1 Codes

1.1 Ordnungen auf X^*

Es sei $X = \{a_1, \ldots, a_r\}$ ein gemäß $a_1 < a_2 < \ldots < a_r$ geordnetes Alphabet.

Definition 1.1 Lexikographische Ordnung

$$w <_{lex} v \quad :\Leftrightarrow \quad \begin{cases} w \sqsubset v & \text{, oder} \\ \exists u \exists i \exists j (i < j \wedge u a_i \sqsubseteq w \wedge u a_j \sqsubseteq v) & . \end{cases}$$

Definition 1.2 Quasilexikographische Ordnung

$$w <_{ql} v \quad :\Leftrightarrow \quad \begin{cases} |w| < |v| & \text{, oder} \\ |w| = |v| \text{ und } w <_{lex} v & . \end{cases}$$

Eigenschaften

Es sei $X = \{0, \ldots, r-1\}$ ein in der natürlichen Ordnung geordnetes Alphabet, und wir setzen $0.w := \sum_{i=1}^{|w|} x_i \cdot r^{-i} \in \mathbb{R}$ für $w = x_1 \cdots x_{|w|},\ x_i \in X$. Dann gelten

1. Aus $w \leq_{lex} v$ folgt $0.w \leq 0.v$.
2. $w <_{lex} v \iff 0.w < 0.v$ für $v \notin X^* \cdot 0$, und
3. $w <_{lex} v \iff (0.w < 0.v \vee v \in w \cdot 0 \cdot 0^*)$
   $\iff (0.w < 0.v \vee w \sqsubset v)$ für $w, v \in \{0, \ldots, r-1\}^*$.
4. Aus $w \sqsubseteq v$ folgt $0 \leq 0.v - 0.w \leq r^{-|w|} - r^{-|v|}$, und
5. $w \sqsubseteq v \iff 0 \leq 0.v - 0.w \leq r^{-|w|} - r^{-|v|}$ für $v \notin X^* \cdot 0$.

1.2 Codes

Definition 1.3 [Code]
Eine Sprache $C \subseteq X^*$ heißt *(eindeutig decodierbarer) Code* : $\Longleftrightarrow$
Für Wörter $w_1, \ldots, w_n, v_1, \ldots, v_m$ folgen aus $w_1 \cdots w_n = v_1 \cdots v_m$ stets $n = m$ und $w_i = v_i$.

Definition 1.4 [Codierung]
Eine Abbildung $\varphi : Y \to X^*$ heißt *(eindeutig decodierbare, verlustfreie) Codierung* : $\Longleftrightarrow$

1. φ ist eineindeutig, und
2. das Bild $\varphi(Y)$ ist ein eindeutig decodierbarer Code.

Satz 1.1 (Ungleichung von *Kraft*) *Es seien* $r = |X|$ *und* $(\ell_i)_{i\in I}$ $(I \subseteq \mathbb{N}_+)$ *mit* $\ell_1 \le \ell_2 \le \ldots$ *eine endliche oder unendliche Familie von natürlichen Zahlen mit der Eigenschaft* $\sum_{i\in I} r^{-\ell_i} \le 1$. *Dann gibt es einen Präfixcode* $C = \{w_i : i \in I\}$ *mit* $|w_i| = \ell_i$.

Algorithmus KRAFT $(\ell_1, \ell_2, \ldots)$;; $\ell_1 \le \ell_2 \le \ldots$, $n = |I|$

$i := 0$, $\ell_0 := 0$, $M_0 := \{e\}$, $C_0 := \emptyset$

While $i \neq n$ do

$i := i + 1$

$M := M_{i-1} \cdot X^{\ell_i - \ell_{i-1}}$

$w_i :=$ erstes Wort in der lexikographischen Ordnung von M

$C_i := C_{i-1} \cup \{w_i\}$, $M_i := M \setminus \{w_i\}$

Endwhile

Output $C := C_n$

Definition 1.5 [Bernoulli-Maß]
Ein Bernoulli Maß auf X^* ist eine Abbildung $\mu : X^* \to [0,1]$ die die folgenden Bedingungen erfüllt:

1. $\sum_{a \in X} \mu(a) = 1$, und
2. $\forall w, v (w, v \in X^* \to \mu(w \cdot v) = \mu(w) \cdot \mu(v))$.

Folgerung 1.2 *Ist μ Bernoulli-Maß auf X^*, so gelten*

1. $\mu(e) = 1$, *und*
2. $\mu(W \cdot V) \leq \mu(W) \cdot \mu(V)$, *wobei für $\prod_{a \in X} \mu(a) > 0$ und $\mu(W), \mu(V) < \infty$ die Gleichheit genau dann eintritt, wenn jedes $u \in W \cdot V$ genau eine Faktorisierung $u = w \cdot v$ mit $w \in W$ und $v \in V$ hat.*

Satz 1.3 (Satz von MacMillan) *Ist μ ein Bernoulli-Maß auf X^*, so gilt für jeden Code $C \subseteq X^*$ die Beziehung $\mu(C) \leq 1$.*

1.3 Präfix-Codes und Bäume

Definition 1.6 [r-verzweigter Wurzelbaum]
Ein *höchstens* r*-verzweigter Wurzelbaum* kann interpretiert werden als präfixabgeschlossene Teilmenge $W \subseteq \{0, 1, \ldots, r-1\}^*$ mit der Wurzel $e \in \{0, 1, \ldots, r-1\}^*$ und den Nachfolgern $w \cdot i$ $(i \in M_w \subseteq \{0, 1, \ldots, r-1\})$ des Knotens $w \in \{0, 1, \ldots, r-1\}^*$.

Wörter $w \in W$ ohne Nachfolger in W sind die Blätter des Baumes, die anderen Wörter $w \in W$ sind die inneren Knoten.

Folgerung 1.4 *Ist* $W \subseteq \{0, 1, \ldots, r-1\}^*$ *präfixabgeschlossen und gilt* $|W| \neq 1$*, so bildet die Menge der Blätter von* W *einen Präfixcode.*

1.4 Mittlere Codewortlänge

Definition 1.7 Es sei $Y = \{a_1, \ldots, a_k\}$, und es sei $P = (p_1, \ldots, p_k)$ mit $\sum_{i=1}^{k} p_i = 1$ ein k-Vektor nichtnegativer Zahlen. Dann nennen wir (Y, P) eine *Quelle*.

Weiter nennen wir $H_m(P) := \sum_{i=1}^{k} -p_i \cdot \log_m p_i$ die *Entropie* der Quelle (Y, P).

Satz 1.5 (Abschätzung für die minimale mittlere Codewortlänge) *Es seien (Y, P) eine Quelle und $\varphi : Y \to X^*$ eine eindeutig decodierbare Codierung. Dann gilt für die mittlere Codewortlänge, $\overline{l(\varphi)}$, von φ die Beziehung:*

$$\overline{l(\varphi)} := \sum_{i=1}^{k} p_i \cdot |\varphi(a_i)| \geq H_{|X|}(P)\,.$$

Satz 1.6 (Shannon) *Zu jeder Häufigkeitsverteilung* $P = (p_1, \ldots, p_k)$ *und zu jedem Alphabet* X *gibt es einen Präfix-Code* $C \subseteq X^*, C = \{w_1, \ldots, w_k\}$*, mit einer mittleren Codewortlänge* $\overline{l(C)}$*, die der Abschätzung* $\overline{l(C)} \leq H_{|X|}(P) + 1$ *genügt.*

Definition 1.8 Eine eindeutig decodierbare Codierung $\varphi : \{a_1, \ldots, a_k\} \to \{x_1, \ldots, x_m\}^*$ heißt *alphabetisch*, wenn $\varphi(a_i) <_{\text{lex}} \varphi(a_{i+1})$.

