STEINER SYSTEMS AND PERFECT CODES

by

Wesleyan University, Middletown, Connecticut

and

University of North Carolina

Institute of Statistics Mimeo Series No. 484.1

July 1966

Presented at the NATO Summer School on
Combinatorial Methods in Coding and
Information Theory, Royan, France
August 26 - September 8, 1965

Organized by:

The Department of Statistics
University of North Carolina
and
The Institute of Statistics
University of Paris

This research was supported by the Air Force Office of Scientific Research Contract No. AF-AFOSR-760-65 and also partially supported by Contract No. AF 19 (604)-8516.

DEPARTMENT OF STATISTICS

UNIVERSITY OF NORTH CAROLINA

Chapel Hill, N. C.

1. Introduction

Near the middle of the last century there arose both in England and on the Continent a circle of combinatorial problems now mostly associated with the names Kirkman and Steiner. One hundred years later much the same problems, in rather different guise, arose in electrical engineering work connected with information transmission. Golay and Hamming made the initial contributions to the discussion of the modern form of the problems, and it was Paige who pointed to the relationship between the problems of Steiner and the coding problems of information transmission.

We wish here to discuss this relationship in some detail, centering it about two general (and easy to prove) theorems which make the connection between perfect codes and Steiner systems precise.

The clearest statement of the older combinatorial problem was given by Steiner in 1852, [29], and the problem is generally known as "Die Steinersche Combinatorische Aufgabe," although Sylvester, Kirkman, and Cayley had already written about aspects of it, [30], [18], and [5], and, in fact, Kirkman had established already the necessary and sufficient conditions for the existence of what are now known as Steiner triple systems.*

The problem is a follows: Given a finite set S (of cardinality n, say), when is it possible to select a collection of subsets of S, each subset consisting of three elements, in such a way that every subset of S of cardinality 2 is contained in precisely one of the selected subsets, which are

---

*Usually attributed to Reiss, [26], this result is: There is a Steiner triple system on a set of cardinality n if and only if n is congruent to 1 or 3 modulo 6.

called the triples of the "system." Assuming this problem solved, when is it possible to select a further collection of subsets of S, each subset consisting of four elements, in such a way that no one of these new subsets contains a triple but such that every subset of S of cardinality 3 which has not been selected as a triple is contained in precisely one of the new subsets, which are called the quadruples of the system. Assuming both these problems solved, when is it possible to select a collection of subsets of S each consisting of five elements in such a way that no one of these contains either a triple or a quadruple but such that every subset of S cardinality 4 which neither contains a triple nor is itself a quadruple is contained in precisely one of the selected subsets, which are called the quintuples of the system. And so on for sextuples, septuples, etc.

As already noted, whether or not one can select the triples is simply a matter of the congruence of n modulo 6. The facts are established nicely by Bruck, [2], where one can also find a general discussion of Steiner triple systems. Although the existence problem for triple systems is rather easy, the problem also posed by Steiner, of the number of inequivalent* triple systems seems more difficult. So far, one knows that up to equivalence the triple systems are unique for n = 1, 3, 7, 9; that there are precisely two inequivalent triple systems for n = 13; and that there are precisely eighty inequivalent triple systems for n = 15.**

---

*Two Steiner triple systems on S areequivalent if there is a permutation of S which carries one collection of triples onto the other.

**Cayley, [6], conjectured there were at least three. F. N. Cole established that there were eighty, a fact later confirmed by computation on SWAC. See [12].

The only general result along these lines that we are aware of is Moore's, [21]; he shows that, for n= 1, 3 (mod 6) and n> 13, there are at least two inequivalent Steiner triple systems. Witt, [36, p. 270], suggested that the number of inequivalent triple systems was likely to grow very fast with n, a fact we have recently confirmed.***

Although the problem of the existence of Steiner triple systems had been solved even before Steiner stated it, the next step, i.e., the introduction of quadruples, was only recently attacked and is partially solved. (Partially, in the sense that for $n \geq 13$ whether or not the quadruples can be introduced may very well depend on the particular triple system one starts with.) Hanani, [14], has shown that, for $n \equiv 2, 4 \pmod 6$, one can always find a collection of subsets (of a set of cardinality n), each consisting of four elements and called a quadruple such that every subset (of the underlying set) of cardinality 3 is in precisely one of the quadruples. It is easy to see that Hanani's result is equivalent to the assertion that, for $n \equiv 1, 3 \pmod 6$, there is a triple system which admits quadruples satisfying Steiner's demands.

