On 2-ranks of Steiner triple systems

E. F. Assmus, Jr.*

Submitted: March 13, 1995; Accepted: April 17, 1995

Abstract

Our main result is an existence and uniqueness theorem for Steiner triple systems which associates to every such system a binary code — called the "carrier" — which depends *only* on the order of the system and its 2-rank. When the Steiner triple system is of 2-rank less than the number of points of the system, the carrier organizes all the information necessary to construct directly *all systems of the given order and* 2*-rank* from Steiner triple systems of a specified smaller order. The carriers are an easily understood, two-parameter family of binary codes related to the Hamming codes.

We also discuss Steiner quadruple systems and prove an analogous existence and uniqueness theorem; in this case the binary code (corresponding to the carrier in the triple system case) is the dual of the code obtained from a first-order Reed-Muller code by repeating it a certain specified number of times.

Some particularly intriguing possible enumerations and some general open problems are discussed. We also present applications of this coding-theoretic classification to the theory of triple and quadruple systems giving, for example, a direct proof of the fact that all triple systems are derived provided those of full 2-rank are and showing that whenever there are resolvable quadruple systems on u and on v points there is a resolvable quadruple system on uv points.

*The author wishes especially to thank Paul Camion and Pascale Charpin. The research atmosphere that they have created at *Projet Codes, INRIA* surely contributed to this investigation, which took place during the early months of 1995 while the author was a visitor.

The methods used in both the classification and the applications make it abundantly clear why the number of triple and quadruple systems grows in such a staggering way and why a triple system that extends to a quadruple system has, generally, many such extensions.[1]

1 Introduction

The work we report on here began as an effort to understand the surprising facts uncovered by a comprehensive computer study of the 80 Steiner triple systems of order 6 (on 15 points) undertaken by Tonchev and Weishaar [22]. Among the results we establish, perhaps the easiest to state and prove is the following:

A Steiner triple system on n points has 2-rank $n-1$ if and only if its binary code is the direct sum of an even code and a full code $\boldsymbol{F}_2^r$. Moreover we have $n = 2r+1$ with the support of the full code the support of the unique maximal subsystem on r points — the support of the even code being the corresponding complementary oval.

This result explains why only one binary code arose from the sixteen Steiner triple systems of 2-rank 14 and order 6 and immediately gives the code's weight enumerator.

But the result cited above was a relatively minor consequence of this investigation since it quickly evolved into a full-fledged investigation of Steiner triple systems of deficient 2-rank — that is, 2-rank less than the number of points of the system. In fact the work can be taken as a *binary view* of the whole range of Steiner triple systems: we show in principle how to construct recursively all Steiner triple systems of deficient 2-rank using the degenerate system on one point and those systems of full 2-rank as a starting point. Thus the systems of full 2-rank are seen as the building blocks[2] since, from the binary point of view, Steiner triple systems of full 2-rank must be viewed as unintelligible and hence taken as given facts of life.

The mandarins in the binary world peopled by Steiner triple systems are the systems given by the points and lines of a projective geometry over the

[1] AMS Primary Classification: 05B07; Secondary Classification: 94B25.

[2] This will undoubtedly strike some readers as going a bit far in deciding what the building blocks should be and, indeed, the vast majority of Steiner triple systems have full 2-rank.

field $\boldsymbol{F}_2$ and the binary codes involved are the Hamming codes. Here the 2-rank is as deficient as it can possibly be: the 2-rank of the design of points and lines of $\mathrm{PG}_{k-1}(\boldsymbol{F}_2)$ is $2^k - 1 - k$, or better, $n - k$, where $n = 2^k - 1$ is the number of points of this classical system. Our basic existence and uniqueness theorem for Steiner triple systems of deficient 2-rank is the following:

For any admissible[3] $n > 7$, *writing* $n + 1 = u \times 2^k$ *with* u *odd, and choosing an* i *with* $1 \leq i < k$, *there is a Steiner triple system on* n *points with* 2*-rank* $n - k + i$. *Moreover, all triple systems on* n *points with* 2*-rank* $n - k + i$ *share the same binary code.*

The results presented here allow one, *in principle*, to construct all the Steiner triple systems with the given deficient 2-rank. We did not allow $i = k$ in the existence theorem above for those are the systems with full 2-rank — which we cannot in general construct. Such systems do, however, exist for $n > 7$ and we construct many such systems via Theorem 7.2. We have honored the classical systems by leaving them unmentioned for those n of the form $2^k - 1$.

In particular, then, we show that the binary code of a Steiner triple system is completely determined by its 2-rank; this explains why Tonchev and Weishaar found only five codes (one for each dimension between 11 and 15) among the 80 Steiner triple systems on 15 points.[4]

Some may wish to see this effort as a "constructive" redoing of a program begun by Luc Teirlinck and brought to what seemed then to be a definitive end by Doyen, Hubaut and Vandensavel when they proved their marvelous theorem describing the modular ranks of Steiner triple systems. We will not, however, use their results here; the reader need only know the basic facts about codes and designs[5] to understand the material to follow.

[3] That is, $n \equiv 3, 7 \pmod{12}$. Note that necessarily $k \geq 2$.

[4] The computer study done by Tonchev and Weishaar also looked at the binary codes given by the *column spaces* of the incidence matrices; these so-called *point codes* are a complete invariant for the 80 triple systems. Thus the 80 incidence matrices of the Steiner triple systems of order 6 have the remarkable property that their binary row spaces produce only five essentially distinct codes of block length 15 while their binary column spaces produce 80 essentially distinct codes of block length 35. This phenomenon may very well be characteristic of Steiner triple systems in general. For a brief discussion of the matter see [2, Section 7].

[5] Easily gleaned from Chapters 1 and 2 of [3] or, indeed, from almost any book discussing designs and codes.

Others may wish to see it as an elaboration of an ancient "doubling" construction frequently attributed to Reiss, who in the Spring of 1856 gave a proof of the fact that Steiner triple systems exist for all $n \equiv 1, 3 \pmod 6$. Again, the reader need not be familiar with the constructions necessary to give such a proof.

So, we will be concerned throughout with Steiner triple systems of 2-rank that is *not* maximal. It is surely true that such systems are rare and that most Steiner triple systems on $n \equiv 3, 7 \pmod{12}$ points have full 2-rank. In order for the rank to drop not only must the point set be of cardinality congruent to 3 modulo 4, as we have insisted in the existence and uniqueness result above, but the system must necessarily have subsystems of maximal size. But, the smaller the 2-rank the closer the system is to the classical system of points and lines of a projective geometry over the two-element field and it makes sense to say something about such systems.

We will associate to each such system a binary code which we will call the *carrier*. We will determine all possible carriers and show how to construct all systems of deficient 2-rank from the carriers and systems of smaller order. The carriers turn out to be a two-parameter family of easily understood binary codes with enormous automorphism groups, and these codes visibly exhibit the structure of the binary projective space attached to each Steiner triple system of deficient 2-rank. Moreover, the carrier organizes the data necessary to construct the Steiner triple systems of which it is the carrier and makes it clear why the number of such systems grows in such a staggering way with n.

One should expect a classification such as the one just described to reduce a question about Steiner triple systems to the same question about those of full 2-rank. As an illustration of just that we give a direct proof of a result (Theorem 6.1) closely related to a result of Mendelsohn[6] that immediately gives the following:

If Steiner triple systems of full 2-rank are derived then all Steiner triple systems are derived.[7]

To be fair this leaves a lot unproved, but it is not entirely out of the question that one could show that those with full 2-rank are derived. Moreover,

[6]Mendelsohn's result (see [13]) is couched in the language of *sloops* and *squiens*; it very well may be equivalent to our result.

[7]A Steiner triple system is derived if it extends to a Steiner quadruple system.

the results we describe in Section 6 also show how to construct all Steiner quadruple systems of deficient 2-rank, an easier task, and Theorem 7.2 yields many derived Steiner triple systems of full 2-rank.

The reader looking for the flavor of the subject may want to read only Section 2 and Section 8. The main technical development comes in Section 3. The construction of all triple systems of deficient 2-rank is treated in Section 4 and Section 5 discusses some particularly easy cases of the construction. Section 6 includes an application to the question of which triple systems are derived and initiates a discussion of Steiner quadruple systems. We complete that discussion in Section 7 by stating and proving our existence and uniqueness theorem for quadruple systems of deficient 2-rank, Theorem 7.1, and giving an application to resolvable Steiner quadruple systems. Section 8 mentions the "ternary" view of Steiner triple systems and makes some concluding remarks.

