Ungleichungen von Kraft & McMillan Proseminar Informationstheorie

Phil Pützstück

November 4, 2018

Inhalt

Bäume

Ungleichung von Kraft

Ungleichung von McMillan

Motivation

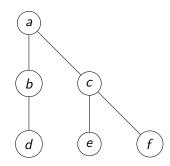
- Gesehen, dass eindeutig bzw. sofort dekodierbare Codes sehr nützlich sind.
- Wann bzw. unter welchen Bedingungen existieren diese?
- ▶ Insbesondere: Wortlängen und Größe des Code-Alphabets
- Ungleichungen setzen diese Aspekte in Relation

Überblick

- ► Graphen und Bäume: Wiederholung und Definitionen
- Zusammenhang Codes und Bäume
- Ungleichung von Kraft
- Ungleichung von McMillan
- ► Intepretationen / Ausblick

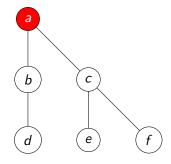
Baum T = (V, E). Knotenmenge V(T) := V. Kantenmenge E(T) := E.

- ungerichtet
- azyklisch
- zusammenhängend



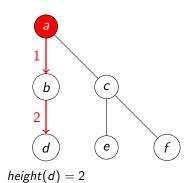
Baum T = (V, E). Knotenmenge V(T) := V. Kantenmenge E(T) := E.

- 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 $height(v), v \in V$

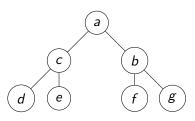


Baum T = (V, E). Knotenmenge V(T) := V. Kantenmenge E(T) := E.

- 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



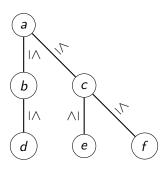
T, T' gewurzelte Bäume.

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

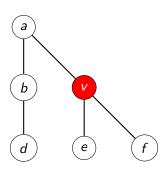
T, T' gewurzelte Bäume.

- ▶ Schreibe $T' \leq T$ wenn T' Teilgraph von T.
- ▶ Schreibe $T' \leq_r T$ wenn $T' \leq T$ und T, T' r- $\ddot{a}r$.

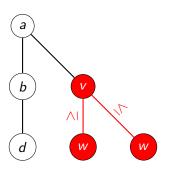
Für $v, v' \in T$ schreiben wir $v' \leq v$, genau dann, wenn der eindeutige Pfad von root(T) zu v den Knoten v' besucht. Hier root(T) = a



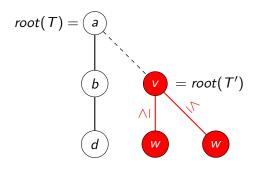
Sei $root(T) \neq v \in V(T)$. Wir wollen v und seine "Nachfolger" $w \in V(T), v \leq w$ von T inklusive Kanten "ausschneiden".



Sei $root(T) \neq v \in V(T)$. Wir wollen v und seine "Nachfolger" $w \in V(T), v \leq w$ von T inklusive Kanten "ausschneiden".



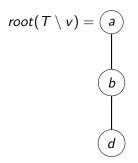
Sei $root(T) \neq v \in V(T)$. Wir wollen v und seine "Nachfolger" $w \in V(T), v \leq w$ von T inklusive Kanten "ausschneiden".



Definiere $T \setminus v := T \setminus T'$, wobei $T' \leq T$ der Teilbaum von T mit Wurzel $v \in V(T) \setminus \{root(T)\}$ ist.

Insbesondere ist $T \setminus v$ wieder ein gewurzelter Baum.

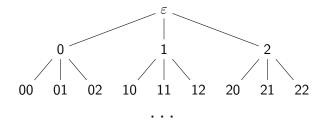
Sei $root(T) \neq v \in V(T)$. Wir wollen v und seine "Nachfolger" $w \in V(T), v \leq w$ von T inklusive Kanten "ausschneiden".



Definiere $T \setminus v := T \setminus T'$, wobei $T' \leq T$ der Teilbaum von T mit Wurzel $v \in V(T) \setminus \{root(T)\}$ ist. Insbesondere ist $T \setminus v$ wieder ein gewurzelter Baum.

