plus (evtl.) der letzten Zeile. Dann ist aber $w(R) = 6$.

∎

Zum Begriff: erweiterter binärer Golay Code

Def.: Sei $C \subseteq \mathbb{F}_q^n$ ein Code. Der erweiterte Code $\overline{C}$ ist definiert als

$$\overline{C} = \left\{ (x_1, \dots, x_{n+1}) \in \mathbb{F}_q^{n+1} : (x_1, \dots, x_n) \in C, \sum_{i=1}^{n+1} x_i = 0 \right\}.$$

Lemma Sei $C \subseteq \mathbb{F}_2^n$ ein binärer Code mit ungeradem Minimaldistanz d. Dann ist die Minimaldistanz von $\overline{C}$ gleich $d+1$.

Bew.: selbst

Def.: Der binäre Golay Code G_{23} ist der Code, den man aus G_{24} erhält, wenn man die Koordinate τ_{10} aus jedem Codewort streicht.

Bem.: a) $\overline{G_{23}} = G_{24}$

b) G_{23} ist ein $[23, 12, 7]$-Code (Kann ab 3 Fehler korrigieren)

c) $\mathcal{G}_{23}$ ist ein perfekter Code.

Ausblick: Warum ist $\mathcal{G}_{24}$ (bzw. $\mathcal{G}_{23}$) so besonders?

* Theorem (van Lint, Tietäväinen, 1973)
Sei C ein binärer Code, der mehr als einen Fehler korrigieren kann, und der perfekt ist.
Dann ist C entweder der Wiederholungscode ($C = \{0^n, 1^n\}$) oder $C = \mathcal{G}_{23}$.

* Spezielle Symmetrien: $\mathrm{Aut}(\mathcal{G}_{24}) = M_{24}$
Mathieugruppe; sporadische einfache Gruppe.
($\rightsquigarrow$ Klassifikation endlicher einfacher Gruppen).

* Kugelpackungen: Mit Hilfe von $\mathcal{G}_{24}$ kann man die dichteste Kugelpackung in Dimension 24 konstruieren ($\rightsquigarrow$ Leech-Gitter).
sehr aktuelle Forschung: Cohn, Kumar, Miller, Radchenko, Viazovska (März 2016).

§2 Reed-Solomon Codes

Singleton-Schranke

Def.: $A_q(n,d) = \max\{M : \exists\, C \subseteq \mathbb{F}_q^n \quad (n,M,d)\text{-Code}\}$.

Satz (Singleton, 1964)

$$A_q(n,d) \leq q^{n-d+1}.$$

Bew.: Es gilt $A_q(n+1,d+1) \leq A_q(n,d)$, weil:

Sei $C \subseteq \mathbb{F}_q^{n+1}$ ein Code mit Minimaldistanz $d(C) \geq 2$.

Definiere den **punktierten Code**

$$\dot{C} = \{x \in \mathbb{F}_q^n : \exists\, x_{n+1} \in \mathbb{F}_q : (x, x_{n+1}) \in C\}$$

Es ist $|\dot{C}| = |C|$, weil $d(C) \geq 2$. Außerdem ist $d(\dot{C}) \in \{d(C), d(C)-1\}$, also

$$A_q(n+1,d+1) \leq A_q(n,d).$$

Induktiv folgt nun die Beh.:

$$A_q(n,d) \leq A_q(n-1,d-1) \leq \ldots \leq A_q(n-d+1,1) = q^{n-d+1}. \quad \boxtimes$$

Def.: Ein linearer Code $C \subseteq \mathbb{F}_q^n$ mit Parametern $[n, k, d]$, der $k = n - d + 1$ ($d = n - k + 1$) erfüllt, heißt MDS-Code.

MDS-Code = maximum distance separable.

erfüllen die Singleton-Schranke mit Gleichheit.

Def: Sei $\mathbb{F}_q$ ein endlicher Körper. Sei $n, k \in \mathbb{N}$, so dass $k \leq n \leq q$. Wähle $\alpha_1, \dots, \alpha_n \in \mathbb{F}_q$ paarweise verschieden. Der Reed-Solomon-Code $RS_{q,n,k}$ ist definiert als

$$RS_{q,n,k} = \{ (f(\alpha_1), \dots, f(\alpha_n)) \in \mathbb{F}_q^n : f \in \mathbb{F}_q[x], \deg f \leq k-1 \}.$$

Bsp: $RS_{3,3,2}$ $\quad (\alpha_1 = 0, \alpha_2 = 1, \alpha_3 = 2)$

$$= \{ \underset{0}{000}, \underset{1}{111}, \underset{2}{222}, \underset{X}{012}, \underset{X+1}{120}, \underset{X+2}{201},$$

$$\underset{2X}{021}, \underset{2X+1}{102}, \underset{2X+2}{210} \}$$

Klar: $RS_{q,n,k}$ ist ein $[n, k]$-Code über $\mathbb{F}_q$.

Erzeugermatrix von $RS_{q,n,k}$: Wähle Monomialbasis $1, X, \dots, X^{k-1}$

Dann ist

$$G = \begin{bmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \vdots & \vdots & & \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_n^{k-1} \end{bmatrix}$$

eine Vandermonde-Matrix der Größe $k \times n$

Satz $RS_{q,n,k}$ ist ein MDS-Code.

Bew.: 2.2. $d(RS_{q,n,k}) \geq n-k+1$.

Wissen: $f \in \mathbb{F}_q[x]$, $\deg f \leq k-1 \Rightarrow f$ hat höchstens $k-1$ Nullstellen in $\mathbb{F}_q$.

[Jede Nullstelle spaltet einen linearen Faktor von f ab.]

Seien $f, g \in \mathbb{F}_q[x]$, $\deg f \leq k-1$, $\deg g \leq k-1$, $f \neq g$.

Dann ist

$$d\big((f(\alpha_1),\dots,f(\alpha_n)) - (g(\alpha_1),\dots,g(\alpha_n))\big)$$

$$= d\big((h(\alpha_1),\dots,h(\alpha_n))\big) \quad \text{für } h = f-g \in \mathbb{F}_q[x],\ \deg h \leq k-1$$

$$= n - |\{\alpha_i : h(\alpha_i) = 0\}|$$

$$\geq n-k+1.$$

☒