As far as we know there have been no further general results concerning the introduction of quintuples, etc. The second of our general theorems concerns these further questions.

Steiner's original problem has been given various twists. Skolem, Carmichael, and Witt are among the Twentieth Century mathematicians who have discussed these twists although again, Sylvester and Cayley had made certain

---

***For $n = 2^m-1$ the number of inequivalent systems is at least 2^x where $x = \frac{2}{9} 4^{m-1} + O(2^m)$.

contributions as early as 1850. Witt, [36], treats the following generalization due to Moore: Given a finite set S of cardinality n and two integers $\ell \leqq d \leqq n$, when is it possible to find a collection of subsets of S, each subset consisting of d elements, such that every subset of S of cardinality ℓ is contained in precisely one of the selected subsets, called lines. (A Steiner triple system is the case: $\ell = 2$, $d = 3$.) Witt's 1938 discussion is still rather complete; here he proves the uniqueness for the cases: (1) $\ell = 5$, $d = 6$, $n = 12$; (2) $\ell = 4$, $d = 5$, $n = 11$; (3) $\ell = 5$, $d = 8$, $n = 24$; (4) $\ell = 4$, $d = 7$, $n = 23$; (5) $\ell = 3$, $d = 6$, $n = 22$. These cases correspond to the Mathieu groups, M_{12}, M_{11}; M_{24}, M_{23}, and M_{22}. Paige, [24], and Assmus and Mattson, [1], have used Witt's results, [35] and [36], to elucidate the connection between the Mathieu groups and well known codes.

Still further, one can ask not that every subset of cardinality ℓ be contained in precisely one line, but that every subset of cardinality ℓ be contained in precisely λ lines, [23, Note 16], [4], [27]. We call such a "combinatorial design" a tactical configuration of type (λ, ℓ, d, n); tactical configurations are the subject of much current research. One way to produce tactical configurations of type (λ, ℓ, d, n) is to find λ disjoint* Steiner systems (in Moore's sense) with parameters ℓ, d, and n. It seems that Sylvester** was the first to attack this problem in this way, producing seven disjoint Steiner triple systems for n = 9, [32] and [33].

---

* Two Steiner systems are said to be disjoint if the lines of one are all distinct from the lines of the other.

** Sylvester also claims, [31], to be the author of the so-called Kirkman School-girls Problem advancing the conjecture that it filtered down to Kirkman via undergraduates at Cambridge.

Emch in 1929, [7], produces the same result. Cayley, [5], noted that there were two but no more disjoint Steiner triple systems for n = 7. Since the seven disjoint Steiner triple systems produced by Sylvester necessarily contain among them every subset of cardinality 3, Sylvester had proved that there are (in modern language) tactical configurations of type (λ , 2, 3, 9) for all possible values of λ ; Cayley had proved that there are tactical configurations of type (λ, 2,3, 7) for λ = 1, 2.*** The relationship between certain triple systems and the Hamming codes, which is a consequence of our first general theorem, will allow us to make some statements about disjoint Steiner triple systems.

The next section is devoted to a statement of the two theorems together with a discussion of some applications. The concluding section discusses the existence problem for disjoint Steiner triple systems.

***By taking complements one then has that there are configurations of type (4, 2, 3, 7) and (3, 2, 3, 7); the configuration of type (5, 2, 3, 7) is merely all possible triples. Thus all possible values of λ are admissible.

