Einbettung mit Trelliskodes

YAECS – Yet Another Error Correcting Code in Steganography

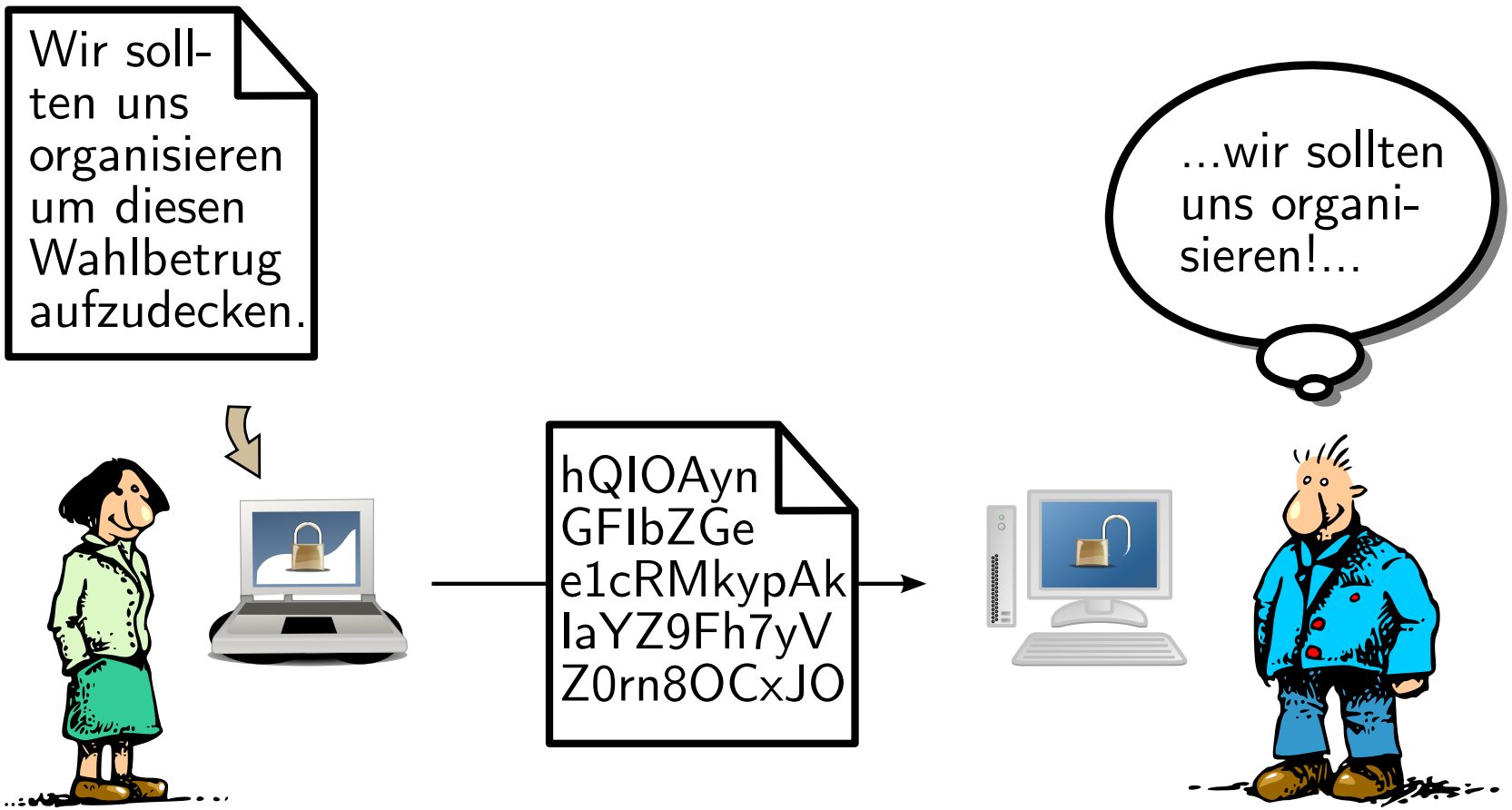
Benjamin Kellermann

Fakultät Informatik
Lehrstuhl Datenschutz und Datensicherheit

20.12.2007

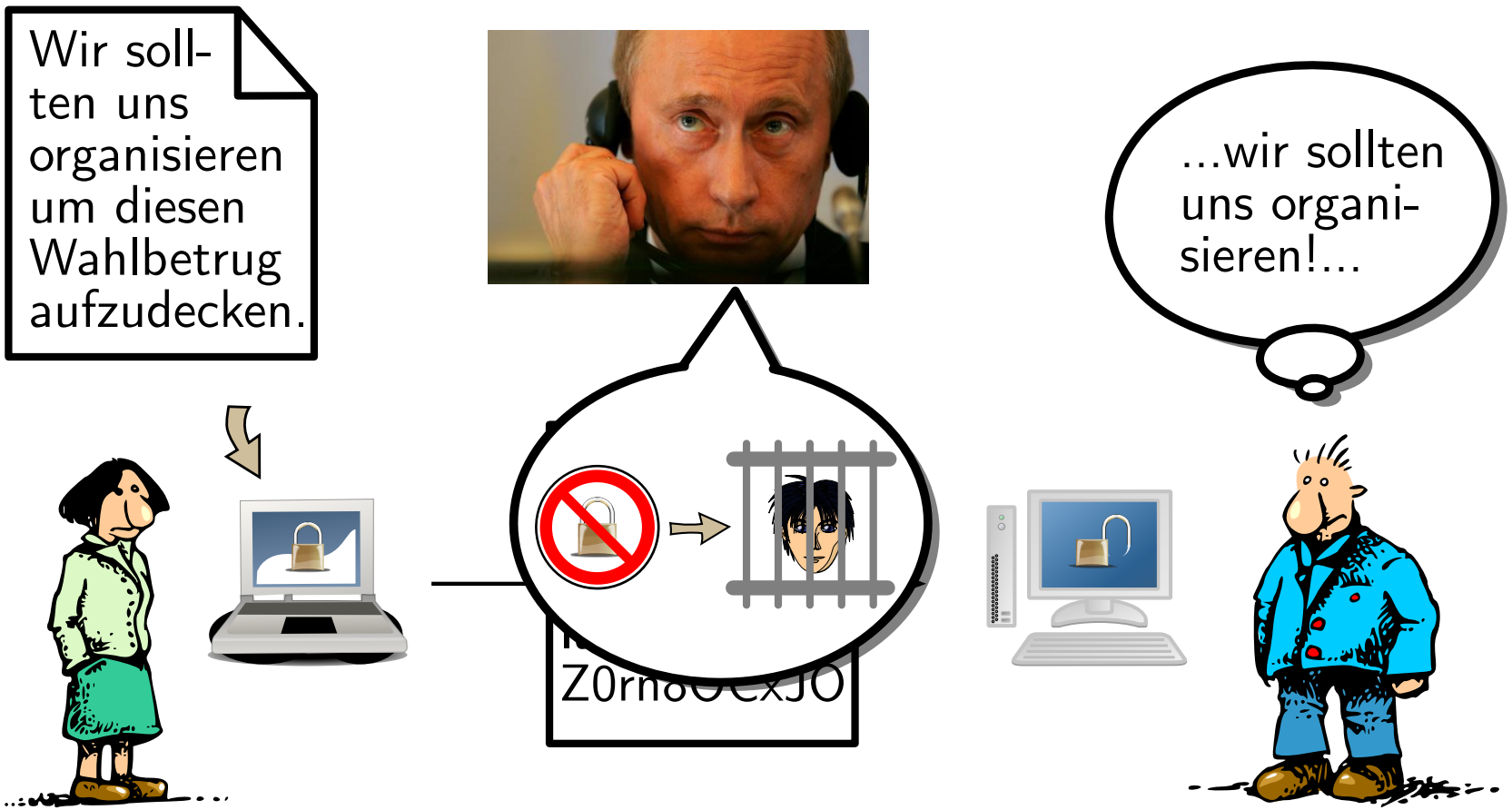
Gliederung

Steganographie?



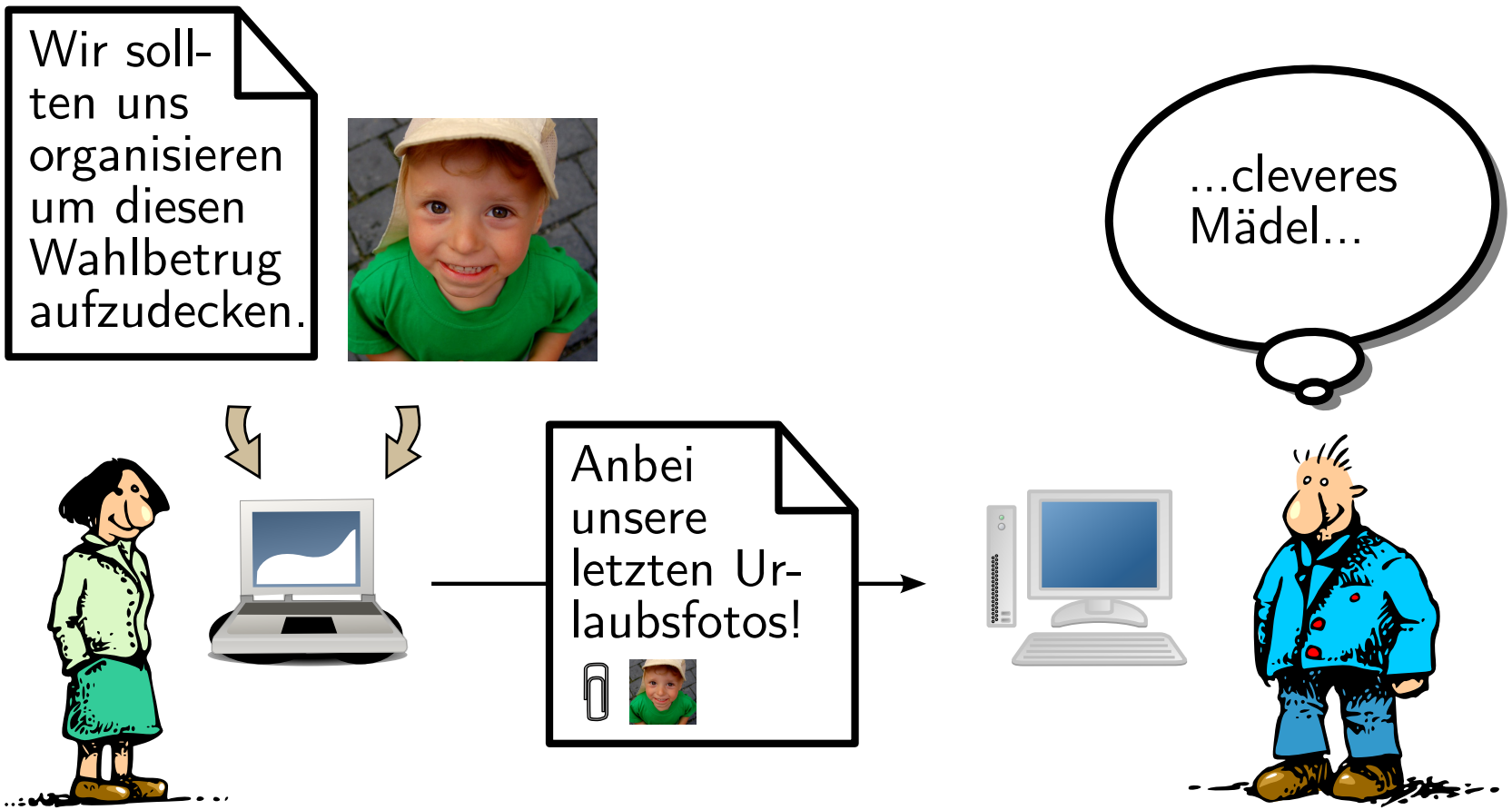
Kryptographie um Nachrichteninhalt zu verbergen

Steganographie?



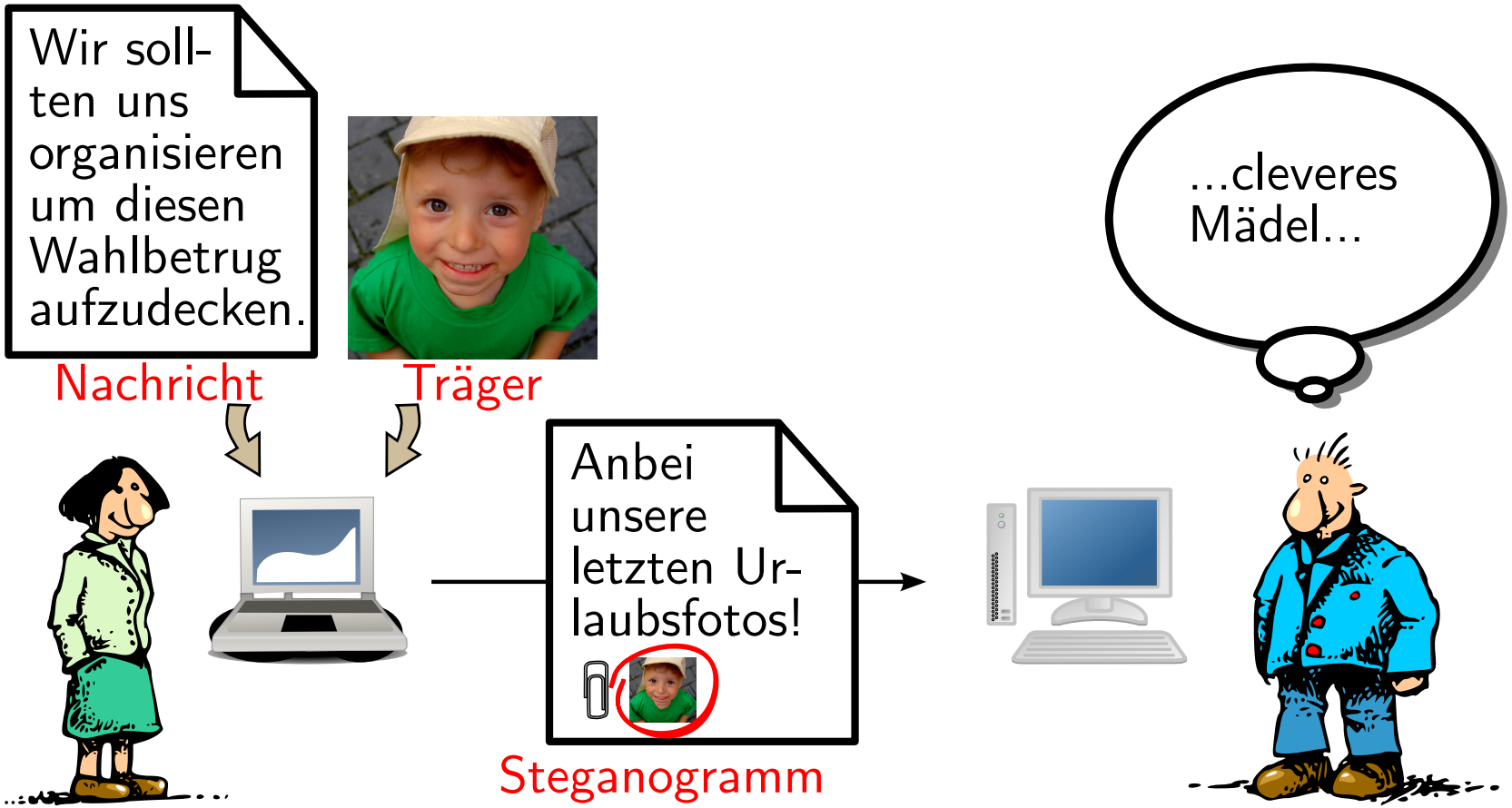
Kryptoverbote machen vertrauliche Kommunikation unmöglich

Steganographie?