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

Seien $h,r\in\mathbb{N}$, A:=[0,r-1] das Code-Alphabet eines r-ären Codes $\mathcal C$ mit maximaler Wortlänge $h\in\mathbb{N}$. Dann ist $W:=\bigcup_{i\in[0,h]}A^i$ die Menge aller Wörter über A mit maximaler Länge h. Definiere gewurzelten r-ären Baum $\mathcal T^h_r$ der Höhe h durch:

$$V(\mathcal{T}_r^h) := \{v_w \mid w \in W\}$$

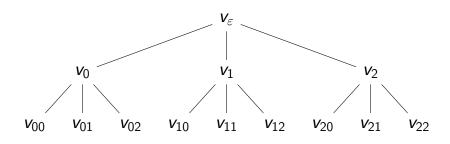
$$E(\mathcal{T}_r^h) := \{(v_w, v_{w'}) \mid w, w' \in W, wx = w', x \in A\}$$

$$root(\mathcal{T}_r^h) := v_{\varepsilon}$$

Insbesondere \mathcal{T}_r^h eindeutig durch r,h bestimmt. (Bis auf Bijektionen des Code-Alphabets).

Bemerkungen zu \mathcal{T}_r^h

Betrachte \mathcal{T}_3^2 :

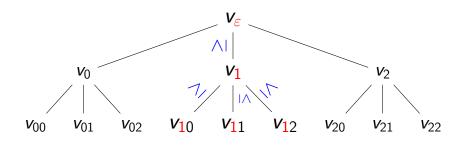


Wir haben:

▶ Für $v_w \in V(\mathcal{T}_r^h)$ gilt $height(v_w) = |w|$.

Bemerkungen zu \mathcal{T}_r^h

Betrachte \mathcal{T}_3^2 :



Wir haben:

- ▶ Für $v_w \in V(\mathcal{T}_r^h)$ gilt $height(v_w) = |w|$.
- Für $v_w, v_{w'} \in V(\mathcal{T}_r^h)$ gilt $v_w \leq v_{w'} \iff w \sqsubseteq w'$.

Inhalt

Bäume

Ungleichung von Kraft

Ungleichung von McMillan

Seien $q, r \in \mathbb{N}, l \in \mathbb{N}^q$. Dann existiert ein r-ärer sofort dekodierbarer 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 sofort dekodierbarer 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 sofort dekodierbarer 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
- Nortlängen l aufsteigend sortiert und $l_1 > 0$

Seien $q, r \in \mathbb{N}, l \in \mathbb{N}^q$. Dann existiert ein r-ärer sofort dekodierbarer 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
- Wortlängen / aufsteigend sortiert und $l_1 > 0$
- ▶ Code-Alphabet von C ist [0, r-1]

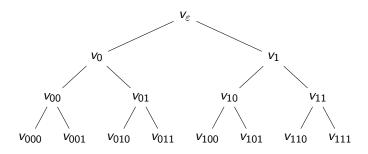
Richtung " $\sum_{k=1}^{q} \frac{1}{r^{l_k}} \leq 1 \implies \mathcal{C}$ existiert".

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

Nach [JJ00]: \mathcal{C} sofort dekodierbar $\iff \mathcal{C}$ Präfixcode. Am Beispiel q=3, r=2, l=(1,2,3). Betrachte \mathcal{T}_2^3 :

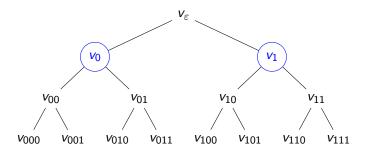
Richtung " $\sum_{k=1}^{q} \frac{1}{r_{k}} \leq 1 \implies \mathcal{C}$ existiert".

Nach [JJ00]: \mathcal{C} sofort dekodierbar $\iff \mathcal{C}$ Präfixcode. Am Beispiel q=3, r=2, l=(1,2,3). Betrachte \mathcal{T}_2^3 :



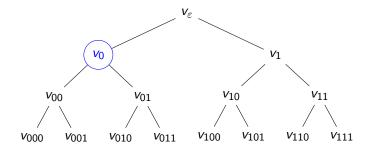
Richtung " $\sum_{k=1}^{q} \frac{1}{r_{k}} \leq 1 \implies \mathcal{C}$ existiert".

Nach [JJ00]: \mathcal{C} sofort dekodierbar $\iff \mathcal{C}$ Präfixcode. Am Beispiel q=3, r=2, l=(1,2,3). Betrachte \mathcal{T}_2^3 :



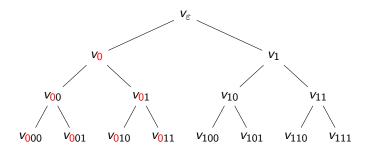
Richtung " $\sum_{k=1}^{q} \frac{1}{r^{l_k}} \le 1 \implies \mathcal{C}$ existiert".

Nach [JJ00]: \mathcal{C} sofort dekodierbar $\iff \mathcal{C}$ Präfixcode. Am Beispiel q=3, r=2, l=(1,2,3). Betrachte $\mathcal{T}_2^3:$ $w_1=0$,



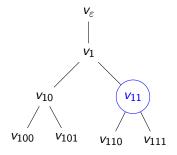
Richtung " $\sum_{k=1}^{q} \frac{1}{r_{l_k}} \le 1 \Longrightarrow \mathcal{C}$ existiert".

