STEINER SYSTEMS FROM BINARY CODES

J. D. Key and F. E. Sullivan
Department of Mathematical Sciences
Clemson University
Clemson SC 29634

August 7, 1996

Abstract

The binary linear code of a Steiner triple system on $2^d - 1$ points, where $d \geq 3$ is an integer, contains a copy of the Hamming code $\mathcal{H}_d$; this fact can be used to characterize those systems on $2^d - 1$ points that have low dimension, and to show that these systems can always be extended to Steiner quadruple systems whose binary code is the extended code of the Steiner triple system.

1 Introduction

One of the questions that Steiner asked in his 1853 paper [9] was whether every Steiner triple system extends to a Steiner quadruple system. Much work has been done on this question, and no counter-examples are known. However, the question has been answered in the affirmative for various classes of triple systems (see the surveys in Phelps [8] and Hartman and Phelps [5]). Among those classes that are known to extend are the classical triple systems obtained from the design of points and lines of a projective space over $\mathbf{F}_2$, $PG_{d,1}(\mathbf{F}_2)$, which extends to the design of points and planes of the affine geometry, i.e. $AG_{d+1,2}(\mathbf{F}_2)$, and, in this extension, the code of the affine-geometry design is the extended code of the projective-geometry design. Here we take a mostly coding-theoretical approach to consider a related class of triple systems and prove the following theorem:

Theorem 1 *Let $\mathcal{D}$ be a Steiner triple system on $v = 2^{d+1} - 1$ points and suppose that the 2-rank of $\mathcal{D}$ is $2^{d+1} - 1 - d$ or $2^{d+1} - d$. Then $\mathcal{D}$ can be extended to a 3-$(2^{d+1}, 4, 1)$ design whose code is the extended code of $\mathcal{D}$.*

It is well known that the theorem is true for dimension $2^d - d - 1$, and, in fact, we use this in the proof of the stated theorem. The fact that the systems extend

when the dimension is $2^d - d$ or $2^d - d + 1$ also follows from other considerations regarding the existence of projective hyperplanes that extend: see Teirlinck [11] for more on this. Our approach here is from the point of view of coding theory. The construction described here is analogous to a construction given by Etzion and Vardy [4] for non-linear perfect binary codes.

The theorem is proved in Section 3. In Section 2 we describe our terminology and give previous results that will be needed for our propositions.

2 Terminology and previous results

An incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, with point set $\mathcal{P}$, block set $\mathcal{B}$ and incidence $\mathcal{I}$, is a t-(v, k, λ) design if every block is incident with precisely k points and any set of t distinct points are together incident with precisely λ blocks. A *Steiner triple system* $\mathcal{D}$ is a 2-$(v, 3, 1)$ design, i.e. every block is incident with precisely three points and any two distinct points are together incident with exactly one block. For 2-designs with $\lambda = 1$, we sometimes refer to the blocks as *lines*. A *Steiner quadruple system* $\mathcal{Q}$ is a 3-$(v, 4, 1)$ design; the *derived design* obtained by deleting any point x and all the blocks not containing that point, forms a Steiner triple $\mathcal{D}$ system with parameters 2-$(v-1, 3, 1)$. The 3-design $\mathcal{Q}$ is an *extension* of $\mathcal{D}$.

We denote by $PG_{d,1}(\mathbf{F}_2)$ the 2-$(2^{d+1} - 1, 3, 1)$ design of points and lines of the projective geometry $PG_d(\mathbf{F}_2)$ of dimension d over $\mathbf{F}_2$.

For any finite incidence structure $\mathcal{D} = (\mathcal{P}, \mathcal{B})$, the *code* $C_p(\mathcal{D})$ of $\mathcal{D}$ over a prime field F_p is the subspace of the space $F_p^{\mathcal{P}}$ of all functions from $\mathcal{P}$ to F_p that is spanned by the incidence vectors of the blocks of $\mathcal{D}$. If $X \subseteq \mathcal{P}$, denoting the characteristic function on X by v^X, we have $C_p(\mathcal{D}) = \langle v^B | B \in \mathcal{B} \rangle$. The dimension of $C_p(\mathcal{D})$ is referred to as the *p-rank* of $\mathcal{D}$. The *all-one vector* in any code will be denoted by j; thus $j = v^{\mathcal{P}}$. The *orthogonal* of a code C defined on the coordinate set $\mathcal{P}$ will be denoted by $C^{\perp}$, and is taken with respect to the standard inner product, i.e.

