Über Binäre (24,10,8)-Codes

B. Blaschke
Universität Bielefeld
Fakultät für Mathematik
33501 Bielefeld
Germany

B. Venkov
St. Petersbourg's department
of the Steklov mathematical institute
Fontanka 27, St. Petersbourg
Russia

Im folgenden werden alle linearen, 10-dimensionalen, binären Codes C der Länge 24 mit Minimum 8 mit dem Gewichtspolynom

$$f_C(x) = 1 + 183x^8 + 656x^{12} + 183x^{16} + x^{24} \tag{1}$$

klassifiziert. Mit Hilfe der Mac Williams Identität sieht man leicht, daß ein binärer (24,10,8)-Code C genau dann dieses Gewichtspolynom besitzt, wenn C doppelt-gerade ist (d.h. alle Codewörter haben eine durch 4 teilbare Länge), der Vektor $(1, 1, \ldots, 1)$ in C liegt und $C^\perp$ keine Vektoren der Länge 2 enthält. Zur Suche solcher Codes wurden wir durch Klassifikationsfragen unimodularer 32-dimensionaler Gitter mit Nachbareffekt 20 angeregt. In [2] Koch, Nebe wurden alle (24,8,8)-Codes mit ähnlichen Eigenschaften im Zusammenhang mit den 32-dim. unimodularen Gittern mit Nachbareffekt 24 klassifiziert.

Wir beweisen den folgenden

Satz: *Bis auf Isomorphie gibt es genau 4 binäre (24,10,8)-Codes C_a, C_b, C_c, C_d mit Gewichtspolynom (1), wobei die Zeilen der Matrizen die Basisvektoren der Codes sind:*

$$\mathbf{C_a} = \begin{pmatrix} 111111110000000000000000 \\ 001101010000000001010011 \\ 010100000110010101100000 \\ 000000001111111100000000 \\ 111100001111000011110000 \\ 111100001111000000001111 \\ 110000001111010100110101 \\ 110000111010000000000101 \\ 110001011100010100000000 \\ 101000001111011001010110 \end{pmatrix} \qquad \mathbf{C_b} = \begin{pmatrix} 111111110000000000000000 \\ 001100000000010100110101 \\ 001101010000000001010011 \\ 001101010011010100000000 \\ 000000001111111100000000 \\ 111100001111000011110000 \\ 111100001111000000001111 \\ 110000111010000000000101 \\ 101000001001010101100000 \\ 101000001111011001010110 \end{pmatrix}$$

$$\mathbf{C_c} = \begin{pmatrix} 111111110000000000000000 \\ 001101010000000001010011 \\ 010100000110010101100000 \\ 010100000000011001010110 \\ 000000001111111100000000 \\ 111100001111000011110000 \\ 111100001111000000001111 \\ 110000001111010100110101 \\ 110000111010000000000101 \\ 110001011100010100000000 \end{pmatrix} \qquad \mathbf{C_d} = \begin{pmatrix} 111111110000000000000000 \\ 111100001111000000000000 \\ 111100000000111100000000 \\ 111100000000000011110000 \\ 111100000000000000001111 \\ 000000001100011001101100 \\ 100101101100000000001100 \\ 000011000110011011000000 \\ 100111000000000011000110 \\ 010111000000110010100000 \end{pmatrix}$$

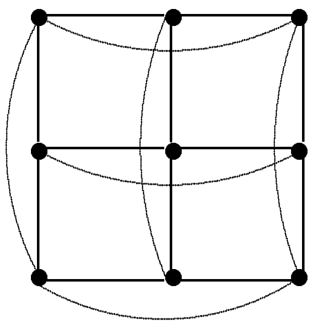
Es ist interessant, daß die Codes C_a und C_c keine Untercodes des [24,12,8]-Golaycodes sind.

Wir möchten uns bei Frau Prof. Dr. Vera Pless für anregende Diskussionen bedanken. Der zweite Autor dankt dem Sonderforschungsbereich 343 (Diskrete Strukturen in der Mathematik) und dem Leibnizpreisfond von Prof. Dr. Zink für seinen Aufenthalt in Bielefeld.