Nach [JJ00]: \mathcal{C} sofort dekodierbar $\iff \mathcal{C}$ Präfixcode. Am Beispiel q=3, r=2, l=(1,2,3). Betrachte \mathcal{T}_2^3 : $w_1=0$,



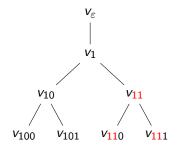
Richtung " $\sum_{k=1}^{q} \frac{1}{r^{l_k}} \leq 1 \implies \mathcal{C}$ existiert".

Nach [JJ00]: \mathcal{C} sofort dekodierbar $\iff \mathcal{C}$ Präfixcode. Am Beispiel q=3, r=2, l=(1,2,3). Betrachte $\mathcal{T}_2^3 \setminus v_0$: $w_1=0, w_2=11$,



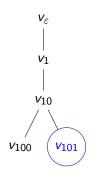
Richtung " $\sum_{k=1}^{q} \frac{1}{r_{l_k}} \le 1 \Longrightarrow \mathcal{C}$ existiert".

Nach [JJ00]: \mathcal{C} sofort dekodierbar $\iff \mathcal{C}$ Präfixcode. Am Beispiel q=3, r=2, l=(1,2,3). Betrachte $\mathcal{T}_2^3 \setminus v_0$: $w_1=0, \ w_2=11$,



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

Nach [JJ00]: \mathcal{C} sofort dekodierbar $\iff \mathcal{C}$ Präfixcode. Am Beispiel q=3, r=2, l=(1,2,3). Betrachte $(\mathcal{T}_2^3 \setminus v_0) \setminus v_{11}$: $w_1=0, \ w_2=11, \ w_3=101$



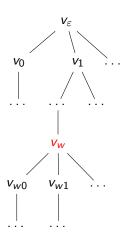
Richtung " $\sum_{k=1}^{q} \frac{1}{r^{l_k}} \leq 1 \implies \mathcal{C}$ existiert".

Nach [JJ00]: $\mathcal C$ sofort dekodierbar $\iff \mathcal C$ Präfixcode. Am Beispiel q=3, r=2, l=(1,2,3). $w_1=0, w_2=11, w_3=101$

- q = 3 Wörter über Alphabet $[0, r 1] = [0, 1] = \{0, 1\}.$
- ▶ Wortlängen $|w_1| = I_1$, $|w_2| = I_2$, $|w_3| = I_3$ eingehalten.
- ▶ Präfixcode $C = \{w_1, w_2, w_3\} = \{0, 11, 101\}$ konstruiert.

Ungleichung von Kraft: "⇒"

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

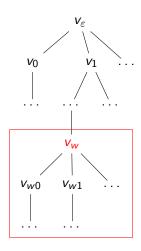


Ungleichung von Kraft: " \Longrightarrow "

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

Setze $h := I_q$ (max. Wortlänge) und $\mathcal{T}_0 := \mathcal{T}_r^h$, $\mathcal{T}_1 := \mathcal{T}_r^h \setminus v_{w_1}$.

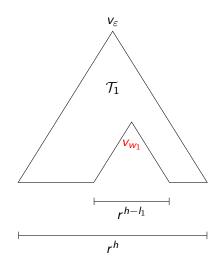
 \mathcal{T}_r^h :



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

Setze $h := I_q$ (max. Wortlänge) und $\mathcal{T}_0 := \mathcal{T}_r^h$, $\mathcal{T}_1 := \mathcal{T}_r^h \setminus v_{w_1}$.

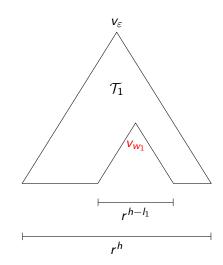
 \mathcal{T}_1 hat dann noch $r^h - r^{h-l_1}$ Blätter.



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

Weiter gilt:

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

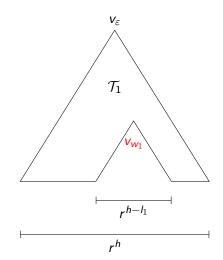


 \mathcal{T}_1 hat dann noch $r^h - r^{h-l_1}$ Blätter.

Weiter gilt:

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

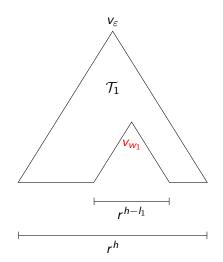
$$> r^{h} \left(1 - \sum_{l=1}^{q} \frac{1}{r^{l_{k}}} \right)$$



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

Weiter gilt:

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

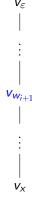


Sei nun $i \in [1, q-1]$ sodass $\mathcal{C} = \{w_j \mid j \in [1, i]\}$ ein Präfix-Code mit $|w_j| = l_j$ ist, und \mathcal{T}_i noch mindestens 1 Blatt v_x hat.

