Übungsblatt 4

Aufgabe 1. Sei $(A,\cdot)$ eine endliche abelsche Gruppe. Zeigen Sie, dass gilt

$$p(A) := \prod_{a\in A} a = 1$$

außer A besitzt genau eine Involution x. Dann ist $p(A) = x$.

Beweis. Weil A abelsch ist, ist $H := \{a \in A \mid a^2 = 1\}$ eine Gruppe. Wegen $\mathrm{ord}(a) = \mathrm{ord}(a^{-1})$ für alle $a \in A$ erhalten wir

$$p(A) = \prod_{a\in A,\ a^2=1} a \cdot \prod_{a\in A,\ a^2\neq 1} a = \prod_{a\in A,\ a^2=1} a = p(H).$$

Da H eine abelsche Gruppe ist, können wir diese als $\mathbb{Z}$-Modul auffassen. Dies induziert eine $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$-Vektorraum Struktur auf H. Wegen $|H| < \infty$ existiert ein $n \in \mathbb{N}_0$ mit $H \cong \mathbb{F}_2^n$.
Nun besitzt H genau eine Involution x, wenn $n = 1$. In diesem Fall gilt

$$p(A) = p(H) = x.$$

Für $n = 0$ ist offensichtlich $p(H) = 0$ erfüllt. Mit $n > 1$ gilt

$$\begin{aligned}
p(H) &= \sum_{x_1,\dots,x_n\in\mathbb{F}_2} (x_1,\dots,x_n)^t \\
&= \sum_{x_1,\dots,x_{n-1}\in\mathbb{F}_2} (x_1,\dots,x_{n-1},0)^t + \sum_{x_1,\dots,x_{n-1}\in\mathbb{F}_2} (x_1,\dots,x_{n-1},1)^t \\
&= \sum_{x_1,\dots,x_{n-1}\in\mathbb{F}_2} (x_1,\dots,x_{n-1},0)^t + \sum_{x_1,\dots,x_{n-1}\in\mathbb{F}_2} \left((x_1,\dots,x_{n-1},0)^t + (0,\dots,0,1)^t\right) \\
&= 2\cdot \sum_{x_1,\dots,x_{n-1}\in\mathbb{F}_2} (x_1,\dots,x_{n-1},0)^t + 2^{n-1}\cdot(0,\dots,0,1)^t \\
&= 0.
\end{aligned}$$

□

Aufgabe 2. (a) Beweisen Sie zwei der noch nicht bewiesenen Bedingungen der Fehlererkennungen in (7.1) (b).

(b) Zeigen Sie Lemma (7.3).

(c) Begründen Sie Lemma (7.4).

Beweis. (a) Wir zeigen, dass die Prüfzeichenkodierung $C = \{(c_1,\dots,c_n) \in A^n \mid \prod_{i=1}^n \sigma_i(c_i) = c\}$ Einzelfehler erkennt. Sei hierfür $(c_1,\dots,c_n) \in C$, das zu $(c_1,\dots,c_k',\dots,c_n)$ decodiert wird, wobei $1 \le k \le n$ und $c_k' \neq c_k$. Es gilt

$$c^{-1}\cdot\sigma_k(c_k')\cdot\prod_{i=1,\ i\neq k}^{n}\sigma_i(c_i) = \left(\prod_{i=1}^{n}\sigma_i(c_i)\right)^{-1}\cdot\sigma_k(c_k')\cdot\prod_{i=1,\ i\neq k}^{n}\sigma_i(c_i) = \sigma_k(c_k)^{-1}\cdot\sigma_k(c_k').$$

Wegen der Injektivität der Permutation σ_k ist letzteres genau dann das neutrale Element, wenn $c_k = c_k'$.