2 Steiner triple systems of deficient 2-rank

Suppose we are given a Steiner triple system on a set S of cardinality n whose binary code D is a proper subspace of $\boldsymbol{F}_2^n$. This implies that n is congruent to 3 modulo 4 since the order, $\frac{n-3}{2}$, of the system must be even. If r is the number of weight-one vectors in D then, of course, $r < n$. But much more is true:

Proposition 2.1 *Let S' be the support of the set of weight-one vectors of the binary code D of a Steiner triple system on the set S. Assume that S' is a proper subset of S. Then either S' is empty and $|S| = 2^k - 1$, with the Steiner system the classical one of points and lines of $PG_{k-1}(\boldsymbol{F}_2)$, or S' is the support of a subsystem*[8] *and D is the direct sum of the full binary code on S' and a code C of minimum weight two whose support is the complement of S' in S.*

Proof: If S' is empty, then D must have minimum weight 3; moreover, the minimum-weight vectors must be precisely the incidence vectors of the given

[8] A *subsystem* of a Steiner triple system is a set of points S' with the property that if a triple has two points in S' its third point is also in S' — so that the point set together with the triples contained in it forms a Steiner triple system; we regard a one-point subset as a subsystem, called the *degenerate* Steiner triple system.

Steiner triple system. It follows (see, for example, [4]) that we have the classical system.

Assume S' is non-empty. Then, clearly, the full binary code on S' is a subcode of D and given any two distinct points of S' the triple containing those points must have its third point in S' for otherwise there would be a weight-one vector with a 1 not in S'. For the same reason the projection of D onto the complement of S' must have minimum weight 2 and, obviously, D is the direct sum of that projection and the full binary code on S'. $\square$

Clearly the code C of the Proposition is uniquely determined by the Steiner triple system; we shall call this code the **carrier** of the Steiner triple system. Its block length will be $|S| - |S'|$ and its dimension will determine the 2-rank of the triple system — which is, of course, the dimension of D: $\dim(D) = \dim(C) + |S'|$. Similarly the subsystem on S' is uniquely determined by the Steiner triple system; we shall call this subsystem the **trivializing** subsystem since that part of D supported by S' is of no use in determining the underlying triple system. This trivializing subsystem may very well be a Steiner triple system with deficient 2-rank; for example those 16 of the 80 systems of order 6 whose 2-rank is 14 must have, as we shall soon see, the Fano plane as their trivializing subsystem.

Proposition 2.2 *Let D be the binary code of a Steiner triple system on a set S of cardinality $n = 2r+1$. Suppose the Steiner triple system has 2-rank less than n. Then, if S' is the support of the set of weight-one vectors of D, $|S'| \leq r$ with equality if and only if the carrier of the triple system is the full, even-weight code on its support. In the case of equality the 2-rank is $n-1$ and D is the direct sum of $\boldsymbol{F}_2^r$ and the full even-weight subcode of $\boldsymbol{F}_2^{r+1}$.*

Proof: It is well-known, and in any case very easy to see, that a proper subsystem can have at most $\frac{n-1}{2} = r$ points and that, for such a maximal subsystem,[9] every triple not in the subsystem meets its point set in one point. Thus, when $|S'| = r$, the carrier contains all the vectors of weight two in its support and, since D is not the entire ambient space, must be the full even-weight code on $r+1$ points. Conversely, if the carrier is the full even-weight

[9] We remind the reader that the complement of the support of a maximal subsystem has the property that every triple meets it in exactly two points if it meets it at all. Since we have a design of even order the complement is, therefore, called an *oval*. For a more complete discussion of ovals in designs see either [1] or [5].

code on its support, then no triple of the system is contained in the support of the carrier and hence every triple of the system must meet the trivializing subsystem; this implies that the trivializing subsystem is maximal.□

Since the 2-rank of a Steiner triple system on n points with carrier C is n minus the codimension of C in its ambient space, in order to characterize the binary codes of those Steiner triple systems on n points with 2-rank $n-1$ we must still show that $|S'| < \frac{n-1}{2}$ implies that the carrier has codimension at least two in its ambient space. But this is a consequence of the following easy coding-theoretic characterization of the even-weight subcode of $\boldsymbol{F}_2^{r+1}$.

Lemma 2.3 *Let E be a binary $[r+1, r]$ code with minimum weight at least 2. Then E is the even-weight subcode of $\boldsymbol{F}_2^{r+1}$.*

Proof: [10] Consider $E^{\perp}$. It is of dimension one and if its non-zero vector were not the all-one vector $\boldsymbol{\jmath}$ there would be vectors of weight one in E. Hence $E = (\boldsymbol{F}_2\boldsymbol{\jmath})^{\perp}$ is the even-weight subcode of $\boldsymbol{F}_2^{r+1}$.□

We have now characterized the binary codes of those Steiner triple systems on n points of 2-rank $n-1$ and hence explained why Tonchev and Weishaar found only one such code for $n = 15$:

Theorem 2.4 *A Steiner triple system on n points has 2-rank $n-1$ if and only if its binary code is the direct sum of an even code and a full code $\boldsymbol{F}_2^r$. Moreover, it follows that $n = 2r+1$, that the support of the full code is the unique maximal subsystem of the given triple system, and that the even code is the code of* all *even-weight vectors supported on the corresponding oval of the system.*

We need only remark that the uniqueness of the maximal subsystem is a consequence of known results (see [9, 21]) but easily follows without recourse to those results. In fact, we have the following, more general result:

Proposition 2.5 *Let D be the binary code of a Steiner triple system of deficient 2-rank and suppose there is a subsystem $\mathcal{T}$ such that the projection of*

[10]The proof given here of Lemma 2.3 is due to John Dillon, who graciously read a very early version of the manuscript. It carries over without change to an arbitrary field and shows, in that case, that the code is *monomially equivalent* to the dual of the code generated by the all-one vector.

D onto the complement of the point set of $\mathcal{T}$ has minimum weight at least 2. Then the trivializing subsystem is contained in the point set of $\mathcal{T}$. In particular, the trivializing subsystem is contained in every maximal subsystem.

Proof: The proof is quite obvious since the projection must, clearly, be in the carrier and for a maximal subsystem the projection must always be the full even-weight subcode on the supporting oval. □

Actually, the trivializing subsystem is the intersection of all the maximal subsystems but we will not need that fact in the development; it will become apparent as we progress.

Writing the weight enumerator of a code of block length n as $\sum_{i=0}^{n} A_i X^i$, where A_i is the number of vectors of weight i in the code, we have immediately:

Corollary 2.6 *The weight enumerator of the binary code of a Steiner triple system on $n = 2r + 1$ points and 2-rank $n - 1$ is*

$$(1+X)^r \sum_{i \geq 0} \binom{r+1}{2i} X^{2i} = \frac{1}{2}(1+X)^r \left((1-X)^{r+1} + (1+X)^{r+1}\right).$$

3 The carrier

We have characterized the carrier in the codimension 1 case: it is the full even-weight code on its support. We wish now to investigate the carrier in the general case. We first of all determine the weight-two vectors in the carrier.

Proposition 3.1 *Let C be the carrier of a Steiner triple system on n points whose trivializing subsystem is a proper subsystem on r points. Then $n - r = 2l$ for some positive integer $l \geq \frac{r+1}{2}$ and the supports of the weight-two vectors of C form a resolvable*[11] *1-$(2l, 2, r)$ design. In particular C has rl vectors of weight 2.*

[11]That is, a resolution with r parallel classes of the given set of 2-subsets of the $2l$-set. Of course, if $2r+1 = n$, we are in the codimension 1 case and C is the even-weight subcode of $\boldsymbol{F}_2^{2l}$; the set of all 2-subsets of a $2l$-set is always resolvable — in fact in many ways for $l > 3$.

Proof: Clearly the weight-two vectors of C coming from the triples of the system meeting the trivializing subsystem in exactly one point yield a resolvable 1-design with parameters 1-$(2l, 2, r)$. We need only show that there are no further weight-two vectors in C. So suppose v were another weight-two vector in C. Then there would be a triple of the system whose support covered the support of v and was disjoint from the trivializing subsystem. Thus the sum of v and the incidence vector of the triple would yield a weight-one vector in C, a contradiction. □

Thus, knowing only the carrier allows one to know the order of the triple system from which it came: since r is intrinsic to the carrier, we know from the carrier alone that the system must have $2l + r$ points and be of order $l + \frac{r-3}{2}$. For any binary code C — of even block length $2l$ and of minimum weight 2 — if the weight-two vectors yield a resolvable 1-$(2l, 2, r)$ design, we shall call r the **index** of C. Thus a binary code of index r and block length $2l$ will have precisely rl vectors of weight two and the index r of such a code will clearly satisfy $1 \leq r \leq 2l - 1$. Note that when $r = 2l - 1$ we are in the codimension 1 case already treated. For such a C to be the carrier of the binary code of a Steiner triple system we must, in addition, have r congruent to 1 or 3 modulo 6. But the condition on the weight-two vectors of C is, alone, very strong as the next proposition will show.