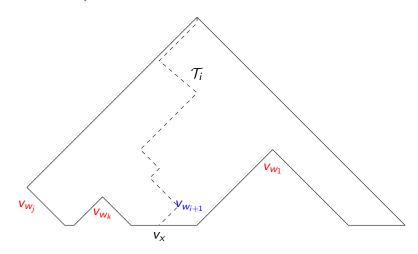


Sei nun $i \in [1, q-1]$ sodass $\mathcal{C} = \{w_j \mid j \in [1, i]\}$ ein Präfix-Code mit $|w_j| = l_j$ ist, und \mathcal{T}_i noch mindestens 1 Blatt v_x hat.

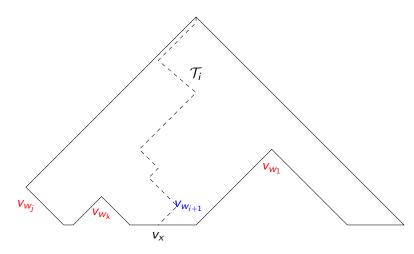
- $ightharpoonup \mathcal{T}_i$ zusammenhängend
- ▶ also ex. $v_w \in V(\mathcal{T}_i)$ mit $height(v_w) = I_{i+1} \leq h$
- ightharpoonup Setze $w_{i+1} := w$.



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 $r^h - \sum_{k=1}^i r^{h-l_k}$ 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 $(l_j \le l_{i+1}$, 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:

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

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:

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

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:

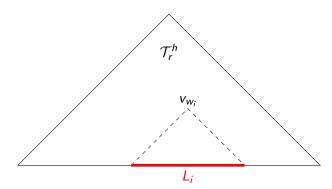
$$r^{h} - \sum_{k=1}^{i+1} r^{h-l_k} > r^{h} - \sum_{k=1}^{q} r^{h-l_k} = r^{h} \left(1 - \sum_{k=1}^{q} \frac{1}{r^{l_k}} \right) \ge 0$$

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

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

Nun zeigen wir, dass wenn C sofort dekodierbar, 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:

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

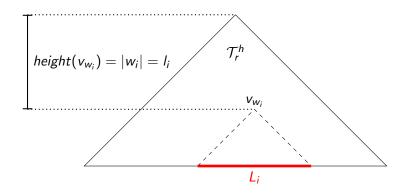
Wir wissen nun, dass für i,j mit $i \neq j$ auch $L_i \cap L_j = \emptyset$ gelten muss

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:

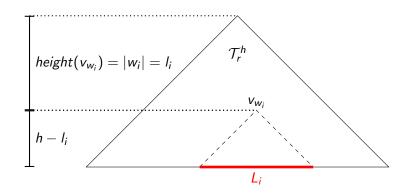
$$v_{w_i} \leq v_w \wedge v_{w_j} \leq v_w \implies w_i \sqsubseteq w \wedge w_j \sqsubseteq w \implies w_i \sqsubseteq w_j$$

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

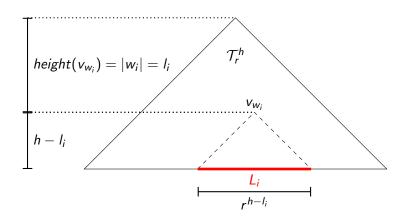
Wir wissen nun, dass für i,j mit $i \neq j$ auch $L_i \cap L_j = \emptyset$ gelten muss Wir wissen weiter, dass \mathcal{T}_r^h nur r^h Blätter hat, und $|L_i| = r^{h-l_i}$.



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 $|L_i| = r^{h-l_i}$.



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 $|L_i| = r^{h-l_i}$.



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}_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}_r^h nur r^h Blätter hat, und $|L_i| = r^{h-l_i}$.

Damit haben wir nun:

$$egin{aligned} r^h &\geq \left| igcup_{i \in [1,q]} L_i
ight| = \sum_{i=1}^q |L_i| = \sum_{i=1}^q r^{h-l_i} = r^h \sum_{i=1}^q rac{1}{r^{l_i}} \ &\iff \sum_{i=1}^q rac{1}{r^{l_i}} \leq 1 \end{aligned}$$

Dies war zu zeigen.

Review of Kraft or smth.

Wir haben also gezeigt [...]

