24.01.11

Mittwoch, 10. Januar 2024 09:22

zu 2 Sei $c = a_1 \dots a_m \in C$ und es werde a_i durch a_i' mit $a_i' \neq a_i$ ersetzt. Dann gilt: dieser Einzelfehler wird nicht erkannt $\overset{(*)}{\Leftrightarrow}$ $g_i a_i' \equiv g_i a_i \bmod q$

Wie in 1) gilt $a_i' - a_i \equiv t \bmod q$ mit $t \neq 0$.

„$\Leftarrow$" g_i teilerfremd zu q $\Rightarrow$ es gibt $g_i^{-1} \in \mathbb{Z}_q$ mit $g_i^{-1} g_i \equiv 1 \bmod q$. $\Rightarrow$ $t \equiv g_i^{-1} g_i (a_i' - a_i) \bmod q$ $\Rightarrow$ $g_i (a_i' - a_i) \equiv g_i t \bmod q$. Da $\operatorname{ggT}(g_i, q) = 1$ und $t \in \{-q+1, \dots, q-1\} \setminus \{0\}$ ist $g_i t \not\equiv 0 \bmod q$ $\overset{(*)}{\Rightarrow}$ Einzelfehler wird erkannt.

„$\Rightarrow$" Angenommen: g_i nicht teilerfremd zu q mit $t > 1$ so dass $t \mid g_i$ und $t \mid q$. Dann wähle $a_i' := \frac{q}{t}$ und $a_i := 0$. Damit $g_i a_i' \equiv \frac{g_i}{t} \cdot q \equiv 0 \bmod q$ $\Rightarrow$ $g_i a_i' - g_i a_i \equiv 0 \bmod q$ $\overset{(*)}{\Rightarrow}$ Einzelfehler wird nicht erkannt im Widerspruch zur Voraussetzung. □

Beispiel 172 ISBN-Code: $q = 11$

3 - 528 - 12345 - 1 $= a_1 a_2 \dots a_{10}$ wobei

↑ Sprache ↑ Verlag ↑ Buch-Nr. ↑ Prüfziffer

$a_i \in \{0, 1, \dots, 9, X\}$

Sprache Verlag Buch Nr. Prüfziffer

mit Gewichten $g_i := 11 - i$. Formal also

$$C := \{ a_1 - a_{10} \mid a_1, \dots, a_{10} \in \{0,1,\dots,9,X\} \text{ mit } 10a_1 + 9a_2 + \dots + 2a_9 + 1a_{10} \equiv 0 \bmod 11 \}$$

Da alle Gewichte teilerfremd zu 11 sind, erkennt C alle Einzelfehler. Da für $i \neq j$ gilt: $|g_i - g_j| \in \{1,\dots,10\}$ ist $g_i - g_j$ teilerfremd zu $q = 11$ also element C auch alle Vertauschungsfehler. Bestimmung der Prüfziffer für den ISBN-Code:

$3-528-06783-?$ $\rightsquigarrow 10\cdot 3 + 9\cdot 5 + \dots + 2\cdot 3 = 235$

$\Rightarrow a_{10} = 7$

$3-528-06786-?$ $\Rightarrow 10\cdot 3 + \dots + 2\cdot 6 = 241$

$\Rightarrow a_{10} \equiv -1 \bmod 11$

$\Rightarrow a_{10} \equiv 10 \bmod 11$

$\Rightarrow a_{10} = X$

Codes über Gruppen

Im folgenden sei $(G,\cdot)$ eine (nicht notwendigerweise kommutative) Gruppe. Dabei sei also $\cdot : G \times G \to G$. (9,4)

mutative) Gruppe. Dabei sei also $\cdot : G \times G \to G$, $(g,h) \mapsto g \cdot h$ die Verknüpfung, e das neutrale Element und g^{-1} das zu g inverse Element.

Beispiele sind $(\mathbb{Q}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}_p, \cdot)$ für p Primzahl, $(\mathbb{Z}_m, +)$.

Definition 173 Ein Code über eine Gruppe $(G, \cdot)$ der Länge n mit Kontrollsymbol $c \in G$ ist gegeben durch $C = \{ (g_1, \dots, g_n) \in G^n \mid g_1 \cdot g_2 \cdot \dots \cdot g_n = c \}$

Beispiel 174 $(G, \cdot) = (\mathbb{Z}_{10}, +)$ mit $c = 0$ liefert den Paritätscode aus Beispiel 164 mit $n = 5$.