$$C^{\perp} = \{u \,|\, u \in F_p^{\mathcal{P}}, (u, w) = \sum_{x \in \mathcal{P}} u(x)w(x) = 0 \text{ for all } w \in C\}.$$

The *support* of a vector $c \in C_p(\mathcal{D})$ is $\{x \in \mathcal{P} \,|\, c(x) \neq 0\}$, denoted by $\mathrm{Supp}(c)$. We say c is a weight-m vector if $|Supp(c)| = m$. The non-zero vector c is *constant* if $c(x) = \alpha$, a constant, for all $x \in \mathrm{Supp}(c)$, i.e. if $c = \alpha v^{\mathrm{Supp}(c)}$.

If $\mathcal{D} = PG_{d,1}(\mathbf{F}_2)$ then $C_2(\mathcal{D})$ is a *Hamming* code, generally denoted by $\mathcal{H}_{d+1}$. The dimension is $2^{d+1} - (d+1) - 1$, the minimum weight is 3, and the minimum-weight vectors are precisely the incidence vectors of the lines: see [2], for example.

The following is well-known and a proof can be found in [6]:

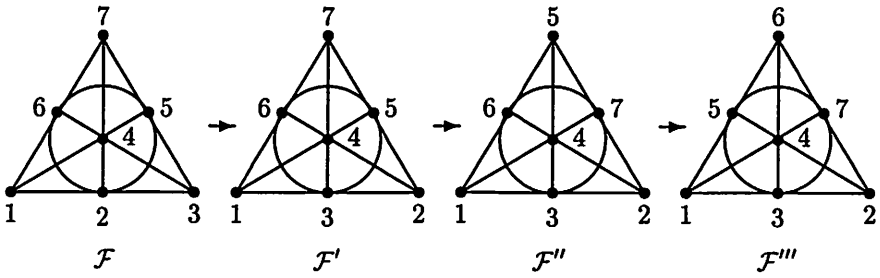

Figure 1: Interchanging points in the Fano Plane

Result 2 *Let $\mathcal{D}$ be a 2-$(v, 3, 1)$ design where $v \geq 7$ and let $C = C_2(\mathcal{D})$. If the minimum weight of C is 3 then the weight-3 vectors are the incidence vectors of the blocks of $\mathcal{D}$. Further, $v = 2^d - 1$ for some $d \geq 3$, $\mathcal{D} = PG_{d-1,1}(\mathbf{F}_2)$ and $C = \mathcal{H}_d$.*

The next result was first proved in [3]:

Result 3 (Doyen, Hubaut and Vandensavel) *Let $\mathcal{D}$ be a 2-$(v, 3, 1)$ design, and let G be its automorphism group. If G is transitive on points then $\text{rank}_2(\mathcal{D}) = v$ or $\mathcal{D}$ is the design of points and lines of a projective geometry over $\mathbf{F}_2$.*

Our construction of extensions is based on the following result that is a particular case of a theorem from Key and Sullivan [6]:

Result 4 *Let $\mathcal{D}$ be a 2-$(2^d - 1, 3, 1)$ design where $d \geq 3$ and let $C = C_2(\mathcal{D})$. Then C contains a subcode isomorphic to the Hamming code $\mathcal{H}_d$. Equivalently, C contains a set of weight-3 vectors whose supports form the blocks of the design $PG_{d-1,1}(F_2)$.*

3 Extensions of the designs and the codes

We show now how the theorem can be proved using the binary codes and their extensions. We first describe the construction, which is based on Figure 1, and make the following observation as a lemma which is easily verified:

Lemma 5 *Let $\mathcal{S}$ and $\mathcal{S}'$ be Steiner triple systems on v points. If $C_2(\mathcal{S}) \subset C_2(\mathcal{S}')$, then $C_2(\mathcal{S}')$ contains a weight-1 vector not in $C_2(\mathcal{S})$.*

