Linear codes supported by Steiner triple systems

LINEAR CODES SUPPORTED BY STEINER TRIPLE SYSTEMS

L.M.H.E. Driessen, G.H.M. Frederix and J.H. van Lint

1. *Introduction.*

This paper is concerned with the connections between t-designs and the words of minimal weight in a linear code. As usual we define t-designs as follows.

DEFINITION 1.1. *A* t*-design, denoted by* t-(v,k,λ), *is a collection* $\mathcal{D}$ *of distinct* k*-subsets (called blocks) of a set* S *of* v *points, such that every* t*-subset of* S *is a subset of exactly* λ *blocks of* $\mathcal{D}$. *If* $\lambda = 1$ *then the design is called a Steiner system and if furthermore* $t = 2$ *and* $k = 3$ *then the design is called a Steiner Triple System and denoted by* STS(v).

We assume that the reader is familiar with the terminology and certain results of coding theory (cf.[6]). Many of the most interesting known t-designs (especially those with $t \geq 3$) can be constructed using coding theory (cf. [2], [4]). The idea is as follows.

DEFINITION 1.2. *Let* C *be a linear* (n,k)*-code over* GF(q). *Let* D *be the subset of* C *consisting of the words of minimal weight* (> 0). *The set* ϕ(D) *of supports of* D *consists of the subsets* B *of* S:= {1,2,...,n} *such that there is a word* $\underline{c} \in D$ *with* $\forall_i$ $[c_i \neq 0 \Leftrightarrow i \in B]$.

We shall say that a t-design $\mathcal{D}$ *supports* the code C if in definition (1.2) we have $\phi(D) = \mathcal{D}$. It is well known (cf.[4]) that the ternary Golay code (which is an (11,6)-code with minimal weight 5) supports the Steiner system 4 - (11,5,1). The shortened code of length 9 must therefore be supported by a 2 - (9,3,1), i.e. the unique Steiner Triple System STS(9), in other words

ARS COMBINATORIA, Vol. 1 (1976), pp. 33–42.

the affine plane of order 3, AG(2,3) (cf. [5]). The parameters do not a priori exclude the possibility of a 9 - (20,10,1). If this design exists and if it supports a linear code over some field GF(q), then by shortening it 7 times we find a linear code supported by a 2 - (13,3,1), i.e. STS(13). A few years ago this fact motivated E.F. Assmus and H.F. Mattson to study the possibility of linear codes supported by Steiner Triple Systems (cf.[3]). No other examples than the one mentioned above and the binary (7,4) Hamming code supported by STS(7), i.e. PG(2,2), came out. However some of their results were useful for our own research and they will be given below. In this paper we shall construct an infinite class of codes supported by STS(9) and we shall show that no STS(13) supports a linear code. As was mentioned above this proves that if a 9 - (20,10,1) exists then it does not support a linear code.

Before starting our systematic treatment of codes supported by a STS(n) we mention one theorem which, although we have not seen it in this form, is undoubtedly known.

THEOREM 1.3. *If* $m \geq 2$, $r \geq 1$, *then there is a* STS($2^m - 1$) *which supports a linear* ($2^m - 1$, $2^m - m - 1$)*-code over* GF(2^r).

Proof. Let H be the parity-check matrix of the binary Hamming code of length $2^m - 1$. Clearly, three columns of H are linearly dependent over GF(2^r) if they are linearly dependent over GF(2). The converse is also true. This follows from the fact that the columns of H are different and have only 0 and 1 as entries. Therefore a linear combination of three columns of H can be $\underline{0}$ only if the three columns have $\underline{0}$ as sum. Since for every two columns of H the sum of these two also occurs in H, it follows that the code over

$GF(2^r)$ with parity-check matrix H is supported by a $STS(2^m - 1)$. □

Remark. In [1] E.E. Assmus and H.F. Mattson proved that for a binary code C the system $\phi(D)$ is a STS(n) if and only if C is perfect. By well known results on perfect codes (cf.[6]) it follows that $n = 2^m - 1$ for some m. Furthermore the STS(n) in Theorem (1.3) is unique because the corresponding Hamming code is unique.