Satz 1.7 *Zu jeder Quelle* (Y, P) *und zu jedem Alphabet* X *gibt es eine alphabetische Codierung* φ*, mit einer mittleren Codewortlänge* $\overline{l(\varphi)}$*, die der Abschätzung* $\overline{l(\varphi)} \leq H_{|X|}(P) + 2$ *genügt.*

Ternärer Shannon – Code

Häufigkeit	r_{j-1}	ternär	$\ell_j = \lceil \log_3 \frac{1}{p_j} \rceil$	Codewort
$p_1 = 0.4$	0.0	0.0000000	1	**0**
$p_2 = 0.2$	0.4	0.1012101	2	**10**
$p_3 = 0.1$	0.6	0.1210121	3	**121**
$p_4 = 0.1$	0.7	0.2002200	3	**200**
$p_5 = 0.1$	0.8	0.2101210	3	**210**
$p_6 = 0.1$	0.9	0.2200220	3	**220**

$$\bar{l} = 2.0\,, \qquad H_{\mathcal{P}} = 1.465$$

Binärer Shannon – Code

Häufigkeit	r_{j-1}	binär	$\ell_j = \lceil \log_2 \frac{1}{p_j} \rceil$	Codewort
$p_1 = 0.4$	0.0	0.000000000	2	00
$p_2 = 0.2$	0.4	0.011001101	3	011
$p_3 = 0.1$	0.6	0.100110011	4	1001
$p_4 = 0.1$	0.7	0.101100110	4	1011
$p_5 = 0.1$	0.8	0.110011010	4	1100
$p_6 = 0.1$	0.9	0.111001101	4	1110

$$\overline{l} = 3.0\ , \qquad H_{\mathcal{P}} = 2.322$$

Binärer Alphabetischer Code

Häufigkeit	r_{j-1}	binär	$\ell_j = \lceil \log_2 \frac{1}{p_j} \rceil + 1$	Codewort
$p_1 = 0.1$	0.05	0.000011010	5	00001
$p_2 = 0.1$	0.15	0.001001101	5	00100
$p_3 = 0.4$	0.4	0.011001101	3	011
$p_4 = 0.1$	0.65	0.101001101	5	10100
$p_5 = 0.2$	0.8	0.110011010	4	1100
$p_6 = 0.1$	0.95	0.111100110	5	11110

$$\bar{l} = 4.0\,, \qquad H_{\mathcal{P}} = 2.322$$

2 Sprachentheoretische Eigenschaften von Codes

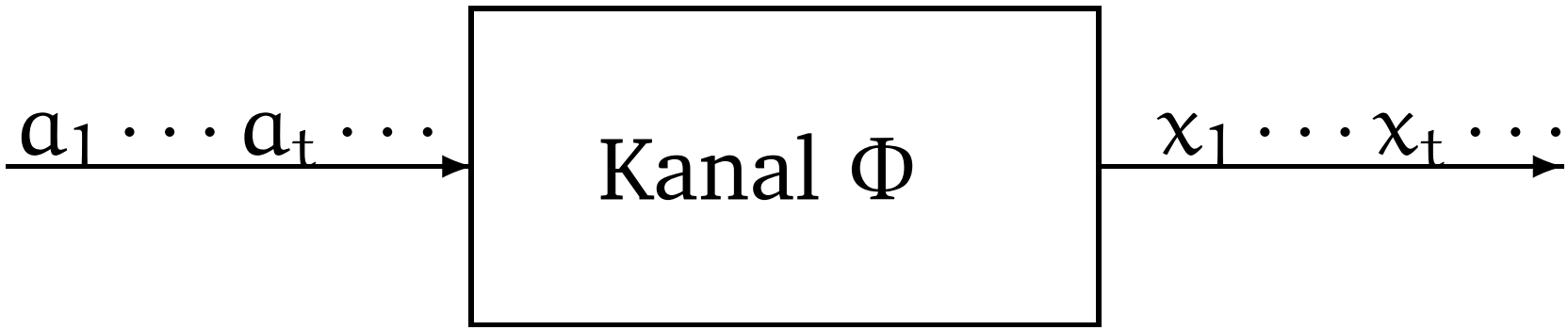
2.1 Maximalität und Vollständigkeit von Codes

Definition 2.1 [Maximale Codes] Eine Sprache $C \subseteq X^*$ heißt *maximaler Code* : $\Longleftrightarrow$
Für jeden Code $C' \subseteq X^*$ mit $C \subseteq C'$ gilt $C' = C$.

Folgerung 2.1 *Es sei μ ein nicht-entartetes Bernoulli-Maß auf X^*. Ist $C \subseteq X^*$ ein Code mit $\mu(C) = 1$, so ist C maximal.*

Satz 2.2 (Über die Existenz von maximalen Codes)
Zu jedem Code $C \subseteq X^*$ gibt es einen maximalen Code, der C enthält.

Shannons Kanalkapazität



$$C(\Phi) := \lim_{t \to \infty} \frac{\log_r |\{x_1 \cdots x_t : x_1 \cdots x_t \text{ ist Ausgabe von } \Phi\}|}{t}$$

Vollständigkeit von Codes

$$\mathbf{T}(W) := \{v : \exists w, v_1, v_2 (w \in W \wedge v_1, v_2 \in X^* \wedge v_1 \cdot v \cdot v_2 = w)\}$$

Definition 2.2 1. Eine Sprache $W \subseteq X^*$ heißt *dicht*, falls $\mathbf{T}(W) = X^*$ erfüllt ist.

2. Anderenfalls nennen wir eine Sprache $W \subseteq X^*$ *mager*.

Folgerung 2.3 *Ist $W \subseteq X^*$ mager, so gilt $\mu(W) < \infty$ für jedes Bernoulli-Maß $\mu : X^* \to (0, 1]$ auf X^*.*

Lemma 2.4 *Es sei μ ein Bernoulli-Maß auf X^*. Dann gelten:*

1. *Ist $\mu(W^*) = \infty$, so gilt $\mu(W) \geq 1$.*
2. *Ist $C \subseteq X^*$ ein Code, so gilt genau dann $\mu(C^*) = \infty$, wenn $\mu(C) = 1$ ist.*

Definition 2.3 Eine Sprache $W \subseteq X^*$ heißt *vollständig*, falls W^* dicht ist.

Satz 2.5 *Ist $W \subseteq X^*$ eine magere und vollständige Sprache, so gilt $\mu(W^*) = \infty$ für jedes Bernoulli-Maß $\mu : X^* \to (0,1]$ auf X^*.*

Lemma 2.6 *Es sei $V \subseteq X^*$ und es gebe ein festes $k \in \mathbb{N}$ derart, dass $\mathbf{T}(V) \subseteq \left\{v : \exists w_1 \exists w_2 (|w_1|, |w_2| \leq k \wedge w_1 \cdot v \cdot w_2 \in V\right\}$.*

Dann gilt für jedes Bernoulli-Maß μ mit $\mu_{\min} := \min\{\mu(x) : x \in X\} > 0$ die Ungleichung

$$\mu(\mathbf{T}(V)) \geq \mu(V) \geq \frac{\mu_{\min}^{2k}}{(k+1)^2} \cdot \mu(\mathbf{T}(V)) \; .$$

Folgerung 2.7 *Ist $C \subseteq X^*$ ein magerer und vollständiger Code, so gilt $\mu(C) = 1$ für jedes Bernoulli-Maß $\mu : X^* \to (0,1]$ auf X^*.*

$\mathcal{M} := \{\mu \mid \mu : X^* \to (0,1]\}$ sei die Menge aller nicht-entarteten Bernoulli-Maße auf X^*. Für $W \subseteq X^*$ gilt:

$$\begin{array}{lcl} W \text{ ist dicht} & \Longleftarrow & \exists\mu(\mu \in \mathcal{M} \wedge \mu(W) = \infty) \\ & & \Uparrow \\ & & \forall\mu(\mu \in \mathcal{M} \to \mu(W) = \infty) \end{array}$$

Für **mageres** (d.h. nicht dichtes) $L \subseteq X^*$ gilt darüberhinaus:

$$\begin{array}{lcl} & & \exists\mu(\mu \in \mathcal{M} \wedge \mu(L) \geq 1) \\ & & \Uparrow \\ L \text{ ist vollständig} & \Longrightarrow & \forall\mu(\mu \in \mathcal{M} \to \mu(L) \geq 1) \end{array}$$

Der Vervollständigungssatz von *Ehrenfeucht* und *Rozenberg*

Definition 2.4 Wir nennen ein Wort $y \in X^*$ *unberandet*, falls $y \neq e$ und kein echtes Präfix $e \sqsubset w \sqsubset y$ zugleich auch Suffix von y ist.

