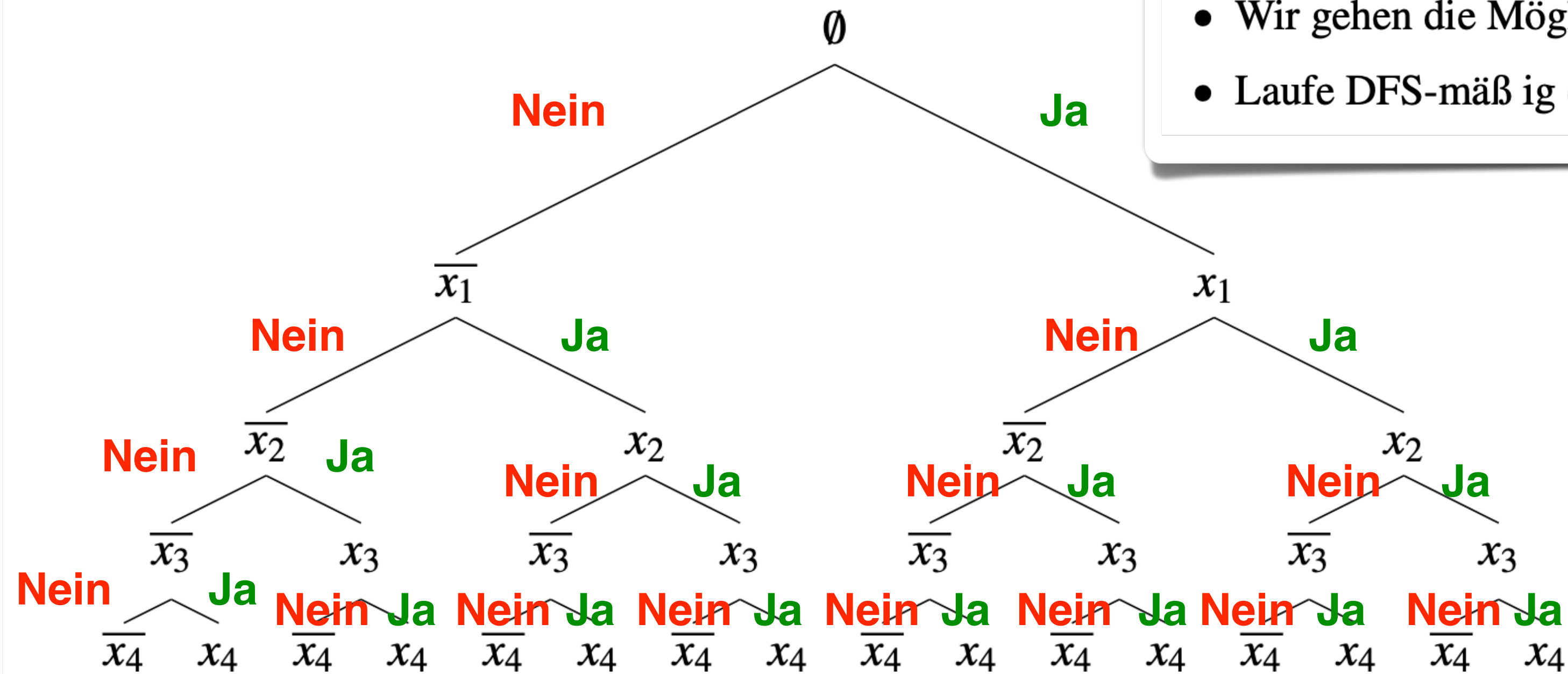
# Ideen

## Grundideen:

1. Enumeriere die möglichen Teilmengen in einem Enumerationsbaum
2. Behalte den Zielfunktionswert im Auge:
  - Untere Schranke: Erreichter Zielfunktionswert im ganzen Baum
  - Obere Schranke: Erreichbarer Zielfunktionswert im jeweiligen Baum
3. Beide Schranken sollten möglichst einfach und schnell zu berechnen sein
4. Wenn der erreichbare Wert in einem Teilbaum kleiner bleiben muss als der im ganzen Baum bereits erreichte, können wir den aktuellen Teilbaum abschneiden

# 1. Enumerationsbaum

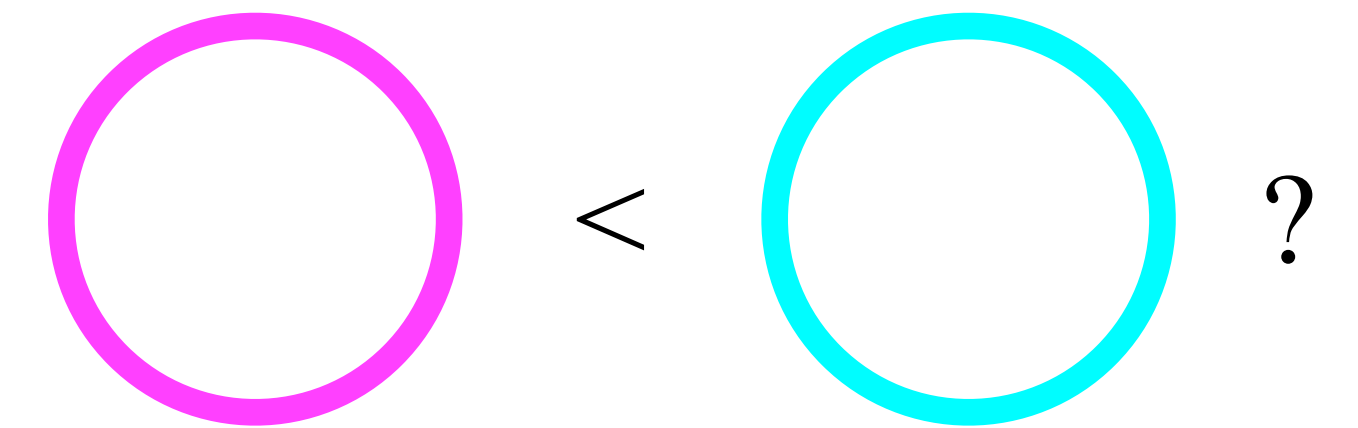
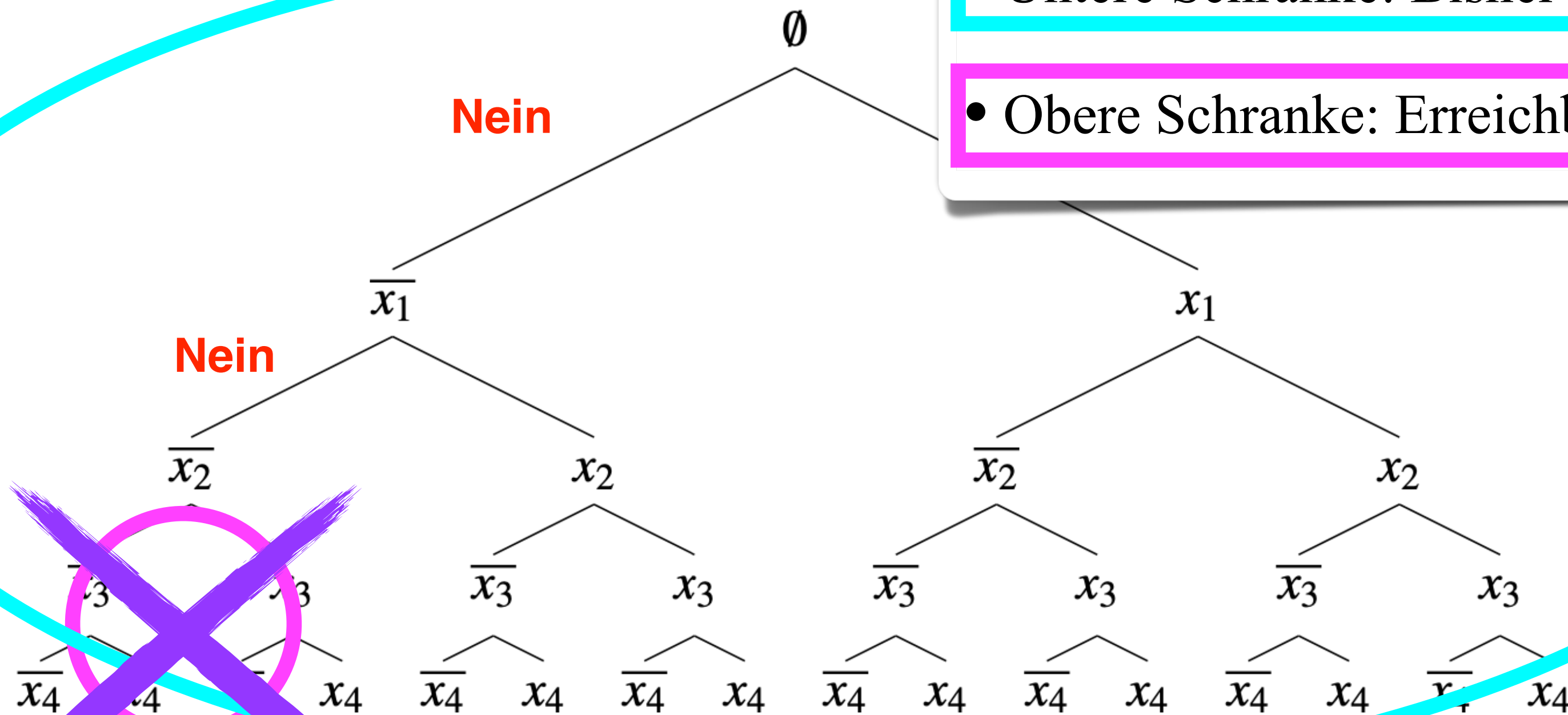
- Probiere nacheinander für  $i = 1, \dots, 7$ , ob  $x_i = 0$  oder  $x_i = 1$
- Wir gehen die Möglichkeiten baumartig durch:
- Laufe DFS-mäßig durch den Baum, d.h. arbeite die Entscheidungen im Stack ab.



# 4. Einsatz von Schranken - Grundidee

• Untere Schranke: Bisher erreichter Zielfunktionswert im ganzen Baum

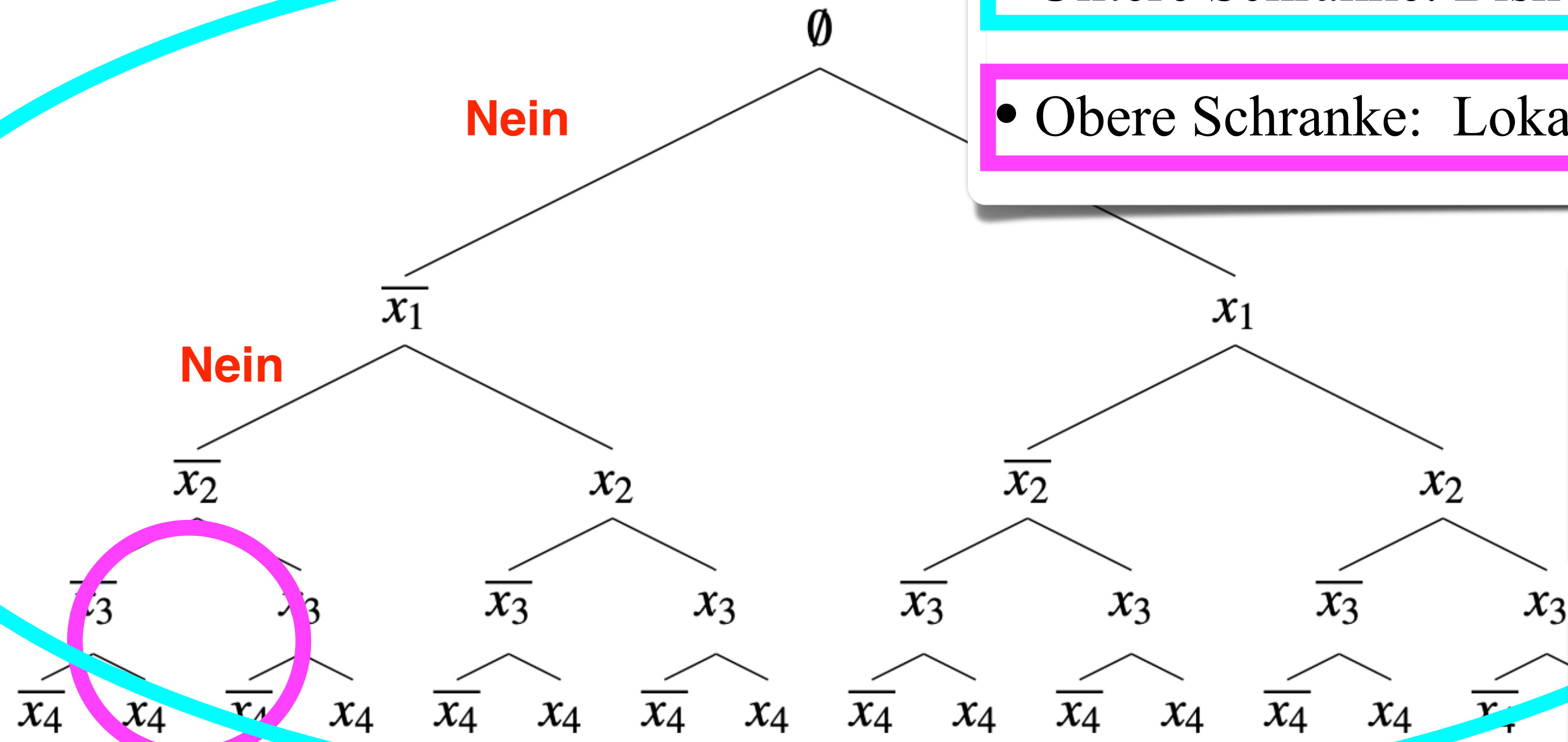
• Obere Schranke: Erreichbarer Zielfunktionswert im jeweiligen Teilbaum



Was sind geeignete Schranken?

# 2. Geeignete Schranken - Knapsack

- Untere Schranke: Bisheriger Bestwert für Greedy (ganzzahlig)
- Obere Schranke: Lokaler erreichbarer Bestwert für Greedy (fraktional)



$i$	6	4	13	12	9	3	15	8	16	10	1	14	5	11	2	7
$z_i$	4	8	16	20	8	40	40	40	24	32	20	20	16	28	32	32
$p_i$	4	5	10	9	2	10	10	9	4	5	3	3	2	3	3	2

$\sum_{i=1}^n p_i x_i = 44$

$i$	6	4	13	12	9	3	15	8	16	10	1	14	5	11	2	7
$z_i$	4	8	16	20	8	40	40	40	24	32	20	20	16	28	32	32
$p_i$	4	5	10	9	2	10	10	9	4	5	3	3	2	3	3	2

$\sum_{i=1}^n p_i x_i = 46$        $x_{15} = 0,6$

Relaxierung: Einfacher durch größere Lösungsmenge

# 3. Berechnung von Schranken

• Untere Schranke: Bisheriger Bestwert für Greedy (ganzzahlig)

• Obere Schranke: Lokaler erreichbarer Bestwert für Greedy (fraktional)

$i$	6	4	13	12	9	3	15	8	16	10	1	14	5	11	2	7
$z_i$	4	8	16	20	8	40	40	40	24	32	20	20	16	28	32	32
$p_i$	4	5	10	9	2	10	10	9	4	5	3	3	2	3	3	2

$\sum_{i=1}^n p_i x_i = 44$

$i$	6	4	13	12	9	3	15	8	16	10	1	14	5	11	2	7
$z_i$	4	8	16	20	8	40	40	40	24	32	20	20	16	28	32	32
$p_i$	4	5	10	9	2	10	10	9	4	5	3	3	2	3	3	2

$\sum_{i=1}^n p_i x_i = 46$        $x_{15} = 0,6$

Heuristik: Schnell zu lösen, aber nicht notwendig optimal

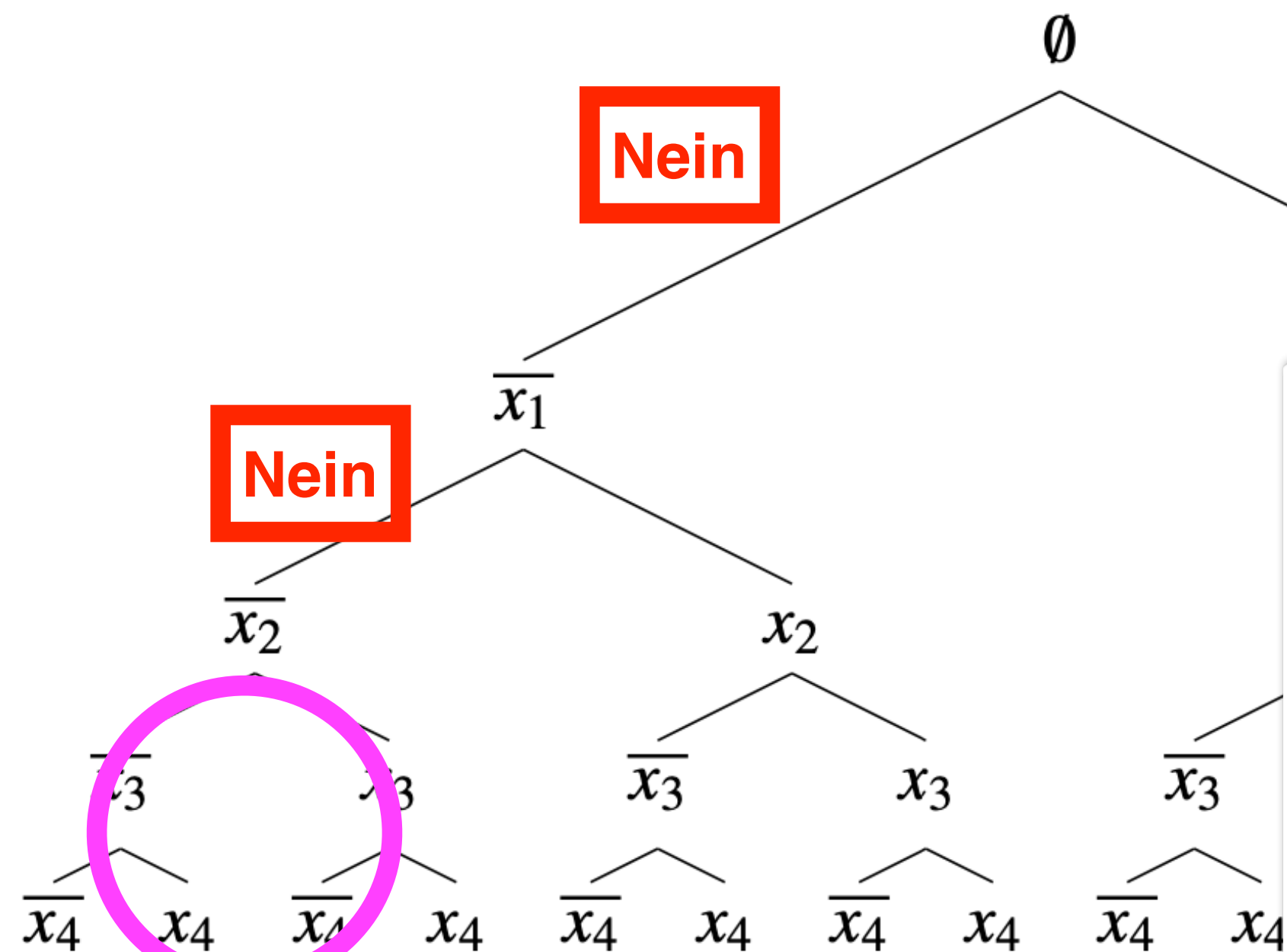
Relaxierung: Schnell und optimal zu lösen durch größere Lösungsmenge

# 3. Berechnung von Schranken II

S: positiv fixiert ( $x_i = 1$ )

S: negativ fixiert ( $x_i = 0$ )

Bisherige Entscheidungen fixieren Teilmenge!



$i$	<del>1</del>	<del>2</del>	3	3	5	6	7
$z_i$	<del>2</del>	<del>3</del>	6	7	5	9	4
$p_i$	<del>6</del>	<del>5</del>	8	9	6	7	3

# 3.3 Durchführung

# Beispiel: Knapsack

## Beispiel 2.4 (Knapsackproblem).

Sei  $Z = 9$  und seien folgende sieben Objekte gegeben:

$i$	1	2	3	4	5	6	7
$z_i$	2	3	6	7	5	9	4
$p_i$	6	5	8	9	6	7	3



# Untere Schranke: Greedy (ganzzahlig)

$$S = \emptyset$$

$$\bar{S} = \emptyset$$

$i$	1	2	3	4	5	6	7
$z_i$	2	3	6	7	5	9	4
$p_i$	6	5	8	9	6	7	3

$$Z = 9$$

$$i=7 : \sum_{i \in S} z_i = 9, \sum_{i \in S} p_i = 14$$

$$LB = 14$$

# Obere Schranke: Greedy (fraktional)

$$S = \emptyset$$

$$\bar{S} = \emptyset$$

$i$	1	2	3	4	5	6	7
$z_i$	2	3	6	7	5	9	4
$p_i$	6	5	8	9	6	7	3

$$Z = 9$$

$$i=2 : \sum_{i \in S} z_i = 5, \sum_{i \in S} p_i = 11$$

$$\text{Bleibt: } Z - \sum_{i \in S} z_i = 4, \text{ also } x_3 = \frac{2}{3} \left( = \frac{4}{6} = \frac{Z - \sum_{i \in S} z_i}{z_3} \right)$$

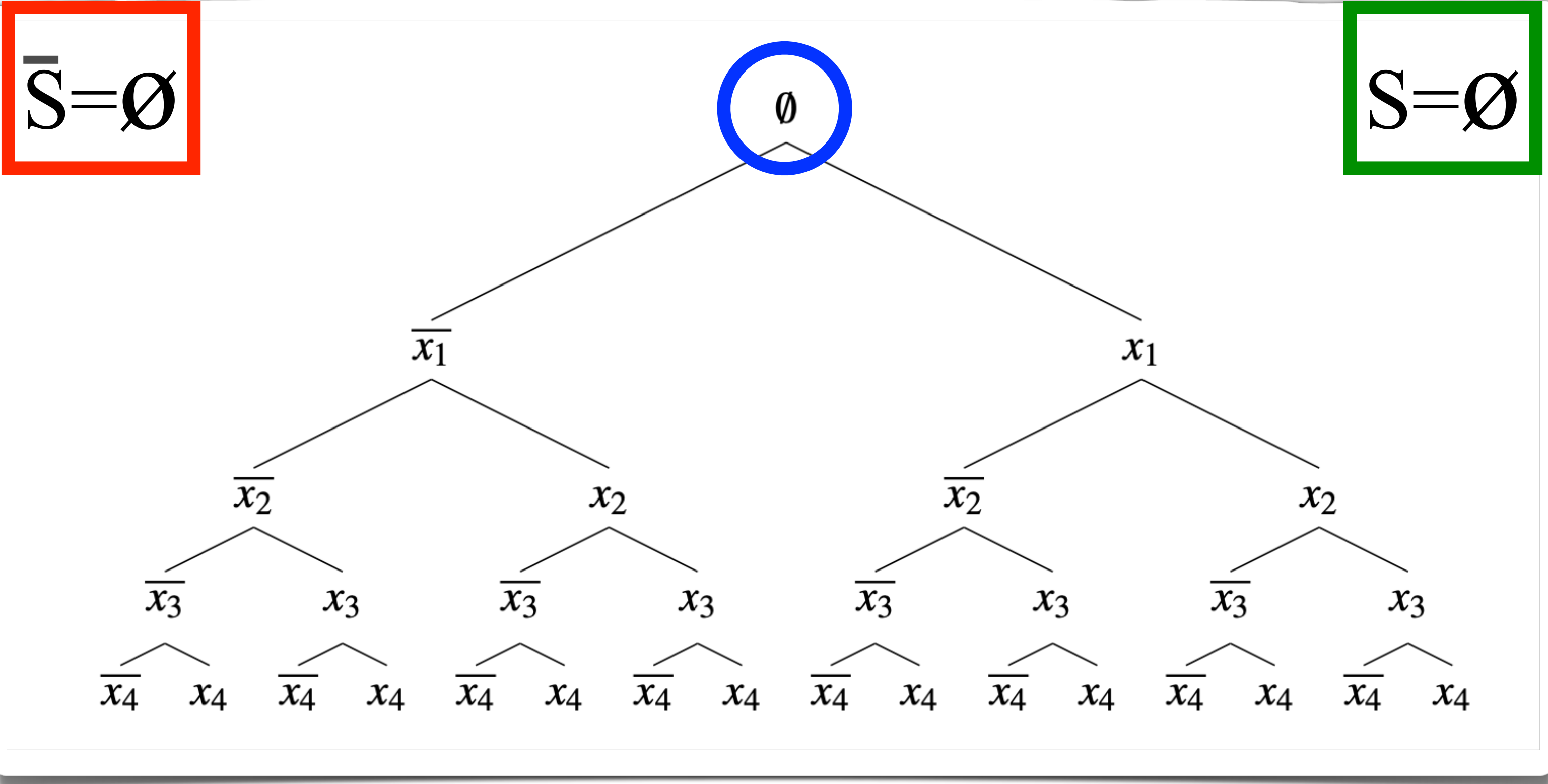
$$\text{Damit: } \sum_{i \in S} x_i z_i = 9, \sum_{i \in S} x_i p_i = 11 + \frac{2}{3} * 8 = 16, \bar{3}$$

$$UB = 16$$

# Gesamtbeispiel

$$\bar{S} = \emptyset$$

$$S = \emptyset$$



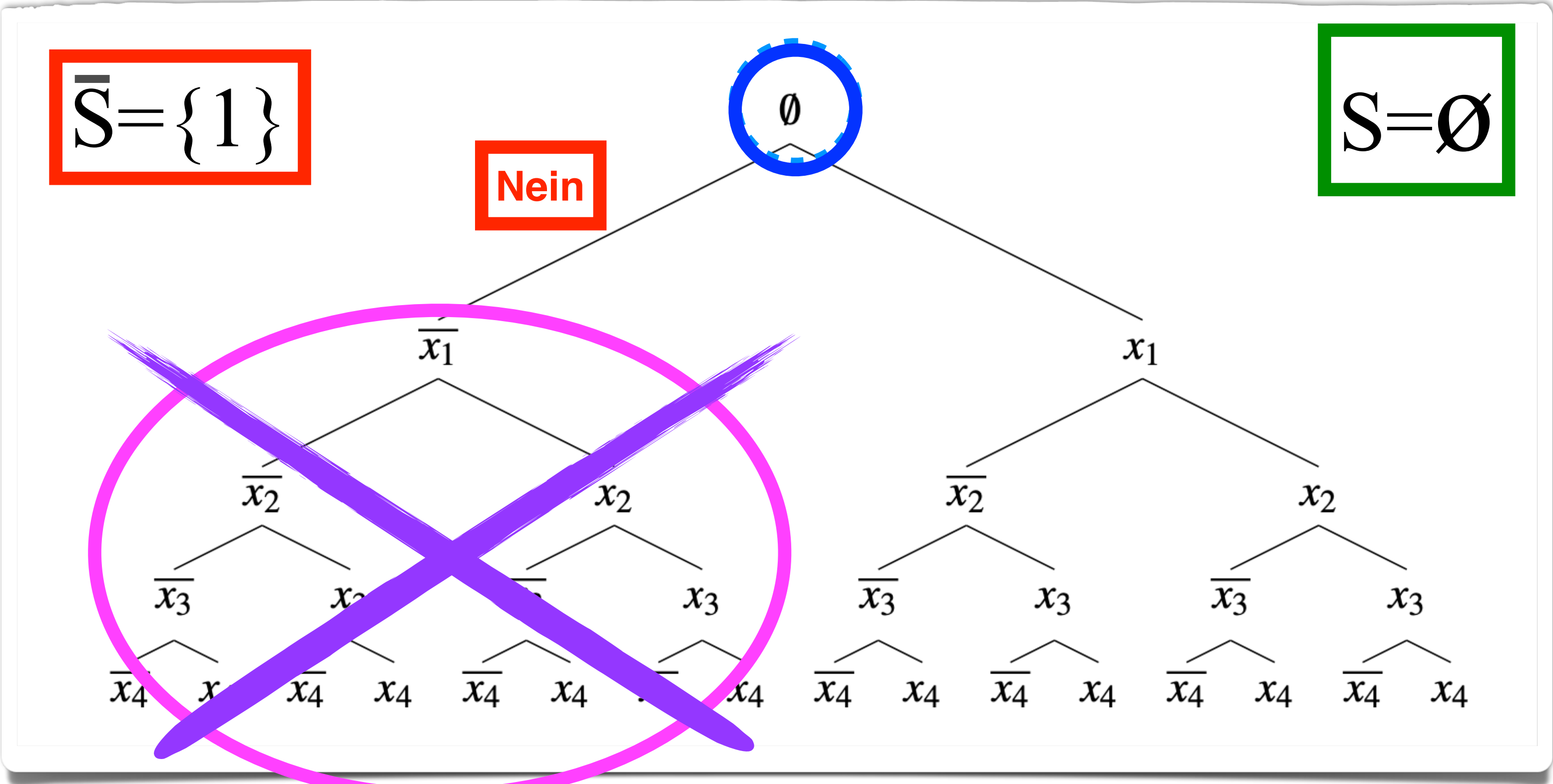
$i$	1	2	3	4	5	6	7
$z_i$	2	3	6	7	5	9	4
$p_i$	6	5	8	9	6	7	3

UB=16

$i$	1	2	3	4	5	6	7
$z_i$	2	3	6	7	5	9	4
$p_i$	6	5	8	9	6	7	3

LB=14

# Gesamtbeispiel



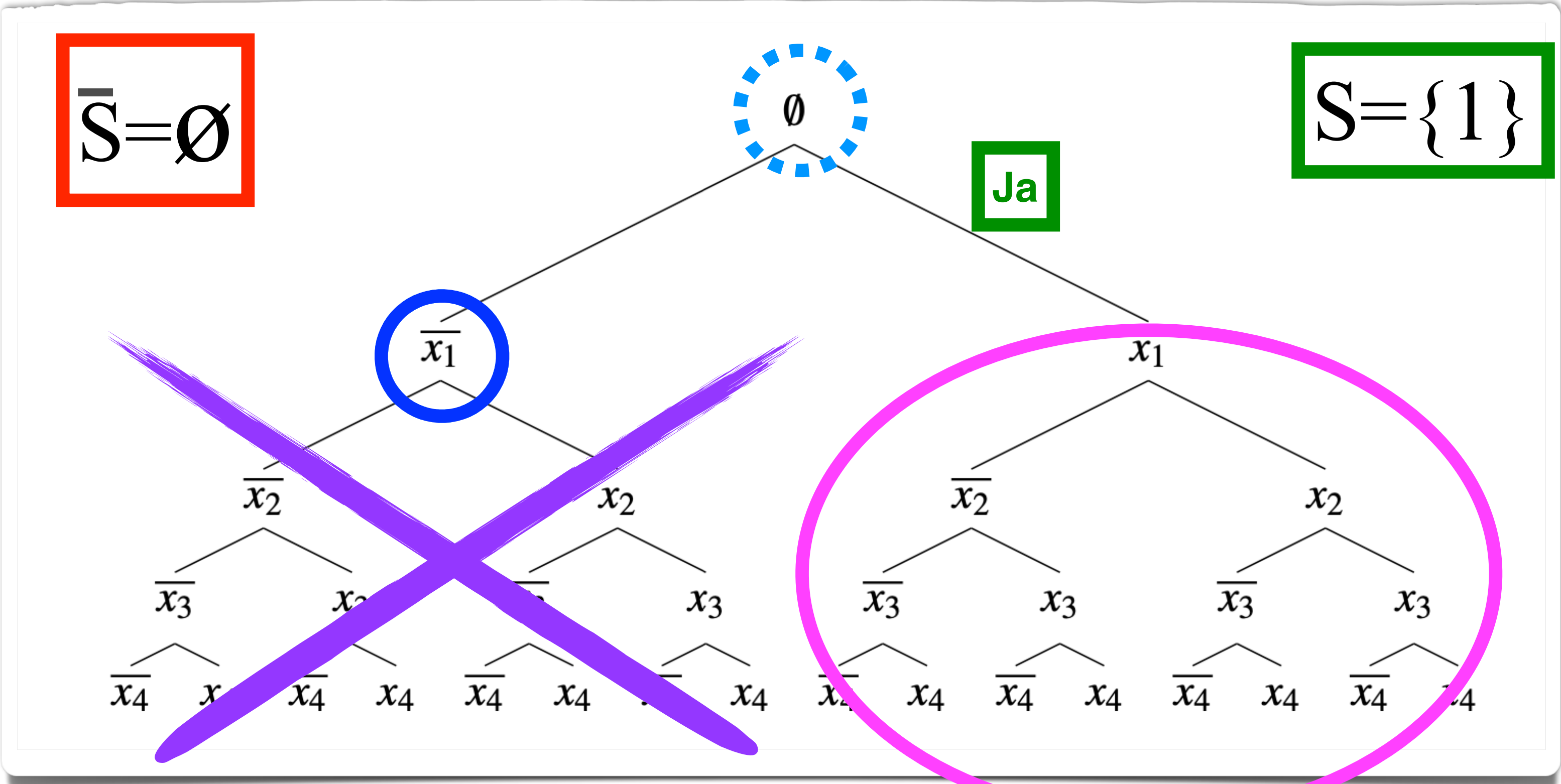
$i$	1	2	3	4	5	6	7
$z_i$	2	3	6	7	5	9	4
$p_i$	6	5	8	9	6	7	3