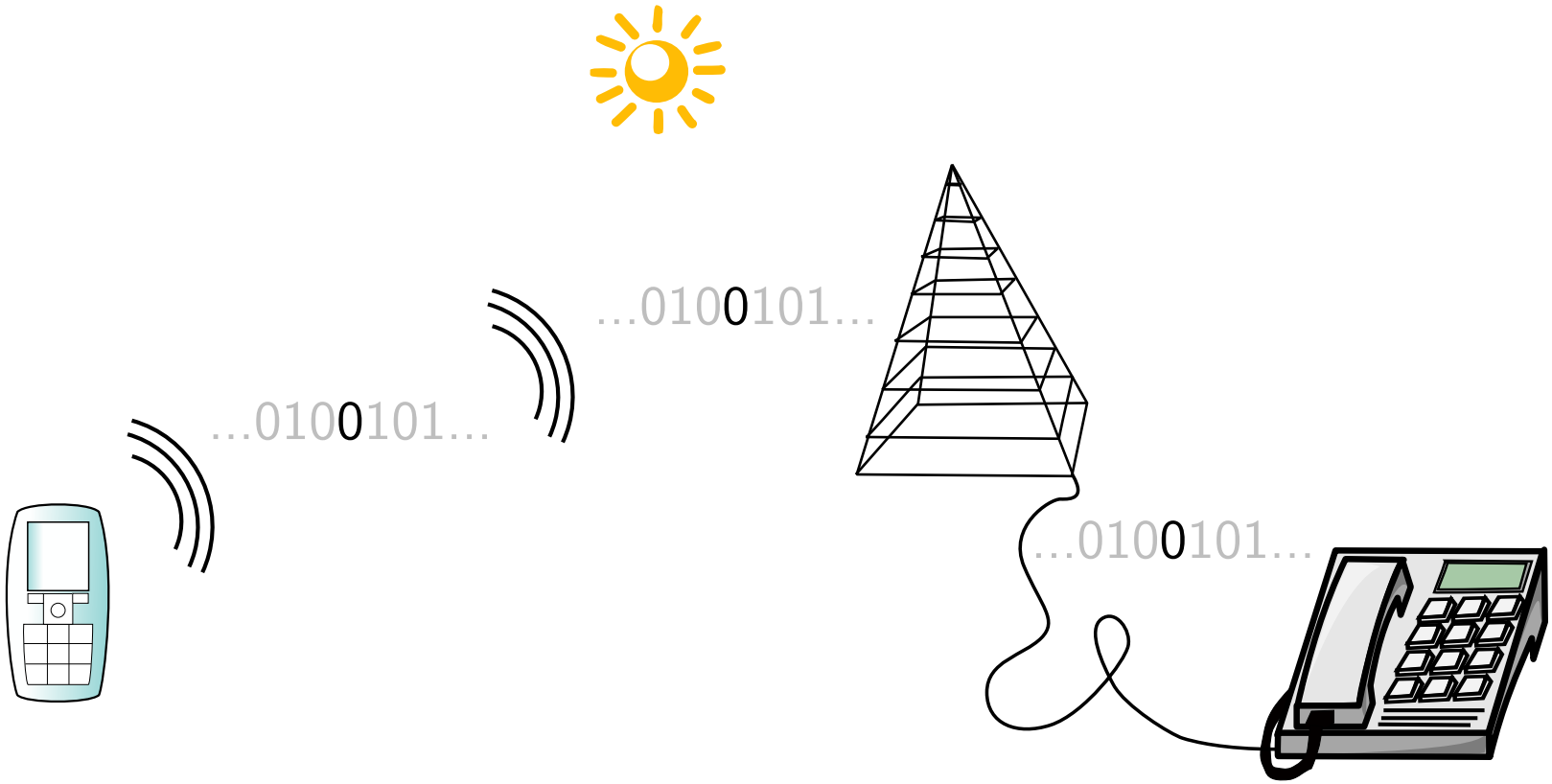
Mit Steganographie ist ein Kryptoverbot nicht durchsetzbar

Steganographie?



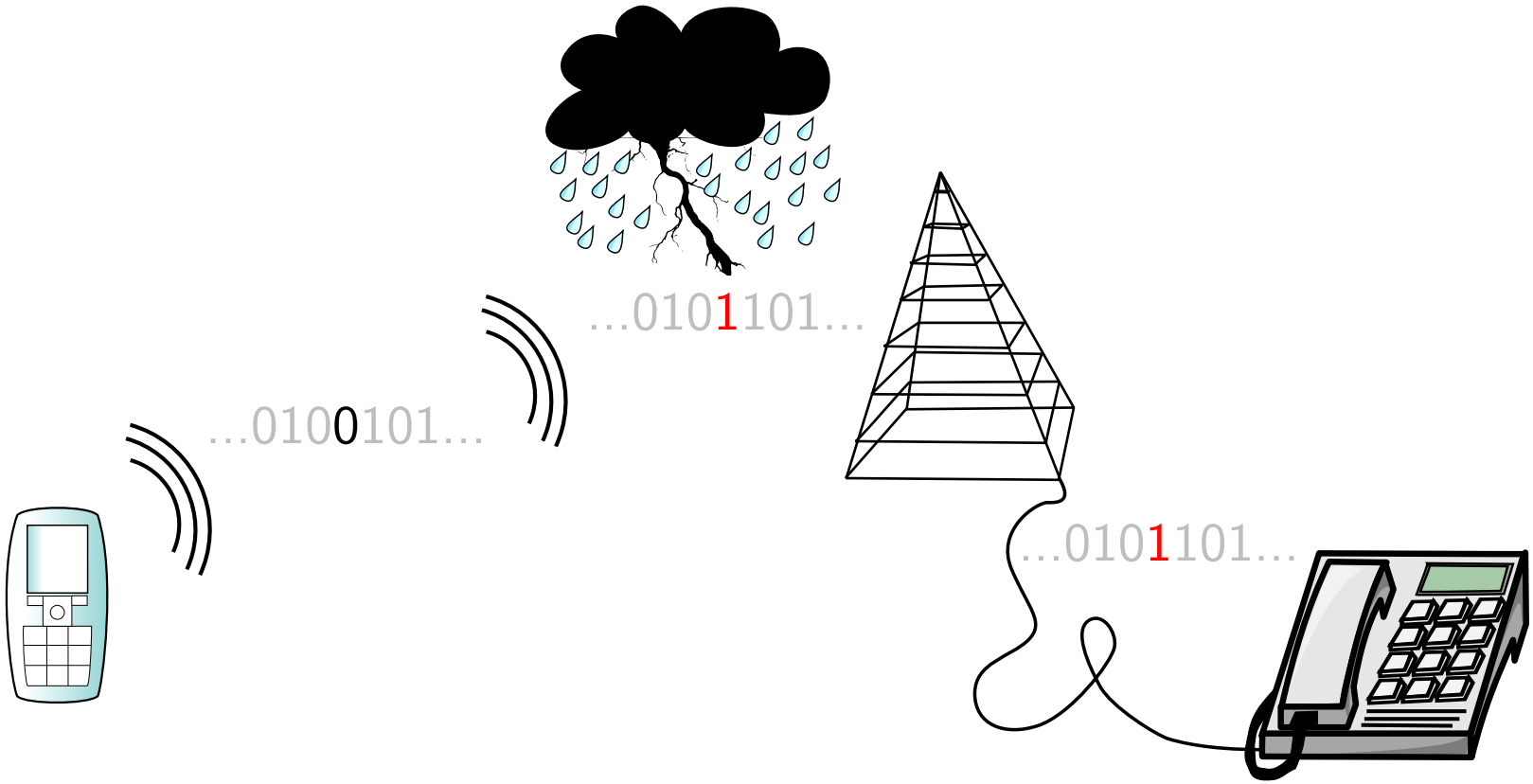
Terminologie

Kanalkodierung?



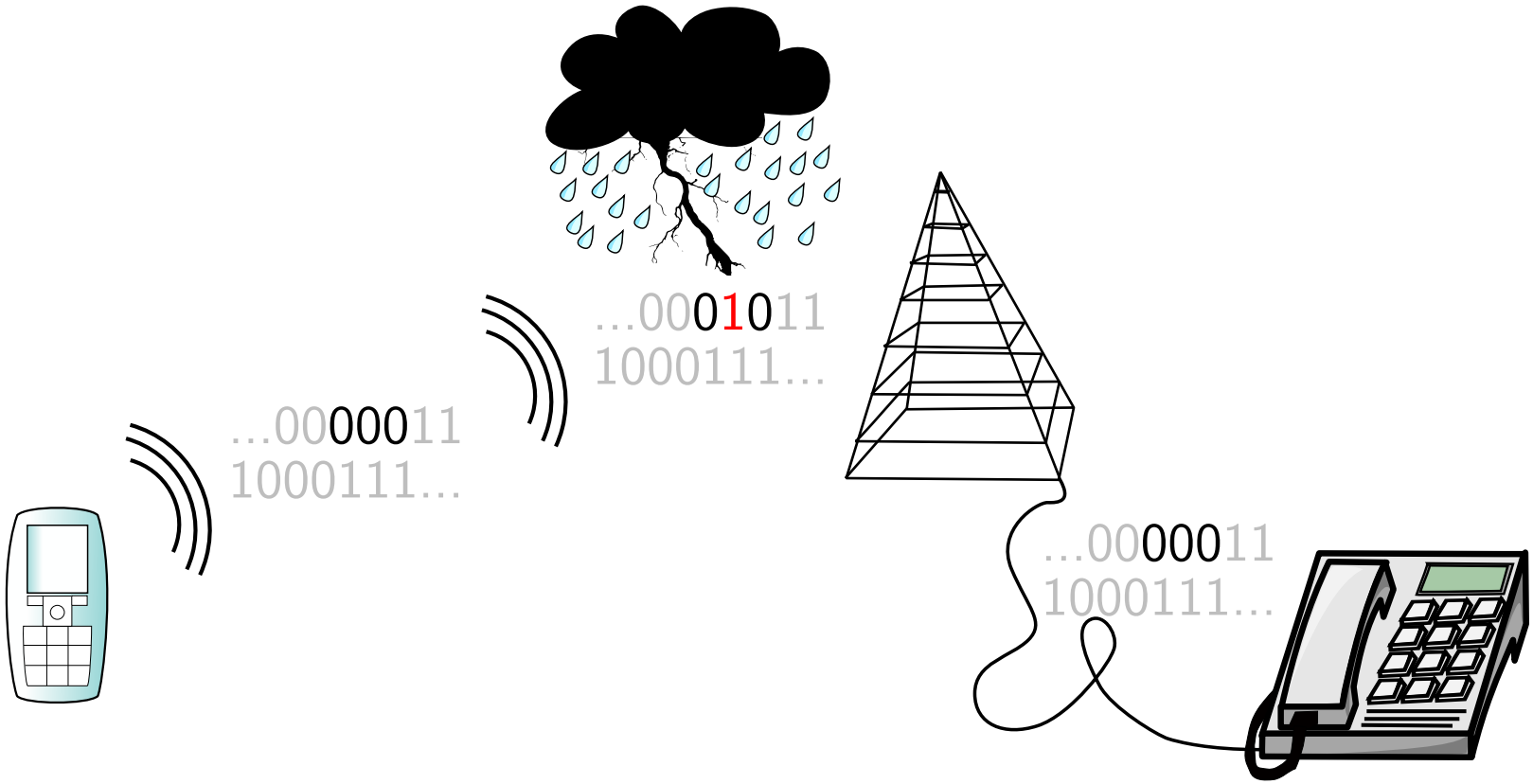
Normale Datenübertragung

Kanalkodierung?



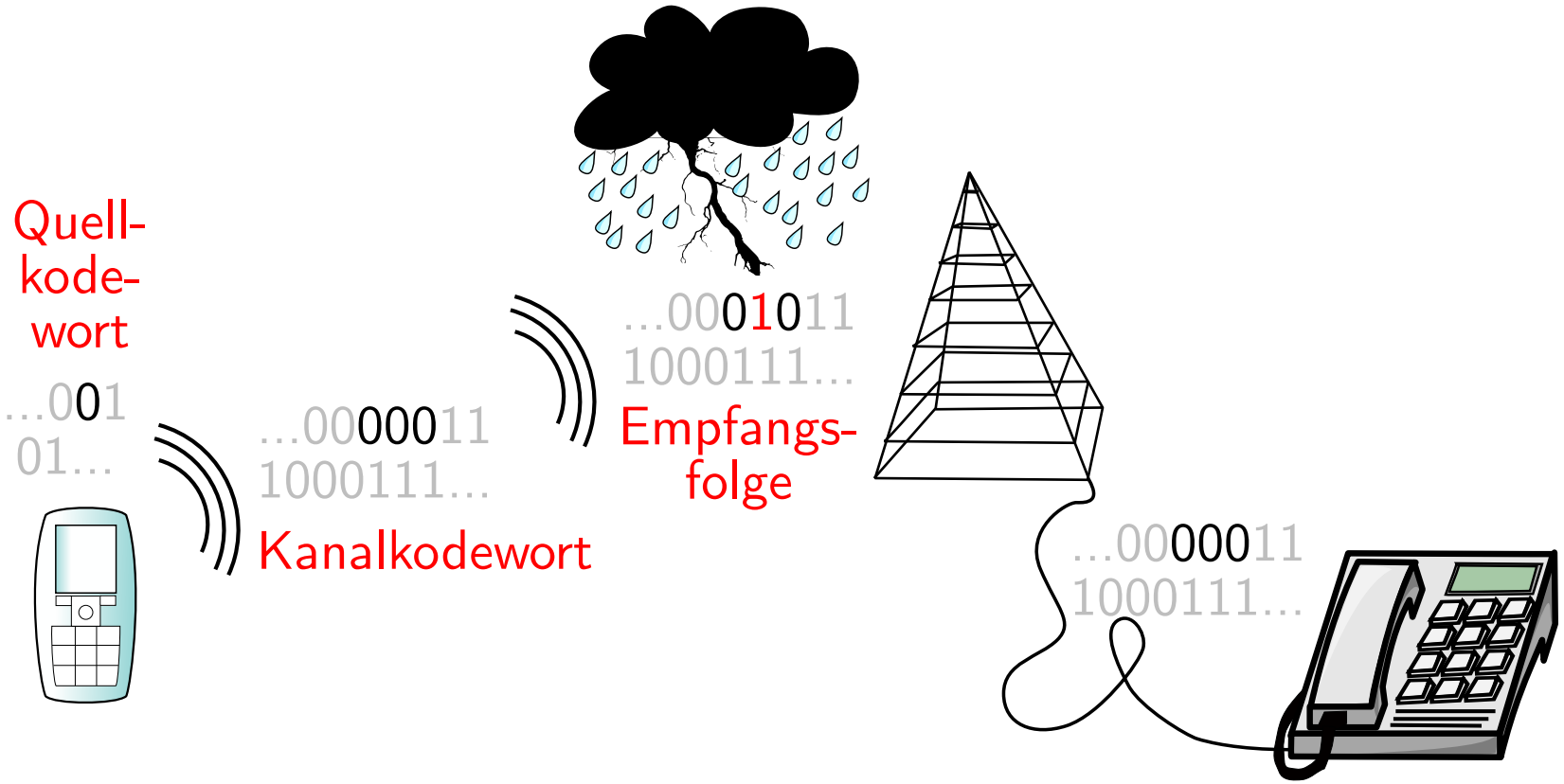
Daten werden u. a. durch Umwelteinflüsse verfälscht

Kanalkodierung?



durch Hinzufügen von Redundanz kann Fehler korrigiert werden

Kanalkodierung?