Satz 2.8 *Es seien $C \subseteq X^*$ ein Code und $y \notin T(C^*)$ ein unberandetes Wort. Weiter sei $U := (X^* \setminus X^* \cdot y \cdot X^*) \setminus C^*$, dann ist $\hat{C} := C \cup y \cdot (U \cdot y)^*$ ein vollständiger Code.*

Lemma 2.9 *Es seien $v \in X^*$ ein unberandetes Wort, $V := X^* \setminus X^* \cdot y \cdot X^*$ die Menge aller Wörter, die y nicht als Infix enthalten. Dann ist $C := V \cdot y$ ein Präfix-Code.*

Satz 2.10 *Ist C ein maximaler Code, so ist C ein vollständiger Code.*

$\mathcal{M} := \{\mu \mid \mu : X^* \to (0,1]\}$ sei die Menge aller nicht-entarteten Bernoulli-Maße auf X^*. Dann gilt für **Codes** $C \subseteq X^*$:

$$\begin{array}{ccc} C \text{ ist maximal} & \Longleftarrow & \exists\mu(\mu \in \mathcal{M} \wedge \mu(C) = 1) \\ \Downarrow & & \Uparrow \\ C \text{ ist vollständig} & \overset{C \text{ mager}}{- - - \to} & \forall\mu(\mu \in \mathcal{M} \to \mu(C) = 1) \end{array}$$

Folgerung 2.11 *Ein Code $C \subseteq X^*$ ist genau dann vollständig, wenn C maximal oder dicht ist.*

Folgerung 2.12 *Ist $C \subseteq X^*$ ein Code, so gibt es einen vollständigen Code $\hat{C}$, der C enthält.*
Ist C darüber hinaus reguläre Sprache, so kann auch $\hat{C}$ regulär gewählt werden.

Lemma 2.13 *Es sei $L \subseteq X^*$ eine reguläre Sprache. Dann sind die folgenden Aussagen äquivalent:*

1. *L ist dicht, d.h. $\boldsymbol{T}(L) = X^*$.*
2. *Es existiert ein Bernoulli-Maß $\mu : X^* \to (0, 1]$ mit $\mu(L) = \infty$.*
3. *Für alle Bernoulli-Maße $\mu : X^* \to (0, 1]$ gilt $\mu(L) = \infty$.*

Folgerung 2.14 *Jeder reguläre Code $C \subseteq X^*$ ist mager.*

Definition 2.5 Ein Code $C \subseteq X^*$ heißt *präfix-maximal*: $\Longleftrightarrow$

1. C ist Präfix-Code, und
2. für jeden Präfix-Code $C' \supseteq C$ gilt $C' = C$.

Lemma 2.15 *Ein Präfix-Code $C \subseteq X^*$ ist genau dann präfix-maximal, wenn für es jedes $w \in X^*$ ein $v \in C$ mit $w \sqsubseteq v$ oder $v \sqsubseteq w$ gibt.*

Der Suffix-Code $\bigcup_{n\in\mathbb{N}} X^n \cdot b \cdot a^n$ enthält einen echten präfix-maximalen Teilcode $\hat{C}$, d.h. $\hat{C}$ ist nicht maximal als Code.

Lemma 2.16 *Jeder (endliche) Präfix-Code ist in einem maximalen (endlichen) Präfix-Code enthalten.*
Jeder endliche maximale Präfix-Code ist auch maximal als Code.

Es sei $\varphi : X \to Y^*$ eine Codierung, deren Erweiterung auf X^* ebenfalls mit φ bezeichnet werde.

Lemma 2.17 *1. Ist $C \subseteq X^*$ ein Code, so ist auch $\varphi(C) \subseteq Y^*$ ein Code.*

2. Ist $C' \subseteq Y^*$ ein Code, so ist auch $\varphi^{-1}(C') \subseteq X^*$ ein Code.

2.2 Entscheidungsprobleme und Decodierverzögerung

Definition 2.6 Wir setzen für $C \subseteq X^*$:

$$\begin{aligned} w <_1 v &:\Longleftrightarrow \exists u(u \in C \wedge u = w \cdot v) \\ \{e\}\ w <_2 v &:\Longleftrightarrow \exists u(u \in C \wedge w = u \cdot v)\ \text{, sowie} \\ w < v &:\Longleftrightarrow w <_1 v \ \vee\ w <_2 v \end{aligned}$$

Lemma 2.18 (Levenštejn) *Es gibt genau dann eine C-Kette* $v_1 < \ldots < v_n$*, wenn es Wörter* $w_1, \ldots, w_i \in C$ *und* $u_1, \ldots, u_j \in C$ *mit* $w_1 \neq u_1$ *und* $i + j = n$ *derart gibt, daß*

1. $v_1 \in \{w_1, u_1\}$,
2. $u_1 \cdots u_j \cdot v_n = w_1 \cdots w_i$ *und*
3. $|v_n| \leq |w_i|$.

Folgerung 2.19 *Eine Sprache* $C \subseteq X^* \setminus \{e\}$ *ist genau dann ein Code, wenn es keine endliche C-Kette* $v_1 < \ldots < v_n$ $(n \geq 2)$*, die auf ein Wort* $v_n \in C$ *endet, gibt.*

Folgerung 2.20 *Es gibt ein Verfahren, welches zu endlichem* $L \subseteq X^* \setminus \{e\}$ *entscheidet, ob* L *ein Code ist.*

Satz 2.21 *Es gibt ein Verfahren, welches zu regulärem* $L \subseteq X^* \setminus \{e\}$ *entscheidet, ob* L *ein Code ist.*

Es gibt kein Verfahren, welches zu kontextfreiem $L \subseteq X^* \setminus \{e\}$ *entscheidet, ob* L *ein Code ist.*

Definition 2.7 [Decodierverzögerung] Es seien $C \subseteq X^*$ ein Code und $w \in C$.

- Das Codewort w hat die Decodierverzögerung $m(w) \in \mathbb{N}$, falls aus $wv_1 \dots v_{m(w)} \sqsubseteq w'u$ mit $v_i, w' \in C$ und $u \in C^*$ stets $w = w'$ folgt.
- C hat endliche Decodierverzögerung, falls jedes $w \in C$ eine endliche Decodierverzögerung hat.
- C hat beschränkte Decodierverzögerung, falls es ein $n \in \mathbb{N}$ mit $\forall w(w \in C \rightarrow m(w) \leq n)$ gibt.

Beispiele für Decodierverzögerung

Verzögerung ist	aber nicht	Gegenbeispiel
–	endlich	$\{a, ab, bb\}$, Suffix-Code
endlich	beschränkt	$ab^*a \cup \{ab^{n+1}ab^na : n \in \mathbb{N}\}$ $\cup \{b^{n+1}ab^na : n \in \mathbb{N}\}$
n $(n \geq 1)$	$n-1$	$\{a, a^nb\}$
0 (Präfix-Code)	Bifix-Code	$\{a, ba\}$

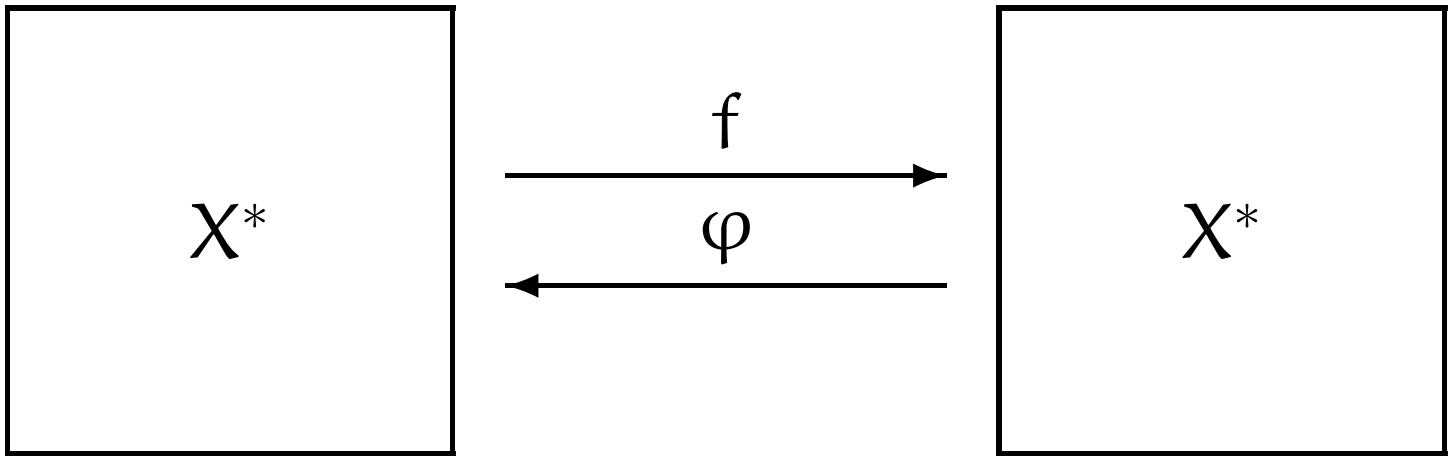
Lemma 2.22 *Wenn für jedes $w \in C$ jede mit w beginnende C-Kette eine Länge $\leq l_w$ hat, so hat C endliche Decodierverzögerung.*