Beweis des Satzes: Sei C ein Code mit Gewichtspolynom (1). Mit Hilfe der Mac Williams Identität sieht man leicht, daß es in $C^\perp$ genau 18 Wörter der Länge 4 und 192 Wörter der Länge 6 gibt. Auf $C^\perp/C$ definieren wir die quadratische Form

$$\begin{array}{rccl} q : & C^\perp/C & \longrightarrow & \mathbb{F}_2 \\ & c+C & \longmapsto & \frac{\|c\|}{2} \bmod 2 \,, \end{array}$$

wobei $\|c\|$ das Hamminggewicht von c bezeichnet. Die Form q ist nicht ausgeartet und der quadratische Raum $(C^\perp/C, q)$ ist isomorph zu $2H$, wobei H eine hyperbolische Ebene ist. In $C^\perp/C$ gibt es neun von Null verschiedene Klassen isotroper Vektoren. Eine sehr wichtige Invariante der Codes ist die Verteilung der 18 Codewörter der Länge 4 aus $C^\perp$ auf diese Klassen. Um diese zu bestimmen, betrachten wir zunächst den folgenden Graphen, der zeigt, ob das Skalarprodukt zwischen zwei isotropen Klassen 0 oder 1 ist.



Jeder Punkt des Graphen entspricht einer isotropen Klasse, und sind zwei Punkte durch eine Kante verbunden, so haben sie Skalarprodukt 0. Die vollständigen Untergraphen der Kardinalität 3 entsprechen den 2-dimensionalen isotropen Unterräumen von $C^\perp/C$.

Wir führen folgende Bezeichnung ein:
Sei $S = \{\langle C, w_1, w_2\rangle\}$, wobei w_1 und $w_2 \in C^\perp$ sind, $w_1 \not\equiv w_2 \bmod (C)$, $\|w_1\| = \|w_2\| \equiv 0(4)$ und $(\bar{w_1}, \bar{w_2}) \equiv 0(2)$ ist, d.h. $\bar{w_1}$ und $\bar{w_2}$ erzeugen einen isotropen Unterraum. S heißt eine Vergrößerung von C der Form $(a_{w_1}, a_{w_2}, a_{w_1+w_2})$, wobei a_x die Anzahl der Vektoren der Länge 4 in $\bar{x} \in C^\perp/C$ bezeichnet.

Der Code S ist offensichtlich selbstdual und doppelt-gerade, und solche Codes sind klassifiziert. Mit der zusätzlichen Bedingung, daß S höchstens 18 Wörter der Länge 4 enthält, ergeben sich die folgenden 4 Möglichkeiten für S, wobei die Bezeichnungen der Codes aus [1] Conway und Pless, S.44, table I übernommen sind:

1. $S_1 = Golaycode$ (keine Wörter der Länge 4)
2. $S_2 = 3d_8 + glue$ (18 Wörter der Länge 4)
3. $S_3 = 4d_6 + glue$ (12 Wörter der Länge 4)
4. $S_4 = 6d_4 + glue$ (6 Wörter der Länge 4)

Behauptung: In jeder isotropen Klasse gibt es genau 0, 2, 4 oder 6 Elemente der Länge 4.

Beweis: Wir erweitern C um eine isotrope Klasse $\bar{v}$ zu einem 11-dimensionalen Code E_v. Da es in C keine Vierer gibt, ist die Anzahl der Vierer in E_v genau die Anzahl der Vierer in $\bar{v}$, bezeichnet mit a_v. Mit Hilfe der Mac Williams Identität läßt sich wieder die Anzahl der Vierer in $E_v^\perp$ bestimmen. Man erhält:

$$(E_v^\perp)_4 = 2a_v + 6\ .$$

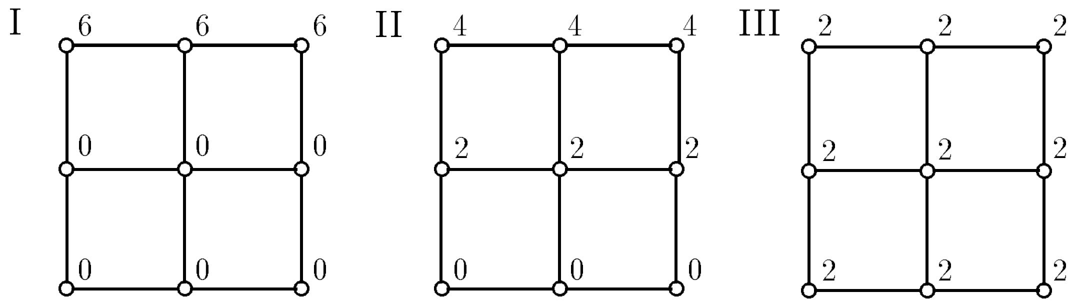
Da $C \subset E_v \subset E_v^\perp \subset C^\perp$ gilt, ist $(E_v^\perp)_4$ genau gleich der Anzahl der Vierer in den isotropen Klassen, die auf $\bar{v}$ senkrecht stehen. Zu jedem Punkt $\bar{v}$ im Graphen gibt es genau vier orthogonale Punkte $\bar{v}_1, \bar{v}_2, \bar{v}_3, \bar{v}_4$, wobei o.B.d.A. $\bar{v}_1$ und $\bar{v}_2$ sowie $\bar{v}_3$ und $\bar{v}_4$ jeweils in einem 2-dimensionalen isotropen Unterraum liegen. Wir erhalten folgende Gleichungen:

$$\begin{array}{rrcl} & a_v + a_{v_1} + a_{v_2} + a_{v_3} + a_{v_4} & = & 2a_v + 6\ , \\ & a_v + a_{v_1} + a_{v_2} & \in & \{0,6,12,18\}\ , \\ & a_v + a_{v_3} + a_{v_4} & \in & \{0,6,12,18\}\ , \\ \text{daraus folgt} & 2a_v + a_{v_1} + a_{v_2} + a_{v_3} + a_{v_4} & \in & \{0,6,12,18,24,30,36\}\quad , \\ & \text{also}\quad 3a_v & \in & \{0,6,12,18,24,30\} \\ & \text{und damit}\quad a_v & \in & \{0,2,4,6,8,10\}\ . \end{array}$$

Es ist $a_v = 8$ oder 10 nicht realisierbar, da zwei Vierer, die in einer Klasse liegen, leeren Schnitt haben müssen, und man im ${\mathbb{F}_2}^{24}$ höchstens 6 Vierer, die paarweise leeren Schnitt haben, verteilen kann. Daraus folgt die Behauptung. $\square$

Nun kann die Verteilung der 18 Codewörter der Länge 4 aus $C^\perp$ auf die neun isotropen Klassen genau besimmmt werden.

Behauptung: Folgende Verteilungen sind möglich:



Dabei entsprechen die Punkte den isotropen Klassen in $C^\perp/C$, die Spalten und Zeilen entsprechen den 2-dimensionalen Unterräumen in $C^\perp/C$, und die Zahlen geben die Anzahl der Vierer in der entsprechenden Klasse $\bar{v}$ an, die wie oben mit a_v bezeichnet wird.

Beweis: Wir wissen schon, daß $a_v = 0, 2, 4$ oder 6 ist und daß die Summe über alle a_v gleich 18 ist. Angenommen es gibt eine Klasse $\bar{v}$ mit $a_v = 6$, in diesem Fall haben die 6 Vierer paarweise leeren Schnitt. Dann ist $C \subset E_v \subset S$, wobei $S = S_2$ oder $S = S_4$ ist. S_1 ist nicht möglich, da es dort keine Wörter der Länge 4 gibt, S_3 ist nicht möglich, da es darin keine 6 paarweise orthogonalen Vierer mit leerem Schnitt gibt. Im Fall S_2 liegen in einem 2-dimensionalen isotropen Unterraum 18 Vierer mit jeweils 6 Vierern in einer Klasse, und im Fall S_4 liegen 6 Vierer in einem 2-dimensionalen isotropen Unterraum mit 6 Vierern in der einen und 0 Vierern in den beiden anderen Klassen. Damit erhält man Typ I.
Angenommen es gibt eine Klasse $\bar{v}$ mit $a_v = 4$, dann ist $S = S_3$ oder $S = S_4$. Der Code S_1 ist wieder nicht möglich, weil es darin keine Vierer gibt, S_2 ist nicht möglich, da es sonst in einer der beiden anderen Klassen mehr als 6 Vierer gäbe. Im Fall S_3 liegen 12 Vierer in einem 2-dimensionalen isotropen Unterraum mit jeweils 4 Vierern in einer Klasse und im Fall S_4 liegen 6 in einem 2-dimensionalen isotropen Unterraum mit 4 Vierern in der ersten Klasse, 2 in der zweiten Klasse und 0 in der dritten Klasse. Das führt zu Typ II.
Damit bleibt nur noch der Fall, wo für alle $\bar{v}$ gilt $a_v = 2$, und das führt zu Typ III. □

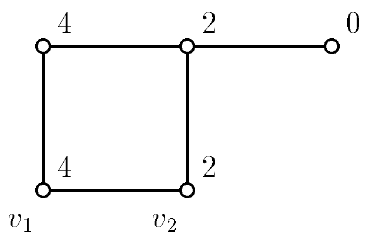
Folgerung: Jeder Code C ist ein Untercode von S_4.

