Satz Sei $C \subseteq \mathbb{F}_2^{24}$ ein $[24, 12, 8]$-Code, der

i) selbst-dual ist $(C = C^\perp)$

ii) doppelt-gerade ist $(4 \mid w(x)$ für alle $x \in C)$.

Dann gilt

$$W_C(X,Y) = X^{24} + 759\, X^{16} Y^8 + 2576\, X^{12} Y^{12} + 759\, X^8 Y^{16} + Y^{24}.$$

Bew.:

Lemma Sei $C \subseteq \mathbb{F}_2^n$ ein linearer Code, der selbst-dual ist und der gerade ist $(2 \mid w(x)$ für alle $x \in C)$. Dann ist $A_{n-i} = A_i$ für alle $i = 0, \dots, n$.

Bew.: $\rightarrow$ Blatt 2.

Nach Lemma und nach Vor. hat W_C die folgende Form

$$W_C(X,Y) = X^{24} + A_8 X^{16} Y^8 + A_{12} X^{12} Y^{12} + A_8 X^8 Y^{16} + Y^{24}.$$

MacWilliams-Identität

$$W_{C^\perp}(X,Y) = W_C(X,Y) = \frac{1}{4096} W_C(X+Y, X-Y)$$

$$= \frac{1}{4096} \Big((X+Y)^{24} + A_8 (X+Y)^{16} (X-Y)^8 + A_{12} (X+Y)^{12} (X-Y)^{12}$$
$$+ A_8 (X+Y)^8 (X-Y)^{16} + (X-Y)^{24} \Big)$$

Koeffizientenvergleich liefert:

(X^{24}) $\quad 4096 = 1 + A_8 + A_{12} + A_8 + 1$

$\qquad\qquad = 2 + 2A_8 + A_{12}$

$(X^{22} Y^2)$ $\quad 0 = 276 + 20 A_8 - 12 A_{12} + 20 A_8 + 276$

$\qquad\qquad = 552 + 40 A_8 - 12 A_{12}.$

Lösen des LGS $\rightsquigarrow$ $A_8 = 759$

$A_{12} = 2576.$ $\boxtimes$

<u>Frage</u>: Gibt es einen solchen Code?

<u>Antwort</u>: Ja (nächstes Kapitel). Dies ist der erweiterte binäre Golay-Code.

N. J. A. Sloane: „one of the most important of all codes".

Kapitel 2 Konstruktionen

§ 1 Der Golay Code

Konstruktion des erweiterten binären Golay Codes $\mathcal{G}_{24}$ mit Parametern $[24, 12, 8]$.

[M. J. E. Golay (1902–1989): Notes on Digital Coding, 1949].

Anwendung: Voyager 1, 2 NASA-Raumsonde
(Bilder von Jupiter, Saturn, ...)

Def.: $\mathcal{G}_{24} \subseteq \mathbb{F}_2^{24}$ ist definiert durch die folgende Erzeugermatrix

$G=$

l												r												
∞	0	1	2	3	4	5	6	7	8	9	10	∞	0	1	2	3	4	5	6	7	8	9	10	row
1	1												1	1		1	1	1				1		0
1		1												1	1		1	1	1				1	1
1			1										1		1	1		1	1	1				2
1				1										1		1	1		1	1	1			3
1					1										1		1	1		1	1	1		4
1						1										1		1	1		1	1	1	5
1							1						1				1		1	1		1	1	6
1								1					1	1				1		1	1		1	7
1									1				1	1	1				1		1	1		8
1										1				1	1	1				1		1	1	9
1											1		1		1	1	1				1		1	10
												1	1	1	1	1	1	1	1	1	1	1	1	11

Fig. 2.13. Generator matrix for extended Golay code $\mathcal{G}_{24}$. The columns are labelled $l_\infty l_0 l_1 \cdots l_{10} r_\infty r_0 \cdots r_{10}$. The 11×11 matrix on the right is A_{11}.