Proposition 3.2 *Let C be a binary code of minimum-weight 2 and block length v. Assume that the weight-two vectors of C form a 1-$(v, 2, r)$ design. Then, $r + 1$ divides v and the weight-two vectors of C generate a subcode isomorphic to the direct sum of $\frac{v}{r+1}$ copies of the even-weight subcode of $\boldsymbol{F}_2^{r+1}$. If the 1-design is resolvable, then r must be odd and any resolution of the 1-$(v, 2, r)$ design is built from $\frac{v}{r+1}$ independently chosen resolutions of the design of weight-two vectors of $\boldsymbol{F}_2^{r+1}$.*

Proof: Since the weight-two vectors of C form a 1-$(v, 2, r)$ design, given any coordinate $\boldsymbol{e}$ of C there are precisely r weight-two vectors of C with a 1 at this coordinate. These r vectors generate an r-dimensional even subcode E of C whose support is the $r + 1$ coordinates supporting the given r vectors. Thus E is isomorphic to the full even-weight subcode of $\boldsymbol{F}_2^{r+1}$. It is easy to see that this process partitions the set of coordinates of the code C into subsets of cardinality $r + 1$ and gives all but the last assertion of the Proposition. So suppose r were even. Let $\mathcal{P}$ be a parallel class of some resolution of the design. Then $\mathcal{P}$ would have at least one of its 2-subsets supporting a vector with a 1 in the support of E and a 1 outside the support of E. But then we could produce a weight-two vector with a 1 at $\boldsymbol{e}$ and a 1 outside the support of E, an impossibility. It follows not only that r is odd, but also that any resolution of the design yields a resolution of the weight-two vectors of E. Clearly, any independently chosen resolutions of the supports of the weight-two vectors of the various even subcodes can be stitched together to give a resolution of the 1-design. $\square$

In particular, we have determined the binary code generated by the weight-two vectors of a carrier of index r. Moreover, all resolutions of the design given by the weight-two vectors of the carrier are obtained by piecing together, however one wishes, $\frac{2l}{r+1}$ arbitrarily chosen resolutions of the 2-subsets of an $(r+1)$-set. As the reader might imagine the number of such choices grows in a staggering way. Even when $2l = r+1$ and we are in the codimension 1 case already treated, the number of ways to choose just *one* resolution of the design of 2-subsets of a $2l$-set grows very quickly with l (see [8, 14]).

Remark: If the trivializing subsystem of a Steiner triple system on n points has r points, then, by the above Proposition, $r+1$ divides $n+1$. In fact, we will show that the quotient is a power of 2, a crucial result.

Suppose C, of block length $2l$ and index r, is the carrier of a Steiner triple system. Then the trivializing subsystem and the weight-two vectors of C account for $rl + \frac{r(r-1)}{6} = r\frac{r+6l-1}{6}$ triples of the triple system. All other triples, in number

$$\frac{l}{3}(2l - r - 1),$$

must have their incidence vectors in the carrier's support and hence yield weight-three vectors of the carrier (unless, of course, $n = 2r+1$ and hence $2l = r+1$ with C the full even-weight subcode of $\boldsymbol{F}_2^{2l}$). Moreover, any weight-two vector in the carrier's ambient space which is *not* in the carrier has its support contained in the support of a unique triple disjoint from the trivializing subsystem. Such a triple yields a weight-three vector of C and, in fact, other weight-three vectors in C which are not incidence vectors of the Steiner triple system at hand since any weight-two vector in C whose support meets the support of the triple non-trivially (in, therefore, precisely one point) gives another weight-three vector in C whose support is not a triple of the Steiner triple system. We have thus proved the following

Proposition 3.3 *Let C be the carrier of a Steiner triple system on n points whose trivializing subsystem is a proper subsystem with r points. Then setting $n-r=2l$ there are, among the weight-three vectors of C,*

$$\frac{l}{3}(2l-r-1)$$

vectors with the property that no two of these vectors have supports meeting in more than one point.

We remark that the proposition is operative only when $2l > r+1$.

Examples:

1) Observe that for $l=1$ (and hence $r=1$) the $[2,1]$ binary code C of minimum weight 2 is unique and looks like a carrier, but is not since the unique Steiner triple system on 3 points has 2-rank one and not two. Nevertheless we will denote this simple code by $\boldsymbol{C}_{1,1}$ below.

2) A slightly more interesting example occurs when $l=2$. Here there is a unique resolution of the set of 2-subsets of a 4-set and the binary even-weight subcode C of $\boldsymbol{F}_2^4$ is a putative carrier of index 3. One can indeed (as we shall see below in a more general context, Theorem 4.1) construct the unique Steiner triple system on 7 points from the data but C will not be the carrier. This code is denoted by $\boldsymbol{C}_{3,1}$ below.

Our final example of this section is more pungent; although it too is not a carrier, it will be a maquette for the carriers we will eventually characterize.

3) Consider the binary $[6,4]$ code $C=\boldsymbol{C}_{1,2}$ with generator matrix

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

corresponding to the case $l=3$ and $r=1$. Its weight enumerator is, visibly,

$$X^0 + 3X^2 + 8X^3 + 3X^4 + X^6$$

and its weight-two vectors yield a resolvable 1-$(6,2,1)$ design; thus C has index 1. But, again, it is not the carrier of a Steiner triple system since that system would have to be the Fano plane, which has 2-rank four and not five. One *can* construct the Fano plane from the code C simply by choosing any four ($4 = \frac{l}{3}(2l - r - 1)$) of the eight weight-three vectors satisfying the criterion of the Proposition. That choice is essentially unique, as the reader can easily verify. For example, a normalized choice is the following:

$$\begin{array}{cccccc} 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{array}$$

and the gross number of choices is two.

The automorphism group of C is clearly the semi-direct product of Sym(3) acting in the obvious way on the elementary abelian group of order 8 (viewed as the direct product of three copies of the cyclic group of order 2). As we shall later see, we should think of the cyclic group as Sym(2) and the Sym(3) here should be thought of as the group of the projective line over $\boldsymbol{F}_2$, that is as $PGL_2(\boldsymbol{F}_2)$. For $l = 3$ no other value for the index is possible since any resolvable 1-$(6, 2, r)$ design with $r > 1$ generates the full even-weight subcode of $\boldsymbol{F}_2^6$ and 5 is not congruent to 1 or 3 modulo 6.)

We now use Proposition 3.2 and the condition of Proposition 3.3 to completely describe all possible carriers.

Theorem 3.4 *Suppose C is the carrier of a Steiner triple system. Then C is a code of block length $2l$, minimum weight 2, and index r for some $r \equiv 1, 3 \pmod 6$. Moreover,*

$$\frac{2l}{r+1} = 2^m - 1$$

for some positive integer m, C is uniquely determined by r and m, and a Steiner system with C as its carrier must have $\frac{n+1}{r+1} = 2^m$ and its 2-rank must be

$$n - m = n - \log_2\left(\frac{n+1}{r+1}\right).$$

Proof: We already know that $r + 1$ divides $2l$; if $2l = r + 1$ we are in the codimension 1 case and C is the full even-weight subcode of $\boldsymbol{F}_2^{2l}$. Here $m = 1$. Assume, therefore, that $r + 1 < 2l$. Setting $\frac{2l}{r+1} = s$ we have that the subcode of C generated by the weight-two vectors is isomorphic to the direct sum of s copies of the even-weight subcode of $\boldsymbol{F}_2^{r+1}$ and that the s supports partition the coordinates of C. Let the set of these s supports be $\mathcal{S}$. Since $r+1 < 2l$ we must have weight-three vectors in C. Suppose v is such a weight-three vector. Then it cannot have two 1s in any given $S \in \mathcal{S}$ and hence defines a triple of the set $\mathcal{S}$. If $\{R, S, T\} \subseteq \mathcal{S}$ is such a triple, then every vector with one 1 in each of R, S and T is a weight-three vector in C. In particular, each such triple of $\mathcal{S}$ yields $(r+1)^3$ weight-three vectors of C. If $\{R, S, T\}$ and $\{R, S, T'\}$ are two such triples then $T = T'$ for, otherwise, we could produce a weight-two vector in C with one 1 in T and another in T', an impossibility. It follows from Proposition 3.3 that we have defined a Steiner triple system on $\mathcal{S}$. We next show that this triple system must be a classical triple system coming from the design of points and lines of some $\mathrm{PG}_{m-1}(\boldsymbol{F}_2)$ and thus produce the m of the Theorem. Suppose the triple system just defined on $\mathcal{S}$ is *not* such a classical system. Then some linear combination of the triples produces a vector of weight one. Ordering each of the subsets in $\mathcal{S}$ and mimicking that linear combination with weight-three vectors of C adjusted, say, flushright, we would produce a vector of weight one in C — which yields the desired contradiction.

