MATH. SCAND. 25 (1969), 149–158

ON GROUP AND NONGROUP PERFECT CODES IN q SYMBOLS

BERNT LINDSTRÖM

1. Introduction.

There is now an extensive literature on error-correcting codes (cf. bibliography in [3]). A brief survey of perfect codes can be found in [2].

In this paper we shall only consider single-error-correcting perfect codes, called SECP codes for brevity. The first instances of SECP codes were found about 1950 by E. W. Hamming and M. J. E. Golay as vector spaces over a finite field (linear codes), and in group theory by E. Mattioli, O. Taussky, J. Todd, J. G. Mauldon and S. K. Zaremba (group codes). The last five authors did not use the word "code", which originates from information theory.

About 1960 Ju. L. Vasilev discovered a large class of SECP codes in two symbols (see [14]). The construction of Vasilev was generalized by J. Schönheim in [9] and independently by the author.

In this paper we shall apply Veblen–Wedderburn systems from the theory of finite projective planes to the construction of SECP codes. There is a close connection between group SECP codes of length $q+1$ and Veblen–Wedderburn systems of order q. Any Veblen–Wedderburn system, which yields a non-Desarguesian plane, can be applied to construct a group code, which can not be obtained from a linear code by permutations of symbols or coordinates.

SECP codes were studied in [10] by R. G. Stanton and J. D. Horton in connection with a covering problem by O. Taussky and J. Todd (see [13, p. 204]). This covering problem was also studied by J. G. Kalbfleisch and R. G. Stanton in [6], [11] and in a series of forthcoming papers.

I take the opportunity to acknowledge my sincere gratitude to Professor Kalbfleisch, who let me see papers by him and his colleagues before they were printed. I am also indebted to Dr. Mattson and J.-E. Roos for valuable information on perfect codes.

Received November 21, 1968; in revised form March 3, 1969.

2. Definitions and notations.

Let F be a finite set of q symbols, $q \geqq 2$. Define F^n as the set of all n-tuples of elements of F. For any two n-tuples $s=(s_1,s_2,\ldots,s_n)$ and $t=(t_1,t_2,\ldots,t_n)$ define the *distance* $\varrho(s,t)$ to be the number of places i where $s_i \neq t_i$, $1 \leqq i \leqq n$.

A *code* C on F, which corrects e errors, is a subset of some F^n such that $\varrho(s,t) \geqq 2e+1$ for any two distinct n-tuples s and t of C. For brevity we shall say that C is a (n,e,q) code. An element s in C is the centre of a sphere of radius e, which consists of all elements of F^n at the distance at most e from s. If all these spheres exhaust F^n, we shall say that C is a *perfect code*. We shall only consider single-error-correcting codes for which codes $e=1$. The number of elements in a sphere of radius 1 in F^n is $1+n(q-1)$. It is necessary for the existence of a perfect $(n,1,q)$ code in F^n that $1+n(q+1)$ divides q^n, and if q is a power of a prime it follows that $n=(q^r-1)/(q-1)$ for an integer $r \geqq 1$. For $n=1$, $q \geqq 2$ we have only *trivial* perfect codes with one element. Nontrivial $(n,1,q)$ perfect codes exist when q is a power of a prime and $n=(q^r-1)/(q-1)$, $r \geqq 2$ (see H-Golay codes in [2]). By Theorem 7 in [10] there is no perfect $(7,1,6)$ code. It is not known if perfect $(n,1,q)$ codes exist when $n>1$ and $q \neq 6$ is not a power of a prime.

Let F be an abelian group and F^n the direct product n times of F. We shall say that a code C in F^n is a *group code*, if C is a subgroup of F^n.

Let F be a finite field and F^n the vector space of dimension n over F. A code C in F^n is a *linear code*, if C is a subspace of F^n.