The construction described in Proposition 6 and Figure 1 can be found essentially in Sullivan [10]:

Proposition 6 *Let $\mathcal{D}$ be the design $PG_{d,1}(\mathbf{F}_2)$ of points and lines of the projective geometry $PG_d(\mathbf{F}_2)$. Let $C = C_2(\mathcal{D}) = \mathcal{H}_{d+1}$, and suppose $d \geq 3$. If the Fano plane $\mathcal{F}$ shown in Figure 1 is a configuration in $\mathcal{D}$, and if two points are interchanged as shown in $\mathcal{F}'$, then the structure $\mathcal{D}'$ formed by taking the lines shown in $\mathcal{F}'$ and all the other original lines of $\mathcal{D}$ is a Steiner triple system with code $C' = C \oplus \langle v^{\{1\}} \rangle$.*

Similarly, if a further change to $\mathcal{F}''$ is performed, it will produce a design $\mathcal{D}''$ with code $C'' = C \oplus \langle v^{\{1\}} \rangle \oplus \langle v^{\{2\}} \rangle$.

Proof: The proof is quite elementary and direct. □

Corollary 7 *Any number of planes containing the point 1 can be altered in the manner described in Proposition 6 and the resulting code will be C' or an isomorphic copy of C.*

Any number of substitutions of the type described in Proposition 6 in planes that intersect in the line $\{1,2,3\}$, or substitutions of the type described, with 1 replaced by 2 or 3, in planes that meet other altered planes only in the points 1, 2 or 3, respectively, will result in a design whose code is C'', or an isomorphic copy of C' or C.

Proposition 8 *The designs $\mathcal{D}'$ and $\mathcal{D}''$ obtained as in Proposition 6 extend to Steiner quadruple systems whose codes are the extended codes $\widehat{C'}$ and $\widehat{C''}$ respectively.*

Proof: In the notation of Proposition 6, $\widehat{C}$ is the extended Hamming code. It is well known (see, for example, Assmus and Key [2]) that the codewords of weight-4 in $\widehat{C}$ form a Steiner quadruple system, $\mathcal{E}$ say, and that $C_2(\mathcal{E}) = \widehat{C}$.

Let $\widehat{C'}$ be the extended code of C'. We describe how to construct the design $\mathcal{E}'$, an extension of $\mathcal{D}'$. We know that the sets

$$\{1,2,4,6\}, \{1,2,5,7\}, \{1,3,5,6\}, \{1,3,4,7\}$$

are the supports of weight-4 codewords in C. Replace these codewords by the four weight-4 vectors in the coset $C + v^{\{1\}}$ with supports

$$\{1,2,4,7\}, \{1,2,5,6\}, \{1,3,4,6\}, \{1,3,5,7\}.$$

Now $\mathcal{E}'$ is defined as follows: take all the triples of $\mathcal{D}'$ with the new point ∞ attached, and the supports of all weight-4 vectors in C, apart from the four substitutions noted above. Notice that all other weight-4 vectors are also in C' since C is a subspace of C'. It is a straightforward process to verify that $C_2(\mathcal{E}') = \widehat{C'}$.

The corresponding construction for $\mathcal{D}''$ and $\widehat{C''}$ proceeds in an analogous manner. □

Proof of Theorem 1: We prove this for $\mathcal{D}$ of rank $2^{d+1}-1-d$; the other case follows similarly. We know, from Lemma 5, that the code C' of $\mathcal{D}$ is $C \oplus \langle e \rangle$ where $C = \mathcal{H}_{d+1}$ and e is a weight-1 vector. Suppose that $e = v^{\{1\}}$. The lines of $\mathcal{D}$ can be found among the supports of the weight-3 vectors in C'. These vectors are either weight-3 vectors of C or are obtained from weight-4 vectors of C whose support contains the point 1. Thus the only weight-3 vectors in C' whose supports contain the point 1 are the incidence vectors of the lines of $\mathcal{P} = PG_{d,1}(\mathbf{F}_2)$. Thus these lines will necessarily be lines of the design $\mathcal{D}$ also. Since the weight-4 vectors in C are precisely the sums of two intersecting lines, they always define a unique Fano plane in $\mathcal{P}$. The new weight-3 vectors thus always define Fano planes containing the point 1 in the design $\mathcal{P}$.