Terminologie

Worum geht es überhaupt?

- erstes Schema 1998 von Ron Crandall vorgestellt (Hamming- und Golaykodes)
- Kanalkodierung nutzen um weniger Bits im Träger zu ändern
- weitere Methoden von Winkler, Schönfeld und Fridrich

wichtige Kenngrößen

- Einbettungsrate $\alpha = \frac{\text{Nutzstellen}}{\text{benötigte Stellen}}$
- Einbettungseffizienz $e = \frac{\text{Nutzstellen}}{\text{durchschnittlich gekippte Bits}}$

Worum geht es überhaupt?

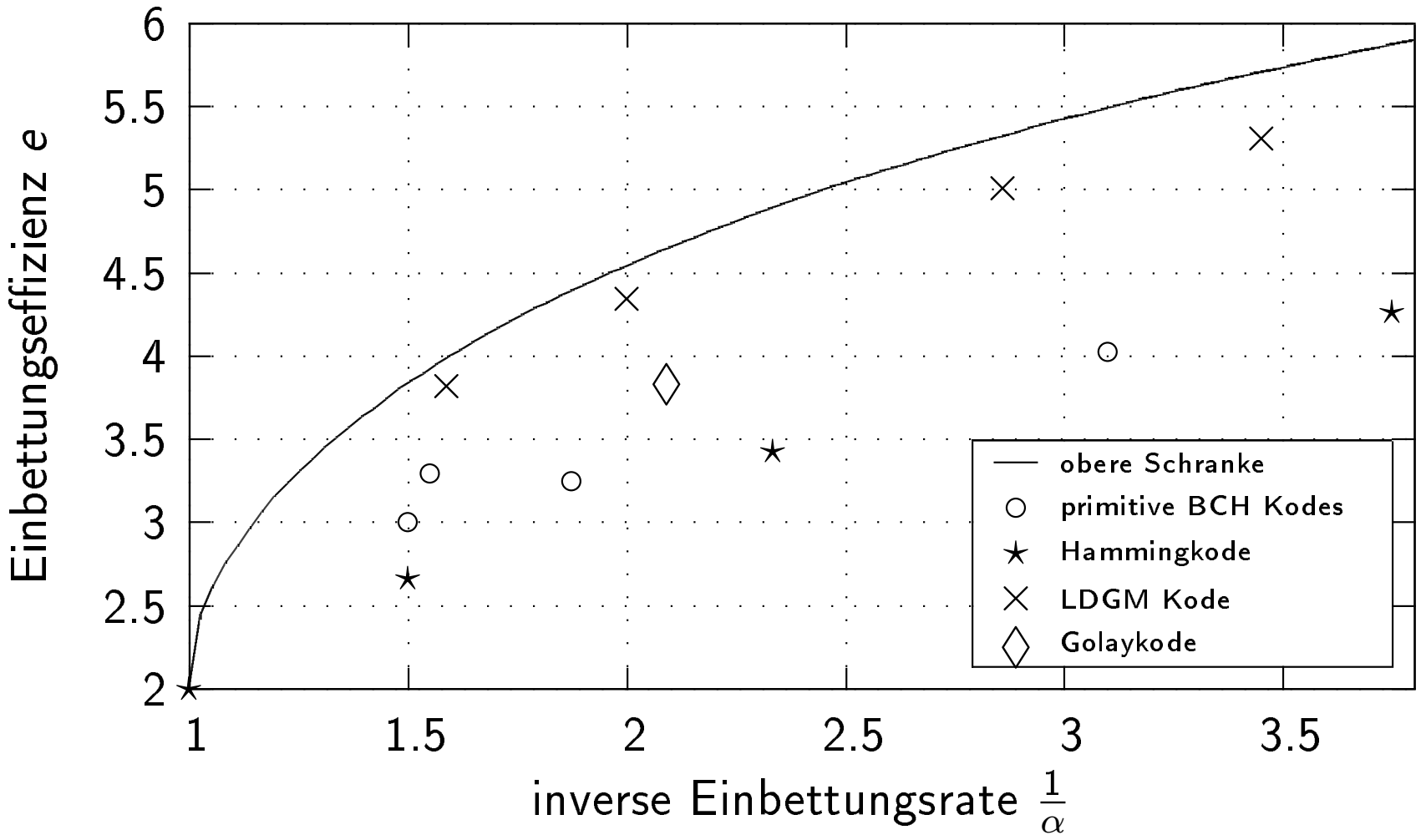
- erstes Schema 1998 von Ron Crandall vorgestellt (Hamming- und Golaykodes)

  Bsp: $(7,4)$-Hammingkode $\Longrightarrow$ 3 Bit in 7 Bit einbetten mit max. 1 Änderung

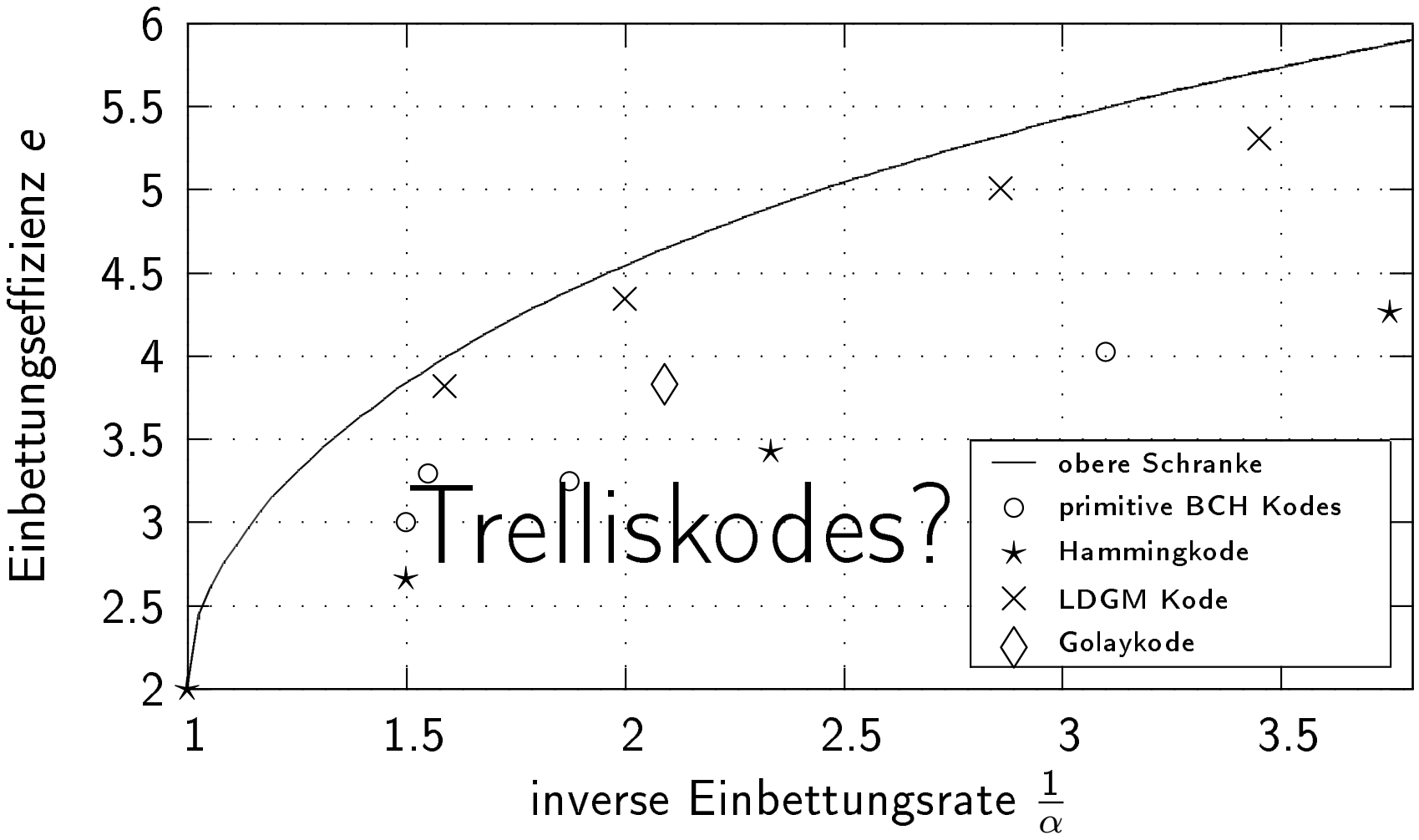
wichtige Kenngrößen

- Einbettungsrate $\alpha = \frac{\text{Nutzstellen}}{\text{benötigte Stellen}} = \frac{3}{7}$
- Einbettungseffizienz $e = \frac{\text{Nutzstellen}}{\text{durchschnittlich gekippte Bits}} = \frac{3}{\frac{1 \cdot 7 + 0 \cdot 1}{8}}$