A simple method to find a new perfect $(n,1,q)$ code from a given perfect $(n,1,q)$ code, is to permute components or symbols in the n-tuples of the code. An n-tuple $(s_1,s_2,\ldots,s_n)$ is then mapped on

$$((s_{i_1})\pi_1,(s_{i_2})\pi_2,\ldots,(s_{i_n})\pi_n)\,,$$

where $i_1,i_2,\ldots,i_n$ is a permutation of the places $1,2,\ldots,n$ and $\pi_1,\pi_2,\ldots,\pi_n$ are permutations of F. The new code is said to be *equivalent* with the old one. More generally, the set of symbols need not be the same for both codes, if $\pi_1,\pi_2,\ldots,\pi_n$ are assumed to be bijective functions.

Ju. L. Vasilev constructed in [14] perfect $(n,1,2)$ codes, which are not equivalent with group codes for $n=2^r-1$, $r \geqq 4$. S. K. Zaremba proved that every perfect $(7,1,2)$ code is equivalent with a group code [15, Prop. 7]. A shorter proof was given in [11, Theorem 5]. O. Taussky and J. Todd observed that every $(4,1,3)$ perfect code is equivalent with a group code (in [12], see also [6, Theorem 4]). It would be interesting to know if every perfect $(q+1,1,q)$ code is equivalent with a group code.

We shall need an important kind of ternary system in projective geometry called *Veblen–Wedderburn system* or VW system for brevity. A VW system consists of elements (a,b,c, etc.), two distinguished elements 0 and 1, and has a well-defined addition $a+b$ and multiplication ab (or occasionally $a \circ b$), which satisfy (cf. [4, p. 180]):

VW 1. Addition yields an abelian group with zero 0.
VW 2. $0a=a0=0$, $1a=a1=a$.
VW 3. In $xy=z$, if any two of x,y,z are given and different from 0, the third is unique and different from 0.
VW 4. $(a+b)c=ac+bc$.
VW 5. If $r \neq s$, $xr=xs+b$ has a unique solution x.

VW 5 is a consequence of the other axioms if the number of elements is finite. Multiplication on the right by a nonzero element is an automorphism of the abelian group. It is easy to prove that the abelian group is of type $(p,p,\ldots,p)$ if the VW system is finite. Hence the order of a finite VW system is a power of a prime p.

If the order of the VW system is a prime, we have a prime field. If the order is 4 or 8 we also have a finite field. For every finite projective plane of order at most 8 is Desarguesian (cf. [5]) and the ternary systems are then finite fields (cf. [1, p. 77]). If q is a proper power of a prime different from 4 and 8, one can find VW systems, which are not fields (cf. [4, pp. 181–185]).

We shall introduce an auxiliary notion. *A perfect system of automorphisms* of an abelian group F of order q is a set of $q-1$ automorphisms $\alpha_1,\alpha_2,\ldots,\alpha_{q-1}$ of F such that $(x)\alpha_i \neq (x)\alpha_j$ for $x \in F$, $x \neq 0$ and $i \neq j$.

The nonzero elements of a finite VW system yield a perfect system of automorphisms of the abelian group. Conversely, if we have an abelian group with a perfect system of automorphisms, we can define multiplication such that it becomes a VW system. Introduce the label 1 for any of the nonzero elements of the abelian group. If $(1)\alpha_i=a_i$ we shall use a_i as a new label for α_i. If α_1 is the identity automorphism, α_1 is now labelled by 1. If α_1 is not the identity we can use another perfect system of automorphisms, viz. $\alpha_i(\alpha_1)^{-1}$, $i=1,2,\ldots,q-1$. Define $a0=0$ and write ab instead of $(a)b$. It is now easy to see that we have a VW system.