- Nach [JJ00] bekannt, dass sofort dekodierbar ⇒ eindeutig dekodierbar
- ▶ Jedoch vorraussetzungen für letzteres **nicht** schwächer:

Inhalt

Bäume

Ungleichung von Kraft

Ungleichung von McMillan

Ungleichung von McMillan

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

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

Ungleichung von McMillan

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

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

Richtung " $(1) \Longrightarrow \mathcal{C}$ existiert" folgt sofort mit Kraft.

Ungleichung von McMillan: Beweisidee

▶ Zu zeigen: $K := \sum_{k=1}^{q} \frac{1}{r^{l_k}} \le 1$

Ungleichung von McMillan: Beweisidee

- ▶ Zu zeigen: $K := \sum_{k=1}^{q} \frac{1}{r^{l_k}} \le 1$
- ▶ Betrachte K^n für beliebiges $n \in \mathbb{N}$.

Ungleichung von McMillan: Beweisidee

- ▶ Zu zeigen: $K := \sum_{k=1}^{q} \frac{1}{r^{l_k}} \le 1$
- ▶ Betrachte K^n für beliebiges $n \in \mathbb{N}$.
- $ightharpoonup K^n$ als Summe abhängig von Wahl von n Wortlängen aus l.

- ightharpoonup Zu zeigen: $K := \sum_{k=1}^{q} \frac{1}{r^{l_k}} \le 1$
- ▶ Betrachte K^n für beliebiges $n \in \mathbb{N}$.
- $ightharpoonup K^n$ als Summe abhängig von Wahl von n Wortlängen aus l.
- ► Fasse Auswahlen (Indextupel) mit selbem Summand zusammen und summiere über möglichen Wertebereich

- ightharpoonup Zu zeigen: $K := \sum_{k=1}^q \frac{1}{r'_k} \le 1$
- ▶ Betrachte K^n für beliebiges $n \in \mathbb{N}$.
- $ightharpoonup K^n$ als Summe abhängig von Wahl von n Wortlängen aus l.
- ► Fasse Auswahlen (Indextupel) mit selbem Summand zusammen und summiere über möglichen Wertebereich
- ▶ Nun finde aus Form von Kⁿ konstante obere Schranke

- ightharpoonup Zu zeigen: $K := \sum_{k=1}^q \frac{1}{r'_k} \le 1$
- ▶ Betrachte K^n für beliebiges $n \in \mathbb{N}$.
- $ightharpoonup K^n$ als Summe abhängig von Wahl von n Wortlängen aus l.
- ► Fasse Auswahlen (Indextupel) mit selbem Summand zusammen und summiere über möglichen Wertebereich
- \triangleright Nun finde aus Form von K^n konstante obere Schranke
- ▶ Dann muss $K \le 1$, da sonst K^n für geeignetes n größer als jede Konstante

Wir müssen also zeigen, dass $K \leq 1$, wobei

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

Wir müssen also zeigen, dass $K \leq 1$, wobei

$$K = \sum_{l=1}^{q} \frac{1}{r^{l_k}}$$

Sei $n \in \mathbb{N}$. Wir betrachten:

$$K^n = \left(\sum_{k=1}^q \frac{1}{r^{l_k}}\right)^n$$

Wir müssen also zeigen, dass $K \leq 1$, wobei

$$K = \sum_{l=1}^{q} \frac{1}{r^{l_k}}$$

Sei $n \in \mathbb{N}$. Wir betrachten:

$$K^{n} = \left(\sum_{k=1}^{q} \frac{1}{r^{l_{k}}}\right)^{n} = \sum_{i \in [1, q]^{n}} \prod_{k=1}^{n} \frac{1}{r^{l_{i_{k}}}}$$

Wir müssen also zeigen, dass K < 1, wobei

$$K = \sum_{l=1}^{q} \frac{1}{r^{l_k}}$$

Sei $n \in \mathbb{N}$. Wir betrachten:

$$K^{n} = \left(\sum_{k=1}^{q} \frac{1}{r^{l_{k}}}\right)^{n} = \sum_{i \in [1, q]^{n}} \prod_{k=1}^{n} \frac{1}{r^{l_{i_{k}}}} = \sum_{i \in [1, q]^{n}} r^{-\sum_{k=1}^{n} l_{i_{k}}}$$

Wir müssen also zeigen, dass $K \leq 1$, wobei

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

Sei $n \in \mathbb{N}$. Wir betrachten:

$$K^{n} = \left(\sum_{k=1}^{q} \frac{1}{r^{l_{k}}}\right)^{n} = \sum_{i \in [1,q]^{n}} \prod_{k=1}^{n} \frac{1}{r^{l_{i_{k}}}} = \sum_{i \in [1,q]^{n}} r^{-\sum_{k=1}^{n} l_{i_{k}}}$$