Now, since such a classical triple system is uniquely determined by m and since C is generated by its weight-two and weight-three vectors, we see that r and m uniquely determine C. Determining the dimension of C and hence the 2-rank of any triple system with C as carrier is easy: the classical triple system has 2-rank $2^m - 1 - m$ and since there are $2^m - 1$ even subcodes, each of dimension r, to take into account the dimension of C is $r(2^m-1) + 2^m - 1 - m$ and the 2-rank of the triple system with C as carrier is $\dim(C) + r = (r+1)2^m - (m+1)$ and, since $2l + r = n$, we are done. □

The carrier determined by r and m will henceforth be denoted by

$$\boldsymbol{C}_{r,m}$$

and its properties described explicitly in the Theorem below.

Corollary 3.5 *If a Steiner triple system has a trivializing subsystem on r points, then the Steiner system is on $n = (r+1)2^m - 1$ points for some positive integer m.*

The proof just given yields more than the Theorem. It allows us to display every possible carrier and determine its automorphism group:

Theorem 3.6 *If C is a carrier of a Steiner triple system, then $C^\perp$ is isomorphic to the code one obtains from the dual of the Hamming code on 2^m-1 points by repeating it $r+1$ times. We denote this carrier C by $\boldsymbol{C}_{r,m}$. It is of block length $(r+1)s$ where $r \equiv 1, 3 \pmod 6$ and $s = (2^m-1)$ and enjoys the following properties:*

- *The $(r+1)s$ coordinates of $\boldsymbol{C}_{r,m}$ are split into s sets each of cardinality $r+1$*
- *On the s sets is imposed a classical Steiner triple system*
- *A vector of weight 2 is in $\boldsymbol{C}_{r,m}$ if and only if its support is contained in one of the s sets*
- *A vector of weight 3 is in $\boldsymbol{C}_{r,m}$ if and only if its support is such that no two elements are in one of the s sets and the three sets that do have a non-empty intersection with its support form a triple of the imposed classical Steiner triple system*
- *$\boldsymbol{C}_{r,m}$ is generated by its vectors of weight 2 and 3.*

Corollary 3.7 *The automorphism group of $\boldsymbol{C}_{r,m}$ is the semi-direct product of $PGL_m(\boldsymbol{F}_2)$ and the direct product of 2^m-1 copies of $\mathrm{Sym}(r+1)$ where the projective group acts on the direct product in the obvious way.*

Corollary 3.8 *A carrier $\boldsymbol{C}_{r,m}$ has*

$$r(\frac{r+1}{2})(2^m-1)$$

vectors of weight 2 and

$$(r+1)^3\frac{(2^m-1)(2^{m-1}-1)}{3}$$

vectors of weight 3.[12]

[12]It is, of course, easy to give the weight enumerator of each $\boldsymbol{C}_{r,m}$ and we will soon do so — thus determining the weight enumerator of all binary codes of Steiner triple systems of deficient 2-rank. We have given the number of vectors of weight 2 and 3 in the Corollary simply to emphasize those aspects of the carrier that are important in the construction of all Steiner triple systems of deficient 2-rank.

We have taken the liberty in the statement of the Theorem to include the binary code $\{0\}$ as an honorary Hamming code of block length one.[13] It corresponds to the case $m = 1$ where we have, of course, simply the even-weight subcode of $\boldsymbol{F}_2^{r+1}$. Letting $\boldsymbol{\jmath}$ be the all-one vector of length $r+1$, observe that the dual of the code $\boldsymbol{F}_2\,\boldsymbol{\jmath}$, which is the dual of the Hamming code of block length one repeated $r+1$ times, is precisely this even code. A resolution of the 1-$(r+1, 2, r)$ design given by its weight-two vectors can, in general, be had in many ways: for $r = 1$ or $r = 3$ just one, but for $r = 7$ six and in 396 ways for $r = 9$ — and then the combinatorial explosion arrives [8].

A resolution of the 1-design given by $\boldsymbol{C}_{r,m}$ when $m > 1$ can be formed by stitching together resolutions, chosen independently, for each of the $2^m - 1$ even subcodes. To choose a collection of weight-three vectors of $\boldsymbol{C}_{r,m}$ satisfying the hypothesis of Proposition 3.3 one must and can choose $(r+1)^2$ vectors, no two with two common 1s, for each of the triples, again independently, of the imposed triple system and that is very easy. We describe all possible choices next:

We think of the choice as an $(r+1) \times 3$ array of square matrices of size $r+1$. The pigeon-hole principle forces one to have $r+1$ 1s in each column of the array. Thus we can assume that in the first of the three columns of matrices we have arranged matters so that the first matrix has 1s in its first column with 0s elsewhere, the second has 1s in its second column with 0s elsewhere, etc. Then we may assume that the second column of matrices is just the identity matrix repeated $r+1$ times. Finally, the third column consists of $r+1$ permutation matrices, $P_1, P_2, \ldots, P_{r+1}$ where $P_i P_j^{-1}$ has no fixed points for distinct i and j. For example, we could take $P_i = Z^{i-1}$, $1 \leq i \leq r+1$, where Z is the cyclic shift. This choice was that given in the Example displaying the code $\boldsymbol{C}_{1,2}$, where there is only one choice up to equivalence.

From the description of $\boldsymbol{C}_{r,m}$ in terms of the dual to the Hamming code of block length $s = 2^m - 1$ one uses the MacWilliams transform to compute

[13] In fact, it deserves the name: it is a single-error correcting code of block length one with every vector in the ambient space at distance 1 or less from a unique vector in the code.

easily its weight enumerator:

$$\frac{1}{s+1}\left((1+X)^{s(r+1)}+s(1-X^2)^{\frac{(r+1)(s-1)}{2}}(1-X)^{r+1}\right).$$

Corollary 3.9 *If D is the binary code of a Steiner triple system on n points of 2-rank $n-m$ with a trivializing subsystem on r points, its weight enumerator is*

$$\frac{1}{2^m}\left((1+X)^{n-r}+(2^m-1)(1-X^2)^{\frac{n-2r-1}{2}}(1-X)^{r+1}\right)(1+X)^r.$$

Proof: We have that $n=(r+1)2^m-1$ with $s=2^m-1$ and that the binary code of the triple system is the direct sum of $\boldsymbol{C}_{r,m}$ and $\boldsymbol{F}_2^r$.$\Box$

4 Constructing systems from a carrier

We begin by pointing out how to construct a Steiner triple system from a putative carrier satifying the criterion of Proposition 3.3. It follows that each of the codes $\boldsymbol{C}_{r,m}$ will define triple systems (which may possibly have larger carriers) and that the number of systems $\boldsymbol{C}_{r,m}$ constructs grows very fast as r and m do.

Theorem 4.1 *Suppose C is a binary code of block length $2l$, minimum weight 2 and index r where $r\equiv 1,3 \pmod 6$. Suppose also that C contains a collection of $\frac{l}{3}(2l-r-1)$ weight-three vectors with the property that no two have supports intersecting in more than one point. Then, given the following data,*

- *A Steiner triple system on r points*
- *A resolution of the supports of the weight-two vectors of C into r parallel classes*
- *A bijection of the parallel classes of the above given resolution with the points of the above given triple system*
- *A collection, possibly empty, of $\frac{l}{3}(2l-r-1)$ weight-three vectors of C with the property that no two have supports intersecting in more than one point,*

there is a Steiner triple system on $2l + r$ points containing the given system on r points as a subsystem. Moreover, if the Steiner triple system given in the data is of 2-rank r, then the carrier of the constructed system is $\boldsymbol{C}_{r,m}$, where $2l = (r+1)(2^m - 1)$, and the trivializing subsystem is that Steiner triple system; if the system on r points is of deficient 2-rank, then the carrier may be larger and that will depend on the choice of the other data.

Proof: Let S' be the set of cardinality r on which the Steiner triple system of the data is given and T the set of coordinate places of the code C. We assume, of course, that S' and T are disjoint; we construct the sought for triple system on the set $S = S' \cup T$. Here are the triples on S:

- The given triples on S'
- For each $x \in S'$ corresponding, under the given bijection, to the parallel class $\mathcal{P}$ of the given resolution the triples of the form $\{x\} \cup P$ where $P \in \mathcal{P}$
- The triples from the supports of the selected weight-three vectors of C

It is easy to see that no two of the 3-subsets we have described meet in more than one point. Moreover, the number of these 3-subsets of S is

$$rl + \frac{r(r-1)}{6} + \frac{l}{3}(2l - r - 1) = \frac{(2l+r)(2l+r-1)}{6}$$

and we have a Steiner triple system on S. Let D be the binary code of the constructed triple system. If the given triple system on S' has 2-rank r it is clear that it must be the trivializing subsystem since the projection of D onto T is contained in C and generated by the weight-two and chosen weight-three vectors of C. If the given triple system on S' has 2-rank less than r it may or may not be the trivializing subsystem but, because the projection is contained in C, it will contain the trivializing subsystem by Proposition 2.5.$\square$

Remarks:

1) If the code C is the full even-weight subcode of $\boldsymbol{F}_2^{2l}$ of maximal index $2l - 1$ with l not divisible by 3, then the construction proceeds without recourse to any weight-three vectors of C (and, in fact, there aren't any). All one needs is a resolution of the set of 2-subsets of a $2l$-set and a Steiner triple system on $2l-1$ points. There are always resolutions and always triple systems (because of our restriction on l). This case of the construction goes back at least as far as Reiss [17] and is very well-known; all Steiner triple systems with a maximal subsystem are clearly so constructible, the carrier, of course, is merely $\boldsymbol{C}_{r,1}$ and the maximal subsytem is on r points.