Wir zeigen, dass die Prüfzeichenkodierung C Transposition benachbarter Elemente unter der Voraussetzung erkennt, dass $x\cdot\sigma_{i+1}\sigma_i^{-1}(y) \neq y\cdot\sigma_{i+1}\sigma_i^{-1}(x)$ für alle $x \neq y$ gilt. Sei hierfür $(c_1,\dots,c_n) \in C$, das zu $(c_1,\dots,c_{k+1},c_k,\dots,c_n)$ decodiert wird, wobei $1 \le k \le n-1$. Es gilt

$$c^{-1}\cdot\sigma_k(c_{k+1})\cdot\sigma_{k+1}(c_k)\prod_{i=1,\ i\neq k,k+1}\sigma_i(c_i) = \sigma_k(c_k)^{-1}\cdot\sigma_{k+1}(c_{k+1})^{-1}\cdot\sigma_k(c_{k+1})\cdot\sigma_{k+1}(c_k) \quad (1)$$

Seien nun $x, y \in A$ mit $\sigma_k^{-1}(y) = c_k$ und $\sigma_k(c_{k+1}) = x$, so kann der Ausdruck (1) wie folgt umgeschrieben werden

$$y^{-1} \cdot (\sigma_{k+1} \circ \sigma_k^{-1}(x))^{-1} \cdot x \cdot \sigma_{k+1} \circ \sigma_k^{-1}(y).$$

Letzteres ist wegen der Voraussetzung genau dann das neutrale Element, wenn $c_k = c_{k+1}$.

Wir zeigen, dass die Prüfzeichenkodierung C Sprungtransposition unter der Voraussetzung erkennt, dass $x \cdot \sigma_{k+2} \circ \sigma_k^{-1}(z) \neq z \cdot \sigma_{k+2} \circ \sigma_{k^{-1}(x)}$ für alle $x \neq z$ gilt. Sei hierfür $(c_1, \ldots, c_n) \in C$, das zu $(c_1, \ldots, c_{k+2}, c_{k+1}, c_k \ldots, c_n)$ decodiert wird, wobei $1 \leq k \leq n-2$. So kann man analog zum vorherigen Fall zeigen, dass die Kodierung Sprungtranspositionen erkennt.

Wir zeigen, dass die Prüfzeichenkodierung C Zwillingsfehler unter der Voraussetzung erkennt, dass $x \cdot \sigma_{k+1} \circ \sigma_k^{-1}(x) \neq y \cdot \sigma_{k+1} \circ \sigma_k^{-1}(y)$ für alle $x \neq y$ gilt. Sei hierfür $(c_1, \ldots, c_k, c_k, \ldots, c_n) \in C$, das zu $(c_1, \ldots, c'_k, c'_k, \ldots, c_n)$ decodiert wird, wobei $1 \leq k \leq n-1$. So gilt mit $x = \sigma_k(c_k)$ und $y = \sigma_k(c'_k)$

$$c^{-1} \cdot \sigma_k(c'_k) \cdot \sigma_k(c'_k) \dot{\prod}_{i=1,\ i \neq k,k+1} \sigma_i(c_i) = x^{-1} \cdot (\sigma_{k+1} \circ \sigma_k^{-1}(x))^{-1} \cdot y \cdot \sigma_{k+1} \circ \sigma_k^{-1}(y).$$

Letzteres ist wegen der Voraussetzung genau dann das neutrale Element, wenn $c_k = c'_k$ gilt.

(b) Sei A eine endliche abelsche Gruppe und $T \in \mathrm{Sym}(A)$. Die Permutation T ist nach Definition genau dann antisymmetrisch, wenn für alle $x, y \in A$ mit $x \neq y$ gilt $xT(y) \neq yT(x)$. Da A abelsch ist, ist letzters äquivalent zu $x^{-1}T(x) \neq y^{-1}T(y)$ für alle $x, y \in A$ mit $x \neq y$, d.h. $\mathrm{inv} \cdot T$ ist injektiv. Da A endlich ist, ist die Injektivität von $\mathrm{inv} \cdot T$ äquivalent zu seiner Surjektivität, d.h. $\mathrm{inv} \cdot T \in \mathrm{Sym}(A)$ und ist somit vollständig.

Analog kann man unter denselben Voraussetzungen beweisen, dass T genau dann antisymmetrisch ist, wenn $\mathrm{inv} \circ T$ vollständig ist.