2. THE MAIN RESULTS

For the purposes of this discussion we will understand by a code a linear subspace of the concrete n-dimensional vector space of n-tuples taken from a finite field F. We will denote by the V the space of n-tuples and by A the subspace or code. n is called the block length of A. For $v \in V$, $v = (v_1, v_2, \ldots, v_n)$, the weight of v, denoted by w (v), is the number of v_i's which are not 0. The minimum weight of A is the minimum of w(a) where a ranges over the non-0 vectors in A; we will habitually denote it by d. It is well known that the "distance function," $\rho(v,v') = w(v-v')$, is metric on V and that for any two distinct elements a, b of A, $\rho(a,b) \geq d$. Let e be the greatest integer less than or equal to $\frac{d-1}{2}$. For each a in A consider the closed sphere of radius e about a; call it O_a. ($O_a = \{ v \in V \mid \rho(v,a) \leq e\}$.) The collection of these spheres is pairwise disjoint. If their union is all of V, the code is said to be perfect. For a perfect code d is necessarily odd and thus $d = 2e + 1$. For every finite field F (of cardinality q, say) and every integer t there is a perfect code of block length $\frac{q^t-1}{q-1}$ and minimum weight 3; these are the so-called Hamming codes. There are only two other perfect codes known, one over the field GF(2) with n = 23 and d = 7 and the other over the field GF(3) with n = 11 and d = 5. There are several isolated results on the non-existence of perfect codes; see, e.g., [8], [17], [19], and [28].

Given a code A with minimum weight d, let S be the set of integers $\{1, 2, \ldots, n\}$ where n is the dimension of the containing space V. If $a = (a_1, a_2, \ldots a_n)$ is a vector in A of weight d, let $D_a = \{ i \mid a_i \neq 0\}$. (Thus D_a is the set of coordinate places where the coordinate of the vector a

is not 0.) Set

$$\mathfrak{B} = \{ D_a \mid a \in A \text{ and } w(a) = d \} .$$

$\mathfrak{B}$ is, of course, a collection of subsets of S each of cardinality d. In certain cases S and $\mathfrak{B}$ form a tactical configuration for parameters λ and ℓ. Precisely, we have

Theorem A. If A is a code over GF(q) of block length n and minimum weight d, then A is perfect if and only if S and $\mathfrak{B}$ form a tactical configuration of type ($\lambda = (q-1)^e$, $\ell = e + 1$, d, n), where $e = \left\lfloor \frac{d-1}{2} \right\rfloor$.

Remarks: (1) Over GF(2) $\lambda = (q-1)^e$ is always 1. Thus the perfect codes over GF(2) produce Steiner systems (in the sense of Moore). The Hamming codes produce Steiner triple systems; Theorem B will have more to say about this particular case. The Golay code over GF(2) of block length 23 and minimum weight 7 produces the Steiner system of type (4, 7, 23) which Witt proved was unique.

(2) The Golay code over GF(3) of block length 11 and minimum weight 5 produces a tactical configuration with $\lambda = 4, \ell = 3$. It is that configuration obtained in an obvious way from the unique Steiner system of type (4, 5, 11).

(3) Theorem A allows one to compute the number of vectors of minimum weight in a perfect code over GF(q), namely

$$(q-1)^{e+1} \frac{\binom{n}{e+1}}{\binom{d}{e+1}} ,$$

where n, d, and e are, respectively, the block length, minimum weight, and $\frac{d-1}{2}$.

(4) It is well known and very easy to show that a necessary condition for the existence of a tactical configuration of type (λ, ℓ, d, n) is that

$$\lambda \frac{\binom{n-h}{\ell-h}}{\binom{d-h}{\ell-h}}$$

should be an integer for h = 0, 1,...,ℓ-1. This yields a necessary condition for the existence of a perfect code over GF(q) of block length n and minimum weight d. It is that

$$(q-1)^e \frac{\binom{n-h}{e+1-h}}{\binom{d-h}{e+1-h}}$$

should be an integer for h = 0, 1,...,e. Over GF(2) the $(q-1)^e$ disappears; Shapiro and Slotnick obtain this result for h = 0 and h = e [28, Theorem 1 and Theorem 3], where, however, they do not assume linearity. The proof of the relevant half of Theorem A can be carried out over GF(2) without assuming linearity and hence it generalizes the results of Shapiro and Slotnick. (Cf. [17, Theorem 1].)