2) It is instructive to take a minimalist approach to this construction and decide what transpires when one begins with the degenerate triple system on one point and does not even assume that the carriers or Hamming codes are known, but "discovers" both in the construction process. The degenerate triple system, yields the binary code $\{0\} \subseteq \boldsymbol{F}_2$ which is the honorary Hamming code of block length 1 which yields the carriers $\boldsymbol{C}_{r,1}$.

At this point we have but one triple system at our disposable and can only use $\boldsymbol{C}_{1,1}$; turning the crank yields the unique triple system on 3 points, giving the Hamming code of block length $3 = 2^2 - 1$ and hence the carriers $\boldsymbol{C}_{r,2}$.

Now we have two triple systems at our disposal and we can use the one on 3 points together with the carrier $\boldsymbol{C}_{3,1}$ which yields only the Fano plane, the unique triple system on 7 points; the Fano plane also arises from the degenerate system and $\boldsymbol{C}_{1,2}$. Using the system on three points together with $\boldsymbol{C}_{3,2}$ yields all the systems on 15 points of 2-ranks 11, 12 and 13. We therefore get the carriers $\boldsymbol{C}_{r,3}$ and $\boldsymbol{C}_{r,4}$.

The next turn of the crank yields, among other systems, the 23 triple systems on 15 points with 2-rank less than 15, more carriers and so on. All possible 2-ranks appear because one can fiddle with the data to make sure that the triple system one uses becomes the trivializing subsystem.[14] The reader may want to show that, restricting the triple systems to only those constructed at a given stage, only triple systems on $n = 2^k - 1$ points can be constructed and all will have deficient 2-rank between $n-k$ and $n-1$. It also follows from Theorem 6.1 that only derived triple systems will arise. Although all 23 triple systems on 15 points with deficient 2-rank will appear, that will cease to be true for the systems on 31 points since we have restricted ourselves only to triple system the construction process produces. Thus we will miss those on 31 points coming from the 57 systems on 15 points with

[14] This sort of fiddling has been used by Key and Sullivan [10] and by Phelps [16, Page 107] to alter one system to get another — but not in the systematic context we are describing.

2-rank 15.

3) A slightly less minimalist approach might admit, say, the classical triple systems coming from affine geometries over $\boldsymbol{F}_3$ — all of which have full 2-rank — besides those constructed during the process. One would then get the Steiner triple systems on 19 points of 2-rank 18, among others. Once again, Theorem 6.1 shows that only derived Steiner triple systems will arise.

4) One could even envision admitting *all* Steiner triple systems of full 2-rank that are derived (thus, for example, admitting the two on 13 points, the 57 on 15 points not produced by the minimalist approach, and those produced by Theorem 7.2). Once again only derived systems result and, for example, one obtains the Steiner triple systems on 27 points of 2-rank 26 and all the triple systems on 31 points of deficient 2-rank.

5) Using the carrier $C = \boldsymbol{C}_{9,1}$ there is only one choice for the Steiner triple system: the affine plane of order 3 of full 2-rank. In this case one always gets C as the carrier and the affine plane of order 3 as the trivializing subsytem. Here there are 396 distinct resolutions (up to equivalence under Sym(10)) and simply using the group of the affine plane cuts the possible number of Steiner triple systems on 19 points with 2-rank 18 to at most 332,640. Moreover, the data allow one to compute the exact number and this has been done by Seah and Stinson [20]: there are 284,457. In this case of Steiner triple systems of order 8 (on 19 points) the 2-rank is either 18 or 19 (from Theorem 3.4) and Brendan McKay estimates that the number of Steiner triple systems is 11 or 12 billion. Thus, the vast majority have full 2-rank. The combinatorial explosion of the number of resolutions of a $2l$-set comes at $l = 6$. The precise number has been computed by Dinitz, Garnick and McKay (see [8]); there are 526,915,620 up to equivalence under Sym(12). It seems unlikely that anything but asymptotic results will be available beyond 19 for the codimension 1 case.

6) Using the carrier $\boldsymbol{C}_{9,2}$ of block length 30 with, again, the affine plane of order 3 being the only choice for the trivializing subsystem, we must choose on each of the three 10-sets a resolution of the set of 2-subsets. There will be a choice of 396 possible resolutions for each of the set of 2-subsets of the three 10-sets — and therefore a gross number of choices of $(396)^3$. The splicing will introduce a factor of $(9!)^2$ with the bijection boosting that factor to $(9!)^3$. There is still the choice of the weight-three vectors which will introduce a another large factor, namely the number of ways to choose nine (since we may assume the first is the identity permutation) fixed-point free permutations from Sym(10) such that the product of any one with the inverse of any other is again fixed-point free. But, since all the automorphism data is available, the calculation might conceivably be within reach and certainly estimates, such as those given by Ferch and Stinson in [19], could be made. If so, the number of Steiner triple systems on 39 points of 2-rank 37 would be determined or estimated — that is Steiner triple systems on 39 points with a trivializing subsystem on 9 points.

7) Observe that not only can one estimate the number of systems one gets by the construction (knowing, of course, that every triple system with the given 2-rank will be constructed) but, in principle, one can determine the automorphism group of the constructed system from the automorphism group of the trivializing subsystem and the subgroup of the known automorphism group of the carrier leaving the data invariant. Although it is known that most Steiner triple systems have a trivial automorphism group, that doesn't prohibit there being automorphisms here since we are *not* able to construct systems of full 2-rank — which dominate at every stage.

8) It is possible to generalize this construction somewhat so as to be able to produce *some* Steiner triple systems of full 2-rank. To do so one partially disregards the coding theory and imposes the triples of *any* triple system on the various $(r+1)$-sets. The matter is more easily explained in terms of Steiner quadruple systems and we do that in Section 7.

We summarize what we have proved in an existence and uniqueness theorem which captures, by Theorem 4.1 and Corollary 3.5, all Steiner triple systems of deficient 2-rank. In particular, for $n > 7$ and $m > 0$ a Steiner triple system on n points of 2-rank $n-m$ has a binary code isomorphic to

$$\boldsymbol{C}_{r,m} \oplus \boldsymbol{F}_2^r$$

and, of course, those of full 2-rank have simply $\boldsymbol{F}_2^n$ as their binary code.

Theorem 4.2 *Let $n > 7$ be congruent to 3 or 7 modulo 12 and set $n+1 = u \times 2^k$ with u odd. Then, for any choice of i with $1 \leq i < k$ there is a Steiner triple system on n points of 2-rank $n-k+i$. Any such Steiner triple system has a binary code isomorphic to*

$$\boldsymbol{C}_{u2^i-1,k-i} \oplus \boldsymbol{F}_2^{u2^i-1}$$

and all such Steiner triple systems can be constructed from $\boldsymbol{C}_{u2^i-1,k-i}$ and Steiner triple systems on $u2^i-1$ points.

Remarks:

1) When $u = 1$ one also has, of course, the Hamming code of block length $2^k - 1$ and 2-rank $n - k$, which is the binary code of the classical Steiner triple system of points and lines of $PG_{k-1}(\boldsymbol{F}_2)$. We have already seen how to construct, starting with merely the degenerate Steiner triple system, all the Hamming codes and examples of the codes of the Theorem when $u = 1$. This bootstrap exercise is reminiscent of the construction of the integers from the empty set.

2) Observe that when we add an overall parity check to the code $\boldsymbol{C}_{r,m} \oplus \boldsymbol{F}_2^r$ we get a certain smoothing and, in particular, we will have 2^m copies of the even-weight subcode of $\boldsymbol{F}_2^{r+1}$ underlying this extended code. As we will see when we discuss Steiner quadruple systems we will have an overarching affine geometry over $\boldsymbol{F}_2$ involved and the first-order Reed-Muller code will take the place of the dual of the Hamming code.