Bisherige Methoden im Überblick



Bisherige Methoden im Überblick



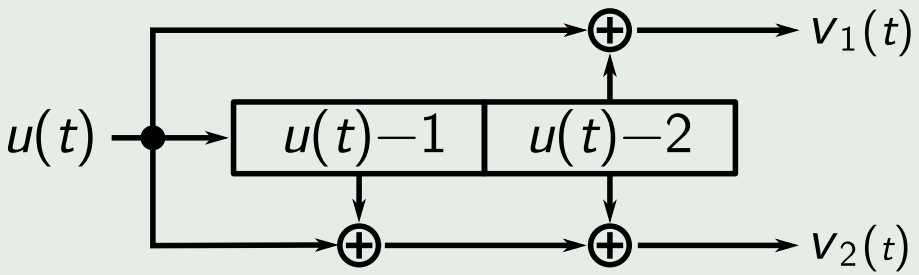
Darstellungsformen

Beispiel

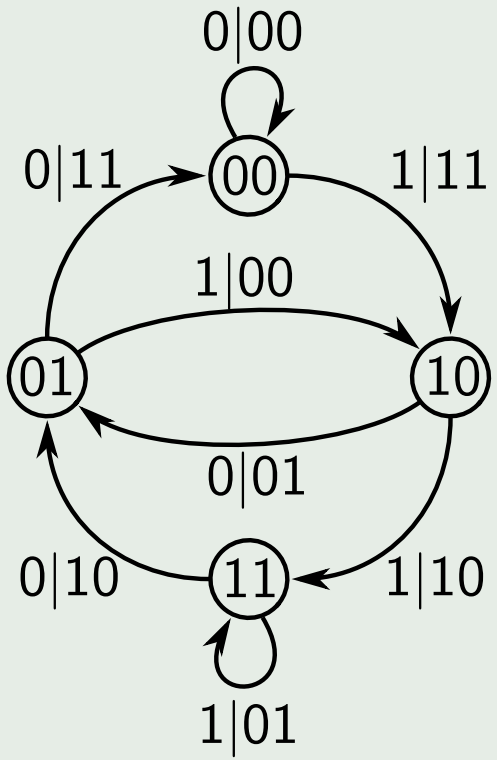
Faltungskode mit der Generatormatrix

$$G = \begin{pmatrix} 101 \\ 111 \end{pmatrix} = (5_8, 7_8).$$

Darstellung als Schieberegister



Darstellung als Zustandsautomat



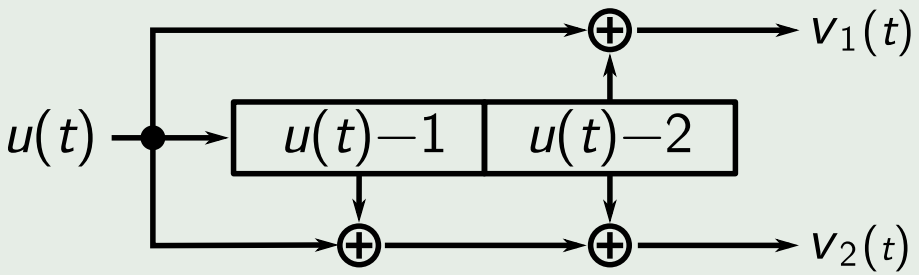
Darstellungsformen

Beispiel

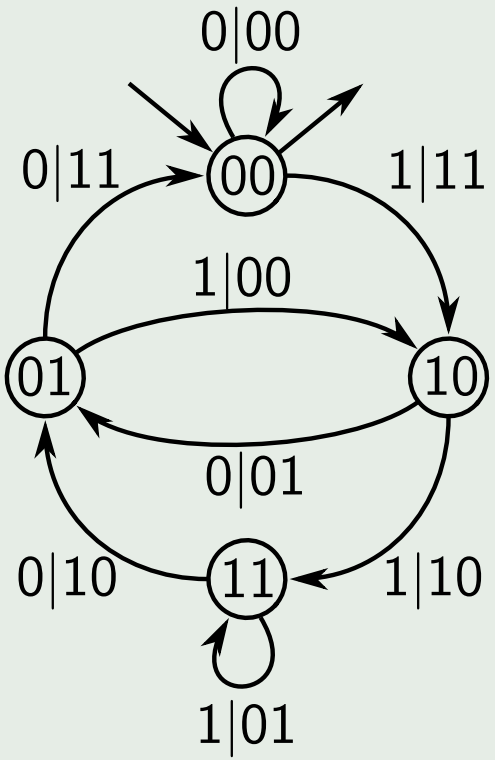
Faltungskode mit der Generatormatrix

$$G = \begin{pmatrix} 101 \\ 111 \end{pmatrix} = (5_8, 7_8).$$

Darstellung als Schieberegister

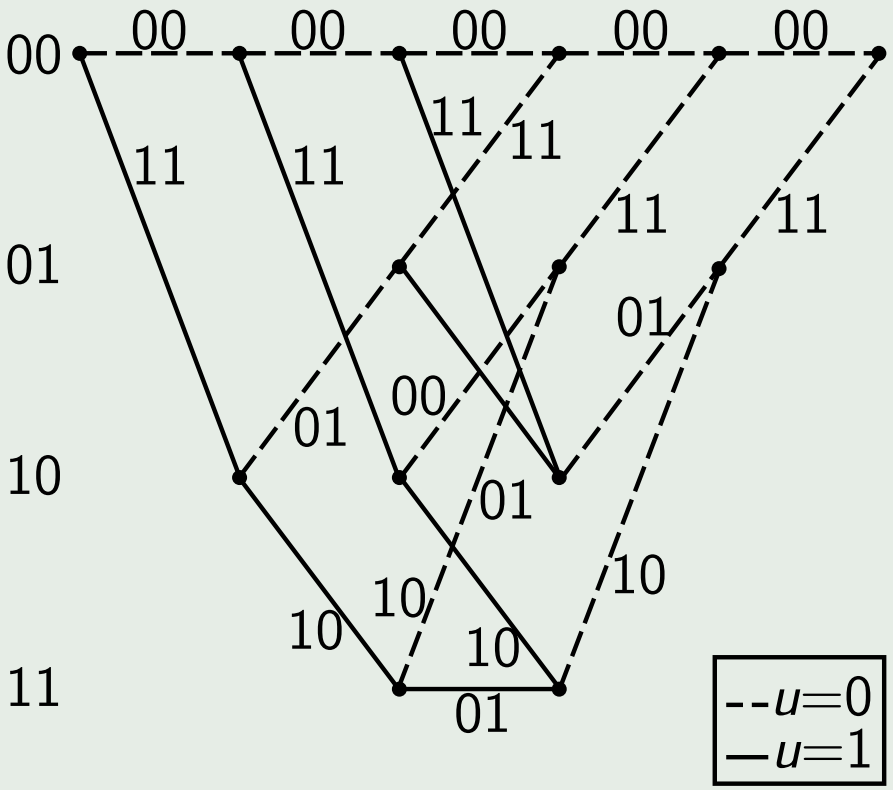


Darstellung als Zustandsautomat

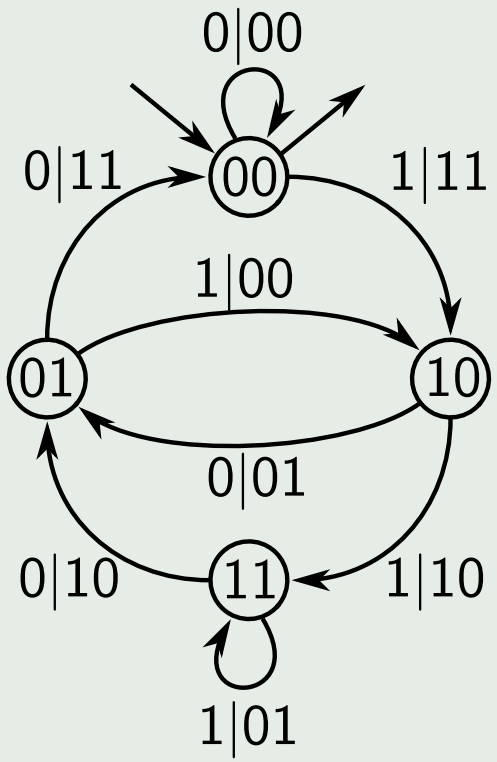


Darstellungsformen

Darstellung als Trellisdiagramm

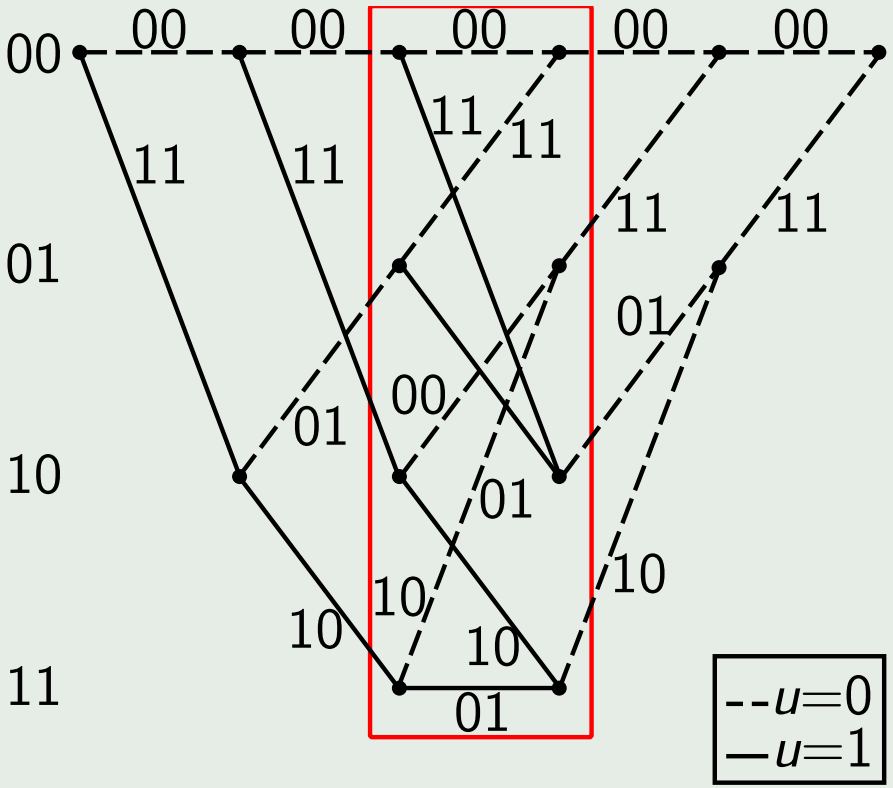


Darstellung als Zustandsautomat

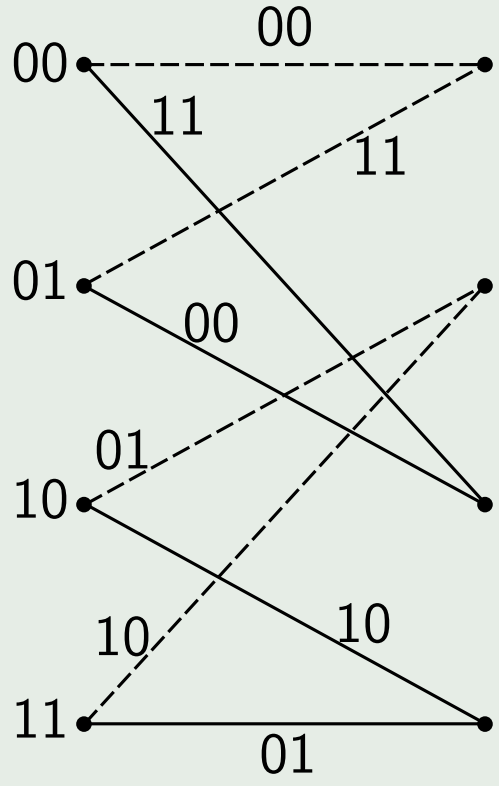


Darstellungsformen

Darstellung als Trellisdiagramm



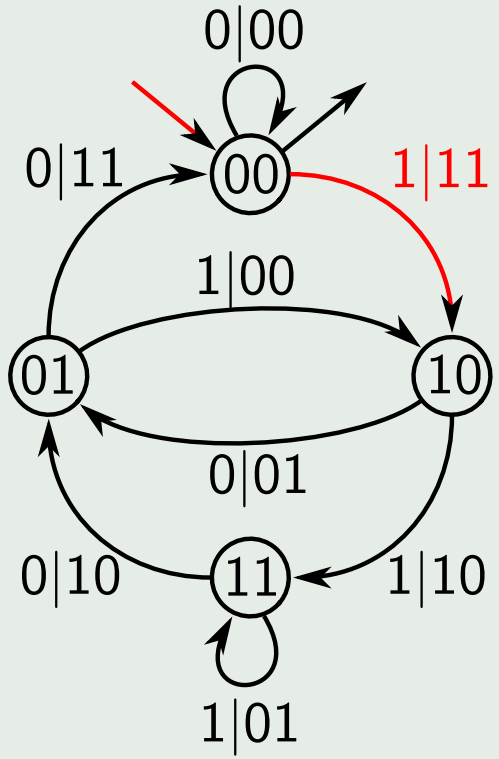
Darstellung als verkürztes Trellis



Kodierung mit Faltungskodes