Lemma 2.23 *Es sei C ein Code.*

1. *Ist jede C-Kette nicht länger als ℓ, so hat C eine Decodierverzögerung von höchstens $\ell - 1$.*
2. *Hat C die Decodierverzögerung $m \in \mathbb{N}$, so ist keine C-Kette länger als $2m + 2$.*

3 Ein allgemeines Modell der Datenkompression

Text $w \in X^*$ Beschreibung (*oder* Programm) $\pi \in X^*$



Raum der Texte Raum der Beschreibungen

f ist injektiv.

Definition 3.1 Wir nennen eine injektive Funktion $f : X^* \to X^*$ *Kompressionsfunktion*.

Eine partielle Funktion $\varphi :\subseteq X^* \to X^*$ heißt *Dekompressionsfunktion* für f, falls $\forall w(w \in X^* \to \varphi(f(w)) = w)$.

Definition 3.2 Die Funktion $k_f : X^* \to \mathbb{N}$ mit $k_f(w) := |f(w)|$ heißt *(Beschreibungs-)Komplexität* von w bezüglich f.

Analog heißt $K_\varphi : X^* \to \mathbb{N} \cup \{\infty\}$ mit

$$K_\varphi(w) := \inf\{\, |\pi| : \pi \in X^* \wedge \varphi(\pi) = w\}$$

(Beschreibungs-)Komplexität von w bezüglich φ.

Lemma 3.1 *Die Funktion* f *ist genau dann berechenbar, wenn* k_f *berechenbar ist.*

Wir führen auf der Menge aller Funktionen $g\colon X^* \to \mathbb{N}$ (bzw. $X^* \to X^*$) die folgende Relation ein:

$$h \preceq g : \Longleftrightarrow \ \exists c(c \in \mathbb{N} \wedge \forall w(w \in X^* \to |h(w)| \leq |g(w)| + c)) \ .$$

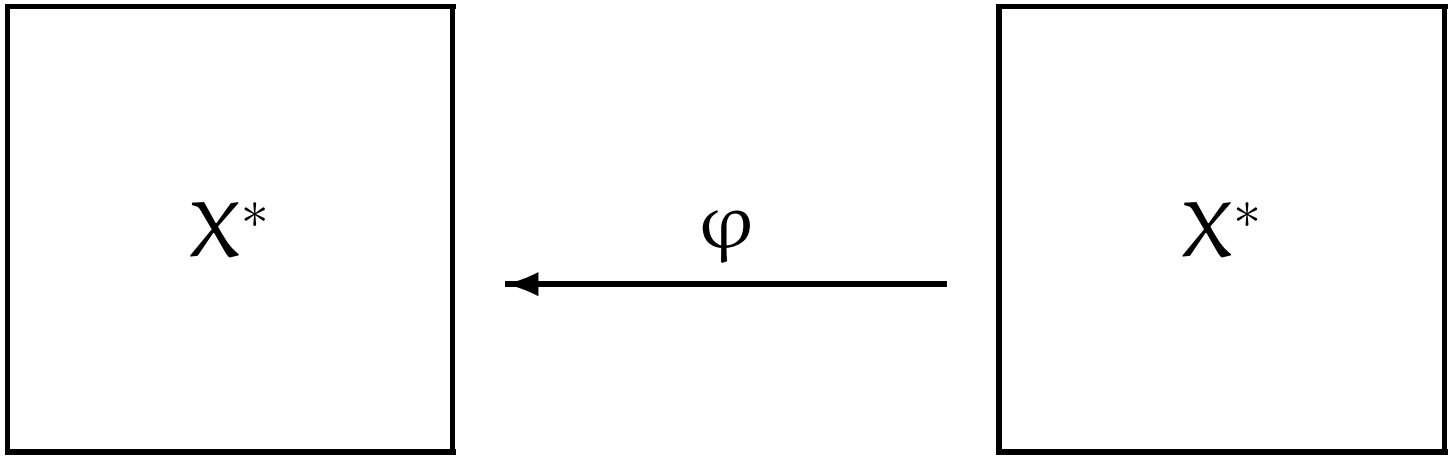
Folgerung 3.2 *Die Relation* $\preceq$ *ist reflexiv und transitiv, aber nicht antisymmetrisch.*

Eine Funktion h heißt *optimal* bezüglich einer Klasse $\mathcal{K}$ von Funktionen, falls $\forall g(g \in \mathcal{K} \to h \preceq g)$.

Satz 3.3 *In der Klasse* $\mathcal{K}_{1\mathrm{rek}}$ *aller eineindeutigen rekursiven (Kompressions-)Funktionen* $f\colon X^* \to X^*$ *gibt es keine optimalen Funktionen.*

4 Kolmogorov-Komplexität von Wörtern

Text $w \in X^*$ Beschreibung (*oder* Programm) $\pi \in X^*$



Raum der Texte Raum der Beschreibungen

φ ist partiell-rekursiv.

Definition 4.1 Es sei $\varphi :\rightarrow X^*$ eine partielle berechenbare (partiell-rekursive) Funktion.
K_φ heißt *Kolmogorov-Komplexität* bezüglich $\varphi :\Longleftrightarrow$

$$K_\varphi : X^* \rightarrow \mathbb{N} \text{ , wobei}$$
$$K_\varphi(w) \quad := \quad \inf\{\,|\pi| : \pi \in X^* \wedge \varphi(\pi) = w\} \,.$$

Definition 4.2 Eine partiell-rekursive Funktion $\mathfrak{U} : X^* \rightarrow X^*$ heißt *optimal* $:\Longleftrightarrow$
Fürb jede partiell-rekursive Funktion $\varphi : X^* \rightarrow X^*$ existiert eine Konstante $c_\varphi \in \mathbb{N}$ derart, daß

$$\forall w\big(w \in X^* \rightarrow K_{\mathfrak{U}}(w) \leq K_\varphi(w) + c_\phi\big) \,.$$

Satz 4.1 ([LV Thm. 2.1, Ca Thm. 2.9])
Es gibt optimale partiell-rekursive Funktionen $\mathfrak{U} : X^* \to X^*$.