Beweis: In jedem der drei Konstellationen I-III existiert mindestens ein 2-dimensionaler isotroper Unterraum mit genau 6 Vierern, also ist jedes C Untercode von S_4. $\square$

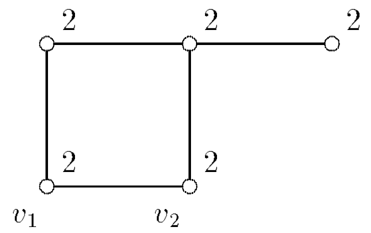
Wir wollen nun die Codes der Konstellation II und III als Untercode von S_4 konstruieren. Es existieren $v_1, v_2 \in {\mathbb{F}_2}^{24} \setminus S_4$ mit $C = \{l \in S_4 | (l, v_i) \equiv 0(2)\}$, wobei v_1 und v_2 in verschiedenen Nebenklassen modulo S_4 liegen, und $\|v_1\| \equiv \|v_2\| \equiv \|v_1 + v_2\| \equiv 0$ modulo 2, denn v_1, v_2 und $v_1 + v_2$ liegen in $C^{\perp}$ und haben daher gerade Länge. Außerdem ist ihre Länge echt größer 2, da $(C^{\perp})_2 = \emptyset$. Zusätzlich muß für jeden Vierer $w \in S_4$ ein i mit $(v_i, w) \equiv 1 \bmod 2$, $i = 1, 2$ existieren, da C keine Vierer enthält.

Behauptung: Um einen Code C der Konstellation II bzw. III zu erhalten, genügt es, $v_1, v_2 \in {\mathbb{F}_2}^{24} \setminus S_4$ mit $\|v_1\| = \|v_2\| = 4$ und $|v_1 \cap v_2| = 0$ zu wählen.

Beweis: Ist S_4 durch eine Vergrößerung von C der Form (4,2,0) entstanden, so kann man v_1 und v_2 aus den folgenden beiden Nebenklassen, die sich am günstigsten graphisch beschreiben lassen, wählen:



Man sieht leicht, daß die Vektoren v_1 und v_2 den gewünschten Eigenschaften genügen, denn in der Klasse von $v_1 + v_2$ gibt es keine Vektoren der Länge 4, also haben v_1 und v_2 leeren Schnitt.
Ist S_4 durch eine Vergrößerung von C der Form (2,2,2) entstanden, so kann man v_1 und v_2 aus den folgenden beiden Nebenklassen wählen:



Es bleibt zu zeigen, daß $v_1 \cap v_2 = 0$. Aber v_1, v_2 und $v_1 + v_2$ erzeugen zusammen mit C wieder ein S_4, und daher haben die Vierer v_1 und v_2 leeren Schnitt. $\square$

Bemerkung: Man sieht, daß man bei einer Vergrößerung von C der Form (6, 0, 0) keine v_1 und v_2 mit $\|v_1\| = \|v_2\| = 4$ finden kann, denn die beiden Nebenklassen modulo C, die noch Vierer enthalten, sind linear abhängig modulo S_4.

Konstruktion der Codes: Um nun ein C aus S_4 konkret zu konstruieren, benötigen wir alle Paare v_1, v_2 die sich nicht durch ein $\sigma \in Aut(S_4)$ ineinander überführen lassen, denn es gilt:

$$C_{\sigma(v_1),\sigma(v_2)} = \sigma(C_{v_1,v_2}) \ .$$

Die Automorphismengruppe von S_4 ist in [1] Conway and Pless, S.31-33 beschrieben. Legt man die 6 Vierer c_1, c_2, c_3, c_4, c_5, c_6 aus S_4 und v_1 o.B.d.A. fest, ergeben sich für v_2 modulo $Aut(S_4)$ noch genau drei Möglichkeiten:

$$\begin{array}{rcccccc}
 & \overbrace{1111}^{c_1} & \overbrace{1111}^{c_2} & \overbrace{1111}^{c_3} & \overbrace{1111}^{c_4} & \overbrace{1111}^{c_5} & \overbrace{1111}^{c_6} \\
v_1 & 1000 & 1000 & 1000 & 1000 & 0000 & 0000 \\
v_{2a} & 0000 & 0000 & 0100 & 0100 & 1000 & 1000 \\
v_{2b} & 0000 & 0000 & 0100 & 0010 & 1000 & 1000 \\
v_{2c} & 0000 & 0000 & 0100 & 0001 & 1000 & 1000
\end{array}$$