(5) Shapiro and Slotnick, [28], have proved that there are no perfect codes over GF(2) with d = 5 and n > 5. There is, however, a (unique) Steiner system of type (3, 5, 17), [36]. Thus, the nonexistence of perfect codes does not imply the nonexistence of the corresponding tactical configuration.

(6) On the other hand, the nonexistence of certain tactical configurations does imply the nonexistence of certain perfect codes. E.g., the "Hamming equation," $1 + n + \binom{n}{2} = 2^k$, has a solution for n = 90, but the

nonexistence of a Steiner system of type (3,5, 90) follows from the fact that 88 is not divisible by 3 (see (1)) and hence there is no 2-error-correcting close-packed subset of the 90-dimensional space over GF(2). Cf. [28].

(7) The existence of a projective plane of order k is equivalent to the existence of a Steiner system of type (2, k+1, k^2+k+1). [27, p. 104]. Now a Steiner system of type (k, 2k-1, k^2+2k-1) gives rise to one of type (2, k+1, k^2+k+1); e.g., the Hamming code of block length 7 "is" the unique projective plane of order 2 and the Golay code of block length 23, on suppression of two coordinate places, gives rise to the unique projective plane of order 4. Thus the nonexistence of a projective plane of order k implies the nonexistence of a close-packed subset of the (k^2+2k-1)- dimensional space over GF(2) with minumum weight 2k-1. The Bruck-Ryser Theorem can, of course, be applied. We know of no cases where its application yields interesting results; indeed computer results, [19], suggest we already know all solutions of the Hamming equation over GF(2).

(8) It follows easily from Theorem A that in a perfect code the vectors of minimal weight generate the code.

Before stating Theorem B we must establish some precise notation for the statement of Steiner's original problem. Let S be a finite set, $\mathfrak{D}_3, \mathfrak{D}_4$, ..., $\mathfrak{D}_k$ collections of subsets of S; set $\mathfrak{D} = \mathfrak{D}_3 \cup \mathfrak{D}_4 \cup \ldots \cup \mathfrak{D}_k$. We say that $\mathfrak{D}$ is a <u>Steiner system of rank k on S</u> if the following are satisfied:

(1) Each set in $\mathfrak{D}_i$ has cardinality i for i = 3, 4, ...,k;

(2) No element of $\mathfrak{D}$ is a subset of another element of $\mathfrak{D}$;

(3) If S' is a subset of S of cardinality i-1, $3 \leq i \leq k$, then either some element of $\mathfrak{D}$ is a subset of S' or there is a unique D in $\mathfrak{D}_i$ with $S' \subset D$.

If $\mathfrak{D} = \mathfrak{D}_3 \cup \mathfrak{D}_4 \cup \ldots \cup \mathfrak{D}_k$ is a Steiner system of rank k on S, then $\mathfrak{D}_3$ is a triple system on S, $\mathfrak{D}_3$ together with $\mathfrak{D}_4$ are a system of triples and quadruples satisfying Steiner's demands, etc. By a <u>complete Steiner system on S</u> we will mean a Steiner system of rank n where n is the cardinality of S. Notice that we do not demand that $\mathfrak{D}_i$ be nonempty; in fact, for a complete Steiner system $\mathfrak{D}_i$ will always be empty for large i.

