# Ungleichungen von Kraft & McMillan Proseminar Informationstheorie

Phil Pützstück

October 28, 2018

Inhalt

Erinnerung: Bäume

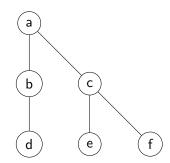
**Ungleichung von Kraft** 

# Motivation / Überblick

- Gesehen, dass uniquely decodable codes und instantenous codes sehr nützlich.
- ▶ Wann bzw. unter welchen Bedingungen existieren diese?
- ▶ Insbesondere: Wortlängen und Größe des Code-Alphabets
- Ungleichungen setzen diese Aspekte in Relation

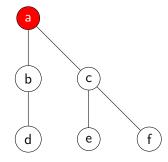
Baum T = (V, E). Knotenmenge V(T) := V. Kantenmenge E(T) := E.

- ungerichtet
- azyklisch
- zusammenhängend



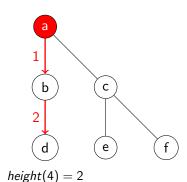
Baum T = (V, E). Knotenmenge V(T) := V. Kantenmenge E(T) := E.

- ungerichtet
- azyklisch
- zusammenhängend
- ▶ eindeutige Wurzel *root*(*T*)



Baum T = (V, E). Knotenmenge V(T) := V. Kantenmenge E(T) := E.

- ungerichtet
- azyklisch
- zusammenhängend
- eindeutige Wurzel root(T)
- ▶ Höhe  $height(v), v \in V$

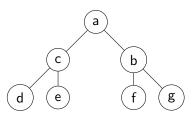


Baum T = (V, E). Knotenmenge V(T) := V. Kantenmenge E(T) := E.

- ungerichtet
- azyklisch
- zusammenhängend
- eindeutige Wurzel root(T)
- ▶ Höhe  $height(v), v \in V$

Nenne T r-är wenn jeder Knoten mit Ausnahme von Blättern genau  $r \in \mathbb{N}$  Kinder hat.

2-är bzw. binär



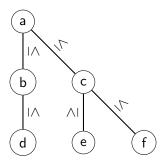
T, T' gewurzelte Bäume.

▶ Schreibe  $T' \leq T$  wenn T' Teilgraph von T.

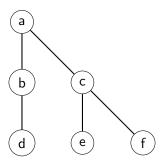
T, T' gewurzelte Bäume.

- ▶ Schreibe  $T' \leq T$  wenn T' Teilgraph von T.
- ▶ Schreibe  $T' \leq_r T$  wenn  $T' \leq T$  und T, T' r-är.

Für  $v, v' \in T$  schreiben wir  $v' \leq v$ , genau dann, wenn der eindeutige Pfad von root(T) zu v den Knoten v' besucht.

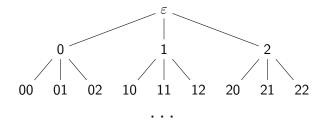


sub(v)?



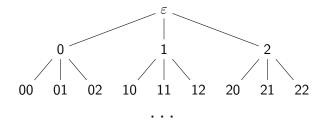
### Code als Baum

Sei C ein Code über dem Code-Alphabet  $\{0,1,2\}$ . C als Teilmenge von V(T), wobei T:



### Code als Baum

Sei C ein Code über dem Code-Alphabet  $\{0,1,2\}$ . C als Teilmenge von V(T), wobei T:



Inhalt

Erinnerung: Bäume

**Ungleichung von Kraft** 

Seien  $q, r \in \mathbb{N}, l \in \mathbb{N}^q$ . Dann existiert ein r-ärer instantaneous Code C mit Wortlängen l genau dann, wenn

$$\sum_{k=1}^{q} \frac{1}{r^{l_k}} \le 1$$

Seien  $q, r \in \mathbb{N}, l \in \mathbb{N}^q$ . Dann existiert ein r-ärer instantaneous Code C mit Wortlängen l genau dann, wenn

$$\sum_{k=1}^{q} \frac{1}{r^{l_k}} \le 1$$

#### Annahmen:

► Anzahl Code-Wörter *q* > 1

Seien  $q, r \in \mathbb{N}, l \in \mathbb{N}^q$ . Dann existiert ein r-ärer instantaneous Code  $\mathcal{C}$  mit Wortlängen l genau dann, wenn

$$\sum_{k=1}^{q} \frac{1}{r^{l_k}} \le 1$$

#### Annahmen:

- ► Anzahl Code-Wörter *q* > 1
- Nortlängen l aufsteigend sortiert und  $l_1 > 0$

Seien  $q, r \in \mathbb{N}, l \in \mathbb{N}^q$ . Dann existiert ein r-ärer instantaneous Code  $\mathcal{C}$  mit Wortlängen l genau dann, wenn

$$\sum_{k=1}^{q} \frac{1}{r^{l_k}} \le 1$$

#### Annahmen:

- ► Anzahl Code-Wörter *q* > 1
- Wortlängen / aufsteigend sortiert und  $l_1 > 0$
- ▶ Code-Alphabet von C ist [0, r-1]

Richtung " $\sum_{k=1}^{q} \frac{1}{r^{l_k}} \leq 1 \implies \mathcal{C}$  existiert".

Richtung " $\sum_{k=1}^{q} \frac{1}{r^{l_k}} \le 1 \implies \mathcal{C}$  existiert".

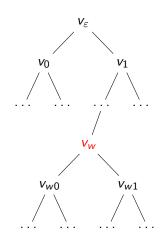
Nach [JJ00] sind die instantaneous Codes genau die Präfixcodes.

Richtung " $\sum_{k=1}^{q} \frac{1}{r_{l_k}} \le 1 \Longrightarrow \mathcal{C}$  existiert".

Nach [JJ00] sind die instantaneous Codes genau die Präfixcodes.

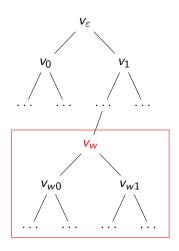
Konstuiere Codewörter  $w_i$  mit  $|w_i| = l_i$  via endlicher Induktion über i. Betrachte dabei den zum Code-Alphabet zug. Baum und wähle die  $w_i$  so, dass am Ende  $\mathcal{C} = \{w_i \mid i \in [1, q]\}$  ein Präfixcode ist.

Sei also i = 1. Wähle Knoten  $v_w$  der Höhe  $l_1 > 0$  beliebig und setze  $w_1 := w$ .



Sei also i = 1. Wähle Knoten  $v_w$  der Höhe  $l_1 > 0$  beliebig und setze  $w_1 := w$ .

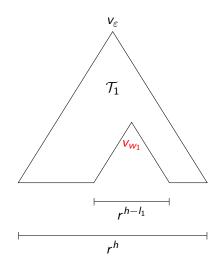
Setze  $h = I_q \text{ (max. Wortlänge)}$ und  $\mathcal{T}_1 := \mathcal{T}_r^h \setminus v_{w_1}$ .



Sei also i=1. Wähle Knoten  $v_w$  der Höhe  $l_1>0$  beliebig und setze  $w_1:=w$ .

Setze  $h = I_q$  (max. Wortlänge) und  $\mathcal{T}_1 := \mathcal{T}_r^h \setminus v_{w_1}$ .

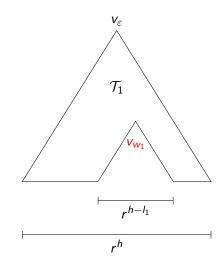
 $\mathcal{T}_1$  hat dann noch  $r^h - r^{h-l_1}$  Blätter.



 $\mathcal{T}_1$  hat dann noch  $r^h-r^{h-l_1}$  Blätter.