2. *Necessary Conditions.*

In this section we shall assume that C is linear (n,k)-code over GF(q) with minimum distance 3 and further more we assume that $\phi(D)$ is a STS(n). We denote by $C^\perp$ the dual code of C. The weight enumerators of C and $C^\perp$ are denoted by

$$A(z) := \sum_{i=0}^{n} A_i z^i \text{ and } B(z) := \sum_{i=0}^{n} B_i z^i .$$

From now on we shall also assume that the Steiner Triple System $\phi(D)$ does not have a nontrivial subsystem on fewer points (because in that case we could study the corresponding shortened code). This implies that $B_i = 0$ for $1 \le i \le n - 4$ since the existence of a word $\underline{x}$ of weight $n - \ell$ in $C^\perp$ implies that $\phi(D)$ has a subsystem on the ℓ points where $\underline{x}$ has coordinates 0. In the same way we see that $B_{n-2} = 0$.

LEMMA 2.1 *If* C *is a linear code such that* $\phi(D)$ *is a* STS(n) ($n > 3$) *with no nontrivial subsystem then* $C^\perp$ *has dimension* 3 *and weight enumerator* $1 + B_{n-3}z^{n-3} + B_{n-1}z^{n-1} + B_n z^n$.

Proof. We have already seen that the minimum distance of $C^\perp$ is at least n-3. Let C have dimension k. Then by the Singleton bound we have $k \ge n - 4$.

If $k = n - 4$ then C and $C^{\perp}$ are optimal and hence any three columns of the parity-check matrix of C are linearly dependent (cf. [6], § 4.2). Then $\phi(D)$ is a 3-design which contradicts the fact that $\phi(D)$ is a Steiner Triple System (unless $n = 3$). Hence $k \geq n - 3$. Since C has minimum distance 3 we must have $k \leq n - 3$, i.e. $k = n - 3$.

Since we know A_3 (because $\phi(D)$ is a STS(n)) and $B(z)$ has only 3 nonzero coefficients we can determine $B(z)$ by using the MacWilliams relations (cf.[6], § 6.1).

LEMMA 2.2. *If C is a linear code over GF(q) such that $\phi(D)$ is a* STS(n) *($n > 3$) with no nontrivial subsystem then $C^{\perp}$ has weight enumerator*

$$B(z) := \sum_{i=0}^{n} B_i z^i$$

where

$$B_0 = 1$$

$$B_{n-3} = \frac{1}{6} n (n - 1) (q - 1),$$

$$B_{n-1} = n(q - 1)(q + 1 - \frac{n - 1}{2}) ,$$

$$B_n = q^3 - 1 - n(q - 1)(q - \frac{n - 4}{3}) ,$$

$$B_i = 0 \textit{ otherwise.}$$

Proof. The number of blocks in a STS(n) is $\frac{1}{6} n(n - 1)$. If two words of weight 3 in C have the same support they are linearly dependent because $A_1 = A_2 = 0$. Hence $A_3 = \frac{1}{6} n(n - 1)(q - 1)$. By the MacWilliams relation we have

$$A(z) = q^{-3}(1 + (q - 1)z)^n B(\frac{1 - z}{1 + (q - 1)z}) ,$$

where

$$B(z) = 1 + B_{n-3} z^{n-3} + B_{n-1} z^{n-1} + B_n z^n .$$

By calculating A_1, A_2 and A_3 we find three equations for B_{n-3}, B_{n-1} and B_n. Solving these we find the required result. □

COROLLARY 2.3. *Under the conditions of* (2.2) *we have*

$$q \geq \frac{1}{2}(n-3) .$$

Proof. $B_{n-1} \geq 0$. □

COROLLARY 2.4. *Under the conditions of* (2.2) *we have*

$$A_4 = \frac{1}{24} n(n-1)(n-3)(n-6)(q-1) .$$

Proof. Since we know B(z) we can find all the coefficients of A(z) from the MacWilliams relations. □