Let A be a Hamming code of block length $n = 2^t - 1$ over GF(2). Thus A is a subspace of the n-dimensional space of n-tuples of 0's and 1's, and A has minimum weight 3 and dimension n-t. For each $a = (a_1, a_2, \ldots, a_n)$ in A let $D_a = \{i \mid a_i = 1\}$. D_a is a subset of $S = \{1,2,\ldots,n\}$ and the cardinality of D_a is the weight of a. Define $\mathfrak{D}_3, \mathfrak{D}_4, \ldots, \mathfrak{D}_n$ as follows: $\mathfrak{D}_3 = \{ D_a \mid w(a) = 3\}$, $\mathfrak{D}_4 = \{D_a \mid w(a) = 4$ and $D_a \supset D_b$ implies $b = 0$ or $b = a\}, \ldots,$ $\mathfrak{D}_i = D_a \mid w(a) = i$ and $D_a \supset D_b$ implies $b = 0$ or $b = a\}$. More briefly, $\mathfrak{D} = \mathfrak{D}_3 \cup \mathfrak{D}_4 \cup \ldots \mathfrak{D}_n$ is the collection of all nonempty D_a which do not contain any other D_b. We can now state

<u>Theorem B</u>. If A is a Hamming code over GF(2) of block length n, then $\mathfrak{D}_3, \mathfrak{D}_4, \ldots, \mathfrak{D}_n$ is a complete Steiner system.

<u>Remarks</u>: (1) The well-known Hamming code of block length 7 gives the first nontrivial instance of this theorem. In this case $\mathfrak{D}_3$, can be identified with the seven weight-3 vectors, $\mathfrak{D}_4$ with the seven weight-4 vectors.

(2) The next nontrivial instance is the Hamming code of block length 15. The only nonempty collections are $\mathfrak{D}_3$, $\mathfrak{D}_4$, and $\mathfrak{D}_5$, and they can be identified respectively with the weight-3, weight-4, and weight-5 vectors since there are no containing relations. In fact, for n = 15, any close-packed,* single-

---

*I.e., either linear or not. Nonlinear close-packed single-error-correcting "codes" of block length 15 are known to exist, [34].

error-correcting subset yields a complete Steiner system. This allows us to make several observations about Steiner's original problem for n = 15:

(a) We know, of course, that for n = 15, triples, quadruples, and quintuples can be chosen satisfying Steiner's demands and that, in fact, one need go no further; i.e., every subset of cardinality at least 5 contains either a triple, or a quadruple, or a quintuple. (b) There are essentially different ways of adjoining quadruples and quintuples to the Steiner triple system of the linear Hamming code of block length 15 to form a complete Steiner system. (We have not, however, any information on the number of essentially distinct completions.) (c) There are inequivalent Steiner triple systems on 15 elements both of which allow the introduction of quadruples and quintuples satisfying Steiner's demands. (d) There are inequivalent close-packed single-error-correcting subsets of the 15-dimensional space over GF(2) which yield the same complete Steiner systems; i.e., there are inequivalent close-packed subsets (containing 0) which have the same vectors of weight 3, weight 4, and weight 5.

3. DISJOINT TRIPLE SYSTEMS

In this section we want to discuss disjoint Steiner systems. As we said already, if we are given m disjoint Steiner systems of type (ℓ, d, n), then we automatically have the existence of tactical configurations of type (λ, ℓ, d, n) for $\lambda = 1, 2, \ldots, m$. (But not conversely.) The coding point of view makes it rather easy in some cases to establish the existence of disjoint Steiner systems. E.g., $x^{23} + 1 = (x+1)\, f(x)\, g(x)$ over GF(2) and as is well known, [25], both $(x+1)f(x)$ and $(x+1)\, g(x)$ define recursively perfect codes of block length 23 and minimum weight 7. (These codes are in fact equivalent.) Their intersection consists of the 1-dimensional subspace generated by the vector $(1, 1, \ldots, 1)$. Now Theorem A tells us that the minimum weight vectors of each code can be identified with Steiner systems of type (4, 7, 23). Since the intersection contains no vectors of weight 7, we get t o disjoint Steiner systems of type (4, 7, 23) and hence a tactical configuration of type ($\lambda = 2$, 4, 7, 23). As far as we know no one had observed this before the relationship with coding became known. One can similarly see that there are two disjoint Steiner systems of type (5, 8, 24) and hence a tactical configuration of type ($\lambda = 2$, 5, 8, 24). Using the same technique for the factorization of $x^{11}-1$ over GF(3) one gets tactical configurations of type ($\lambda = 2$, 4, 5, 11) and ($\lambda = 2$, 5, 6, 12). For further details see [1].

