Anwendung: Prüfziffern

In gewissen Situationen ist die Vergabe einer eindeutigen Nummer hilfreich (IBAN, Produktnummern, ISBN$_{000}$). Gesucht sind Systeme, die Eingabefehler möglichst gut erkennen.

Der häufigste Fehler ist, dass eine Ziffer falsch ist.

echt: 5473 eingegeben 5873

Lösung: Eine weitere Ziffer, so dass die Quersumme ein Vielfaches von 10 ist.

code: 54731 eingeg: 58731

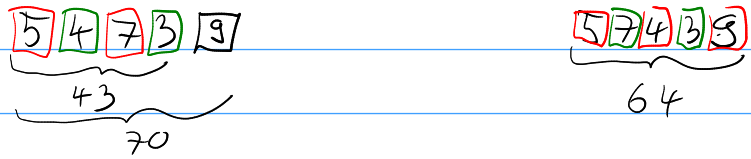
Dies deckt bereits ca. 80% der Fehler ab.

Der zweithäufigste Fehler ist das Vertauschen zweier benachbarter Ziffern.

z.B. statt 54731 : 57431 (ca. 10%)

Unser System mit Quersumme hilft hier nicht weiter.

Lösung (ISBN): Quersumme der geraden Stellen + 3× Quersumme der ungeraden ist vielfaches von 10:



Allgemein: Vertauschte Ziffer z_j und z_{j+1}. (o.B.d.A. $j=1$)

echt: $3z_1 + z_2 +$ Rest ist Vielfaches von 10.

fehlerhaft: $3z_2 + z_1 +$ Rest soll kein Vielfaches von 10 sein, dann wird der Fehler erkannt.

Differenz: $2z_1 - 2z_2 \stackrel{?}{=}$ Vielfaches von 10

$2(z_1 - z_2)$ ist Vielfaches von 10 ?

Falls $z_1 - z_2 = \pm 5$ wird Fehler nicht erkannt,

$z_1 - z_2 \neq \pm 5$ wird Fehler erkannt.

Diese Systeme lassen sich mit Hilfe von Gruppentheorie verbessern:

Ziffern: $\{0, 1, \ldots, q\}$ wir fassen diese als Elemente einer Gruppe auf, z.B. $\{\bar{0}, \bar{1}, \ldots \bar{q}\} = \mathbb{Z}/10\mathbb{Z}$

Allgemeines Prüfziffernsystem: gegeben sind n Permutationen π_j auf G, $j = 1, \ldots n$ und ein $g_0 \in G$.
(G muß nicht unbedingt 10 Elemente haben)

Der Algorythmus überprüft, ob $\sum_{j=1}^{n} \pi_j(z_j) = g_0$

(Im letzten Bsp. war $g_0 = \bar{0}$, $\pi_j = id$ bzw. $\pi_j(z) = 3z$ falls j gerade bzw. ungerade)

Satz: Ein solches Prüfziffernsystem erkennt den Fehler "Vertippen bei einer Stelle", d.h.

$$\sum_{j=1}^{n} \pi_j(z_j) \neq \sum_{j=1}^{n} \pi_j(\tilde{z}_j) \quad \text{falls}$$

$z_j \neq \tilde{z}_j$ für genau ein $j \in \{1, \ldots, n\}$

Beweis: Wir benutzen die Kürzungsregel

$$\pi_1(z_1) \oplus \pi_2(z_2) \oplus \ldots \oplus \pi_j(z_j) \oplus \ldots = \pi_1(z_1) \oplus \ldots \pi_j(\tilde{z}_j) \oplus \ldots$$

$\Leftrightarrow$ (Kürzungsregel) $\quad \pi_j(z_j) \oplus \ldots = \pi_j(\tilde{z}_j) \oplus \ldots$

$\Leftrightarrow$ " $\quad \pi_j(z_j) = \pi_j(\tilde{z}_j)$

$\Leftrightarrow$ π bijektiv $\quad z_j = \tilde{z}_j$

ooo

Ringe und Körper

Definition: Sei R eine Menge, $\oplus : R \times R \to R$ und $\odot : R \times R \to R$ seien Verknüpfungen. $(R, \oplus, \odot)$ heißt Ring mit Einselement falls gelten:

a) $(R, \oplus)$ ist eine kommutative Gruppe

b) Es existiert ein Element $1_R \in R$ mit $1_R \odot a = a \odot 1_R = a$ für alle $a \in R$.

c) Es gilt für $\odot$ das Assoziativitätsgesetz

$$(a \odot b) \odot c = a \odot (b \odot c)$$

d) Es gelten folgende Distributivitätsgesetze:

$$(a \oplus b) \odot c = (a \odot c) + (b \odot c) \quad \text{und} \quad a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$$

Falls zusätzlich das Kommutativgesetz für $\odot$ gilt, also

e) $a \odot b = b \odot a$.

so nennt man $(R, \oplus, \odot)$ kommutativen Ring.

Falls $(R \setminus \{0\}, \odot)$ auch eine kommutative Gruppe ist, nennt man den Ring $(R, \oplus, \odot)$ auch Körper.

(Falls $(R \setminus \{0\}, \odot)$ eine nicht-kommutative Gruppe, dann nennt man $(R, \oplus, \odot)$ auch Schiefkörper).

Notation: Wir schreiben einfach 0 und 1 für die entsprechenden neutralen Elemente von $\oplus$ bzw. $\odot$.

Wir benutzen die Punkt vor Strich Konvention.

Bemerkung: Falls $0 = 1$ so ist $R = \{0\}$ (Nullring).

Beweis: ~~betrachte $0 \cdot 1 = 1$ da $0 = 1$ $(1 \cdot 1 = 1)$~~

~~$0 \cdot 1 = 0$ trivial, da 1 neutral~~

Sei $a \in R$ betrachte $a \cdot 1 = a \cdot 0 = 0$

$= a$

Warum ist $(a \cdot 0) = 0$?

$a \cdot 0 = a \cdot (0 \oplus 0) = a \cdot 0 \oplus a \cdot 0$

Kürzungsregel: $0 = (a \cdot 0)$

Bsp: a) $(\mathbb{Z}, +, \cdot)$ ist kommutativer Ring.

b) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ sind Körper

c) $(M(n \times n), +, \cdot)$ ist Ring.

d) Die Menge aller Polynome zum Körper K in einer Variablen ist mit $+$ und $\cdot$ ein Ring (kommutativ).

$$K[t] := \left\{ \sum_{i=0}^{\infty} a_i t^i \text{ mit } a_i \neq 0 \text{ für endlich viele } i \in \mathbb{N} \right\}$$

Das größte i mit $a_i \neq 0$ nennen wir Grad des Polynoms, das zugehörige a_i "Leitindex".