Folgerung 4.2 *Sind* $\mathfrak{U}, \mathfrak{U}'$ *optimale partiell-rekursive Funtionen, so gibt es eine Konstante* c *mit*

$$|K_{\mathfrak{U}}(w) - K_{\mathfrak{U}'}(w)| \leq c \ .$$

Wir setzen $\mathbf{K} := K_{\mathfrak{U}}$

Satz 4.3 ([LV Thm. 2.7, Ca Thm. 5.1]) *Es gibt eine rekursive Funktion* $h : \mathbb{N} \times X^* \to \mathbb{N}$, *die im ersten Argument monoton nicht wachsend ist, derart, daß*

$$\lim_{t \to \infty} h(t, w) = \mathbf{K}(w) \ .$$

Satz 4.4 ([LV Thm. 2.6, Ca Thm. 5.1]) *Die Funktion* $\mathbf{K} : X^* \to \mathbb{N}$ *stimmt mit keiner partiell-rekursiven Funktion* $\psi : X^* \to \mathbb{N}$ *mit unendlichem Definitionsbereich dom* (ψ) *auf dom* (ψ) *überein.*

Folgerung 4.5 *Es sei* $f : \mathbb{N} \to \mathbb{N}$ *eine rekursive Funktion mit* $\lim_{n\to\infty} f(n) = \infty$. *Dann ist*

$$A := \{w : \mathbf{K}(w) \leq f(|w|)\}$$

rekursiv aufzählbar, während das Komplement $X^* \setminus A$ *keine unendliche rekursiv aufzählbare Teilmenge enthält.*

Schreibweise: $\mathbf{K}'(n) := \mathbf{K}(\mathsf{string}(n))$

Folgerung 4.6

1. $\exists c : \forall n : |\mathbf{K}'(n+1) - \mathbf{K}'(n)| \leq c$
2. $\exists c : \forall w : |\mathbf{K}(wx) - \mathbf{K}(w)| \leq c$

Folgerung 4.7

1. $\exists c : \forall n : \mathbf{K}'(n) \leq \log_r n + c$
2. *Die Funktion* $\kappa(n) := \min\{\mathbf{K}'(i) : i \geq n\}$ *ist unbeschränkt.*

Satz 4.8 ([LV Thm. 2.5]) *Es sei* $\psi : \mathbb{N} \to \mathbb{N}$ *eine beliebige auf ihrem Definitionsbereich dom* (ψ) *monoton nicht fallende unbeschränkte partiell-rekursive Funktion. Dann gibt es für die Funktion* $\kappa\colon \mathbb{N} \to \mathbb{N}$ *aus Folgerung 4.7.2 ein* $m_\psi \in \mathbb{N}$ *derart, daß*

$$\forall n(n \in \mathit{dom}\,(\psi) \wedge n \geq m_\psi \to \kappa(n) < \psi(n)) \ .$$

Satz 4.9 *Die Funktion* $\mathbf{K} : X^* \to \mathbb{N}$ *ist das Minimum bezüglich „*$\preceq$*“ in der Klasse aller von oben approximierbaren Funktionen* $h : X^* \to \mathbb{N}$*, die der Bedingung* $|\{w : h(w) = n\}| \leq r^{n+O(1)}$ *genügen.*

Einfache Eigenschaften von K

Folgerung 4.10 *1. Ist* $\varphi :\subseteq X^* \to X^*$ *partiell-rekursiv, so gilt* $\mathbf{K}(\varphi(w)) \leq \mathbf{K}(w) + O(1)$ *für* $w \in dom\,(\varphi)$.

2. Es gibt ein $c > 0$ *derart, dass* $c \cdot r^n \leq |\{w : \mathbf{K}(w) \leq n\}| < \frac{r^{n+1}}{r-1}$.

3. $$\frac{|\{w : |w| = n \wedge \mathbf{K}(w) \leq n - c\}|}{r^n} < \frac{r}{r-1} \cdot r^{-c}$$

4. Es sei $V \subseteq X^* \times \mathbb{N}$ *rekursiv aufzählbar und genüge der Bedingung* $\forall n(n \in \mathbb{N} \to \left|\{v : (v, n) \in V\}\right| \leq r^n)$.

Dann gilt $\mathbf{K}(w) \leq m + c$ *falls* $(w, m) \in V$.

5 Verbundkomplexität und bedingte Komplexität

Definition 5.1 Es sei $\phi : X^* \times \{0,1\} \to X^*$ eine partiell-rekursive Funktion.
K_ϕ heißt *Verbundkomplexität* :$\Longleftrightarrow$

$$\begin{aligned} K_\phi &: X^* \times X^* \to \mathbb{N} \text{ , wobei} \\ K_\phi(w,v) &:= \inf\{|\pi| : \pi \in X^* \wedge \phi(\pi,0) = w \wedge \phi(\pi,1) = v\} . \end{aligned}$$

Satz 5.1 *Es gibt eine optimale partiell-rekursive Funktion* $\mathfrak{U}^{(2)} : X^* \times \{0,1\} \to X^*$ *derart, dass* $K_{\mathfrak{U}^{(2)}}(w,v) \leq K_\phi(w,v) + c_\phi$ *für alle* $w, v \in X^*$ *gilt.*

Es sei wieder $\mathbf{K} := \mathrm{K}_{\mathfrak{U}(2)}$.

Folgerung 5.2 *Es gelten*

1. $\mathbf{K}(w) \leq \mathbf{K}(w,v) + \mathcal{O}(1)$ *und* $\mathbf{K}(v) \leq \mathbf{K}(w,v) + \mathcal{O}(1)$,
2. $|\mathbf{K}(w,v) - \mathbf{K}(v,w)| = \mathcal{O}(1)$
3. *Ist* $\psi :\subseteq X^* \to X^*$ *partiell-rekursiv, so ist* $\mathbf{K}(w,\psi(w)) \leq \mathbf{K}(w) + \mathcal{O}(1)$ *für* $v \in dom\,(\psi)$.

Lemma 5.3
$\mathbf{K}(w,v) \leq \mathbf{K}(w) + \mathbf{K}(v) + 2 \cdot \min\left\{\log_r \mathbf{K}(w), \log_r \mathbf{K}(v)\right\} + \mathcal{O}(1)$

Satz 5.4 *Es sei* $c \in \mathbb{N}$. *Dann gibt es unendlich viele Paare* w, v *derart, dass* $\mathbf{K}(w,v) > \mathbf{K}(w) + \mathbf{K}(v) + c$.

5.1 Bedingte Komplexität

Definition 5.2 Es sei $\phi : X^* \times X^* \to X^*$ eine partiell-rekursive Funktion.
K_ϕ heißt *bedingte Kolmogorov Komplexität* :$\Longleftrightarrow$

$$\begin{aligned} K_\phi &: X^* \times X^* \to \mathbb{N} \text{ , wobei} \\ K_\phi(w/v) &:= \inf\{|\pi| : \pi \in X^* \wedge \phi(\pi, v) = w\} . \end{aligned}$$

Spezialfall: $K_\phi(w) := K_\phi(w/e)$.

Satz 5.5 *Es gibt eine optimale partiell-rekursive Funktion* $\mathfrak{U}^b : X^* \times X^* \to X^*$ *derart, dass* $K_{\mathfrak{U}^b}(w/v) \leq K_\phi(w/v) + c_\phi$ *für alle* $w, v \in X^*$ *gilt.*

Eigenschaften der Bedingten Komplexität

Es sei wieder $\mathbf{K} := \mathrm{K}_{\mathfrak{U}^b}$.

Folgerung 5.6 *1.* $\mathbf{K}(w/v) \leq |w| + \mathcal{O}(1)$

2. *Ist* $\psi :\subseteq X^* \times X^* \to X^*$ *partiell-rekursiv, so gilt* $\mathbf{K}(\psi(w,v)/v) \leq \mathbf{K}(w/v) + \mathcal{O}(1)$ *für alle Paare* $(w,v) \in dom\,(\psi)$.

3. *Es gibt ein* $c > 0$ *derart, dass für* $v \in X^*$ *die Beziehung* $c \cdot r^n \leq |\{w : \mathbf{K}(w,v) \leq n\}| < \frac{r^{n+1}}{r-1}$ *gilt.*

4. $\dfrac{|\{w : |w| = n \wedge \mathbf{K}(w,v) \leq n - c\}|}{r^n} < \dfrac{r}{r-1} \cdot r^{-c}$ *für* $v \in X^*$.

5. *Es sei* $V \subseteq X^* \times X^* \times \mathbb{N}$ *rekursiv aufzählbar und genüge der Bedingung* $\forall n \forall v (n \in \mathbb{N} \wedge v \in X^* \to \left|\{w : (w,v,n) \in V\}\right| \leq r^n)$. *Dann gilt* $\mathbf{K}(w/v) \leq m + c$ *falls* $(w,,v,m) \in V$.

