Mathematische Codierungstheorie: Das Sicherstellen von Klarheit in einer verrauschten Welt

Joachim Rosenthal
Universität Zürich

Lehrerfortbildungen in Mathematik, Passau, 12. Dezember 2025.

Inhaltsverzeichnis:

Claude Shannons grundlegende Arbeiten in der Informationstheorie

Claude Shannon gilt als Begründer der mathematischen Informationstheorie. Er legte den Grundstein für folgende fundamentale Fragen:

Claude Shannons grundlegende Arbeiten in der Informationstheorie

Claude Shannon gilt als Begründer der mathematischen Informationstheorie. Er legte den Grundstein für folgende fundamentale Fragen:

- Redundanz: Wie kann Information mit einer minimalen Anzahl von Bits beschrieben werden?

Claude Shannons grundlegende Arbeiten in der Informationstheorie

Claude Shannon gilt als Begründer der mathematischen Informationstheorie. Er legte den Grundstein für folgende fundamentale Fragen:

- Redundanz: Wie kann Information mit einer minimalen Anzahl von Bits beschrieben werden?
- Zuverlässigkeit: Wie überträgt man Information fehlerfrei?

Claude Shannons grundlegende Arbeiten in der Informationstheorie

Claude Shannon gilt als Begründer der mathematischen Informationstheorie. Er legte den Grundstein für folgende fundamentale Fragen:

- Redundanz: Wie kann Information mit einer minimalen Anzahl von Bits beschrieben werden?
- Zuverlässigkeit: Wie überträgt man Information fehlerfrei?
- Sicherheit: Wie überträgt man Information privat zwischen zwei Parteien.

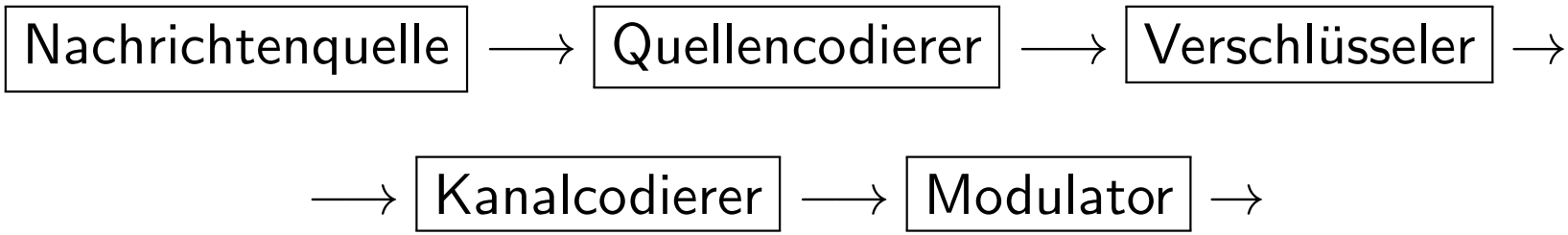
Claude Shannons grundlegende Arbeiten in der Informationstheorie

Claude Shannon gilt als Begründer der mathematischen Informationstheorie. Er legte den Grundstein für folgende fundamentale Fragen:

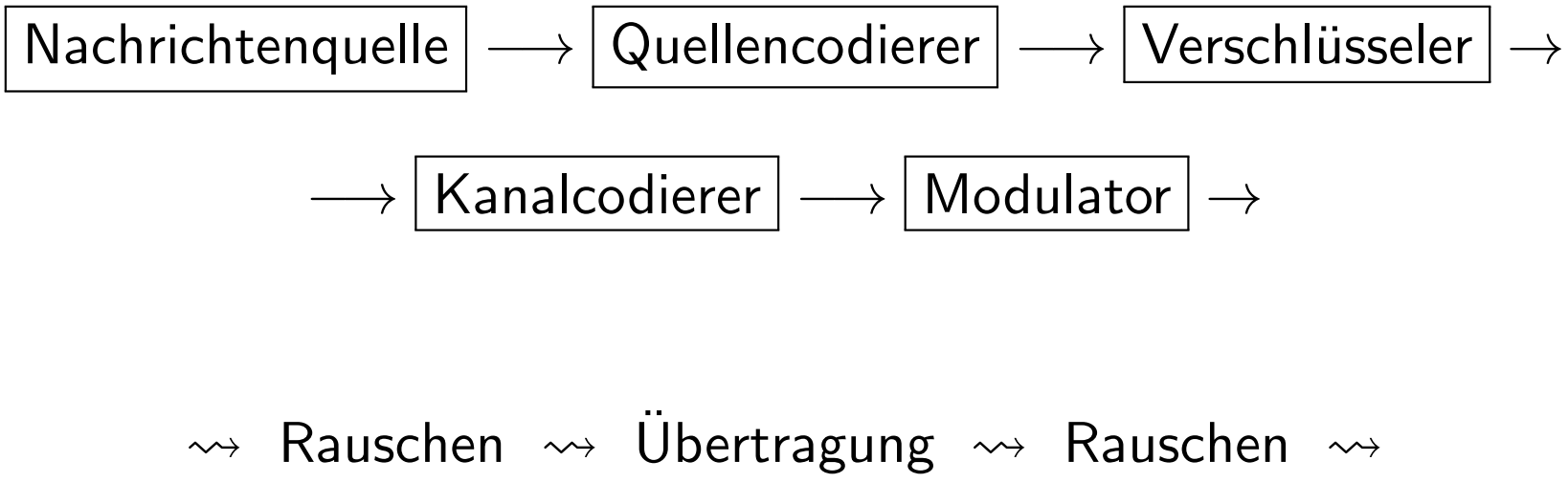
- Redundanz: Wie kann Information mit einer minimalen Anzahl von Bits beschrieben werden?
- Zuverlässigkeit: Wie überträgt man Information fehlerfrei?
- Sicherheit: Wie überträgt man Information privat zwischen zwei Parteien.

Shannon betonte die Wichtigkeit eines 'Separationsprinzips', das die Ziele in verschiedene Aufgaben unterteilt.

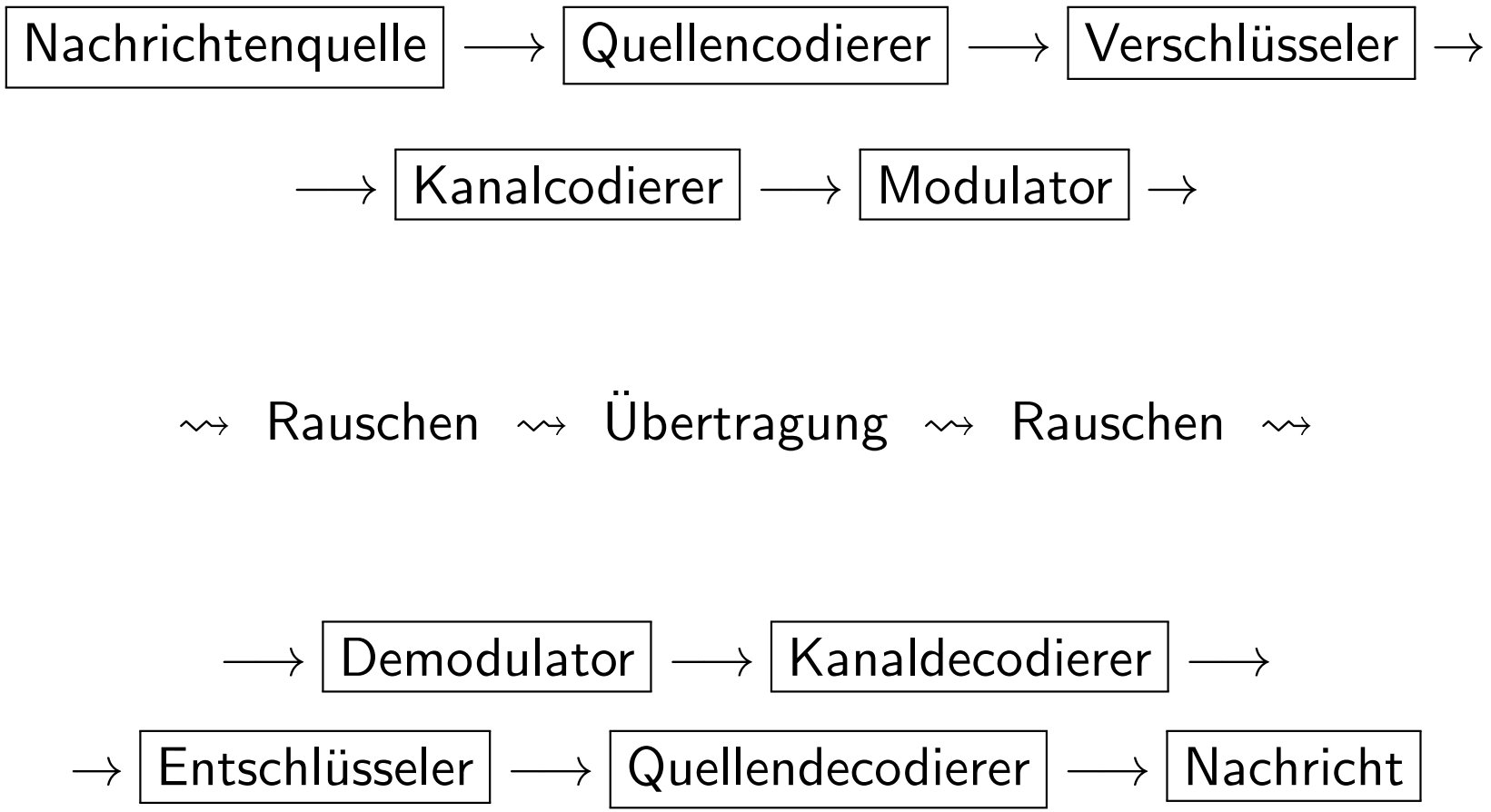
Kommunikation unter dem Separationsprinzip