5 Carriers of index one and three

When the carrier is either $\boldsymbol{C}_{1,m}$ or $\boldsymbol{C}_{3,m}$ there is only one choice available for each of the first three data items described in Theorem 4.1: Clearly, the choice of Steiner triple system is the degenerate triple system in one case and the 3-point system in the other. For $\boldsymbol{C}_{1,m}$ it is obvious that there is but one resolution and one bijection. But, that is also true for $\boldsymbol{C}_{3,m}$ since the only resolution of the set of 2-subsets of $\{1, 2, 3, 4\}$ is $\{\{12, 34\}, \{13, 24\}, \{14, 23\}\}$ on which $\mathrm{Sym}(4)$ acts triply-transitively. Hence, the $2^m - 1$ symmetric groups on $r+1 = 4$ elements can be used to "straighten" all the seams one has in piecing together the unique resolutions of the 4-sets and $\mathrm{Sym}(3)$, the automorphism group of the Steiner triple system on 3 points, can be used to "straighten" the bijection with the three points of the triple system. Thus the Steiner triple system one gets in these two cases rests entirely with the choice of the weight-three vectors one chooses. In each of these cases the triple system produced will be on $2^{m+1} - 1$ points and one can certainly choose triples so as to produce the Hamming code; in fact, the Hamming code will clearly be contained in any code one produces via Theorem 4.1. The only question is whether or not, by properly choosing the weight-three vectors, we can get others. The binary codes of the Steiner triple systems obtained will either be the Hamming code $\boldsymbol{H}$ of block length $2^{m+1} - 1$, the code $\boldsymbol{H} \oplus \boldsymbol{F}_2\boldsymbol{e}$ where $\boldsymbol{e}$ is a weight-one vector, or $\boldsymbol{H}+\boldsymbol{F}_2\boldsymbol{e}+\boldsymbol{F}_2\boldsymbol{f}+\boldsymbol{F}_2\boldsymbol{g} = \boldsymbol{H}\oplus\boldsymbol{F}_2\boldsymbol{e}\oplus\boldsymbol{F}_2\boldsymbol{f}$ where $\boldsymbol{e}$, $\boldsymbol{f}$ and $\boldsymbol{g}$ are three weight-one vectors whose supports form a weight-three vector of the Hamming code. In fact, this has already been thoroughly investigated by Key and Sullivan [10] and, indeed, the data can be so chosen. We formalize the discussion above in the following two propositions.

Proposition 5.1 *If a Steiner triple system has a one-point trivializing subsystem, then it is on $2^{m+1}-1$ points for some $m>2$ and its binary code is obtained from the corresponding Hamming code by simply adjoining a vector of weight one.*

Proposition 5.2 *If a Steiner triple system has a three-point trivializing subsystem then it is on $2^{m+1}-1$ points for some $m>2$ and its binary code is obtained from the corresponding Hamming code by simply adjoining two weight-one vectors.*

It should not be a difficult matter to determine all the Steiner triple systems that arise in these two cases; we have not tried to do so. A more interesting case arises when one takes the Fano plane as the trivializing subsystem; here one employs the carrier $\boldsymbol{C}_{7,m}$ and there will be a choice available both for the resolution of the set of 2-subsets of the 8-set, for the seams and for the bijection. A computer study seems appropriate; all the Steiner triple systems on 31 points of 2-rank 27, 28 and 29 could, perhaps, be enumerated.

Clearly one expects the number of triple systems to increase markedly with i as this parameter increases from 1 to $k-1$ in Theorem 4.2. We have here a nice example of how lowering the rank constrains the systems being discussed. Even for triple systems on 19 points one has billions of systems of 2-rank 19 but only hundreds of thousands with 2-rank 18. (The Tonchev-Weishaar study recorded one system of rank 12, five of rank 13, and sixteen of rank 14.)

6 Applications

In November of 1852 when Steiner originally asked for those n for which there was a Steiner triple system and for the number of such systems for each such n, he also asked [15] whether or not such systems extended to Steiner quadruple

[15]Question (b) of the infinite list of questions he posed: [18].

systems, that is he asked, for any given Steiner triple system, whether or not it was possible to introduce a collection of 4-subsets of the underlying set with the property that no one of these 4-subsets contained a triple but every 3-subset not a triple was in a unique member of the introduced 4-subsets.

Now we would express Steiner's question as follows: "Does every Steiner triple system on n points extend to a Steiner quadruple system on $n+1$ points?" or "Is every Steiner triple system derived?" since one gets such a system from a Steiner quadruple system by suppressing a point and using only the quadruples through that point. All classical systems are derived and, in general, in many ways so; in particular, the unique systems on 3, 7 and 9 points are derived. Both triple systems on 13 points are derived as are all 80 triple systems on 15 points; these results were computer generated. It is widely believed that all Steiner triple systems are derived and an enormous effort has gone into proving this result; for a survey of what is known about derived systems see [16].

We make a contribution to the subject by reducing the question to those Steiner triple systems with full 2-rank. But, more importantly, the proof is very robust and sheds a lot of light on the question; the proof explicitly displays the quadruple systems that are the extension and thus also clearly shows why an enormous number of extensions arise. Here is what we prove:

Theorem 6.1 *Any Steiner triple system whose trivializing subsystem is derived is itself derived.*

Proof: We assume the carrier of the system is $\boldsymbol{C}_{r,m}$ and view the point set of the system as $s = 2^m - 1$ disjoint $(r+1)$-sets and a disjoint r set in the obvious way. We must define 4-subsets covering each triangle (i.e. a 3-subset which is not itself a triple of the system) exactly once with none of the introduced 4-subsets containing a triple. On the r-set we use those 4-subsets that define one of the trivializing subsystem's extensions since the r-subset is the support of the trivializing subsystem — which we are assuming is derived. Similarly, we use (independently as always in this work) Steiner quadruple systems on $r+1$ points on each of the $(r+1)$-sets; these quadruple systems need have no relation to the trivializing subsystem. These choices are rather obvious ones; the first introduces

$$\frac{1}{24}r(r-1)(r-3)$$

4-subsets and the second

$$\frac{s}{24}(r+1)r(r-1).$$

We next itemize some not quite so obvious choices:

- For each point p of the r-set, each choice of two, R and S say, of the $(r+1)$-sets, and each choice of $P_R \subseteq R$ and $P_S \subseteq S$ say, where P_R and P_S are in the parallel class defined by p, we use the 4-subset $P_R \cup P_S$. This introduces
$$r\binom{s}{2}(\frac{r+1}{2})^2$$
4-subsets.

- For each triple t of the trivializing subsystem on the r-set, each $p \in t$, and each of the 2-subsets, P say, in the parallel class defined by p we use the 4-subset $P \cup t'$, where t' is the triple t with p removed. This introduces
$$\frac{1}{2}r(r-1)s(\frac{r+1}{2})$$
4-subsets.

- For each triple $\{R, S, T\}$ of the classical system on the $(r+1)$-sets, each point p of the trivializing subsystem, and every triple $\{x, y, z\}$ of the constructed triple system, with $x \in R, y \in S$ and $z \in T$, we use the three 4-subsets $\{x', y, z, p\}, \{x, y', z, p\}$ and $\{x, y, z', p\}$ where $\{x, x'\}, \{y, y'\}$ and $\{z, z'\}$ are in the parallel class defined by p. This introduces
$$\frac{1}{2}s(s-1)r(r+1)^2$$
4-subsets.

And finally we employ the classical system on the $(r+1)$-sets to introduce 4-subsets with the property that they have one point in each of four $(r+1)$-sets. We pick, of course, four $(r+1)$-sets corresponding to some extension of the classical system. Any extension of the classical system will do, but, as we shall see later, one gets a "nicer" quadruple system if one chooses the natural extension arising from the points and 2-flats of $AG_m(\boldsymbol{F}_2)$. If $\{R, S, T, U\}$ is such a 4-subset we will need to pick $(r+1)^3$ 4-subsets of the form $\{x, y, z, w\}$ with $x \in R, y \in S, z \in T$ and $w \in U$ with no two meeting in more than two points to insure that each of the $4 \times (r+1)^3$ of those 3-subsets of the underlying point set that are contained in $R \cup S \cup T \cup U$ — but with no two points in an individual one of the $(r+1)$-sets — is covered exactly once. One again can normalize the choice much as was done in picking the triples in the construction given in Section 4. So, for example, the first column would be $(r+1)^2$ 1s followed by 0s, the second $(r+1)^2$ 0s followed by $(r+1)^2$ 1s followed by 0s, etc. through the $(r+1)$-st column. Then, for the next three columns against the 1s in column one we would put the same array as we did for the triples; for the 1s in column two we can repeat with, say, a cyclic shift on the last $r+1$ columns consisting of the fixed-point free permutation matrices. Here is an illustration for the case we have already treated with $r = 1$:

$$\begin{array}{cccccccc}
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1
\end{array}$$

This introduces

$$\frac{1}{24} s(s-1)(s-3)(r+1)^3$$

4-subsets.