(c) Wir beweisen, dass es genau dann einen Prüfzeichencode auf einer endlichen abelschen Gruppe A gibt, der Nachbarschaftstranspositionen erkennt, wenn A eine vollständige Permutation besitzt.

Sei C eine Prüfzeichenkodierung mit assoziierten Permutationen σ_i $(1 \leq i \leq n)$, die Nachbarschaftstranspostionen erkennt. Nach Vorlesung gilt $x\sigma_{i+1} \circ \sigma_i^{-1}(y) \neq y\sigma_{i+1} \circ \sigma_i^{-1}(x)$ mit $x \neq y$. So ist $\sigma_{i+1} \circ \sigma_i^{-1}$ eine vollständige Permutation von A. Sei andersherum T eine vollständige Permutation von A, so setze $\sigma_i := T^i$ für $1 \leq i \leq n$. Es gilt $x\sigma_{i+1} \circ \sigma_i^{-1}(y) = xT(y) \neq yT(x) = y\sigma_{i+1} \circ \sigma_i^{-1}(x)$ für $x \neq y$.

□

Aufgabe 3. Sei A eine abelsche Gruppe der Ordnung $a \in \mathbb{N}_0$.

(a) Zeigen Sie: Ist A eine zyklische Gruppe, dann besitzt A zu jedem Teiler d von a genau eine Untergruppe der Ordnung d.

(b) Zeigen Sie, dass auch für allgemeines abelsches A zu jedem Teiler d von a eine Untergruppe der Ordnung d gibt. Ist diese im Allgemeinen eindeutig?

(a) *Beweis.* Seien $A = \langle x \rangle$ und $a = d \cdot k$ für ein $1 \leq k \leq a$, so hat die Untergruppe $\langle x^k \rangle$ die Ordnung d. Sei nun H eine Untergruppe von A der Ordnung d, so zeigen wir im Folgenden, dass $H = \langle x^k \rangle$ gilt. Betrachte den folgenden Gruppenepimorphismus

$$\pi : \mathbb{Z} \longrightarrow A,\ 1 \longmapsto x.$$

Es existiert ein $n \in \mathbb{N}_0$ mit $\pi^{-1}(H) = n\mathbb{Z}$. D.h. $\pi(n) = x^n$ ist ein Erzeuger von H und damit folgt $n = \frac{a}{d} = k$.

□

(b) *Beweis.* Nach dem Hauptsatz endlich erzeugter abelscher Gruppen existieren $t \in \mathbb{N}_0$ und Primzahlpotenzen $1 < r_1 \leq \ldots \leq r_t$, sodass $A \cong \bigoplus_{i=1}^{t} \mathbb{Z}/r_i\mathbb{Z}$. Insbesondere gilt $a = \prod_{i=1}^{t} r_i$ und für einen Teiler d von a existieren somit (nicht zwigend eindeutige) $d_1, \ldots, d_t$ mit $d_i \mid r_i$ für alle $1 \leq i \leq t$ und $d = d_1 \cdots d_t$. Da die Faktoren $\mathbb{Z}/r_i\mathbb{Z}$ zyklisch sind, existieren nach Teilaufgabe (a) Untergruppen $H_i \leq \mathbb{Z}/r_i\mathbb{Z}$ der Ordnung d_i. Die Untergruppe $H = H_1 \oplus \ldots \oplus H_t \subseteq A$ hat nun die gewünschte Ordnung $|H| = \prod_{i=1}^{t} |H_i| = d_1 \cdots d_t = d$. □

Die Eindeutigkeit ist i.A. nicht gegeben. Betrachte hierfür zwei endliche Gruppen G_1 und G_2 mit jeweils gerader Ordnung. So existieren nach dem Satz von Cauchy $g_1 \in G_1$ und $g_2 \in G_2$ mit $\operatorname{ord}(g_1) = \operatorname{ord}(g_2) = 2$. Die Untergruppen $\langle g_1 \rangle \times \{1\}$ und $\{1\} \times \langle g_2 \rangle$ von $G_1 \times G_2$ sind verschieden und der Ordnung zwei. Man kann z.B. $G_1 = G_2 = \mathbb{Z}/2\mathbb{Z}$ wählen.