UB=13

$i$	1	2	3	5	6	7
$z_i$	2	3	6	5	9	4
$p_i$	6	5	8	9	7	3

LB=14

# Gesamtbeispiel



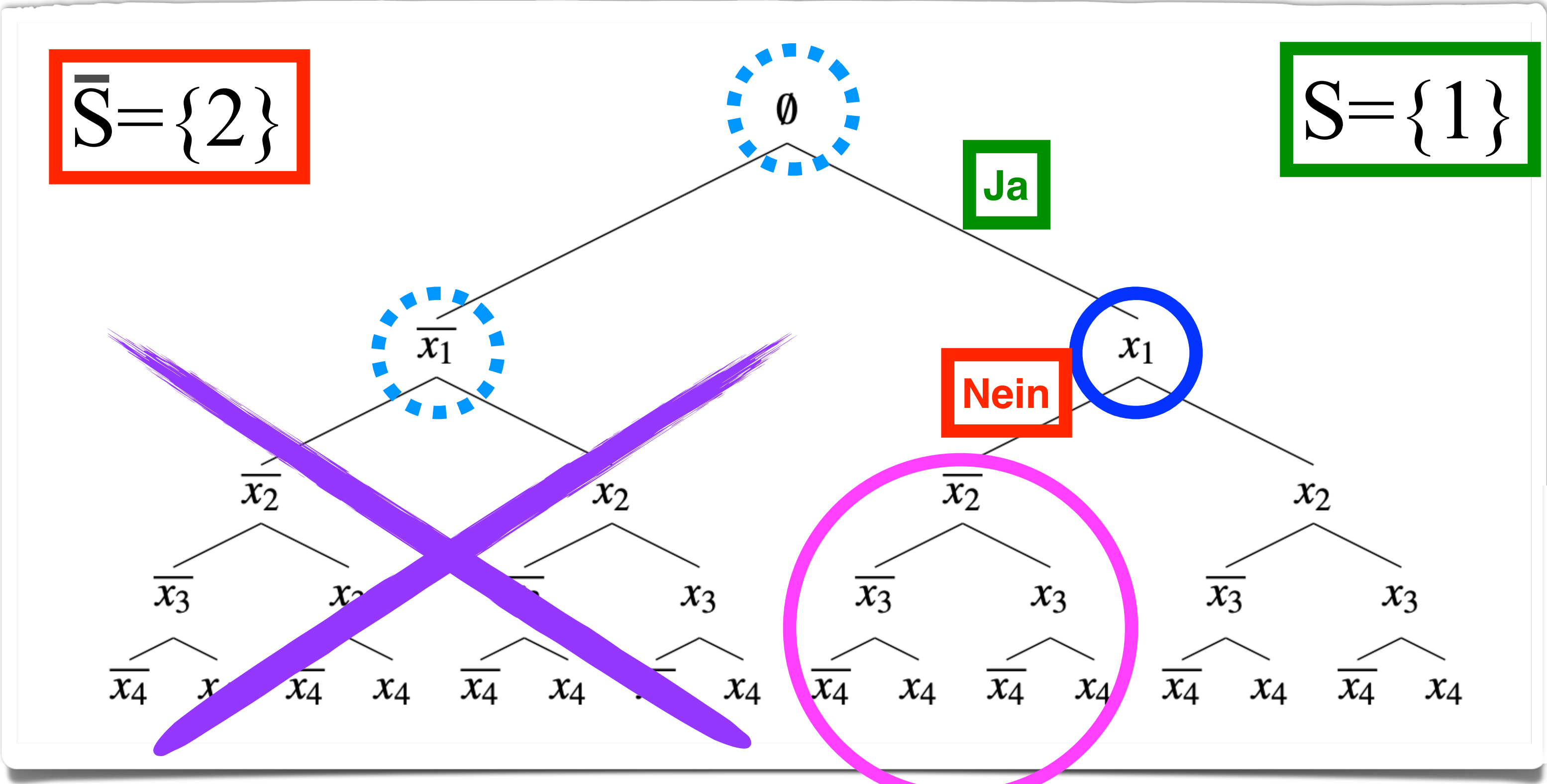
$i$	1	2	3	4	5	6	7
$z_i$	2	3	6	7	5	9	4
$p_i$	6	5	8	9	6	7	3

UB=16

$i$	1	2	3	4	5	6	7
$z_i$	2	3	6	7	5	9	4
$p_i$	6	5	8	9	6	7	3

LB=14

# Gesamtbeispiel



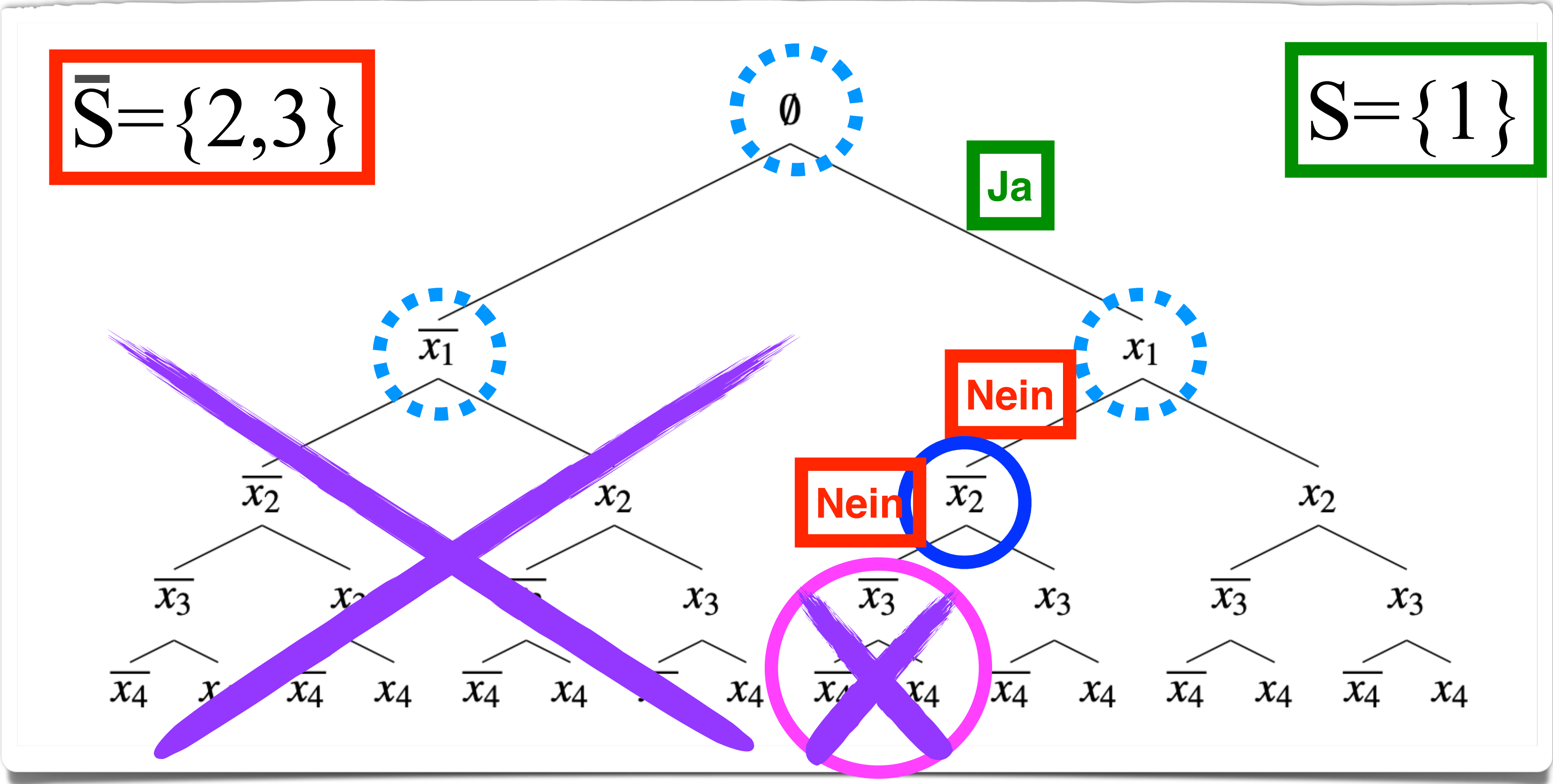
$i$	1	2	3	4	5	6	7
$z_i$	2	3	6	7	5	9	4
$p_i$	6	5	8	9	6	7	3

UB=15

$i$	1	2	3	4	5	6	7
$z_i$	2	3	6	7	5	9	4
$p_i$	6	5	8	9	6	7	3

LB=14

# Gesamtbeispiel



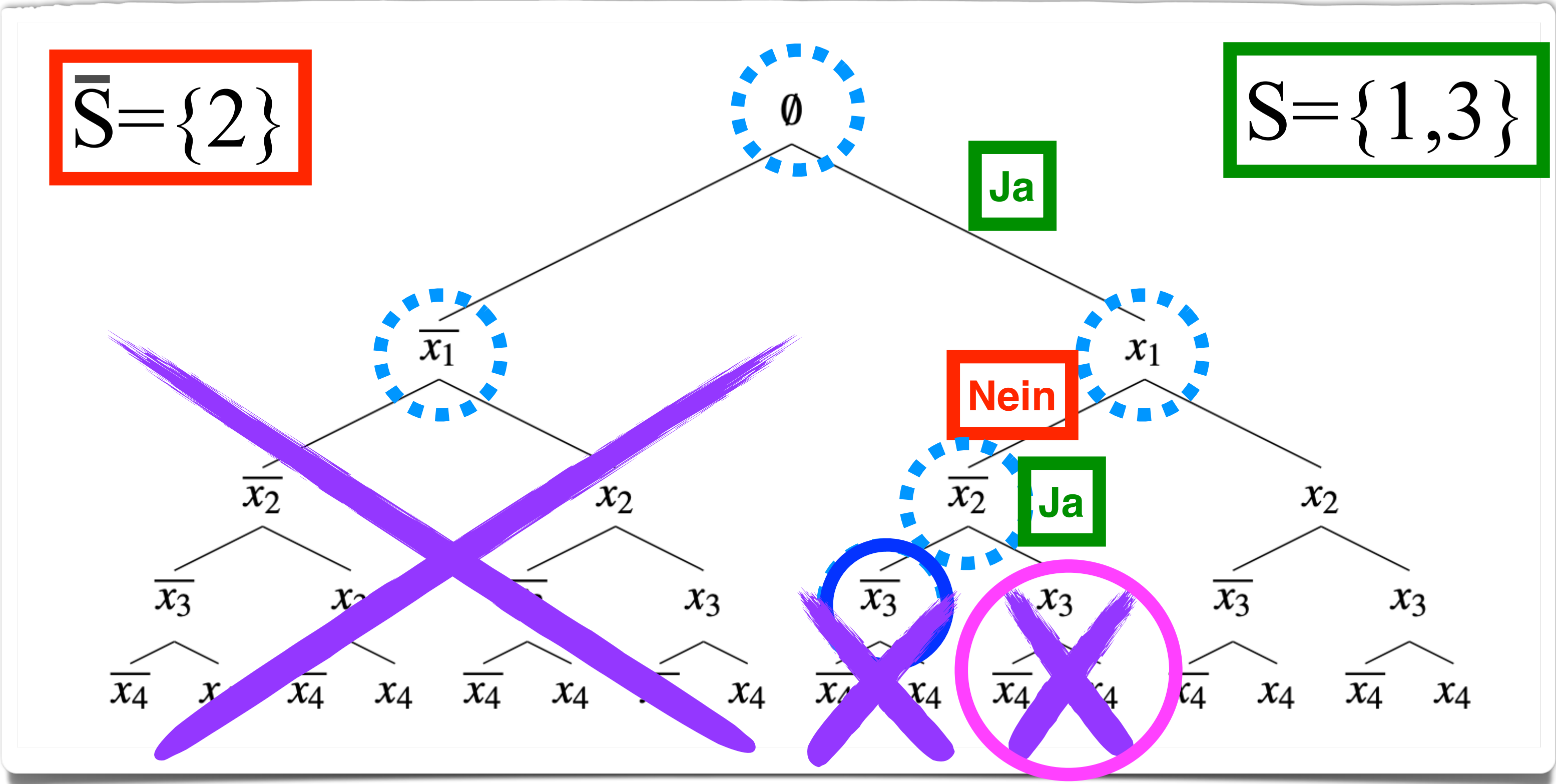
$i$	1	2	3	4	5	6	7
$z_i$	2	3	6	7	5	9	4
$p_i$	6	5	8	9	6	7	3

UB=15

$i$	1	2	3	4	5	6	7
$z_i$	2	3	6	7	5	9	4
$p_i$	6	5	8	9	6	7	3

LB=14

# Gesamtbeispiel



$i$	1	2	3	4	5	6	7
$z_i$	2	3	6	7	5	9	4
$p_i$	6	5	8	9	6	7	3

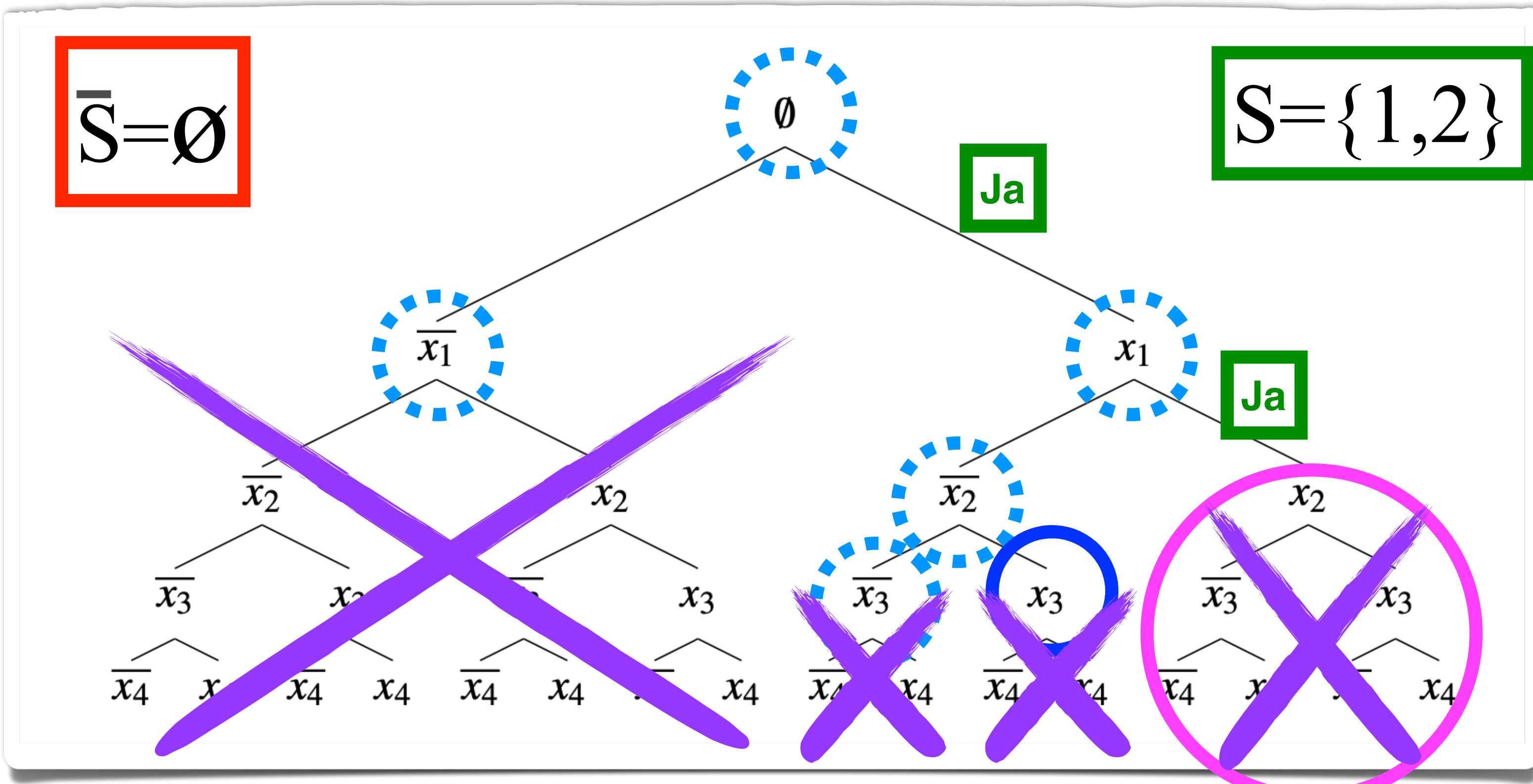
UB=15

$i$	1	2	3	4	5	6	7
$z_i$	2	3	6	7	5	9	4
$p_i$	6	5	8	9	6	7	3

LB=15



# Gesamtbeispiel



↓ ↓ ↓ ↓ ↓

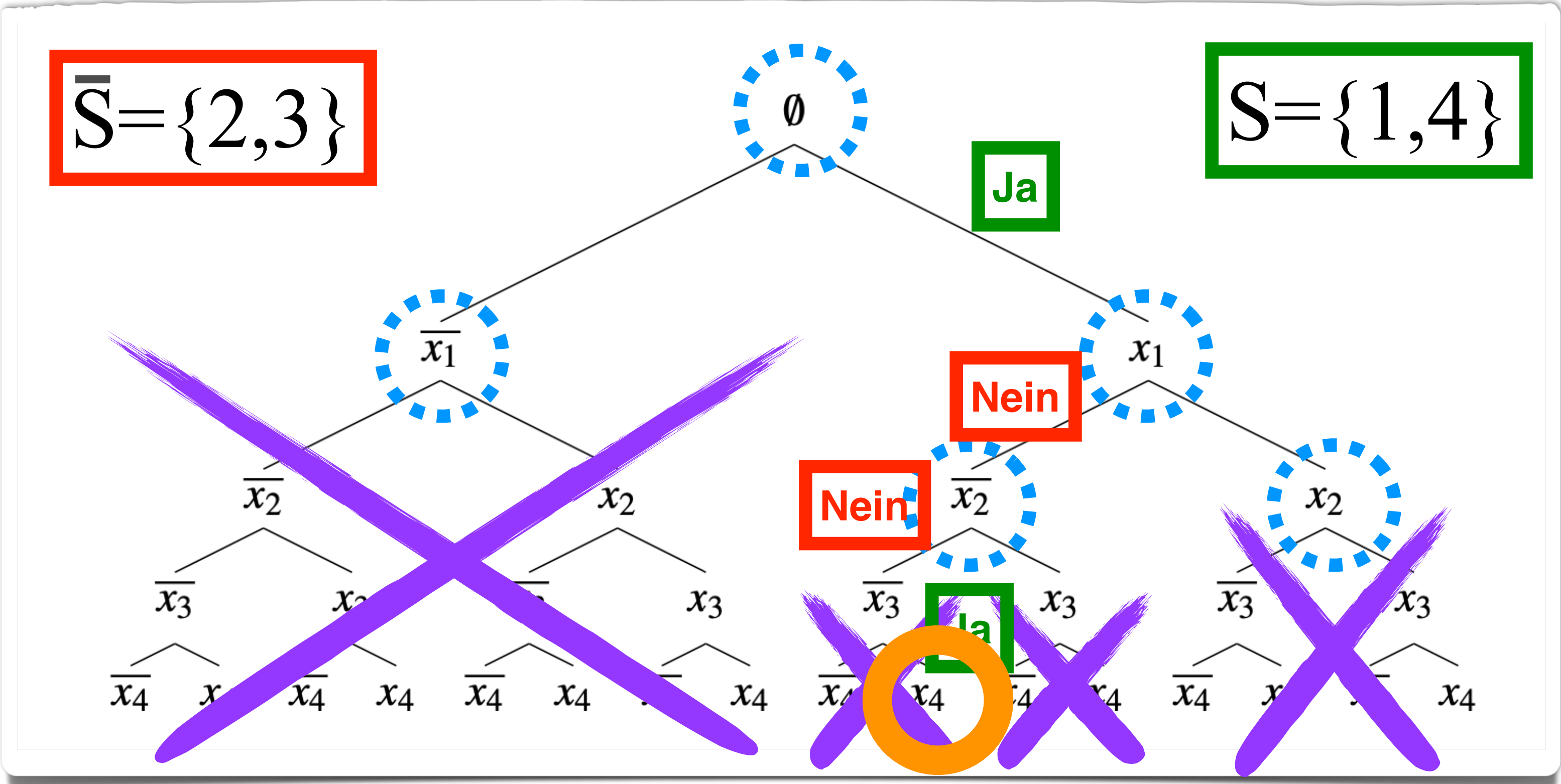
<i>i</i>	1	2	3	4	5	6	7
<i>z<sub>i</sub></i>	2	3	6	7	5	9	4
<i>p<sub>i</sub></i>	6	5	8	9	6	7	3

UB=14

<i>i</i>	1	2	3	5	6	7
<i>z<sub>i</sub></i>	2	3	6	5	9	4
<i>p<sub>i</sub></i>	6	5	8	9	6	3

LB=15

# Gesamtbeispiel



$$\bar{S} = \{2, 3\}$$

$$S = \{1, 4\}$$

Also: Das Optimum ist 15 mit  $S = \{1, 4\}$

$i$	1	2	3	4	5	6	7
$z_i$	2	3	6	7	5	9	4
$p_i$	6	5	8	9	6	7	3

LB=15

# Algorithmus

## Algorithmus 3.1 (Branch-And-Bound als Unterroutine).

**Eingabe:**  $z_1, \dots, z_n, Z, p_1, \dots, p_n$  (global: Kosten/Nutzenwerte, Kostenschranke)  
 $P$  (bester bekannter Lösungswert)  
 $\ell$  (nächster Index, über den verzweigt werden soll)  
 $x_j = b_j$  für  $j = 1, \dots, \ell - 1$  mit  $b_j \in \{0, 1\}$  (bislang fixierte Binärvariable)

**Ausgabe:**  $\max \left\{ \sum_{j=1}^{\ell-1} b_j p_j + \sum_{j=\ell}^n x_j p_j \mid \sum_{j=1}^{\ell-1} b_j z_j + \sum_{j=\ell}^n x_j z_j \leq Z, x_j \in \{0, 1\} \right\}$

Also: Lösung des Knapsackproblems mit den ersten  $\ell - 1$  Variablen fixiert

- 1: **procedure** BRANCH-AND-BOUND( $\ell$ )
- 2:     **if** ( $\sum_{j=1}^{\ell-1} b_j z_j > Z$ ) **then return** ▷ unzulässig
- 3:     Compute  $L := LB(b_1, \dots, b_{\ell-1})$
- 4:     **if**  $L > P$  **then**  $P := L$  ▷ Lösungswert verbessert
- 5:     **if** ( $\ell > n$ ) **then return** ▷ Blatt im Baum erreicht
- 6:      $U := UB(b_1, \dots, b_{\ell-1})$  ▷ (Obere Schranke berechnen)
- 7:     **if** ( $U > P$ ) **then**
- 8:          $b_\ell := 0$ ; BRANCH-AND-BOUND( $\ell + 1$ );
- 9:          $b_\ell := 1$ ; BRANCH-AND-BOUND( $\ell + 1$ );
- 10:    **return**

# Satz

**Satz 3.2** *Algorithmus 2.10 (als rekursiv arbeitende Unterroutine) berechnet eine optimale Lösung für das Knapsackproblem in einer Worst-Case-Laufzeit  $O(2^n f(n))$ , wobei  $f(n)$  die Zeit für die Berechnung der oberen Schranke ist.*

**Beweis.** Es werden systematisch alle Teillösungen durchprobiert. (Dabei werden Teilmengen nur dann ausgelassen, wenn sie erwiesenermaßen unzulässig sind (Zeile 2) oder keine Verbesserung bringen (Zeile 4))  
Die Zahl der Rekursionsaufrufe (Schritt 9 und 11) ist insgesamt  $2^n$ , die sonstigen Berechnungen benötigen jeweils  $f(n)$ . □

# 3.4 Ausblicke

# Historie

## ECONOMETRICA

VOLUME 28

July, 1960

NUMBER 3

### AN AUTOMATIC METHOD OF SOLVING DISCRETE PROGRAMMING PROBLEMS

By A. H. LAND AND A. G. DOIG

In the classical linear programming problem the behaviour of continuous, nonnegative variables subject to a system of linear inequalities is investigated. One possible generalization of this problem is to relax the continuity condition on the variables. This paper presents a simple numerical algorithm for the solution of programming problems in which some or all of the variables can take only discrete values. The algorithm requires no special techniques beyond those used in ordinary linear programming, and lends itself to automatic computing. Its use is illustrated on two numerical examples.

#### 1. INTRODUCTION

THERE IS A growing literature [1, 3, 5, 6] about optimization problems which could be formulated as linear programming problems with additional constraints that some or all of the variables may take only integral values. This form of linear programming arises whenever there are indivisibilities. It is not meaningful, for instance, to schedule 3-7/10 flights between two cities, or to undertake only 1/4 of the necessary setting up operation for running a job through a machine shop. Yet it is basic to linear programming that the variables are free to take on any positive value,<sup>1</sup> and this sort of answer is very likely to turn up.

In some cases, notably those which can be expressed as transport problems, the linear programming solution will itself yield discrete values of the variables. In other cases the percentage change in the maximand<sup>2</sup> from common sense rounding of the variables is sufficiently small to be neglected. But there remain many problems where the discrete variable constraints are significant and costly.

Until recently there was no general automatic routine for solving such problems, as opposed to procedures for proving the optimality of conjectured solutions, and the work reported here is intended to fill the gap. About the time of its completion an alternative method was proposed by Gomory [5] and subsequently extended by Beale [1]. Gomory's method

<sup>1</sup> Or more generally, any value within a bounded interval.

<sup>2</sup> We shall speak throughout of maximisation, but of course an exactly analogous argument applies to minimisation.

497

#### 1. INTRODUCTION

THERE IS A growing literature [1, 3, 5, 6] about optimization problems which could be formulated as linear programming problems with additional constraints that some or all of the variables may take only integral values. This form of linear programming arises whenever there are indivisibilities. It is not meaningful, for instance, to schedule 3-7/10 flights between two cities, or to undertake only 1/4 of the necessary setting up operation for running a job through a machine shop. Yet it is basic to linear programming that the variables are free to take on any positive value,<sup>1</sup> and this sort of answer is very likely to turn up.

