Wichtige Sätze und Definitionen zu
§2: Minimale Erzeugendensysteme, Worthalbgruppen und Codes
aus der Vorlesung:

LV-NR	150 239
Veranstaltung	Diskrete Mathematik II, 4.0 std
Dozent	Holtkamp, R.

2.1
Sei H Halbgruppe und $E \subseteq H$ Teilmenge.

a) *E heißt* **Erzeugendensystem** *von H $:\Longleftrightarrow$ die kleinste Unterhalbgruppe von H, die E enthält, ist H.*

b) *Allgemein heißt die kleinste Unterhalbgruppe von H, die E enthält, die von E erzeugte Unterhalbgruppe. Bez.: $\langle E \rangle$.*
(Das kleinste Untermonoid von H, das E enthält, heißt von E erzeugtes Untermonoid.)

c) *Ist $\langle E' \rangle \subsetneq \langle E \rangle$ für jede echte Teilmenge $E' \subseteq E$, so sagt man: E ist* **minimales Erzeugendessystem**.

Beispiel
$(\mathbb{N}, +)$, $E = \{1\}$.

Satz 1 (Erzeugung von Unterhalbgruppen)
Für $E_1 := E \subseteq H$ Teilmenge der Halbgruppe H sei $E_n = \{a_1 \circ \ldots \circ a_n \mid a_i \in E\}$, $n \geq 1$ und $U := \bigcup_{n \geq 1} E_n \subseteq H$. Dann ist U Unterhalbgruppe von H und $\langle E \rangle = U$.

Beispiel
$(\mathbb{N}, +)$, $E = \{3, 5\}$.

2.2
Seien $(H, \circ_H)$ und $(H', \circ_{H'})$ Halbgruppen (bzw. Monoide) und $\varphi : H \to H'$ eine Abbildung. Dann heißt φ

a) **Homomorphismus** *von Halbgruppen (bzw. Monoiden)* $\Longleftrightarrow \varphi(a \circ_H b) = \varphi(a) \circ_{H'} \varphi(b)\ \forall\ a, b \in H$ *(und für Monoide fordert man zusätzlich $\varphi(e) = e'$)*

b) **Isomorphismus** *von Halbgruppen (bzw. Monoiden)* $\Longleftrightarrow$ *φ ist bijektiver Homomorphismus (man schreibt $H \cong H'$ falls eine solcher Isomorphismus existiert)*

Beispiel
$\mathbb{N}_0 \to \mathrm{Pot}(\mathbb{N})$

Beispiel
$\left(\mathbb{N}_0^2, +\right)$, $E = \{(1,0), (1,1)\}$, $\langle E \rangle \to \mathbb{N}_0^2 - \{(0,0)\}$

2.3
H heißt **zyklische Halbgruppe** $:\Longleftrightarrow\ \exists\ a \in H$ *mit $E = \{a\}$ ist Erzeugendensytem von H.*

2.4
Sei $\emptyset \neq X$ Menge

a) *Ein Wort der Länge $n \in \mathbb{N}_0$ über (dem Alphabet) X ist eine Abbildung $w : \underline{n} \to X$.*
Bez.: $w = w(1)\, w(2) \ldots w(n)$ oder $w = w_1 w_2 \ldots w_n$
$W_n = W_n(X) :=$ Menge der Wörter der Länge n. Im Fall $n = 0$: $W_0 = \{\varepsilon\}$, wobei ε das **leere Wort** *ist.*

b) *$\mathbb{W}(X) := \bigcup_{n \geq 0} W_n$, die Elemente $v, w \in \mathbb{W}(X)$ heißen* **Wörter** *über X.*
$\mathbb{W}^+(X) := \bigcup_{n \geq 1} W_n = \mathbb{W}(X) - \{\varepsilon\}$

c) **Konkatenation** *von $v \in W_m$ und $w \in W_n$:*
$v \cdot w$ sei das Wort in W_{m+n} mit

$$(v \cdot w)(i) = \begin{cases} v(i) & : 1 \leq i \leq m \\ w(i-m) & : m < i \leq m+n \end{cases}$$

also

$$v \cdot w = v_1 v_2 \ldots v_m w_1 w_2 \ldots w_n$$

Beispiel
abc, 012

Satz 2 (Wortmonoid)
$\mathbb{W}(X)$ zusammen mit der Konkatenation „$\cdot$“ ist Monoid. Das neutrale Element ist das leere Wort ε.
$\mathbb{W}^+(X)$ ist Halbgruppe. Die Zuordnung

$$\begin{aligned} L : \mathbb{W}(X) &\to (\mathbb{N}_0, +) \\ w &\mapsto \text{Länge von } w \end{aligned}$$

ist ein Homomorphisums. L ist ein Isomorphismus, falls $\#X = 1$.