Suppose ℓ is a line of $\mathcal{D}$ that is not a line of $\mathcal{P}$. Then $1 \notin \ell$ and $\ell \cup \{1\}$ is on a Fano plane, say $\mathcal{F}$ as shown in Figure 1 of $\mathcal{P}$. Suppose $\ell = \{2,4,6\}$. Since our lines through 1 are the same as the original, we have to choose our other lines in this plane to be those shown in $\mathcal{F}'$ in Figure 1. These observations show that any line ℓ of $\mathcal{D}$ that is not a line of $\mathcal{P}$ generates, together with the point 1, a Fano plane as a subsystem of $\mathcal{D}$. Of course this will not be true for ℓ together with an arbitrary point not on ℓ. For any line ℓ of $\mathcal{D}$ that is also a line of $\mathcal{P}$, if $1 \notin \ell$, then again $\ell \cup \{1\}$ generates a Fano plane. Notice that we have shown that the design $\mathcal{D}$ has been obtained according to the method described in Corollary 7.

Now we show how to extend $\mathcal{D}$ to a Steiner quadruple system whose code is the extended code of $\mathcal{D}$. Let ∞ be the new point. Then the blocks containing ∞ are given. Suppose now we take a set S of three points that form a triangle in $\mathcal{D}$. If S also forms a triangle in $\mathcal{P}$ then S is in a Fano plane $\mathcal{F}$ of $\mathcal{P}$. If the lines of $\mathcal{F}$ are lines of $\mathcal{D}$, then define the quadruple containing S as is done by extending $\mathcal{F}$. If $\mathcal{F}$ is a relabelled plane (and thus contains the point 1), then extend S as would be done for the relabelled plane. In either case, the extension is achieved within $\widehat{C'}$.

Now suppose S is a triangle in $\mathcal{D}$ but a line of $\mathcal{P}$. Then $1 \notin S$, and S is in a unique Fano plane, as a subsystem of $\mathcal{D}$, containing 1. This Fano plane necessarily has the three lines through 1 common to $\mathcal{D}$ and $\mathcal{P}$, and the remaining four lines interchanged for triangles, as in $\mathcal{F}$ and $\mathcal{F}'$ above. There is a unique fourth point x such that $S \cup \{x\}$ is the support of a weight-4 vector in C', and we choose this set to be a block. All cases are covered, and $\mathcal{D}$ extends to a Steiner quadruple system whose binary code is $\widehat{C'}$.

In fact, to get the Steiner quadruple system that extends $\mathcal{D}$, only the weight-4 vectors whose supports contain 1 need be replaced, since if a weight-4 vector is in the Hamming code it is the sum of the incidence vectors of two lines that meet and hence span a Fano plane in $\mathcal{P}$; if 1 is in this plane then the support will still form a quadrangle in $\mathcal{D}$, and thus all the weight-4 vectors of the Hamming code C that do not contain the point 1 in their support can be taken as blocks. For the remaining blocks not containing ∞, we choose as follows: if w is a weight-4 vector in C with support $S \ni 1$, then if $S - \{1\}$ is one of the lines ℓ of $\mathcal{D}$ that

replaces a line ℓ' of $\mathcal{P}$, then replace S by $\ell' \cup \{1\}$; if $S - \{1\}$ is not a line of $\mathcal{D}$, then S is included as a block. □

This completes the proof of the theorem.

Further applications seem more complicated, since the number of weight-3 vectors increases, and the choice is harder. However we can produce a chain of designs that all extend, using the construction of Proposition 6.

Proposition 9 *Let $\mathcal{D}_0$ be the design $PG_{d,1}(\mathbf{F}_2)$ of points and lines of the projective geometry $PG_d(\mathbf{F}_2)$ where $d \geq 3$. Then we can define a sequence of Steiner triple systems, $\mathcal{D}_i$, for $1 \leq i \leq d$, such that $\dim(C_2(\mathcal{D}_i)) = 2^{d+1} - d - 2 + i$, and*

$$C_2(\mathcal{D}_0) \subset C_2(\mathcal{D}_1) \subset \ldots \subset C_2(\mathcal{D}_i) \subset \ldots \subset C_2(\mathcal{D}_d) \subset \mathbf{F}_2^{2^{d+1}-1}.$$

Further, each design is extendable to a Steiner quadruple system, $\mathcal{Q}_i$, and the extended code $\widehat{C_2(\mathcal{D}_i)} = C_2(\mathcal{Q}_i)$ for each i.