3. On perfect $(q+1,1,q)$ group codes.

LEMMA 1. *Let F be an abelian group of order $q \geqq 2$ and let $\alpha_1,\alpha_2,\ldots,\alpha_{q-1}$ be a perfect system of automorphisms of F. Then the $(q+1)$-tuples*

(3.1) $(u_1, u_2, \ldots, u_{q-1}, \sum_{i=1}^{q-1} u_i, \sum_{i=1}^{q-1} (u_i)\alpha_i), \quad u_1, u_2, \ldots, u_{q-1} \in F$,

yield a perfect $(q+1, 1, q)$ *group code.*

PROOF. The number of $(q+1)$-tuples (3.1) is q^{q-1}. The number of $(q+1)$-tuples in a sphere of radius 1 is q^2. If we can prove that the distance between different $(q+1)$-tuples (3.1) is at least 3, it follows that the spheres of radius 1 with centre in points (3.1) cover the entire space F^{q+1}, that is, the code is perfect.

Let u' be another $(q+1)$-tuple (3.1) with u_i' in place of u_i everywhere. Assume $u_k \neq u_k'$ for a fixed k and $u_i = u_i'$ for every $i \neq k$. Then we have $\varrho(u, u') \geqq 3$.

Next assume $u_j \neq u_j'$ and $u_k \neq u_k'$ for fixed j and k, $j \neq k$. If $\varrho(u, u') = 2$, we find, after subtraction of equal terms in both members, the equations

$$u_j + u_k = u_j' + u_k' ,$$
$$(u_j)\alpha_j + (u_k)\alpha_k = (u_j')\alpha_j + (u_k')\alpha_k .$$

It follows from these equations $(u_j - u_j')\alpha_j = (u_j - u_j')\alpha_k$, which is a contradiction since $u_j - u_j' \neq 0$ and $j \neq k$. Hence $\varrho(u, u') \geqq 3$ for any two different $(q+1)$-tuples (3.1). It is easy to see that we have a group code, and the lemma follows.

If we have a VW system, then the nonzero elements of F yield a perfect system of automorphisms of the additive abelian group. In this case we shall say that (3.1) defines a *first order F-code.*

The following theorem establishes a close connection between perfect $(q+1, 1, q)$ group codes and VW systems.

THEOREM 1. *A first order F-code of* $(q+1)$*-tuples is a perfect* $(q+1, 1, q)$ *group code. A perfect* $(q+1, 1, q)$ *group code C is equivalent with a first order F-code. If a perfect* $(q+1, 1, q)$ *linear code is equivalent with a first order F-code, then F is the finite field* GF(q).

PROOF. The first part of the theorem was proved in Lemma 1.

Let C be a perfect $(q+1, 1, q)$ group code. Since the distance between different $(q+1)$-tuples in C is at least 3, it follows that there is at most one $(q+1)$-tuple in C for which the first $q-1$ components are given in advance. Since the number of $(q+1)$-tuples in C is q^{q-1}, it follows that all combinations of values occur in the $q-1$ first components of $(q-1)$-tuples in C.

Let u_i be the ith component of a $(q+1)$-tuple in C, $1 \leqq i \leqq q+1$. If

$1 \leqq k \leqq q-1$ and $u_i = 0$ for $1 \leqq i \leqq q-1$ except possibly when $i = k$, we define σ_k and τ_k by

$$u_q = (u_k)\sigma_k, \quad u_{q+1} = (u_k)\tau_k .$$

σ_k and τ_k are permutations of F, for the distance between different $(q+1)$-tuples in C is at least 3. Since C is a group it follows that σ_k and τ_k are automorphisms of the additive group F. If C is linear over $F = \mathrm{GF}(q)$, then σ_k and τ_k mean multiplication by two nonzero elements of F.

If we apply σ_i to the ith component of every $(q+1)$-tuple in C for $1 \leqq i \leqq q-1$, we find an equivalent group code C' and corresponding automorphisms σ_i' and τ_i' such that σ_i' is the identity and $\tau_i' = (\sigma_i)^{-1}\tau_i$. We can assume that τ_1' is the identity, for in other case we apply $(\tau_1')^{-1}$ to the $(q+1)$st component of every word in C. With the aid of the group property of C' it is now easy to see that the general element in C' has the form (3.1), if $\alpha_i = \tau_i'$ for $1 \leqq i \leqq q-1$.

