24.01.09

Dienstag, 2. Januar 2024 09:54

Fehlererkennung

Grundidee: Sei V eine Menge. Eine Teilmenge $C \subset V$ heißt fehlererkennender Code, wenn es folgende Prozedur ermöglicht: ein Sender übermittelt $c \in C$, der Empfänger empfängt ein möglicherweise verändertes $c' \in V$ und prüft ob $c' \in C$ ist. Dabei ist C so gewählt, dass der Empfänger eine Prüfprozedur durchführen kann

Definition 163 Es sei $q \in \mathbb{N}$, $q \geq 2$. Für $V := \{ a_1 a_2 \dots a_n \mid a_1, \dots, a_n \in \{0, \dots, q-1\} \}$ heißt $C := \{ a_1 \dots a_n \in V \mid a_1 + \dots + a_n \equiv 0 \mod q \}$ Paritätscode zur Basis q der Länge n

Beispiel 164 $q = 10$ und $n = 5$.

$$C = \{ a_1 a_2 a_3 a_4 a_5 \in V \mid a_1 + a_2 + a_3 + a_4 + a_5 \equiv 0 \mod 10 \}$$

$a_1 a_2 a_3 a_4$ = Information, a_5 = Prüfziffer

Die Prüfziffer wird so gewählt, dass die Summe aller Ziffern durch 10 teilbar ist.

Information: 1342 → Prüfziffer = 0 → $13420 \in C$

Dagegen ist $13426 \notin C$ denn $1+3+4+2+6 \equiv 16 \equiv 6 \bmod 10$

Definition 165 Es sei $C \subset V$ ein Code. Ein Element $c \in C$ nennt man Codewort. Wird ein Codewort an einer Stelle verändert so nennt man dies einen Einzelfehler. Werden zwei verschiedene Stellen des Codewortes vertauscht heißt das Vertauschungsfehler

Beispiel 166 Der Code aus Dfn 163 erkennt keine Vertauschungsfehler.

Satz 167 Jeder Paritätscode C zur Basis q der Länge n erkennt Einzelfehler.

Beweis Es sei $c = a_1 \dots a_n \in C$ o.B.d.A. verändert zu $c' := a_1' a_2 \dots a_n$ mit $a_1 \neq a_1' \in \{0, \dots, q-1\}$. Annahme: $c' \in C \Rightarrow a_1' + \dots + a_n \equiv 0 \equiv a_1 + \dots + a_n \bmod q$

$\Rightarrow a_1' \equiv a_1 \bmod q \Rightarrow a_1 = a_1'$ ↯ □

Beispiel 168 Um Vertauschungsfehler zu erkennen, stattet man Paritätscodes mit Gewichten aus, zum Bsp wie bei Kontonummern:

Kto No 1 8 9 8 2 0 1 8

Gewichte 1 2 1 2 1 2 1 2

Produkt 1 16 9 16 2 0 1 16 $\xrightarrow{\Sigma}$ 61 $\rightsquigarrow$ Prüfziffer = 9

durch Aufrunden auf 10er $\rightsquigarrow$ KtoNo mit Prüfziffer =

1 8 9 8 2 0 1 9

Prüfziffer

Formal: $C := \{ a_1 a_2 \cdots a_8 \mid 1\cdot a_1 + 2\cdot a_2 + \cdots + 1\cdot a_8 \equiv 0 \mod 10 \}$

Definition 169 Eine Menge

$C := \{ a_1 a_2 \ldots a_m \mid a_1, \ldots, a_n \in \{0, \ldots, q-1\},\ \sum_{i=1}^{n} g_i a_i \equiv 0 \mod q \}$

heißt Paritätscode der Basis $q \in \mathbb{N}$, $q \geq 2$, der Länge $n \in \mathbb{N}$ mit Gewichten $g_1, \ldots, g_n \in \mathbb{Z}$ (PCBG)

Lemma 170 Ist in Dfn 169 die Zahl g_n teilerfremd zu q, dann lässt sich (die Prüfziffer) a_n aus (der Information) $a_1, \ldots, a_{n-1}$ und den Gewichten berechnen.

Beweis Nach Satz 154 gibt es $g_n^{-1} \in \mathbb{Z}$ so dass $g_n^{-1} \cdot g_n \equiv 1 \mod q$ ist. Dann: $c \in C \Rightarrow \sum_{i=1}^{n} g_i a_i \equiv 0 \mod q$

$$\Rightarrow g_n a_n \equiv -\sum_{i=1}^{n-1} g_i a_i \mod q$$

$$\Rightarrow a_n \equiv g_n^{-1} \left(-\sum_{i=1}^{n-1} g_i a_i \right) \mod q \quad \square$$

Satz 17.1 Ein PCBG erkennt

1) Vertauschungen an den Stellen $i<j$ genau dann, wenn $g_j - g_i$ teilerfremd zu q ist

2) Einzelfehler an der Stelle i genau dann, wenn g_i teilerfremd zu q ist.

Beweis zu 1) sei $c = a_1 - a_n \in C$ und a_i, a_j die vertauschten Stellen, also insbesondere $a_i \neq a_j$ $(i<j)$.

Es gilt: die Vertauschung wird nicht erkannt

$$\Longleftrightarrow \quad g_1 a_1 + \cdots + g_i a_j + \cdots + g_j a_i + \cdots + g_n a_n \equiv 0$$

$$\equiv \sum_{i=1}^{n} g_i a_i \mod q$$

$$\Longleftrightarrow \quad g_i a_j + g_j a_i \equiv g_i a_i + g_j a_j \mod q$$

$$\Longleftrightarrow \quad (g_i - g_j)(a_j - a_i) \equiv 0 \mod q$$

$\Longleftarrow$: Sei $g_i - g_j$ teilerfremd zu q. Nach Voraussetzung ist $a_i \neq a_j \in \{0, \ldots, q-1\}$ also $a_j - a_i = t \in \{-q+1, \ldots, q-1\}$ also $a_j - a_i \equiv t \mod q$ mit $t \neq 0$. Damit ist $(g_i - g_j)(a_j - a_i) \equiv (g_i - g_j)\, t \mod q$. Es ist aber $(g_i - g_j)\, t \not\equiv 0 \mod q$, denn andernfalls: $(g_i - g_j)\, t = N \cdot q$

$$\Rightarrow \quad \frac{(g_i - g_j)\, t}{q} = N \in \mathbb{Z} \quad \Rightarrow \quad q \mid t \;\; \text{↯ zu}$$

$\Rightarrow \quad \frac{(g_i - g_j)\, t}{q} = N \in \mathbb{Z} \quad \Rightarrow \quad q \mid t$ ↯ an ✓

$q \nmid (g_i - g_j)$

Also wird die Vertauschung erkannt.

$\Leftarrow$" Annahme: $g_i - g_j$ ist nicht teilerfremd zu q und $t > 1$ so dass $t \mid g_i - g_j$ und $t \mid q$. Wähle $a_i := \frac{q}{t}$ und $a_j = 0$, dann gilt: $(g_i - g_j)(a_j - a_i) = (g_j - g_i)\frac{q}{t}$

$= \underbrace{\frac{(g_j - g_i)}{t}}_{\in \mathbb{Z}} \cdot q \equiv 0 \mod q$ im ↯ dazu dass die Vertauschung nach Voraussetzung erkannt wird.