Auf diese Weise erhält man drei Untercodes von S_4:

$$C_a = C_{v_1,v_{2a}} \ , \ C_b = C_{v_1,v_{2b}} \ , \ C_c = C_{v_1,v_{2c}} \ .$$

Mit Hilfe des Computers stellt man fest, daß diese Codes verschieden sind und daß C_a und C_c die Konstellation III haben und C_b die Konstellation II besitzt. Daß diese Codes unseren Eigenschaften genügen, ist per Konstruktion klar. Es wurden folgende Schritte durchgeführt:

1. Man bestimmt alle Vierer in $C^\perp$.

2. Man ergänzt C um einen Vierer zu einem 11-dimensionalen Code F und bestimmt die Anzahl der Vierer in F. Diese ist genau gleich der Anzahl der Vierer in einer isotropen Klasse von $C^{\perp}/C$. Es ergibt sich, daß C_a und C_c vom Typ III sind und C_b zum Typ II gehört.

3. Um festzustellen, ob C_a und C_c verschieden sind, bestimmen wir die Anzahl der Sechser, die im Erzeugnis der Vierer aus $C_a^{\perp}$ bzw. $C_c^{\perp}$ liegen. Es ergeben sich zwei verschiedene Werte, also sind C_a und C_c nicht isomorph.

Es bleibt noch die Frage, wieviele Codes C der Konstellation I existieren.
Behauptung: Es existiert genau ein Code $C = C_d$ mit Konstellation I.

Beweis: Wir wissen, daß es 192 Codewörter der Länge 6 in $C^{\perp}$ gibt. Um deren Verteilung auf die sechs anisotropen Klassen in $C^{\perp}/C$ zu bestimmen, erweitern wir C um eine anisotrope Klasse zu einem 11-dimensionalen Code F. Da die Anzahl der doppelt-geraden Codewörter aus F und C gleich ist, in $F^{\perp}$ keine Codewörter der Länge 2 existieren und die Anzahl der nicht doppelt-geraden Codewörter in F gleich 2^{10} ist, erhält man mit Hilfe der Mac Williams Identität genau 32 Sechser in F, d.h. in jeder anisotropen Klasse von $C^{\perp}/C$ gibt es 32 Codewörter der Länge 6.
Also läßt sich C um eine isotrope Klasse A, die sechs Vierer enthält, und eine anisotrope Klasse B, die dazu orthogonal ist, zu einem 12-dimensionalen Code G erweitern. Der Code G ist selbstdual und enthält genau 6 Vierer und 64 Sechser. Davon gibt es nach der Klassifikation von [3], Pless and Sloane genau zwei Codes:

1. $G_1 = 3d_4 + d_6 + (111111) + glue$,

2. $G_2 = 6d_4 + glue$.

Es ist $F = \{g \in G | (g, v) \equiv 0(2)\}$, wobei $v \in F^{\perp} \setminus G$. Da es in $C^{\perp}/C$ eine anisotrope Klasse gibt, die zu A und B nicht orthogonal ist, kann v als Codewort der Länge 6 gewählt werden. Für die 3 Vierer c_1, c_2, c_3 aus G_1, die durch d_6 gebildet werden, existiert kein v, so daß $(c_1, v) \equiv (c_2, v) \equiv (c_3, v) \equiv 1(2)$, also gibt es kein F als Untercode von G_1.
So bleibt nur der Fall $G = G_2$. Sind die 6 Vierer c_1, c_2, c_3, c_4, c_5, c_6 aus G_2 so festgelegt wie im Fall S_4, dann gibt es bis auf Isomorphie bzgl. $Aut(G_2)$ ein eindeutiges $v = (010010001000100010001000)$, so daß $(c_1, v) \equiv (c_2, v) \equiv (c_3, v) \equiv (c_4, v) \equiv (c_5, v) \equiv (c_6, v) \equiv 0(2)$ ist. Auf diese Weise erhält man den Code F. Der doppelt-gerade Untercode von F ist dann der gewünschte Code C_d der Konstellation I.

Damit ist der Satz bewiesen.

Die Basisvektoren der Codes wurden mit Hilfe des Computers bestimmt.

Literatur

[1] Conway, J.H., Pless, V.: On the Enumeration of Self-Dual Codes; Journal of Combinatorial Theorie, Series A 28, 26-53 (1980)

[2] Koch, H., Nebe, G.: Extremal Even Unimodular Lattices of Rank 32 and Related Codes; Math. Nachr. 161, 309-319 (1993)

[3] Pless, V., Sloane, N.J.A.: On the classification and enumeration of self-dual codes, J. Combinatorial Theorie, Series A 18, 313-335 (1975)