We shall prove that $\tau_1', \tau_2', \ldots, \tau_{q-1}'$ is a perfect system of automorphisms. Since τ_1' is the identity, it follows then that multiplication can be defined in F such that F becomes a VW system (cf. the end of section 2).

Put $u_j = x$ and $u_k = -x$ for two fixed indices j and k, $1 \leqq j < k \leqq q-1$, and put $u_i = 0$ when $i \neq j, k$, $1 \leqq i \leqq q-1$. From (3.1) it follows that $u_q = 0$ and $u_{q+1} = (x)\tau_j' - (x)\tau_k'$. Since the distance between distinct words in C' is at least 3, it follows that $u_{q+1} \neq 0$ if $x \neq 0$. Hence $\tau_1', \tau_2', \ldots, \tau_{q-1}'$ is a perfect system of automorphisms, and we have proved that C' is a first order F-code. If C is a linear code over $\mathrm{GF}(q)$, we find easily that F is $\mathrm{GF}(q)$.

Note that we did not permute coordinates when we passed from the group code C to the first order F-code C' in the above proof.

Assume that a perfect $(q+1, 1, q)$ linear code C is equivalent with a first order F-code K, where F is a VW system with multiplication denoted by $a \circ b$ to distinguish it from multiplication in $\mathrm{GF}(q)$, which is denoted by ab.

After permutation of coordinates in C we have a linear code C', which is equivalent with K even without assuming permutations of coordinates when passing from C' to K, that is, we need only permute symbols in each coordinate. By a remark is C' equivalent with a first order $\mathrm{GF}(q)$-code even without permutations of coordinates. Hence a first order $\mathrm{GF}(q)$-code C'' is equivalent with a first order F-code even without permutations of coordinates. Let $(u_1, u_2, \ldots, u_{q+1})$ be the general element in K and $(v_1, v_2, \ldots, v_{q+1})$ the general element in C''. We know that

there are permutations π_i such that $v_i=(u_i)\pi_i$ for $1\leqq i\leqq q+1$. We now find by (3.1)

$$(3.2)\qquad (\textstyle\sum_{i=1}^{q-1}u_i)\pi_q = \sum_{i=1}^{q-1}(u_i)\pi_i, \qquad u_1,u_2,\ldots,u_{q-1}\in F\,,$$

$$(3.3)\qquad (\textstyle\sum_{i=1}^{q-1}u_i\circ\alpha_i)\pi_{q+1} = \sum_{i=1}^{q-1}(u_i)\pi_i a_i, \qquad u_1,u_2,\ldots,u_{q-1}\in F\,,$$

where $a_1,a_2,\ldots,a_{q-1}$ are the nonzero elements of GF(q) and $\alpha_1,\alpha_2,\ldots,\alpha_{q-1}$ are the nonzero elements of the VW system F.

Define π_i' by $(u)\pi_i'=(u)\pi_i-(0)\pi_i$ for $1\leqq i\leqq q+1$. If we substitute this into (3.2) and (3.3), we find two equalities of the same type with π_i' in place of π_i everywhere, $1\leqq i\leqq q+1$. Observe that $(0)\pi_i'=0$. By putting $u_i=0$ for every i except one in $1\leqq i\leqq q-1$, we have by the first equality $\pi_i'=\pi_q'$ for $1\leqq i\leqq q-1$, and it follows that π_q' is an automorphism of the abelian group. From the second equality we find similarly

$$(3.4)\qquad (u\circ\alpha_i)\pi'_{q+1} = (u)\pi_q' a_i, \qquad u\in F,\ 1\leqq i\leqq q-1\,.$$

Put $u=1$ in (3.4). We find

$$(3.5)\qquad (\alpha_i)\pi'_{q+1} = (1)\pi_q' a_i, \qquad 1\leqq i\leqq q-1\,.$$