Satz 5.7 ([LV Thm. 2.6/2.7, Ca Thm. 5.1])

1. *Für kein* $v \in X^*$ *stimmt die Funktion* $\mathbf{K}(\cdot/v) : X^* \to \mathbb{N}$ *mit einer partiell-rekursiven Funktion* $\psi : X^* \to \mathbb{N}$ *mit unendlichem Definitionsbereich dom* (ψ) *auf dom* (ψ) *überein.*

2. *Es gibt eine rekursive Funktion* $h : \mathbb{N} \times X^* \times X^* \to \mathbb{N}$, *die im ersten Argument monoton nicht wachsend ist, derart, daß*

$$\lim_{t \to \infty} h(t, w, v) = \mathbf{K}(w/v).$$

5.2 Beziehungen zwischen Verbund- und bedingter Komplexität

Lemma 5.8 *Es gelten die folgenden Ungleichungen*

$$\begin{aligned}\mathbf{K}(w,v) &\leq \mathbf{K}(v) + \mathbf{K}(w/v) + 2\cdot\log_r \mathbf{K}(v) + \mathcal{O}(1),\\ \mathbf{K}(w,v) &\leq \mathbf{K}(v) + \mathbf{K}(w/v) + 2\cdot\log_r \mathbf{K}(w/v) + \mathcal{O}(1),\end{aligned}$$

und für unendlich viele Paare $w,v \in X^*$ gilt die Ungleichung

$$\mathbf{K}(w,v) > \mathbf{K}(v) + \mathbf{K}(w/v) + \mathcal{O}(1).$$

Satz 5.9 *Es sei $\varepsilon > 0$. Dann gilt*

$$\mathbf{K}(v) + \mathbf{K}(w/v) \leq \mathbf{K}(w,v) + (3+\varepsilon)\cdot\log_r \mathbf{K}(w,v) + \mathcal{O}(1)$$

für $w,v \in X^*$.

6 Präfix-Komplexität

6.1 Präfix-Algorithmen

Definition 6.1 Eine Funktion $\phi :\subseteq X^* \to X^*$ heißt *Präfix-Funktion*, falls *dom* (ϕ) präfixfrei, d.h. ein Präfix-Code oder *dom* $(\phi) = \{e\}$ ist.

Satz 6.1 *Es gibt eine universelle partiell-rekursive Präfix-Funktion, d.h. eine Präfix-Funktion* φ *derart, dass für jede partiell-rekursive Präfix-Funktion* ψ *ein* $u_\psi \in X^*$ *mit der Eigenschaft* $\forall w(w \in X^* \to \psi(w) = \varphi(u_\psi \cdot w))$ *existiert.*

Eigenschaften rekursiv-aufzählbarer Präfix-Codes

Lemma 6.2 *Ist ein rekursiv-aufzählbarer Präfix-Code* $C \subseteq X^*$ *präfix-maximal, so ist* C *rekursiv entscheidbar.*

Definition 6.2 1. Eine Zahl $\alpha \in \mathbb{R}$ heißt *berechenbar*, wenn es eine rekursive Funktion $f_\alpha : \mathbb{N} \to \mathbb{Q}$ derart gibt, dass $\forall n(n \in \mathbb{N} \to |f_\alpha(n) - \alpha| < 2^{-n})$ gilt.

2. Eine Zahl $\alpha \in \mathbb{R}$ heißt *links berechenbar*, wenn es eine monoton nicht fallende rekursive Funktion $f_\alpha : \mathbb{N} \to \mathbb{Q}$ mit $\lim_{n\to\infty} f_\alpha(n) = \alpha$ gibt.

Lemma 6.3 *Es sei* $C \subseteq X^*$ *ein rekursiv-aufzählbarer Präfix-Code, und es sei* $\sum_{v\in C} r^{-|v|}$ *eine berechenbare relle Zahl. Dann ist* C *rekursiv entscheidbar.*

Satz 6.4 *Es sei* $f : \mathbb{N} \to \mathbb{N}$ *eine rekursive Funktion mit der Eigenschaft* $\sum_{i \in \mathbb{N}} r^{-f(i)} \leq 1$. *Dann gibt es einen rekursiv aufzählbaren Präfix-Code* $C = \{w_i : i \in \mathbb{N}\}$ $(w_i \neq w_j$ *für* $i \neq j)$ *mit* $|w_i| = f(i)$.

Lemma 6.5 *Es sei* $D \subseteq X^*$ *ein Präfix-Code mit* $m := \min\{|w| : w \in D\}$ *und* $|D \cap X^l| \leq |X| - 1$ *für alle* $l \in \mathbb{N}$. *Dann gilt* $\sum_{v \in D} |X|^{-|v|} \leq |X|^{-(m-1)}$, *wobei die Gleichheit nur dann gilt, wenn* $|D \cap X^l| = |X| - 1$ *für alle* $l \geq m$ *erfüllt ist.*

Folgerung 6.6 (Zum Beweis von Satz 6.4) *Ist* $D \subseteq X^*$ *ein endlicher Präfix-Code und gelten* $\sum_{v \in D} |X|^{-|v|} \geq |X|^{-k}$ *sowie* $|D \cap X^l| < |X|$ *für alle* $l \in \mathbb{N}$, *so gibt es ein* $v \in D$ *mit* $|v| \leq k$.

Algorithmus KRAFT-CHAITIN: $f : \mathbb{N} \to \mathbb{N}$, $X = \{0, 1, \ldots, r-1\}$

$i := 0$, $C_0 := \emptyset$, $D_0 := \{e\}$, $\ell_0(j) :=$ if $j = 0$ then 1 else 0

While $i < \infty$ do

1 $\quad n_i := \max\{|w| : w \in D_i \wedge |w| \le f(i)\}$

2 $\quad v_i := \min_{ql}(D_i \cap X^{n_i})$

3 $\quad w_i := v_i \cdot 0^{f(i)-n_i}$

4 $\quad i := i + 1$

5 $\quad C_i := C_{i-1} \cup \{w_{i-1}\}$

6 $\quad \ell_i(j) :=$ if $j = n_{i-1}$ then $\ell_{i-1}(j) - 1$ else $\ell_{i-1}(j)$

7 $\quad D_i :=$ if $f(i-1) = n_{i-1}$ then $\left(D_{i-1} \setminus \{v_{i-1}\}\right)$

$$\bigcup_{j=0}^{f(i-1)-n_{i-1}-1} v_{i-1} \cdot 0^j \cdot (X \setminus \{0\})$$

8 $\quad$ else $\left(D_{i-1} \setminus \{v_{i-1}\}\right) \cup$

9 $\quad$ and

10 $\quad$ for $j = n_{i-1} + 1$ to $f(i-1)$ do $\ell_i(j) := r - 1$

Endwhile

Folgerung 6.7 *Es seien* $f : \mathbb{N} \to \mathbb{N}$ *und* $g : \mathbb{N} \to X^*$ *rekursive Funktionen mit der Eigenschaft* $\sum_{i \in \mathbb{N}} r^{f(i)} \leq 1$. *Dann gibt es eine eineindeutige rekursive Funktion* $h : \mathbb{N} \to X^*$ *derart, dass die Menge* $\{(h(i), g(i)) : i \in \mathbb{N}\}$ *der Graph einer partiell-rekursiven Präfix-Funktion* $\psi :\subseteq X^* \to X^*$ *mit den Eigenschaften*

1. $\psi(dom\,(\psi)) = \{g(i) : i \in \mathbb{N}\}$ *und*
2. $\forall i(i \in \mathbb{N} \to |h(i)| = f(i) \wedge \psi(h(i)) = g(i)))$ *ist.*

6.2 Präfix-Komplexität

Definition 6.3 Es sei φ eine universelle Präfix-Funktion. Die Funktion $\mathbf{KP} := K_\varphi$ nennen wir *Präfix-Komplexität*.

$$\mathbf{KP}(w) := \min\{|\pi| : \varphi(\pi) = w\}$$

Satz 6.8 *Es gibt eine rekursive Funktion* $h : \mathbb{N} \times X^* \to \mathbb{N}$ *, die im ersten Argument monoton nicht wachsend ist, derart, daß*

$$\lim_{t \to \infty} h(t, w) = \mathbf{KP}(w) \ .$$

Satz 6.9 *Die Funktion* $\mathbf{KP} : X^* \to \mathbb{N}$ *stimmt mit keiner partiell-rekursiven Funktion* $\psi : X^* \to \mathbb{N}$ *mit unendlichem Definitionsbereich dom* (ψ) *auf dom* (ψ) *überein.*