Mit Zustandsautomat

a^*	1	0	1

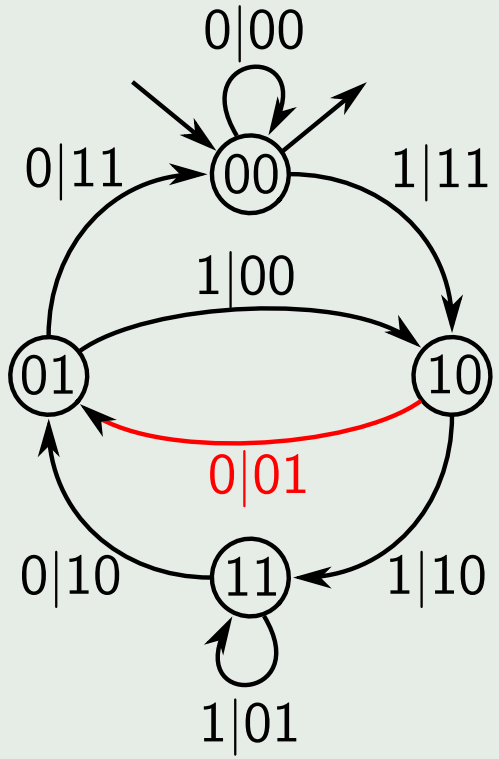


a	11	01	00	01	11

Kodierung mit Faltungskodes

Mit Zustandsautomat

$a*$	1	0	1

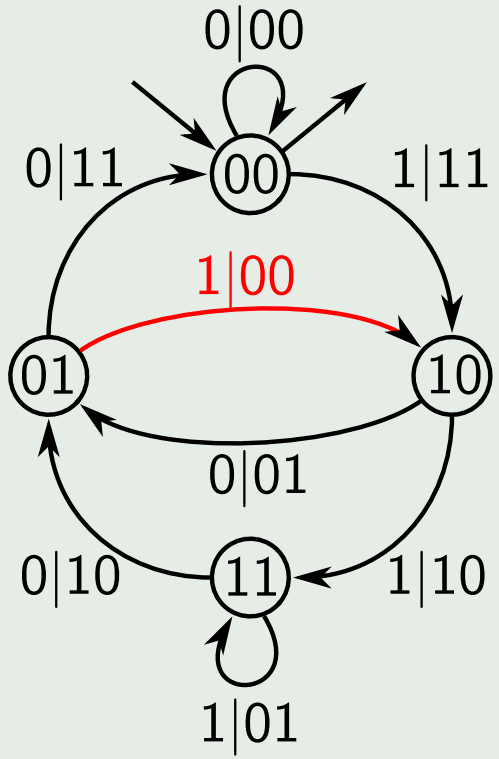


a	11	01	00	01	11

Kodierung mit Faltungskodes

Mit Zustandsautomat

$a*$	1	0	1

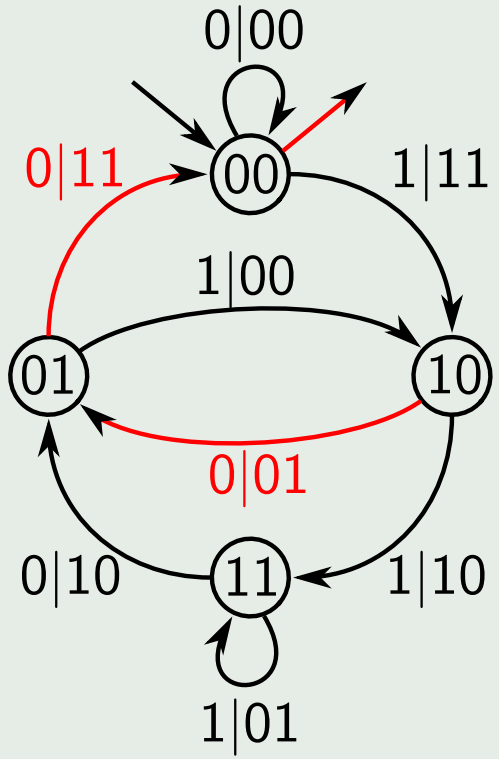


a	11	01	00	01	11

Kodierung mit Faltungskodes

Mit Zustandsautomat

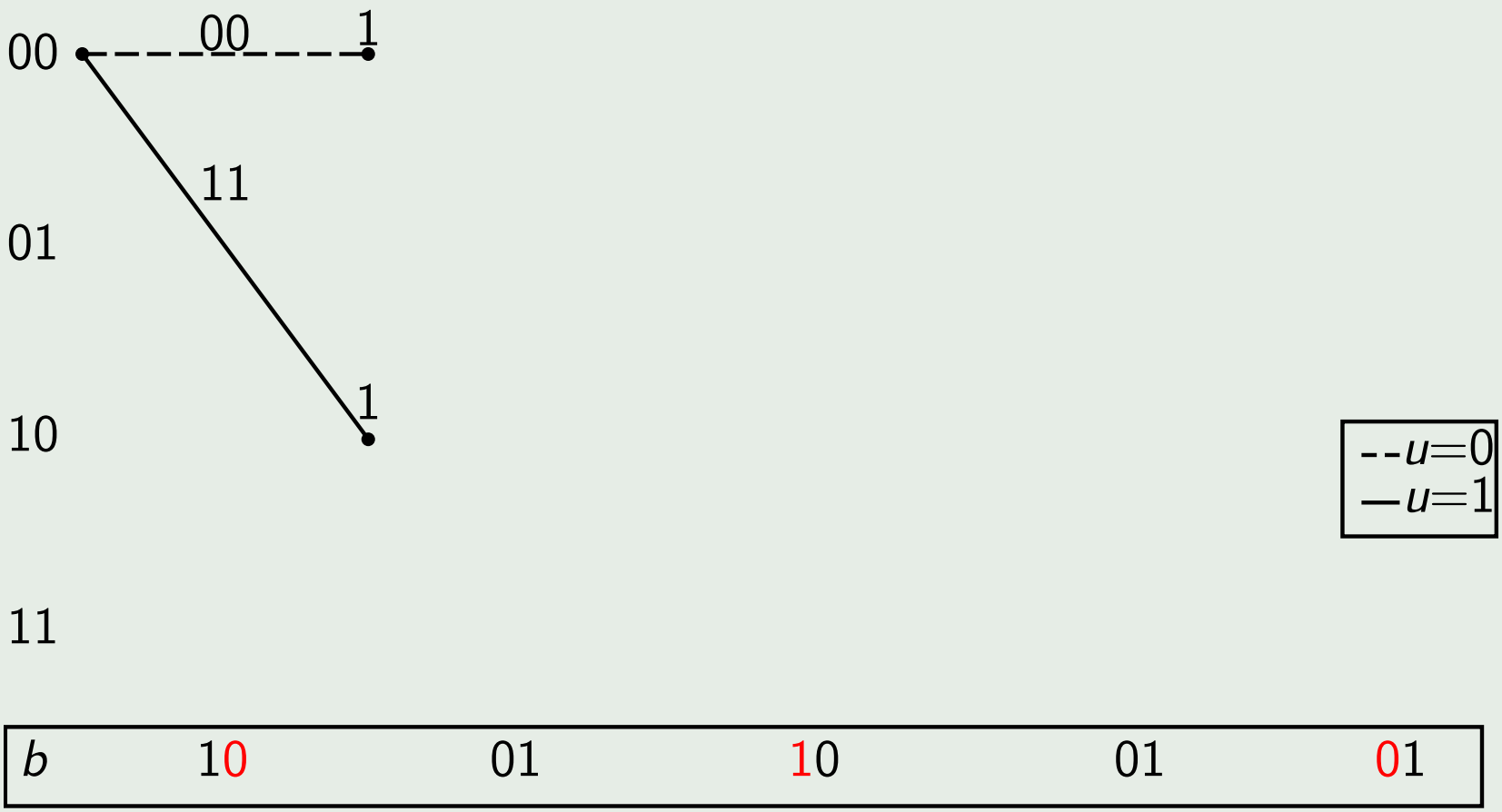
$a*$	1	0	1



a	11	01	00	01	11

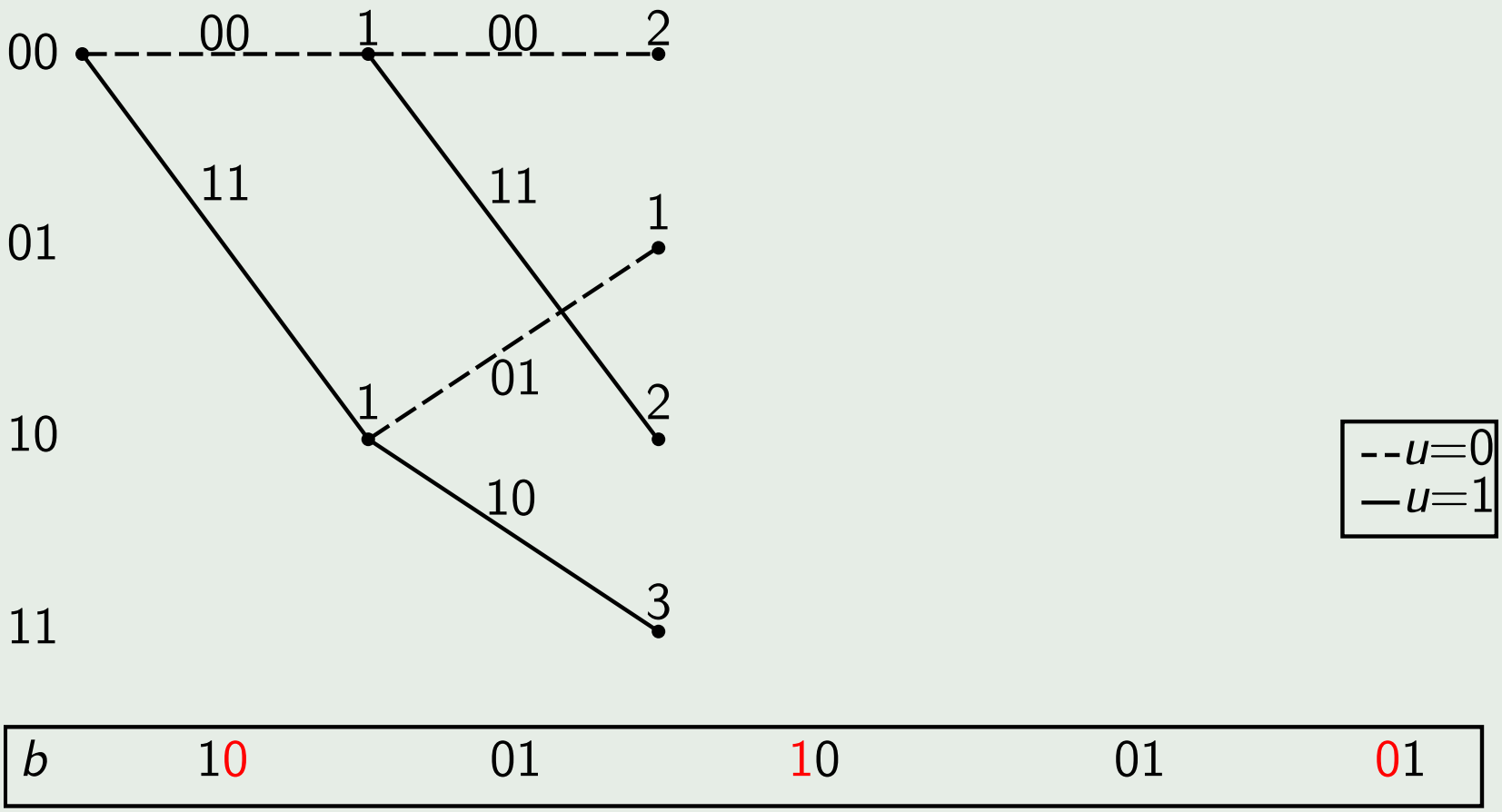
Dekodierung mit Faltungskodes

Algorithmus von Viterbi



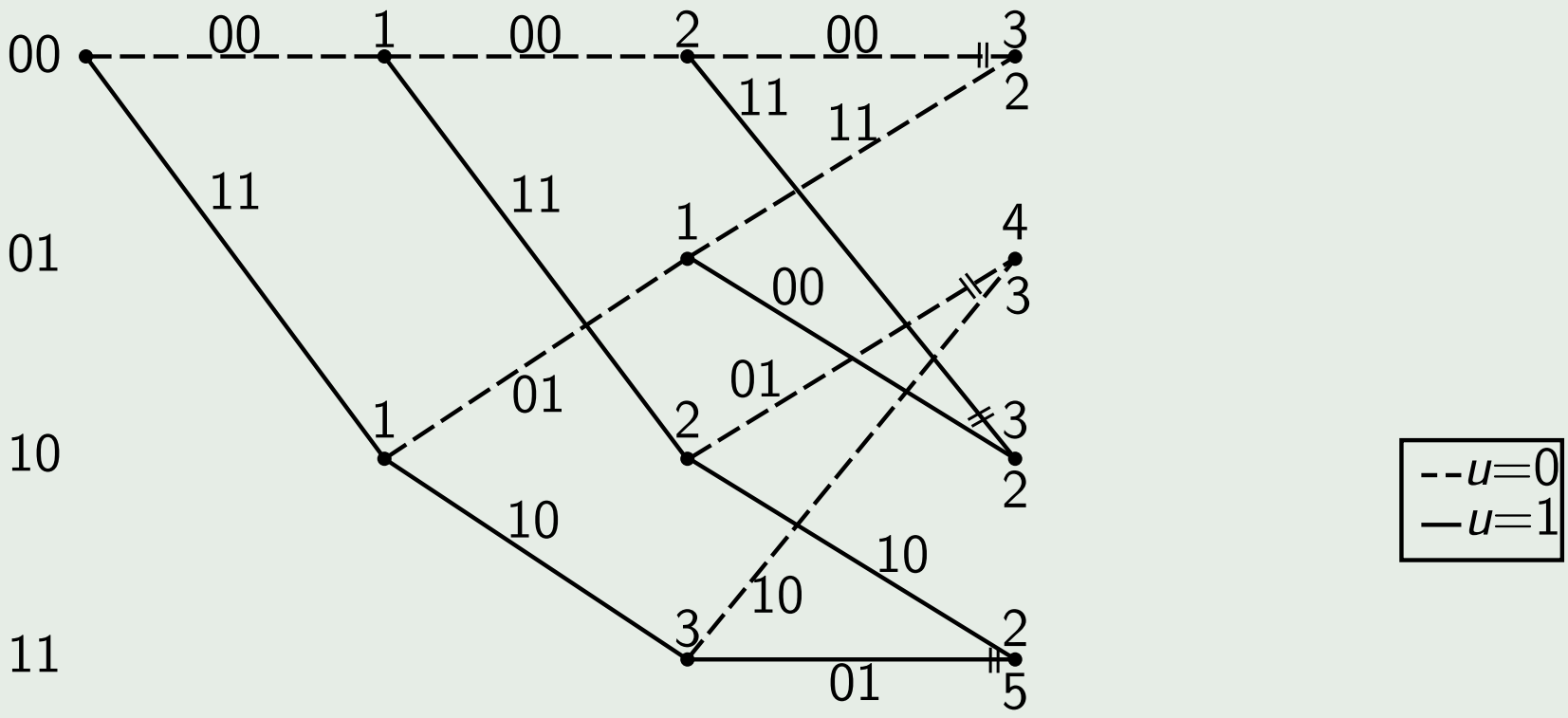
Dekodierung mit Faltungskodes

Algorithmus von Viterbi



Dekodierung mit Faltungskodes

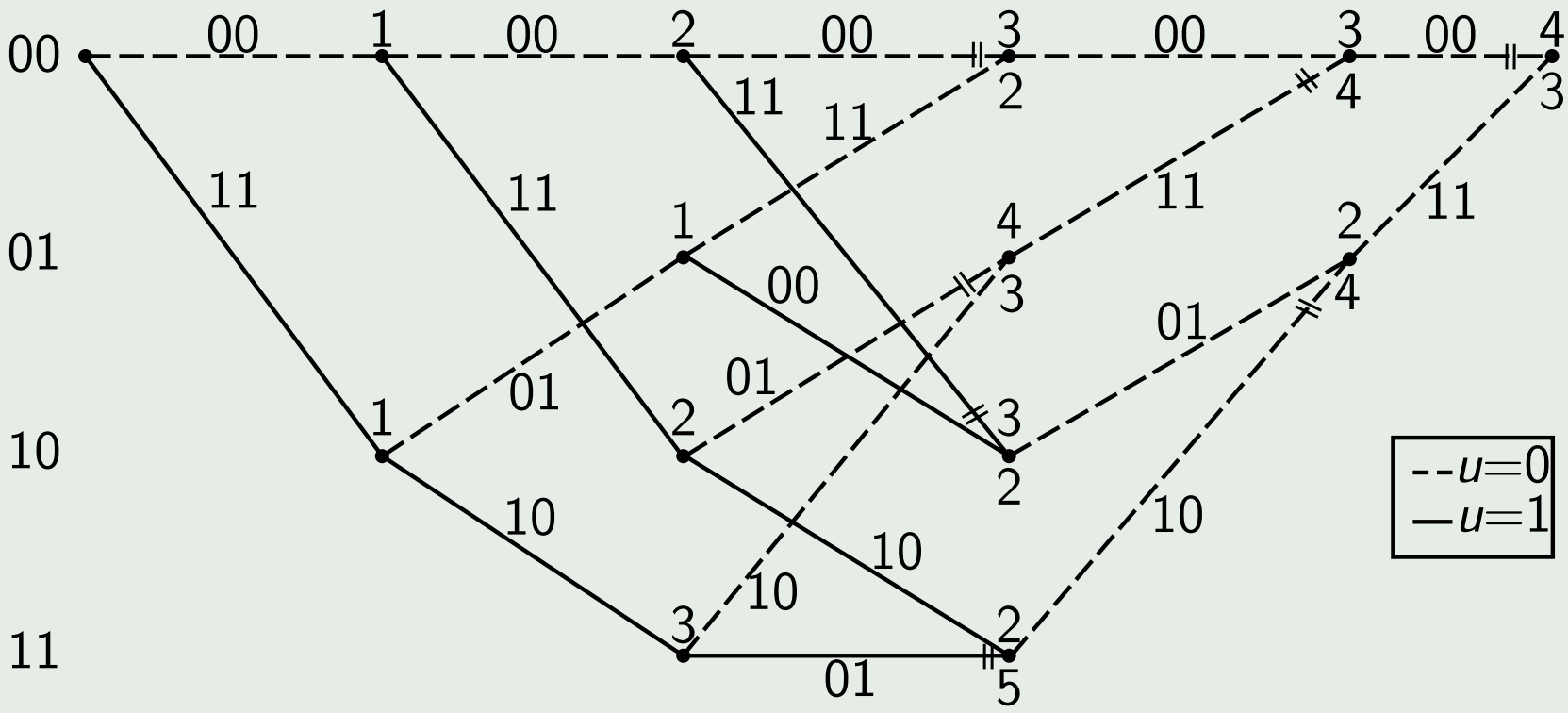
Algorithmus von Viterbi



b	10	01	10	01	01

Dekodierung mit Faltungskodes

Algorithmus von Viterbi



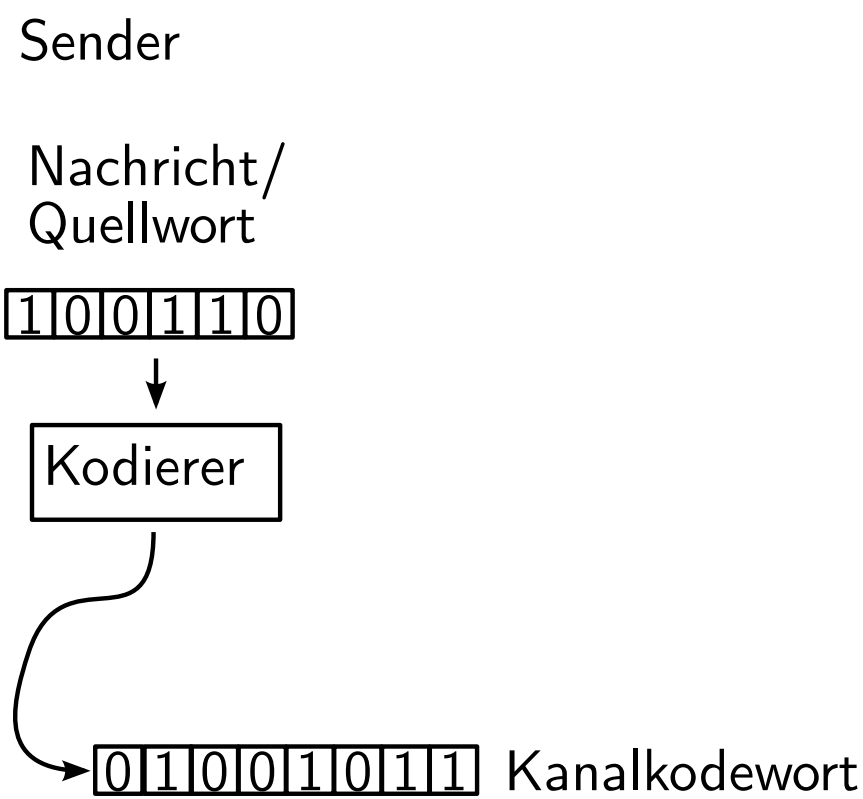
Problem

- klassische Kodes verwenden Syndromeinbettung:

$$m = s = H \cdot c^T$$

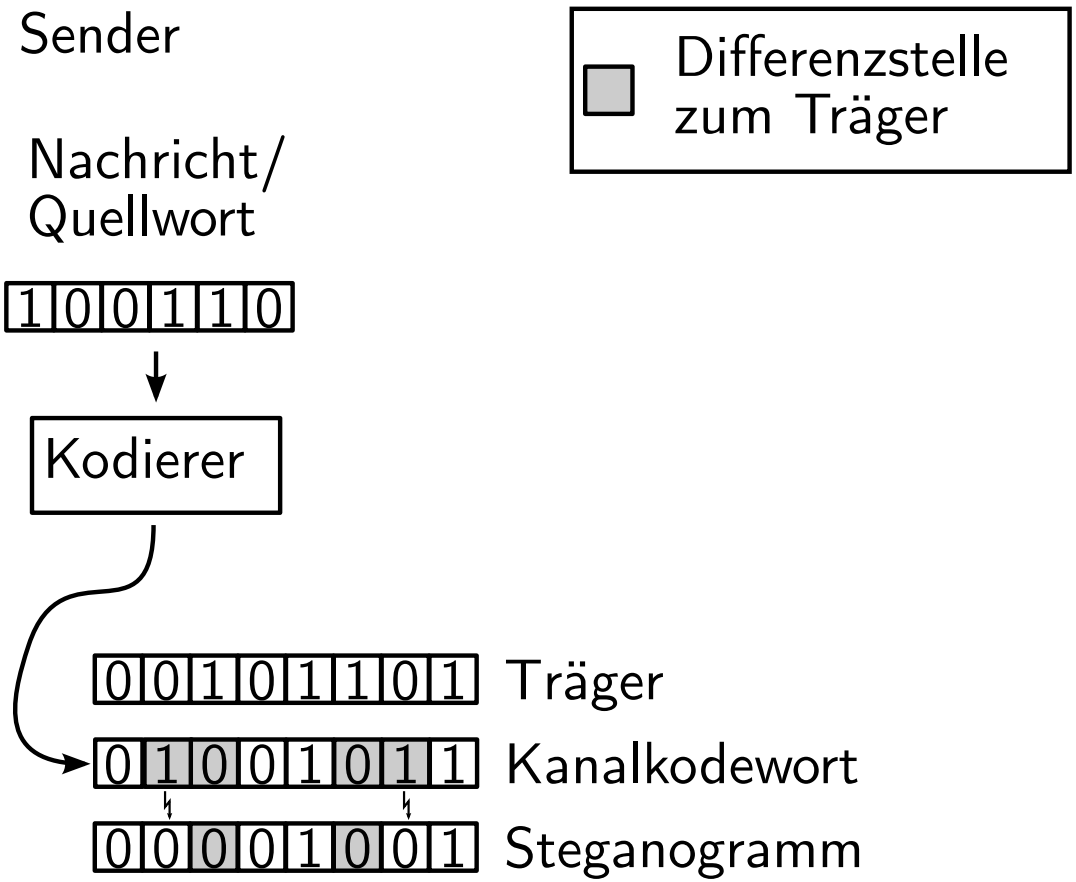
- mangels Syndrom nicht auf Trelliskodes erweiterbar