Kommunikation unter dem Separationsprinzip



Kommunikation unter dem Separationsprinzip



Shannons Herausforderungen

1948/49 veröffentlichte Claude Shannon [Sha48, Sha49] drei grundlegende Ergebnisse, die Quellencodierung, Kanalcodierung und Kryptographie abdeckten. Jedes Ergebnis zeigte, was 'theoretisch möglich' ist. Jedes Ergebnis war 'unpraktisch'.

- 'Satz über die rauschfreie Codierung': *Daten können bis zur Entropie komprimiert werden, sobald die Wahrscheinlichkeitsverteilung der Quelle bekannt ist.*

Shannons Herausforderungen

1948/49 veröffentlichte Claude Shannon [Sha48, Sha49] drei grundlegende Ergebnisse, die Quellencodierung, Kanalcodierung und Kryptographie abdeckten. Jedes Ergebnis zeigte, was 'theoretisch möglich' ist. Jedes Ergebnis war 'unpraktisch'.

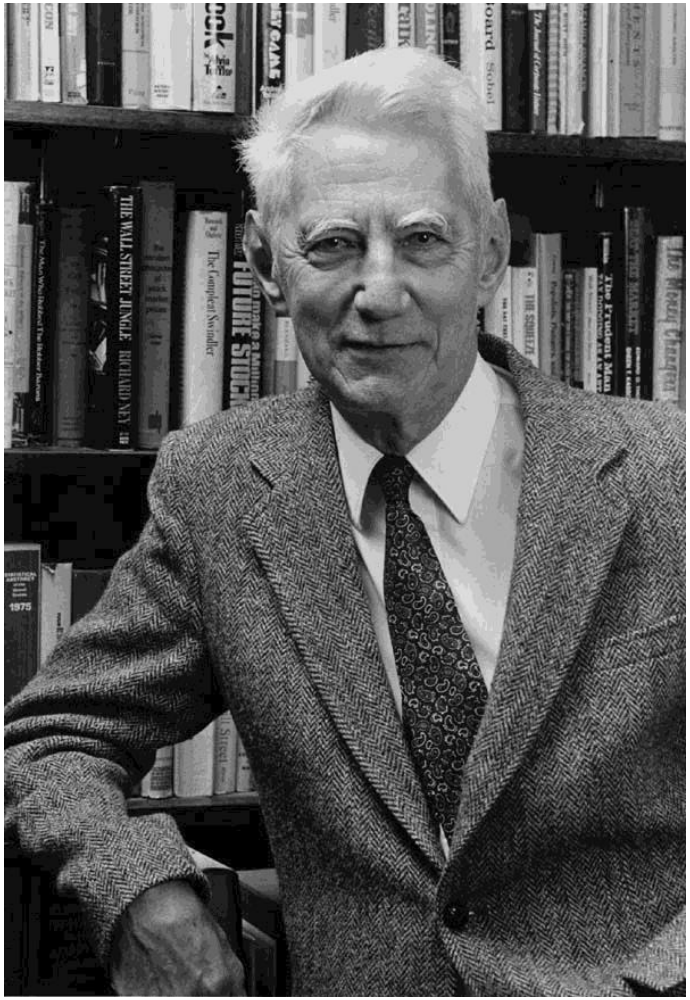
- 'Satz über die rauschfreie Codierung': *Daten können bis zur Entropie komprimiert werden, sobald die Wahrscheinlichkeitsverteilung der Quelle bekannt ist.*
- 'Satz über die rauschbehaftete Codierung' (Kanalcodierungssatz): *Jeder Übertragungskanal hat eine 'Kapazität'. Eine zuverlässige Übertragung ist bei einer Übertragungsrate unterhalb der Kapazität möglich.*

Shannons Herausforderungen

1948/49 veröffentlichte Claude Shannon [Sha48, Sha49] drei grundlegende Ergebnisse, die Quellencodierung, Kanalcodierung und Kryptographie abdeckten. Jedes Ergebnis zeigte, was 'theoretisch möglich' ist. Jedes Ergebnis war 'unpraktisch'.

- 'Satz über die rauschfreie Codierung': *Daten können bis zur Entropie komprimiert werden, sobald die Wahrscheinlichkeitsverteilung der Quelle bekannt ist.*
- 'Satz über die rauschbehaftete Codierung' (Kanalcodierungssatz): *Jeder Übertragungskanal hat eine 'Kapazität'. Eine zuverlässige Übertragung ist bei einer Übertragungsrate unterhalb der Kapazität möglich.*
- *Es gibt bedingungslos und beweisbar sichere kryptographische Protokolle.*

Claude Shannon (1916-2001)



Quelle: *http://www.bell-labs.com/*

Codierung an der Quelle

Ziel: Redundanz eliminieren.

Example

Angenommen, die Nachricht ist ein Text bestehend aus den Buchstaben A, C, G, T.

Codierung an der Quelle

Ziel: Redundanz eliminieren.

Example

Angenommen, die Nachricht ist ein Text bestehend aus den Buchstaben A, C, G, T.

Die Codierung erfolgt:

$$\begin{aligned} A &\xmapsto{\varphi} 00 \\ C &\xmapsto{\varphi} 01 \\ G &\xmapsto{\varphi} 10 \\ T &\xmapsto{\varphi} 11 \end{aligned}$$

Im Durchschnitt werden zwei Bits pro Buchstabe benötigt.

Codierung an der Quelle

Beispiel

Angenommen, die Buchstaben A, C, G, T kommen bekanntermaßen mit folgenden Häufigkeiten im Text vor:

Buchstabe:	*A*	*C*	*G*	*T*
Wahrscheinlichkeit:	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{8}$

Codierung an der Quelle

Beispiel

Angenommen, die Buchstaben A, C, G, T kommen bekanntermaßen mit folgenden Häufigkeiten im Text vor:

Buchstabe:	A	C	G	T
Wahrscheinlichkeit:	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{8}$

Die Codierung erfolgt:

$$\begin{aligned} A &\overset{\varphi}{\longmapsto} 0 \\ C &\overset{\varphi}{\longmapsto} 10 \\ G &\overset{\varphi}{\longmapsto} 110 \\ T &\overset{\varphi}{\longmapsto} 111 \end{aligned}$$

Codierung an der Quelle

Beispiel

Angenommen, die Buchstaben A, C, G, T kommen bekanntermaßen mit folgenden Häufigkeiten im Text vor:

Buchstabe:	A	C	G	T
Wahrscheinlichkeit:	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{8}$

Die Codierung erfolgt:

$$\begin{aligned} A &\overset{\varphi}{\longmapsto} 0 \\ C &\overset{\varphi}{\longmapsto} 10 \\ G &\overset{\varphi}{\longmapsto} 110 \\ T &\overset{\varphi}{\longmapsto} 111 \end{aligned}$$

Im Durchschnitt werden 1,75 Bits pro Buchstabe benötigt.