We restrict ourselves now to triple systems, in fact, to those arising from the perfect Hamming codes over GF(2). Thus there is one (and only one up to equivalence) for each n of the form 2^t-1. For t = 1 and 2 they are trivial. For t = 3 Cayley showed there were two disjoint triple systems, a fact easily established as above by considering the splitting of x^7+1 over

GF(2). For t = 4 (i.e., n = 15) the polynomial approach breaks down. The two "cyclic" Hamming codes one gets do not yield disjoint triple systems. Sylvester, [31], asked for 13 disjoint triple systems for n = 15 (the maximum number possible); we know of no result along these lines.

For t = 5 (i.e., n = 31) a computation was made by Prange. The six "cyclic" Hamming codes are pairwise disjoint both in their weight 3 and weight 4 vectors. Thus one knows that these are 6 disjoint Steiner triple systems for n = 31 and that there are 6 disjoint Steiner systems of type (3, 4, 32).

These are the only particular cases for which we have precise results. In general for $n = 2^t-1$, x^n+1 factors over GF(2) into irreducibles of which $m = \frac{\phi(n)}{t}$ lead to Hamming codes. We are able to prove only the rather weak

Proposition. If t is odd, there are two equivalent but disjoint Steiner triple systems on a set of cardinality 2^t-1, and there are two equivalent but disjoint Steiner systems of type $(3, 4, 2^t)$.

Remark: If n is a Mersenne prime, then $m = \frac{\phi(n)}{t} = \frac{2^t-2}{t}$; one might reasonably hope for m disjoint triple systems in this case. For n = 7 and n = 31 one does get them. For n = 127 we have only the information given by the Proposition.

Details, proofs, and some further results concerning the questions treated above will appear elsewhere. We wish to thank Andrew Gleason, Eugene Prange, and Richard Turyn for their help and interest during the past year when the research reported on here was carried out.

The bibliography which follows is by no means complete. Petersons' book contains an extensive bibliography on coding. The books of Carmichael, Netto, and Ryser may be consulted for further information and bibliographies concerning tactical configurations (or combinatorial designs).

REFERENCES

[1] E. F. Assmus, Jr., and H. F. Mattson, "Perfect Codes and the Mathieu Groups," Archiv der Math. (to appear).

[2] R. H. Bruck, "What is a Loop?," Studies in Modern Algebra, M.A.A. Studies in Mathematics, 2, 59-99.

[3] W. Burnside, "On an Application of the Theory of Groups to Kirkman's Problem," Messenger of Mathematics, XXIII (1893-1894), 137-143.

[4] R. D. Carmichael, Groups of Finite Order, Dover edition (1956).

[5] Arthur Cayley, "On the Triadic Arrangements of Seven and Fifteen Things," Philosophical Magazine, XXXVII (1850), 50-53 (Collected Mathematical Papers, I, 481-484).

[6] Arthur Cayley, "On a Tactical Theorem Relating to the Triads of Fifteen Things," London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science, XXV(1863), Ser. 4, 59-61 (Collected Mathematical Papers, V, 95-97).

[7] Arnold Emch, "Triple and Multiple Systems, Their Geometric Configurations and Groups," Trans. A.M.S., 31 (1929), 25-42.

[8] Carl Engleman, "On Close-Packed Double Error Correcting Codes on P Symbols," IRE Trans., IT-7 (1961), 51-52.

[9] M. J. E. Golay, "Notes on Digital Coding, " Proc. IRE, 37 (1949), Correspondence, 657.

[10] M. J. E. Golay, "Binary Coding," IRE Trans., PGIT-4 (1954), 23-28.

[11] M. J. E. Golay, "Notes on the Penny-Weight Problem, Lossless Symbol Coding with Nonprimes, Etc.," IRE Trans., IT-4 (1958), 103-109.