Werden Summe über Auswahl an Wortlängen noch oft brauchen, definiere:

$$\mathcal{S}:[1,q]^n o \mathbb{N}, \ i \mapsto \sum_{i=1}^n I_{i_k}$$

Anzahl Codewörter q=3. Wortlängen l=(1,3,5). n=2.

$$[1,q]^n = \{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3)\}$$

$$i = (3,1) \in [1,q]^n \implies S(i) = \sum_{k=1}^n l_{i_k} = l_{i_1} + l_{i_2} = l_3 + l_1 = 5 + 1$$

$$i = (2,3) \in [1,q]^n \implies S(i) = \sum_{k=1}^n l_{i_k} = l_2 + l_3 = 3 + 5$$

$$i = (2,2) \in [1,q]^n \implies S(i) = \sum_{k=1}^n l_{i_k} = l_2 + l_2 = 3 + 3$$

Anzahl Codewörter q=3. Wortlängen I=(1,3,5). n=2.

$$[1,q]^n = \{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3)\}$$

$$i = (3,1) \in [1,q]^n \implies S(i) = \sum_{k=1}^n l_{i_k} = l_{i_1} + l_{i_2} = l_3 + l_1 = 5 + 1 = 6$$

$$i = (2,3) \in [1,q]^n \implies S(i) = \sum_{k=1}^n l_{i_k} = l_2 + l_3 = 3 + 5$$

$$i = (2,2) \in [1,q]^n \implies S(i) = \sum_{k=1}^n l_{i_k} = l_2 + l_2 = 3 + 3 = 6$$

Also auch selber Wert bei unterschiedlichen Indextupeln.

Anzahl Codewörter q = 3. Wortlängen I = (1, 3, 5). n = 2.

- Summe minimal 3, maximal 15.
- Fasse Indextupel mit gleicher Summe $j \in [3, 15]$ zusammen

$$N_6 := S^{-1}(\{6\}) = \{i \in [1,3]^2 \mid S(i) = 6\} = \{\underbrace{(1,3)}_{l_1 + l_3 = 6}, \underbrace{(3,1)}_{l_2 + l_2 = 6}, \underbrace{(2,2)}_{l_2 + l_2 = 6}\}$$

Anzahl Codewörter q = 3. Wortlängen l = (1, 3, 5). n = 2.

- ► Summe minimal 3, maximal 15.
- Fasse Indextupel mit gleicher Summe $j \in [3, 15]$ zusammen

$$N_6 := S^{-1}(\{6\}) = \{i \in [1,3]^2 \mid S(i) = 6\} = \{\underbrace{(1,3)}_{l_1 + l_3 = 6}, \underbrace{(3,1)}_{l_2 + l_2 = 6}, \underbrace{(2,2)}_{l_2 + l_2 = 6}\}$$

$$N_{j} := S^{-1}(j) = \{i \in [1, q]^{n} \mid S(i) = \sum_{k=1}^{n} I_{i_{k}} = j\}$$

Anzahl Codewörter q = 3. Wortlängen l = (1, 3, 5). n = 2.

▶ Betrachte Alphabet [0,1], $C = \{\underbrace{0}_{1100},\underbrace{100}_{1100},\underbrace{11111}_{1100}\}$

Anzahl Codewörter q = 3. Wortlängen I = (1, 3, 5). n = 2.

- $\blacktriangleright \ \, \mathsf{Betrachte} \ \, \mathsf{Alphabet} \ \, [0,1], \mathcal{C} = \{\underbrace{0}_{w_1},\underbrace{100}_{w_2},\underbrace{11111}_{w_3}\}$
- ightharpoonup Zu $i \in [1,q]^n$ eindeutige Code-Sequenz $\mathcal{W}(i) = w_{i_1}w_{i_2}\cdots w_{i_n}$.

Anzahl Codewörter q=3. Wortlängen l=(1,3,5). n=2.

- $\blacktriangleright \ \, \mathsf{Betrachte} \ \, \mathsf{Alphabet} \ \, [0,1], \mathcal{C} = \{\underbrace{0}_{w_1}, \underbrace{100}_{w_2}, \underbrace{11111}_{w_3}\}$
- ightharpoonup Zu $i \in [1,q]^n$ eindeutige Code-Sequenz $\mathcal{W}(i) = w_{i_1}w_{i_2}\cdots w_{i_n}$.

$$\mathcal{W}(N_6) = \{\mathcal{W}(t) \mid t \in N_6\} = \{\mathcal{W}(t) \mid t \in \{(1,3), (3,1), (2,2)\}\}$$
$$= \{w_1 w_3, w_3 w_1, w_2 w_2\} = \{011111, 111110, 100100\}$$

Anzahl Codewörter q=3. Wortlängen l=(1,3,5). n=2.