Satz über die rauschfreie Codierung

Definition

Sei X eine diskrete Zufallsvariable mit der Wahrscheinlichkeitsfunktion

$$f_X(x_i) = p_i, \ \ i = 1, \ldots, n.$$

Dann ist die *Entropie* von X definiert als

$$H(X) := -\sum_{i=1}^{n} p_i \log_2 p_i.$$

Satz über die rauschfreie Codierung

Definition

Sei X eine diskrete Zufallsvariable mit der Wahrscheinlichkeitsfunktion

$$f_X(x_i) = p_i, \ \ i = 1, \ldots, n.$$

Dann ist die *Entropie* von X definiert als

$$H(X) := -\sum_{i=1}^{n} p_i \log_2 p_i.$$

Bemerkung

$$0 \leq H(X) \leq \log_2 n$$

Beispiel

In Beispiel 1 gilt:

$$H(X) = \frac{1}{2}\log_2(2) + \frac{1}{4}\log_2(4) + \frac{1}{8}\log_2(8) + \frac{1}{8}\log_2(8) = 1.75$$

Beispiel

In Beispiel 1 gilt:

$$H(X) = \frac{1}{2}\log_2(2) + \frac{1}{4}\log_2(4) + \frac{1}{8}\log_2(8) + \frac{1}{8}\log_2(8) = 1.75$$

Theorem (Satz über die rauschfreie Codierung [Sha48])

Seien $a_1, a_2, a_3, \ldots$ eine Zufallsstichprobe einer diskreten Zufallsvariablen X, die einen Text repräsentiert. Dann beträgt die durchschnittliche Anzahl von Bits pro Symbol in jedem binären Codierungsschema mindestens $H(X)$. Außerdem gibt es Codierungsschemata, die im Durchschnitt höchstens ϵ Bits pro Symbol mehr als $H(X)$ benötigen, für jedes beliebige $\epsilon > 0$.

Praktische Lösung

Huffman [Huf52] leitete einen effizienten Algorithmus für ein 'sofort lesbares Codierungsschema' her, das im Durchschnitt t Bits pro Symbol benötigt, wobei

$$H(X) \leq t \leq H(X) + 1.$$

Das Codierungsschema erforderte die genaue Kenntnis der Wahrscheinlichkeitsfunktion von X.

Praktische Lösung

Huffman [Huf52] leitete einen effizienten Algorithmus für ein 'sofort lesbares Codierungsschema' her, das im Durchschnitt t Bits pro Symbol benötigt, wobei

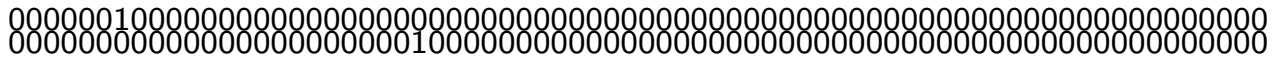
$$H(X) \leq t \leq H(X) + 1.$$

Das Codierungsschema erforderte die genaue Kenntnis der Wahrscheinlichkeitsfunktion von X.

Ziv und Lempel [ZL77, ZL78] leiteten ein 'universelles Codierungsschema' her, das asymptotisch $H(X)$ Bits pro Symbol benötigt und auf jede unabhängig und identisch verteilte Quelle angewendet werden kann.

Ein anschauliches Beispiel

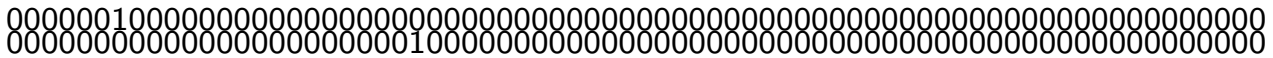
Angenommen, es gibt einen Text, der aus 10^6 Bits besteht.
Angenommen, es gibt im Durchschnitt nur eine 1 in jedem 100-Bit-Block.



Eine Übertragungsmethode ohne Kompression benötigt 10^6 Bits.

Ein anschauliches Beispiel

Angenommen, es gibt einen Text, der aus 10^6 Bits besteht.
Angenommen, es gibt im Durchschnitt nur eine 1 in jedem 100-Bit-Block.



Eine Übertragungsmethode ohne Kompression benötigt 10^6 Bits.
Shannon sagt voraus, dass dies in:

$$(0.01 \log_2 100 + 0.99 \log_2 \frac{100}{99})10^6 \text{ Bits} \approx 80793 \text{ Bits}$$

geschehen kann.

Ein einfaches Kompressionsschema

Zähle die Gesamtanzahl n der Bits und die Gesamtzahl k der Einsen. Im Folgenden nehmen wir an, dass

$$n := 10^6 \quad \text{und } k := 10^4.$$

Die Übertragung von k, n benötigt ungefähr:

$$\log_2 n + \log_2 k \text{ Bits } \approx (20 + 13) \text{ Bits } = 33 \text{ Bits}$$

Ein einfaches Kompressionsschema

Zähle die Gesamtanzahl n der Bits und die Gesamtzahl k der Einsen. Im Folgenden nehmen wir an, dass

$$n := 10^6 \quad \text{und } k := 10^4.$$

Die Übertragung von k, n benötigt ungefähr:

$$\log_2 n + \log_2 k \text{ Bits } \approx (20 + 13) \text{ Bits } = 33 \text{ Bits}$$

Unter Verwendung der Stirling-Formel $\left(n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}\right)$ berechnet man leicht:

$$\log_2 \binom{n}{k} \text{ Bits} \approx 80785 \text{ Bits}.$$

Die gesamte Übertragung benötigt $80785 + 33 = 80818$ Bits, etwas mehr als Shannons Grenze von 80793 Bits.

Ein kleines Kartenspiel

Sie werden gebeten, folgendes Spiel zu spielen:

Ein kleines Kartenspiel

Sie werden gebeten, folgendes Spiel zu spielen:

- Ihnen werden 10 Karten mit den Nummern 1-10 in einer bestimmten Reihenfolge präsentiert. Sie dürfen die Nummern auf den Karten nicht sehen.

Ein kleines Kartenspiel

Sie werden gebeten, folgendes Spiel zu spielen:

- Ihnen werden 10 Karten mit den Nummern 1-10 in einer bestimmten Reihenfolge präsentiert. Sie dürfen die Nummern auf den Karten nicht sehen.
- Sie dürfen jede Umgruppierung der Karten verlangen.

Ein kleines Kartenspiel

Sie werden gebeten, folgendes Spiel zu spielen:

- Ihnen werden 10 Karten mit den Nummern 1-10 in einer bestimmten Reihenfolge präsentiert. Sie dürfen die Nummern auf den Karten nicht sehen.
- Sie dürfen jede Umgruppierung der Karten verlangen.
- Sie können Fragen stellen wie: Ist der Wert dieser Karte größer als der Wert jener Karte? Sie können auch fragen: Trägt diese Karte die Nummer 7? Oder: Sind die Karten jetzt in aufsteigender Reihenfolge angeordnet? Jede Frage kostet Sie \$1.

Ein kleines Kartenspiel

Sie werden gebeten, folgendes Spiel zu spielen:

- Ihnen werden 10 Karten mit den Nummern 1-10 in einer bestimmten Reihenfolge präsentiert. Sie dürfen die Nummern auf den Karten nicht sehen.
- Sie dürfen jede Umgruppierung der Karten verlangen.
- Sie können Fragen stellen wie: Ist der Wert dieser Karte größer als der Wert jener Karte? Sie können auch fragen: Trägt diese Karte die Nummer 7? Oder: Sind die Karten jetzt in aufsteigender Reihenfolge angeordnet? Jede Frage kostet Sie \$1.
- Sobald Sie den Zahlenwert jeder Karte bestimmt haben, erhalten Sie eine Auszahlung von \$20.

Ein kleines Kartenspiel

Sie werden gebeten, folgendes Spiel zu spielen:

- Ihnen werden 10 Karten mit den Nummern 1-10 in einer bestimmten Reihenfolge präsentiert. Sie dürfen die Nummern auf den Karten nicht sehen.
- Sie dürfen jede Umgruppierung der Karten verlangen.
- Sie können Fragen stellen wie: Ist der Wert dieser Karte größer als der Wert jener Karte? Sie können auch fragen: Trägt diese Karte die Nummer 7? Oder: Sind die Karten jetzt in aufsteigender Reihenfolge angeordnet? Jede Frage kostet Sie \$1.
- Sobald Sie den Zahlenwert jeder Karte bestimmt haben, erhalten Sie eine Auszahlung von \$20.

Würden Sie die Herausforderung annehmen, dieses Spiel zu spielen?!

Kanalcodierungssatz [Sha48]

Satz

Angenommen, ein Übertragungskanal hat die Kapazität C. Sei $R < C$ eine beliebige rationale Zahl und $\epsilon > 0$ beliebig. Dann existiert ein Codierungsschema mit der Übertragungsrate R und einer Symbolfehlerrate von höchstens ϵ.

Kanalcodierungssatz [Sha48]

Satz

Angenommen, ein Übertragungskanal hat die Kapazität C. Sei $R < C$ eine beliebige rationale Zahl und $\epsilon > 0$ beliebig. Dann existiert ein Codierungsschema mit der Übertragungsrate R und einer Symbolfehlerrate von höchstens ϵ.
Wenn die Rate $R > C$ ist, kann ein Restfehler nicht eliminiert werden.

Kanalcodierungssatz [Sha48]

Satz

Angenommen, ein Übertragungskanal hat die Kapazität C. Sei $R < C$ eine beliebige rationale Zahl und $\epsilon > 0$ beliebig. Dann existiert ein Codierungsschema mit der Übertragungsrate R und einer Symbolfehlerrate von höchstens ϵ.
Wenn die Rate $R > C$ ist, kann ein Restfehler nicht eliminiert werden.

Bemerkung

Shannons Beweis war probabilistisch und die vorhergesagten Codes waren weder für die praktische Codierung noch für die Decodierung realisierbar.

Redundanz der Deutschen Sprache

Die Bcuhstbaenrehenifloge in eneim Wrot ist eagl

Ncah enier nueen Sutide, die uetnr aerdnem von der Cmabirdge Uinertvisy dührruchgeft wrdoen sien slol, ist es eagl, in wlehcer Rehenifloge Bcuhstbaen in eneim Wrot sethen, Huaptschae, der esrte und ltzete Bcuhstbae snid an der rhcitgien Setlle. Die rsetclhien Bshcuteban kenönn ttoal druchenianedr sien, und man knan es tortzedm onhe Poreblme lseen, wiel das mneschilhce Gherin nhcit jdeen Bcuhstbaen enizlen leist, snodren das Wrot als gnazes. Mti dme Pähonemn bchesfätgein shci mherere Hhcochsluen, acuh die aerichmkianse Uivnäseritt in Ptstbigurh. Esrtmlas üebr das Tmeha gchseibren hat aebr breteis 1976 - und nun in der rgchitien Bruecihhsetnafoelngbe - Graham Rawlinson in sieenr Dsiestraiton mit dem Tetil *The Significance of Letter Position in Word Recognition* an der egnlsicehn Uitneivrsy of Ntitongahm.

Kanalcodierung

Das Verständnis vor Shannons Arbeit war:

Repetitio est mater communicationis

Z.B. angenommen, 10% der Buchstaben sind falsch. Sende jeden Buchstaben 11 Mal und führe eine Mehrheitsentscheidung durch:

IIIIIIIIIIInnnnnnnnnnn

1111111111199999999994444444448888888888

Kanalcodierung

Das Verständnis vor Shannons Arbeit war:

Repetitio est mater communicationis

Z.B. angenommen, 10% der Buchstaben sind falsch. Sende jeden Buchstaben 11 Mal und führe eine Mehrheitsentscheidung durch:
lllllllllllnnnnnnnnnnn
11111111111999999999944444444488888888888

Nota Bene: Dies vergrößert den Text um das 11-fache und es besteht immer noch die Möglichkeit, dass ein Buchstabe falsch decodiert wird.

Kanalcodierung

Das Verständnis vor Shannons Arbeit war:

Repetitio est mater communicationis

Z.B. angenommen, 10% der Buchstaben sind falsch. Sende jeden Buchstaben 11 Mal und führe eine Mehrheitsentscheidung durch:
lllllllllllnnnnnnnnnnn
11111111111999999999944444444488888888888

Nota Bene: Dies vergrößert den Text um das 11-fache und es besteht immer noch die Möglichkeit, dass ein Buchstabe falsch decodiert wird.

Shannons Theorem impliziert, dass es für einen langen Text mit dem obigen Fehlermuster ausreicht, etwa 20% Redundanz hinzuzufügen, und dies den Fehler pro Symbol auf Null bringt.

Shannons Lösung war nicht praktikabel!!!

Blockcodes

Definition

Sei $\mathcal{M} := \{m_1, \ldots, m_s\}$ eine endliche Menge von "Nachrichtenwörtern" und sei $\mathcal{A} := \{a_1, \ldots, a_t\}$ ein endliches Alphabet. Eine injektive Abbildung

$$\varphi : \mathcal{M} \longrightarrow \mathcal{A}^n$$

heißt Encoder und

$$\mathcal{C} := Im(\varphi) \subset \mathcal{A}^n$$

heißt Blockcode der Länge n.

Blockcodes

Definition

Sei $\mathcal{M} := \{m_1, \ldots, m_s\}$ eine endliche Menge von "Nachrichtenwörtern" und sei $\mathcal{A} := \{a_1, \ldots, a_t\}$ ein endliches Alphabet. Eine injektive Abbildung

$$\varphi : \mathcal{M} \longrightarrow \mathcal{A}^n$$

heißt Encoder und

$$\mathcal{C} := Im(\varphi) \subset \mathcal{A}^n$$

heißt Blockcode der Länge n.

Beispiel

Zuweisung von Telefonnummern an Telefonkunden.

Bemerkungen zu Blockcodes:

Definition

Angenommen $x, y \in \mathcal{A}^n$. *Dann wird*

$$d(x, y) := \sharp\{i \mid x_i \neq y_i\}$$

als die Hamming-Distanz von x, y *bezeichnet.* **(Dies ist eine Metrik!!)**

Bemerkungen zu Blockcodes:

Definition

Angenommen $x, y \in \mathcal{A}^n$. *Dann wird*

$$d(x, y) := \sharp\{i \mid x_i \neq y_i\}$$

als die Hamming-Distanz von x, y *bezeichnet.* **(Dies ist eine Metrik!!)**
Wenn $\mathcal{C} \subset \mathcal{A}^n$ *ein Blockcode ist, dann heißt*

$$d(\mathcal{C}) := \min\{d(x, y) \mid x, y \in \mathcal{C}, x \neq y\}$$

die **Distanz** *des Codes.*

Bemerkungen zu Blockcodes:

Definition

Angenommen $x, y \in \mathcal{A}^n$. *Dann wird*

$$d(x, y) := \sharp\{i \mid x_i \neq y_i\}$$

als die Hamming-Distanz von x, y *bezeichnet.* **(Dies ist eine Metrik!!)**
Wenn $\mathcal{C} \subset \mathcal{A}^n$ *ein Blockcode ist, dann heißt*

$$d(\mathcal{C}) := \min\{d(x, y) \mid x, y \in \mathcal{C}, x \neq y\}$$

die **Distanz** *des Codes.*

Bemerkung Ein Code mit Distanz d kann bis zu $d - 1$ Fehler erkennen und bis zu $\left\lfloor \frac{d-1}{2} \right\rfloor$ Fehler 'korrigieren'.

Das Distanzproblem:

Sei $\mathrm{Ham}(x, y)$ die *Hamming-Distanz* zwischen zwei Vektoren $x, y \in \mathcal{A}^n$. Wenn $\mathcal{C}$ ein Blockcode ist, dann wird

$$d(\mathcal{C}) := \min_{\substack{u,v \in \mathcal{C} \\ u \neq v}} \mathrm{Ham}(u, v) \tag{1}$$

als die *Hamming-Distanz* des Codes bezeichnet.