If $\alpha_k=1$, we have by (3.4)

$$(3.6)\qquad (u)\pi'_{q+1} = (u)\pi_q' a_k, \qquad u\in F\,.$$

From (3.4), (3.5) and (3.6) it follows that

$$((1)\pi'_{q+1})((u\circ\alpha_i)\pi'_{q+1}) = ((u)\pi'_{q+1})((\alpha_i)\pi'_{q+1}), \qquad u\in F\,.$$

Since π'_{q+1} is an automorphism of the additive group F, we find that the mapping

$$u\to((u)\pi'_{q+1})((1)\pi'_{q+1})^{-1}$$

is an isomorphism between the VW system F and the finite field GF(q), and the theorem is proved.

With the aid of Theorem 1 and well-known properties of VW systems (cf. section 2), we find the following corollary.

COROLLARY 1. *Perfect $(q+1,1,q)$ group codes exist if and only if q is a power of a prime. If q is a prime or 4 or 8, such a code must be equivalent with a linear code over* GF(q). *If q is neither a prime nor 4 or 8, there is at least one perfect $(q+1,1,q)$ group code which is not equivalent with any linear code.*

PROOF. A perfect $(q+1,1,q)$ group code is equivalent with a first order F-code for some VW system F of order q by Theorem 1. Hence q

is necessarily a power of a prime. If q is a prime or 4 or 8 F must be a finite field and the code is equivalent with a linear code over GF(q). If q is not a prime and $q \neq 4$ and 8, one can find a VW system of order q, which is not a field. In this case a first order F-code can be found, which is not equivalent with a linear code by Theorem 1.

4. On nongroup perfect single-error-correcting codes.

We shall prove a theorem, which generalizes theorems by Ju. L. Vasilev in [14] and J. Schönheim in [9].

We define two functions $m(r,q)$ and $n(r,q)$ for integers $r,q \geqq 2$ by

$$(4.1) \qquad m(r,q) = (q^{r-1}-1)/(q-1), \quad n(r,q) = (q^r-1)/(q-1)\,.$$

In the proof we shall write m instead of $m(r,q)$ and n instead of $n(r,q)$ for brevity.

THEOREM 2. *Let F be a Veblen–Wedderburn system of order q. Given a perfect $(m(r,q),1,q)$ code C and a function λ defined on C with values in F, one can find a perfect $(n(r,q),1,q)$ code K. Distinct pairs (C,λ) will yield distinct codes K. If $q=2$ and $r \geqq 4$ or $q \geqq 3$ and $r \geqq 3$, one can find a perfect $(n(r,q),1,q)$ code K, which is not equivalent with any group code.*

PROOF. If $u \in F^m$ let $p(u)$ be the sum of all m components in u. Let $\alpha_1, \alpha_2, \ldots, \alpha_{q-1}$ be all nonzero elements in F. Write

$$(4.2) \qquad \begin{aligned} u &= (u_1, u_2, \ldots, u_{q-1}, \textstyle\sum_{i=1}^{q-1} u_i, \sum_{i=1}^{q-1} p(u_i)\alpha_i)\,, \\ p(u) &= (p(u_1), p(u_2), \ldots, p(u_{q-1}), \textstyle\sum_{i=1}^{q-1} p(u_i), \sum_{i=1}^{q-1} p(u_i)\alpha_i)\,, \\ v &= (0,0,\ldots,0,w,\lambda(w)), \qquad u_1, u_2, \ldots, u_{q-1} \in F^m, \quad w \in C\,, \end{aligned}$$

where the $(q-1)m$ first components of v are 0.

Let K be the set of all sums $u+v$. Both u and v have dimension $qm+1=n$. The number of elements of C are q^{m-r+1}, for C is a perfect single-error-correcting code. The sums $u+v$ are different. It follows that the number of n-tuples in K is $q^{m(q-1)}q^{m-r+1} = q^{n-r}$. It follows that K is a perfect code, if we can prove that the distance between distinct elements in K is at least 3. We shall prove this now.