- ▶ Betrachte Alphabet [0,1], $\mathcal{C} = \{\underbrace{0}_{w_1},\underbrace{100}_{w_2},\underbrace{11111}_{w_3}\}$
- ightharpoonup Zu $i \in [1,q]^n$ eindeutige Code-Sequenz $\mathcal{W}(i) = w_{i_1}w_{i_2}\cdots w_{i_n}$.

$$\mathcal{W}(N_6) = \{\mathcal{W}(t) \mid t \in N_6\} = \{\mathcal{W}(t) \mid t \in \{(1,3), (3,1), (2,2)\}\}$$
$$= \{w_1w_3, w_3w_1, w_2w_2\} = \{011111, 111110, 100100\}$$

Da N_6 gerade die Indextupel Wortlängensumme 6:

$$\forall i \in N_6 : |\mathcal{W}(i)| = 6$$
 und $\mathcal{W}(N_6) \subseteq \{0,1\}^6$

Kürzeste Wortlänge $m:=\min_{k\in[1,q]}I_k$, längste $M:=\max_{k\in[1,q]}I_k$

Kürzeste Wortlänge $m:=\min_{k\in[1,q]}I_k$, längste $M:=\max_{k\in[1,q]}I_k$ Damit gilt auch

$$n \cdot m \leq S(i) = \sum_{k=1}^{n} I_{i_k} \leq n \cdot M$$

für alle Indextupel $i \in [1, q]^n$.

Kürzeste Wortlänge $m:=\min_{k\in[1,q]}I_k$, längste $M:=\max_{k\in[1,q]}I_k$ Damit gilt auch

$$n \cdot m \leq S(i) = \sum_{k=1}^{n} I_{i_k} \leq n \cdot M$$

für alle Indextupel $i \in [1, q]^n$. Definiere für $j \in [nm, nM]$:

$$N_j := S^{-1}(j) = \{i \in [1, q]^n \mid S(i) = \sum_{k=1}^n I_{i_k} = j\}$$

Kürzeste Wortlänge $m:=\min_{k\in[1,q]} I_k$, längste $M:=\max_{k\in[1,q]} I_k$ Damit gilt auch

$$n \cdot m \leq S(i) = \sum_{k=1}^{n} I_{i_k} \leq n \cdot M$$

für alle Indextupel $i \in [1, q]^n$. Definiere für $j \in [nm, nM]$:

$$N_j := S^{-1}(j) = \{i \in [1, q]^n \mid S(i) = \sum_{k=1}^n I_{i_k} = j\}$$

$$W: [1,q]^n \to [0,r-1]^*, i \mapsto w_{i_1}w_{i_2}\cdots w_{i_n}$$

Kürzeste Wortlänge $m:=\min_{k\in[1,q]} I_k$, längste $M:=\max_{k\in[1,q]} I_k$ Damit gilt auch

$$n \cdot m \leq S(i) = \sum_{k=1}^{n} I_{i_k} \leq n \cdot M$$

für alle Indextupel $i \in [1, q]^n$. Definiere für $j \in [nm, nM]$:

$$N_j := S^{-1}(j) = \{i \in [1, q]^n \mid S(i) = \sum_{k=1}^n I_{i_k} = j\}$$

$$W: [1,q]^n \to [0,r-1]^*, i \mapsto w_{i_1}w_{i_2}\cdots w_{i_n}$$

 \mathcal{C} eindeutig dekodierbar $\Longrightarrow \mathcal{W}$ injektiv, da $i \in [1, q]^n$ die eindeutige Kombination von Codewörtern aus \mathcal{C} für $\mathcal{W}(i)$.

 $j \in [nm, nM]$ zwischen min / max Wortlängensumme.

$$N_j := \mathcal{S}^{-1}(j), \quad \mathcal{W} : [1,q]^n \to [0,r-1]^*, \ i \mapsto w_{i_1}w_{i_2}\cdots w_{i_n}$$

 $ightharpoonup \mathcal{W}$ injektiv $\Longrightarrow |N_j| = |\mathcal{W}(N_j)|$

 $j \in [nm, nM]$ zwischen min / max Wortlängensumme.

$$N_j := S^{-1}(j), \quad \mathcal{W} : [1, q]^n \to [0, r-1]^*, \ i \mapsto w_{i_1} w_{i_2} \cdots w_{i_n}$$

- $ightharpoonup \mathcal{W}$ injektiv $\Longrightarrow |N_i| = |\mathcal{W}(N_i)|$
- ▶ $|\mathcal{W}(i)| = j$ für $i \in N_j$ nach Konstruktion

 $j \in [nm, nM]$ zwischen min / max Wortlängensumme.