# Knapsack-Probleme

## 0-1-Knapsack

$$\max \sum_{i=1}^n x_i p_i$$

$$\sum_{i=1}^n x_i z_i \leq Z$$

$$x_i \in \{0, 1\}$$

Schwieriger

## Fraktionales Knapsack

$$\max \sum_{i=1}^n x_i p_i$$

$$\sum_{i=1}^n x_i z_i \leq Z$$

$$x_i \in [0, 1]$$

Einfacher

# Ganzzahlige und lineare Optimierungsprobleme

## Ganzzahliges Optimierungsproblem

$$\max \sum_{i=1}^n x_i p_i$$

$$\begin{array}{rcccc} a_{11}x_1 & + \dots & + a_{1n}x_n & \leq & b_1 \\ a_{21}x_1 & + \dots & + a_{2n}x_n & \leq & b_2 \\ \vdots & \vdots & \vdots & \vdots & \\ a_{m1}x_1 & + \dots & + a_{mn}x_n & \leq & b_m \end{array}$$

$$x_i \in \{0, 1\}$$

**Beweisbar schwer zu lösen**

## Lineares Optimierungsproblem

$$\max \sum_{i=1}^n x_i p_i$$

$$\begin{array}{rcccc} a_{11}x_1 & + \dots & + a_{1n}x_n & \leq & b_1 \\ a_{21}x_1 & + \dots & + a_{2n}x_n & \leq & b_2 \\ \vdots & \vdots & \vdots & \vdots & \\ a_{m1}x_1 & + \dots & + a_{mn}x_n & \leq & b_m \end{array}$$

$$x_i \in [0, 1]$$

**Beweisbar effizient lösbar**

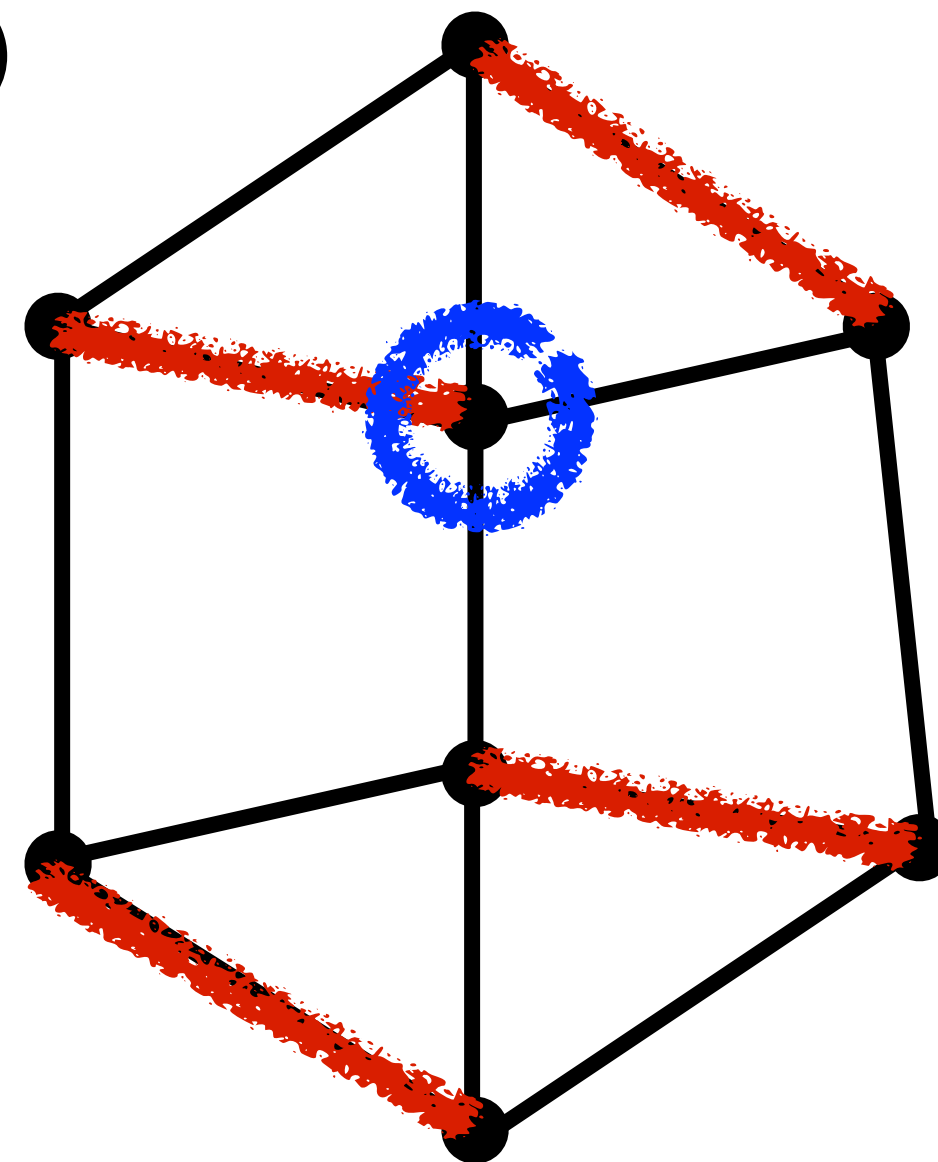


# Ganzzahlige Optimierungsprobleme: Matching

Gegeben: Ein Graph  $G=(V,E)$

  $x_e = 1$

$$\sum_{e \in E} x_e = 4$$



$$\begin{aligned} & \max \sum_{e \in E} x_e \\ \forall v \in V : & \sum_{e \in \delta(v)} x_e \leq 1 \\ & x_e \in \{0, 1\} \end{aligned}$$

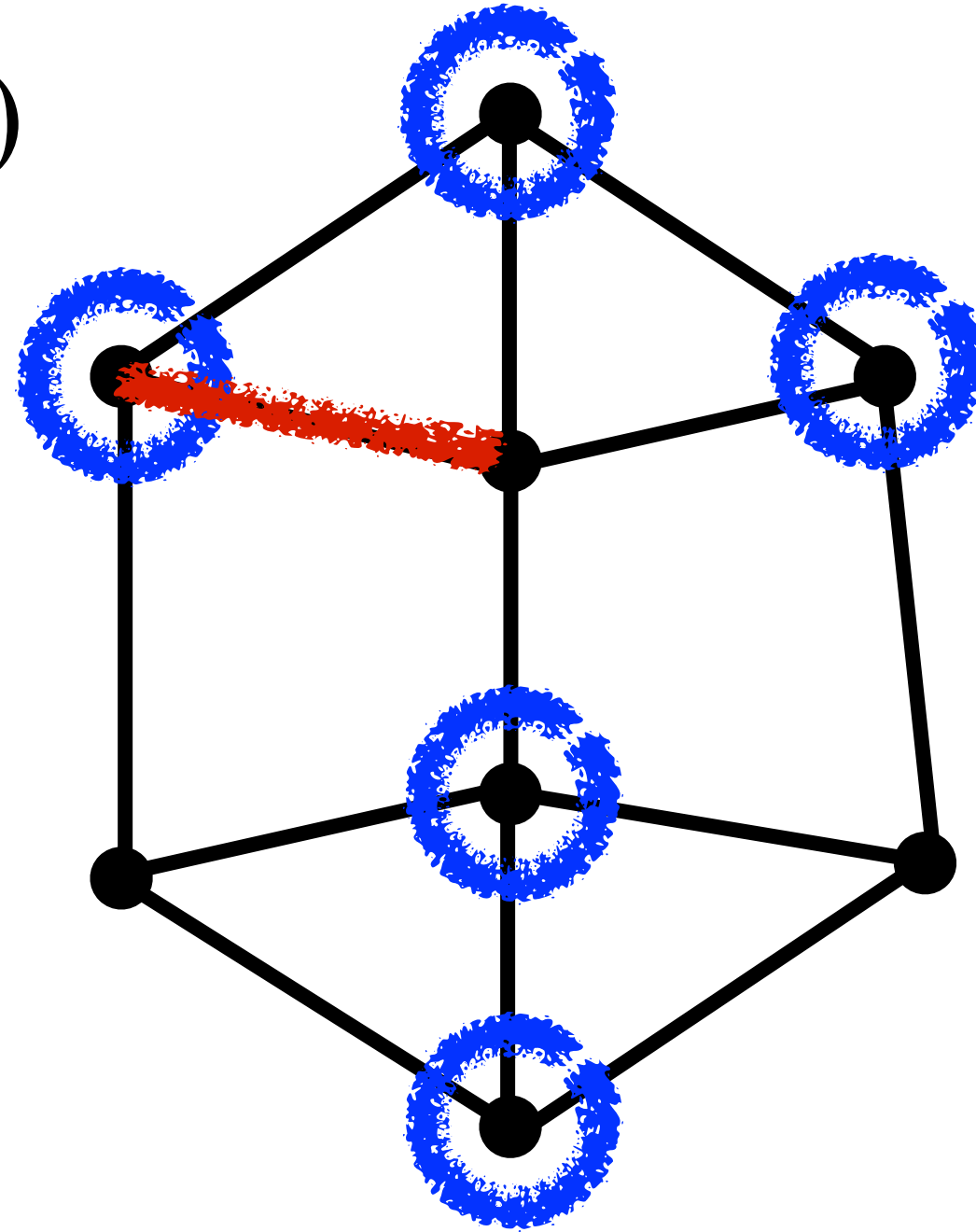
**Gesucht:** Ein größtmögliches **Matching**  $M$  in  $G$ :  
eine möglichst große Menge disjunkter Kanten

# Ganzzahlige Optimierungsprobleme: Vertex Cover

Gegeben: Ein Graph  $G=(V,E)$

$$\bigcirc y_v = 1$$

$$\sum_{v \in V} y_v = 5$$



$$\begin{aligned} \min \sum_{v \in V} y_v \\ \forall e \in E : \sum_{v \in \delta(e)} y_v \geq 1 \\ y_v \in \{0, 1\} \end{aligned}$$

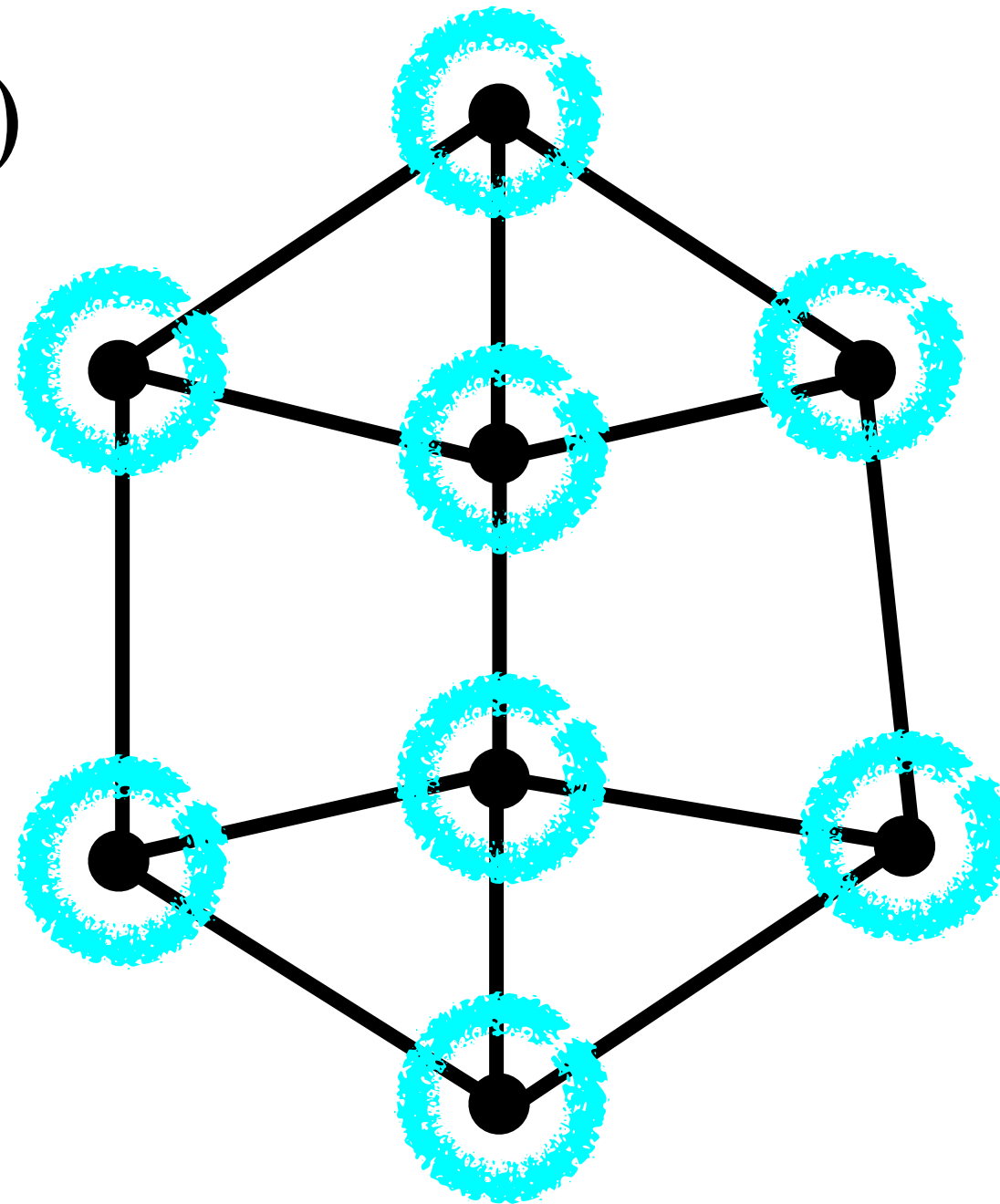
**Gesucht:** Ein kleinstmögliches **Vertex Cover**  $S$  in  $G$ :  
eine möglichst kleine Menge von Knoten,  
die alle Kanten überdecken

# Lineare Optimierungsprobleme: Vertex Cover

Gegeben: Ein Graph  $G=(V,E)$

$$y_v = \frac{1}{2}$$

$$\sum_{v \in V} y_v = 4$$



Ganzzahlig?!

$\forall e \in E :$

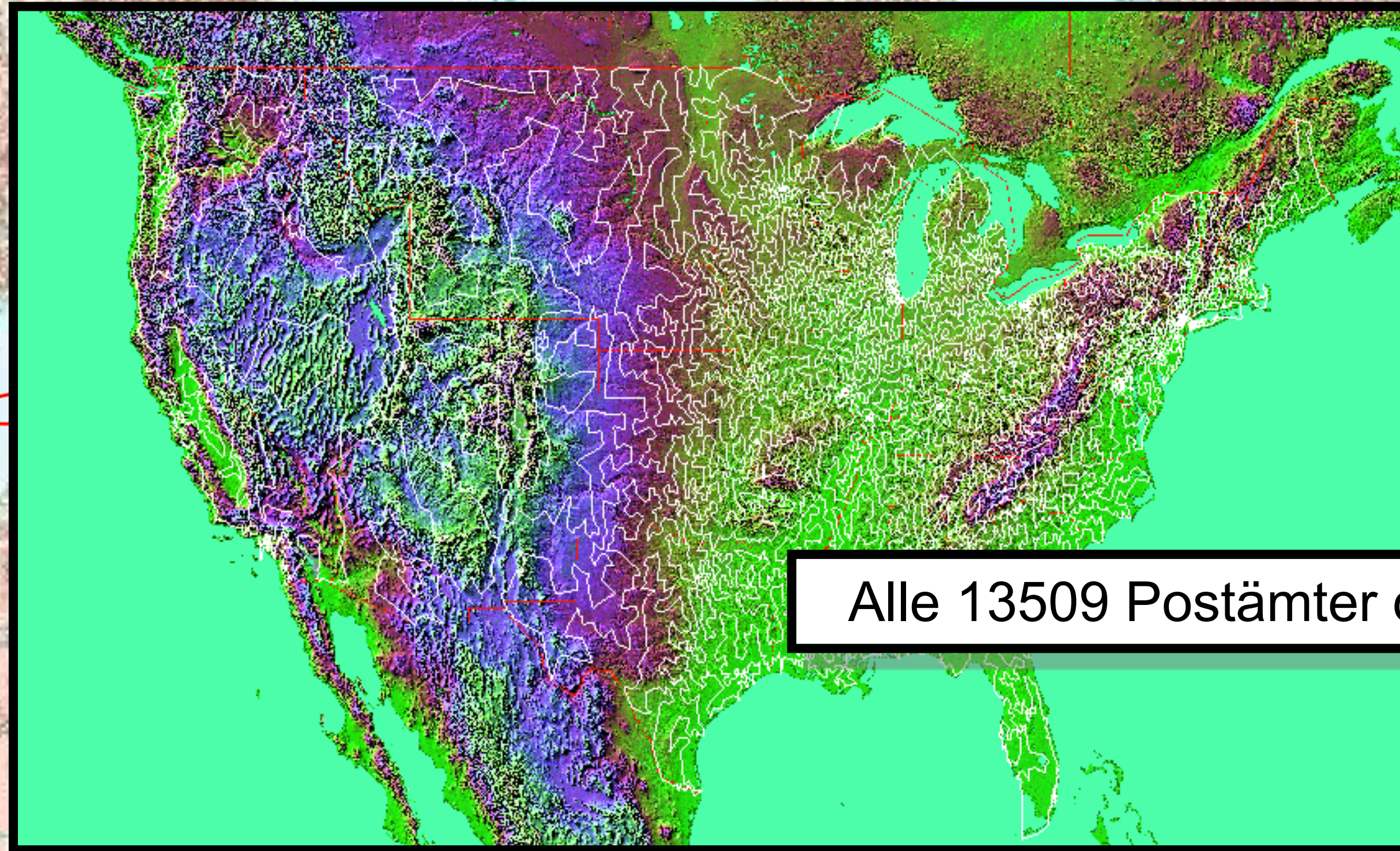
$$\sum_{e \in \delta(v)} y_v \geq 1$$

$$y_v \in [0, 1]$$

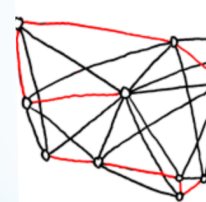
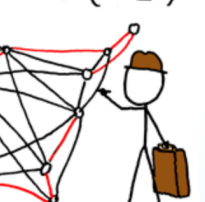
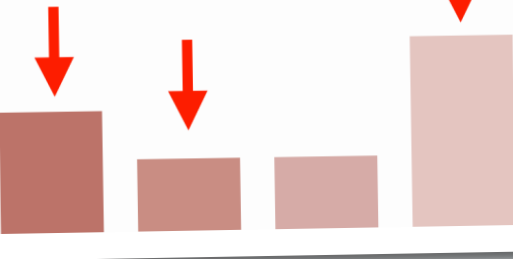
**Gesucht:** Ein kleinstmögliches **Vertex Cover**  $S$  in  $G$ :  
eine möglichst kleine Menge von Knoten,  
die alle Kanten überdecken

Relaxierung

# Das Rundreiseproblem



Alle 13509 Postämter der USA

<p>BRUTE-FORCE SOLUTION: <math>O(n!)</math></p> 	<p>DYNAMIC PROGRAMMING ALGORITHMS: <math>O(n^2 2^n)</math></p> 	<p><b>Algorithmus 4.3 Greedy:</b>          Eingabe: <math>z_1, \dots, z_n, Z, p_1, \dots, p_n</math>          Ausgabe: <math>S \subseteq \{1, \dots, n\}</math>  <math>G_0 = \max_{S \subseteq \{1, \dots, n\}} \sum_{i \in S} p_i</math>          return <math>S</math></p>	
---	---	--	---

# 4 Approximation

*Algorithmen und Datenstrukturen 2  
Sommer 2023*

**Prof. Dr. Sándor Fekete**

# 4.1 Motivation

# Laufzeit?

## 0-1 Knapsack

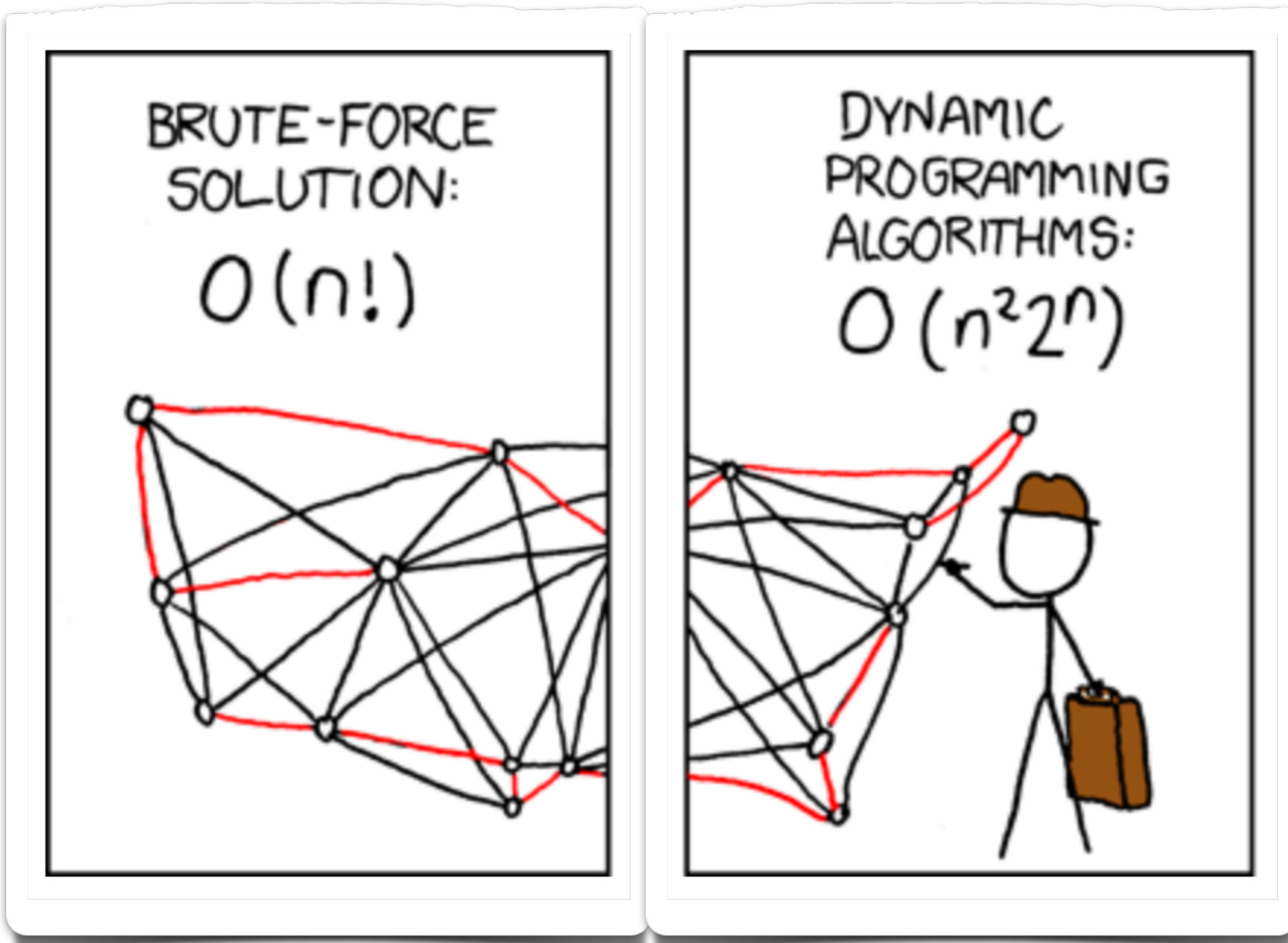
$O(nZ)$

$O(2^n f(n))$

1	2	3	4	5	6
1	2	3	4	5	6
20	32	40	8	16	4
3	3	10	5	2	4
	10				
	32				
	5				
7	8	11	12	16	13
32	40	28	20	24	16
2	9	3	9	4	10
	8				
	2	14			
		20			
		3	15		
			40		
			10		

**Kann Knut die Klausur bestehen?**

## Traveling Salesman

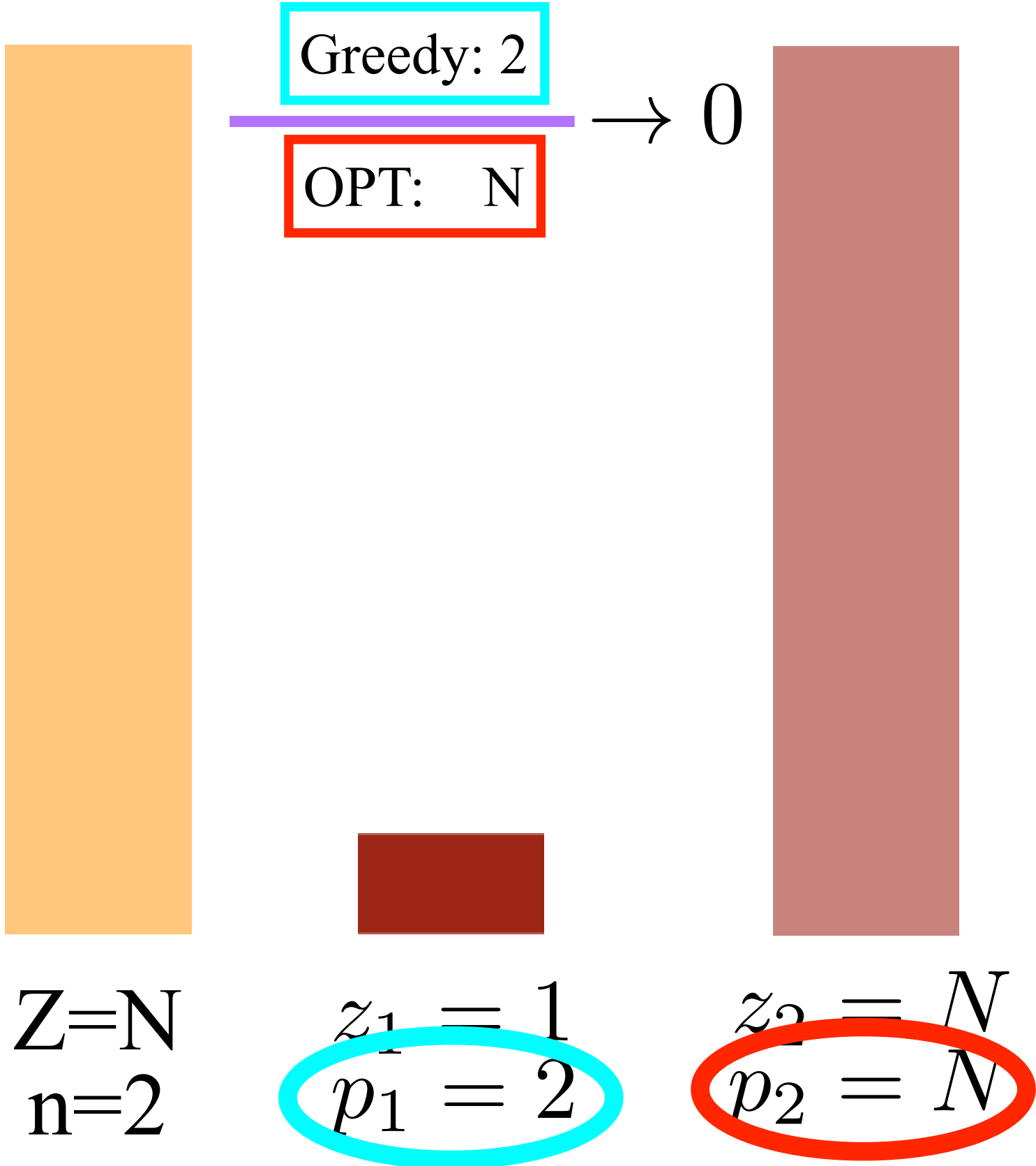


**Ziel:** Vielleicht nicht die *bestmögliche* Lösung, sondern eine *gute*, aber dafür schneller...?!

# 4.2 Greedy und Approximation



# Beispiel 4.1: Knapsack



## Algorithmus 4.2 GREEDY<sub>0</sub>

**Eingabe:**  $z_1, \dots, z_n, Z, p_1, \dots, p_n$

**Ausgabe:**  $S \subseteq \{1, \dots, n\}$  und  $G_0$

mit

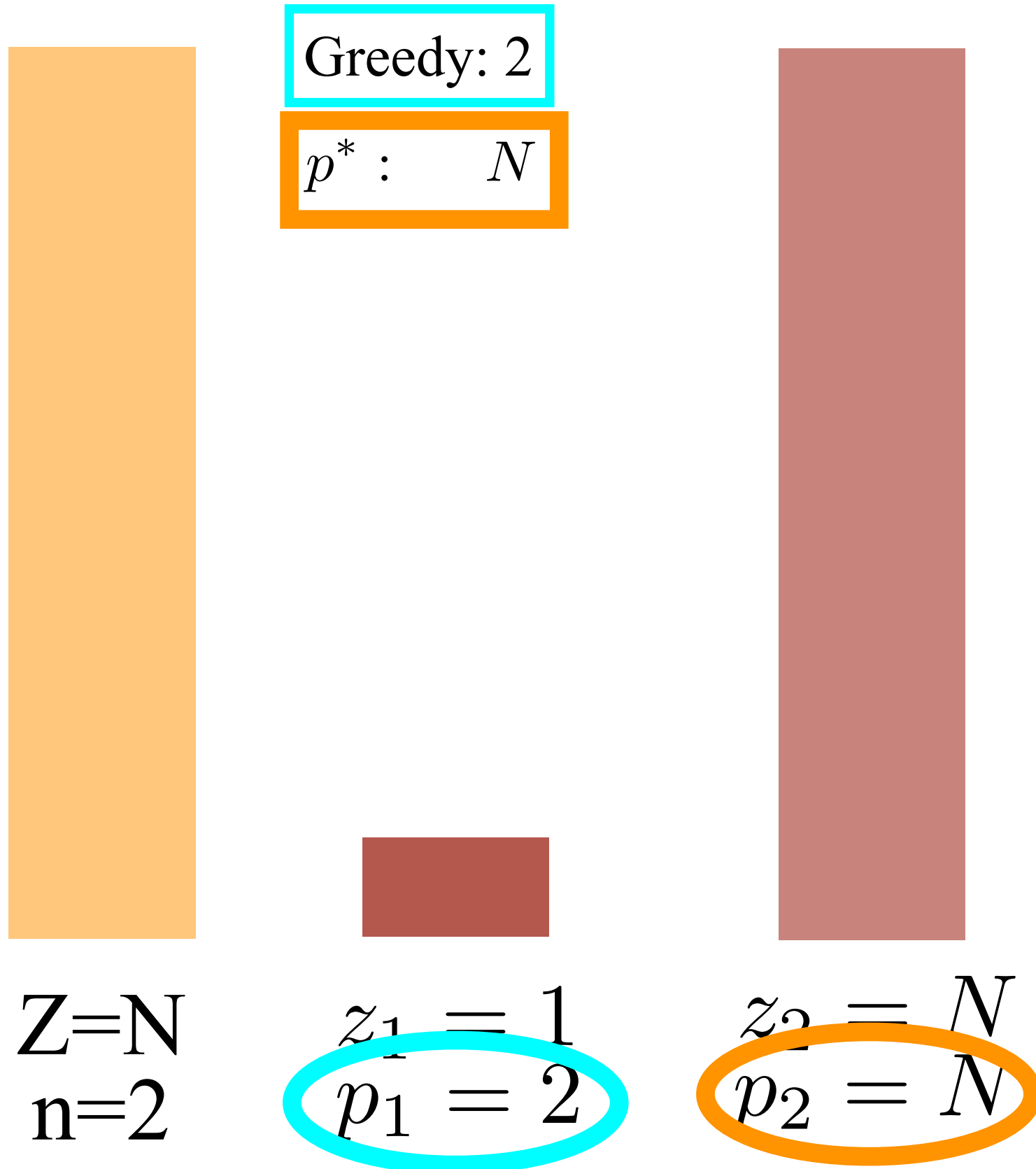
$$\sum_{i \in S} z_i \leq Z$$

und

$$G_0 := \sum_{i \in S} p_i = \textit{Maximal}$$

- 1: Sortiere  $\{1, \dots, n\}$  nach  $\frac{z_i}{p_i}$  aufsteigend;  
Dies ergibt die Permutation  $\pi(1), \dots, \pi(n)$ .  
Setze  $j = 1$ .
- 2: **while** ( $j \leq n$ ) **do**
- 3:     **if** ( $\sum_{i=1}^{j-1} z_{\pi(i)} x_{\pi(i)} + z_{\pi(j)} \leq Z$ ) **then**
- 4:          $x_{\pi(j)} := 1$
- 5:      $j := j + 1$
- 6: **return**

# Verbesserung?!



## Algorithmus 4.3 GREEDY<sub>0</sub>'

**Eingabe:**  $z_1, \dots, z_n, Z, p_1, \dots, p_n$

**Ausgabe:**  $S \subseteq \{1, \dots, n\}$  und  $G_0$

mit

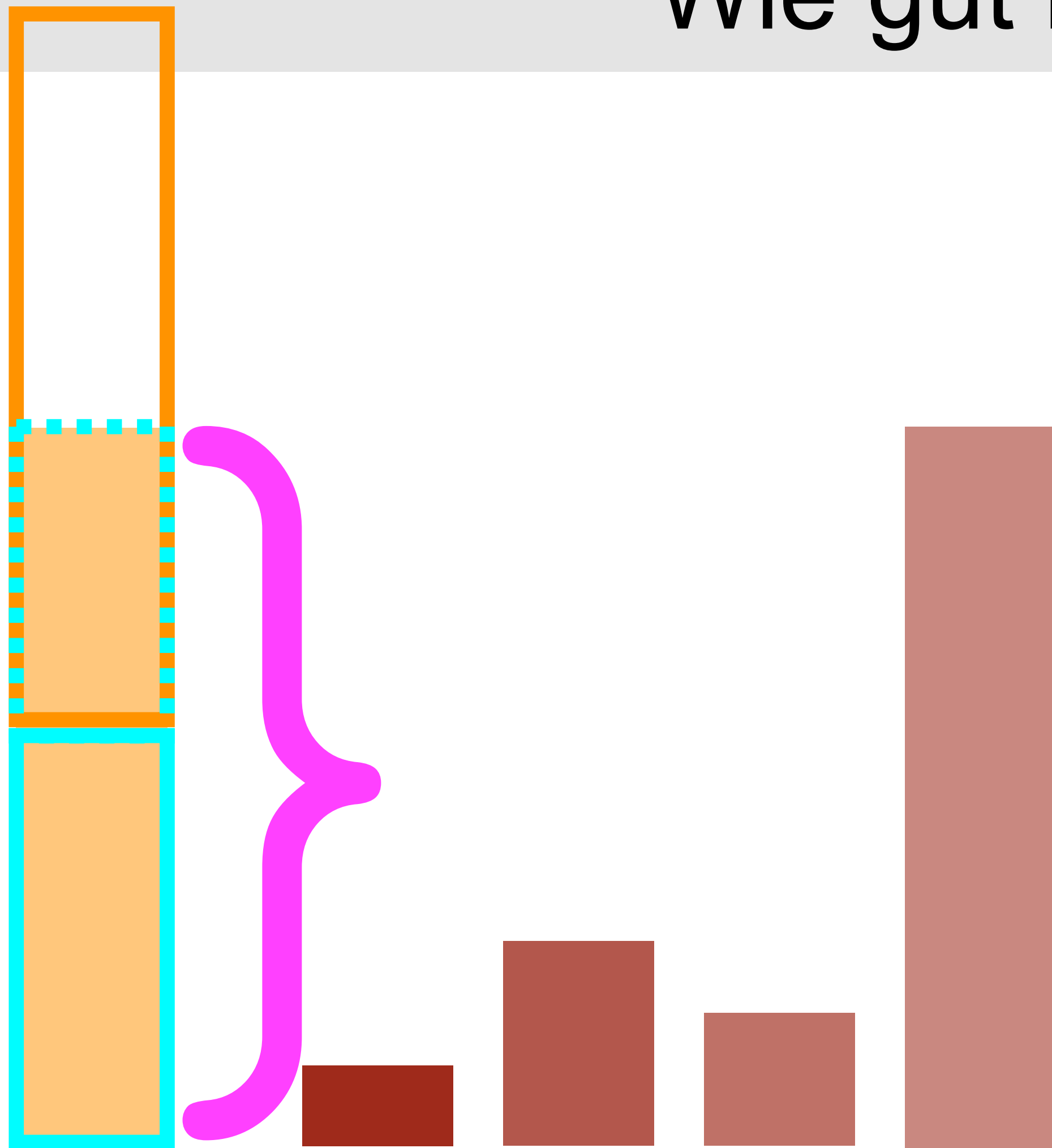
$$\sum_{i \in S} z_i \leq Z$$

und

$$G_0 := \sum_{i \in S} p_i = \text{Maximal}$$

- 1: Sortiere  $\{1, \dots, n\}$  nach  $\frac{z_i}{p_i}$  aufsteigend;  
Dies ergibt die Permutation  $\pi(1), \dots, \pi(n)$ .  
Setze  $j = 1$ .
- 2: **while** ( $j \leq n$ ) **do**
- 3:     **if** ( $\sum_{i=1}^{j-1} z_{\pi(i)} x_{\pi(i)} + z_{\pi(j)} \leq Z$ ) **then**
- 4:          $x_{\pi(j)} := 1$
- 5:      $j := j + 1$
- 6:  $G'_0 := \max \{ G_0, \max \{ p_i \mid z_i < Z, i \in \{1, \dots, n\} \} \}$
- 7: **return**