Das Distanzproblem:

Sei $\mathrm{Ham}(x, y)$ die *Hamming-Distanz* zwischen zwei Vektoren $x, y \in \mathcal{A}^n$. Wenn $\mathcal{C}$ ein Blockcode ist, dann wird

$$d(\mathcal{C}) := \min_{\substack{u,v \in \mathcal{C} \\ u \neq v}} \mathrm{Ham}(u, v) \tag{1}$$

als die *Hamming-Distanz* des Codes bezeichnet.

Bemerkung

Wenn ein Code $\mathcal{C}$ die Hamming-Distanz d hat, kann der Code bis zu $d-1$ Fehler 'erkennen' und er kann bis zu $\left\lfloor \frac{d-1}{2} \right\rfloor$ Fehler 'korrigieren'. Das Hauptproblem der linearen Codierung fragt nach der Konstruktion von Codes mit 'großer' Distanz.

Lineare Blockcodes

Definition

Sei $\mathbb{F}$ ein endlicher Körper (oder allgemeiner ein endlicher Ring). Ein linearer Blockcode *ist ein linearer k-dimensionaler Unterraum $\mathcal{C} \subset \mathbb{F}^n$. Man spricht von einem linearen $[n, k]$-Blockcode.*

Lineare Blockcodes

Definition

Sei $\mathbb{F}$ ein endlicher Körper (oder allgemeiner ein endlicher Ring). Ein linearer Blockcode *ist ein linearer k-dimensionaler Unterraum $\mathcal{C} \subset \mathbb{F}^n$. Man spricht von einem linearen $[n, k]$-Blockcode.*

Wenn $\mathcal{C}$ ein $[n, k]$-Blockcode ist, gibt es zwei lineare Abbildungen φ und ψ:

$$0 \longrightarrow \mathbb{F}^k \xrightarrow{\varphi} \mathbb{F}^n \xrightarrow{\psi} \mathbb{F}^{n-k} \longrightarrow 0$$

sodass $\mathcal{C} = \operatorname{im}(\varphi) = \ker(\psi)$. Wir nennen φ einen Encoder und ψ einen Syndromformer.

Lineare Blockcodes

Definition

Sei $\mathbb{F}$ ein endlicher Körper (oder allgemeiner ein endlicher Ring). Ein linearer Blockcode *ist ein linearer k-dimensionaler Unterraum $\mathcal{C} \subset \mathbb{F}^n$. Man spricht von einem linearen $[n, k]$-Blockcode.*

Wenn $\mathcal{C}$ ein $[n, k]$-Blockcode ist, gibt es zwei lineare Abbildungen φ und ψ:

$$0 \longrightarrow \mathbb{F}^k \xrightarrow{\varphi} \mathbb{F}^n \xrightarrow{\psi} \mathbb{F}^{n-k} \longrightarrow 0$$

sodass $\mathcal{C} = \operatorname{im}(\varphi) = \ker(\psi)$. Wir nennen φ einen Encoder und ψ einen Syndromformer.

In Bezug auf Matrizen kann φ durch eine $k \times n$-Matrix G und ψ durch eine $(n-k) \times n$-Matrix H dargestellt werden. Es gilt $HG^t = 0$.

Lineare Blockcodes

Lemma

Für einen linearen Code $\mathcal{C} \subset \mathbb{F}^n$ *gilt*

$$d(\mathcal{C}) := \min\{d(x,0) \mid x \in \mathcal{C}, x \neq 0\}.$$

Lineare Blockcodes

Lemma

Für einen linearen Code $\mathcal{C} \subset \mathbb{F}^n$ gilt

$$d(\mathcal{C}) := \min\{d(x,0) \mid x \in \mathcal{C}, x \neq 0\}.$$

Beweis.

$$d(x,y) := d(x-y,0)$$

□

Lineare Blockcodes

Lemma

Für einen linearen Code $\mathcal{C} \subset \mathbb{F}^n$ gilt

$$d(\mathcal{C}) := \min\{d(x,0) \mid x \in \mathcal{C}, x \neq 0\}.$$

Beweis.

$$d(x,y) := d(x-y,0)$$

□

Bemerkung

Für allgemeine Blockcodes müssen $\binom{|\mathcal{C}|}{n}$ Hamming-Distanzen für die Berechnung von $d(\mathcal{C})$ berechnet werden.

Lineare Blockcodes

Lemma

Für einen linearen Code $\mathcal{C} \subset \mathbb{F}^n$ gilt

$$d(\mathcal{C}) := \min\{d(x,0) \mid x \in \mathcal{C}, x \neq 0\}.$$

Beweis.

$$d(x,y) := d(x-y,0)$$

□

Bemerkung

Für allgemeine Blockcodes müssen $\binom{|\mathcal{C}|}{n}$ Hamming-Distanzen für die Berechnung von $d(\mathcal{C})$ berechnet werden.

Lemma

In Bezug auf die Paritätsprüfmatrix H ist die Distanz:

$$d(\mathcal{C}) = \min\{l \mid \exists l \text{ linear abhängige Spalten von } H\}.$$

ASCII-Code:

Grundkörper: $\mathbb{F} = \mathbb{Z}_2 = \{0, 1\}$.

ASCII-Code:

Grundkörper: $\mathbb{F} = \mathbb{Z}_2 = \{0, 1\}$.

$$\mathcal{C} = \{x \in \mathbb{F}^8 \mid \sum_{i=1}^{10} x_i = 0\}.$$

ASCII-Code:

Grundkörper: $\mathbb{F} = \mathbb{Z}_2 = \{0, 1\}$.

$$\mathcal{C} = \{x \in \mathbb{F}^8 \mid \sum_{i=1}^{10} x_i = 0\}.$$

Eine Paritätsprüfmatrix ist $H = (1, 1, \ldots, 1)$.

ASCII-Code:

Grundkörper: $\mathbb{F} = \mathbb{Z}_2 = \{0, 1\}$.

$$\mathcal{C} = \{x \in \mathbb{F}^8 \mid \sum_{i=1}^{10} x_i = 0\}.$$

Eine Paritätsprüfmatrix ist $H = (1, 1, \ldots, 1)$.

Die Kardinalität $|\mathcal{C}|$ ist 128.

ASCII-Code:

Grundkörper: $\mathbb{F} = \mathbb{Z}_2 = \{0, 1\}$.

$$\mathcal{C} = \{x \in \mathbb{F}^8 \mid \sum_{i=1}^{10} x_i = 0\}.$$

Eine Paritätsprüfmatrix ist $H = (1, 1, \ldots, 1)$.

Die Kardinalität $|\mathcal{C}|$ ist 128.

Die Distanz ist 2.

ASCII-Code:

Grundkörper: $\mathbb{F} = \mathbb{Z}_2 = \{0, 1\}$.

$$\mathcal{C} = \{x \in \mathbb{F}^8 \mid \sum_{i=1}^{10} x_i = 0\}.$$

Eine Paritätsprüfmatrix ist $H = (1, 1, \ldots, 1)$.

Die Kardinalität $|\mathcal{C}|$ ist 128.

Die Distanz ist 2.

Folglich kann bis zu einem Fehler erkannt werden. Im Allgemeinen können keine Fehler korrigiert werden.

ISBN Code:

Definition

(ISBN-Code)

$$\mathcal{C} = \{x \in \mathbb{F}_{11}^{10} \mid \sum_{i=1}^{10} i x_i \equiv 0 \ mod\ 11\}$$

ISBN Code:

Definition

(ISBN-Code)

$$\mathcal{C} = \{x \in \mathbb{F}_{11}^{10} \mid \sum_{i=1}^{10} i x_i \equiv 0 \ mod\ 11\}$$

ISBN Code:

Definition

(ISBN-Code)

$$\mathcal{C} = \{x \in \mathbb{F}_{11}^{10} \mid \sum_{i=1}^{10} i x_i \equiv 0 \ mod\ 11\}$$

Hier: $H = (1, 2, \ldots, 9, 10)$ ist eine Paritätsprüfmatrix, die Distanz $d(\mathcal{C}) = 2$ und die Mächtigkeit $|\mathcal{C}|$ ist 11^9.