Aufgabe 4. Untersuchen Sie den ISBN-Code in Beispiel 7.1 (c) daraufhin, ob er Einzelfehler, Nachbarschaftstranspositionen, Sprungtranspositionen oder Sprung-Zwillingsfehler erkennt.

(1) Wir zeigen, dass der ISBN-Code $C = \left\{(c_1, \ldots, c_{10})^t \in \mathbb{Z}/11\mathbb{Z} \mid 0 = \sum_{i=1}^{10} c_i(11-i)\right\}$ Einzelfehler erkennt. Sei hierfür $(c_1, \ldots, c_{10})^t \in C$, das zu $(c_1, \ldots, c_k', \ldots, c_{10})^t$ decodiert wird, wobei $1 \leq k \leq 10$ und $c_k' \neq c_k$. Es gilt

$$-kc_k' - \sum_{i=1,\ i\neq k}^{10} c_i \cdot i = -kc_k' - \sum_{i=1,\ i\neq k}^{10} c_i \cdot i + \sum_{i=1,}^{10} c_i \cdot i = k(c_k - c_k').$$

Da $\mathbb{Z}/11\mathbb{Z}$ ein Körper ist, ist obiger Ausdruck genau dann 0, wenn $c_k = c_k'$.

Der ISBN-Code ist eine Prüfzeichenkodierung und somit folgt die Erkennung von Einzelfehlern aus Aufgabe 2 (a).

(2) Wir zeigen, dass C Nachbartranspositionen erkennt. Sei hierfür $(c_1, \ldots, c_{10})^t \in C$, das zu $(c_1, \ldots, c_{k+1}, c_k, \ldots, c_{10})^t$ decodiert wird, wobei $1 \leq k \leq 9$. Es gilt

$$\begin{aligned}
&-(k+1)c_k - kc_{k+1} - \sum_{i=1,\ i\neq k,k+1}^{10} c_i \cdot i \\
=&-(k+1)c_k - kc_{k+1} - \sum_{i=1,\ i\neq k,k+1}^{10} c_i \cdot i + \sum_{i=1}^{10} c_i \cdot i \\
=&-(k+1)c_k - kc_{k+1} + kc_k + (k+1)c_{k+1} \\
=&-c_k + c_{k+1}.
\end{aligned}$$

Letzteres ist genau dann 0, wenn $c_k = c_{k+1}$.

(3) Wir zeigen, dass C Sprungtranspositionen erkennt. Sei hierfür $(c_1, \ldots, c_{10})^t \in C$, das zu $(c_1, \ldots, c_{k+2}, c_{k+1}, c_k, \ldots, c_{10})^t$ decodiert wird, wobei $1 \leq k \leq 8$. Es gilt

$$-kc_{k+2} - (k+2)c_k - \sum_{i=1,\ i\neq k,k+2}^{10} c_i \cdot i + \sum_{i=1}^{10} c_i \cdot i = 2(c_{k+2} - c_k).$$

Letzteres ist genau dann 0, wenn $c_k = c_{k+2}$.

(4) Wir zeigen, dass C Sprungzwillingsfehler erkennt. Sei hierfür $(c_1, \ldots, c_{10})^t \in C$ mit $c_k = c_{k+2}$, das zu $(c_1, \ldots, c_k', c_{k+1}, c_k', \ldots, c_{10})^t$ decodiert wird, wobei $1 \leq k \leq 8$. Es gilt wegen $c_k = c_{k+2}$ und $c_k' = c_{k+2}'$

$$-kc_k' - (k+2)c_{k+2}' - \sum_{i=1,\ i\neq k,k+2}^{10} c_i \cdot i + \sum_{i=1}^{10} c_i \cdot i = 2(k+1)(c_k - c_k').$$

Da $1 \leq k \leq 9$ gilt, ist $2(k+1) \neq 0$ und somit ist die Gleichung genau dann 0, wenn $c_{k+2} = c_k = c_k' = c_{k+2}'$.