# Wie gut ist das allgemein?



## Algorithmus 4.3 Greedy-Approximation

**Eingabe:**  $z_1, \dots, z_n, Z, p_1, \dots, p_n$

**Ausgabe:**  $S \subseteq \{1, \dots, n\}$  mit  $\sum_{i \in S} z_i \leq Z$  und Wert  $G'_0 := \sum_{i \in S} p_i$

- 1:  $G'_0 = \max_{G_0} \max\{p_i \mid z_i < Z, i \in \{1, \dots, n\}\}$
- 2: return

**Satz 4.4.** Algorithmus 4.3 berechnet eine Lösung mit  $G'_0$ ;  
im Vergleich mit dem Optimalwert  $OPT$  gilt:  $G'_0 \geq \frac{1}{2}OPT$ .

$$\begin{aligned}
 & G'_0 \geq G_0 & G'_0 & \geq p^* \\
 OPT & \leq \text{FractionalKP} = G_0 + x_i p_i \leq G_0 + p^* \leq 2G'_0
 \end{aligned}$$

# 4.3 Approximationsalgorithmen

# Approximation

## Definition 4.5 (Approximationsalgorithmus).

1. Für ein **Maximierungsproblem MAX** ist ein Algorithmus ALG ein *c-Approximationsalgorithmus* für MAX, wenn für jede Instanz  $I$  von MAX
  - a) ALG in *polynomieller Zeit* in der Größe von  $I$  eine zulässige Lösung mit Wert ALG liefert
  - b) für den Vergleich mit dem zugehörigen Optimalwert  $\text{OPT}(I)$  gilt  **$\text{ALG}(I) \geq c \cdot \text{OPT}(I)$**  (dabei ist  **$c \leq 1$** )
2. Entsprechend für **Minimierungsproblem** wiederum:
  - a) ALG liefert in *polynomieller Zeit* in der Größe von  $I$  eine zulässige Lösung mit Wert  $\text{ALG}(I)$
  - b) es gilt für den Vergleich mit dem zugehörigen Optimalwert  $\text{OPT}(I)$ :  **$\text{ALG}(I) \leq c \cdot \text{OPT}(I)$**  (dabei ist  **$c \geq 1$** )

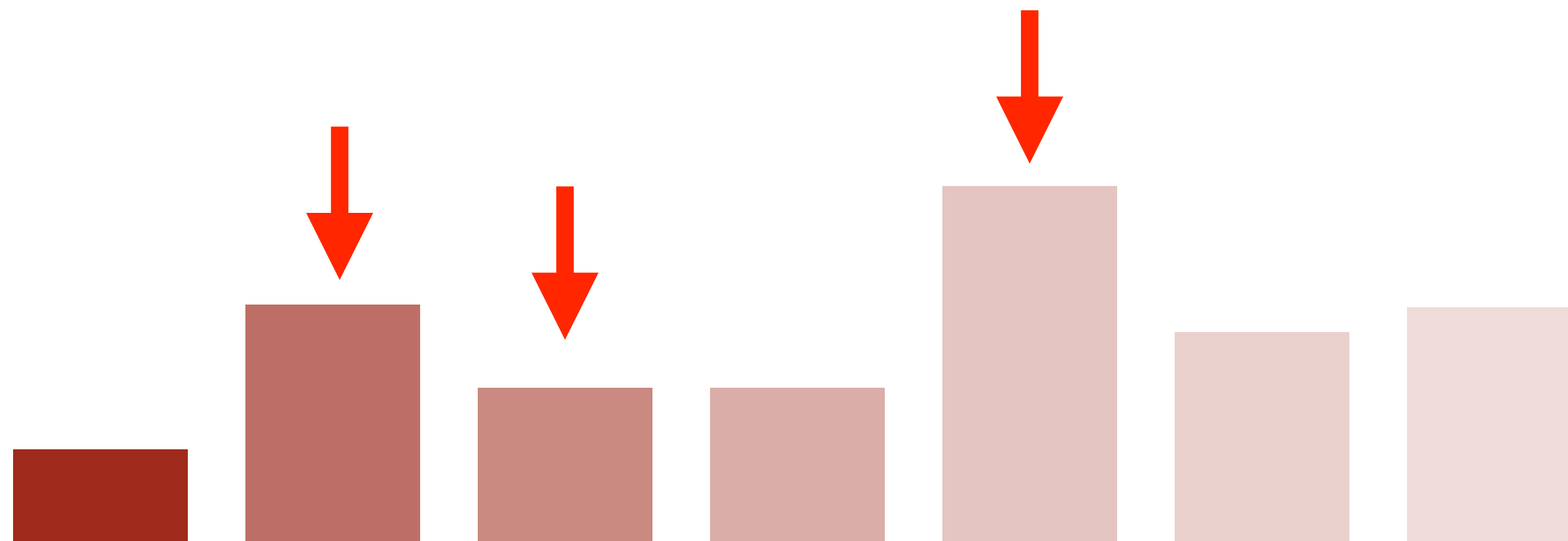
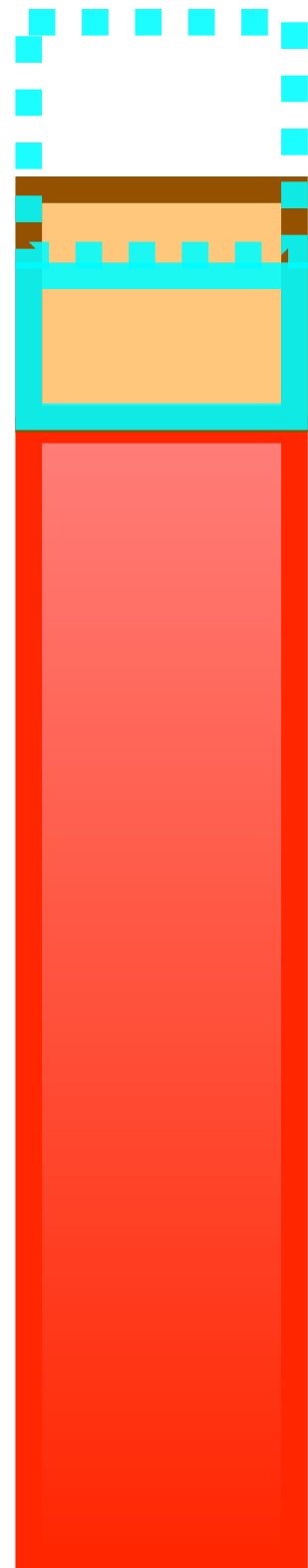
# 4.4 Bessere Approximation

# Ideen:

- Verwende die  $k$  wertvollsten Objekte aus einer Optimallösung.
- Wende Greedy auf den Rest an.
- Der Fehler ist durch *ein* Objekt beschränkt.

Wie findet man die  $k$  wertvollsten Objekte?

- Enumeriere alle Teilmengen der Größe  $k$ !  $\rightarrow O(n^k)$  Teilmengen



# Bessere Approximation von Knapsack

## Algorithmus 4.6 GREEDY<sub>k</sub>

**Eingabe:**  $z_1, \dots, z_n, Z, p_1, \dots, p_n$  [Parameter  $k$  fixiert]

**Ausgabe:**  $S \subseteq \{1, \dots, n\}$  mit  $\sum_{i \in S} z_i \leq Z$  und Wert  $G_k := \sum_{i \in S} p_i$

1:  $G_k := 0, S := \emptyset$

2: **for all**  $\bar{S} \subseteq \{1, \dots, n\}$  mit  $|\bar{S}| \leq k$  **do**

3:     **if**  $(\sum_{i \in \bar{S}} z_i \leq Z)$  **then**

4:          $G_k := \max\{G_k, \sum_{i \in \bar{S}} p_i + \text{GREEDY}_0(\{z_i | i \notin \bar{S}\}, Z - \sum_{i \in \bar{S}} z_i, \{p_i | i \notin \bar{S}\})\};$

5:         Update  $S$ ;

6: **return**  $G_k, S$




# Gütegarantie

**Satz 4.7.**  $\text{GREEDY}_k$  ist ein  $(1 - \frac{1}{k+1})$ -Approximationsalgorithmus.

**Definition 4.5** (Approximationsalgorithmus).

1. Für ein Maximierungsproblem MAX ist ein Algorithmus ALG ein  $c$ -Approximationsalgorithmus für MAX, wenn für jede Instanz  $I$  von MAX

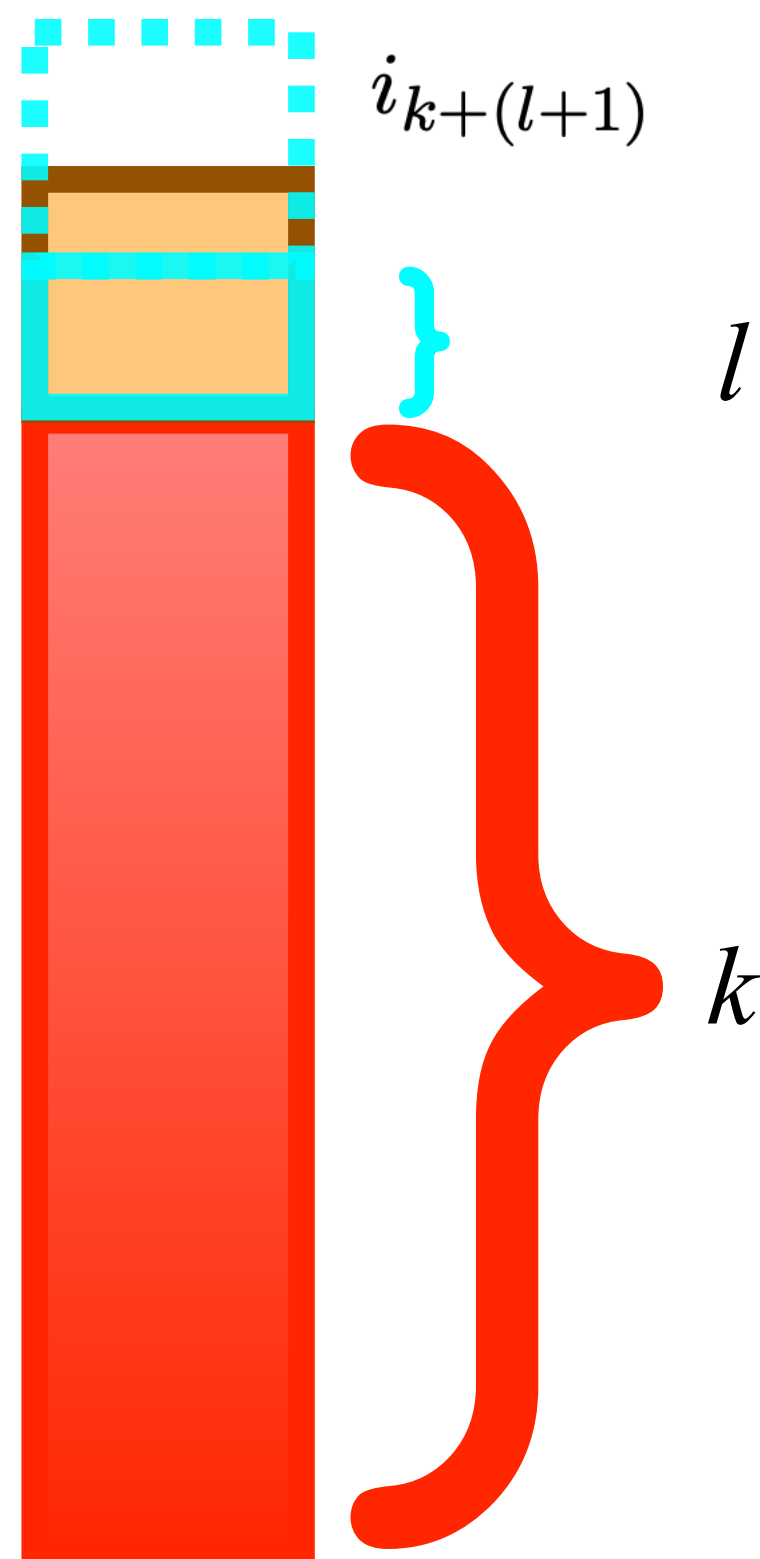
-  a) ALG in polynomieller Zeit in der Größe von  $I$  eine zulässige Lösung mit Wert ALG liefert
- b) für den Vergleich mit dem zugehörigen Optimalwert  $\text{OPT}(I)$  gilt:  $\text{ALG}(I) \geq c \cdot \text{OPT}(I)$  (dabei ist  $c \leq 1$ )

(a) Die Laufzeit ist nicht mehr als  $O(n^{k+2})$  - also polynomiell.

Nicht  $2^n$ , sondern  $n^2$

# Gütegarantie

**Satz 4.7.**  $\text{GREEDY}_k$  ist ein  $(1 - \frac{1}{k+1})$ -Approximationsalgorithmus.



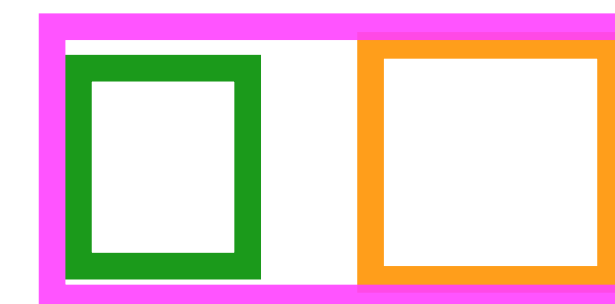
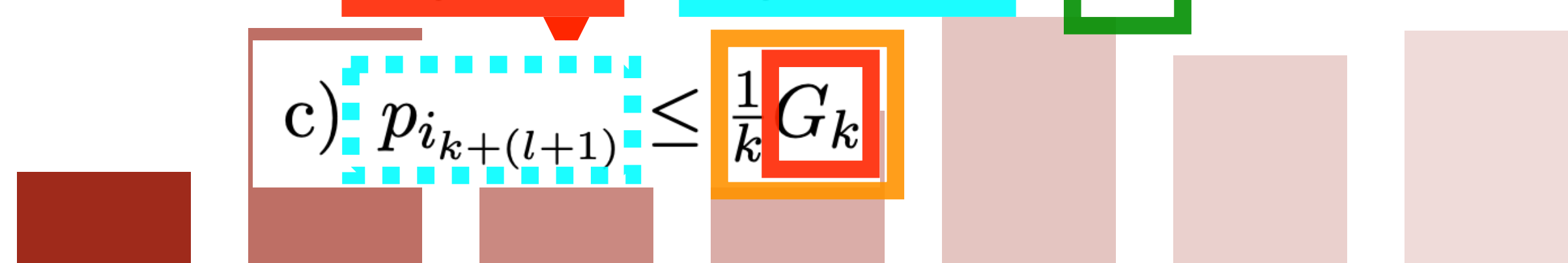
Betrachte OPT mit  $S^* \subseteq \{1, \dots, n\}$ .

$|S^*| \leq k \implies$  OPT wird gefunden.

a)  $\sum_{j=1}^k p_{i_j} + \sum_{j=1}^l p_{i_{k+j}} + p_{i_{k+(l+1)}} \geq \text{OPT}$

b)  $\sum_{j=1}^k p_{i_j} + \sum_{j=1}^l p_{i_{k+j}} \leq G_k$

c)  $p_{i_{k+(l+1)}} \leq \frac{1}{k} G_k$



# Zusatzbemerkungen

Man kann zeigen:

- Für  $\text{GREEDY}_k$  ist der Faktor  $(1 - \frac{1}{k+1})$  bestmöglich.
- Wenn man  $G_0$  in Zeile 4 von Algorithmus 4.6 durch  $G'_0$  ersetzt, bekommt man einen Approximationsalgorithmus mit Gütegarantie  $(1 - \frac{1}{k+2})$ .

# Approximationschemata

Man sieht: Für jedes feste  $\epsilon > 0$  gibt es einen polynomiellen Algorithmus für Knapsack, der eine  $(1 - \epsilon)$ -Approximation liefert. Das motiviert:

**Definition 4.8** (PTAS). Ein polynomielles Approximationsschema (Engl.: Polynomialtime approximation scheme. Kurz: PTAS) für ein Optimierungsproblem ist eine Familie von Algorithmen, die für jedes beliebige, aber feste  $\epsilon > 0$  einen  $(1 - \epsilon)$ -Approximationsalgorithmus (bzw.  $(1 + \epsilon)$ ) liefert.

**Korollar 4.9.**  $\{\text{GREEDY}_k \mid k \in \mathbb{N}\}$  ist ein PTAS für Knapsack.

# 4.4 Ausblicke

# Approximationsfaktoren

## 0-1 Knapsack

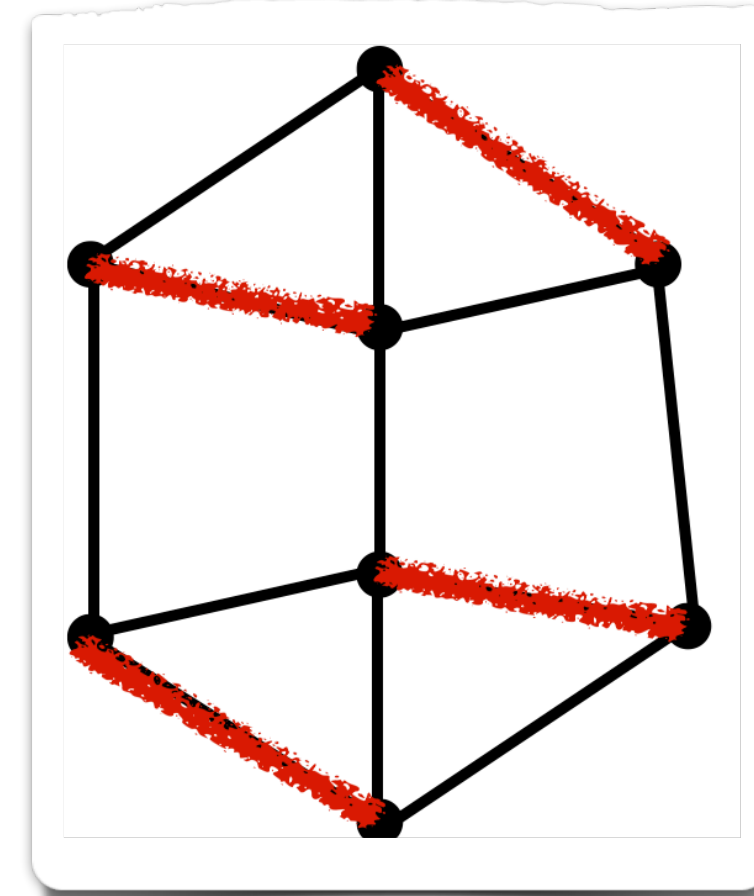
1	2	3	4	5	6
20	32	40	8	16	4
3	3	10	5	2	4
8	10	11	12	16	13
40	32	28	20	24	16
9	5	3	9	4	10
7	9	14	15	16	13
32	8	20	40	24	16
2	2	3	10	4	10

Kann Knut die Klausur bestehen?

**Max**

$$1 - \frac{1}{k + 2}$$

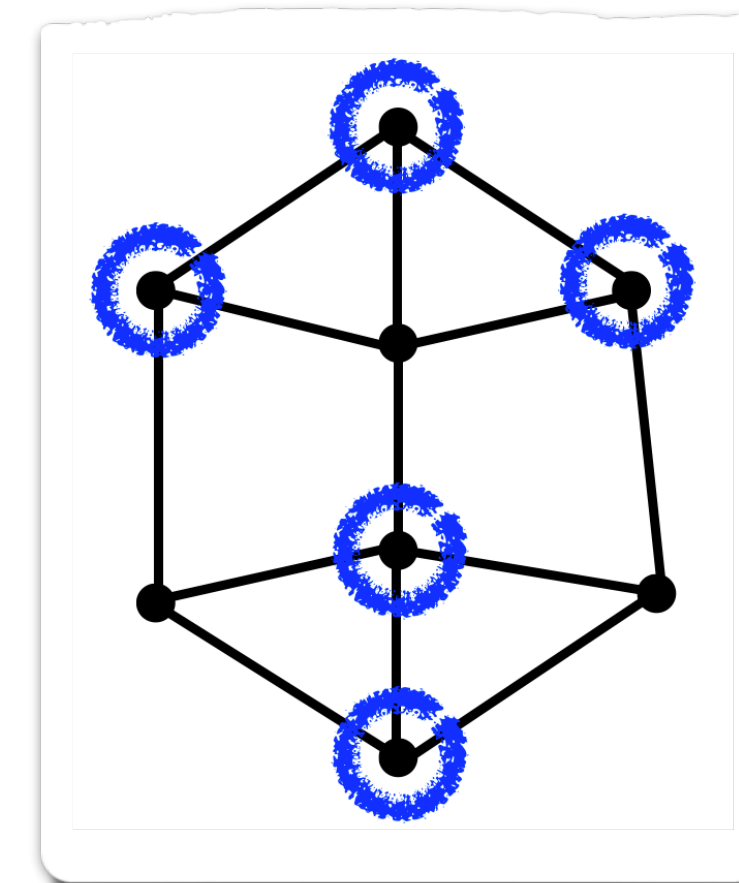
## Matching



**Max**

$$1$$

## Vertex Cover



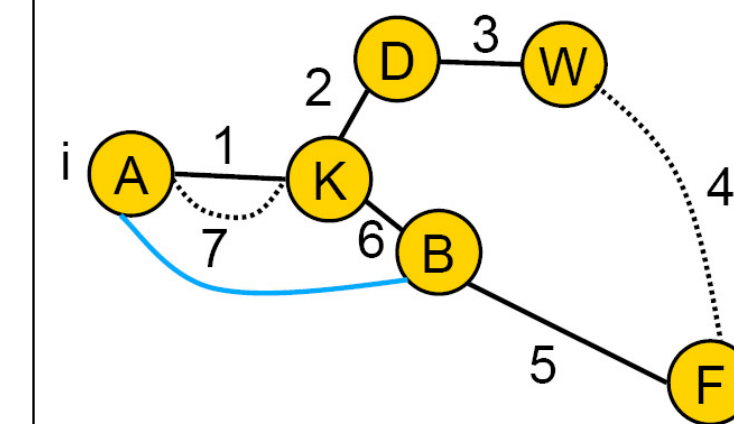
**Min**

$$2$$

## Traveling Salesman

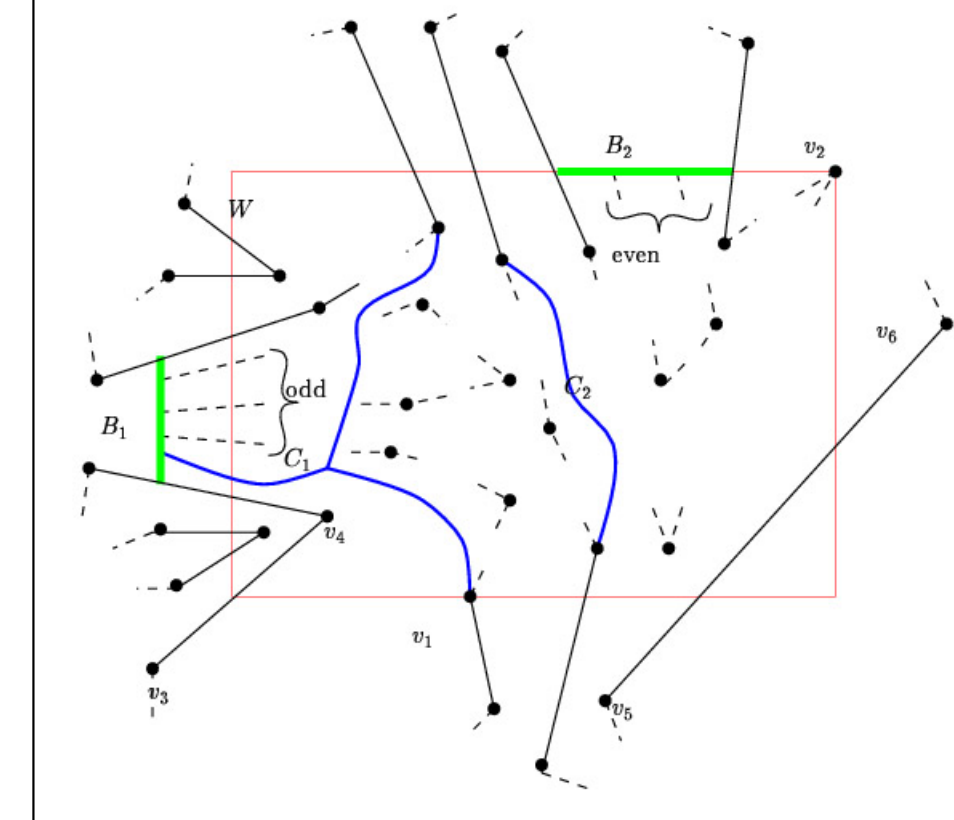
**Min**

Beispiel für CH-Heuristik

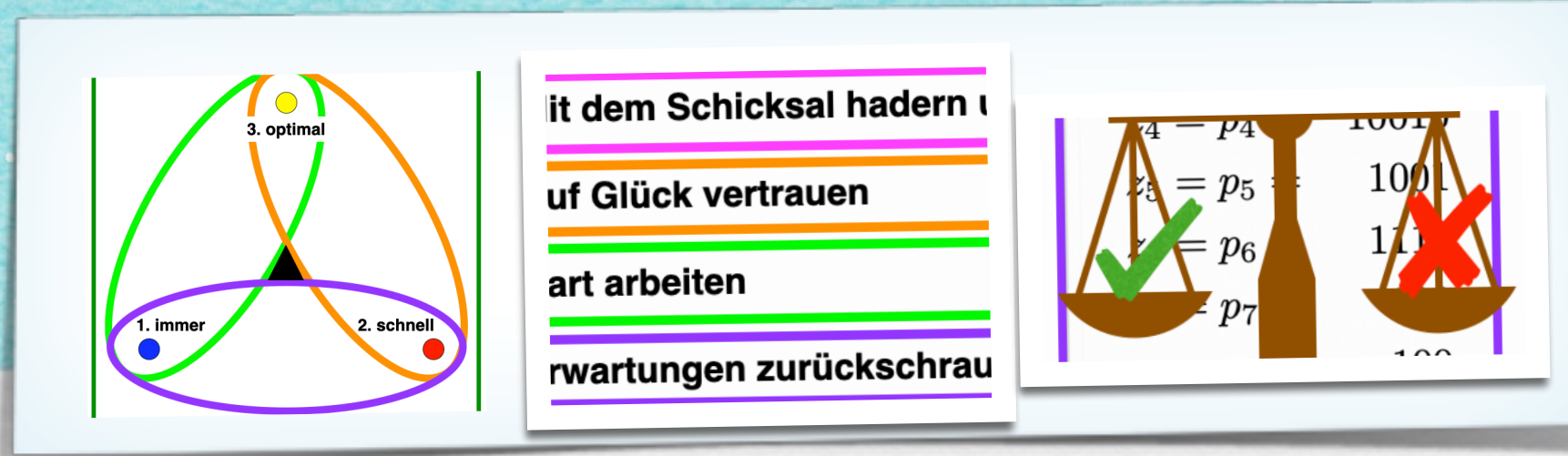


$$\frac{3}{2}$$

Example Subproblem (TSP)



$$1 + \epsilon$$



# 5 Komplexität

*Algorithmen und Datenstrukturen 2*  
*Sommer 2023*

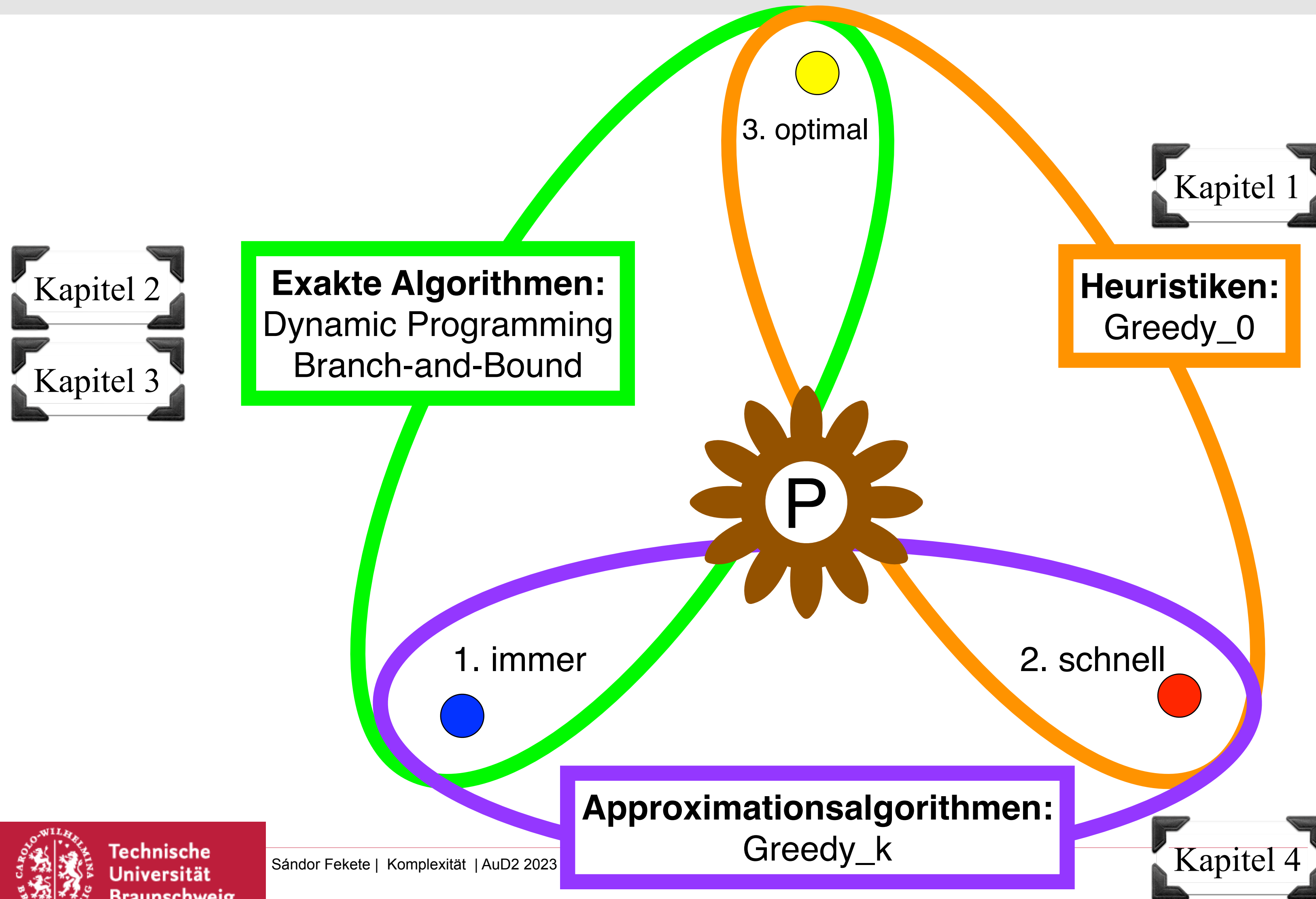
**Prof. Dr. Sándor Fekete**

# 5.1 Die Klasse P: „Perfekte“ Algorithmen





# Das Dreieck der Perfektion



## Fractional Knapsack

1	Nummer	2	3	4	5
20	Minuten	32	40	8	
3	Punkte	3	10	10	
		8			

Algorithmus 1.4 Greedy-Algorithmus für FRACTIONAL KNAPSACK  
 Eingabe:  $z_1, \dots, z_n, Z, p_1, \dots, p_n$   
 Ausgabe:  $x_1, \dots, x_n \in [0, 1]$

	15	24	10
3	40	4	
	10		

Kann Knut die Klausur bestehen?