Weiter gilt:

$$r^h - r^{h-l_1} = r^h \left( 1 - \sum_{k=1}^1 \frac{1}{r^{l_k}} \right)$$

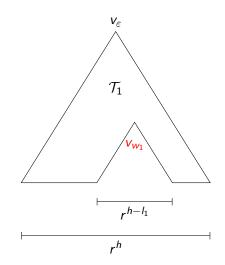


 $\mathcal{T}_1$  hat dann noch  $r^h - r^{h-l_1}$  Blätter.

Weiter gilt:

$$r^{h} - r^{h-l_{1}} = r^{h} \left( 1 - \sum_{k=1}^{1} \frac{1}{r^{l_{k}}} \right)$$

$$> r^{h} \left( 1 - \sum_{k=1}^{q} \frac{1}{r^{l_{k}}} \right)$$

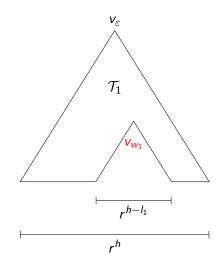


 $\mathcal{T}_1$  hat dann noch  $r^h-r^{h-l_1}$  Blätter.

Weiter gilt:

$$r^{h} - r^{h-l_{1}} = r^{h} \left( 1 - \sum_{k=1}^{1} \frac{1}{r^{l_{k}}} \right)$$

$$> r^{h} \left( 1 - \sum_{k=1}^{q} \frac{1}{r^{l_{k}}} \right) \ge 0$$

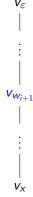


Sei nun  $i \in [1, q-1]$  sodass  $\mathcal{C} = \{w_j \mid j \in [1, i]\}$  ein Präfix-Code mit  $|w_j| = l_j$  ist, und  $\mathcal{T}_i$  noch mindestens 1 Blatt  $v_x$  hat.

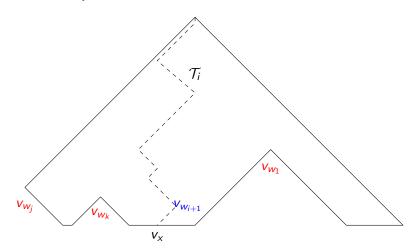


Sei nun  $i \in [1, q-1]$  sodass  $\mathcal{C} = \{w_j \mid j \in [1, i]\}$  ein Präfix-Code mit  $|w_j| = l_j$  ist, und  $\mathcal{T}_i$  noch mindestens 1 Blatt  $v_x$  hat.

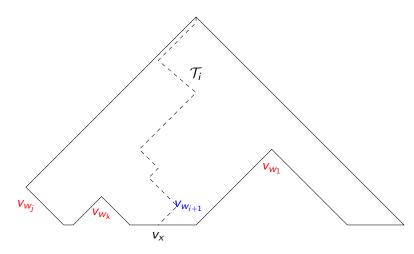
- $ightharpoonup \mathcal{T}_i$  zusammenhängend
- ▶ also ex.  $v_w \in V(\mathcal{T}_i)$  mit  $height(v_w) = l_{i+1} \le h$
- ightharpoonup Setze  $w_{i+1} := w$ .



Sei  $j \in [1,i]$ . Wir haben bereits alle Knoten  $v_w \ge v_{w_j}$  im Schritt  $\mathcal{T}_j := \mathcal{T}_{j-1} \setminus v_{w_j}$  gelöscht. Da wir  $v_{w_{i+1}}$  aus  $\mathcal{T}_i$  gewählt haben, kann also **nicht**  $v_{w_i} \le v_{w_{i+1}}$  gelten.



Folglich haben wir auch  $w_j \not\sqsubseteq w_{i+1}$  für  $j \in [1, i]$ .  $\mathcal{C}$  bleibt also durch Wahl von  $w_{i+1}$  ein Präfix-Code  $(l_j \leq l_{i+1}, \text{ also } w_{i+1} \not\sqsubseteq w_j)$ .