Since the triples of the constructed triple system either lie completely in the r-set, have one point in the r-set and two points in some $(r+1)$-set, or three points distributed over three $(r+1)$-sets defining a triple of the classical system on the collection of $(r+1)$-sets, one sees easily that no one of the 4-subsets introduced contains a triple of the constructed Steiner triple system.

Seeing that no two of the chosen 4-subsets meet in more than two points is not difficult. One can then sum and find the right number of 4-subsets, namely

$$\frac{1}{24}[s(r+1)+r][s(r+1)+r-1][s(r+1)+r-3]$$

— or what may be more instructive and is, moreover, fun, actually see how each triangle is covered. For example, if a triangle has two points in one $(r+1)$-set and one in the r-set one uses the doubleton to define a point p in the r-set (which must be different from the point we were given) and uses these two points of the r-set to get a triple t of the trivializing subsystem and then employs the second of the itemized prescriptions above. This completes the proof. $\square$

Corollary 6.2 *If all Steiner triple systems on n points and 2-rank n are derived, then all Steiner triple systems are derived.*

Proof: The proof is quite obvious and proceeds via induction on the order of the triple system. $\square$

The Theorem is more robust than it first appears. For example it shows that all Steiner triple systems on 31 points with 2-rank less than 31 are derived since we know those of smaller order are. Even without one line of computation the Theorem shows that all Steiner triple systems on 19 points of 2-rank 18 are derived — but this was already known. As far as I know it had not, however, been observed that all Steiner triple systems on 39 points of 2-rank 37 are derived, an immediate consequence of the Theorem since the trivializing subsystem must be the affine plane over $\boldsymbol{F}_3$ — although this could have been seen via existing methods. In fact, the Theorem itself could have been proved with existing methods since Kevin Phelps [15] had shown that any system with a maximal derived subsystem was itself derived, and combining this with Teirlinck's notion of projective dimension [21] gives the result. But the direct proof above is simple and exhibits explicitly an enormous number of the extensions.

There is another point to be made about the proof: except for the arbitrarily chosen quadruple systems on the $(r+1)$-sets and the 4-subsets given to us on the r-set by our hypothesis, one sees easily that all the 4-subsets chosen are contained in the linear span of the constructed Steiner triple system. This is because we have chosen the design of points and 2-flats of an affine geometry to extend the classical Steiner triple system on the $(r+1)$-sets. But for this extraneous data the same thing is true since on each of the $(r+1)$-sets we see the full even-weight subcode and on the r-set the full code. Thus we have the following

Corollary 6.3 *If the trivializing subsystem of a Steiner triple system is derived, then not only is the Steiner system derived, but the extension can be so chosen that the binary code of the resulting quadruple system is simply that of the Steiner system with an overall parity check added and its code is given by* 2^m *full even-weight subcodes of* $\boldsymbol{F}_2^{r+1}$ *with the planes of the affine geometry* $AG_m(\boldsymbol{F}_2)$ *imposed as those weight-four vectors with one* 1 *in each of four of these even subcodes.*

Both the Theorem and this Corollary were proved by Key and Sullivan in the cases $r = 1$ and $r = 3$; these cases correspond to the degenerate triple system and the one on three points, both of which are derived.[16]

And the proof isn't through yielding information: it can be read as a construction vehicle for Steiner quadruple systems; as such it gives the following

Corollary 6.4 *Given any* 2^m *Steiner quadruple systems on* $r + 1$ *points, where* m *is a positive integer, there is a Steiner quadruple system on* $2^m(r+1)$ *points containing each of the given systems as subsystems, one on each of* 2^m *disjoint subsets of the constructed system. Moreover, the Steiner quadruple system can be chosen so that its* 2*-rank is* $2^m(r + 1) - m - 1$.

Such a construction in the case $m = 1$ has been known for a long time and was used by Lindner and Rosa [11] to construct 31,021 Steiner quadruple systems on 16 points. It should be clear to the reader why so many systems arose. In this case the construction is, as our discussion clearly shows, essentially Reiss's "doubling" construction, but that does not seem to have been explicitly acknowledged in the literature [12, Construction A*].

Since the binary code of a Steiner quadruple system is an even code, the maximal 2-rank for a Steiner quadruple system on v points is $v-1$ and if it is $v-1$ its binary code is the full even-weight subcode of $\boldsymbol{F}_2^v$. The construction we have just given constructs *all* Steiner quadruple systems of deficient 2-rank.[17] It would have been easier to classify Steiner quadruple systems of deficient 2-rank first, but then we would have missed those Steiner triple systems, if any, that are not derived. The carrier is constructed by taking the first-order Reed-Muller code, repeating it $r+1$ times, and then dualizing as we shall soon see.

[16] The degenerate quadruple system has two points and no blocks.

[17] I.e. 2-rank strictly less than $v - 1$.

Since the classification presented above should reduce a question about Steiner triple systems to the same question about those of full 2-rank — as we did above for Steiner's question (b) — Kevin Phelps's question of whether or not every Steiner triple system on $2^k - 1$ points can be seen as the set of weight-three vectors of a perfect binary code containing the zero vector (see [2]) ought to be so reduced. In this case all such Steiner systems of deficient 2-rank are built from Steiner systems on $2^i - 1$ points for some $i < k$ and an inductive proof should work. I have not tried to find such a proof.

7 Steiner quadruple systems

We already discused Steiner quadruple systems in Section 6 but we here want to indicate how easy it is to begin, ab initio, and classify those of deficient 2-rank. As a byproduct we describe a construction that produces many Steiner quadruple systems of full 2-rank and hence many Steiner triple systems of full 2-rank which are derived.

Given a Steiner quadruple system on $n + 1$ points [18] the binary code generated by the incidence vectors of the blocks is contained in the full even-weight subcode of $\boldsymbol{F}_2^{n+1}$ and full 2-rank means simply that the code of the quadruple system *is* the full even-weight subcode and hence of 2-rank n. If the 2-rank is strictly less than n then either the minimum weight of the code is 4 — in which case $n + 1 = 2^m$ and the Steiner quadruple system is the the design of points and 2-flats of $AG_m(\boldsymbol{F}_2)$ in direct analogy to the triple system case — or else there must exist vectors of weight two in the code. If v is such a vector, then using the quadruples of the system whose support contains the support of v produces a parallel class of 2-subsets that are the supports of the weight-two vectors one obtains. One sees easily from this that the weight-two vectors of the code form a resolvable 1-design. If the index of the code generated by the weight-two vectors is n we are in the presence of a Steiner quadruple system of full 2-rank. When the quadruple system is of deficient 2-rank we apply Proposition 3.2 and we find that the code generated by the weight-two vectors is simply the direct sum of codes isomorphic to the full even-weight subcode of $\boldsymbol{F}_2^{r+1}$ where r is the index and

[18] I.e., a 3-$(n + 1, 4, 1)$ design, frequently described as an $S(3, 4, n + 1)$ in the literature.

$r+1$ divides $n+1$. Set

$$s+1=\frac{n+1}{r+1}.$$

The quadruple system imposes a resolution on the 1-$(n+1,2,r)$ design given by the weight-two vectors of the code. Many of the vectors of weight four with support the union of two weight-two vectors in the same parallel class of this imposed resolution are the support of a quadruple of the system. All other quadruples of the system have their four 1s distributed among four of the $s+1$ sets of cardinality $r+1$ given by Proposition 3.2. This imposes a Steiner quadruple system on these $s+1$ sets and just as in the triple system case, it must be the classical system of points and planes of $AG_m(\boldsymbol{F}_2)$, with $s+1=2^m$, or else there would be unaccounted for weight-two vectors. One sees immediately that the role of the carrier is played by the dual of the code obtained from the first-order Reed-Muller code $\mathcal{R}(1,m)$ by repeating it $r+1$ times and this code becomes the binary code of the Steiner quadruple system. Its rank is $n-m$. Thus we have proved most of the following

Theorem 7.1 *For any $n\equiv 1,3 \pmod 6$ writing $n+1=u\times 2^k$ and choosing any i with $1\leq i<k$ there is a Steiner quadruple system of 2-rank $n-k+i$. All Steiner quadruple systems of 2-rank $n-k+i$ share the same code, namely the dual of the code obtained by repeating the first order Reed-Muller code, $\mathcal{R}(1,k-i)$, $u\times 2^i$ times. Every Steiner quadruple system of 2-rank $n-k+i$ can be constructed from this code and Steiner quadruple systems of smaller order.*

Proof: We have only to describe the construction. In fact, we describe a more general construction below which not only produces the quadruple systems of the Theorem but also many of full 2-rank. □

Remark: Computing the weight enumerator of the binary code of a Steiner quadruple system on $n+1=(r+1)2^m$ points of 2-rank $n-m$ poses no difficulty. It is even easier than in the Steiner triple system case. We leave the exercise to the reader.

The following construction for Steiner quadruple systems will produce systems with full 2-rank at least when the ingredients have full 2-rank. Hence it will produce many derived triple systems of full 2-rank.