Let $u+v$ and $u'+v'$ be two distinct elements of K. We consider three cases.

CASE 1. Assume $v=v'$ and $p(u) \neq p(u')$. From Lemma 1 in section 3 it follows that $\varrho(p(u),p(u')) \geqq 3$. Then $\varrho(u,u') \geqq 3$, and $\varrho(u+v,u'+v') \geqq 3$ follows since $v=v'$.

CASE 2. Assume $v=v'$ and $p(u)=p(u')$. If $u_i \neq u_i'$ for only one i, $1 \leqq i \leqq q-1$, we have $p(u_i)=p(u_i')$ and $\varrho(u_i,u_i') \geqq 2$. Hence $\varrho(u,u') \geqq 4$ by (4.2). If $u_i \neq u_i'$ for at least two i's, then $\varrho(u_i,u_i') \geqq 2$ for these i's, and we find $\varrho(u,u') \geqq 4$ again. Hence $\varrho(u+v,u'+v') \geqq 4$.

CASE 3. Assume $v \neq v'$. Since C is a single-error-correcting code, we have $\varrho(w,w') \geqq 3$. Put

$$\varrho\big((u_1,u_2,\ldots,u_{q-1}),(u_1',u_2',\ldots,u_{q-1}')\big) = k\,. \tag{4.3}$$

We conclude from (4.3)

$$\varrho\big(\textstyle\sum_{i=1}^{q-1} u_i, \sum_{i=1}^{q-1} u_i'\big) \leqq k\,,$$

and then, since $\varrho(w,w') \geqq 3$,

$$\varrho\big(w+\textstyle\sum_{i=1}^{q-1} u_i,\ w'+\sum_{i=1}^{q-1} u_i'\big) \geqq 3-k\,. \tag{4.4}$$

From (4.2), (4.3) and (4.4) it follows that $\varrho(u+v,u'+v') \geqq 3$.

Hence $\varrho(u+v,u'+v') \geqq 3$ in all cases, and we have proved that K is a perfect $(n,1,q)$ code.

It is easy to see that $u+v$ determines u, w and $\lambda(w)$ uniquely. It follows that distinct pairs (C,λ) yield distinct codes K.

Beginning with a trivial code, the construction yields, if it is repeated, perfect $(n(r,q),1,q)$ codes for every $r \geqq 2$. The first nontrivial instance is the first order F-code, which was studied in section 3.

We shall prove the existence of codes K, which are not equivalent with group codes. Assume that $q \geqq 2$ and $r \geqq 4$ or $q \geqq 3$ and $r \geqq 3$. Let C be any perfect $(m,1,q)$ code. Choose the function λ such that it does not take every value in its range the same number of times. This is possible if C has at least 3 elements, which is granted by the assumptions on q and r.

Define K as before and assume that $\overline{K}$ is an equivalent group code. If $u+v$ is an element of K, the corresponding element in $\overline{K}$ is denoted $\overline{u+v}$. We shall use the same symbol 0 for the zero in F and for m-tuples and n-tuples of this zero. The meaning of 0 will be clear from the context. Assume that $\lambda(0)=0$, and $0 \in C$. It follows then $0 \in K$. It is easy to see that the set $G=\{\bar{v}-\bar{0};\ w \in C\}$ is a subgroup of $\overline{K}$. The last component in v is $\lambda(w)$ and the corresponding component in $\bar{v}$ is denoted by $\overline{\lambda(w)}$. The set

$$H = \{\overline{\lambda(w)}-\overline{\lambda(0)};\ w \in C\}$$

is a subgroup of F and the mapping

$$\bar{v}-\bar{0} \to \overline{\lambda(w)}-\overline{\lambda(0)}$$

is a homomorphism of G on H. Hence $\lambda(w)$ takes every value in its range the same number of times, a contradiction.