The result of (2.4) is remarkable for the following reason. If two words of weight 4 in C have the same support they must be linearly dependent. If this were not so we could make linear combinations of these two words which have weight 3 in four ways, thus constructing 4 blocks of $\phi(D)$ on 4 points which is impossible. A similar argument shows that the support of a word of weight 3 cannot be a subset of the support of a word of weight 4. Combining these, we find that C has at most $\frac{(q-1)}{4!} n(n-1)(n-3)(n-6)$ words of weight 4. By (2.4) equality holds in this a priori estimate! Apparently every 3-subset of the n positions is either a block of STS(n) or a subset of the support of n - 6 code words of weight 4 in C. This means that the supports of the code words of weight 4 form a $2 - (n,4,\frac{(n-3)(n-6)}{2})$. It is not difficult to show that for $n > 9$ every 5-subset is the support of a code word, i.e. no interesting designs are found using such words or words of larger weight. The codes for $n \leq 9$ are treated below.

3. Codes supported by STS(7).

The design STS(7) is unique. Let C be a linear code over GF(q) supported by this design $\mathcal{D}$. By (2.1) C has dimension 4. By the remarks following (2.4) C is equivalent to a code with generator

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & x & 0 \\ 0 & 0 & 0 & 1 & y & z & 1 \end{bmatrix},$$

where the positions 5,6,7 have been chosen so that $\{5,6,7\} \notin \mathcal{D}$ and as many entries of G as possible have been made 1 by multiplying rows and columns by suitable constants. We now have 3 triples of $\mathcal{D}$. To get $\{1,4,5\} \in \mathcal{D}$ we must have z = 1; to get $\{2,4,6\} \in \mathcal{D}$ we must have y = 1 and finally $\{3,4,7\} \in \mathcal{D}$ yields x = 1. The only way to get $\{1,2,3\} \in \mathcal{D}$ is to have z = 0 in which case the sum of the first three rows of G yields the required code word. Combining this with (1.3) we find

THEOREM 3.1. *The design* STS(7) *supports a linear code over* GF(q) *if and only if* $q = 2^r$.

4. Codes supported by STS(9).

In this section $\mathcal{D}$ is the affine plane of order 3 which is the unique STS(9). We prove a theorem similar to (3.1).

THEOREM 4.1. *If* STS(9) *supports a linear code over* GF(q) *then* $q \not\equiv 2 \pmod 3$.

Proof. We number the points in such a way that the blocks of $\mathcal{D}$ are {1,2,3}, {1,4,5}, {1,6,7},{1,8,9},{2,4,6}, {2,5,8}, {2,7,9}, {3,4,9}, {3,5,7} {3,6,8}, {4,7,8}, {5,6,9}.

By multiplying rows and columns by suitable constants we find a generator G for the code using the first six blocks where

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & A & 0 & B & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & C & 0 & 0 & D & 0 \end{bmatrix} .$$

Here we use the fact that by (2.1) the code has dimension 6 and that G has rank 6 over any field. We must now construct the remaining triples of STS(9) as linear combinations of rows of G. To get $\{2,7,9\}$ we must have

$$(0,a_2,a_3,a_4,a_5,a_6)G = (0,1,0,0,0,0,a_3,0,a_4) ,$$

which yields the equation

(4.2) $\quad AC + AD + BC = 0.$

In a similar way we find:

(4.3) $\quad A + B = -1 \qquad$ (using $\{3,5,7\}$),

(4,4) $\quad C = B \qquad$ (using $\{4,7,8\}$),

(4.5) $\quad A = D \qquad$ (using $\{5,6,9\}$).

By expressing B,C,D, in A and substituting the result in (4.2) we find

(4.6) $\quad A^2 + A + 1 = 0.$

Now (4.6) implies that either $A = 1$ and $q = 3^r$ or $A \neq 1$, $A^3 = 1$ which is possible in GF(q) only if $q \equiv 1 \pmod 3$. □

It turns out that the condition of (4.1) is also sufficient. To show this we explicitly construct codes with the required properties.

THEOREM 4.7. *Let* $q \equiv 1 \pmod 3$. *Let* α *be a primitive* 3rd *root of* 1 *in* GF(q) *and*

$$H := \begin{bmatrix} 0 & 0 & 0 & -1 & -\alpha & -\alpha^2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & -1 & -\alpha & -\alpha^2 \\ -1 & -\alpha & -\alpha^2 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix} .$$

Then the (9,6)-linear code over GF(q) *with* H *as parity check matrix is supported by* STS(9).