Bekannte Blockcodes:

Bemerkung

Es gibt eine große Theorie für die Konstruktion sowie für die Decodierung von linearen Blockcodes.

Bekannte Blockcodes:

Bemerkung

Es gibt eine große Theorie für die Konstruktion sowie für die Decodierung von linearen Blockcodes.

Wohlbekannte lineare Blockcodes sind:

- Zyklische Codes
- Reed-Solomon-Codes
- Hamming-Codes
- BCH-Codes
- Klassische und Geometrische Goppa-Codes.

Bekannte Blockcodes:

Bemerkung

Es gibt eine große Theorie für die Konstruktion sowie für die Decodierung von linearen Blockcodes.

Wohlbekannte lineare Blockcodes sind:

- Zyklische Codes
- Reed-Solomon-Codes
- Hamming-Codes
- BCH-Codes
- Klassische und Geometrische Goppa-Codes.

Für die Klasse der Goppa- und BCH-Codes bietet der **Berlekamp-Massey-Algorithmus** einen effizienten Decodierungsalgorithmus.

Binäre Hamming-Codes:

Definiere eine Paritätsprüfmatrix der Größe $r \times n$, deren Spalten aus allen nicht- Null Vektoren in $\mathbb{F}_2^r$ bestehen. Es gibt $n = 2^r - 1$ Spalten.

Definition

Der Code $\mathcal{C} = \ker H$ wird als Hamming-Code bezeichnet.

Binäre Hamming-Codes:

Definiere eine Paritätsprüfmatrix der Größe $r \times n$, deren Spalten aus allen nicht- Null Vektoren in $\mathbb{F}_2^r$ bestehen. Es gibt $n = 2^r - 1$ Spalten.

Definition

Der Code $\mathcal{C} = \ker H$ wird als Hamming-Code bezeichnet.

- $d(\mathcal{C}) = 3$, d.h. ein Fehler kann korrigiert werden.
- Hamming-Codes sind perfekt in dem Sinne, dass es keine anderen Blockcodes (linear oder nichtlinear) innerhalb von $\mathbb{F}^n$ mit einer Distanz von 3 und einer größeren Kardinalität als $|\mathcal{C}|$ gibt.
- Hamming-Codes sind leicht zu decodieren.

Beispiel eines Hamming-Codes:

$\mathbb{F} = \mathbb{Z}_2$ und $r = 3$:

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Beispiel eines Hamming-Codes:

$\mathbb{F} = \mathbb{Z}_2$ und $r = 3$:

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Wenn $y = x + e$ empfangen wird, dann ist $Hy = He$. Wenn kein Fehler aufgetreten ist, ist $Hy = 0$. Wenn ein Fehler aufgetreten ist, gibt Hy den Ort des Fehlers in binärer Darstellung an.

Syndrom-Decodierung:

Angenommen $x \in \mathcal{C} \subset \mathbb{F}^n$ wurde gesendet und

$$y = x + e \in \mathbb{F}^n$$

wurde empfangen. Wir nehmen an, dass der Fehlervektor e das Gewicht $\mathrm{wt}(e) < \frac{d(\mathcal{C})}{2}$ hat.

Syndrom-Decodierung:

Angenommen $x \in \mathcal{C} \subset \mathbb{F}^n$ wurde gesendet und

$$y = x + e \in \mathbb{F}^n$$

wurde empfangen. Wir nehmen an, dass der Fehlervektor e das Gewicht $\mathrm{wt}(e) < \frac{d(\mathcal{C})}{2}$ hat.

Hinweis: Die Syndrome erfüllen
$\psi(y) = \psi(x) + \psi(e) = \psi(e)$

Syndrom-Decodierung:

Angenommen $x \in \mathcal{C} \subset \mathbb{F}^n$ wurde gesendet und

$$y = x + e \in \mathbb{F}^n$$

wurde empfangen. Wir nehmen an, dass der Fehlervektor e das Gewicht $\mathrm{wt}(e) < \frac{d(\mathcal{C})}{2}$ hat.

Hinweis: Die Syndrome erfüllen
$\psi(y) = \psi(x) + \psi(e) = \psi(e)$

Schlussfolgerung: $e + \mathcal{C} = y + \mathcal{C}$ und e ist der Vektor mit dem kleinsten Gewicht innerhalb der Nebenklasse $y + \mathcal{C} \in \mathbb{F}^n/\mathcal{C}$.

Decodierungsalgorithmus:

Für jedes mögliche Syndrom $\psi(y) \in \mathbb{F}^{n-k}$ berechne den Vektor mit dem kleinsten Gewicht innerhalb von $y + \mathcal{C}$. Erstelle dann eine 'Look-up-Tabelle'. Wenn y empfangen wird, wird $\psi(y)$ berechnet und die Look-up-Tabelle liefert $e = y - x$ und somit x.

Decodierungsalgorithmus:

Für jedes mögliche Syndrom $\psi(y) \in \mathbb{F}^{n-k}$ berechne den Vektor mit dem kleinsten Gewicht innerhalb von $y + \mathcal{C}$. Erstelle dann eine 'Look-up-Tabelle'. Wenn y empfangen wird, wird $\psi(y)$ berechnet und die Look-up-Tabelle liefert $e = y - x$ und somit x.

Problem: Die Anzahl der möglichen Syndrome $|\mathbb{F}^{n-k}| = q^{n-k}$ sowie die Kardinalität $|y + \mathcal{C}| = |\mathcal{C}| = |\mathbb{F}|^k = q^k$ ist im Allgemeinen zu groß für die Erstellung einer praktischen Look-up-Tabelle.

MDS-Blockcodes:

Sei H eine $(n-k) \times n$-Matrix mit vollem Rang. Dann ist H die *Paritätsprüfmatrix* des $[n, k]$-Codes:

$$\mathcal{C} = \ker H = \{v \in \mathbb{F}^n \mid Hv = 0\}.$$

MDS-Blockcodes:

Sei H eine $(n-k) \times n$-Matrix mit vollem Rang. Dann ist H die *Paritätsprüfmatrix* des $[n, k]$-Codes:

$$\mathcal{C} = \ker H = \{v \in \mathbb{F}^n \mid Hv = 0\}.$$

Lemma

(Singleton) Ein linearer $[n, k]$-Code $\mathcal{C}$ hat höchstens die Distanz

$$d(\mathcal{C}) \leq n - k + 1. \tag{2}$$

MDS-Blockcodes:

Sei H eine $(n-k) \times n$-Matrix mit vollem Rang. Dann ist H die *Paritätsprüfmatrix* des $[n, k]$-Codes:

$$\mathcal{C} = \ker H = \{v \in \mathbb{F}^n \mid Hv = 0\}.$$

Lemma

(Singleton) Ein linearer $[n, k]$-Code $\mathcal{C}$ hat höchstens die Distanz

$$d(\mathcal{C}) \leq n - k + 1. \tag{2}$$

Bemerkung

Ein Code $\mathcal{C}$, der Gleichheit in (2) erreicht, wird MDS-Code genannt. H ist die Paritätsprüfmatrix eines MDS-Codes genau dann, wenn die Minoren voller Größe von H invertierbar sind.

Reed-Solomon-Konstruktion:

Sei $\mathbb{F}_{<k}[x]$ die Menge der Polynome vom Grad höchstens $k-1$. Dann ist ein Reed-Solomon-Code das Bild unter der Auswertungsabbildung:

$$\begin{aligned} ev : \mathbb{F}_{<k}[x] &\longrightarrow \mathbb{F}^n, \\ \phi(x) &\longmapsto (\phi(1), \phi(\alpha), \ldots, (\phi(\alpha^{n-1})). \end{aligned}$$

Reed-Solomon-Konstruktion:

Sei $\mathbb{F}_{<k}[x]$ die Menge der Polynome vom Grad höchstens $k-1$. Dann ist ein Reed-Solomon-Code das Bild unter der Auswertungsabbildung:

$$\begin{aligned} ev : \mathbb{F}_{<k}[x] &\longrightarrow \mathbb{F}^n, \\ \phi(x) &\longmapsto (\phi(1), \phi(\alpha), \ldots, (\phi(\alpha^{n-1})). \end{aligned}$$

Bemerkung

Die Grundidee hinter Goppas Konstruktion [Gop88, LG88] von algebraisch-geometrischen Codes ist: Ersetze $\mathbb{F}_{<k}[x]$ durch eine Menge von Funktionen, die auf einer algebraischen Kurve oder einer anderen Varietät definiert sind.