Folgerung 6.10 *Es sei* $f : \mathbb{N} \to \mathbb{N}$ *eine rekursive Funktion mit* $\lim_{n \to \infty} f(n) = \infty$*. Dann ist*

$$A := \{w : \mathbf{KP}(w) \leq f(|w|)\}$$

rekursiv aufzählbar, während das Komplement $X^* \setminus A$ *keine unendliche rekursiv aufzählbare Teilmenge enthält.*

Lemma 6.11 *Es gelten*

1. $\mathbf{KP}(w) \leq |w| + 2 \cdot \log_r |w| + \mathcal{O}(1)$,
2. *für jedes* $n \in \mathbb{N}$ *gilt*
   $\max\{\mathbf{KP}(w) : |w| = n\} \leq n + \mathbf{KP}(\mathsf{string}_r(n)) + \mathcal{O}(1)$,
3. $\sum_{w \in X^*} r^{-\mathbf{KP}(w)} \leq 1$, *und*
4. *die Zahl* $\sum_{w \in X^*} r^{-\mathbf{KP}(w)}$ *ist links berechenbar.*

Satz 6.12 *Die Funktion* $\mathbf{KP} : X^* \to \mathbb{N}$ *ist das Minimum bezüglich „*$\preceq$*“ in der Klasse aller von oben approximierbaren Funktionen* $f : X^* \to \mathbb{N}$*, die der Bedingung* $\sum_{w \in X^*} r^{-f(w)} < \infty$ *genügen.*

Folgerung 6.13 *1. Zu jedem* $c > 0$ *gibt es unendlich viele* $w \in X^*$ *derart, dass* $\mathbf{KP}(w) > |w| + \log_r |w| + \log_r \log_r |w| + c$.

2. Es gibt ein $c > 0$ *mit* $\mathbf{KP}(w) \leq |w| + \log_r |w| + 2 \cdot \log_r \log_r |w| + c$.

6.3 Berechenbare endliche Maße auf X^*

Definition 6.4 Wir nennen eine Funktion $\mu : X^* \to [0, \infty)$ ein *endliches Maß* auf X^*, falls $\mu(X^*) = \sum_{w \in X^*} \mu(w) < \infty$.

Definition 6.5 Es seien μ, ν endliche Maße. μ *dominiert* ν, falls es ein $c > 0$ mit $\forall w(\mu(w) \geq c \cdot \nu(w))$ gibt.

Satz 6.14 *In der Menge $\mathcal{M}_1$ aller links berechenbaren endlichen Maße μ mit $\mu(X^*) \leq 1$ gibt es ein Maß $\mathbf{m}$ welches alle $\mu \in \mathcal{M}_1$ dominiert.*

Lemma 6.15 *Die Menge $\mathcal{M}_1$ ist numerierbar, d.h. es gibt eine aufzählbare Teilmenge $K \subseteq X^* \times X^* \times (\mathbb{Q} \cap [0,1])$ derart, dass für jedes $\mu \in \mathcal{M}_1$ ein Programm $\pi_\mu \in X^*$ existiert, für welches*

$$\mu(w) = \sup\{q : (\pi_\mu, w, q) \in K\} \quad \textit{gilt.}$$

Lemma 6.16 *Die Funktion $\mu_{\mathbf{KP}} : X^* \to [0,1]$ mit $\mu_{\mathbf{KP}}(w) := |X|^{-\mathbf{KP}(w)}$ gehört zu $\mathcal{M}_1$ und dominiert alle $\mu \in \mathcal{M}_1$.*

Folgerung 6.17 $\mathbf{KP}(w) = -\log_r \mathbf{m}(w) + \mathcal{O}(1)$

6.4 Verbundkomplexität und bedingte Komplexität

Definition 6.6 $\phi : X^* \times \{0,1\} \to X^*$ heißt *partiell-rekursive Präfix-Funktion* $:\Longleftrightarrow$

1. ϕ ist partiell-rekursive Funktion, und
2. $dom\,(\phi) = W \times \{0,1\}$, wobei $W \subseteq X^*$ präfix-frei ist.

Satz 6.18 *Es gibt eine optimale partiell-rekursive Präfix-Funktion* $\varphi^{(2)} : X^* \times \{0,1\} \to X^*$ *derart, dass* $K_{\varphi^{(2)}}(w,v) \leq K_\phi(w,v) + c_\phi$ *für alle partiell-rekursiven Präfix-Funktionen* ϕ *und alle* $w, v \in X^*$ *gilt.*

Es sei wieder $\mathbf{KP} := \mathrm{K}_{\varphi(2)}$.

Folgerung 6.19 *Es gelten*

1. $\mathbf{KP}(w) \leq \mathbf{KP}(w,v) + \mathcal{O}(1)$ *und* $\mathbf{KP}(v) \leq \mathbf{KP}(w,v) + \mathcal{O}(1)$,
2. $\left|\mathbf{KP}(w,v) - \mathbf{KP}(v,w)\right| = \mathcal{O}(1)$
3. *Ist* $\psi :\subseteq X^* \to X^*$ *partiell-rekursiv, so ist* $\mathbf{KP}(w,\psi(w)) \leq \mathbf{KP}(w) + \mathcal{O}(1)$ *für* $v \in dom\,(\psi)$.
4. $\mathbf{KP}(w, \mathsf{string}_r(\mathbf{KP}(w))) = \mathbf{KP}(w) + \mathcal{O}(1)$

Lemma 6.20 $\mathbf{KP}(w,v) \leq \mathbf{KP}(w) + \mathbf{KP}(v) + \mathcal{O}(1)$

Definition 6.7 $\phi : X^* \times X^* \to X^*$ heißt *partiell-rekursive Präfix-Funktion* $:\Longleftrightarrow$

1. ϕ ist partiell-rekursive Funktion, und
2. $\forall \pi, \pi', \nu((\pi, \nu), (\pi', \nu) \in dom\,(\phi) \wedge \pi \sqsubseteq \pi' \to \pi = \pi')$

Satz 6.21 *Es gibt eine optimale partiell-rekursive Funktion* $\varphi^b : X^* \times X^* \to X^*$ *derart, dass*

$$K_{\varphi^b}(w/v) \leq K_\phi(w/v) + c_\phi$$

für alle partiell-rekursiven Präfix-Funktionen ϕ *und alle* $w, v \in X^*$ *gilt.*

Es sei wieder $\mathbf{KP} := \mathrm{K}_{\varphi^{\mathrm{b}}}$.

Folgerung 6.22 *Ist* $\psi :\subseteq X^* \times X^* \to X^*$ *partiell-rekursiv, so gilt* $\mathbf{KP}(\psi(w,v)/v) \leq \mathbf{KP}(w/v) + \mathcal{O}(1)$ *für alle Paare* $(w,v) \in \mathit{dom}\,(\psi)$.

Notation: $\langle w,v\rangle := \mathsf{string}_{\mathrm{r}}(|w|)\cdot w \cdot v$ und
$\langle w,n\rangle := \mathsf{string}_{\mathrm{r}}(|w|)\cdot w \cdot \mathsf{string}_{\mathrm{r}}(n)$ für $n \in \mathbb{N}$.