**Gehört 0-1 Knapsack zu P?**

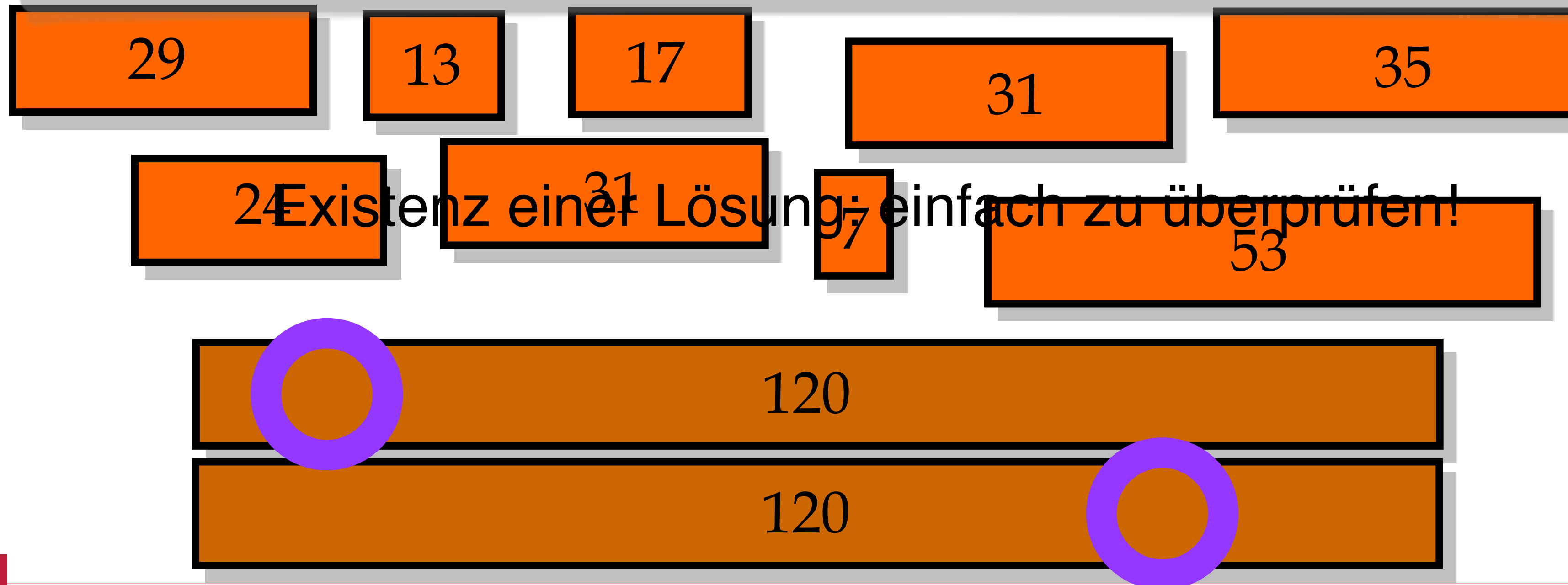
# 5.2 Die Klasse NP: „NachPrüfen“

# Nachprüfen!

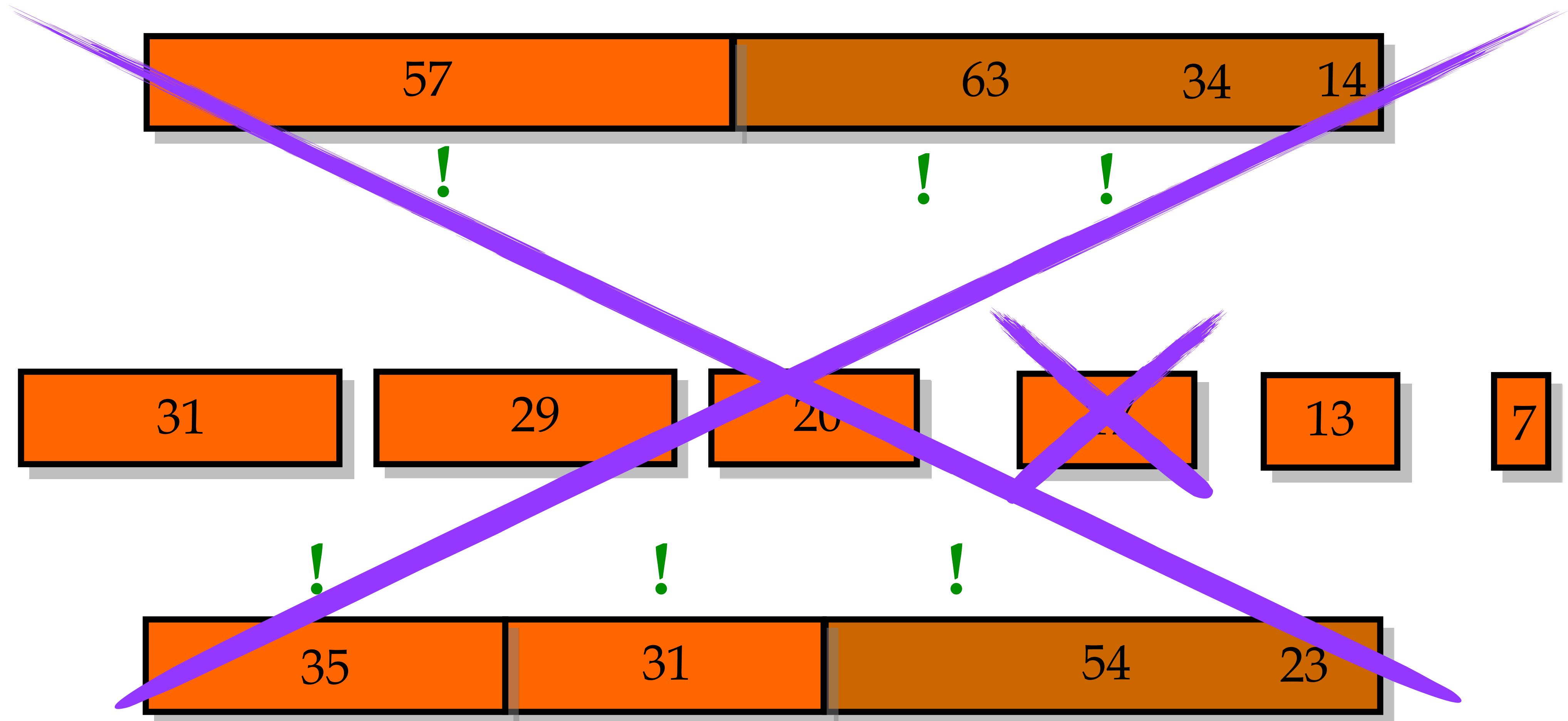
## Beispiel 1.10.

Partition für  $\{z_1, \dots, z_9\} = \{7, 13, 17, 24, 29, 31, 31, 35, 53\}$

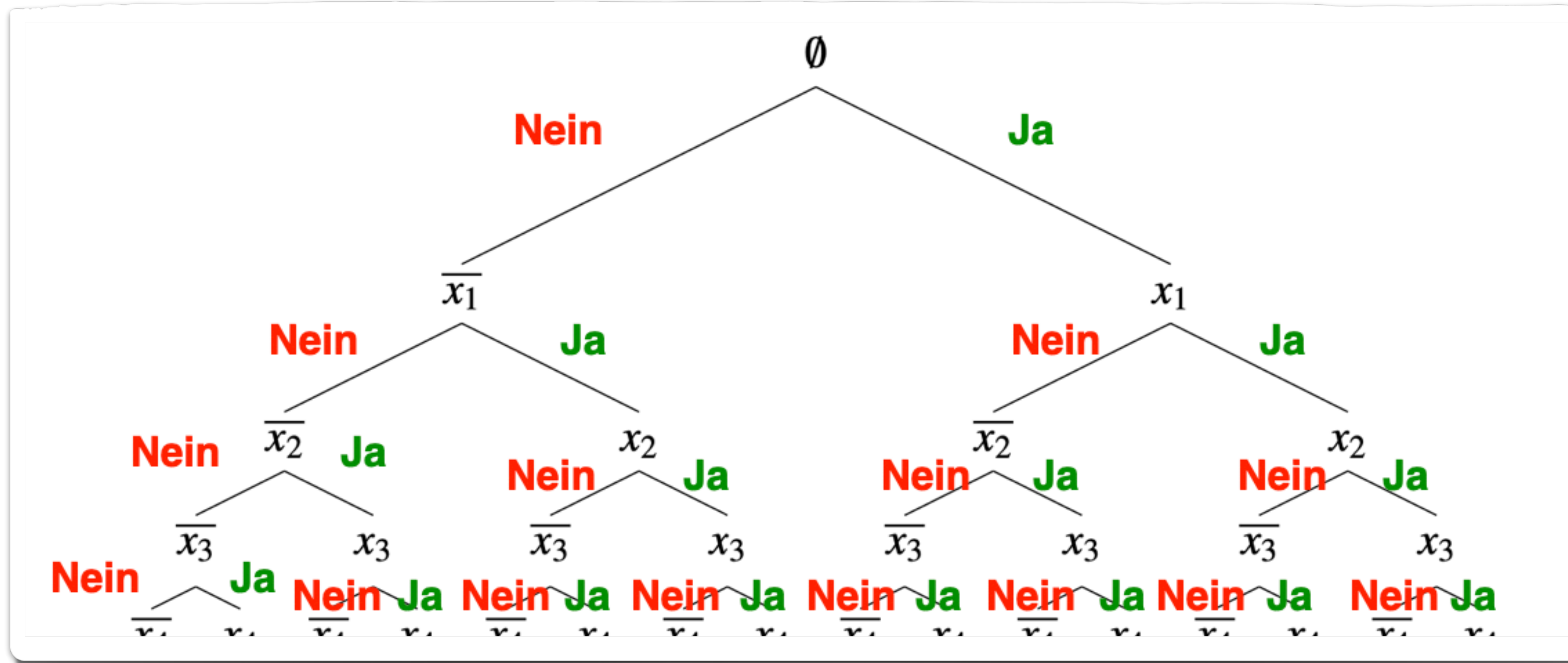
Gesamtsumme: 240



# Keine Lösung?!



# Enumeration



- Exponentiell viele Fälle!
- Kann man Arbeit sparen?

# P vs. NP

Clay Mathematics Institute  
dedicated to increasing and disseminating mathematical knowledge

news prize problems events researchers students awards schools workshops about cmi

home / millennium prize problems /

search

## Millennium Prize Problems

- P versus NP**
- The Hodge Conjecture
- ~~The Poincaré Conjecture~~
- The Riemann Hypothesis
- Yang–Mills Existence and Mass Gap
- Navier–Stokes Existence and Smoothness
- The Birch and Swinnerton–Dyer Conjecture

Announced 16:00, on Wednesday, May 24, 2000  
Collège de France

# Feinheiten

- Definition der Klasse NP über schnelle Verifizierbarkeit ist anschaulich.
- Eine formalere Definition (über nichtdeterministische Turingmaschinen) lernt man in Theoretischer Informatik.
- Genau genommen sind Probleme in der Klasse NP Entscheidungsprobleme:  
Gibt es eine Lösung?
- Die zugehörigen Optimierungsprobleme kann man aber durch eine Reihe von Entscheidungsproblemen lösen:
  - ✓ Gibt es eine Lösung mindestens vom Wert OPT?



# 5.3 Ein Beispiel mit Logik

# Beispiel 5.5: Knapsack

## Beispiel 5.5.

Wir betrachten die folgende Knapsack-Instanz mit  $n = 12$ ,  $z_i = p_i$ ,  $Z = 111444$  und den folgenden Objekten:

Gibt es eine Menge  $S \subseteq \{1, \dots, 12\}$  mit  $\sum_{i \in S} z_i = \sum_{i \in S} p_i = Z$ ?

$z_1 = p_1 =$	100110
$z_2 = p_2 =$	100001
$z_3 = p_3 =$	10101
$z_4 = p_4 =$	10010
$z_5 = p_5 =$	1001
$z_6 = p_6 =$	1110
$z_7 = p_7 =$	200
$z_8 = p_8 =$	100
$z_9 = p_9 =$	20
$z_{10} = p_{10} =$	10
$z_{11} = p_{11} =$	2
$z_{12} = p_{12} =$	1

# Beispiel 5.5: Beobachtungen

$$x_1 \vee \overline{x_1}$$

$$x_2 \vee \overline{x_2}$$

$$x_3 \vee \overline{x_3}$$

$$(x_1 \vee x_2 \vee \overline{x_3})$$

$$(x_1 \vee \overline{x_2} \vee \overline{x_3})$$

$$(\overline{x_1} \vee x_2 \vee x_3)$$

**1. Ziffer:** Man muss 1 oder 2 auswählen, aber nicht beide.

**2. Ziffer:** Man muss 3 oder 4 auswählen, aber nicht beide.

**3. Ziffer:** Man muss 5 oder 6 auswählen, aber nicht beide.

**4. Ziffer:** Man muss 1, 3 oder 6 auswählen, dann kann man mit 7 und 8 den Wert 4 erzeugen.

**5. Ziffer:** Man muss 1, 4 oder 6 auswählen, dann kann man mit 9 und 10 den Wert 4 erzeugen.

**6. Ziffer:** Man muss 2, 3 oder 5 auswählen, dann kann man mit 11 und 12 den Wert 4 erzeugen.

$z_1 = p_1 =$	1	0	1	1	0
$z_2 = p_2 =$	1	0	0	0	1
$z_3 = p_3 =$	1	0	1	0	1
$z_4 = p_4 =$	1	0	0	1	0
$z_5 = p_5 =$	1	0	0	1	0
$z_6 = p_6 =$	1	1	1	0	0
$z_7 = p_7 =$	2	0	0	0	0
$z_8 = p_8 =$	1	0	0	0	0
$z_9 = p_9 =$	2	0	0	0	0
$z_{10} = p_{10} =$	1	0	0	0	0
$z_{11} = p_{11} =$	2	0	0	0	0
$z_{12} = p_{12} =$	1	0	0	0	0

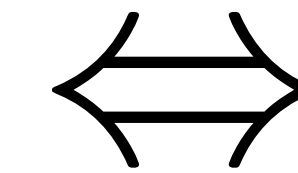
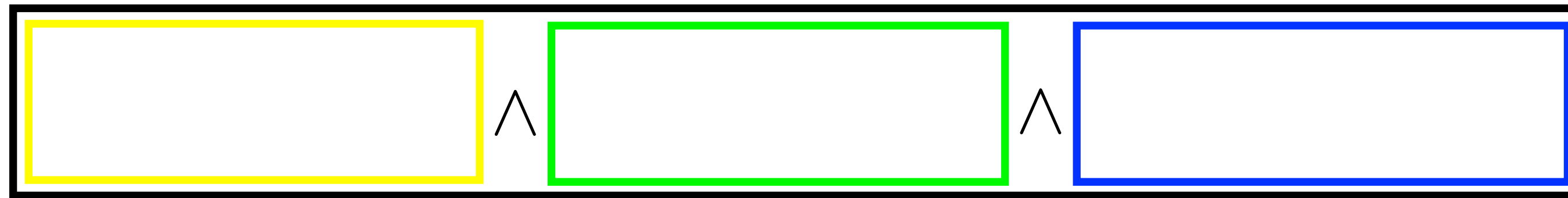
1 1 1 4 4

# Beispiel 5.5: Äquivalenz

$$x_1 \vee \overline{x_1}$$

$$x_2 \vee \overline{x_2}$$

$$x_3 \vee \overline{x_3}$$



$z_1 = p_1 =$	100110
$z_2 = p_2 =$	100001
$z_3 = p_3 =$	10101
$z_4 = p_4 =$	10010
$z_5 = p_5 =$	1001
$z_6 = p_6 =$	1110
$z_7 = p_7 =$	200
$z_8 = p_8 =$	100
$z_9 = p_9 =$	20
$z_{10} = p_{10} =$	10
$z_{11} = p_{11} =$	2
$z_{12} = p_{12} =$	1

**Konkret:** Jede Lösung der logischen Formel entspricht einer Lösung der Instanz SUBSET SUM – und umgekehrt.

**Allgemein:** Für jede logische Formel dieser Art lässt sich schnell eine äquivalente Instanz von SUBSET SUM konstruieren.

**Also:** Wenn wir einen „perfekten“ Algorithmus für SUBSET SUM haben, dann können wir auch schnell entscheiden, ob eine logische Formel lösbar ist.

# 5.4 3SAT

# Das Logikproblem 3SAT




## Definition 5.6. (3-Satisfiability (3SAT))

**Gegeben:** Eine Boolesche Formel, zusammengesetzt aus:

- $n$  Boolesche Variablen  $x_1, \dots, x_n$ , aus denen wir Literale  $\ell_i$  der Form  $x_k$  oder  $\bar{x}_k$  bilden können.
- $m$  Klauseln, jede zusammengesetzt aus genau drei Literalen  $C_j = (\ell_{j,1} \vee \ell_{j,2} \vee \ell_{j,3})$  mit  $1 \leq j \leq m$ .

**Gesucht:** Eine alle  $m$  Klauseln erfüllende (engl: satisfying) Wahrheitsbelegung der  $n$  Variablen.

# Wie schwer sind 3SAT und KNAPSACK?

$$(x_1 \vee x_2 \vee \overline{x_3}) \wedge (x_1 \vee \overline{x_2} \vee \overline{x_3}) \wedge (\overline{x_1} \vee x_2 \vee x_3)$$



$z_i$	$p_i$	KNAPSACK	Weight
$z_1$	$p_1$	110	110
$z_2$	$p_2$	100001	100001
$z_3$	$p_3$	10101	10101
$z_4$	$p_4$	1001	1001
$z_5$	$p_5$	1001	1001
$z_6$	$p_6$	111	111
$z_7$	$p_7$		
$z_8$	$p_8$		100
$z_9$	$p_9$		20
$z_{10}$	$p_{10}$		10
$z_{11}$	$p_{11}$		2
$z_{12}$	$p_{12}$		1

**Satz 5.9.** Wenn 0-1-KNAPSACK  $\in P$  ist, dann ist auch 3SAT  $\in P$ .

**Satz 5.12** (Satz von Cook 1971). Wenn 3SAT  $\in P$ , dann gilt  $P = NP$ .

**Korollar 5.11.** Wenn Knapsack  $\in P$ , dann gilt  $P = NP$ .

# 5.5 Konsequenzen



# Algorithmen und Investmentbanker

**Ziele:** Ein „perfekter“ Algorithmus liefert

**1. immer**

**2. schnell**

**3. eine optimale Lösung.**

**Ziele:** Ein „perfekter“ Finanzberater ist ein

**1. ehrlicher**

**2. intelligenter**

**3. Investmentbanker.**

WE OFFER THREE • KINDS OF SERVICE

GOOD • FAST • CHEAP

YOU CAN PICK ANY TWO



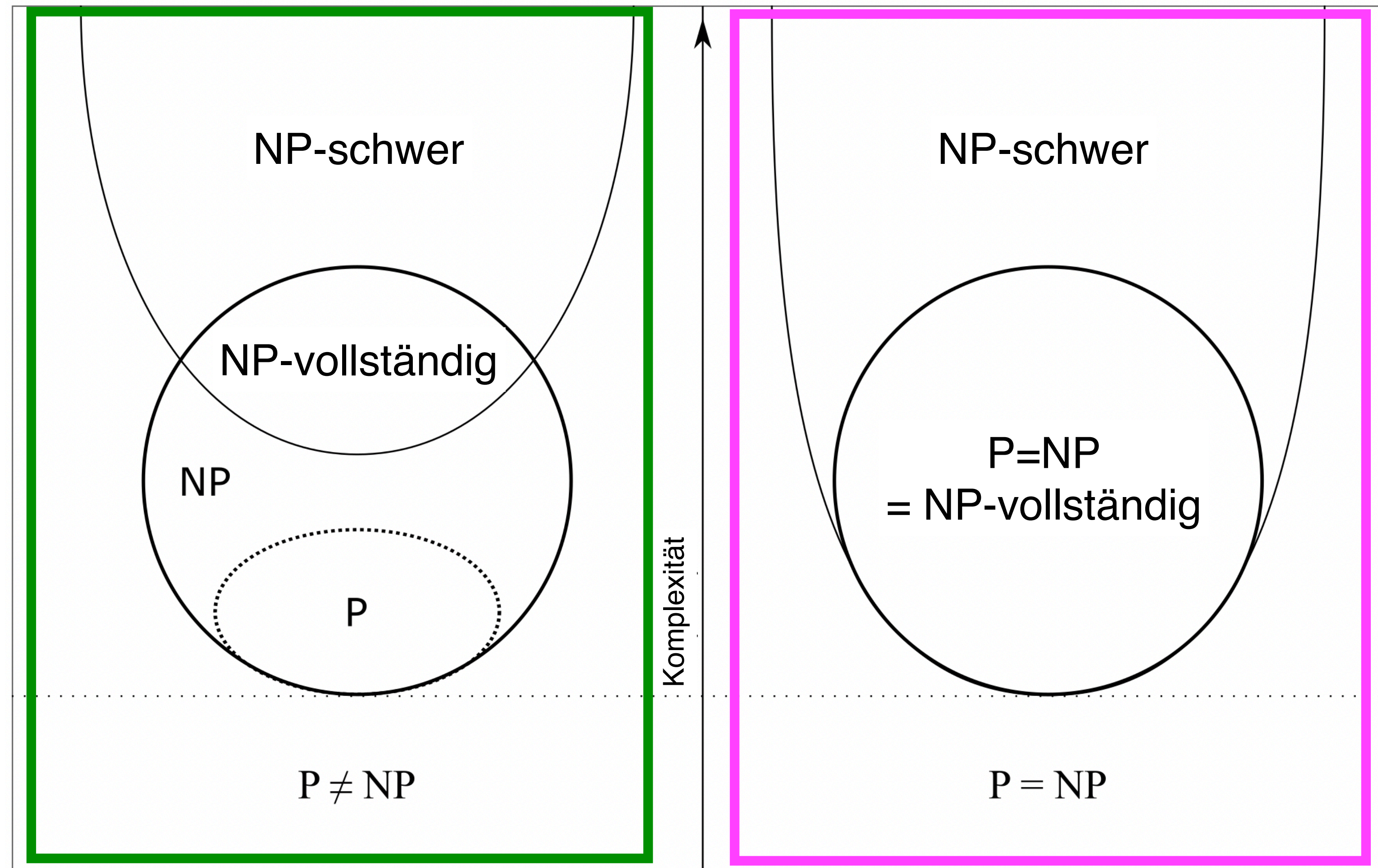
GOOD & CHEAP WONT BE FAST

GOOD & FAST WON'T BE CHEAP

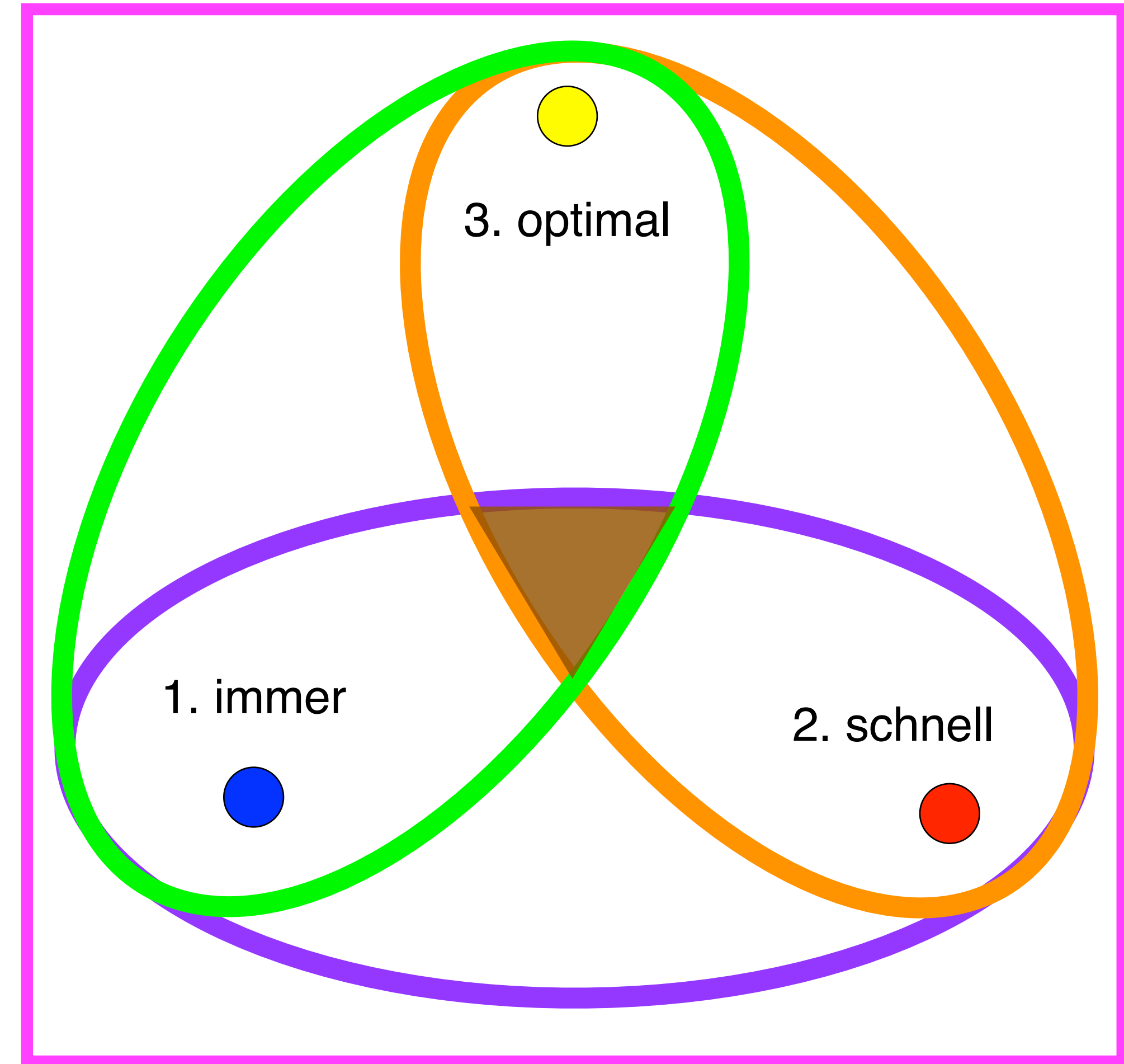
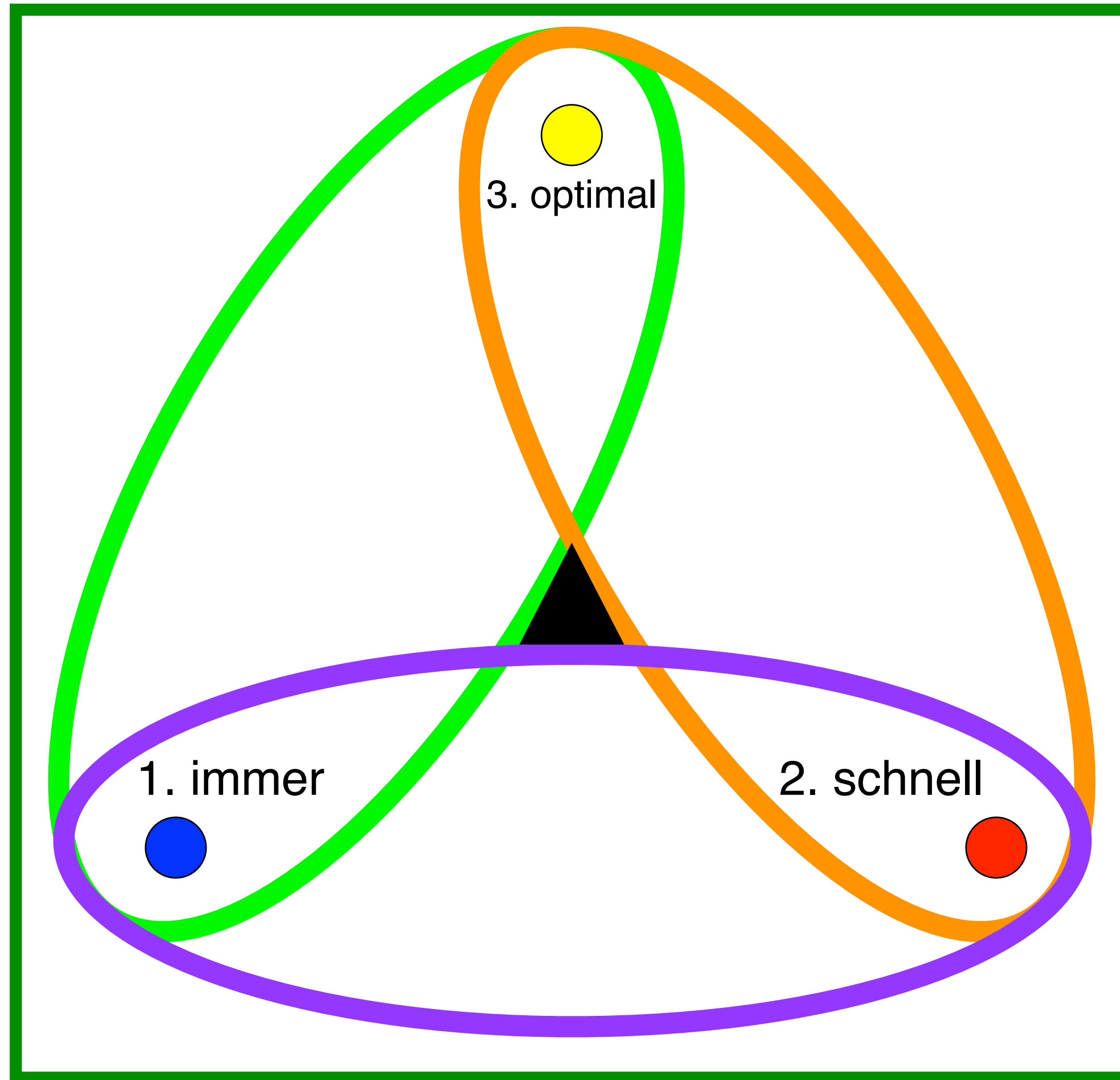
FAST & CHEAP WON'T BE GOOD



# Die Komplexitätslandschaft



# Das Bild für Knapsack



# Umgang mit schwierigen Situationen

**Ziel:** Algorithmus für NP-schweres Problem

1. immer

2. schnell

3. eine optimale Lösung.

