«LE MATEMATICHE»
Vol. XLV (1990) - Fasc. I, pp. 187-195

EVEN TYPE AND ODD TYPE SETS IN A STEINER SYSTEM AND LINEAR CODES

GIUSEPPE TALLINI (Roma)

1. General properties of even type and odd type sets in $S(2, k, v)$.

Let $(S, \mathcal{L})$ be a Steiner system $S(2, k, v)$, that is a linear space in which every line has k points and $|S| = v$. It is:

$$r = n^\circ \text{ lines through a point } = (v-1)/(k-1)$$

$$b = |\mathcal{L}| = v(v-1)/k(k-1).$$

In $(S, \mathcal{L}) = S(2, k, v)$ a subset P is an *even type set* iff every line meets it in an even number of points. We denote by $\mathcal{P}$ the family of even type sets of $(S, \mathcal{L})$. A subset D of $(S, \mathcal{L})$ is an *odd type set* iff every line meets it in an odd number of points.

We denote by $\mathcal{D}$ the family of odd type sets of $(S, \mathcal{L})$. We set:

$$\mathcal{H} = \mathcal{P} \cup \mathcal{D} \tag{1.1}$$

It is:

$$\emptyset \in \mathcal{P};\ k \text{ even} \mapsto S \in \mathcal{P};\ k \text{ odd} \mapsto S \in \mathcal{D}. \tag{1.2}$$

Moreover it is:

$$(1.3)\qquad \begin{cases} k \text{ even} \mapsto [X \in \mathcal{P} \mapsto X' = S - X \in \mathcal{P}; \\ \qquad X \in \mathcal{D} \mapsto X' = S - X \in \mathcal{D}] \\ k \text{ odd} \mapsto [X \in \mathcal{P} \leftrightarrow X' = S - X \in \mathcal{D}] \end{cases}$$

Since for any $l \in \mathcal{L}$ it is:

$$X, Y \subseteq S \mapsto |(X \cup Y - X \cap Y) \cap l| = |X \cap l| + |Y \cap l| - 2|X \cap Y \cap l|,$$

we get:

$$(1.4)\qquad \begin{cases} X, Y \in \mathcal{P} \mapsto (X \cup Y - X \cap Y) \in \mathcal{P}, \\ X, Y \in \mathcal{D} \mapsto (X \cup Y - X \cap Y) \in \mathcal{P}, \\ X \in \mathcal{P}, Y \in \mathcal{D} \mapsto (X \cup Y - X \cap Y) \in \mathcal{D}. \end{cases}$$

It is known that the power set of S, with respect to the symmetric difference:

$$(1.5)\qquad X, Y \subseteq S, \quad X \oplus Y = X \cup Y - X \cap Y$$

and to the product times a scalar in Z_2:

$$(1.5')\qquad 0 \cdot X = \emptyset, \quad 1 \cdot X = X, \quad 0, 1 \in Z_2$$

is a vector space over Z_2, $(\mathbb{P}(S), \oplus, \cdot, Z_2)$ isomorphic to $Z_2^v (v = |S|)$. By (1.4) we get that $(\mathcal{H}, \oplus, \cdot, Z_2)$ is a subspace of $(\mathbb{P}(S), +, \cdot, Z_2)$, such that, if $\mathcal{D} \neq \emptyset$, $\mathcal{P}$ is an index two subspace.

We easily prove:

$$(1.6)\qquad \begin{cases} X \in \mathcal{P}, \ X \neq S \mapsto |X| \equiv 0 \mod 2, \\ X \in \mathcal{P}, \ X \neq \emptyset \mapsto |X| \equiv 1 + r \mod 2, \end{cases}$$

Moreover:

$$(1.7)\qquad \begin{cases} X \in \mathcal{D}, \ X \neq S \mapsto |X| \equiv r \mod 2, \\ X \in \mathcal{D}, \ X \neq \emptyset \mapsto |X| \equiv 1 \mod 2. \end{cases}$$

It follows:

I. *If r is even the only either even type sets or odd type sets are the trivial ones, that is $\emptyset$, S. Moreover if r is odd:*

$$\begin{cases} X \in \mathcal{P},\ X \neq \emptyset, S \mapsto |X| \text{ even}, \\ X \in \mathcal{D},\ X \neq \emptyset, S \mapsto |X| \text{ odd}. \end{cases} \tag{1.8}$$

From now on we assume r odd:

$$r = 2\rho + 1. \tag{1.9}$$

We easily prove:

$$D \in \mathcal{D} \mapsto [|D| \geq r; |D| = r \leftrightarrow k \text{ odd}, D \text{ is of type } (1, k)] \tag{1.10}$$

$$P \in \mathcal{P}, P \neq \emptyset \mapsto [|P| \geq r+1;\ |P| = r+1 \leftrightarrow P \text{ is of type } (0, 2)]. \tag{1.11}$$

By (1.10), (1.8) we get

$$k \text{ even} \mapsto |D| \geq r+2,\ D \in \mathcal{D}. \tag{1.12}$$

By (1.10), (1.11), (1.12) we have:

II. *Every non-zero vector of $(\mathcal{H}, +, \cdot, Z_2)$ has weight $w \geq r$ if k is odd, $w \geq r+1$ if k is even (we recall that the weight of $U \in \mathcal{H}$ is the number of non-zero components of the vector U, that is the number of points of U). It follows that $\mathcal{H}$ is a linear code of Z_2^v correcting $e \geq (r-1)/2$ errors.*

Assume now $\mathcal{D} \neq \emptyset$ and let be $D \in \mathcal{D}$. Set $|D| = 2n+1$. The equation of characters, [2], with respect to D provides:

$$\begin{aligned} &\sum t_{2s+1} = b, \sum (2s+1) t_{2s+1} = (2n+1) r, \\ &\sum (2s+1) 2s t_{2s+1} = (2n+1) 2n. \end{aligned} \tag{1.13}$$

By $(1.13)_1$, $(1.13)_2$ we get:

$$2 \sum s \cdot t_{2s+1} + b = 2nr + r \mapsto b = r + 2\sigma, \quad \sigma \in N.$$

Therefore:

$$\sum st_{2s+1} = nr - \sigma,\ b = r + 2\sigma. \tag{1.14}$$

By $(1.13)_3$, (1.14) we get:

$$2\sum s^2 t_{2s+1} + nr - \sigma = 2n^2 + n$$

and then, since r is odd, it is:

$$\sigma = 2\tau, \quad b = r + 4\tau.$$

Since it is $vr = kb$, we have:

$$vr = k(r+4\tau) \mapsto r(v-k) = 4\tau k \mapsto \begin{cases} v \equiv k \bmod 4 \\ v \equiv k \bmod 8 \text{ if } k \text{ is even.} \end{cases}$$

So we prove:

III. *If $\mathcal{D}$ is non empty, it is $b \equiv r$ mod 4 and $v \equiv k$ mod 4; it is $v \equiv k$ mod 8 if k is even. Moreover for any $D \in \mathcal{D}$, $|D| = 2n+1$, set $b = r + 4\tau$, it is $(r = 2\rho + 1)$:*

$$\sum st_{2s+1} = nr - 2\tau,\ \sum s^2 t_{2s+1} = n^2 + \tau - n\rho. \tag{1.15}$$

By (1.15) we get $(r = 2\rho + 1)$:

$$\sum (s^2 - s)t_{2s+1} = n(n-1) - 3n\rho + 3\tau. \tag{1.16}$$

Since the left hand side in (1.16) is even, by (1.16) we get:

$$n\rho \equiv \tau \bmod 2 \quad (b = r + 4\tau,\ r(v-k) = 4\tau k). \tag{1.17}$$

If ρ is even, that is $r \equiv 1 \bmod 4$, by (1.17) we obtain that τ is even, that is $b \equiv r \bmod 8$, whence $v \equiv k \bmod 8$, $v \equiv k \bmod 16$ if k is even, that is:

IV. *If $\mathcal{D}$ is non empty and $r \equiv 1 \bmod 4$, it is $b \equiv r \bmod 8$, $v \equiv k \bmod 8$ and $v \equiv k \bmod 16$ if k is even.*

If ρ is odd (that is $r \equiv 3 \bmod 4$) and τ is even, that is $b \equiv r \bmod 8$, then n is even, that is $|D| = 2n+1 \equiv 1 \bmod 4$. If τ is odd, that is $b \not\equiv r \bmod 8$, then n is odd, that is $|D| = 2n+1 \equiv 3 \bmod 4$. So we prove:

V. *If $\mathcal{D}$ is non empty and $r \equiv 3 \bmod 4$, it is:*

$$\begin{cases} b \equiv r \bmod 8 \mapsto \forall D \in \mathcal{D}, |D| \equiv 1 \bmod 4, \\ b \not\equiv r \bmod 8 \mapsto \forall D \in \mathcal{D}, |D| \equiv 3 \bmod 4. \end{cases} \tag{1.18}$$

As corollaries of I, III, IV we get:

VI. *In $S(2, q, q^m)$, q even and $m \geq 2$ (for istance in an affine plane of order q even) it is $\mathcal{D} = \emptyset$.*

VII. *In $S(2, a+1, a^3+1)$ (abstract unital) if a is even, it is $\mathcal{D} = \{S\}$. If a is odd and $a \not\equiv 1 \bmod 8$ it is $\mathcal{D} = \emptyset$.*

VIII. *In $S(2, n, n(cn - c + 1))$ (maximal arc) it is:*

$$\begin{cases} c, n \text{ odd} \rightarrow \mathcal{D} = \{S\}, \\ c \text{ odd } n \text{ even} \mapsto \mathcal{D} = \emptyset, \\ c, n \text{ even}, c \not\equiv 0 \bmod 8 \mapsto \mathcal{D} = \emptyset. \end{cases}$$

Assume now that in $S(2, k, v)$ a non-empty even type set P exists and let k be odd. Then $D = S - P \in \mathcal{D}$ (see (1.3)) and by Theorems III, IV, V we get:

IX. *$S(2, k, v)$, k odd and $\mathcal{P} \neq \{\emptyset\}$, it is $b \equiv r \bmod 4$ and $v \equiv k \bmod 4$. If $r \equiv 1 \bmod 4$ it is $b \equiv r \bmod 8$ and $v \equiv k \bmod 8$. If $r \equiv 3 \bmod 4$ it is*

$$\begin{cases} b \equiv r \bmod 8 \mapsto \forall P \in \mathcal{P} - \{\emptyset\}, |P| \equiv v - 1 \bmod 4, \\ b \not\equiv r \bmod 8 \mapsto \forall P \in \mathcal{P} - \{\emptyset\}, |P| \equiv v - 3 \bmod 4. \end{cases} \tag{1.19}$$

Let be $P \in \mathcal{P}$ and $|P| = 2n$. By the equations of characters referred to P, we get:

$$|P| = 2n, \sum st_{2s} = nr, \sum s(2s-1)t_{2s} = n(2n-1)$$

whence (since $r = 2\rho + 1$):

$$\sum s^2 t_{2s} = n(n+\rho), \sum s t_{2s} = n(2\rho+1),$$

so that:

$$\sum (s^2 - s) t_{2s} = n(n-\rho-1).$$

If ρ is odd, that is $r \equiv 3 \bmod 4$, since the left hand side of the previous equation is even, we get: $n \equiv 0 \bmod 2$, that is $|P| \equiv 0 \bmod 4$. So we state:

X. *In* $S(2,k,v)$, $r \equiv 3 \bmod 4$, *for any* $P \in \mathcal{P}$, *it is* $|P| \equiv 0 \bmod 4$.

If $r \equiv 3 \bmod 4$ and k is odd, by prop X and (1.3) we get (see prop. V):