$$N_j := S^{-1}(j), \quad \mathcal{W} : [1, q]^n \to [0, r - 1]^*, \ i \mapsto w_{i_1} w_{i_2} \cdots w_{i_n}$$

- $ightharpoonup \mathcal{W}$ injektiv $\Longrightarrow |N_i| = |\mathcal{W}(N_i)|$
- ▶ $|\mathcal{W}(i)| = j$ für $i \in N_j$ nach Konstruktion
- $\qquad \mathcal{W}(N_j) \subseteq [0, r-1]^j \implies |\mathcal{W}(N_j)| \le |[0, r-1]^j|$

 $j \in [nm, nM]$ zwischen min / max Wortlängensumme.

$$N_j := S^{-1}(j), \quad \mathcal{W} : [1,q]^n \to [0,r-1]^*, \ i \mapsto w_{i_1} w_{i_2} \cdots w_{i_n}$$

- $ightharpoonup \mathcal{W}$ injektiv $\Longrightarrow |N_j| = |\mathcal{W}(N_j)|$
- ▶ |W(i)| = j für $i \in N_j$ nach Konstruktion
- $\blacktriangleright \ \mathcal{W}(N_j) \subseteq [0,r-1]^j \implies |\mathcal{W}(N_j)| \le |[0,r-1]^j|$
- $|N_j| \leq r^j$

Recap:

$$K := \sum_{i=1}^{q} \frac{1}{r^{l_i}}$$

$$K^n = \sum_{i \in [1,q]^n} r^{-\sum_{k=1}^n l_{i_k}} = \sum_{i \in [1,q]^n} r^{-S(i)}$$

$$K := \sum_{i=1}^{q} \frac{1}{r^{l_i}}$$

$$K^n = \sum_{i \in [1,q]^n} r^{-\sum_{k=1}^n l_{i_k}} = \sum_{i \in [1,q]^n} r^{-S(i)}$$

▶ $|N_j| \le r^j$ Anzahl der $i \in [1, q]^n$ mit gleichem S(i).

$$K := \sum_{i=1}^{q} \frac{1}{r^{l_i}}$$

$$K^n = \sum_{i \in [1,q]^n} r^{-\sum_{k=1}^n l_{i_k}} = \sum_{i \in [1,q]^n} r^{-S(i)}$$

- ▶ $|N_j| \le r^j$ Anzahl der $i \in [1, q]^n$ mit gleichem S(i).
- Fasse zusammen via N_j , summiere über [nm, nM]

$$K^{n} = \sum_{j=nm}^{nM} |N_{j}| r^{-j} = \sum_{j=nm}^{nM} \frac{|N_{j}|}{r^{j}}$$

$$K := \sum_{i=1}^{q} \frac{1}{r^{l_i}}$$

$$K^n = \sum_{i \in [1,q]^n} r^{-\sum_{k=1}^n l_{i_k}} = \sum_{i \in [1,q]^n} r^{-S(i)}$$

- ▶ $|N_j| \le r^j$ Anzahl der $i \in [1, q]^n$ mit gleichem S(i).
- Fasse zusammen via N_j , summiere über [nm, nM]

$$K^{n} = \sum_{j=nm}^{nM} |N_{j}| r^{-j} = \sum_{j=nm}^{nM} \frac{|N_{j}|}{r^{j}} \leq \sum_{j=nm}^{nM} 1 = (M-m)n + 1$$

$$K:=\sum_{i=1}^q rac{1}{r^{l_i}}, \quad K^n \leq (M-m)n+1$$

$$K:=\sum_{i=1}^{q}\frac{1}{r^{l_i}},\quad K^n\leq (M-m)n+1\implies \frac{K^n}{n}\leq (M-m)+1$$

- ▶ Code C gegeben; q = |C|, Alphabetgröße r, Wortlängen I fix.
- ▶ Damit auch m, M, K fix.
- ▶ $n \in \mathbb{N}$ beliebig; Ungleichung muss für alle $n \in \mathbb{N}$ gelten.

$$\mathcal{K} := \sum_{i=1}^{q} \frac{1}{r^{l_i}}, \quad \mathcal{K}^n \leq (M-m)n+1 \implies \frac{\mathcal{K}^n}{n} \leq (M-m)+1$$

- ▶ Code C gegeben; q = |C|, Alphabetgröße r, Wortlängen I fix.
- ▶ Damit auch *m*, *M*, *K* fix.
- ▶ $n \in \mathbb{N}$ beliebig; Ungleichung muss für alle $n \in \mathbb{N}$ gelten.
- Nach Analysis bekannt: nur möglich für $K \leq 1$.

$$\implies \sum_{i=1}^{q} \frac{1}{r^{l_i}} = K \le 1$$

Review of McMillan or smth.

[...]