Naive Methode



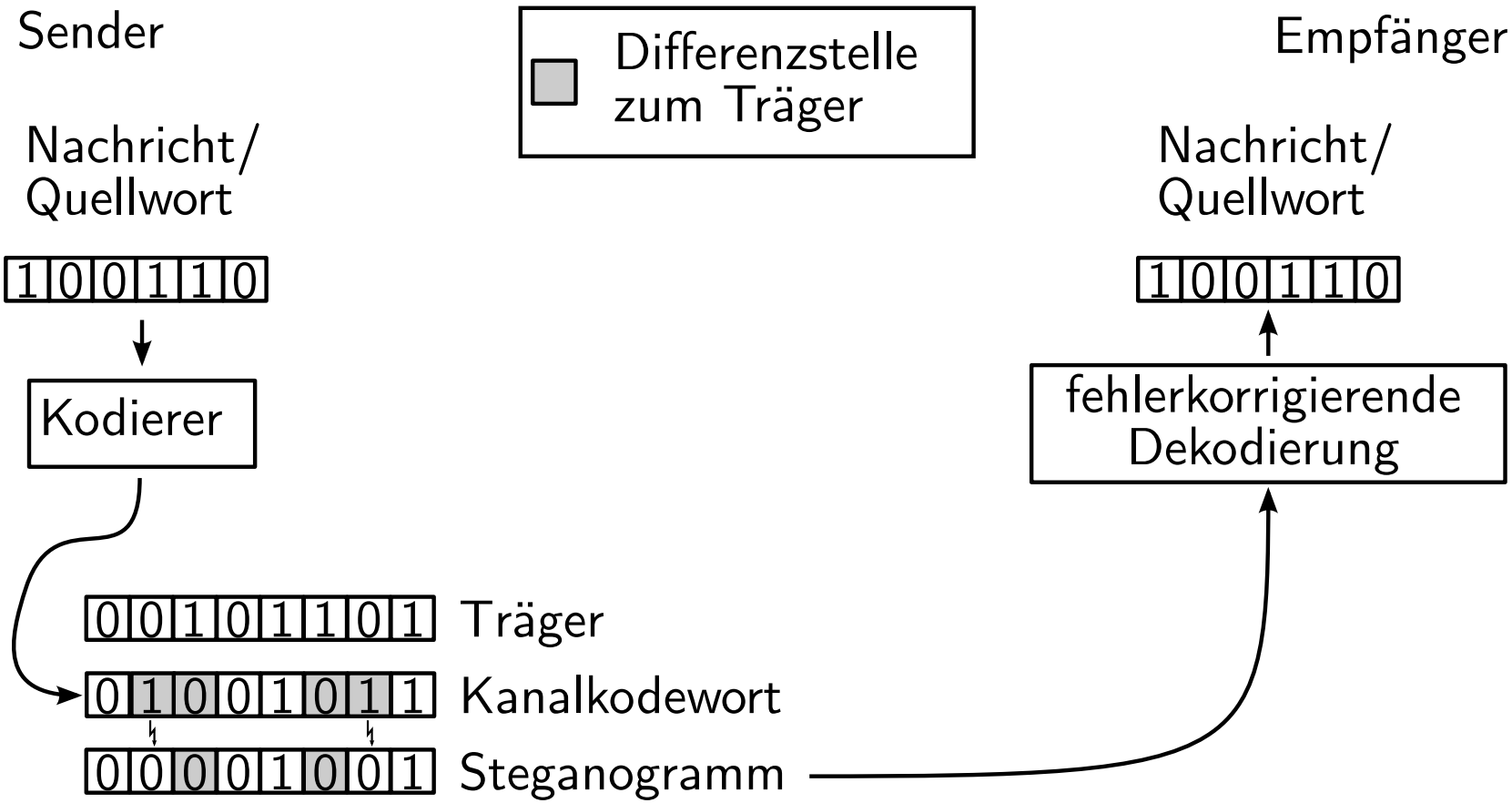
Nachricht wird mit Kodierer kodiert

Naive Methode



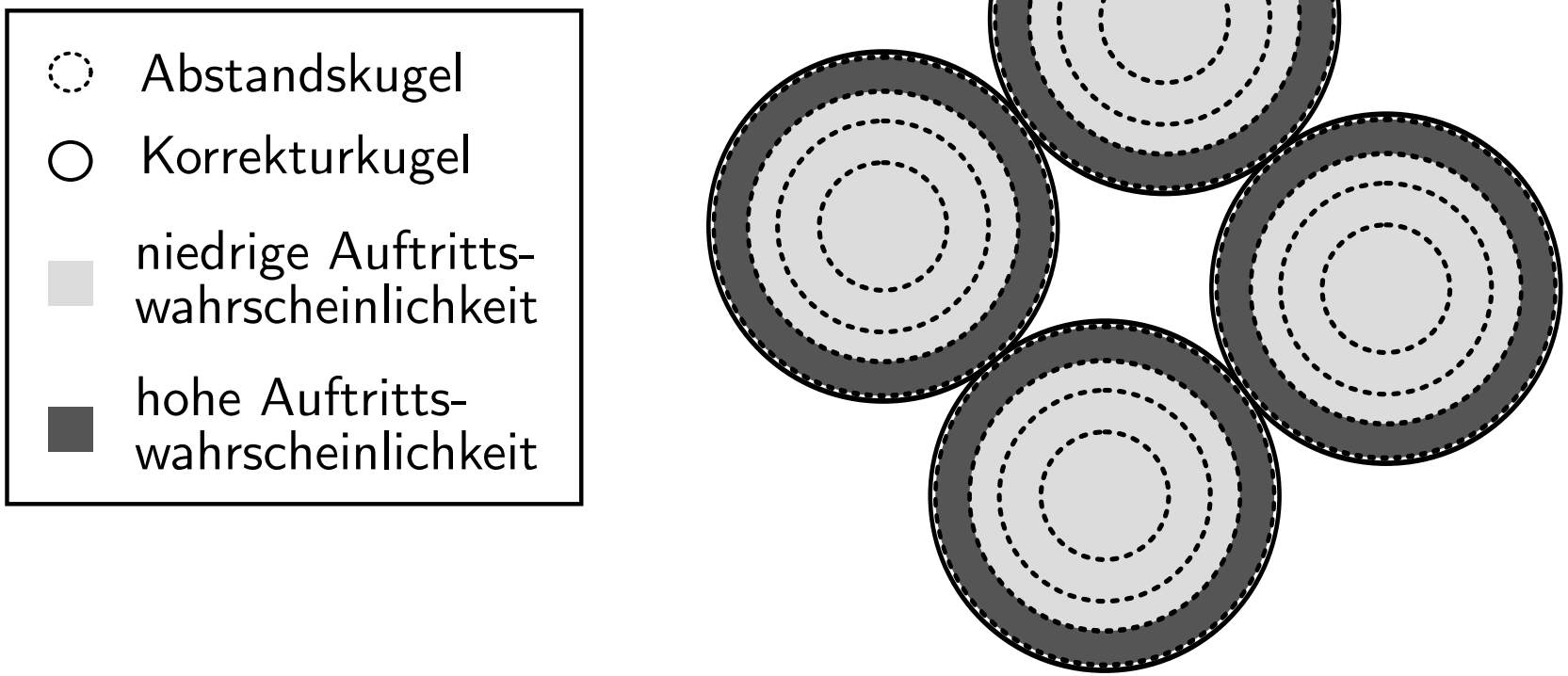
Differenzen zum Träger werden gekippt

Naive Methode



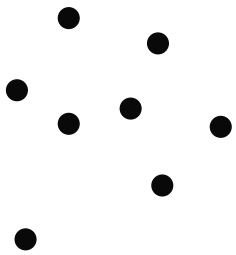
Durch Fehlerkorrektur wird die Nachricht wiederhergestellt