XI. *In* $S(2,k,v)$, $r \equiv 3 \bmod 4$ *and* k *odd, if* $\mathcal{D} \neq \emptyset$, *for any* $D \in \mathcal{D}$ *it is* $|D| = v \bmod 4$, *whence*:

$$(1.20) \qquad \begin{cases} b \equiv r \bmod 8 \mapsto v \equiv 1 \bmod 4, \\ b \not\equiv r \bmod 8 \mapsto v \equiv 3 \bmod 4. \end{cases}$$

2. Linear codes related to a $S(2,k,v), r \equiv 3 \bmod 4$.

Let $S(2,k,v) = (S, \mathcal{L})$ be a Steiner system with $r \equiv 3 \bmod 4$. As we previously considered we associated to it the subspace $\mathcal{H} = \mathcal{P} \cup \mathcal{D}$ of the vector space $\mathbb{P}(S) = (\mathbb{P}(S), \oplus, \cdot, Z_2)$ that is a *linear* (v, w, d)*-code*, where $v = \dim \mathbb{P}(S) = |S|$, w=weight of $\mathcal{H} \geq r$, d =dim$\mathcal{H}$. Our aim is now to calculate d.

In $\mathcal{P}(S)$ we define a scalar product in the classical way:

$$X, Y \in \mathbb{P}(S), X(x_i), Y = (y_i), \; X \cdot Y = \sum x_i y_i (\in Z_2).$$

We easily prove:

$$X, Y, \in \mathbb{P}(S), \; X \cdot Y = |X \cap Y|_2 = \begin{cases} = 0 \text{ if } |X \cap Y| \text{ is even} \\ = 1 \text{ if } |X \cap Y| \text{ is odd.} \end{cases}$$

So in $\mathbb{P}(S)$ the following orthogonality is defined:

$$X \perp Y \leftrightarrow |X \cap Y|_2 = 0, \quad X, Y \in \mathbb{P}(S). \tag{2.1}$$

If T is a subspace of $\mathbb{P}(S)$ we set:

$$T^{\perp} = \{X \in \mathcal{P}(S) : X \perp Y, \forall Y \in T\}. \tag{2.2}$$

We easily prove:

$$\dim T + \dim T^{\perp} = \dim \mathbb{P}(S) = v. \tag{2.3}$$

By proposition X we get:

$$\begin{cases} X \in \mathcal{P} \mapsto \forall Y \in \mathcal{P}, |X \oplus Y| = |X \cup Y - X \cap Y| = \\ \qquad = |X| + |Y| - 2|X \cap Y| \equiv 0 \bmod 4, \\ |X| \equiv 0 \bmod 4, |Y| \equiv 0 \bmod 4 \mapsto |X \cap Y| \equiv \\ \qquad \equiv 0 \bmod 2 \mapsto X \perp Y, \forall Y \in \mathcal{P} \end{cases} \tag{2.4}$$

Set $a = 1$ if $b \equiv r \bmod 8$, $a = 3$ if $b \not\equiv r \bmod 8$. By prop. V we get:

$$\begin{cases} X \in \mathcal{P} \mapsto \forall Y \in \mathcal{D}, |X \oplus Y| = |X| + |Y| - 2|X \cap Y| \equiv a \bmod 4, \\ |X| \equiv 0 \bmod 4, |Y| \equiv a \bmod 4 \mapsto |X \cap Y| \equiv 0 \bmod 2 \mapsto X \perp Y, \\ \qquad \forall Y \in \mathcal{D}. \end{cases} \tag{2.5}$$

By (2.4), (2.5) we get:

$$X \in \mathcal{P} \mapsto \forall Y \in \mathcal{H}, \; X \perp Y \leftrightarrow X \in \mathcal{H}^{\perp} \tag{2.6}$$

that is:

$$\mathcal{P} \subseteq \mathcal{H}^{\perp} \mapsto \dim \mathcal{P} \leq \dim \mathcal{H}^{\perp}. \tag{2.7}$$