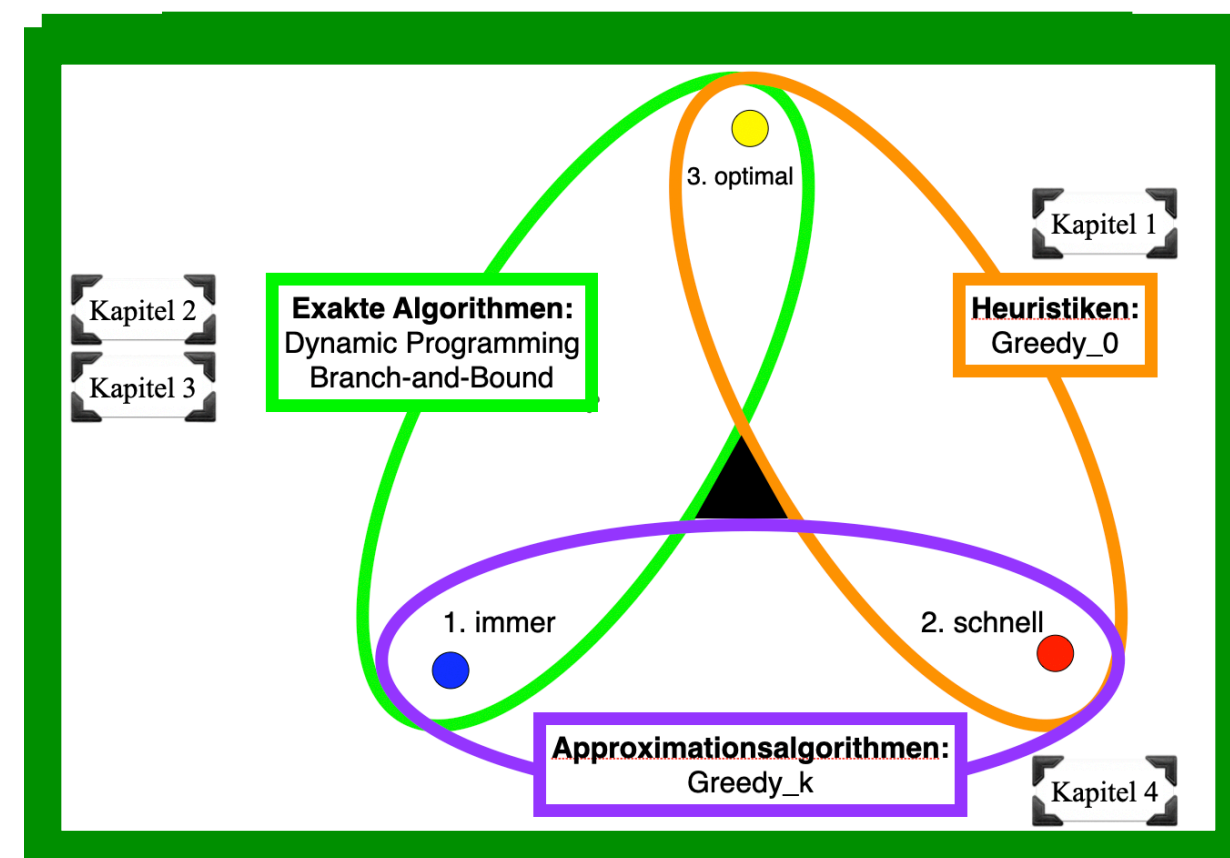
## Persönlichkeitsprofile:

(A) Mit dem Schicksal hadern und diskutieren

(B) Auf Glück vertrauen

(C) Hart arbeiten

(D) Erwartungen zurückschrauben



(A) Komplexitätsanalyse: Spezialfall nicht NP-schwer?

(B) Heuristiken: raten und hoffen

(C) Exakte Algorithmen

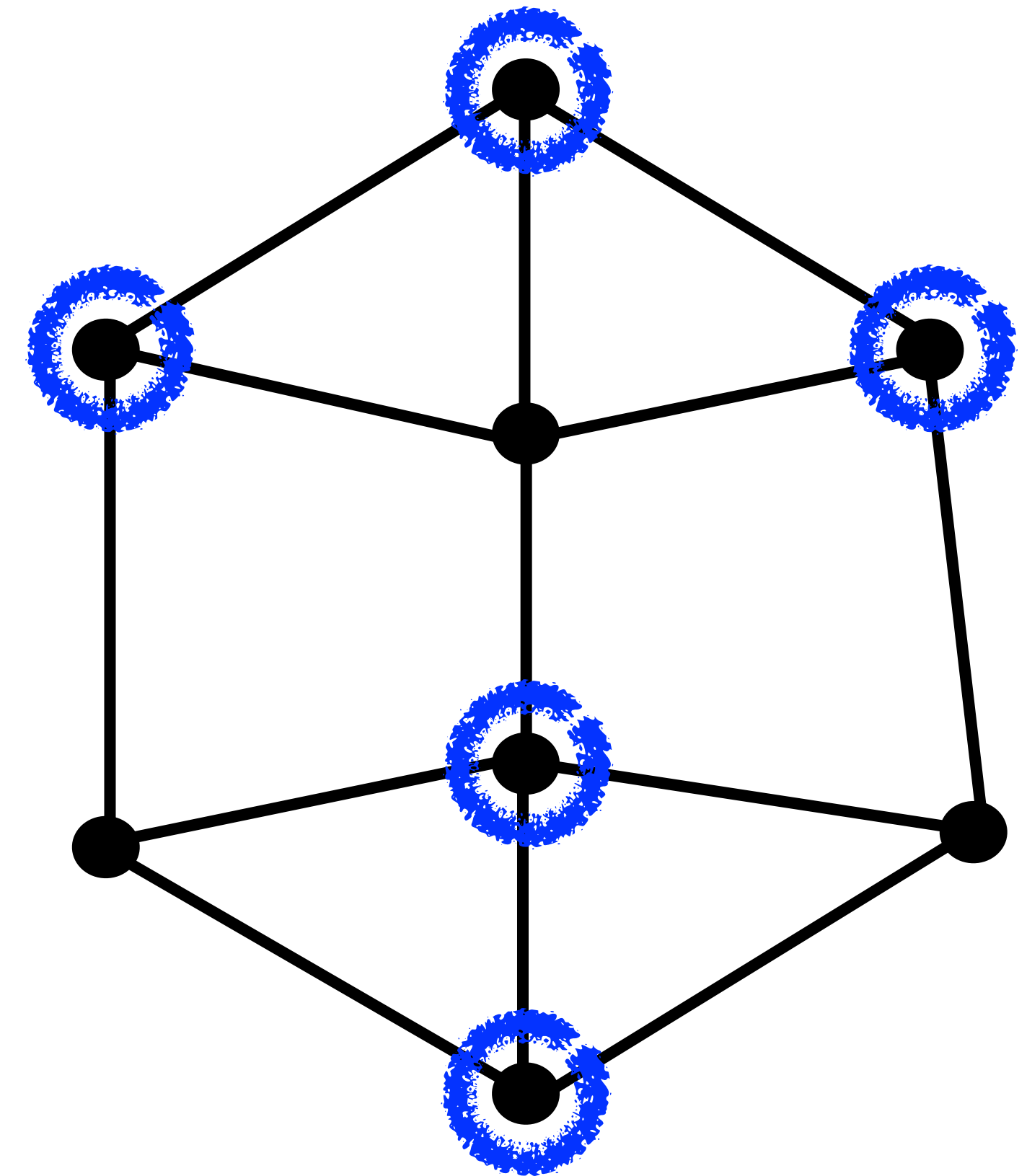
(D) Approximationsalgorithmen: „gut“ statt „optimal“

# 5.6 Ausblick

# Vertex Cover

**Gegeben:** Ein Graph  $G=(V,E)$

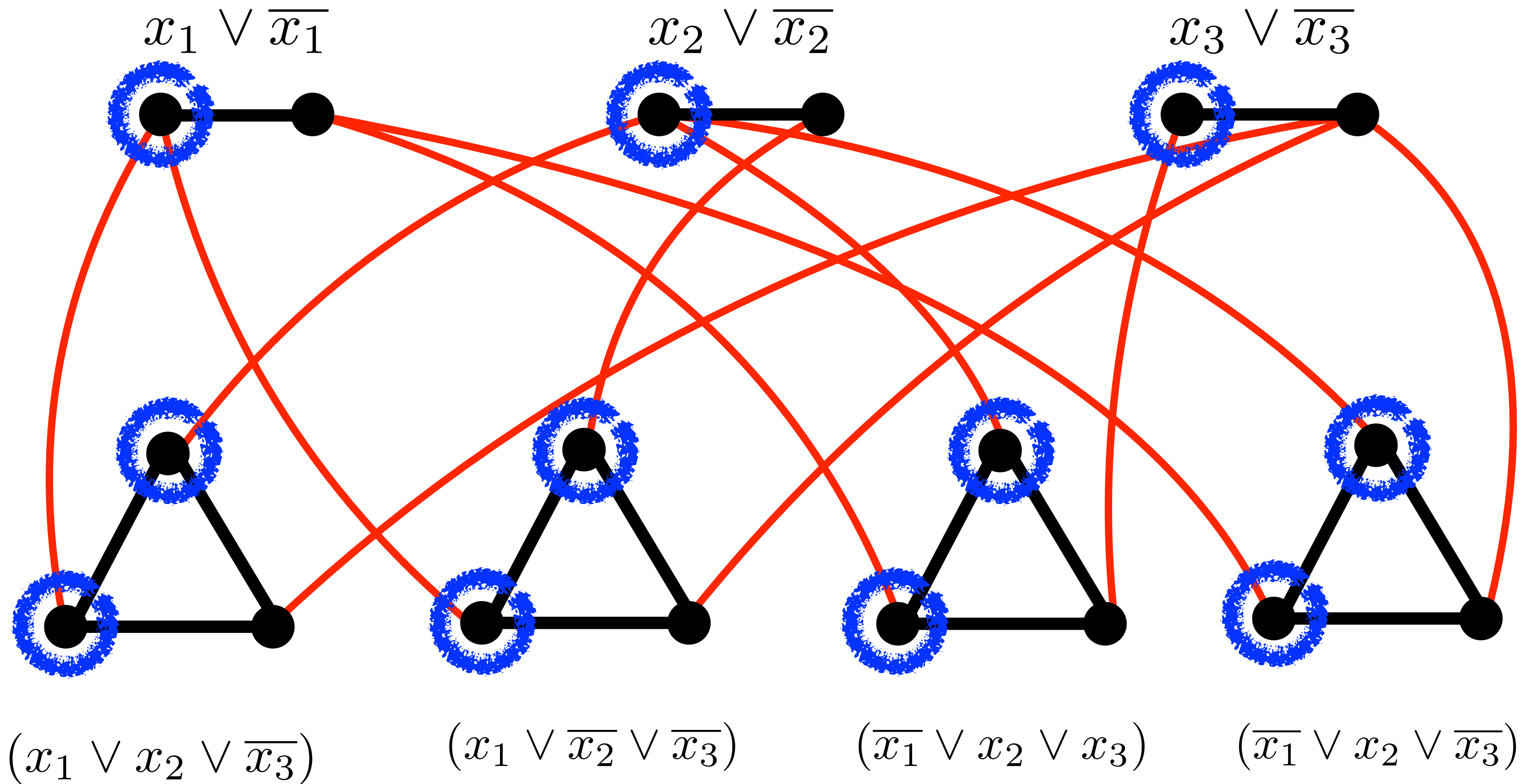
**Gesucht:** Ein kleinstmögliches **Vertex Cover**  $S$  in  $G$ :  
eine möglichst kleine Menge von Knoten,  
die alle Kanten überdecken



# Entscheidungskomponenten

$n$  Variablen

$m$  Klauseln



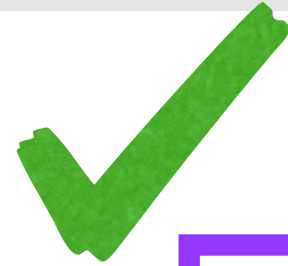
$n$  Knoten

$0$  Knoten

$2m$  Knoten



# Reduktion von 3SAT auf VERTEX COVER

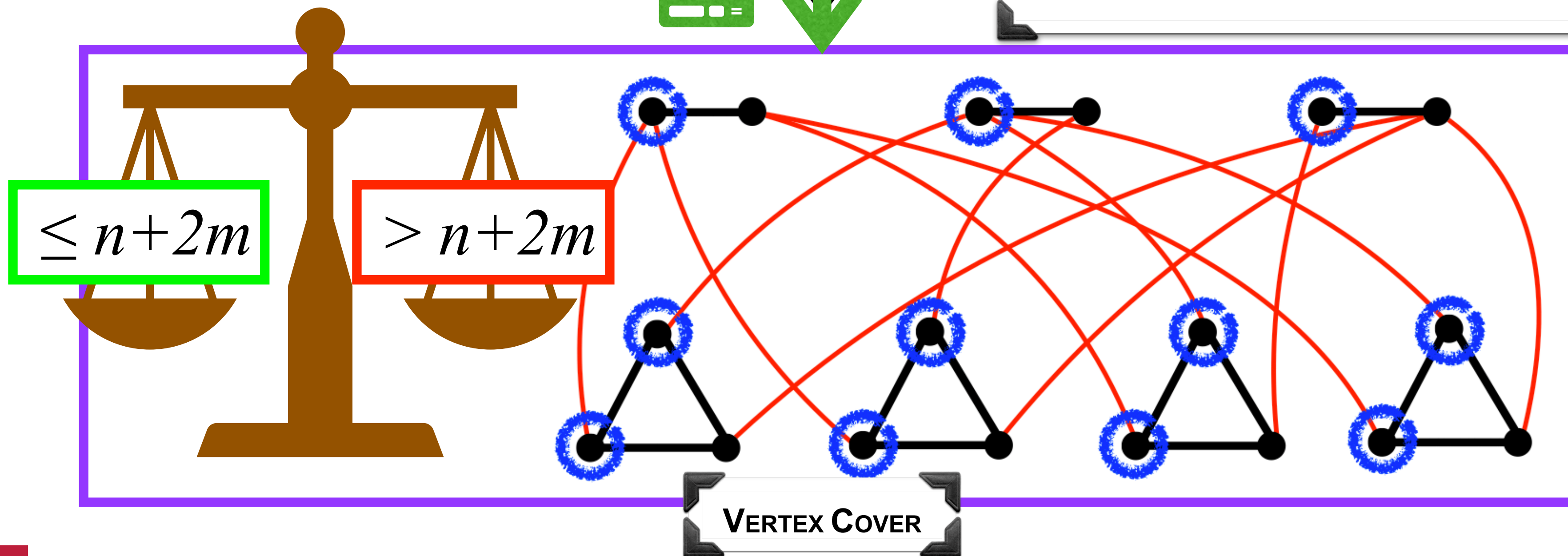


3SAT

$$(x_1 \vee x_2 \vee \overline{x_3}) \wedge (x_1 \vee \overline{x_2} \vee \overline{x_3}) \wedge (\overline{x_1} \vee x_2 \vee x_3) \wedge (\overline{x_1} \vee x_2 \vee \overline{x_3})$$



Satz 6.4. *Vertex Cover ist NP-schwer.*



# Optimierungsmethoden für höherdimensionale Packprobleme

Sándor P. Fekete  
TU Braunschweig  
s.fekete@tu-bs.de



# 7 Hashing

*Algorithmen und Datenstrukturen 2  
Sommer 2023*

**Prof. Dr. Sándor Fekete**

# 7.1 Motivation

# Aufgabenstellung

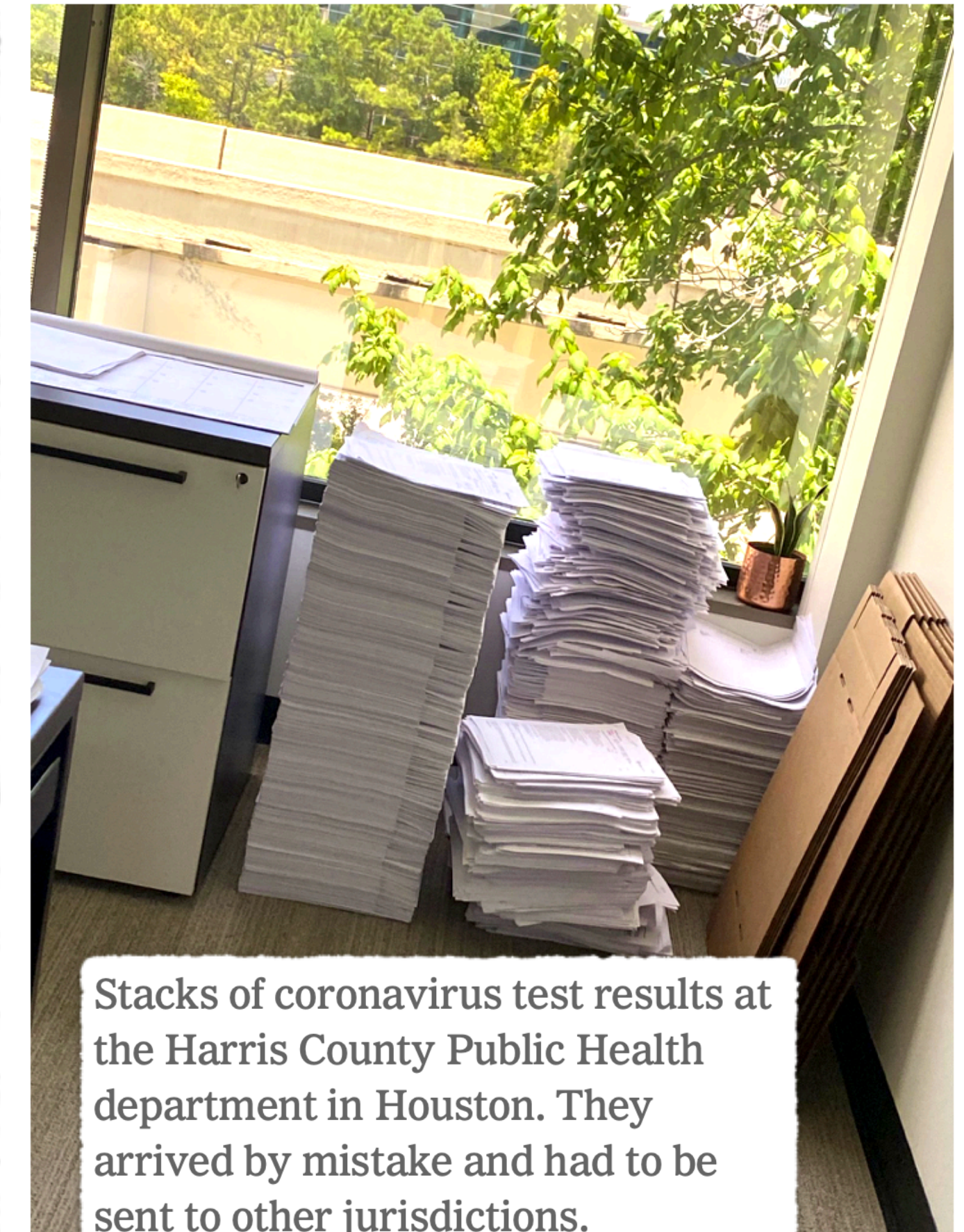
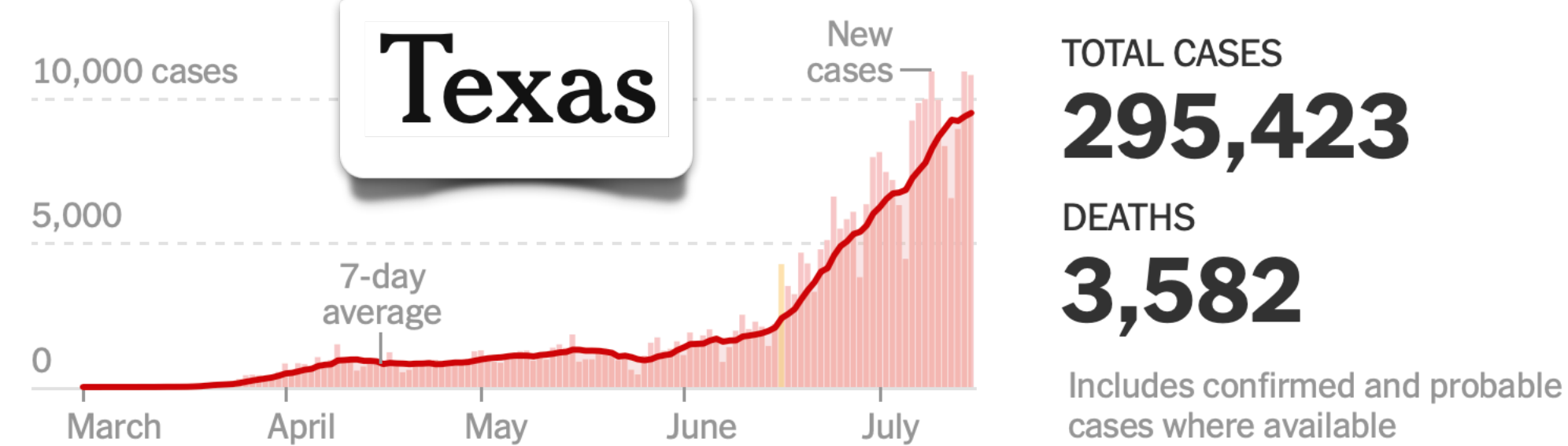
The New York Times

July 13, 2020

## Bottleneck for U.S. Coronavirus Response: The Fax Machine

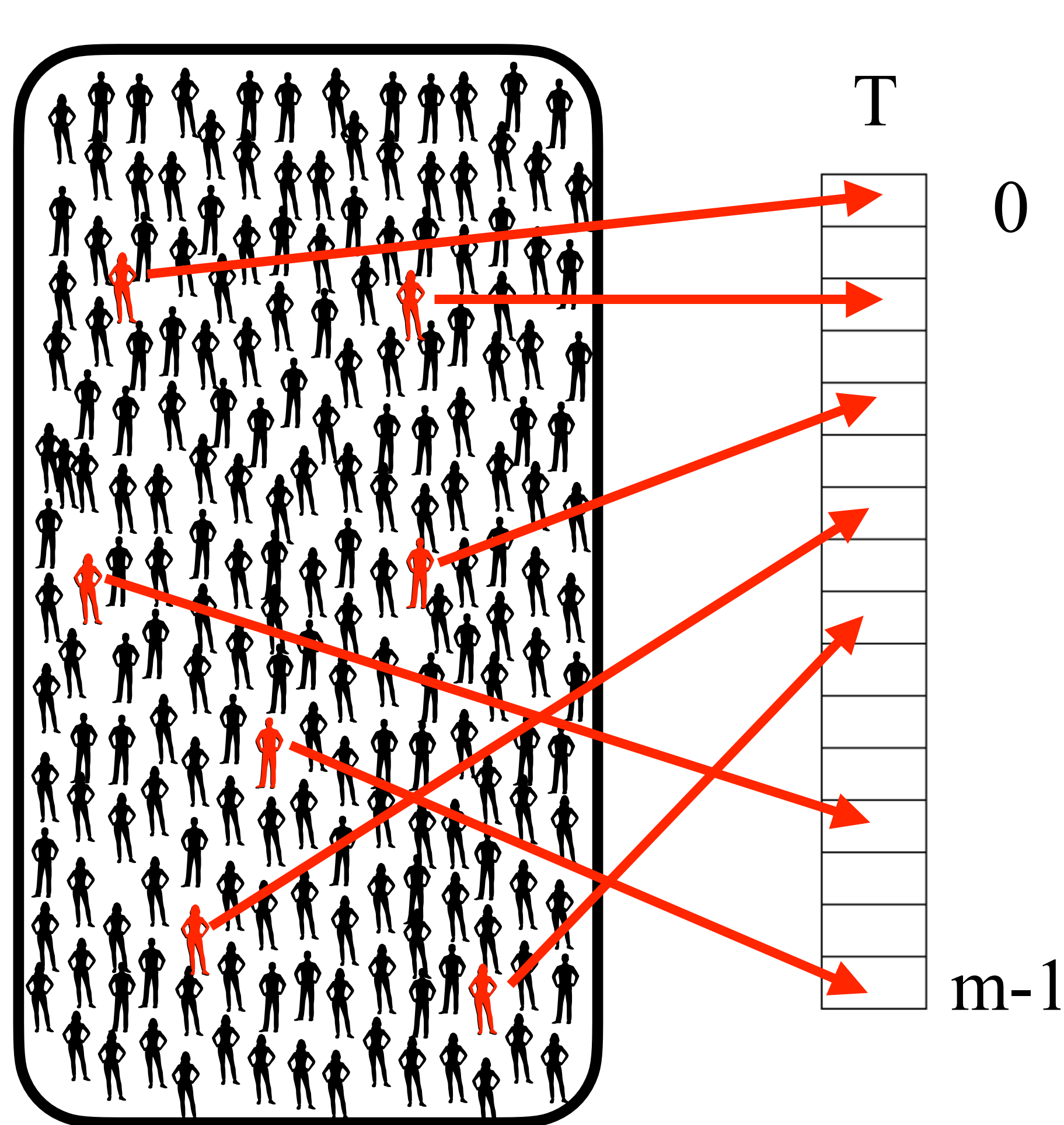
Before public health officials can manage the pandemic, they must deal with a broken data system that sends incomplete results in formats they can't easily use.

By The New York Times Updated July 16, 2020, 12:06 A.M. E.T.



Stacks of coronavirus test results at the Harris County Public Health department in Houston. They arrived by mistake and had to be sent to other jurisdictions.

# Aufgabenstellung



  $U$         $S$

0

## Hashing

- Menge  $U$  potentieller Schlüssel sehr groß, aktuelle Schlüsselmenge  $S$  jeweils nur kleine Teilmenge des Universums (im allgemeinen  $S$  nicht bekannt)
- **Idee:** durch Berechnung feststellen, wo Datensatz mit Schlüssel  $x$  gespeichert
- Abspeicherung der Datensätze in einem Array  $T$  mit Indizes  $\{0, 1, \dots, m - 1\}$ : **Hashtabelle**
- **Hashfunktion**  $h$  liefert für jeden Schlüssel  $x \in U$  eine Adresse in Hashtabelle, d.h.  $h : U \rightarrow \{0, 1, \dots, m - 1\}$ .

$m-1$

# 7.2 Aufgabenstellung

# Aufgabenstellung

## Aufgabe

Dynamische Verwaltung von Daten, wobei jeder Datensatz eindeutig durch einen Schlüssel charakterisiert ist

Viele Anwendungen benötigen nur einfache Daten-Zugriffsmechanismen (**dictionary operations**):

- Suche nach Datensatz bei gegebenem Schlüssel  $x$   
**search( $x$ )**
- Einfügen eines neuen Datensatzes  $d$  mit Schlüssel  $x$   
**insert( $x, d$ )** (abgekürzt **insert( $x$ )**)
- Entfernen eines Datensatzes bei gegebenem Schlüssel  $x$   
**delete( $x$ )**

Menge potentieller Schlüssel (**Universum**) kann **sehr** groß sein!





# Alternativen

Sei  $n := |S|$ .

- Balancierte Suchbäume (AVL-Bäume, B-Bäume):  
dictionary operations haben Komplexität  $O(\log n)$
- Hashing:  
für alle Operationen **mittlere** Komplexität  $O(1)$

## Belegungsfaktor

Quotient  $\beta := n/m$  heißt Belegungsfaktor oder Auslastungsfaktor einer Hashtabelle der Größe  $m$ .

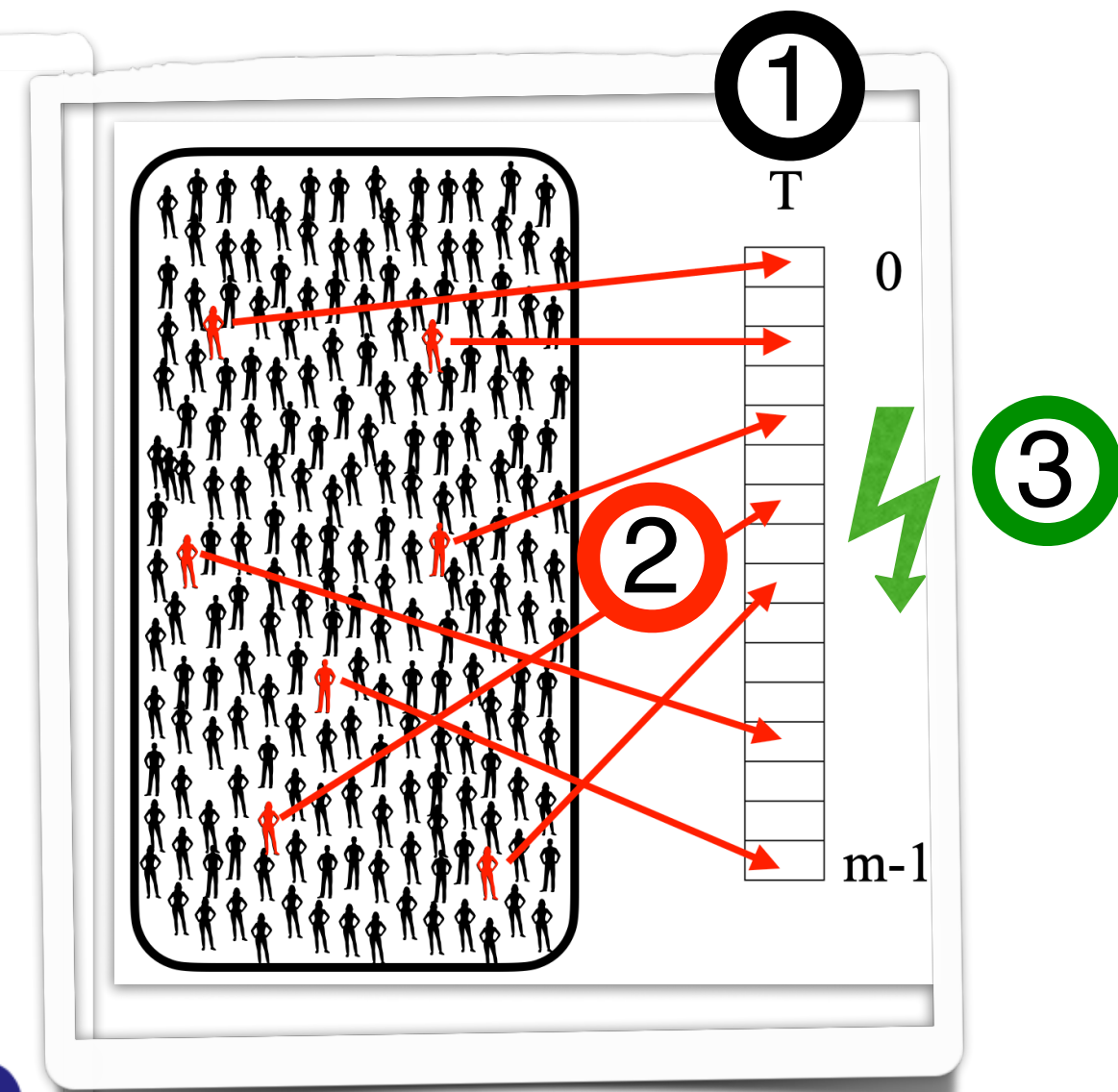
Mittlerer Aufwand für dictionary operations als Funktion in  $\beta$  abschätzbar

→ Anzahl aktueller Schlüssel geht nur indirekt in Aufwand ein

# Herausforderungen

Anzahl möglicher Schlüssel viel größer als Hashtabelle, also  $|U| \gg m$

- Hashfunktion muss verschiedene Schlüssel  $x_1$  und  $x_2$  auf gleiche Adresse abbilden.
- $x_1$  und  $x_2$  beide in aktueller Schlüsselmenge  
→ Adresskollision



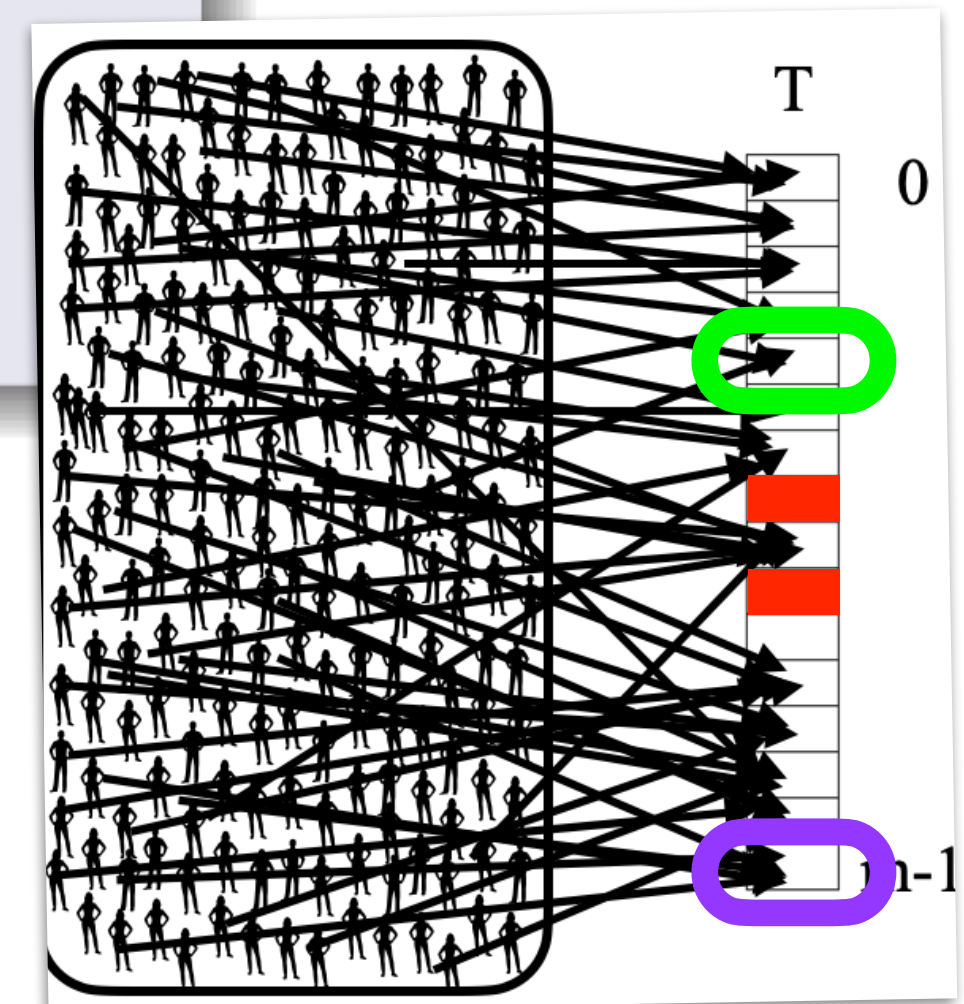
Hashverfahren gegeben durch:

- ① eine Hashtabelle,
- ② eine Hashfunktion, die Universum der möglichen Schlüssel auf Adressen einer Hashtabelle abbildet,
- ③ eine Strategie zur Auflösung möglicher Adresskollisionen.