(S. 65, MacWilliams, Sloane – The theory of error correcting codes, 1977)

<u>Theorem</u> Der Golay-Code $\mathcal{G}_{24}$ besitzt die folgenden Eigenschaften:

a) $\mathcal{G}_{24}$ ist ein $[24,12]$-Code

b) $\mathcal{G}_{24}$ ist selbstdual, $(\mathcal{G}_{24})^\perp = \mathcal{G}_{24}$

c) Für alle $x \in \mathcal{G}_{24}$ gilt $4 \mid w(x)$, d.h. $\mathcal{G}_{24}$ ist doppelt gerade.

d) $\mathcal{G}_{24}$ ist invariant unter Permutation der Koordinaten

$$\sigma = (l_\infty\ r_\infty)(l_0\ r_0)(l_1\ r_{10})(l_2\ r_9)\ldots(l_{10}\ r_1)$$

e) $d(\mathcal{G}_{24}) = 8$.

<u>Bew.:</u> a) Die Spalten $l_0, \ldots, l_{10}, l_\infty$ sind linear unabhängig.

b) Es genügt zu zeigen, dass $\mathcal{G}_{24} \subseteq (\mathcal{G}_{24})^\perp$ gilt, da i.A. $n = \dim C + \dim C^\perp$.

Betrachte die Matrix A_{11} (Zeilen: $0, \ldots, 10$, Spalten $r_0, \ldots, r_{10}$)

Dies ist eine zyklische 11×11-Matrix. Für je zwei versch. Zeilen u, v von A_{11} gilt $w(u+v) = 6$.

(Es genügt die Fälle zu betrachten, in der u Zeile 0 ist, weil A_{11} eine zyklische Matrix ist.)

Nun sieht man, dass für Zeilen u, v von G gilt

$$\sum_{i=1}^{24} u_i v_i = 0, \quad \text{d.h. } \mathcal{G}_{24} \subseteq \mathcal{G}_{24}^{\perp}.$$

c) Für alle Zeilen u von G gilt $4 \mid w(u)$.

Außerdem

$$w(u+v) = w(u) + w(v) - 2\, w(u \cap v),$$

wobei $u \cap v \in \mathbb{F}_2^{24}$ mit $(u \cap v)_i = \begin{cases} 1, & \text{falls } u_i = 1, v_i = 1 \\ 0, & \text{sonst.} \end{cases}$

Es ist: $w(u \cap v)$ gerade $\Longleftrightarrow \sum_{i=1}^{n} u_i v_i = 0$

Also folgt aus b): $w(u \cap v)$ gerade.

Also $4 \mid w(u+v)$. $\Longrightarrow$ Beh.

d) Wir überprüfen, ob $\sigma u \in \mathcal{G}_{24}$ ist für alle Zeilen u von G:

<u>Zeile 0:</u> σ bildet Zeile 0 ab auf

$$\begin{array}{c|ccccccccccc|c|ccccccccccc}
\infty & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \infty & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}$$

Dies ist die Summe der Zeilen 0, 2, 6, 7, 8, 10, 11, liegt also im Code.

Zeile 1 – 10: genauso.

Zeile 11: σ bildet Zeile 11 ab auf

$1|1111111111|0|00000000000$

Dies ist die Summe der Zeilen 0 bis 10, liegt also im Code.

e) Schreibe Codewörter von $\mathcal{G}_{24}$ als

$|L|R|$, wobei L die Koordinaten $l_\infty, \ldots, l_{10}$ enthält, und R die Koordinaten $r_\infty, \ldots, r_{10}$.

Angenommen $\exists\, x \in \mathcal{G}_{24}$ mit $w(x) = 4$.

Dann $x = |L|R|$ und $w(L) = w(R) = 0 \pmod 2$.

Wegen d) können wir uns auf zwei Fälle beschränken:

1. Fall: $w(L) = 0$, $w(R) = 4$

Unmöglich: Falls $w(L) = 0$, muss $w(R) = 0$ oder $w(R) = 12$ sein.

2. Fall: $w(L) = 2$, $w(R) = 2$

Unmöglich: x ist Summe von zwei Zeilen von G