Lemma 6.23 *1.* $\mathbf{KP}(w,v) \leq \mathbf{KP}(v) + \mathbf{KP}(w/\langle v, \mathbf{KP}(v)\rangle) + \mathcal{O}(1)$

2. $\mathbf{KP}(w,v) \leq \mathbf{KP}(v) + \mathbf{KP}(w/v) + \mathcal{O}(1)$

Satz 6.24 $\mathbf{KP}(w,v) = \mathbf{KP}(v) + \mathbf{KP}(w/\langle v, \mathbf{KP}(v)\rangle) + \mathcal{O}(1)$

7 Komplexität unendlicher Wörter

7.1 X^ω als CANTORscher Raum

Metrik: $\rho(\eta, \xi) := \inf\{r^{-|w|} : w \sqsubset \eta \wedge w \sqsubset \xi\}$

Kugeln in (X^ω, ρ)**:** $w \cdot X^\omega = \{\eta : w \sqsubset \eta\}$

Durchmesser: $\operatorname{diam} w \cdot X^\omega = r^{-|w|}$

Beziehungen zum Einheitsintervall (r-näre Entwicklung)

$$0{,}\eta \in [0,1] \subseteq \mathbb{R} \longleftrightarrow \eta \in X^\omega$$

$$|0{,}\eta - 0{,}\xi| \leq \rho(\eta, \xi)$$

Beispiel

$$\tfrac{1}{5} \longleftrightarrow 00110011\ldots \quad \text{für } r = 2, \text{ aber}$$

$$\tfrac{1}{5} \longleftrightarrow \begin{cases} 19999\ldots \\ 20000\ldots \end{cases} \quad \text{für } r = 10 \qquad \square$$

Satz 7.1 *Ist* $|X|$ *endlich, so ist* (X^ω, ρ) *ein kompakter metrischer Raum.*

Definition 7.1 Eine Teilmenge $F \subseteq X^\omega$ heißt $\mathbf{G}_\delta$*-Menge* $:\Longleftrightarrow$
Es gibt eine abzählbare Familie von offenen Mengen $(E_i)_{i\in\mathbb{N}}$ derart, dass

$$F = \bigcap\nolimits_{i\in\mathbb{N}} E_i \quad \text{gilt.}$$

Satz 7.2 *Es sei* $F \subseteq X^\omega$.

1. F *ist genau dann offen in* (X^ω, ρ) *wenn es ein* $W \subseteq X^*$ *mit* $F = W \cdot X^\omega$ *gibt.*
2. F *ist genau dann abgeschlossen, wenn aus* $\mathbf{A}(\xi) \subseteq \mathbf{A}(F)$ *stets* $\xi \in F$ *folgt.*
3. F *ist genau dann* $\mathbf{G}_\delta$*-Menge in* (X^ω, ρ)*, wenn es ein* $V \subseteq X^*$ *mit*

$$F = \{\xi : \xi \in X^\omega \wedge |\mathbf{A}(\xi) \cap V| = \aleph_0\} \quad \textit{gibt.}$$

Das Lebesgue-Maß auf (X^ω, ρ)

Definition 7.2 Das Lebesgue-Maß auf (X^ω, ρ) ist die durch $\lambda(w \cdot X^\omega) := r^{-|w|}$ auf den Kugeln definierte Mengenfunktion, die in üblicher Weise auf die meßbaren Teilmengen des metrischen Raumes (X^ω, ρ) ausgedehnt wird.

Folgerung 7.3 *1. Ist $W \subseteq X^*$ präfix-frei, so ist*
$\lambda(W \cdot X^\omega) = \sum_{w \in W} r^{-|w|}$.

2. Ist $F \subseteq X^\omega$ abgeschlossen, so gilt
$\lambda(F) = \lim_{n \to \infty} \sum_{w \in \mathbf{A}(F) \cap X^n} r^{-|w|}$.

3. Ist $F \subseteq X^\omega$ eine $\mathbf{G}_\delta$-Menge, so ist genau dann $\lambda(F) = 0$ wenn es ein $V \subseteq X^*$ mit $F = \{\xi : \xi \in X^\omega \wedge |\mathbf{A}(\xi) \cap V| = \aleph_0\}$ derart gibt, dass $\lim_{n \to \infty} \lambda(\{v : v \in V \wedge |v| > n\} \cdot X^\omega) = 0$ gilt.

7.2 Zufällige Reelle Zahlen

Satz 7.4 (MARTIN-LÖF) *Für jedes $\xi \in X^\omega$ gibt es ein $c \in \mathbb{N}$ und unendlich viele $n \in \mathbb{N}$ derart, dass $\mathbf{K}(\xi[0..n]) \leq n - \log_r n + c$.*

Effektive Nullmengen in (X^ω, ρ)

Definition 7.3 Eine Teilmenge $\mathcal{V} \subseteq \mathbb{N} \times X^*$ heißt MARTIN-LÖF-*Test*, falls $\mathcal{V}$ rekursiv aufzählbar ist und für alle $n \in \mathbb{N}$ die Ungleichung $\lambda(\{v : (n, v) \in \mathcal{V}\} \cdot X^\omega) \leq r^{-n}$ gilt.

Wir setzen $V_n := \{v : (n, v) \in \mathcal{V}\}$.

Folgerung 7.5 *Es sei $\mathcal{V}$ ein* MARTIN-LÖF-*Test. Dann gelten:*

1. $\lambda(\bigcap_{i \in \mathbb{N}} V_i \cdot X^\omega) = 0$,
2. *auch $\{(n, w) : \exists v(v \sqsubseteq w \wedge (n, v) \in \mathcal{V})\}$ ist ein* MARTIN-LÖF-*Test.*
3. *Es einen* MARTIN-LÖF-*Test $\mathcal{W}$ derart, dass für alle $i \in \mathbb{N}$ die Menge W_i präfix-frei ist und $\lambda(V_i \cdot X^\omega) = \lambda(W_i \cdot X^\omega)$ gilt.*

Satz 7.6 *Es gibt einen universellen* MARTIN-LÖF*-Test, d.h. einen* MARTIN-LÖF*-Test $\mathcal{U}$ derart, dass für alle* MARTIN-LÖF*-Tests $\mathcal{V}$ die Beziehung $\bigcap_{i\in\mathbb{N}} V_i \cdot X^\omega \subseteq \bigcap_{i\in\mathbb{N}} U_i \cdot X^\omega$ erfüllt ist.*

Definition 7.4 Ein ω-Wort $\xi \in X^\omega$ heißt *zufällig* $:\Longleftrightarrow$ $\xi \notin \bigcap_{i\in\mathbb{N}} U_i \cdot X^\omega$.

Definition 7.5 Ein ω-Wort $\xi \in X^\omega$ heißt *rekursiv* (oder: *berechenbar*) $:\Longleftrightarrow$ die Abbildung $f_\xi : \mathbb{N} \to X^*$ mit $\{f_\xi(n)\} = \mathbf{A}(\xi) \cap X^n$ ist rekursiv.

Folgerung 7.7 *1.* $\lambda(X^\omega \setminus \bigcap_{i\in\mathbb{N}} U_i \cdot X^\omega) = 1$

2. *Kein rekursives ω-Wort ist zufällig.*

3. *Enthält eine der Mengen $\{n : \xi(n) = x\},\ (x \in X)$, eine unendliche rekursive Teilmenge, so ist ξ ist nicht zufällig.*

Lemma 7.8 *Ist $\xi \in X^\omega$ nicht zufällig, so ist die Differenz $|w| - \mathbf{KP}(w)$ für $w \sqsubset \xi$ unbeschränkt.*

Lemma 7.9 *Ist $\xi \in X^\omega$ zufällig, so konvergiert die Reihe $\sum_{w \sqsubset \xi} r^{|w| - \mathbf{KP}(w)}$.*

Satz 7.10 *Es sei $\xi \in X^\omega$. Dann sind die folgenden Bedingungen äquivalent:*

1. *ξ ist zufällig.*
2. *Es gibt eine Konstante $c \in \mathbb{N}$ derart, dass $\mathbf{KP}(w) \geq |w| - c$ für alle $w \sqsubset \xi$ erfüllt ist.*
3. *Es gilt $\sum_{w \sqsubset \xi} r^{|w| - \mathbf{KP}(w)} < \infty$.*

Kolmogorov-Komplexität unendlicher Wörter

$$\begin{aligned} \xi[0..n] &:= \text{Präfix der Länge } n \\ \mathbf{K}_{\mathfrak{U}}(\xi/\cdot) : \mathbb{N} &\to \mathbb{N} \\ \mathbf{K}_{\mathfrak{U}}(\xi/n) &:= \mathbf{K}_{\mathfrak{U}}(\xi[0..n]) \end{aligned}$$

oberer Anstieg:

$$\kappa(\xi) := \limsup_{n\to\infty} \frac{\mathbf{K}_{\mathfrak{U}}(\xi/n)}{n}$$

unterer Anstieg:

$$\underline{\kappa}(\xi) := \liminf_{n\to\infty} \frac{\mathbf{K}_{\mathfrak{U}}(\xi/n)}{n}$$