Beispiel: Ein-Fehler-korrigierender ISBN-Code:

$$\mathbb{F} = \mathbb{Z}_{11}.\ H := \begin{pmatrix} 1 & 2 & 3 & \dots & \dots & X \\ 1 & 2^2 & 3^2 & \dots & \dots & X^2 \end{pmatrix}.$$

Beispiel: Ein-Fehler-korrigierender ISBN-Code:

$$\mathbb{F} = \mathbb{Z}_{11}.\ H := \begin{pmatrix} 1 & 2 & 3 & \dots & \dots & X \\ 1 & 2^2 & 3^2 & \dots & \dots & X^2 \end{pmatrix}.$$

Angenommen $x \in \mathbb{F}^{10}$ wird gesendet und $y = x + e$ wird empfangen. Angenommen $e^t = (0, \dots, 0, e_i, 0, \dots, 0)$. Dann

$$Hy = He = \begin{pmatrix} ie_i \\ i^2 e_i \end{pmatrix} =: \begin{pmatrix} S_1 \\ S_2 \end{pmatrix}$$

i und e_i werden berechnet als:

$$i = \frac{S_2}{S_1} \text{ und } e_i = \frac{S_1^2}{S_2}.$$

Bemerkungen:

- Für einen linearen $[n, k]$-Blockcode, der nahe an die Kapazität herankommt, ist es wichtig, dass sowohl die Distanz als auch die Blockgrößen groß sind.

Bemerkungen:

- Für einen linearen $[n, k]$-Blockcode, der nahe an die Kapazität herankommt, ist es wichtig, dass sowohl die Distanz als auch die Blockgrößen groß sind.
- Die ‘Nearest-Neighbor’-Decodierung eines allgemeinen linearen Blockcodes ist ein NP-schweres Problem. [BMvT78]

Bemerkungen:

- Für einen linearen $[n, k]$-Blockcode, der nahe an die Kapazität herankommt, ist es wichtig, dass sowohl die Distanz als auch die Blockgrößen groß sind.
- Die 'Nearest-Neighbor'-Decodierung eines allgemeinen linearen Blockcodes ist ein NP-schweres Problem. [BMvT78]
- Es war immer das Ziel in der Blockcodierungstheorie, 'große Codes' zu finden, die eine 'gute Distanz' haben und die effizient decodiert werden könnten.

Low-Density-Parity-Check (LDPC) Codes

LDPC-Codes, eingeführt von Gallager [Gal62], sind eine Klasse von linearen Blockcodes, die durch eine dünnbesetzte Paritätsprüfmatrix H gekennzeichnet sind.

- LDPC-Codes können auch graphisch durch Tanner-Graphen dargestellt werden.

Low-Density-Parity-Check (LDPC) Codes

LDPC-Codes, eingeführt von Gallager [Gal62], sind eine Klasse von linearen Blockcodes, die durch eine dünnbesetzte Paritätsprüfmatrix H gekennzeichnet sind.

- LDPC-Codes können auch graphisch durch Tanner-Graphen dargestellt werden.
- LDPC-Codes bieten eine Leistung nahe der Kapazität und erlauben gleichzeitig implementierbare Decoder.

Low-Density-Parity-Check (LDPC) Codes

LDPC-Codes, eingeführt von Gallager [Gal62], sind eine Klasse von linearen Blockcodes, die durch eine dünnbesetzte Paritätsprüfmatrix H gekennzeichnet sind.

- LDPC-Codes können auch graphisch durch Tanner-Graphen dargestellt werden.
- LDPC-Codes bieten eine Leistung nahe der Kapazität und erlauben gleichzeitig implementierbare Decoder.
- Die Dünnbesetztheit von H macht Paritätsprüfungen einfach zu berechnen, da sie relativ wenige Argumente beinhalten.

LDPC-Beispiel

Sei C ein LDPC-Code, definiert durch die folgende Paritätsprüfmatrix H.

$H =$

$Paritaet \downarrow \backslash Bit \rightarrow$	x_0	x_1	x_2	x_3	x_4	x_5	x_6
p_0	1	0	0	1	0	1	1
p_1	1	1	0	0	1	0	1
p_2	1	1	1	0	0	1	0
p_3	0	1	1	1	0	0	1
p_4	1	0	1	1	1	0	0
p_5	0	1	0	1	1	1	0
p_6	0	0	1	0	1	1	1

$$cH^T = \mathbf{0} \Rightarrow (x_0, x_1, \ldots, x_6)H^T = \mathbf{0}$$

LDPC-Beispiel

Sei C ein LDPC-Code, definiert durch die folgende Paritätsprüfmatrix H.