# Anforderungen

## Gute Hashfunktionen sollten:

- surjektiv sein, d.h. den ganzen Wertebereich umfassen,
- die zu speichernden Schlüssel (möglichst) gleichmäßig verteilen, d.h. für alle Speicherplätze  $i$  und  $j$  sollte gelten  $|h^{-1}(i)| \approx |h^{-1}(j)|$ ,
- effizient berechenbar sein.



# 7.3 Hashfunktionen

# Divisions-Rest-Methode

## Divisions-Rest-Methode

$$h(x) = x \bmod m := x - \left\lfloor \frac{x}{m} \right\rfloor \cdot m$$

**Beispiel:**  $m=11$ ,  $S=\{49, 22, 6, 52, 76, 34, 13, 29\}$

**Hashwerte:**  $h(49) = 5$

$h(22) = 0$

$h(6) = 6$

$h(52) = 8$

$h(76) = 10$

$h(34) = 1$

$h(13) = 2$

$h(29) = 7$

# Wahl von $m$

Problem: Daten oft nicht gleichverteilt!

Beispiel: Texte in Zahlen übertragen, oft viele Leerzeichen, bestimmte Wörter häufiger etc.

Wichtig: geeignete Wahl von  $m$

- $m$  Zweierpotenz:  $x \bmod m$  wählt nur die letzten  $\log m$  Bits
- $m$  Primzahl:  $x \bmod m$  beeinflusst alle Bits

# 7.4 Kollisionen

# Auftreten von Kollisionen

## Zur Erinnerung:

Im Allgemeinen unvermeidbar, dass Kollisionen auftreten, denn aus  $N \gg m$  folgt Existenz eines Speicherplatzes  $i$  mit  $|h^{-1}(i)| \geq N/m$ .

## Frage:

Sei  $n := |S|$ . Wie wahrscheinlich sind Kollisionen bei  $n \ll m$ ?

## Geburtstagsparadoxon

Bei wie vielen (zufällig gewählten) Personen ist es *wahrscheinlich*, dass hiervon zwei am selben Datum (Tag und Monat) Geburtstag haben?



# Geburtstagsparadoxon

## Annahme:

- Daten unabhängig
- $\text{Prob}(h(x) = j) = 1/m$

Prob( $i$ -tes Datum kollidiert nicht mit den ersten  $i - 1$  Daten, wenn diese kollisionsfrei sind) =  $\frac{m - (i - 1)}{m}$

## Intuition:

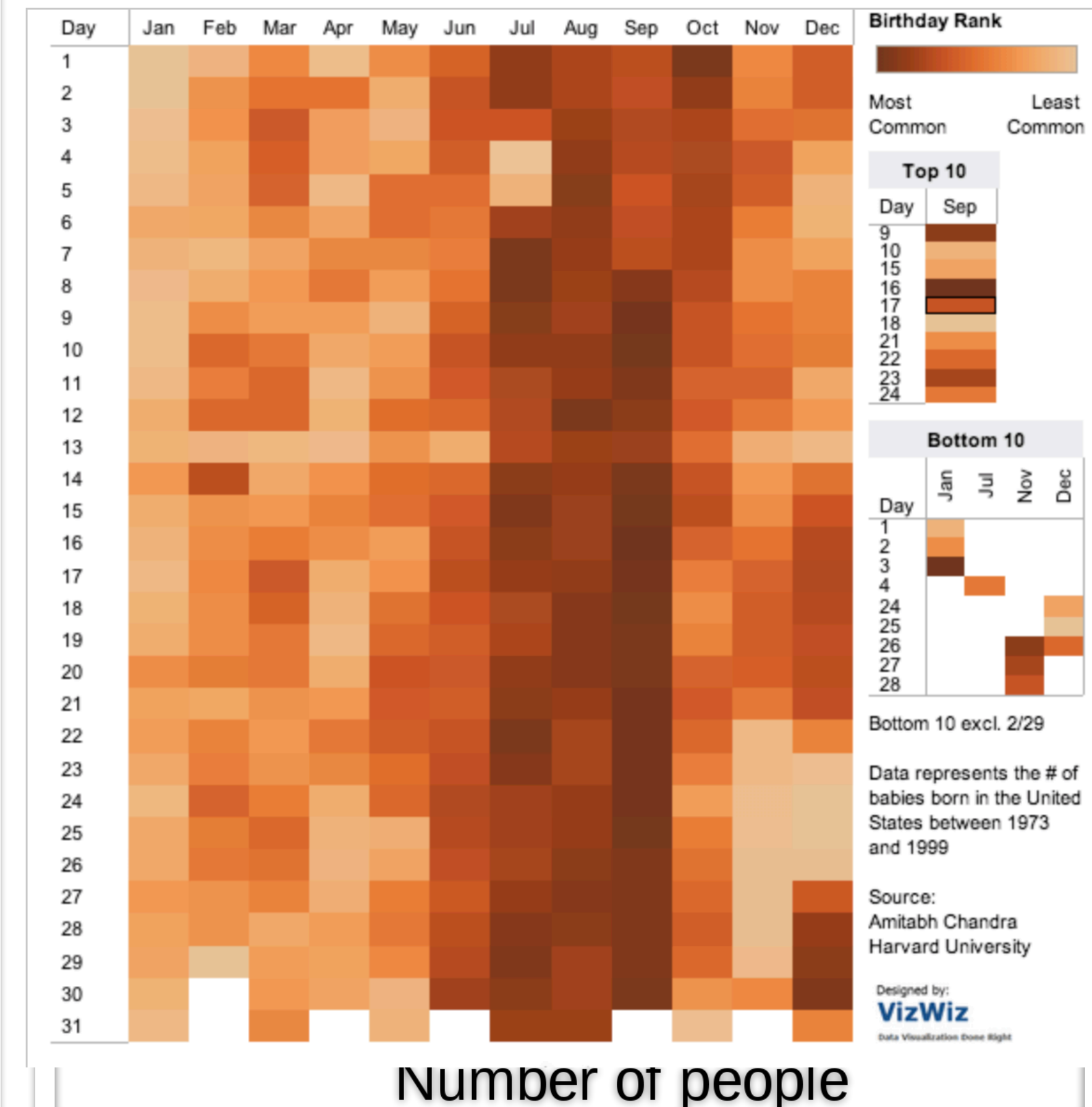
Egal welche Speicherplätze die ersten  $i - 1$  Daten belegen,  $m - i + 1$  der  $m$  Möglichkeiten sind *gut*.

Prob( $n$  Daten kollisionsfrei) =  $\frac{m-1}{m} \cdot \frac{m-2}{m} \dots \frac{m-n+1}{m}$

**Beispiel:**  $m = 365$

Prob(23 Daten kollisionsfrei)  $\approx 0.49$

Prob(50 Daten kollisionsfrei)  $\approx 0.03$



# Geburtstagsparadoxon (verallgemeinert)

Prob( $2m^{1/2}$  Daten kollisionsfrei) =

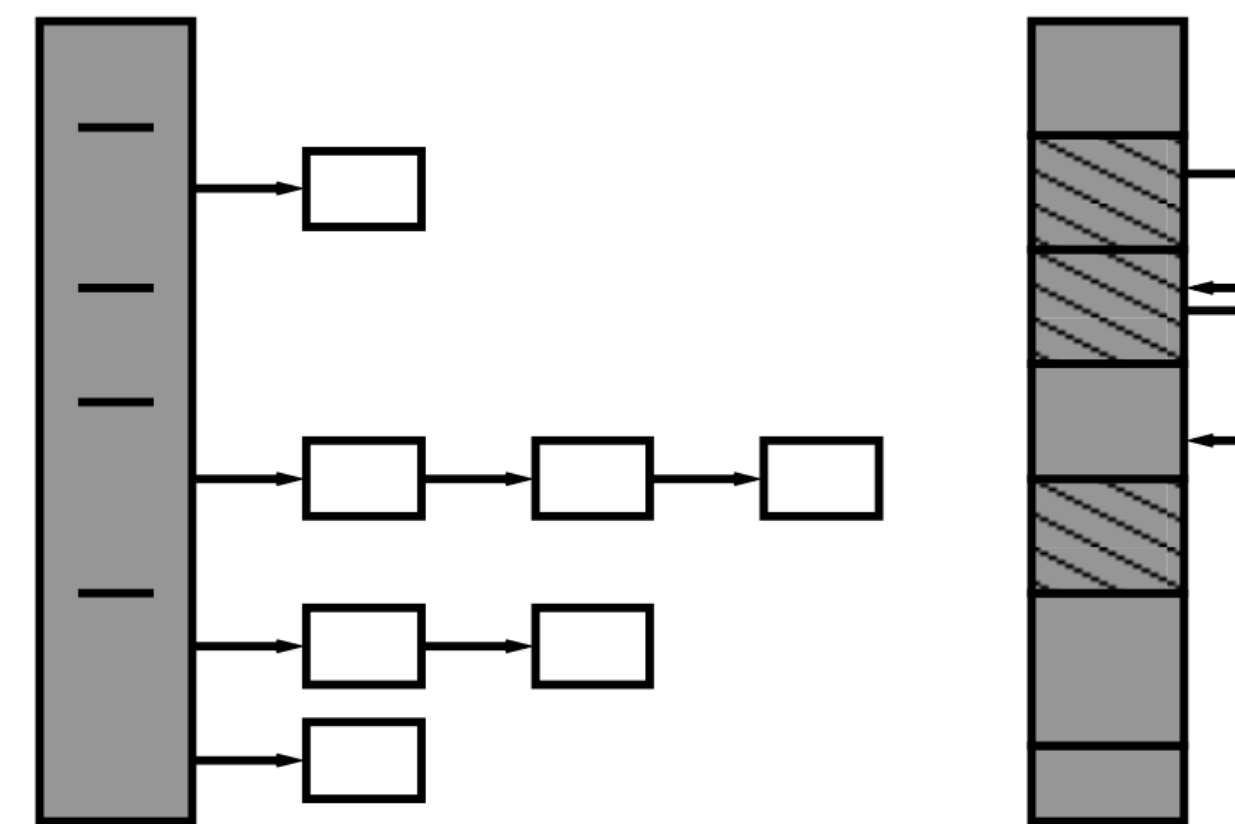
$$\frac{m-1}{m} \dots \frac{m-m^{1/2}}{m} \dots \frac{m-2m^{1/2}+1}{m}$$
$$\leq 1 \cdot \left( \frac{m-m^{1/2}}{m} \right)^{m^{1/2}} = \left( 1 - \frac{1}{m^{1/2}} \right)^{m^{1/2}} \approx \frac{1}{e}$$

Hashing muss mit Kollisionen leben und benötigt Strategien zur Kollisionsbehandlung!

# Kollisionbehandlung

Verschiedene Arten der Kollisionsbehandlung:

- mittels verketteter Listen  
(links)
- mittels offener Adressierung  
(rechts)



# 7.5 Verkettung von Überläufern

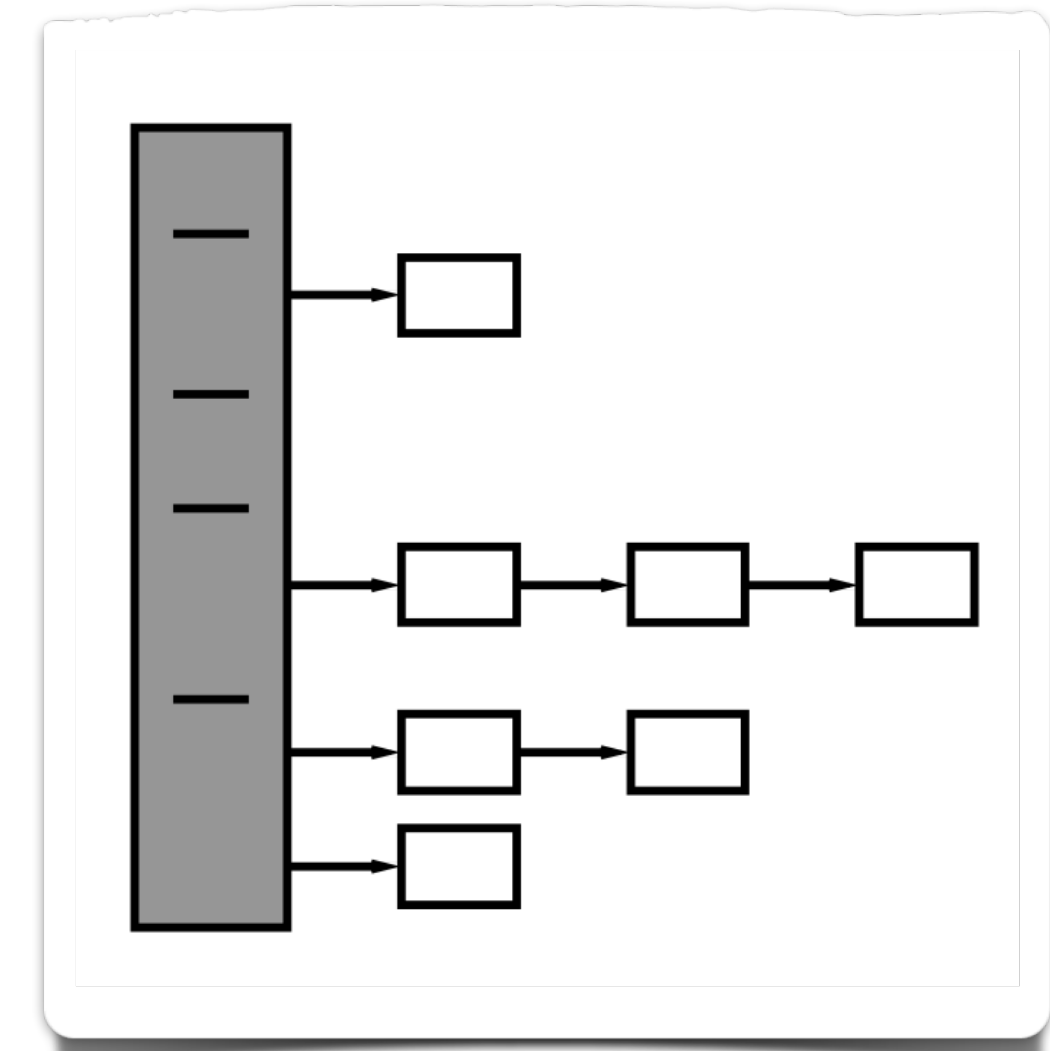
# Verkettung: Realisierung

## Realisierung:

Jede Komponente der Hashtabelle enthält Zeiger auf paarweise disjunkte lineare Listen. Die  $i$ -te Liste  $L(i)$  enthält alle Schlüssel  $x \in S$  mit  $h(x) = i$ .

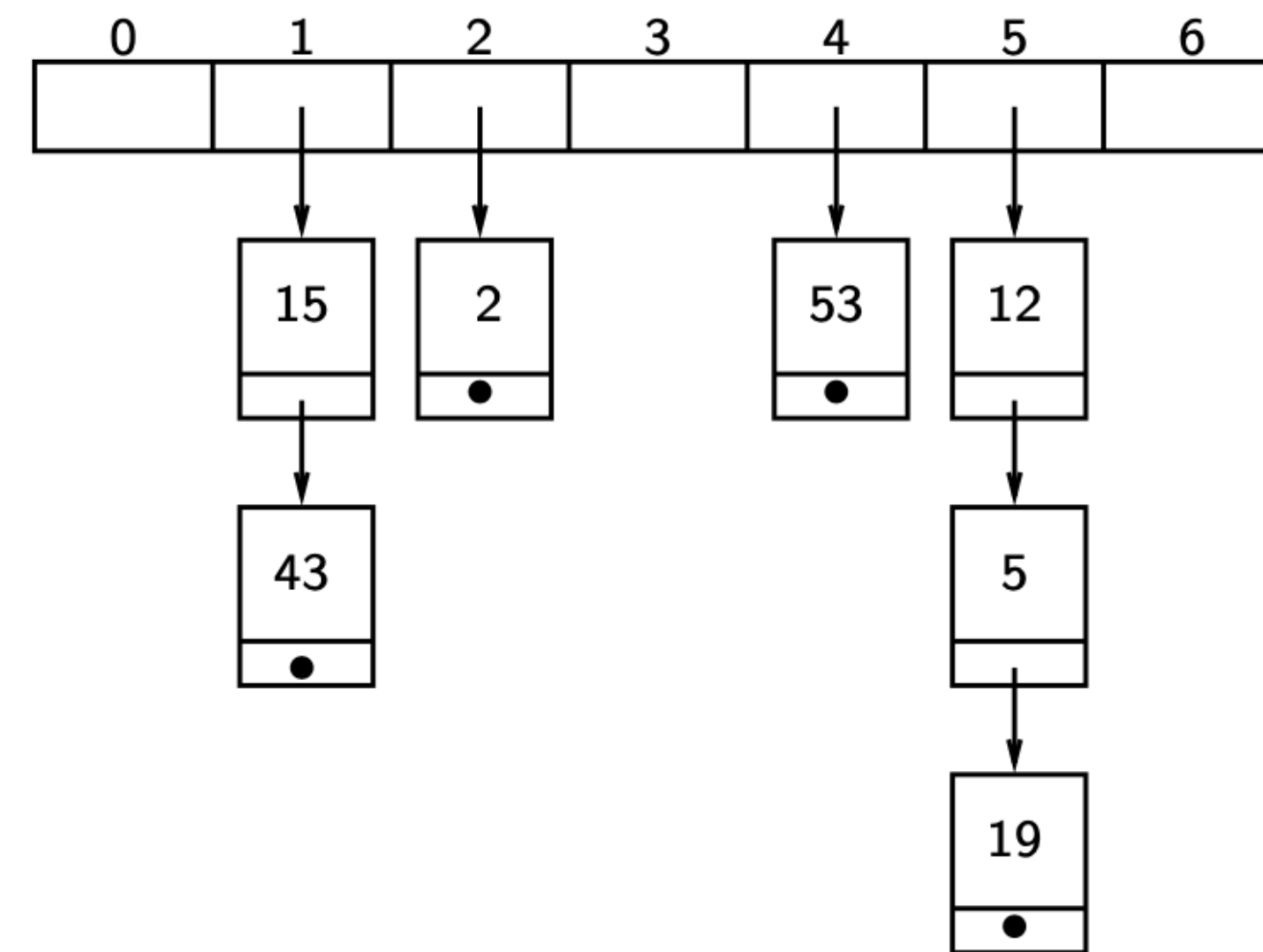
Vorteil: Alle Operationen werden unterstützt und  $n > m$  ist möglich. (Für  $n \gg m$  jedoch Rehashing ratsam) Nachteil: Speicherplatzbedarf für Zeiger

- $\text{search}(x)$ : Berechne  $h(x)$  und suche in Liste  $L(h(x))$ .
- $\text{insert}(x)$  (nach erfolgloser Suche): Berechne  $h(x)$  und füge  $x$  in Liste  $L(h(x))$  ein.
- $\text{delete}(x)$  (nach erfolgreicher Suche): Berechne  $h(x)$ , suche  $x$  in Liste  $L(h(x))$  und entferne  $x$ .



# Beispiel

Beispiel:  $m = 7$  und  $h(x) = x \bmod m$   
 $S = \{2, 12, 5, 15, 19, 43, 53\}$



# Analyse

Bei zufälligen Daten und ideal streuenden Hashfunktion gilt für

$$X_{ij} := \begin{cases} 1 & i\text{-tes Datum kommt in Liste } L(j) \\ 0 & \text{sonst} \end{cases}$$

$$\text{Prob}(X_{ij} = 1) = \frac{1}{m}$$

$$\rightarrow \text{E}(X_{ij}) = 1 \cdot \frac{1}{m} + 0 \cdot \frac{m-1}{m} = \frac{1}{m}$$

$X_j = X_{1j} + \dots + X_{nj}$  zählt Anzahl Daten in Liste  $L(j)$ .

$$\text{E}(X_j) = \text{E}(X_{1j} + \dots + X_{nj}) = \text{E}(X_{1j}) + \dots + \text{E}(X_{nj}) = \frac{n}{m}$$

# Analyse (2)

- Erfolgreiche Suche in Liste  $L(j)$ :

Inklusive nil-Zeiger durchschnittlich  $1 + \frac{n}{m} = 1 + \beta$  Objekte betrachten

**Beispiel:** Für  $n \approx 0.95 \cdot m$  ist dies  $\approx 1.95$ .

- Erfolgreiche Suche in Liste  $L(j)$  der Länge  $\ell$ :

Jede Position in der Liste hat Wahrscheinlichkeit  $1/\ell$ , also  $\frac{1}{\ell}(1 + 2 + \dots + \ell) = \frac{\ell+1}{2}$ .

Durchschnittliche Listenlänge hier:  $1 + \frac{n-1}{m}$

(Liste enthält sicher das gesuchte Datum, und die anderen  $n - 1$  Daten sind zufällig verteilt.)

Also erwartete Suchdauer  $\frac{1}{2}(1 + \frac{n-1}{m} + 1) = 1 + \frac{n-1}{2m} \approx 1 + \frac{\beta}{2}$

**Beispiel:** Für  $n \approx 0.95 \cdot m$  ist dies  $\approx 1.475$ .



# 7.6 Offene Adressierung

# 7.6 Offene Adressierung

# Anforderungen

## Zur Erinnerung:

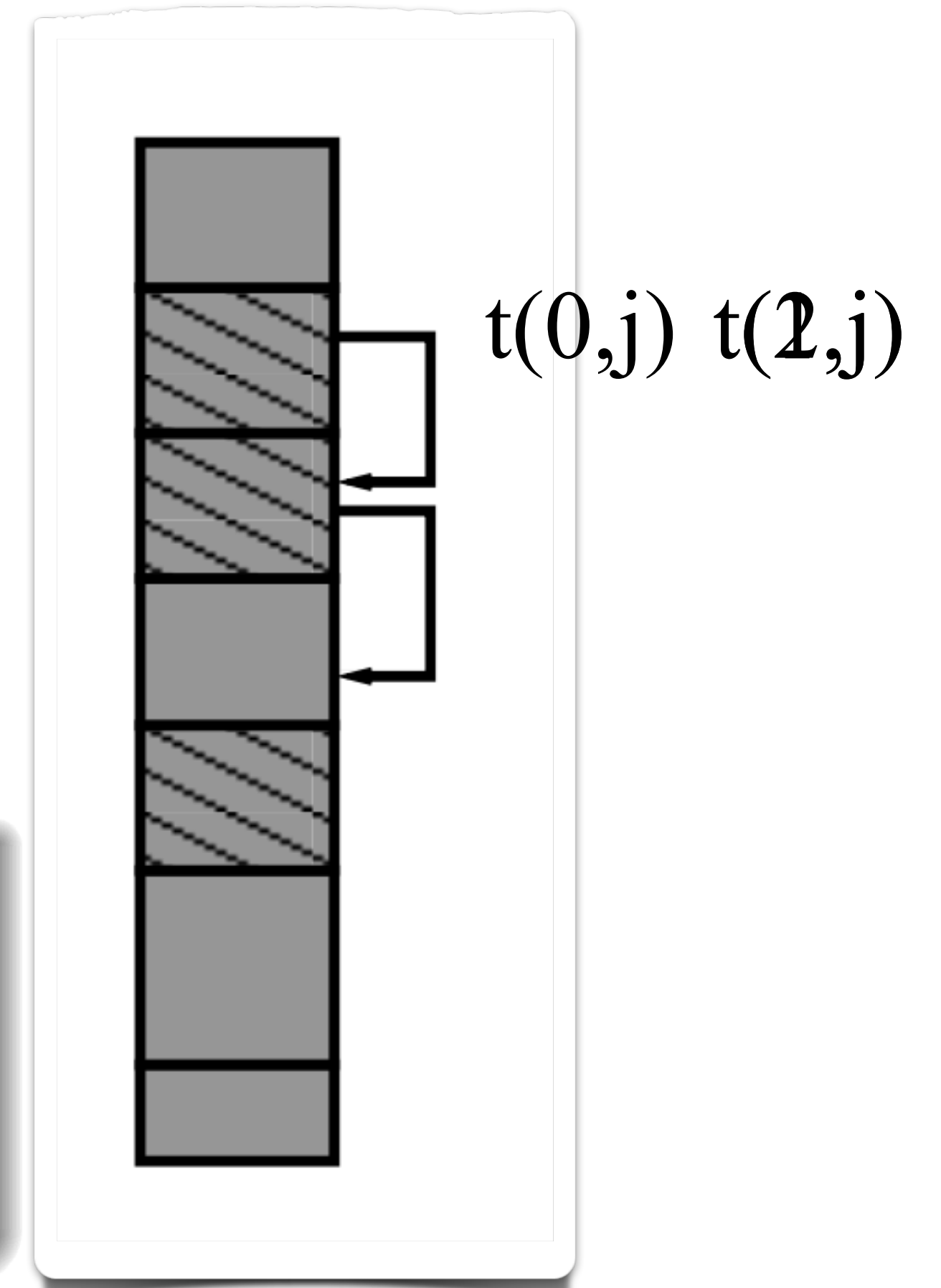
Im Kollisionsfall nach fester Regel alternativen freien Platz in Hashtabelle suchen (**Sondierungsfolge**).

**Voraussetzung:** Auswertung von  $h$  gilt als eine Operation.

$t(i, j) :=$  Position des  $i$ -ten Versuchs zum Einfügen von Daten  $x$  mit  $h(x) = j$

## Anforderung an Funktion $t$ :

- auch  $t$  in Zeit  $O(1)$  berechenbar
- $t(0, j) = j$
- $t(\cdot, j) : \{0, \dots, m - 1\} \rightarrow \{0, \dots, m - 1\}$  bijektiv



# Operationen

- $\text{search}(x)$ :
  - Berechne  $j := h(x)$ .
  - Suche  $x$  an den Positionen  $t(0, j), \dots, t(m-1, j)$ .
  - Abbruch, wenn  $x$  gefunden oder freie Stelle entdeckt (kein Datum mit Schlüssel  $x$ ).
- $\text{insert}(x)$  nach erfolgloser Suche:
  - Freien Platz finden (sonst Overflow) und  $x$  dort einfügen.
- $\text{delete}(x)$  nach erfolgreicher Suche:
  - Das Datum kann nicht einfach entfernt werden, da  $\text{search}$  frühzeitig Lücken finden würde und eine Suche fälschlicherweise als erfolglos abbrechen könnte.

# Löschen?!

Problem: Datum kann bei Operation `delete( $x$ )` nicht ohne weiteres gelöscht werden.

Ausweg: Speicherplatz/Position als `besetzt`, `noch nie besetzt` oder `wieder frei` markieren.

→ Suche wird nur an Positionen mit Markierung `noch nie besetzt` vorzeitig abgebrochen.

Problem: Im Laufe der Zeit keine Position mehr, die mit `noch nie besetzt` markiert ist.

→ Hashing wird ineffizient.

Offenes Hashing nur bei Anwendungen mit `search` und `insert`.