Proof: Starting in $\mathcal{D}_0$ as usual, choose first a point 1, say, and add its incidence vector to $C_2(\mathcal{D}_0)$; choose $\mathcal{D}_1$ as described in Proposition 6. Then proceed with another point 2, say, and obtain $\mathcal{D}_2$ as in Proposition 6. Now add the vector $v^{\{7\}}$, where this is a point not on the line through 1, 2, as illustrated in Figure 1. Adding this vector gives *all* the weight-1 vectors from this plane. All the triples are now changed, as shown in $\mathcal{F}'''$ of Figure 1. This gives the next design $\mathcal{D}_3$ with code $C_2(\mathcal{D}_2) \oplus \langle v^{\{7\}} \rangle$. For the next step we must choose a Fano plane in $\mathcal{D}_0$ that is disjoint from $\mathcal{F}'''$: this is possible within our restrictions on the dimension of the code. In this new plane we need make only one switch, as in Proposition 6, in order to have 15 weight-1 vectors. We continue in this manner to get the triple systems and their codes, all satisfying the conditions stated. The extension to quadruple systems with the desired codes follows easily, using our previous arguments. □

We are unable to extend this result to the full dimension because the choice of triples becomes too numerous. However, Steiner triple systems with transitive automorphism groups always have the full space as binary code, unless they are the projective-geometry design: this is clear from Result 3 or by the simple observation that if the design is not the projective-geometry design then the code has weight-1 vectors, and by transitivity it will have all the weight-1 vectors.

Notes

(1) Bases of weight-3 and weight-1 vectors for the codes of these Steiner triple systems can now easily be found, using the basis of minimum-weight vectors for the binary Hamming code as described in [6].

(2) Similar results for ternary codes can be found in Key and Sullivan [7].

(3) After this paper was first submitted in October 1994, a paper of E. F. Assmus [1] giving a comprehensive analysis of the binary codes of Steiner triple systems appeared. That paper mentions our results.

References

[1] E. F. Assmus, Jr. On 2-ranks of Steiner triple systems. *Electron. J. Combin.*, 2:Research Paper 9, 1995.

[2] E. F. Assmus, Jr. and J. D. Key. *Designs and their Codes.* Cambridge University Press, 1992. Cambridge Tracts in Mathematics, Vol. 103 (Second printing with corrections, 1993).

[3] Jean Doyen, Xavier Hubaut, and Monique Vandensavel. Ranks of incidence matrices of Steiner triple systems. *Math. Z.*, 163:251–259, 1978.

[4] Tuvi Etzion and Alexander Vardy. Perfect binary codes: constructions, properties and enumeration. *IEEE Trans. Inform. Theory*, 40:754–763, 1994.

[5] Alan Hartman and Kevin T. Phelps. Steiner quadruple systems. In Jeffrey H. Dinitz and Douglas R. Stinson, editors, *Contemporary Design Theory*, pages 205–240. John Wiley & Sons, 1992.

[6] J. D. Key and F. E. Sullivan. Codes of Steiner triple and quadruple systems. *Des. Codes Cryptogr.*, 3:117–125, 1993.

[7] J. D. Key and F. E. Sullivan. Steiner triple systems with many affine hyperplanes. *Congressus Numerant.*, 107:105–112, 1995.

[8] K. T. Phelps. A survey of derived triple systems. *Ann. of Discrete Math.*, 7:105–114, 1980.

[9] J. Steiner. Combinatorische Aufgabe. *J. Reine Angew. Math.*, 45:181–182, 1853.

[10] F. E. Sullivan. Some comments on weight-1 vectors. *Congressus Numerant.*, 101:151–154, 1994.

[11] Luc Teirlinck. On projective and affine hyperplanes. *J. Combin. Theory, Ser. A*, 28:290–306, 1980.