Beispiele
$X = \{0, 1\}$

- $W_1(X) = X$
- $W_2(X) = \{00, 01, 10, 11\}$
- $W_3(X) = \{000, 001, 010, 011, 100, 101, 110, 111\}$

Satz 3 (Induzierter Homomorphismus)
H sei Halbgruppe (bzw. Monoid), X Menge, $\alpha : X \to H$ Abbildung. Dann existiert genau ein Homomorphismus $\bar{\alpha} : \mathbb{W}^+(X) \to (\mathbb{N}_0, +)$ mit $\bar{\alpha}(X) = \alpha(X)$ (für Monoide zusätzlich $\bar{\alpha}(\varepsilon) = 1_H$). Man nennt $\bar{\alpha}$ den von α **induzierten Homomorphismus**.
Weiter gilt:

$$\bar{\alpha} \text{ ist surjektiv} \iff \alpha(X) := \{\alpha(x) : x \in X\} \text{ ist Erzeugendensystem von } H$$

2.5
Sei $C \subseteq \mathbb{W}^+(X)$. C heißt **Code** $:\iff$
wenn $v_1, \ldots, v_m, w_1, \ldots, w_n \in C$ und $v_1 \ldots v_m = w_1 \ldots w_n$ gilt, so folgt $m = n$ und $v_i = w_i \; \forall \; i$.

Folgerung aus Satz 3
Sei $C \subseteq \mathbb{W}^+(X)$ und α die Abbildung

$$\alpha : C \to \mathbb{W}^+(X)$$
$$w \mapsto w$$

Dann ist

$$\bar{\alpha} : \mathbb{W}^+(C) \to \mathbb{W}^+(X)$$

ein Homomorphismus und Bild$\bar{\alpha} = \langle C \rangle$ die Unterhalbgruppe von $\mathbb{W}^+(X)$ erzeugt von C.
Es ist C Code $\iff$ $\bar{\alpha}$ ist injektiv.

2.6
Ein Code C heißt **Präfix-Code** *(oder präfixfreier Code) geanu dann, wenn gilt*

$$\forall\ v \in C \text{ existiert kein } w \in C - \{v\} \text{ mit } w = vv' \text{ für ein } v' \in \mathbb{W}(X)$$

Ein Code C heißt **Suffix-Code** *(oder suffixfreier Code) geanu dann, wenn gilt*

$$\forall\ v \in C \text{ existiert kein } w \in C - \{v\} \text{ mit } w = v'v \text{ für ein } v' \in \mathbb{W}(X)$$

Beispiel
$C = \{00, 0011, 10, 01\}$ *Suffix-Code, aber nicht präfixfrei*
$C = \{0, 010\}$ *weder Suffix- noch Präfix-Code, aber Code*

2.7
Es sei $(H, \circ_H)$ Halbgruppe (bzw. Monoid). Weiter sei

$$\circ_H^{op} : H \times H \to H$$
$$a \circ_H^{op} b \mapsto b \circ_H^{op} a\ \forall\ a, b \in H$$

Man zeigt: H zusammen mit $\circ_H^{op}$ ist eine Halbgruppe (bzw. Monid). Wir bezeichnen $(H, \circ_H^{op})$ auch mit H^{op}.

Satz 4 (Involution der Worthalbgruppe)
Es gilt

$$\mathbb{W}(X)^{op} \cong \mathbb{W}(X)$$

Aufgabe

Es sei $W = \mathbb{W}(\{x_1, x_2, x_3, x_4\})$ und $x_i \neq x_j$ für $i \neq j$.
Es gibt einen Homomorphismus $\varphi : W \to (\mathbb{N}^4, +)$, der x_1 auf $(1,0,0,0)$, x_2 auf $(0,1,0,0)$, x_3 auf $(0,0,1,0)$ und x_4 auf $(0,0,0,1)$ abbildet.
Es sei $C = \{w \in W : \varphi(w) = (1,2,3,4)\}$.

a) Man berechne $\#C$.

b) Ist C ein Code in W?

c) Ist $C \cup \{x_1^2\}$ ein Code in W?

Zunächst: was bewirkt φ?
$\varphi(x_1x_1) = \varphi(x_1) + \varphi(x_1) = (1,0,0,0) + (1,0,0,0) = (2,0,0,0)$
$\varphi(x_1x_2x_1x_4) = \varphi(x_1)+\varphi(x_2)+\varphi(x_1)+\varphi(x_4) = (1,0,0,0)+(0,1,0,0)+(0,0,0,1)+(1,0,0,0) = (2,1,0,1)$
φ zählt die Aufkommen der einzelnen Buchstaben aus dem Alphabet im Wort und stellt die Häufigkeiten in einem Vektor dar.

zu a): Da jedes Wort in C genau 10 Buchstaben hat $(1+2+3+4=10)$, ergeben sich für x_4 zunächst $\binom{10}{4}$ mögliche Stellen im Wort. Nun bleiben für x_3 noch 6 frei Plätze im Wort, also $\binom{6}{3}$ Möglichkeiten. Schließlich bleiben für x_2 noch $\binom{3}{2}$ und für x_1 noch $\binom{1}{1}$ Möglichkeiten. Das ergibt insgesamt $\binom{10}{4} \cdot \binom{6}{3} \cdot \binom{3}{2} \cdot \binom{1}{1} = 12600$ mögliche Wörter.

zu b): Ja. Da jedes Element in C aus genau 10 Buchstaben besteht, ist C sowohl Präfix- als auch Suffix-Code.

zu c): Ja. Durch die Hinzunahme von x_1^2 verliert C weder sein Präfix- noch seine Suffix-Eigenschaft, denn kein Wort in C fängt mit x_1^2 an oder hört mit x_1^2 auf.