# Sondieren

- Lineares Sondieren
- Quadratisches Sondieren
- Multiplikatives Sondieren
- Doppeltes Hashing

Hilfsmittel bei der Analyse: **ideales Hashing**

# Lineares Sondieren

$$t(i, j) := (i + j) \bmod m$$

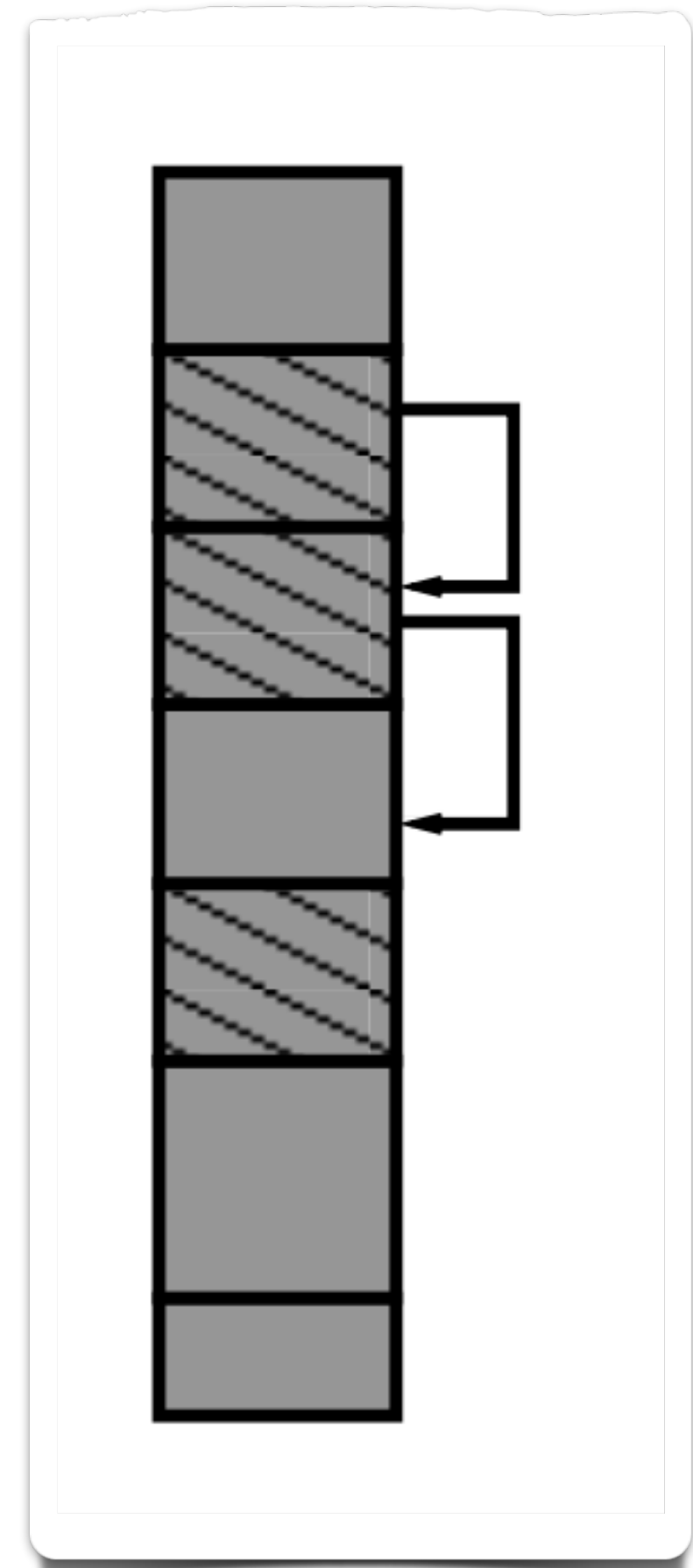
Beispiel:  $m = 19$  und  $j = h(x) = 7$

Sondierungsfolge:

7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 0, 1, 2, 3, 4, 5, 6

Problem: *Clusterbildung*

Tendenz, dass immer längere zusammenhängende, belegte Abschnitte in der Hashtabelle entstehen, sogenannte *Cluster*  
→ erhöhte Suchzeiten



# Problem des Linearen Sondieren

Beispiel:  $m = 19$ , Positionen 2, 5, 6, 9, 10, 11, 12, 17 belegt

$h(x)$ :	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
landet an																			
Position:	0	1	3	3	4	7	7	7	8	13	13	13	13	13	14	15	16	18	18
W.keit:	$\frac{1}{19}$	$\frac{1}{19}$	0	$\frac{2}{19}$	$\frac{1}{19}$	0	0	$\frac{3}{19}$	$\frac{1}{19}$	0	0	0	0	$\frac{5}{19}$	$\frac{1}{19}$	$\frac{1}{19}$	$\frac{1}{19}$	0	$\frac{2}{19}$





# Ideales Hashing

## Wunsch:

Zu jedem Zeitpunkt haben alle Positionen die gleiche Wahrscheinlichkeit, besetzt zu werden.

## Beobachtung:

Das geht numerisch nicht genau, im Beispiel 11 freie Plätze, 19 mögliche Hashwerte, also alle Wahrscheinlichkeiten  $k/19$ , nicht  $k/11$ .

## Modell des idealen Hashings:

Alle  $\binom{m}{n}$  Möglichkeiten, die  $n$  besetzten Plätze für  $m$  Schlüssel auszuwählen, haben die gleiche Wahrscheinlichkeit.

Lineares Sondieren ist weit vom idealen Hashing entfernt.

# Quadratisches Sondieren

$$t(i, j) := j + (-1)^{i+1} \cdot \lfloor \frac{i+1}{2} \rfloor^2 \bmod m$$

Sondierungsfolge:

$$j, j + 1^2, j - 1^2, j + 2^2, j - 2^2, \dots, j + (\frac{m-1}{2})^2, j - (\frac{m-1}{2})^2$$

Beispiel:  $m = 19$  und  $j = h(x) = 7$

Sondierungsfolge:

$$\begin{array}{cccccc} 7, & 8, & 6, & 11, & 3, & 16, & -2 & 23 & -9 & 32 & -18 \\ & & & & & & = 17, & = 4, & = 10, & = 13, & = 1, \end{array}$$

$$\begin{array}{cccccc} 43 & -29 & 56 & -42 & 71 & -57 & 88 & -74 \\ = 5, & = 9, & = 18, & = 15, & = 14, & = 0, & = 12, & = 2 \end{array}$$

# Quadratisches Sondieren (2)

Frage: Ist  $t(\cdot, j)$  für alle  $j$  und  $m$  bijektiv?

**Nein**, aber immer wenn  $m \equiv 3 \pmod{4}$  und  $m$  eine Primzahl ist  
(Beweis: Zahlentheorie)

Besser als **lineares Sondieren**, aber für großes  $m$  sind die ersten Werte noch *nah* an  $j$

# Multiplikatives Sondieren

Hier:  $h(x) = x \bmod (m - 1) + 1$  und damit in  $\{1, \dots, m - 1\}$

$$t(i, j) := i \cdot j \bmod m, 1 \leq i \leq m - 1$$

Hashwerte  $1, \dots, m - 1$

Beispiel:  $m = 19$  und  $j = h(x) = 7$

Sondierungsfolge:

$i \cdot j$	7	14	21	28	35	42	49	56	63
$i \cdot j \bmod 19$	7	14	2	9	16	4	11	18	6

$i \cdot j$	70	77	84	91	98	105	112	119	126
$i \cdot j \bmod 19$	13	1	8	15	3	10	17	5	12

# Multiplikatives Sondieren (2)

Frage: Ist  $t(\cdot, j)$  für alle  $j$  und  $m$  bijektiv?

**Nein**, aber immer wenn  $m$  Primzahl und  $j \neq 0$

**Beweis:** Durch Widerspruch!

Falls nicht, gibt es  $1 \leq i_1 < i_2 \leq m - 1$  mit

$$i_1 \cdot j \equiv i_2 \cdot j \pmod{m}$$

$$\Rightarrow j \cdot (i_2 - i_1) \equiv 0 \pmod{m}$$

$$\Rightarrow j \cdot (i_2 - i_1) \text{ ist Vielfaches von } m$$

$$\Rightarrow \text{Primfaktorzerlegung von } j \cdot (i_2 - i_1) \text{ muss } m \text{ enthalten}$$

Widerspruch zu  $1 \leq j \leq m - 1, 1 \leq i_2 - i_1 \leq m - 1$

# Doppeltes Hashing

Sei  $h_1(x) \equiv x \pmod{m}$  und  $h_2(x) \equiv x \pmod{(m-2)+1}$ .

$i$ -te Position für  $x$ :  $h_1(x) + i \cdot h_2(x) \pmod{m}$ ,  $1 \leq i \leq m-1$

**Beispiel:**  $m = 19$  und  $x = 47$

$h_1(47) \equiv 47 \pmod{19} = 9$  und  $h_2(47) \equiv 47 \pmod{17+1} = 14$

**Sondierungsfolge:**

9, 4, 18, 13, 8, 3, 17, 12, 7, 2, 16, 11, 6, 1, 15, 10, 5, 0, 14

# Doppeltes Hashing (2)

## Beobachtung:

$i \cdot h_2(x)$  durchläuft für  $1 \leq i \leq m - 1$  die Werte  $1, \dots, m - 1$  in irgendeiner Reihenfolge, ergänzt wird  $0 = 0 \cdot h_2(x)$

Durch den Summanden  $h_1(x)$  wird der Anfang zufällig verschoben.

Doppeltes Hashing kommt dem **idealen Hashing** am nächsten.

# Zusammenfassung

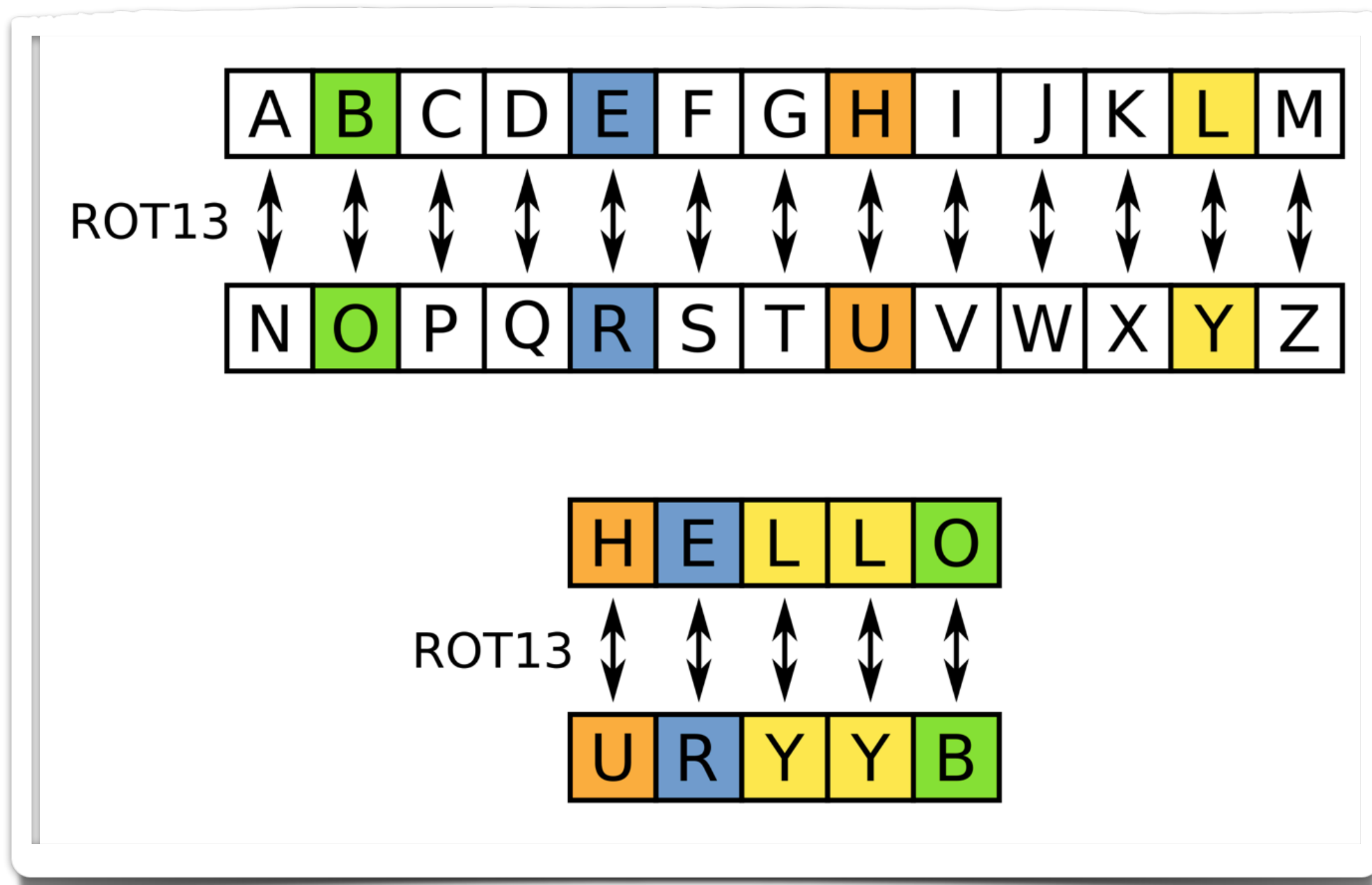
- Auch die beste Hashfunktion kann Kollisionen nicht ganz vermeiden, deshalb sind Hashverfahren im *Worst Case* ineffiziente Realisierungen der Operationen **search**, **insert**, **delete**.
- Im **Durchschnitt** sind sie jedoch weitaus effizienter als Verfahren, die auf Schlüsselvergleichen basieren.
- Die Anzahl benötigter Schritte zum Suchen, Einfügen und Entfernen hängt (im Durchschnitt) im wesentlichen vom Belegungsfaktor, d.h. dem Verhältnis von Anzahl aktueller Schlüssel zur Größe der Hashtabelle, ab.



# 7.7 Kryptographie

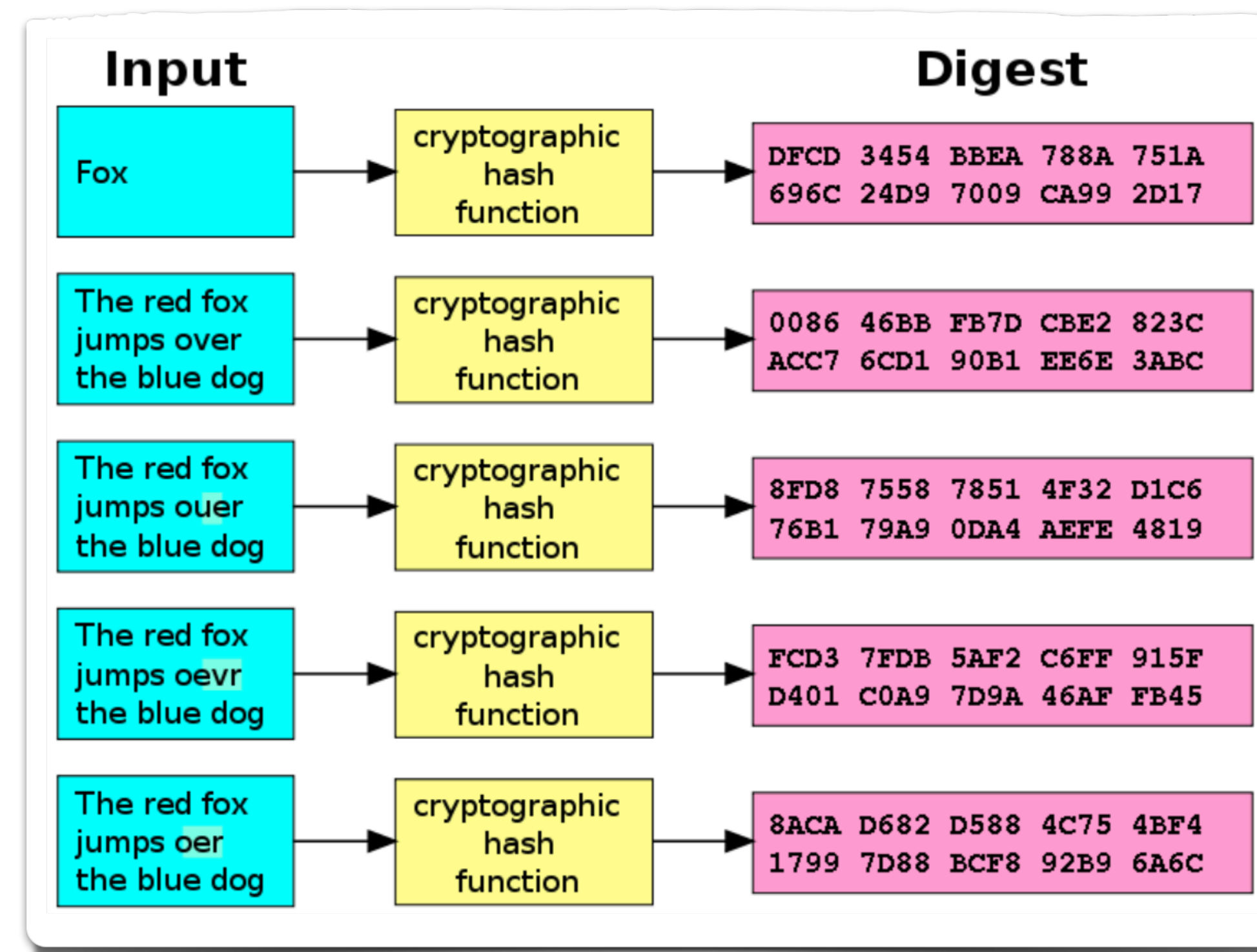
# Veränderte Ziele

- Text codieren:
  1. Berechtigter Empfänger soll Nachricht entschlüsseln können.
  2. Unberechtigter Empfänger soll Nachricht nicht entschlüsseln können.

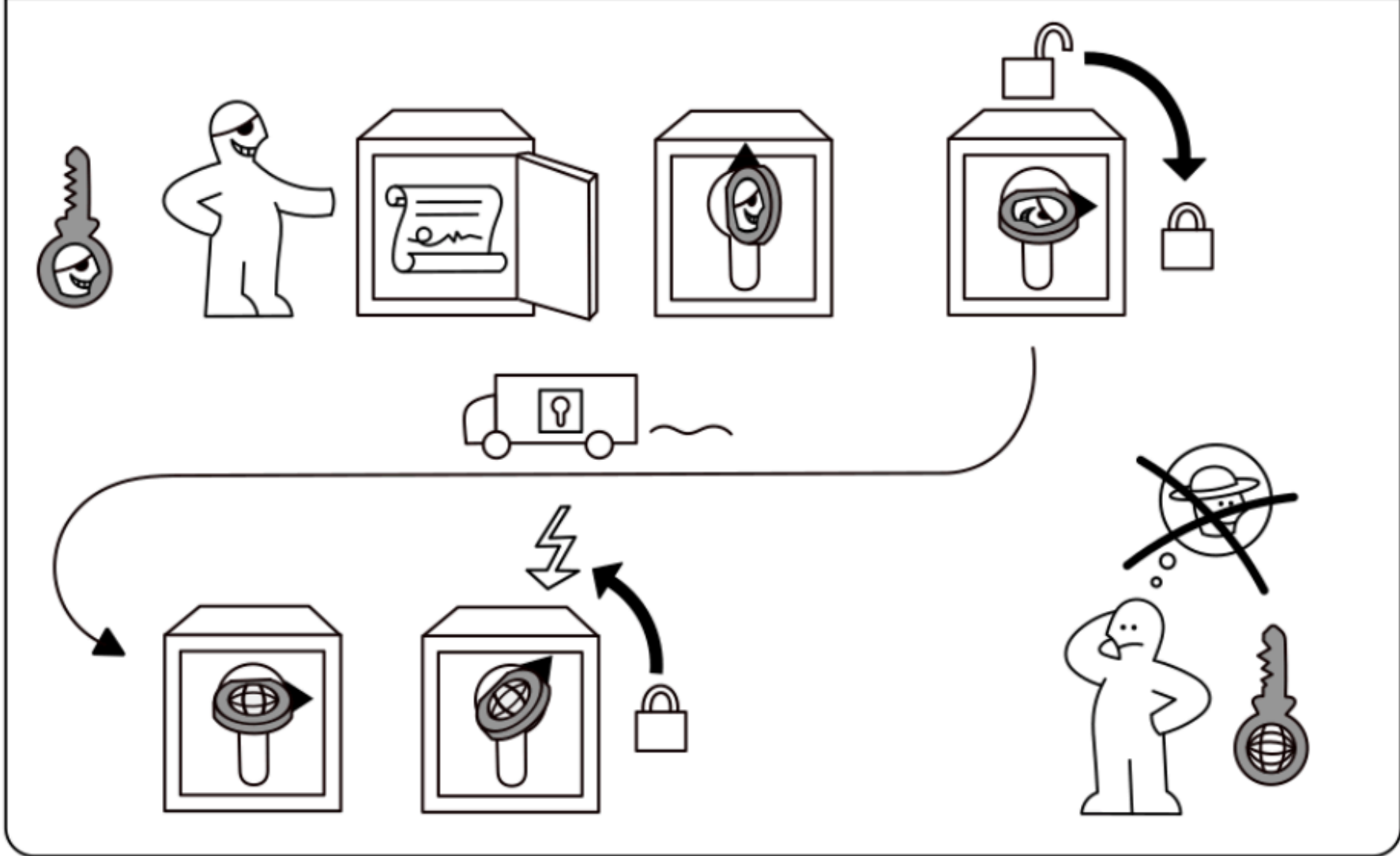
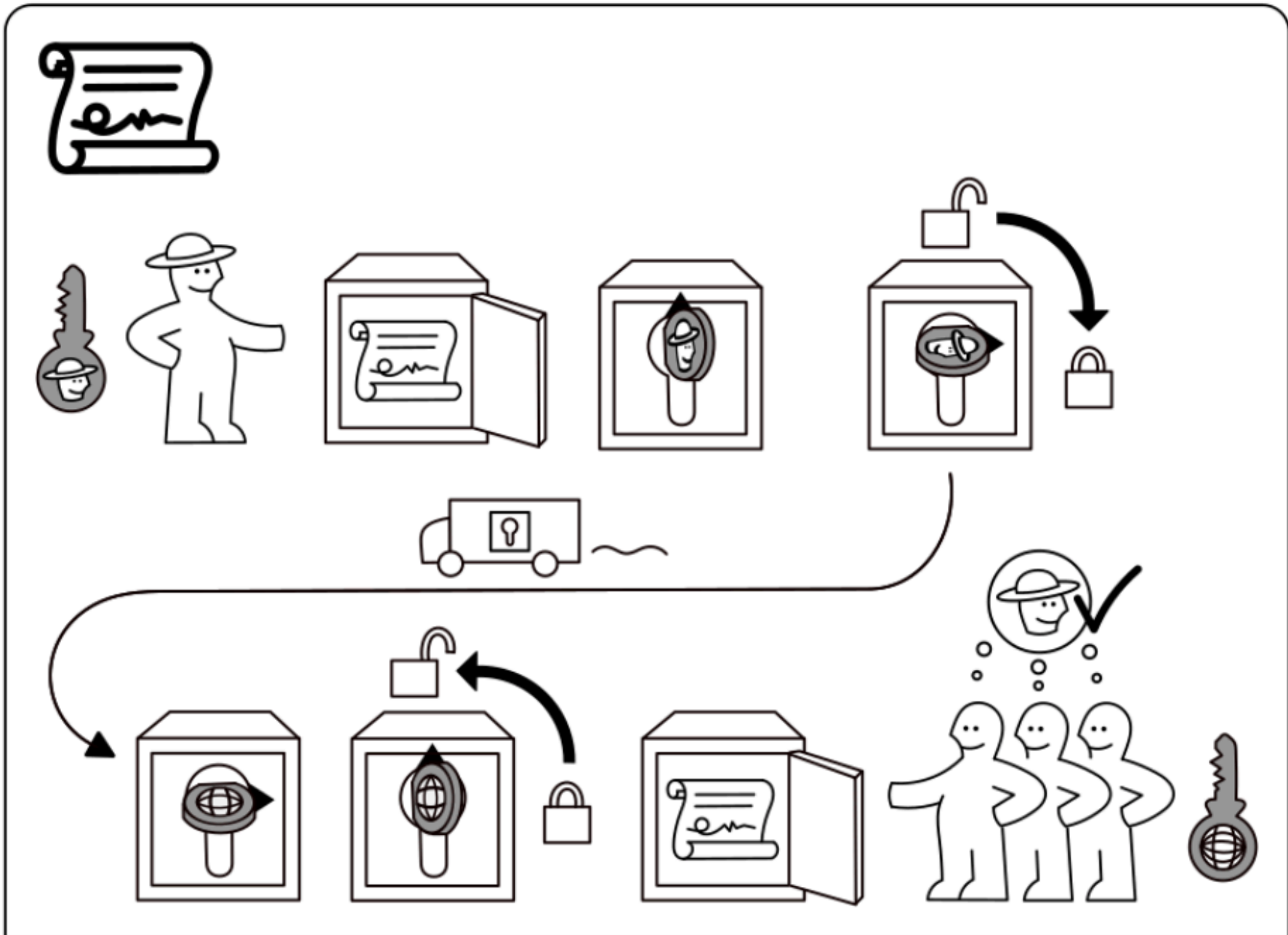
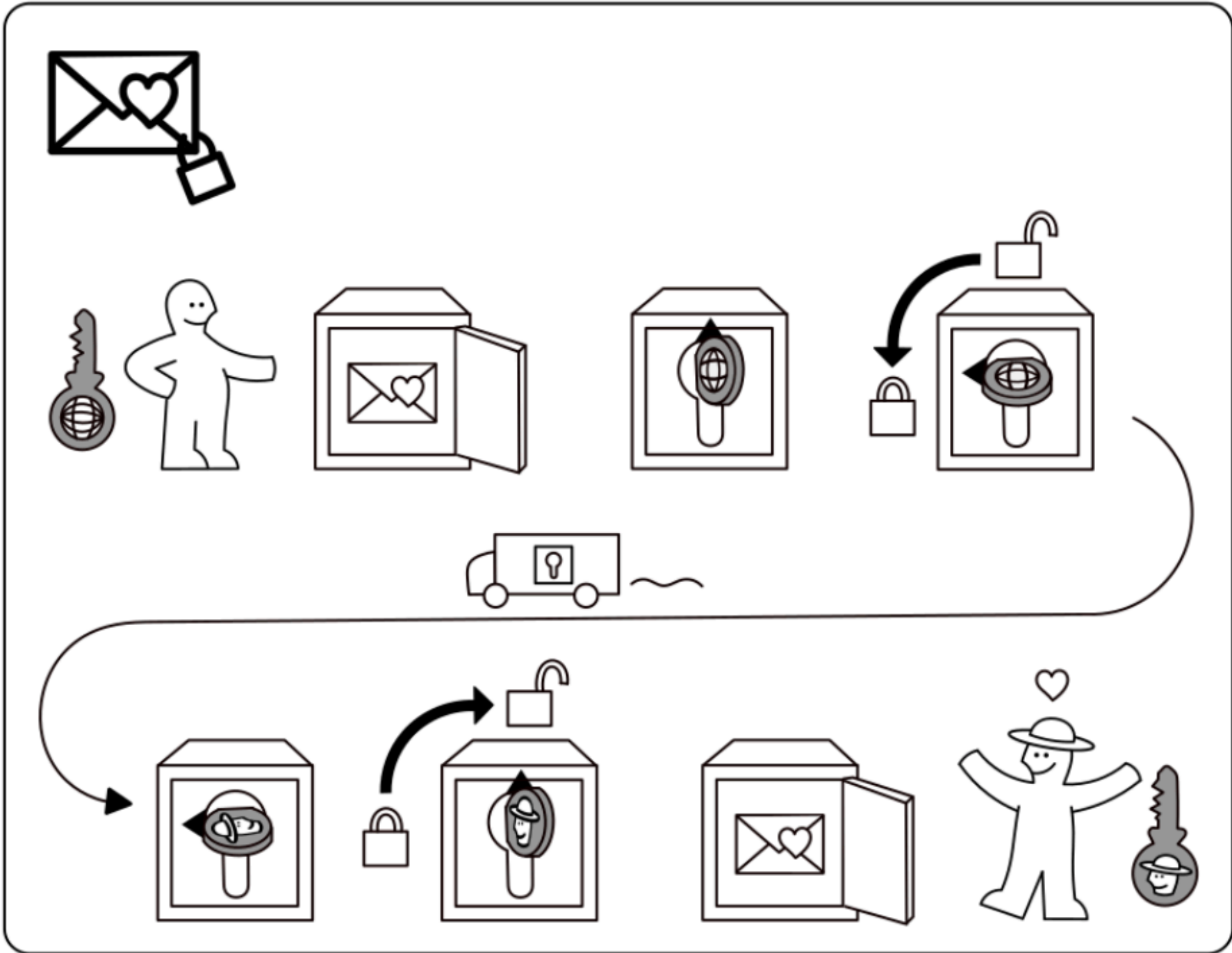
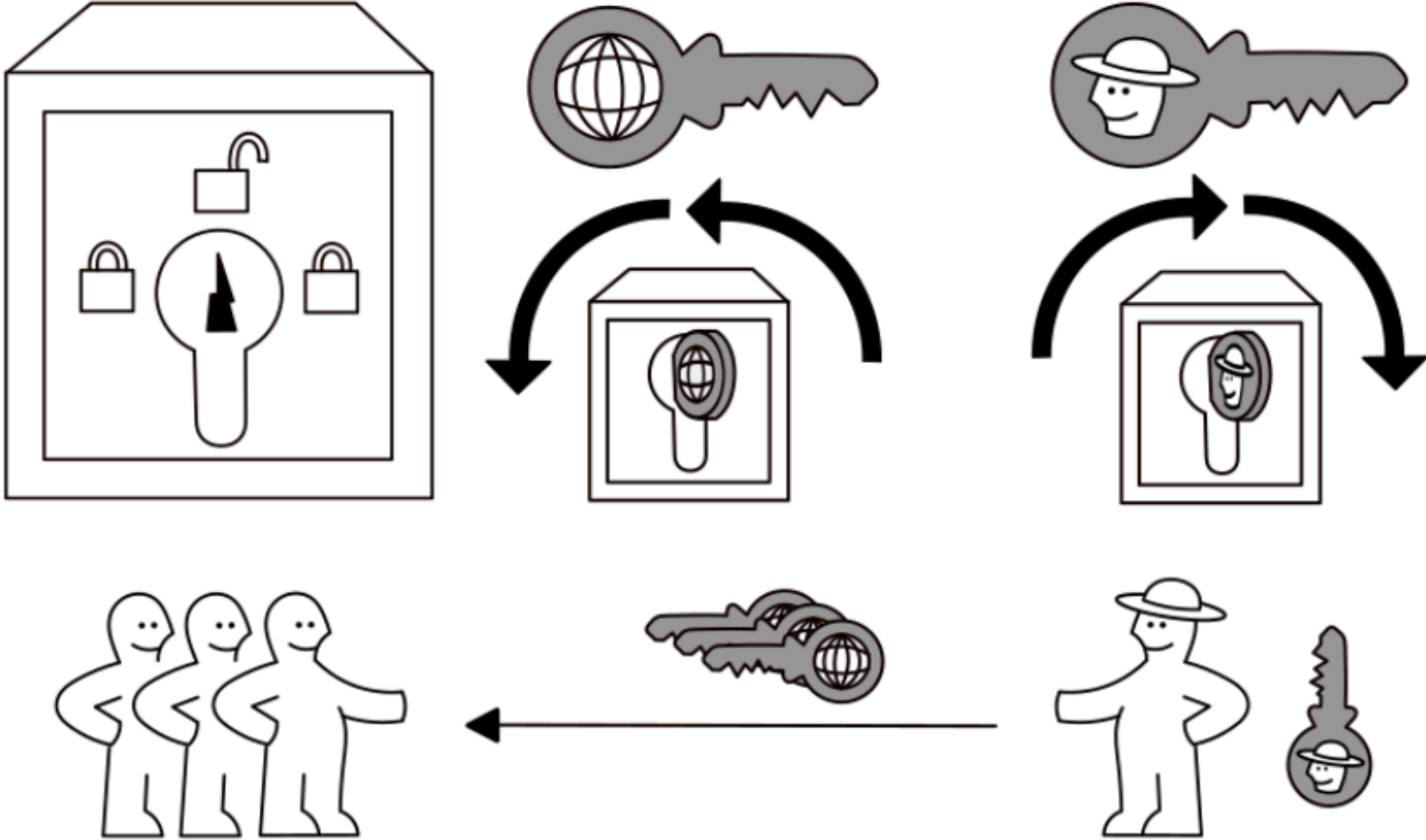


# Veränderte Ziele

- Deterministisch, d.h. dieselbe Nachricht ergibt immer den selben Wert.
- Hashwert lässt sich schnell berechnen.
- SEHR schwer eine Nachricht mit demselben Hashwert zu generieren.
- SEHR schwer zwei Nachrichten mit demselben Hashwert zu finden.
- Ein kleine Änderung in der Nachricht ändert das Ergebnis so stark, dass man aus den Hashwerten nicht auf ähnliche Nachrichten schließen kann.



# PUBLIK KEY KRYPTO



*Vielen Dank!*

*[s.fekete@tu-bs.de](mailto:s.fekete@tu-bs.de)*