Naive Methode – Angriff

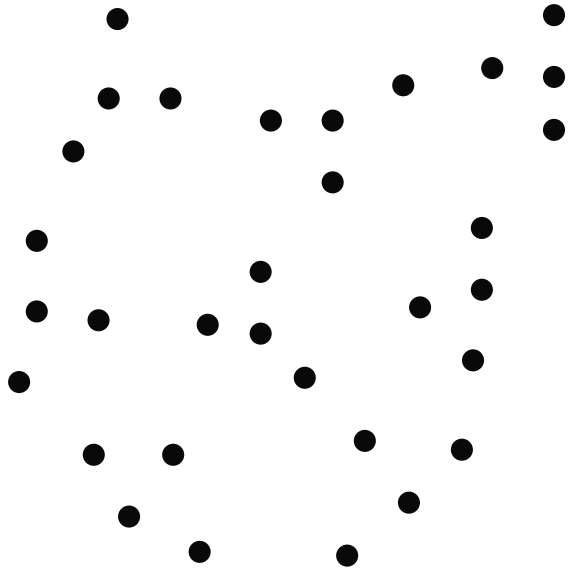


Zuordnung Nachricht – Stegowort

Nachrichten

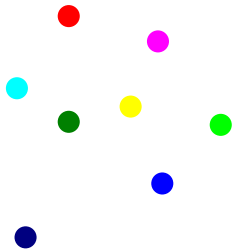


Stegowörter

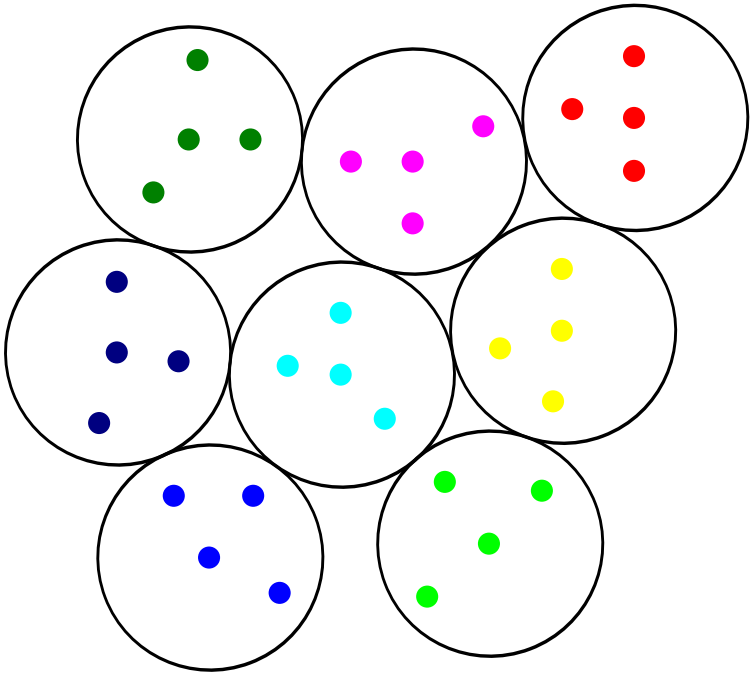


Zuordnung Nachricht – Stegowort

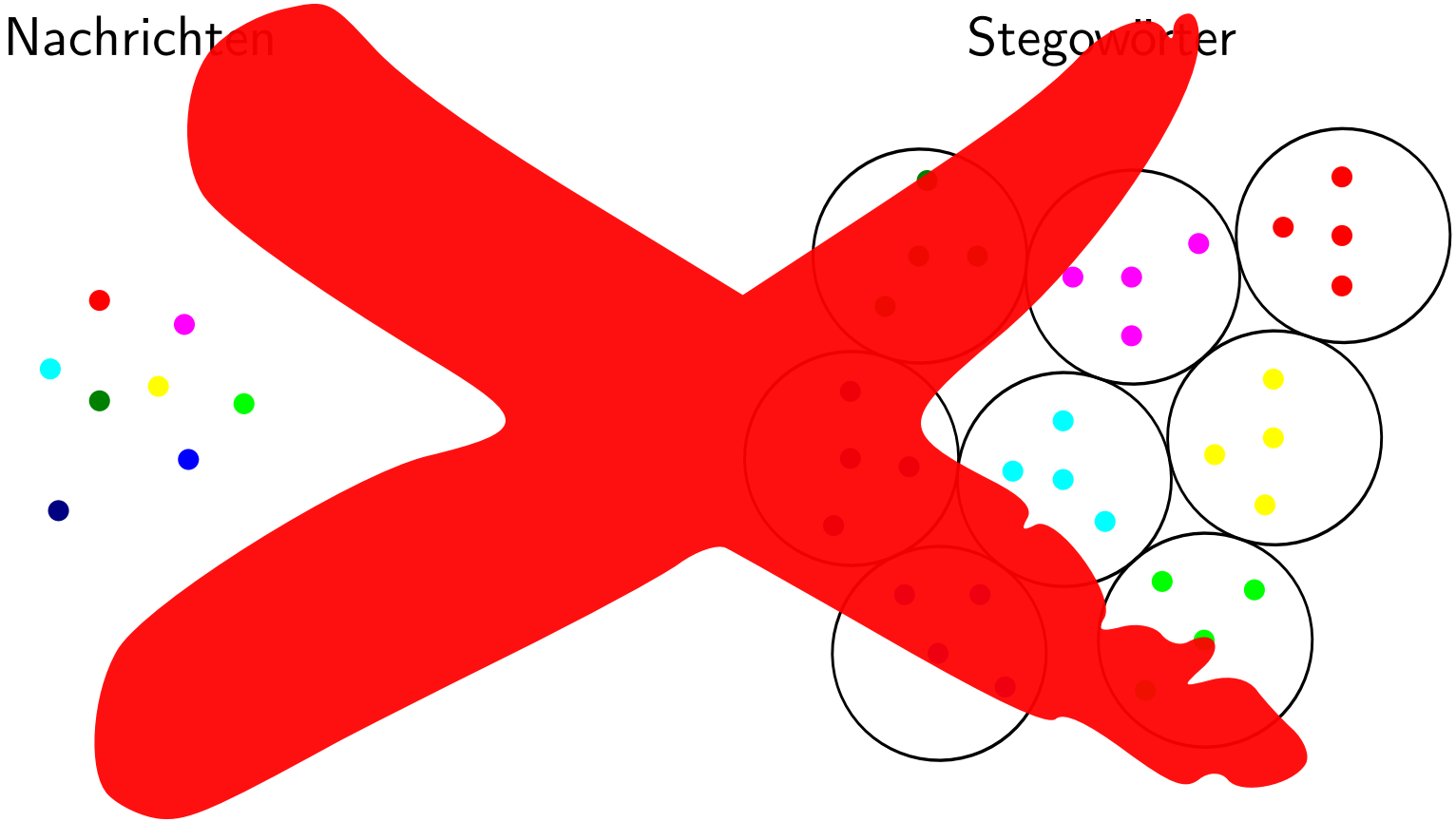
Nachrichten



Stegowörter

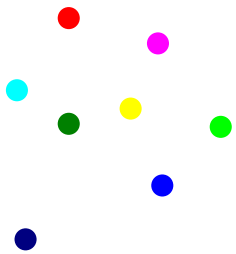


Zuordnung Nachricht – Stegowort

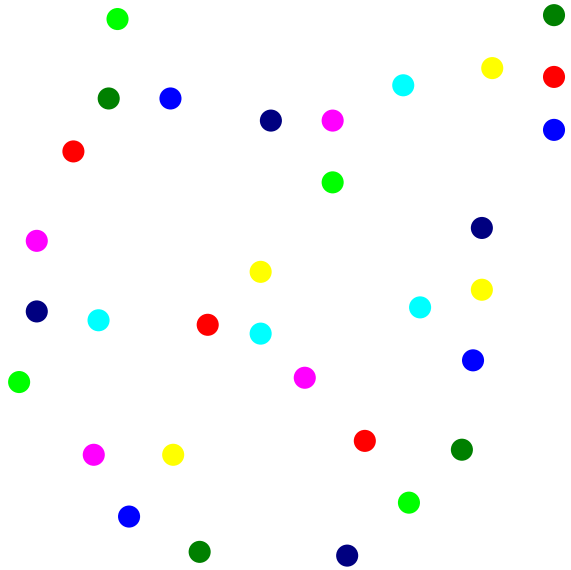


Zuordnung Nachricht – Stegowort

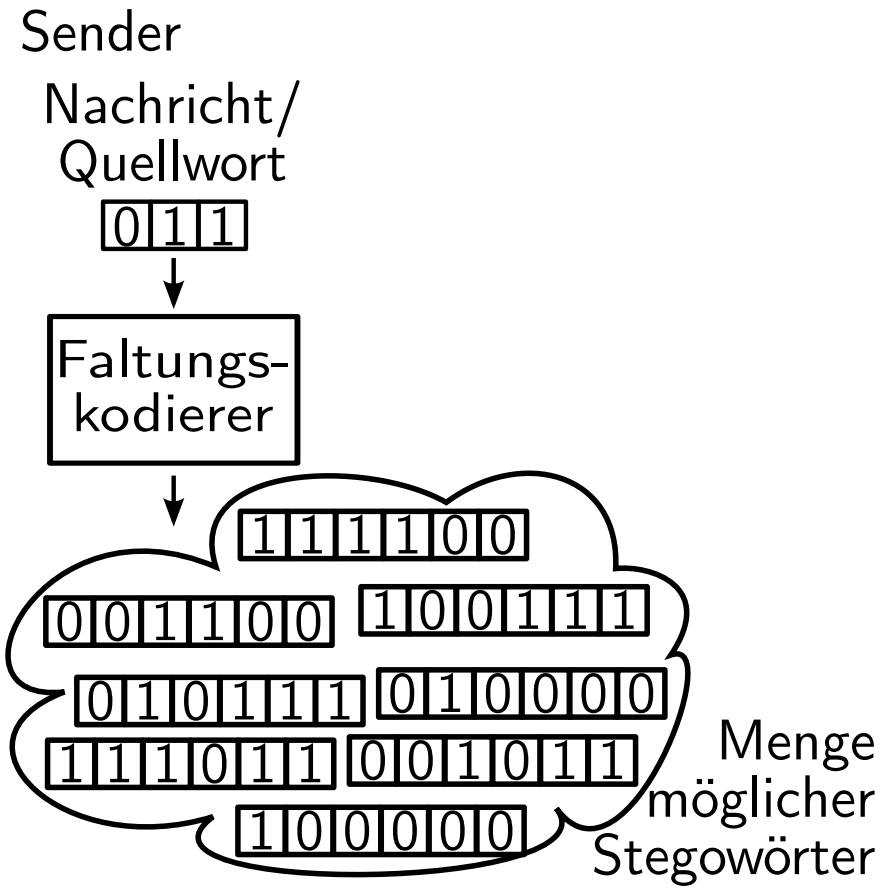
Nachrichten



Stegowörter

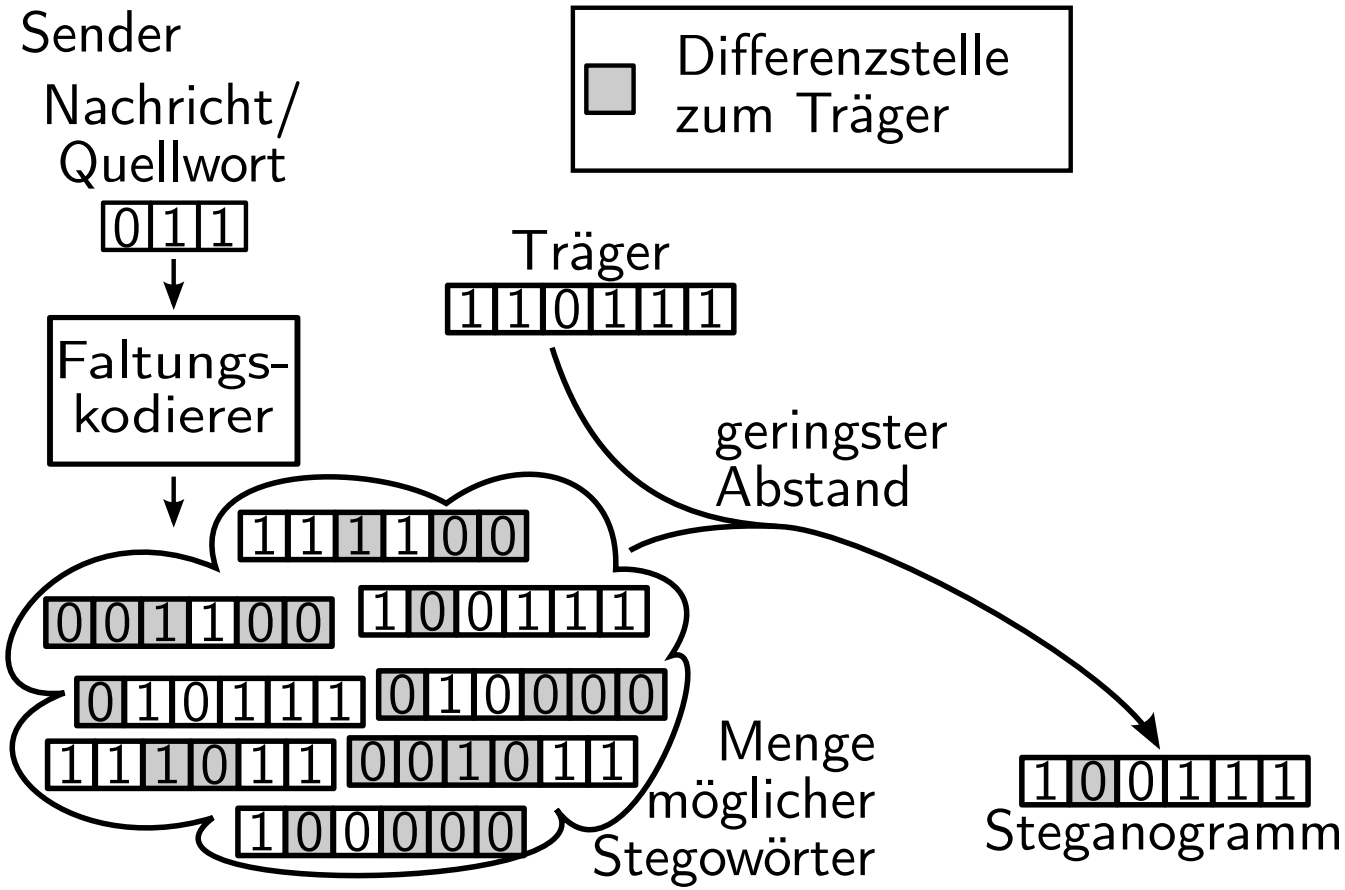


Variabler Startzustand



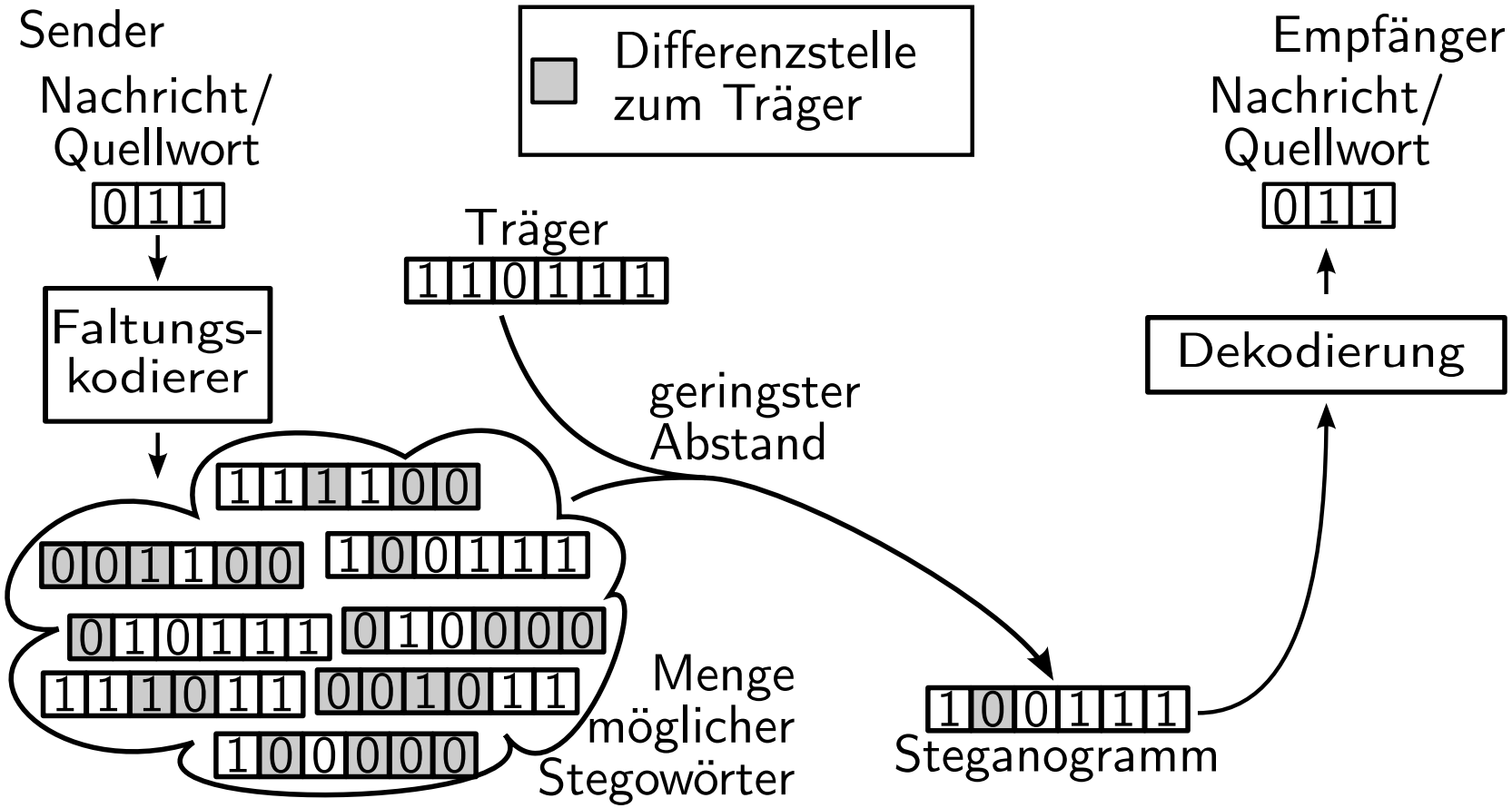
Nachricht wird von jedem Startzustand einmal kodiert

Variabler Startzustand



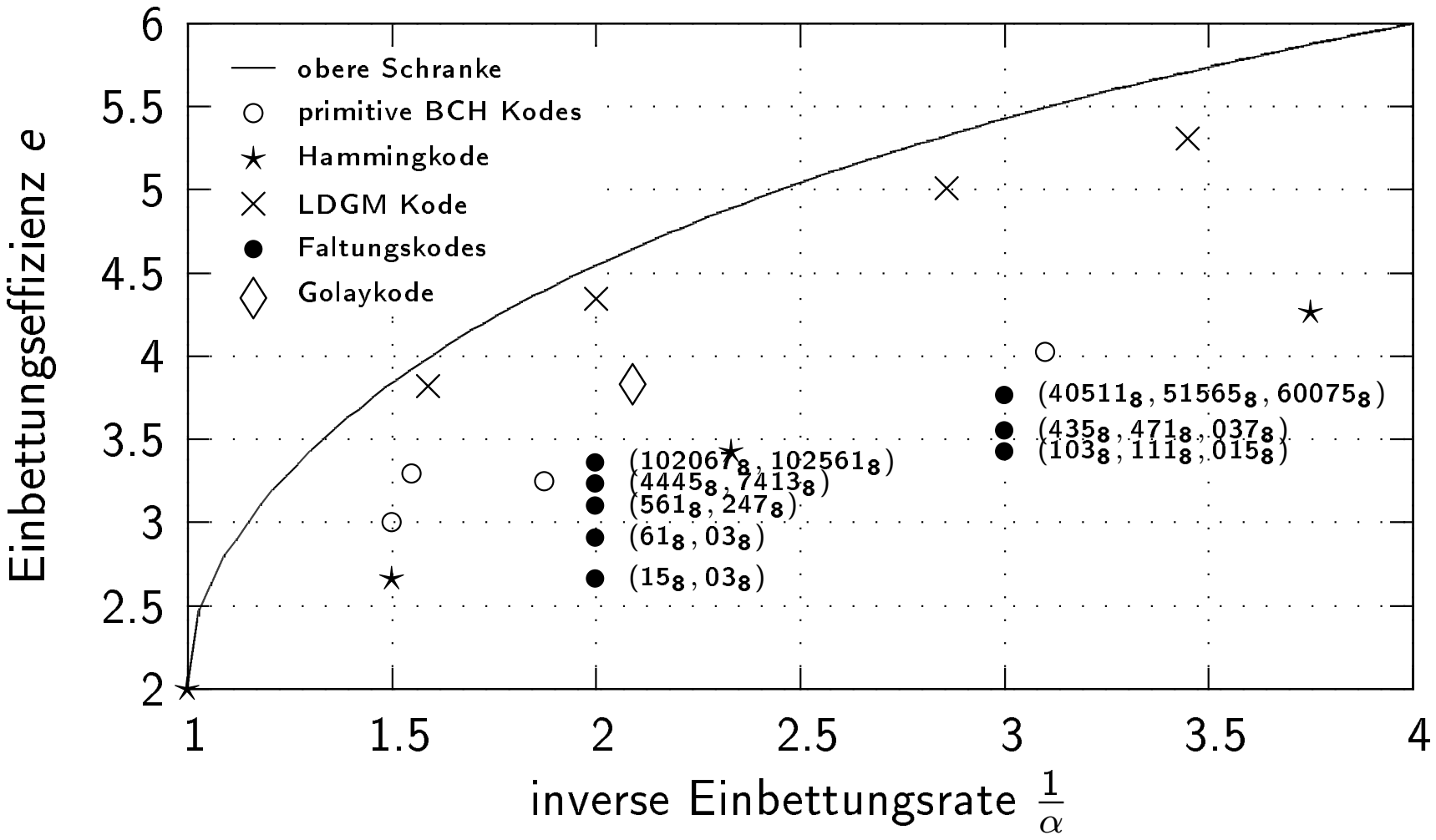
Stegowort mit geringstem Abstand zum Träger wird ausgewählt