If $\mathcal{D} = \emptyset$, that is $\mathcal{P} = \mathcal{H}$, by (2.7) and (2.3) we get: $2 \dim \mathcal{P} \leq \dim \mathcal{P} + \dim \mathcal{P}^{\perp} = v$, that is

$$\mathcal{D} = \emptyset \mapsto d \leq v/2. \tag{2.8}$$

If $\mathcal{D} \neq \emptyset$, whence $\dim \mathcal{P} = d - 1$, by (2.7) and (2.3) we get: $2d - 1 = \dim \mathcal{H} + \dim \mathcal{P} \leq \dim \mathcal{H} + \dim \mathcal{H}^{\perp} = v$, that is:

$$\mathcal{D} \neq \emptyset \mapsto d \leq (v+1)/2. \tag{2.9}$$

Assume now $\mathcal{L} \subset \mathcal{H}$, whence $\mathcal{L} \subset \mathcal{D}$ and k is odd, moreover $S(2, k, v)$ is a projective plane of order $q = k - 1$, that is a $S(2, q+1, q^2+q+1)$, with $q \equiv 2 \bmod 4$ (since $r = q + 1 \equiv 3 \bmod 4$). We have:

$$X \in \mathcal{H}^{\perp} \leftrightarrow \forall Y \in \mathcal{H}, X \perp Y \leftrightarrow |X \cap Y| \equiv 0 \bmod 2, \forall Y \in \mathcal{H} \mapsto$$

$$\mapsto \forall l \in \mathcal{L}, |X \cap l| \text{ is even } \leftrightarrow X \in \mathcal{P},$$

that is:

$$\mathcal{H}^{\perp} \subseteq \mathcal{P} \mapsto \dim \mathcal{H}^{\perp} \leq \dim \mathcal{P}. \tag{2.10}$$

By (2.10) and (2.3) we get: $v = \dim \mathcal{H} + \dim \mathcal{H}^{\perp} \leq \dim \mathcal{H} + \dim \mathcal{P} = 2d - 1 \mapsto d \geq (v+1)/2$, that is:

$$\mathcal{L} \subseteq \mathcal{D} \mapsto d \geq (v+1)/2. \tag{2.11}$$

By (2.9) and (2.11) we obtain:

I. *In a projective plane* $S(2, q+1, q^2+q+1)$ *with* $q \equiv 2 \bmod 4$, *it is* $d = (q^2+q+2)/2$ *and* $\mathcal{H}$ *is a linear* $(v = q^2+q+1, w = q+1, d = (q^2+q+2)/2)$-*code.*

At last we prove:

II. *In* $PG(m, 2) = S(2, 3, \theta_m)$, $\mathcal{H}$ *is a linear* $(v = \theta_m, w = \theta_{m-1}, m+2)$-*code (where* $\theta_m = 2^{m+1} - 1$).

Proof. In $PG(m, 2)$ every odd type set is either $PG(m, 2)$ or a hyperplane (since it is of class [1,3]). Then every even type set is either $\emptyset$ or the complement of hyperplane. It follows $w = \theta_{m-1}$, $|\mathcal{H}| = 2\theta_m + 2 = 2^{m+2}$ and then $d = m + 2$.

Theorems I and II are well known but here they follows as particular cases of the general geometric theory previously explained.

REFERENCES

[1] Cameron P.J., van Lint J.H., *Graph Theory and Block Designs,* LMS Lecture Note Series **19**, (1975).

[2] Tallini G., *Graphic characterizations of algebraic varieties in a Galois Space,* Atti Convegno «Teorie Combinatorie» Roma Sett. 1973, Acc. Naz. Lincei, Roma, Tomo II, 153-165.

[3] Tallini G., *Spazi parziali di rette e codici Correttori,* Rivista di Mat. pura ed appl. Univ. Udine, (1987) 43-69.

[4] Tallini G., *Linear codes associated with geometric structures,* Results in Math., Birkhäuser Verlag, Basel, (1987) 411-422.

Dipartimento di Matematica
"Guido Castelnuovo"
Università "La Sapienza"
P.le A. Moro, 2
00185 Roma (Italy)