Folglich haben wir auch  $w_j \not\sqsubseteq w_{i+1}$  für  $j \in [1, i]$ .  $\mathcal{C}$  bleibt also durch Wahl von  $w_{i+1}$  ein Präfix-Code  $(I_j \leq I_{i+1}$ , also  $w_{i+1} \not\sqsubseteq w_j)$ .

Wenn nun i+1=q war, so sind wir fertig, da wir das letzte Wort  $w_q$  soeben  $\mathcal C$  hinzugefügt haben.

Folglich haben wir auch  $w_j \not\sqsubseteq w_{i+1}$  für  $j \in [1, i]$ .  $\mathcal{C}$  bleibt also durch Wahl von  $w_{i+1}$  ein Präfix-Code  $(l_j \leq l_{i+1}$ , also  $w_{i+1} \not\sqsubseteq w_j)$ .

Wenn nun i+1=q war, so sind wir fertig, da wir das letzte Wort  $w_q$  soeben  $\mathcal C$  hinzugefügt haben.

Falls hingegen i+1 < q, so definiere  $\mathcal{T}_{i+1} := \mathcal{T}_i \setminus v_{w_{i+1}}$ . Dann hat  $\mathcal{T}_{i+1}$  immernoch mindestens 1 Blatt, denn:

$$\mathcal{T}_i$$
 hat nach Konstruktion  $r^h - \sum_{l=1}^i r^{h-l_k}$  Blätter

Folglich haben wir auch  $w_j \not\sqsubseteq w_{i+1}$  für  $j \in [1, i]$ .  $\mathcal C$  bleibt also durch Wahl von  $w_{i+1}$  ein Präfix-Code  $(l_j \le l_{i+1}$ , also  $w_{i+1} \not\sqsubseteq w_j)$ .

Wenn nun i+1=q war, so sind wir fertig, da wir das letzte Wort  $w_q$  soeben  $\mathcal C$  hinzugefügt haben.

Falls hingegen i+1 < q, so definiere  $\mathcal{T}_{i+1} := \mathcal{T}_i \setminus v_{w_{i+1}}$ . Dann hat  $\mathcal{T}_{i+1}$  immernoch mindestens 1 Blatt, denn:  $\mathcal{T}_{i+1}$  hat nach Konstruktion also:

$$r^h - \sum_{k=1}^{i+1} r^{h-l_k}$$

Folglich haben wir auch  $w_j \not\sqsubseteq w_{i+1}$  für  $j \in [1, i]$ .  $\mathcal C$  bleibt also durch Wahl von  $w_{i+1}$  ein Präfix-Code  $(l_j \leq l_{i+1}$ , also  $w_{i+1} \not\sqsubseteq w_j)$ .

Wenn nun i+1=q war, so sind wir fertig, da wir das letzte Wort  $w_q$  soeben  $\mathcal C$  hinzugefügt haben.

Falls hingegen i+1 < q, so definiere  $\mathcal{T}_{i+1} := \mathcal{T}_i \setminus v_{w_{i+1}}$ . Dann hat  $\mathcal{T}_{i+1}$  immernoch mindestens 1 Blatt, denn:  $\mathcal{T}_{i+1}$  hat nach Konstruktion also:

$$r^h - \sum_{k=1}^{i+1} r^{h-l_k} > r^h - \sum_{k=1}^{q} r^{h-l_k}$$

Folglich haben wir auch  $w_j \not\sqsubseteq w_{i+1}$  für  $j \in [1, i]$ .  $\mathcal C$  bleibt also durch Wahl von  $w_{i+1}$  ein Präfix-Code  $(l_j \le l_{i+1}$ , also  $w_{i+1} \not\sqsubseteq w_j)$ .

Wenn nun i+1=q war, so sind wir fertig, da wir das letzte Wort  $w_q$  soeben  $\mathcal C$  hinzugefügt haben.