Variabler Startzustand

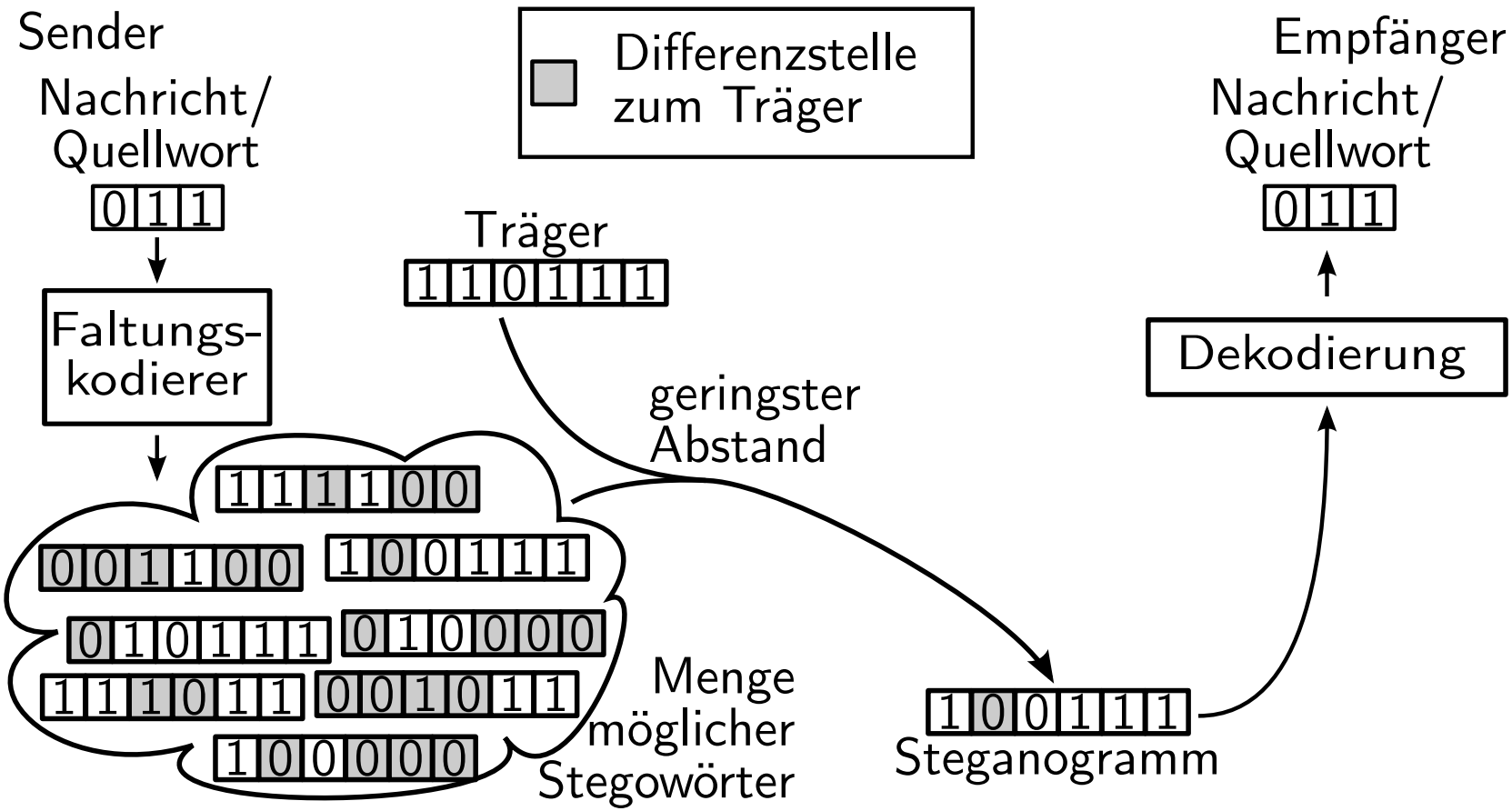


Empfänger dekodiert mit Viterbi

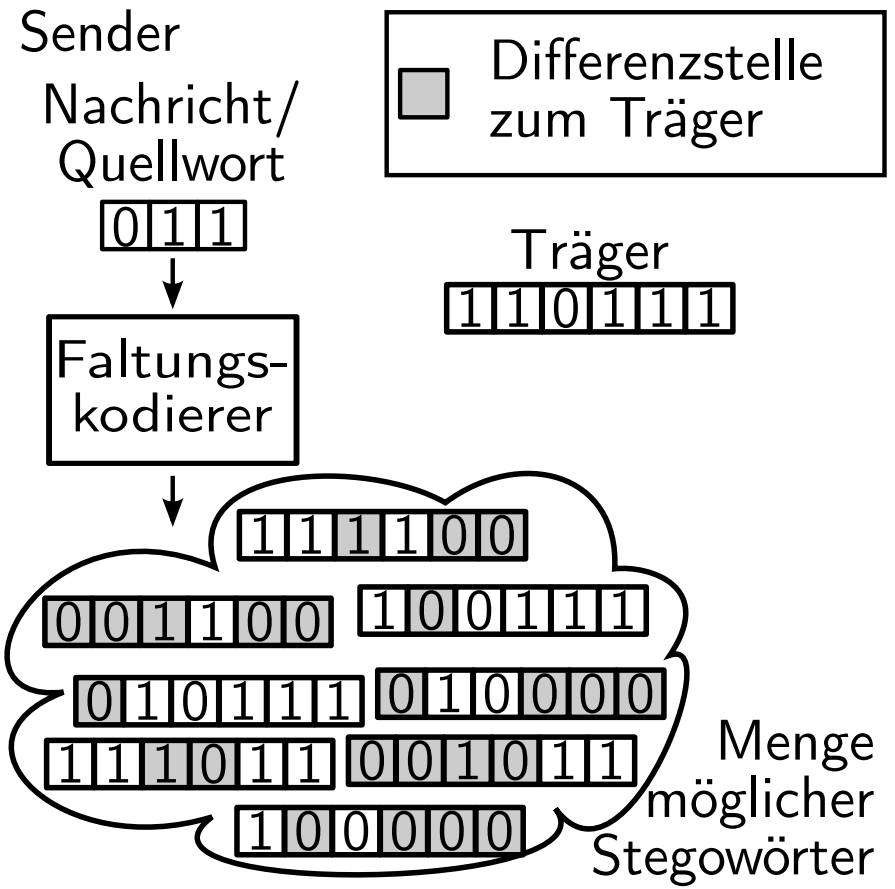
Variabler Startzustand – Ergebnis



Einbeziehung des Startzustandes

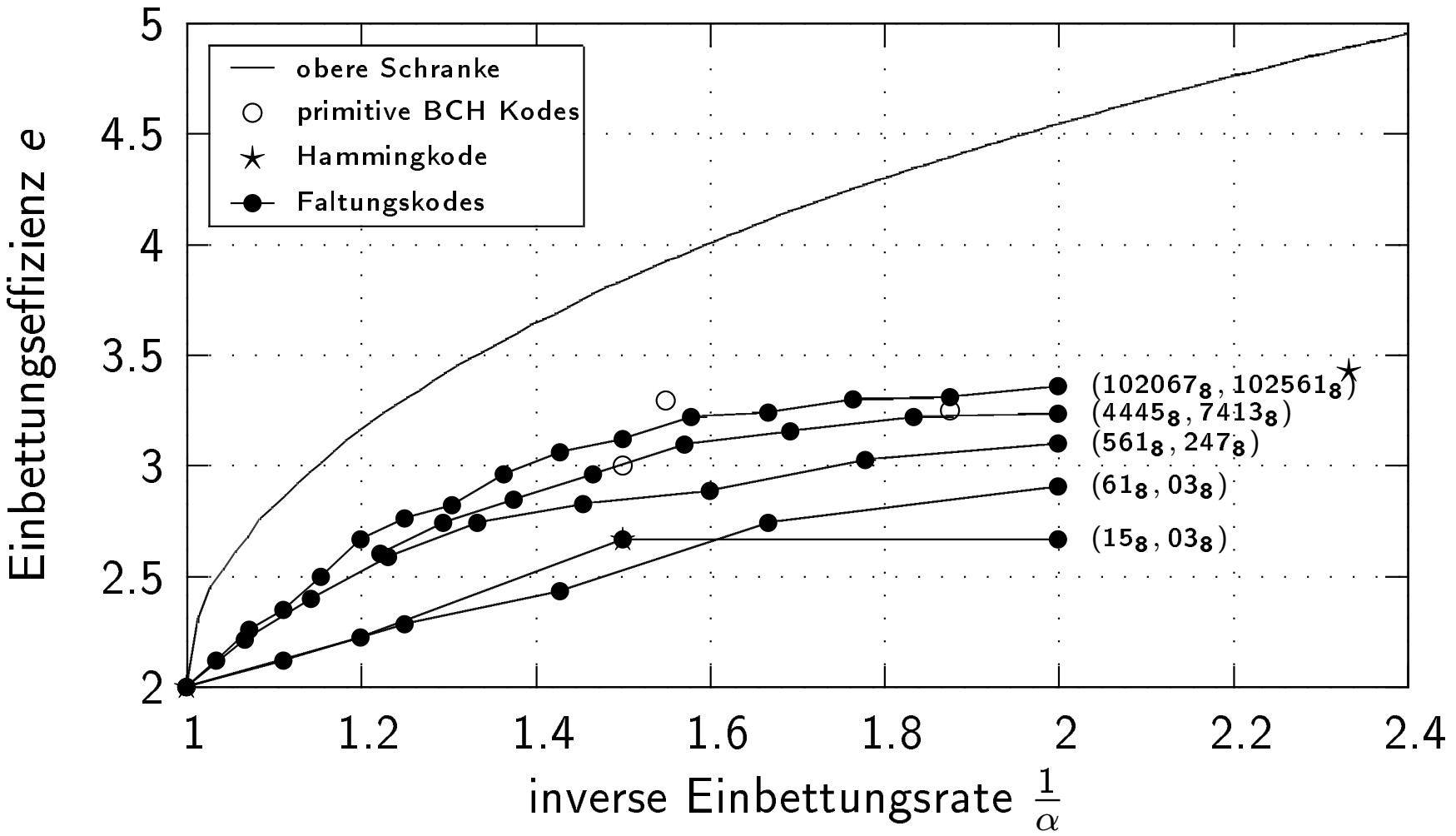


Einbeziehung des Startzustandes



Start-zustand	Stegowort	Abstand zum Träger
000	001100	5
001	111100	3
010	010000	4
011	100000	4
100	111011	2
101	001011	4
110	100111	1
111	010111	1

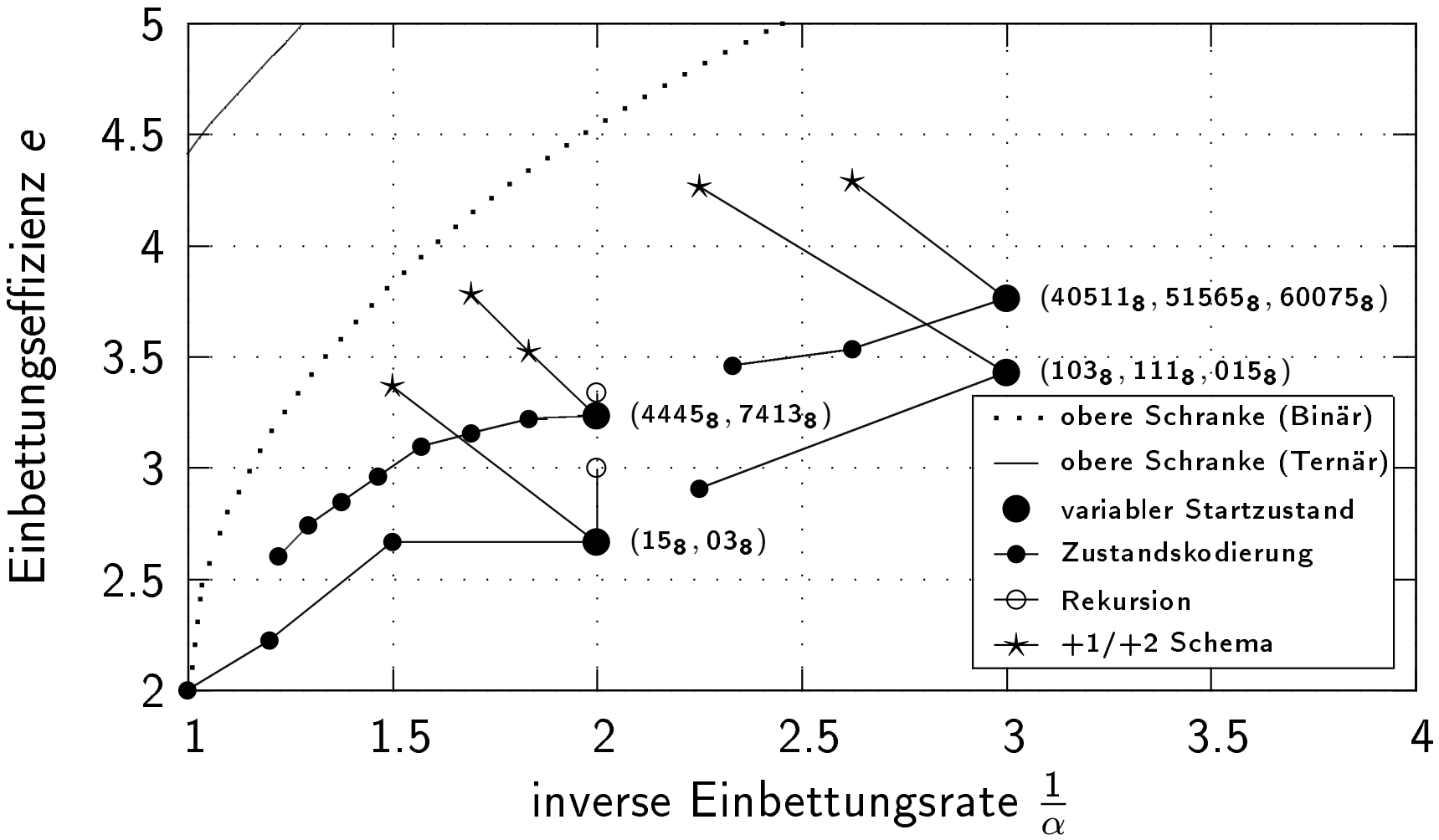
Einbeziehung des Startzustandes – Ergebnis



Weitere Verbesserungen

- Vorschläge um Berechnungsaufwand zu senken
- rekursive Faltungskodierer
- +1/+2 Schema von Zhang et al.

Zusammenfassung



Ausblick

- Bedingungen für zufällige Kantenbeschriftung?
- Mehr als 2 Zustandsübergänge von jedem Zustand?
- Klassische Blockkodes als Trellisdiagramm?
- Soft-decision Dekodierung nutzbar?

Fragen?

Vielen Dank für Ihre Aufmerksamkeit!