Theorem 7.2 *Let r and s be integers congruent to* 1 *or* 3 *modulo* 6 *and suppose given a Steiner quadruple system on $s+1$ points, $s+1$ Steiner quadruple systems on $r+1$ points, and a resolution of the* 1-$((s+1)(r+1),2,r)$ *design given by the weight-two vectors of the direct sum of $s+1$ copies of the full even-weight subcode of $\boldsymbol{F}_2^{r+1}$. Then there is a Steiner quadruple system on $n+1=(s+1)(r+1)$ points containing each of the given systems on $r+1$ points on disjoint supports. If the given system on $s+1$ points has 2-rank $s-m$, then the constructed system will have 2-rank at most $n-m$. The 2-rank will be $n-m$ whenever one of the quadruple systems on $r+1$ points has full 2-rank.*

Proof: The proof, by now, will probably be quite clear to the reader but we sketch it nevertheless. One chooses the underlying $(s+1)(r+1)$-set to be $s+1$ disjoint $(r+1)$-sets and on each we impose one of the given quadruple systems on $r+1$ points. This introduces

$$(s+1)\frac{(r+1)r(r-1)}{24}$$

quadruples. For each of the r parallel classes of the given resolution of the 1-design, each choice of two of the $(r+1)$-sets and each choice of a 2-subset in each from the parallel class, we introduce the 4-subset that is the union of the two 2-subsets. This introduces

$$r\binom{s+1}{2}\left(\frac{r+1}{2}\right)^2$$

quadruples. For each of the quadruples from the given quadruple system on $s+1$ points we introduce $(r+1)^3$ 4-subsets each with a 1 in each of the four $(r+1)$-sets given by the quadruple and no two meeting more than twice. This introduces

$$(r+1)^3\frac{(s+1)s(s-1)}{24}$$

4-subsets. It is a very simple matter to check that we have the desired Steiner quadruple system. The rank calculation is easy since it is transparent that the code of the constructed system is built from the direct sum of the even subcodes and the overarching quadruple system on $s+1$ points. $\square$

Remark: We even allow $s=1$ and $r=1$ here, corresponding to the degenerate quadruple system. In fact when $r=s=1$ we simply produce the unique Steiner quadruple system on four points. For $r = 1$ and $s = 13$, for example, the quadruple systems on 28 points will have full 2-rank and thus produce derived Steiner triple systems of full 2-rank.

Corollary 7.3 *There are Steiner quadruple systems on 2^m points, and hence derived Steiner triple systems on $2^m - 1$ points, with full 2-rank for every $m > 3$.*

Proof: For $m = 4$ we cannot use the Theorem but there are precisely 57 such triple systems. From then on the Theorem produces the systems — taking $r = 1$, for example. □

One can even impose conditions on the ingredient quadruple systems to force a condition on the constructed system. As an illustration of the method we give the following construction of "resolvable" quadruple systems, i.e. quadruple systems for which the quadruples can themselves be organized into parallel classes. Here we must be in the even-order case: the quadruple system must be on a set of points whose cardinality is congruent to 4 or 8 modulo 12.

Corollary 7.4 *If there are resolvable quadruple systems on $r + 1$ and $s + 1$ points, then there is a resolvable quadruple system on $(r + 1)(s + 1)$ points.*

Proof: Since in the construction we can clearly piece the resolutions of the systems on $r + 1$ points together and those quadruples given by resolution of the weight-two vectors themselves form several parallel classes, we need only worry about the overarching quadruple system on $s + 1$ points which we, of course, assume is resolvable — just as we assume the systems chosen on $r + 1$ points are. We need to show that we can organize the choice of the 4-subsets for each quadruple into parallel classes and then use the resolution of the overarching system. We simply give an illustration for the case $r = 1$

treated extensively above:

$$\begin{matrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{matrix}$$

$$\begin{matrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{matrix}$$

$$\begin{matrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{matrix}$$

$$\begin{matrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{matrix}$$

8 Conclusions

The reader familiar with the work of Teirlinck and of Doyen, Hubaut and Vandensavel will surely be asking about a "ternary" view of Steiner triple systems and, to be sure, such a view exists and the above program is easily carried out. We leave as an exercise for the reader the task of exploring this ternary world, making the appropriate definitions, and proving the analogous results. We merely mention that one system is a mandarin in both worlds: the Steiner triple system on 3 points is both the projective line over $\boldsymbol{F}_2$ and the affine line over $\boldsymbol{F}_3$. Note, however, that there are triple systems that are welcome neither in the binary nor the ternary world. Such is the lot, for example, of the two systems on 13 points.

The classification in the case of Steiner quadruple systems bears a superficial resemblance to the ternary view of Steiner triple systems since the mandarins in both cases are the *affine geometries* and instead of seeing a "point at infinity" as we did in defining the trivializing subsystem one sees an array of systems spread, much like parallel classes, on the point set — just as in Corollary 6.4 — with a mandarin as overseer.

A more serious question concerns possible generalization to Steiner systems of the form $S(t, t+1, v)$ for $t > 3$. Here the reader will surely want to consult Teirlinck's work and perhaps also Cameron's book [6], where the matter is discussed. It does not seem likely, however, that anything further can be said and $t = 3$ seems to be the natural boundary — as Michel Dehon's work [7] indicates even when one goes to $S_\lambda(t, t+1, v)$.

A mathematician dipping into the vast literature on the topic of Steiner triple systems — as I did when writing up the results described above — has to be struck with the chaotic nature of many of the results and most of the constructions and the lack of organizing principles. One can only hope that the single construction that quite loudly presented itself for discovery as this work developed will be a step in the direction of organization.

ADDRESS:
Projet Codes, INRIA
Domaine de Voluceau - Roquencourt, B.P. 105
78153 Le Chesnay CEDEX, France
E-mail address: Edward.Assmus@inria.fr

PERMANENT ADDRESS:
Department of Mathematics
Lehigh University, 14 E. Packer Avenue
Bethlehem, PA 18015-3174, USA
E-mail: efa0@lehigh.edu

References

[1] Bruno Ratsimandefitra Andriamanalimanana. *Ovals, Unitals and Codes*. PhD thesis, Lehigh University, 1979.

[2] E. F. Assmus, Jr. and J. D. Key. Designs and codes: an update. Submitted to Des. Codes Cryptogr.

[3] 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).

[4] E. F. Assmus, Jr. and H. F. Mattson, Jr. On tactical configurations and error-correcting codes. *J. Combin. Theory*, 2:243–257, 1967.

[5] E. F. Assmus, Jr. and J. H. van Lint. Ovals in projective designs. *J. Combin. Theory, Ser. A*, 27:307–324, 1979.

[6] Peter J. Cameron. *Parallelisms of Complete Designs.* Cambridge: Cambridge University Press, 1976. London Mathematical Society Lecture Notes Series 23.

[7] Michel Dehon. Designs et hyperplans. *J. Combin. Theory, Ser. A*, 23:264–274, 1977.

[8] Jeffrey H. Dinitz, David K. Garnick, and Brendan D. McKay. There are 526,915,620 nonisomorphic one-factorizations of K_{12}. *J. Combin. Des.*, 2:273–285, 1994.

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

[10] J. D. Key and F. E. Sullivan. Steiner systems from binary codes. Submitted.

[11] C. C. Lindner and A. Rosa. There are at least 31,021 nonisomorphic Steiner quadruple systems of order 16. *Utilitas Math.*, 10:61–64, 1976.

[12] Charles C. Lindner and Alexander Rosa. Steiner quadruple systems – a survey. *Discrete Math.*, 22:147–181, 1978.

[13] E. Mendelsohn. The smallest non-derived Steiner triple system is simple as a loop. *Algebra Universalis*, 8:256–259, 1978.

[14] Eric Mendelsohn and Alexander Rosa. One-factorizations of the complete graph – a survey. *J. Graph Theory*, 9:43–65, 1985.

[15] K. T. Phelps. Some sufficient conditions for a Steiner triple system to be a derived system. *J. Combin. Theory, Ser. A*, 20:393–397, 1976.

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

[17] Reiss. Ueber eine *Steiner*sche combinatorische Aufgabe welche in 45^{sten} Bande dieses Journals, Seite 181, gestellt worden ist. *J. Reine Angew. Math.*, 56:326–344, 1859.

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

[19] D. R. Stinson and H. Ferch. 2000000 Steiner triple systems of order 19. *Math. Comp.*, 44:533–535, 1985.

[20] D. R. Stinson and E. Seah. 284457 Steiner triple systems of order 19 contain a subsystem of order 9. *Math. Comp.*, 46:717–729, 1986.

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

[22] Vladimir D. Tonchev and Robert S. Weishaar. Steiner triple systems of order 15 and their codes. *J. Statist. Plann. Inference*. To appear.