Beispiel 162

Für $K = \mathbb{Z}_2 = GF(2)$ und $p(x) = x^2 + x + 1$ gilt in ähnlicher Weise

$$\mathbb{Z}_2[x]/(p) = \{0, 1, x, x+1\} .$$

Für die Addition und Multiplikation modulo p ergibt sich

$+_p$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot_p$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Aus diesen beiden Tabellen folgt, dass $\mathbb{Z}_2[x]/(p)$ mit den angegebenen Verknüpfungen $+_p$ und $\cdot_p$ einen Körper mit 4 Elementen bildet (den wir schon früher gesehen haben).

Beispiel 163

Für $K = \mathbb{Z}_2$ und $q(x) = x^2 + 1$ gilt wiederum

$$\mathbb{Z}_2[x]/(q) = \{0, 1, x, x+1\} .$$

Für die Addition und Multiplikation modulo q ergibt sich nunmehr jedoch

$+_q$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot_q$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	1	$x+1$
$x+1$	0	$x+1$	$x+1$	0

Aus der zweiten Tabelle folgt, dass $\mathbb{Z}_2[x]/(q) \setminus \{0\}$ bzgl. $\cdot_q$ keine Gruppe bildet. Der Grund ist, dass q nicht irreduzibel ist.

3.8 Redundante Datenspeicherung und Fehlerkorrektur

Seien natürliche Zahlen k, t und s so gewählt, dass

$$k + 2t \leq 2^s - 1 \; .$$

Sei weiter $K = GF(2^s)$, und seien $c_0, \ldots, c_{k-1} \in K$. Wir fassen die c_i sowohl als Elemente von K als auch (in frei festzulegender, eindeutiger Weise) als *Binärwörter der Länge* s auf.

Sei weiter α ein primitives Element in $K = GF(2^s)$ (existiert nach Satz 127) und seien

$$
\begin{aligned}
g(x) &:= \prod_{i=1}^{2t}(x-\alpha^i)\ , \\
c(x) &:= \sum_{i=0}^{k-1} c_i x^i\ , \text{ und} \\
d(x) = \sum_{i=0}^{k+2t-1} d_i x^i &:= g(x)\cdot c(x)\ .
\end{aligned}
$$

Wir sagen, dass der Vektor der Koeffizienten von $d(x)$ den Vektor $(c_0, \ldots, c_{k-1})$ kodiert (Reed-Solomon-Code $RS(s,k,t)$).

Satz 164

Für jedes $s \in \mathbb{N}$ und $k, t \in \mathbb{N}$ mit $k + 2t \leq 2^s - 1$ ist der Reed-Solomon-Code $RS(s, k, t)$ t-fehlerkorrigierend und $2t$-fehlererkennend.

Das bedeutet, dass, falls bei der Übertragung des Vektors der d_i nicht mehr als $2t$ der d_i's verändert werden, dies erkannt werden kann. Werden höchstens t der d_i's verändert, so können die ursprünglichen d_i's sogar rekonstruiert werden.

Beweis:

Sei $(f_0, \ldots, f_{k+2t-1})$ der sich nach der Übertragung ergebende Code-Vektor, sei $e_i := f_i - d_i$ für $i = 0, \ldots, k + 2t - 1$, und seien

$$e(x) := \sum_{i=0}^{k+2t-1} e_i x^i \text{ und } f(x) := \sum_{i=0}^{k+2t-1} f_i x^i \ .$$

Dann gilt $f(x) = d(x) + e(x)$, und es folgt

$$f(\alpha^i) = e(\alpha^i) \qquad \text{für alle } 1 \leq i \leq 2t \ .$$

Beweis (Forts.):

In Matrixschreibweise sieht dies wie folgt aus:

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \dots & \alpha^{k+2t-1} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \dots & \alpha^{2(k+2t-1)} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \dots & \alpha^{3(k+2t-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{2t} & \alpha^{4t} & \alpha^{6t} & \dots & \alpha^{2t(k+2t-1)} \end{pmatrix} \cdot \begin{pmatrix} e_0 \\ e_1 \\ e_2 \\ \vdots \\ e_{k+2t-2} \\ e_{k+2t-1} \end{pmatrix} = \begin{pmatrix} f(\alpha) \\ f(\alpha^2) \\ f(\alpha^3) \\ \vdots \\ f(\alpha^{2t}) \end{pmatrix} .$$

Falls nur $e_{i_1}, \dots, e_{i_r}$ ungleich 0 sind, fallen Spalten weg und es ergibt sich

$$\begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_r} \\ \alpha^{2i_1} & \alpha^{2i_2} & \dots & \alpha^{2i_r} \\ \alpha^{3i_1} & \alpha^{3i_2} & \dots & \alpha^{3i_r} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{2ti_1} & \alpha^{2ti_2} & \dots & \alpha^{2ti_r} \end{pmatrix} \cdot \begin{pmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_r} \end{pmatrix} = \begin{pmatrix} f(\alpha) \\ f(\alpha^2) \\ f(\alpha^3) \\ \vdots \\ f(\alpha^{2t}) \end{pmatrix} .$$

Beweis (Forts.):

Immer wenn die Anzahl r der Spalten $\leq$ der Anzahl $2t$ der Zeilen ist, hat diese Matrix vollen Spaltenrang (Vandermonde-Matrix).

- Wenn $(e(\alpha^i) =)\ f(\alpha^i) = 0$ für $i = 1, \ldots, 2t$, dann ist $e_i = 0$ für alle i eine Lösung, und zwar dann die einzige (Spaltenrang).
- Falls $\leq t$ Fehler aufgetreten sind, können wir entsprechende e_{i_j} eindeutig bestimmen (z.B. durch Probieren) und damit die d_i rekonstruieren.

□

4. Die elementaren Zählfunktionen

4.1 Untermengen

Definition 165 (Binomialkoeffizienten)

$$\binom{n}{0} := 1 \qquad \forall n \in \mathbb{N}_0$$

$$\binom{n}{k} := 0 \qquad n < k, n \in \mathbb{N}_0, k \in \mathbb{N}$$

$$\binom{n}{k} := \binom{n-1}{k} + \binom{n-1}{k-1} \qquad \text{sonst} \quad (n, k \in \mathbb{N})$$

Satz 166

Sei N eine Menge mit $|N| = n$ Elementen. Die Menge aller k-elementigen Untermengen von N wird bezeichnet mit

$$\binom{N}{k}.$$

Es gilt:

$$\left|\binom{N}{k}\right| = \binom{|N|}{k} = \binom{n}{k}.$$

Beweis:

Seien $n, k \geq 0$, $a \in N$.

1. $\binom{n}{0}$ und $k > n$ sind klar.
2. Definiere

$$S_a := \left\{ A \in \binom{N}{k};\ a \in A \right\},$$

$$\tilde{S}_a := \left\{ A \in \binom{N}{k};\ a \notin A \right\}.$$

Beweis (Forts.):

3. Damit gilt

$$S_a \cup \tilde{S}_a = \binom{N}{k}, \quad S_a \cap \tilde{S}_a = \emptyset.$$

$$|S_a| = \left|\binom{N \setminus \{a\}}{k-1}\right| = \binom{n-1}{k-1} \quad \text{(per Induktion)}$$

$$|\tilde{S}_a| = \left|\binom{N \setminus \{a\}}{k}\right| = \binom{n-1}{k} \quad \text{(per Induktion)}$$

Daraus folgt

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

□

Zwischenbemerkung zur Nomenklatur:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = (a+b)\cdot(a+b)\cdots(a+b)$$

4.2 Partitionen von Mengen und Zahlen

4.2.1 Ungeordnete Partitionen

1. Mengenpartitionen

Sei N eine Menge der Kardinalität n und sei $k \in \mathbb{N}_0$. Eine Zerlegung von N in k nichtleere, paarweise disjunkte Teilmengen heißt eine k-Partition von N. Die einzelnen Teilmengen heißen auch Klassen. Ihre Anzahl wird mit

$$S_{n,k}$$

bezeichnet (die sog. Stirling-Zahlen der 2. Art).

Beispiel 167

$N = \{1, 2, 3, 4, 5\},\ k = 2$

$$\{1\} \cup \{2, 3, 4, 5\} \qquad \{1, 2\} \cup \{3, 4, 5\}$$
$$\{2\} \cup \{1, 3, 4, 5\} \qquad \{1, 3\} \cup \{2, 4, 5\}$$
$$\{3\} \cup \{1, 2, 4, 5\} \qquad \{1, 4\} \cup \{2, 3, 5\}$$
$$\{4\} \cup \{1, 2, 3, 5\} \qquad \{1, 5\} \cup \{2, 3, 4\}$$
$$\{5\} \cup \{1, 2, 3, 4\} \qquad \{2, 3\} \cup \{1, 4, 5\}$$
$$\{2, 4\} \cup \{1, 3, 5\}$$
$$\{2, 5\} \cup \{1, 3, 4\}$$
$$\{3, 4\} \cup \{1, 2, 5\}$$
$$\{3, 5\} \cup \{1, 2, 4\}$$
$$\{4, 5\} \cup \{1, 2, 3\}$$

$\Rightarrow S_{5,2} = 15.$

Weiter gilt: $S_{n,1} = 1, S_{n,2} =$ Übung, $S_{n,n} = 1.$

2. Zahlpartitionen

Sei

$$\mathbb{N}_0 \ni n = n_1 + n_2 + \ldots + n_k$$

mit $n_1, \ldots, n_k \in \mathbb{N}$ und $n_1 \geq n_2 \geq \ldots \geq n_k$.

Eine solche Zerlegung heißt k-Partition der Zahl n.

Die Anzahl aller k-Partitionen von $n \in \mathbb{N}$ wird mit

$$P_{n,k}$$

bezeichnet.

Beispiel 168

$n = 8$, $k = 4$.

$$
\begin{aligned}
8 &= 5 + 1 + 1 + 1 \\
&= 4 + 2 + 1 + 1 \\
&= 3 + 3 + 1 + 1 \\
&= 3 + 2 + 2 + 1 \\
&= 2 + 2 + 2 + 2
\end{aligned}
$$

$\Rightarrow P_{8,4} = 5$

4.2.2 Geordnete Partitionen

1. Mengenpartitionen

Seien N, n, k wie vorher. Eine (beliebig) *geordnete* k-Menge $\subseteq N$ heißt k-Permutation aus N. Ihre Anzahl ist

$$n \cdot (n-1) \cdots (n-k+1) = n^{\underline{k}}$$

(„n hoch k fallend“, „fallende Fakultät“).

Analog:

$$n^{\overline{k}} := n \cdot (n+1) \cdots (n+k-1)$$