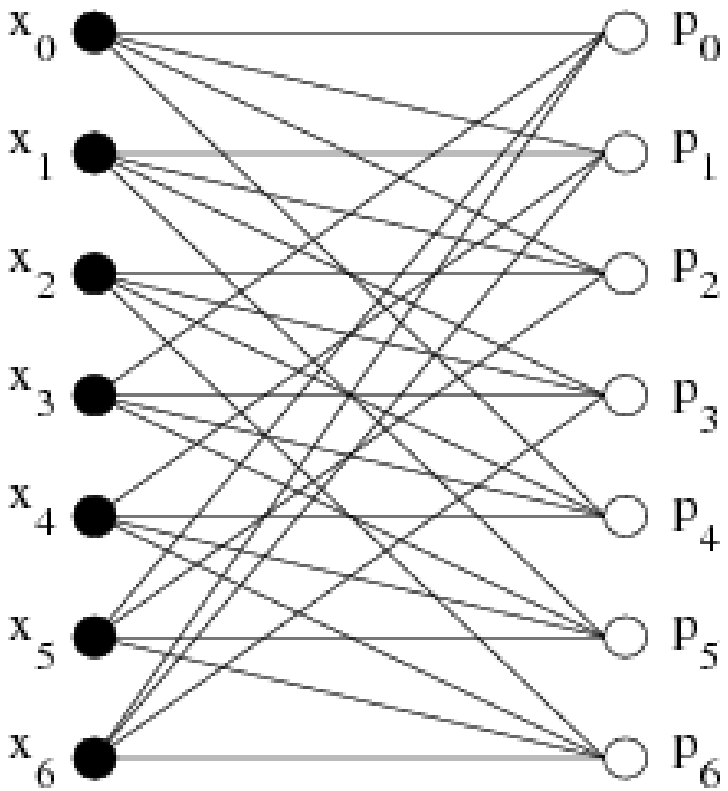
$H =$

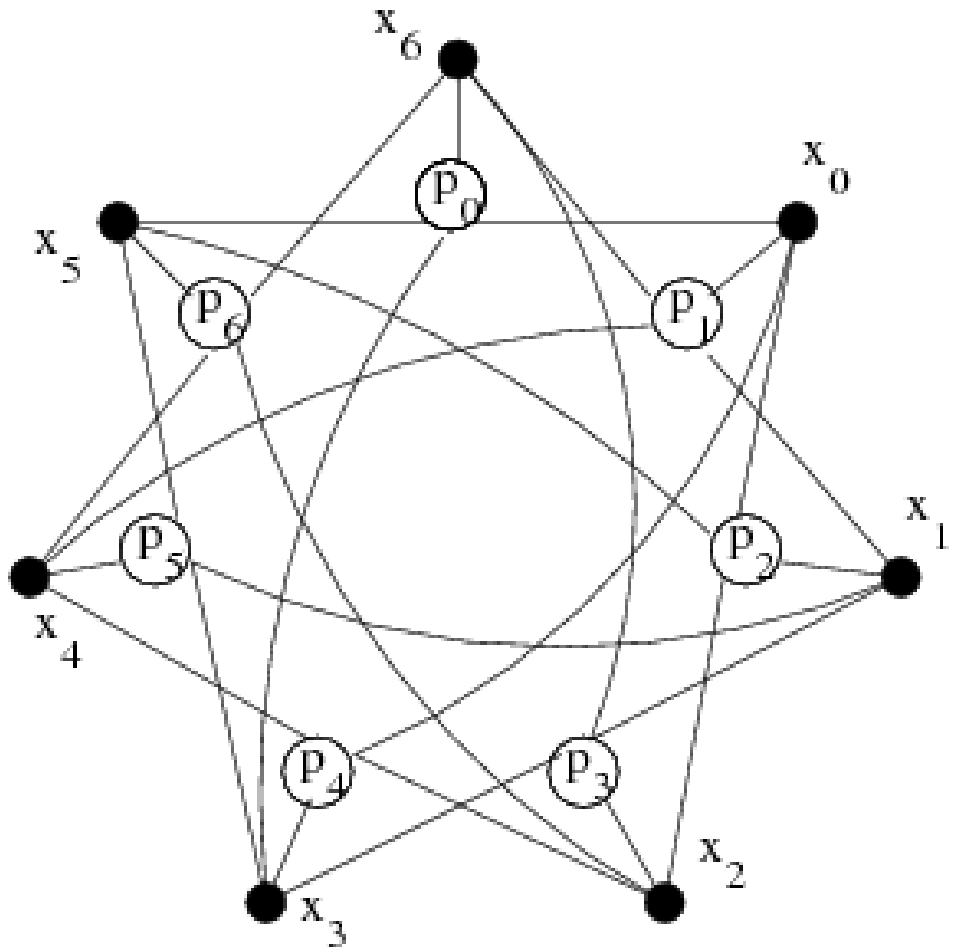
$Paritaet \downarrow \backslash Bit \rightarrow$	x_0	x_1	x_2	x_3	x_4	x_5	x_6
p_0	1	0	0	1	0	1	1
p_1	1	1	0	0	1	0	1
p_2	1	1	1	0	0	1	0
p_3	0	1	1	1	0	0	1
p_4	1	0	1	1	1	0	0
p_5	0	1	0	1	1	1	0
p_6	0	0	1	0	1	1	1

$$cH^T = \mathbf{0} \Rightarrow (x_0, x_1, \ldots, x_6)H^T = \mathbf{0}$$

Stellen Sie sich vor, sie wäre dünnbesetzt!

Darstellungen durch Tanner-Graphen





Arithmetik in endlichen Körpern:

$$\mathbb{F}_{101} := \{0, 1, 2, \ldots, 100\}$$

der endliche Körper mit $q = 101$ Elementen. Berechnen Sie von Hand:

1. $25 \times 36 - 49$.
2. 64^{-1}.
3. 81^{100}.

Hamming-Code [7,4] in Aktion:

Gegeben sei die Paritätsprüfmatrix H (Spalten binär aufsteigend sortiert):

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Sie empfangen das Wort $y = (1, 0, 1, 1, 0, 0, 0)$.

1. Berechnen Sie das Syndrom $S = Hy^T$.
2. An welcher Position liegt der Fehler? Wie lautet das korrigierte Codewort?

Zwerghut Problem 1:

Szenario: Es gibt 3 Zwerge. Jeder bekommt einen Hut aufgesetzt mit zufälliger Farbe, entweder Rot oder Blau.
Die Regeln: Jeder Zwerg sieht die Hüte der anderen, aber nicht seinen eigenen. Sie dürfen nicht kommunizieren. Alle müssen **gleichzeitig** eine Entscheidung treffen: "Rot", "Blau" oder "Ich passe".
Das Ziel: Die Gruppe gewinnt als Ganzes, wenn mindestens einer die Farbe korrekt rät und kein einziger falsch rät. (Wer passt, zählt nicht als falsch).
Entwickle eine Strategie die garantiert, dass die Gruppe mit Wahrscheinlichkeit $\frac{3}{4}$ gewinnt.

Zwerghut Problem 2:

Szenario: Es gibt 7 Zwerge. Jeder bekommt einen Hut aufgesetzt mit zufälliger Farbe, entweder Rot oder Blau.
Die Regeln: Jeder Zwerg sieht die Hüte der anderen, aber nicht seinen eigenen. Sie dürfen nicht kommunizieren. Die Zwerge sind erlaubt **sequentiell** zu antworten und müssen die eigene Farbe erraten. Jeder Zwerg muss eine Antwort geben, entweder "Rot" oder"Blau".
Das Ziel: Die Gruppe gewinnt als Ganzes, wenn jeder seine Farbe korrekt rät.
Entwickle eine Strategie die garantiert, dass die Gruppe mit Wahrscheinlichkeit $\frac{7}{8}$ gewinnt.

Zwerghut Problem 3:

Szenario: Es gibt n Zwerge. Jeder bekommt einen Hut aufgesetzt mit zufälliger Farbe, von k verschiedenen Farbmöglichkeiten.
Die Regeln: Jeder Zwerg sieht die Hüte der anderen, aber nicht seinen eigenen. Sie dürfen nicht kommunizieren. Die Zwerge sind erlaubt **sequentiell** zu antworten und müssen die eigene Farbe erraten. Jeder Zwerg muss eine Antwort geben.
Das Ziel: Die Gruppe gewinnt als Ganzes, wenn bis auf einen alle ihre Farbe korrekt erraten.
Entwickle eine Strategie die garantiert, dass die Gruppe gewinnt.

Entropie und Codierung:

Eine Wetterstation sendet jeden Tag einen Status: “Sonne” (50%), “Wolken” (25%), “Regen” (12.5%), “Schnee” (12.5%).

1. Berechnen Sie die Entropie $H(X)$ dieser Quelle.
2. Entwerfen Sie einen binären Code, dessen mittlere Wortlänge genau der Entropie entspricht.

MDS-Eigenschaft:

Betrachten Sie einen Code der Länge $n = 4$ über $\mathbb{F}_2$ mit nur zwei Codewörtern $\mathcal{C} = \{(0,0,0,0),(1,1,1,1)\}$.

1. Bestimmen Sie Dimension k und Minimaldistanz d.
2. Prüfen Sie mittels der Singleton-Schranke, ob dieser Code ein MDS-Code ist.

ISBN-13 Analyse:

Gegeben sei eine fehlerhafte ISBN-13, bei der zwei Ziffern vertauscht wurden: 978-3-03-02**50**42-5 (fiktives Beispiel). Die korrekte Sequenz an dieser Stelle wäre . . . **05** . . . . Zeigen Sie rechnerisch, dass das Prüfsummenverfahren (Gewichte 1, 3 modulo 10) diesen spezifischen Fehler (Vertauschung von 0 und 5 an benachbarter Position) *nicht* erkennen kann.

Tanner-Graph zeichnen:

Zeichnen Sie den Tanner-Graphen für folgende Paritätsprüfmatrix:

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Markieren Sie die Variablenknoten $x_1 \dots x_5$ und die Prüfknoten $p_1 \dots p_3$.

Vielen Dank für Ihre Aufmerksamkeit.

E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg.

On the inherent intractability of certain coding problems.

IEEE Trans. Information Theory, IT-24(3):384–386, 1978.

R.G. Gallager.

Low-density parity-check codes.

IRE Trans. on Info. Theory, IT-8:21–28, 1962.

V. D. Goppa.

Geometry and Codes.

Kluwer Academic Publisher, 1988.

D. A. Huffman.

A method for the construction of minimum redundancy codes.

Proc. IRE, 40:1098–1101, 1952.

J. H. van Lint and G. van der Geer.

Introduction to Coding Theory and Algebraic Geometry.

Birkhäuser Verlag, 1988.

C.E. Shannon.

A mathematical theory of communication.

Bell Syst. Tech. J., 27:379–423 and 623–656, 1948.

C. E. Shannon.

Communication theory of secrecy systems.

Bell System Tech. J., 28:656–715, 1949.

J. Ziv and A. Lempel.

A universal algorithm for sequential data compression.

IEEE Trans. Information Theory, IT-23(3):337–343, 1977.

J. Ziv and A. Lempel.

Compression of individual sequences via variable-rate coding.

IEEE Trans. Inform. Theory, 24(5):530–536, 1978.