Proseminar „Codierungstheorie“
Thema 3: Perfekte Codes

Wiederholung

Sei C ein Code der Länge n über einem Alphabet K.

1. Für $|C| > 1$, ist $d(C) = \min\{d(c, c')|c, c' \in C, c \neq c'\}$ die Minimaldistanz von C. Für $|C| = 1$, setzen wir $d(C) = 0$.
2. Ist $d(C) = d$ und $M = |C|$, so sagen wir, dass C ein (n, M, d)-Code über K.
3. Ist $|K| = q$, so gilt:
   $|B_r(u)| = \sum_{j=0}^{r} \binom{n}{j}(q-1)^j$. Insbesondere ist $B_r(u)$ nicht von u abhängig.

Perfekte Codes

Definition:
Sei C ein Code der Länge n über dem Alphabet K.
Wir nennen C **perfekt**, falls ein $e \in \mathbb{N}$ exisitiert, so dass $K^n = \bigsqcup_{c \in C} B_e(c)$.

Satz:

Sei C ein Code der Länge n über dem Alphabet K mit $|K| = q$. Ferner gelte für die Minimaldistanz $d(C) \geq 2e + 1$ mit $e \in \mathbb{N}_0$.

1. **Hammingschranke**
   Es gilt: $q^n \geq |C| \sum_{j=0}^{e} \binom{n}{j}(q-1)^j$
2. **Kugelpackungsgleichung**
   C ist perfekt $\iff q^n = |C| \sum_{j=0}^{e} \binom{n}{j}(q-1)^j$

Beispiele: (triviale perfekte Codes)
$C = K^n$ und einelementige C sind stets perfekte Codes.
Im Fall $C = K^n$ ist die Minimaldistanz $d(C) = 1$. Aus $d(C) \geq 2e + 1$ ergibt sich dann $e = 0$ und damit ist die Kugelpackungsgleichung erfüllt:

$$q^n = |C| \sum_{j=0}^{e} \binom{n}{j}(q-1)^j = |K^n| \sum_{j=0}^{e} \binom{n}{j}(q-1)^j = |K^n| = q^n$$

Im Fall $|C| = 1$ gilt mit dem binomischen Lehrsatz:

$$q^n = \sum_{j=0}^{\infty} \binom{n}{j}(q-1)^j = \sum_{j=0}^{e} \binom{n}{j}(q-1)^j \text{ für } e \geq n \text{ da n ganzzahlig.}$$

Ferner ist der binäre Wiederholungscode ungerader Länge $n = 2e+1$ perfekt. Er enthält nur die beiden Codeworte $c = (0, ..., 0)$ und $c' = (1, ..., 1)$. Also ist die Minimaldistanz $d(C) = d(c, c') = 2e + 1$ und man kann ganz K^n mit den beiden Kugeln vom Radius $e = \frac{n-1}{2}$ um c und c' überdecken.
Man nennt diese Codes die **trivialen perfekten Codes**.

Weiteres Beispiel:
Sei $K = \mathbb{F}_2 = \{0, 1\}$ der Körper mit zwei Elementen.

$$\text{Wir setzen } C = \left\{ (c_1, \ldots, c_7) | c_i \in K, \begin{array}{r} c_1 + c_4 + c_6 + c_7 = 0 \\ c_2 + c_4 + c_5 + c_7 = 0 \\ c_3 + c_4 + c_6 + c_7 = 0 \end{array} \right\}$$

$\Rightarrow$ C ist ein perfekter 1-fehlerkorrigierender $(7, 2^4, 3)$-Code.

Singleton-Schranke

Satz:
Ist $q \geq 3, e \geq 3$ oder $q = 2, e \geq 4$ und $n \leq e + 1$, so gibt es keinen perfekten $(n, |C|, 2e + 1)$-Code über einem Alphabet mit q Elementen.

Satz:
Sei C ein Code der Länge n über einem Alphabet mit q Elementen. Ist d die Minimaldistanz von C, so gilt:

$$\mathbf{d \leq n - \log_q |C| + 1}$$

Codes, für welche Gleichheit gilt, heißen MDS-Codes (Maximum Distance Spearable Codes).

Beispiel:
Sei $K = \mathbb{F}_2 = \{0, 1\}$ wieder der Körper mit zwei Elementen.
Setze $C = \{(c_1, \ldots, c_4) | c_i \in K,\ c_1 + c_2 + c_3 + c_4 = 0\}$, d.h.
C ist die Menge aller binären 4-Tupel mit einer geraden Anzahl von Einsen.
Somit ist $|C| = 8$ und die Minimaldistanz $d = 2$.

$$\Rightarrow n - \log_q |C| + 1 = 4 - \underbrace{\log_2 8}_{3} + 1 = 2 = d$$

Damit ist C ein binärer $(4, 2^3, 2)$-MDS-Code.