Proof. We divide the 9 positions into three groups, namely {1,2,3}, {4,5,6}, {7,8,9}. Since $1 + \alpha + \alpha^2 = 0$ each of these groups is a block of $\phi(D)$. Furthermore $\alpha \neq 1$, $\alpha \neq \alpha^2$ and $\alpha^2 \neq 1$ imply that no code word has weight 2. Clearly a code word with two coordinates in the same group must be one of the three mentioned above. It remains to check words of D with one element in each of these groups. Let such a word have support $\{u,v+3,w+6\}$ where $(u,v,w) \in \{1,2,3\}^3$. Then, if the nonzero coordinates are (ξ,η,ζ) we find

$$\begin{array}{lll} -\eta\alpha^{v-1} + \zeta & = 0 \\ \xi \qquad\qquad - \zeta\alpha^{n-1} & = 0 \\ -\xi\alpha^{u-1} \qquad\quad + \eta & = 0\ , \end{array}$$

i.e. $\alpha^{u+v+w} = 1$ which means that the remaining code words of weight 3 are characterized by $u + v + w \equiv 0 \pmod 3$. Therefore $\phi(D)$ is STS(9). □

THEOREM 4.8. *For* $r \geq 1$ *there is a* (9,6)*-code over* $GF(3^r)$ *supported by* STS(9).

Proof. Let

$$H := (I \quad J-I \quad J-2I)$$

be the parity check matrix of a (9,6)-code over $GF(3^r)$. In the same way as in (4.7) one easily checks that the set $\phi(D)$ is STS(9). □

Remark. The parity check matrices which we used in (4.7) and (4.8) provide us with a set of 9 points in the Desarguesian projective plane PG(2,q), ($q \not\equiv 2 \pmod 3$), forming a subconfiguration isomorphic to the affine plane of order 3. It was pointed out to the authors recently that this geometric formulation of our result was given by Ostrom and Sherk [7].

5. *The designs* STS(13).

There are two nonisomorphic designs STS(13) (cf. [5], p.237). For both designs we can (in the same way as in (4.1)) form a generator matrix of a code possibly supported by the design:

$$\begin{bmatrix}
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & A & 0 & B & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & C & 0 & 0 & D & 0 \\
0 & 0 & 1 & 0 & E & 0 & 0 & 0 & 0 & 0 & 0 & F & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & G & 0 & 0 & 0 & H & 0 & 0
\end{bmatrix} .$$

It is now straightforward (although a rather tedious task) to repeat the argument of (4.1) and try to write the remaining triples of each of the two designs STS(13) as linear combinations of the rows of this generator matrix. We find a number of equations like (4.2) to (4.5). We omit the details which the reader can easily check for himself. In both cases the result is that one of the entries A,B,C,D must be 0 which is a contradiction. We state this as

THEOREM 5.1. *A design* STS(13) *does not support a linear code.*

REFERENCES

[1] E.F. Assmus Jr., and H.F. Mattson Jr., *On tactical configurations and error-correcting codes*, J. Combinatorial Theory 2 (1967), 243-257.

[2] E.F. Assmus Jr., and H.F. Mattson Jr., *New 5-designs*, J. Combinatorial Theory 6 (1969), 122-151.

[3] E.F. Assmus Jr., and H.F. Mattson Jr., *Algebraic theory of codes II*, AFCRL-71-0013 Report of the Applied Research Laboratory of Sylvania Electronic Systems (1971).

[4] P.J. Cameron and J.H. van Lint, *Graph theory, coding theory and block designs*, London Math. Soc. Lecture Note Series 19 (1975), Cambridge Univ. Press.

[5] M. Hall, Jr., *Combinatorial theory*, Blaisdell, Waltham, Mass. (1967).

[6] J.H. van Lint, *Coding theory*, Lecture Notes in Math. 201 Springer-Verlag, Berlin, (1971).

[7] T.G. Ostrom and F.A. Sherk, *Finite projective planes with affine subplanes*, Canadian Math. Bull 7 (1964), 549-559.

Technological University Eindhoven

The Netherlands.

Received April 12, 1976