[12] Marshall Hall, Jr., and J. D. Swift, "Determination of Steiner Triple Systems of Order 15," Math. Tables and Aids to Comput., 9 (1955), 146-152.

[13] R. W. Hamming, "Error Detecting and Error Correcting Codes," Bell System Technical J., 29 (1950), 147-160.

[14] Haim Hanani, "On Quadruple Systems, " Can J. Math. 12 (1960), 145-157.

[15] Haim Hanani, "The Existence and Construction of Balanced Incomplete Block Designs," Ann. Math. Stat. 32 (1961), 361-368.

[16] Haim Hanani, "On Some Tactical Configurations," Can. J. Math. 15 (1963) 702-722.

[17] Selmer Johnson, "On Perfect Error-Correcting Codes," The RAND Corporation Memorandum RM-3403-PR (1962).

[18] Rev. Thomas Kirkman, "On a Problem in Combinations," Cambridge and Dublin Mathematical Journal, II (1847), 191-204.

[19] M. H. McAndrew, "An Algorithm for Solving a Polynomic Congruence, and its Application to Error-Correcting Codes," Mathematics of Computation, 19 (1965), 68-72.

[20] H. F. Mattson and Gustave Solomon, "A New Treatment of B ose-Chaudhuri Codes," J. Soc. Indust. Appl. Math., 9 (1961), 654-669.

[21] E. H.Moore, "Concerning Triple Systems," Math Ann., 43 (1893), 271-285.

[22] E. H. Moore, "Tactical Memoranda," Amer. J. Math., 18 (1896), 264-303.

[23] E. Netto, Lehrbuch der Combinatorik, Leipzig, Teubner, 2nd edition, 1927, reprinted by Chelsea.

[24] L. J. Paige, "A Note on the Mathieu Groups," Can. J. Math., 9 (1956), 15-18.

[25] W. Wesley Peterson, Error-Correcting Codes, MIT Press and John Wiley and Sons, Inc., New York, (1961).

[26] M. Reiss, "Uber eine Steinersche Combinatorische Aufgabe Welche im 45sten Bande Dieses Journals, Seite 181, Gestellt Worden ist," Crelle's J., 56 (1859), 326-344.

[27] H. J. Ryser, Combinatorial Mathematics, John Wiley and Sons (1963).

[28] H. S. Shapiro and D. L. Slotnick, "On the Mathematical Theory of Error-Correcting Codes," I.B.M. J. of Research and Development, 3 (1959), 25-34.

[29] J. Steiner, "Combinatorische Aufgabe," J. fur die Reine und Angewandte Mathematik, 45 (1853), 181-182.

[30] J. J. Sylvester, "Elementary Researches in the Analysis of Combinatorial Aggregation," Philosphical Magazine, XXIV (1844), 285-296. (Mathematical Papers, I, 91-102.)

[31] J. J. Sylvester, "Note on the Historical Origin of the Unsymmetrical Six-Valued Function of Six Letters," Philosophical Magazine, XXI (1861), 369-377. (Mathematical Papers, II 264-271.)

[32] J. J. Sylvester, "Remark on the Tactic of Nine Elements," Philosophical Magazine, XXII (1861) 144-147. (Mathematical Papers, II, 286-289.)

[33] J. J. Sylvester, "Note on a Nine Schoolgirls Problem," Messenger of Mathematics XXII (1892-1893), 159-160 and (Correction) 192. (Mathematical Papers, IV, 732-733.)

[34] Ju. L. Vacil'ev, "On Nongroup Close-Packed Codes," Problems of Cybernetics, 8, Pergamon Press translation (to appear).

[35] Ernst Witt, "Die 5-fach Transitiven Gruppen von Mathieu," Abhandlungen aus dem Mathematischen Seminar der Hansischen Universitat, 12 (1936), 256-264.

[36] Ernst Witt, "Uber Steinersche Systeme," Abhandlungen aus dem Mathematischen Seminar der Hansischen Universitat, 12 (1936), 265-275.