Algebra 4

Eine Anwendung: Prüfziffersysteme

- In vielen praktischen Fällen spielen Ziffernfolgen eine Rolle, zum Beispiel Kontonummern, Artikelnummern bei Waren (Strichcode), oder Nummern von Geldscheinen.

  Bei der Verarbeitung dieser Zahlen können Fehler auftreten, etwa durch falsche Eingabe per Hand oder durch Probleme beim automatischen Einlesen. Um fehlerhafte Nummern zu erkennen, verwendet man nun die folgende Idee: man fügt bei jeder Nummer eine zusätzliche Ziffer hinzu — sie wird als ***Prüfziffer*** bezeichnet —, die nach einem bestimmten Algorithmus aus den vorherigen Ziffern berechnet wird.

  Nehmen wir an, wir haben eine Nummer, bei der die letzte Stelle eine Prüfziffer ist. Wir kennen den Algorithmus zur Berechnung der Prüfziffer. Dann nehmen wir die erste bis vorletzte Stelle der Zahl, berechnen die Prüfziffer und vergleichen mit der letzten Stelle. Stimmen die Ziffern nicht überein, ist die vorliegende Nummer fehlerhaft.

  Die Umsetzung dieser Idee nennt man ein ***Prüfziffersystem***, man spricht auch von ***Prüfzeichencodierung***.

- Bekannte Prüfziffersysteme.

  Die Idee der Prüfzeichencodierung wird in vielen bekannten Fällen verwendet. Wir zählen vier Beispiele auf, die mit unterschiedlichen Algorithmen zur Prüfzeichenberechnung arbeiten.

  - Der EAN-Code, besonders der EAN-13-Code wird bei den meisten Waren des täglichen Lebens verwendet. Er besteht aus 13 Ziffern und wird üblicherweise auch als Strichcode zum automatischen Einlesen angegeben. EAN steht für „Europäische Artikelnummer“.
  - Die (alten) ISBN-Nummern zur Kennzeichnung von Büchern. ISBN ist die Abkürzung für „Internationale Standardbuchnummer“.
  - Die Postgironummern.
  - Die Nummern der alten deutschen Geldscheine.

- Verwendung algebraischer Strukturen.

  Man muß bei einem Prüfziffersystem nicht unbedingt Nummern haben, die aus den Ziffern 0, 1, ..., 9 bestehen; der ISBN-Code verwendet beispielsweise 11 Zeichen. Der Algorithmus zur Berechnung der Prüfziffer arbeitet dann eventuell nicht mehr mit den Regeln des normalen Zahlenrechnens, sondern mit den Verknüpfungen einer passenden algebraischen Struktur; beim ISBN-Code arbeitet man in der Struktur $(\mathbb{Z}_{11}, \oplus, \odot)$.

- Typen von Fehlern.

  Prüfziffersysteme sollen Fehler aufdecken. Angenommen, die Ziffernfolge 200741803 ist korrekt. Wir machen uns die drei häufigsten Fehlertypen an Beispielen klar.

  Einzelfehler: 200741303

  Nachbartransposition (Zahlendreher): 200748103

  Sprungtransposition: 200740813

- Welche Fehler werden erkannt?

  Die vier oben genannten Prüfziffersysteme verwenden unterschiedliche Algorithmen. Das hat Auswirkungen auf die Fehlererkennung.

  - Der EAN-13-Code erkennt zwar alle Einzelfehler aber nicht alle Transpositionsfehler; es gibt auch Nachbar-Transpositionsfehler, die nicht erkannt werden.
  - Der ISBN-Code erkennt alle Einzelfehler und alle Transpositionsfehler, sogar Sprungtranspositionen!

- Beispiel: Zur Einführung betrachten wir einen einfachen Algorithmus für Ziffernfolgen beliebiger Länge, die aus den Ziffern 0, 1, ..., 9 bestehen können. Die Prüfziffer wird bei unserem Verfahren so gewählt, daß die Quersumme der Ziffernfolge ein Vielfaches von 10 ist.

  Wir zeigen:

  (a) Einzelfehler werden erkannt.

  (b) Transpositionsfehler werden nicht erkannt.

- Beispiel: Der EAN-13-Code.

  Der EAN-13-Code besteht aus 13-stelligen Artikelnummern. Für die 13 Positionen sind alle Zahlen 0, 1, ..., 9 erlaubt. Die Prüfziffer an der 13. Stelle wird so berechnet, daß die Kontrollgleichung

  $$a_1+a_3+a_5+a_7+a_9+a_{11}+a_{13}+3(a_2+a_4+a_6+a_8+a_{10}+a_{12}) \equiv 0 \pmod{10}$$

  gilt. Die gerade Stellen werden also mit dem Faktor 3 gewichtet.

Wir zeigen:

(a) Einzelfehler werden erkannt.

(b) Transpositionsfehler werden teilweise erkannt.

- Beispiel: Der ISBN-Code.

  Der ISBN-Code besteht aus 10 Stellen, wobei für jede Stelle die Symbole 0, 1, ..., 9 sowie X erlaubt sind; X ist die römische Zehn und steht für das Element 10 aus $(\mathbb{Z}_{11}, \oplus, \odot)$. Das Prüfzeichen an der letzten Stelle wird so berechnet, daß die Kontrollgleichung

  $$a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9 + 10a_{10} \equiv 0 \pmod{11}$$

  erfüllt ist.

  Wir zeigen:

  (a) Einzelfehler werden erkannt.

  (b) Alle Transpositionsfehler werden erkannt (auch Sprungtranspositionsfehler).

  Bei dem Beweis kann man verwenden, daß $(\mathbb{Z}_{11}, \oplus, \odot)$ ein Körper ist und deshalb keine Nullteiler enthält.

  Der EAN-13-Code leistet im Grunde deshalb weniger als der ISBN-Code, weil $(\mathbb{Z}_{10}, \oplus, \odot)$ ein Ring mit Nullteilern und kein Körper ist.

- Beispiel: Der Code der Postgironummern.

  Postgironummern sind 10-stellige Zahlen, für jede Stelle sind die Zeichen 0, 1, ..., 9 erlaubt, die letzte Stelle ist die Prüfziffer. In der Kontrollgleichung wird Modulo 10 gerechnet; vorher werden die einzelnen Stellen nicht wie beim EAN- oder beim ISBN-Code unterschiedlich gewichtet, sondern speziellen Permutationen unterworfen.

  Es werden alle Einzelfehler aber nicht alle Nachbartranspositionsfehler erkannt. Details siehe Literatur.

- Beispiel: Der Code der alten deutschen Geldscheine.

  Bei diesem Code werden zunächst spezielle Permutationen verwendet, dann wird zur Berechnung der Prüfziffer mit einer Kontrollgleichung gearbeitet, deren Verknüpfungen in der nichtkommutative Diedergruppe D_5 berechnet werden.

  Es werden alle Einzelfehler und fast alle Nachbartranspositionsfehler erkannt. Details siehe Literatur[1].

[1] Albrecht Beutelspacher, *Vertrauen ist gut, Kontrolle ist besser! Vom Nutzen elementarer Mathematik zum Erkennen von Fehlern.* Erschienen in: Jahrbuch Überblicke Mathematik 1995, Seite 27–37. Vieweg-Verlag. (Ist in der Bibliothek vorhanden.)