Falls hingegen i+1 < q, so definiere  $\mathcal{T}_{i+1} := \mathcal{T}_i \setminus v_{w_{i+1}}$ . Dann hat  $\mathcal{T}_{i+1}$  immernoch mindestens 1 Blatt, denn:  $\mathcal{T}_{i+1}$  hat nach Konstruktion also:

$$r^h - \sum_{k=1}^{i+1} r^{h-l_k} > r^h - \sum_{k=1}^{q} r^{h-l_k} = r^h \left( 1 - \sum_{k=1}^{q} \frac{1}{r^{l_k}} \right)$$

Folglich haben wir auch  $w_j \not\sqsubseteq w_{i+1}$  für  $j \in [1, i]$ .  $\mathcal{C}$  bleibt also durch Wahl von  $w_{i+1}$  ein Präfix-Code  $(l_j \leq l_{i+1}$ , also  $w_{i+1} \not\sqsubseteq w_j)$ .

Wenn nun i+1=q war, so sind wir fertig, da wir das letzte Wort  $w_q$  soeben  $\mathcal C$  hinzugefügt haben.

Falls hingegen i+1 < q, so definiere  $\mathcal{T}_{i+1} := \mathcal{T}_i \setminus v_{w_{i+1}}$ . Dann hat  $\mathcal{T}_{i+1}$  immernoch mindestens 1 Blatt, denn:  $\mathcal{T}_{i+1}$  hat nach Konstruktion also:

$$r^{h} - \sum_{k=1}^{i+1} r^{h-l_k} > r^{h} - \sum_{k=1}^{q} r^{h-l_k} = r^{h} \left( 1 - \sum_{k=1}^{q} \frac{1}{r^{l_k}} \right) \ge 0$$

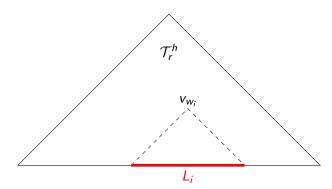
Blätter. Somit können wir einen Präfix-Code  $\mathcal C$  unter den gegebenen Bedingungen konstruieren. Dieser ist nach [JJ00] auch instantaneous.

Nun zeigen wir, dass wenn  $\mathcal C$  instantaneous, also ein Präfix-Code ist, auch die Ungleichung gelten muss.

Nun zeigen wir, dass wenn  $\mathcal C$  instantaneous, also ein Präfix-Code ist, auch die Ungleichung gelten muss.

Betrachte für  $i \in [1, q]$  die Menge der Blätter unter  $v_{w_i}$ :

$$L_i := \{ v \in V(\mathcal{T}_r^h) \mid v_{w_i} \leq v \land height(v) = h \}$$



Wir wissen nun, dass für i,j mit  $i \neq j$  auch  $L_i \cap L_j = \varnothing$  gelten muss

Wir wissen nun, dass für i, j mit  $i \neq j$  auch  $L_i \cap L_j = \emptyset$  gelten muss

Sei o.E.  $i < j, v_w \in L_i \cap L_j$ , also  $v_w$  gleichzeitig Blatt unter  $v_{w_i}$  und  $v_{w_j}$ .

Wir wissen nun, dass für i, j mit  $i \neq j$  auch  $L_i \cap L_j = \emptyset$  gelten muss

Sei o.E.  $i < j, v_w \in L_i \cap L_j$ , also  $v_w$  gleichzeitig Blatt unter  $v_{w_i}$  und  $v_{w_j}$ . Dann gilt:

$$v_{w_i} \leq v_w \wedge v_{w_j} \leq v_w$$

Wir wissen nun, dass für i, j mit  $i \neq j$  auch  $L_i \cap L_j = \emptyset$  gelten muss

Sei o.E.  $i < j, v_w \in L_i \cap L_j$ , also  $v_w$  gleichzeitig Blatt unter  $v_{w_i}$  und  $v_{w_j}$ . Dann gilt:

$$v_{w_i} \le v_w \land v_{w_j} \le v_w \implies w_i \sqsubseteq w \land w_j \sqsubseteq w$$

Wir wissen nun, dass für i, j mit  $i \neq j$  auch  $L_i \cap L_j = \emptyset$  gelten muss

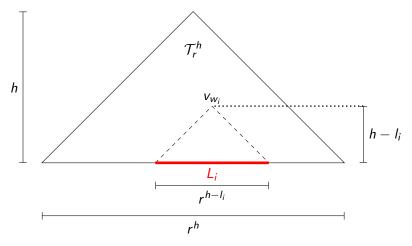
Sei o.E.  $i < j, v_w \in L_i \cap L_j$ , also  $v_w$  gleichzeitig Blatt unter  $v_{w_i}$  und  $v_{w_j}$ . Dann gilt:

$$v_{w_i} \leq v_w \wedge v_{w_j} \leq v_w \implies w_i \sqsubseteq w \wedge w_j \sqsubseteq w \implies w_i \sqsubseteq w_j$$

Widerpruch, denn  $w_i, w_j \in \mathcal{C}$  und  $\mathcal{C}$  ist Präfix-Code!

Wir wissen nun, dass für i,j mit  $i \neq j$  auch  $L_i \cap L_j = \varnothing$  gelten muss

Wir wissen weiter, dass  $\mathcal{T}_r^h$  nur  $r^h$  Blätter hat, und  $|L_i| = r^{h-l_i}$ .



Wir wissen nun, dass für i, j mit  $i \neq j$  auch  $L_i \cap L_j = \emptyset$  gelten muss

Wir wissen weiter, dass  $\mathcal{T}_r^h$  nur  $r^h$  Blätter hat, und  $|L_i| = r^{h-l_i}$ .

$$r^h \ge \left| \bigcup_{i \in [1,q]} L_i \right|$$

Wir wissen nun, dass für i,j mit  $i \neq j$  auch  $L_i \cap L_j = \emptyset$  gelten muss

Wir wissen weiter, dass  $\mathcal{T}_r^h$  nur  $r^h$  Blätter hat, und  $|L_i| = r^{h-l_i}$ .

$$r^h \ge \left| \bigcup_{i \in [1,q]} L_i \right| = \sum_{i=1}^q |L_i|$$

Wir wissen nun, dass für i, j mit  $i \neq j$  auch  $L_i \cap L_j = \emptyset$  gelten muss

Wir wissen weiter, dass  $\mathcal{T}_r^h$  nur  $r^h$  Blätter hat, und  $|L_i| = r^{h-l_i}$ .

$$r^h \ge \left| \bigcup_{i \in [1,q]} L_i \right| = \sum_{i=1}^q |L_i| = \sum_{i=1}^q r^{h-l_i} = r^h \sum_{i=1}^q \frac{1}{r^{l_i}}$$

Wir wissen nun, dass für i, j mit  $i \neq j$  auch  $L_i \cap L_j = \emptyset$  gelten muss

Wir wissen weiter, dass  $\mathcal{T}^h_r$  nur  $r^h$  Blätter hat, und  $|L_i| = r^{h-l_i}$ .

$$r^h \ge \left| \bigcup_{i \in [1,q]} L_i \right| = \sum_{i=1}^q |L_i| = \sum_{i=1}^q r^{h-l_i} = r^h \sum_{i=1}^q \frac{1}{r^{l_i}}$$

Wir wissen nun, dass für i, j mit  $i \neq j$  auch  $L_i \cap L_j = \emptyset$  gelten muss

Wir wissen weiter, dass  $\mathcal{T}_r^h$  nur  $r^h$  Blätter hat, und  $|L_i| = r^{h-l_i}$ .

Damit haben wir nun:

$$r^h \ge \left| igcup_{i \in [1,q]} L_i 
ight| = \sum_{i=1}^q |L_i| = \sum_{i=1}^q r^{h-l_i} = r^h \sum_{i=1}^q rac{1}{r^{l_i}}$$
 $\iff \sum_{i=1}^q rac{1}{r^{l_i}} \le 1$ 

Dies war zu zeigen.