Satz 175 Jeder Code aus Dfn 173 erkennt Einzelfehler

Beweis Wir betrachten oBdA die erste Stelle. Sei dazu $(g_1, \dots, g_n) \in C$ und $g_1' \neq g_1$. Zu zeigen: $(g_1', \dots, g_n) \notin C$. Annahme: $(g_1', \dots, g_n) \in C \Rightarrow g_1' g_2 \dots g_n = c = g_1 \dots g_n$. Multipliziere nun nacheinander $g_n^{-1}, \dots, g_2^{-1}$ von rechts, so ergibt sich der Widerspruch

$g_n = g_i^{-1}$ □

Bemerkung 176 1) Der Beweis zu 175 zeigt, dass die Wahl von c unerheblich ist. 2) Vorteil von Gruppencodes ist, dass Gruppen i. Allg. nicht kommutativ sind, also $gh \neq hg$ möglich ist. Man erhält folgende Verallgemeinerung um Vertauschungsfehler zu erkennen.

Definition 177 Ein Code der Länge n über die Gruppe $(G,\cdot)$ mit Kontrollsymbol $c \in G$ und Permutationen $\pi_1, \dots, \pi_n \in S_G := \{\pi : G \to G \mid \pi \text{ bijektiv}\}$ ist gegeben durch

$$C := \{(g_1, \dots, g_n) \in G^n \mid \pi_1(g_1) \cdot \pi_2(g_2) \cdot \dots \cdot \pi_n(g_n) = c\}$$

Beispiel 178 $(G,\cdot) = (\mathbb{Z}_{10}, +)$ und C Paritätscode mit Gewichten $s_1, \dots, s_n$ wobei s_i teilerfremd zu 10 ist. für $i \in \{1, \dots, n\}$. Dann ist durch $\pi_i : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$, $x \mapsto s_i \cdot x$ eine Permutation (mit Umkehrabbildung $y \mapsto s_i^{-1} \cdot y$) gegeben. So ist C ein Gruppencode über $(\mathbb{Z}_{10}, +)$ mit Permutationen $\pi_1, \dots, \pi_n$.

Gruppencode über $(\mathbb{Z}_{10}, +)$ mit Permutationen $\pi_1 - \pi_n$.

Nachweis, dass π_i bijektiv ist:

injektiv $\pi_i(x) = \pi_i(y) \Rightarrow s_i x \equiv s_i y \mod 10 \Rightarrow$

$\Rightarrow s_i(x-y) \equiv 0 \mod 10 \overset{s_i \nmid 10}{\Rightarrow} 10 \mid x-y \Rightarrow x = y$,

denn $x, y \in \{0, \dots, 9\}$

surjektiv Sei $x \in \mathbb{Z}_{10}$, $ggT(10, s_i) = 1 \overset{\text{Bezout}}{\Rightarrow}$

$1 = 10 \cdot a + s_i \cdot b \Rightarrow x \equiv s_i \cdot b \cdot x \mod 10$

$\Rightarrow \pi_i(bx) = s_i bx \equiv x \mod 10$

Satz 179 Ein Gruppencode wie im Dfn 177 erkennt

a) Einzelfehler

b) Vertauschungen benachbarter Stellen $i, i+1$ für $i \in \{1, \dots, n-1\}$ falls $\pi_i(g)\pi_{i+1}(h) \neq \pi_i(h)\pi_{i+1}(g)$ für alle $g, h \in G$ gilt. (*)

Beweis a) Übung

b) Sei $(g_1, \dots, g_n) \in C$, also $\pi_1(g_1) \cdots \pi_n(g_n) = c \in G$.

Eine Vertauschung an den Stellen i und $i+1$ wird

nicht erkannt $\Leftrightarrow$ $\pi_1(g_1) \cdots \pi_i(g_{i+1})\pi_{i+1}(g_i) \cdots \pi_n(g_n)$

$= c = \pi_1(g_1) \cdots \pi_n(g_n) \Leftrightarrow \pi_i(g_{i+1})\pi_{i+1}(g_i) \overset{(*)}{=} \pi_i(g_i)\pi_{i+1}(g_{i+1})$

Multiplikation mit $\pi_n(g_n)^{-1}, \dots, \pi_{i+2}(g_{i+2})^{-1}$ von rechts

Multiplikation mit $\pi_1(g_1)^{-1}, \dots, \pi_{i-1}(g_{i-1})^{-1}$ von links

Wenn die Voraussetzung in 2) erfüllt ist, folgt also aus dass Vertauschungen erkannt werden. □

Bemerkung 180 In $(\mathbb{Z}_{10}, +)$ kann man keine Permutationen wählen so dass (✗) erfüllt ist. Soll die Prüfziffer aus 10 Element wählbar sein, benutzt man eine nicht-kommutative Gruppe mit 10 Elementen. Man kann Symmetriegruppe des regulären 5 Ecks nehmen: