Übungsblatt 9

Kryptographie und Kodierungstheorie
WiSe 16/17

Aufgabe 9.1. Für einen Körper F mit q Elementen sei $G_n^k(F)$ die Menge der k-dimensionalen Unterräume von F^n. Zeigen Sie, dass $|G_n^k(F)|$ gleich dem *Gaußschen Binomialkoeffizienten* $\binom{n}{k}_q$ ist, d.h.

$$|G_n^k(F)| = \binom{n}{k}_q = \frac{[q]_n}{[q]_k[q]_{n-k}},$$

wobei wir für ein beliebiges q und ein $n \in \mathbb{Z}_{\geq 0}$ die Schreibweise

$$[q]_n = (q^n - 1)(q^{n-1} - 1) \cdots (q - 1)$$

benutzen und per Konvention $[q]_0 = 1$ ist.
Hinweis: Die Kardinalität in der Frage ist gleich der Anzahl der Folgen von k linear unabhängigen Vektoren in F^n dividiert durch $|\mathrm{GL}(k, F)|$. Als nächstes sollten Sie sich fragen, wie viele Vektoren ungleich 0 es in F^n gibt. Falls w ein solcher Vektor ist, wie viele Vektoren ungleich 0 gibt es in $F^n \backslash \{a \cdot w \mid a \in F\}$ usw.

Aufgabe 9.2. Gegeben sei der lineare Code $C \subseteq \mathbb{F}_2^6$ mit Erzeugermatrix

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

a) Welche Abschätzungen für das Minimalgewicht von C liefert die Griesmer-Schranke?

b) Man bestimme eine Kontrollmatrix H von C.

c) Man bestimme aus der Kontrollmatrix das Minimalgewicht von C.

Aufgabe 9.3. Sei C ein $[n, k, d]_q$-Code und sei $d \geq 2$. Zeige, dass es eine Stelle i gibt, so dass der Code C' ein $[n-1, k, d-1]_q$-Code ist, welcher aus C durch streichen der i-ten Stelle in allen Codewörtern hervorgeht.

Aufgabe 9.4. Mit einer geeigneten Anpassung des Beweises der Gilbert-Varshamov-Schranke beweise man, dass für einen gegebenen Körper $\mathbb{F}_q$ und gegebenem $d \leq n$ auch ein linearer $[n, k, d]_q$-Code existiert, so dass $n - \log_q V_q(n, d-1) \leq k$ gilt.

Aufgabe 9.5. *Wiederholung (Bonus)*
Sei C ein (n, k)-Code über $\mathbb{F}_q$ und sei D ein (n, l)-Code über demselben Körper.

a) Für $E = \{(x, y) \mid x \in C, y \in D\}$ zeige man $d(E) = \min\{d(C), d(D)\}$.

b) Für $E = \{(x, x+y) \mid x \in C, y \in D\}$ zeige man $d(E) = \min\{2d(C), d(D)\}$.

c) Wie kann man in Teil b) aus Erzeugermatrizen für C und D eine Erzeugermatrix von E konstruieren?

d) Wie kann man unter Ausnutzung von Teil b) rekursiv $(2^m, m+1)$-Codes mit Minimalgewicht 2^{m-1} für $m \in \mathbb{Z}_{\geq 1}$ konstruieren?

e) Man bestimme eine Erzeugermatrix eines $(32, 6)$-Codes mit Minimalgewicht 16.