Theorem 2 is proved.

Let G be an abelian group and A, B two subsets of G such that every element in G can be written uniquely as $a+b$ with $a \in A$ and $b \in B$. Then it is customary to write $G=A+B$ and call this a *factorization* of G (cf. [8]). If G is an abelian group with n base elements $g_1, g_2, \ldots, g_n$ each of order p (a prime), define

$$S = \{0, g_1, 2g_1, \ldots, (p-1)g_1, g_2, 2g_2, \ldots, (p-1)g_2, \ldots, p-1)g_n\}\,. \tag{4.5}$$

Let C be a subset of G such that $G=S+C$ is a factorization, then C is evidently a perfect single-error-correcting code. In [15] S. K. Zaremba posed the question if C is equivalent with a subgroup of G. By Theorem 2 it is seen that this is not in general the case, but it leaves undecided the cases $q=2$, $n=3$, 7 and $p \geqq 3$, $n=p+1$. In the first three cases the answer is positive as S. K. Zaremba [15] and O. Taussky–J. Todd [12] showed.

By Theorem 2 there are at least two equivalence classes of perfect $(n(r,q),1,q)$ codes if $q=2$ and $r \geqq 4$ or $q \geqq 3$ and $r \geqq 3$. By Theorem 1 this is also the case if $r=2$ and q is not a prime and $q \neq 4$, 8. It is easy to prove that the number of equivalence classes tends to infinity with r. For the number of codes in an equivalence class is at most $n!\,(q!)^n < q^{n(q+\log n)}$ (q-logarithm) and the number of different codes K for different λ is at least q^{q^u}, where $u=(n-1)/q-{}^q\log n$, by Theorem 2.

If $G=A+B$ is a factorization of G, an element $g \in G$ such that $g+A=A$, $g \neq 0$ is said to be a *period* of A. The codes constructed in Theorem 2 have a large number of periods. It would be interesting to know if there are perfect $(n,1,q)$ codes with a small number of periods. There is an interesting theorem by J.-E. Roos (Theorem 4 in [7]) from which it follows that every perfect $(n,e,2)$ code has at least one period.

REFERENCES

1. A. A. Albert and R. Sandler, *An introduction to finite projective planes*, Holt, New York, 1968.
2. E. F. Assmus, Jr. and H. F. Mattson, Jr., *On tactical configurations and error-correcting codes*, J. Combinatorial Theory 2 (1967), 243–257.
3. E. R. Berlekamp, *Algebraic coding theory*, McGraw–Hill, New York, 1968.
4. M. Hall, Jr., *Combinatorial theory*, Blaisdell, Waltham, Mass., 1967.
5. M. Hall, Jr., J. Dean and R. J. Walker, *Uniqueness of the projective plane of order eight*, Math. Comp. 10 (1956), 186–194.

6. J. G. Kalbfleisch and R. G. Stanton, *A combinatorial problem in matching*, J. London Math. Soc. 44 (1968), 60–64.
7. J.-E. Roos, *An algebraic study of group and nongroup error-correcting codes*, Information and Control 8 (1965), 195–214.
8. A. D. Sands, *Factorization of cyclic groups*, Proc. Colloq. Abelian Groups, ed. L. Fuchs and E. T. Schmidt, Budapest 1964, 139–146.
9. J. Schönheim, *On linear and nonlinear single-error-correcting q-nary perfect codes*, Information and Control 12 (1968), 23–26.
10. R. G. Stanton and J. D. Horton, *Some results on perfect covering sets* (submitted).[1]
11. R. G. Stanton and J. G. Kalbfleisch, *Covering problems for dichotomized matchings*, Aequationes Math. 1 (1968), 94–103.
12. O. Taussky and J. Todd, *Covering theorems for groups*, Ann. Soc. Polon. Math. 21 (1948), 303–305.
13. O. Taussky and J. Todd, *Some discrete variable computations*, Proc. Symp. Appl. Math. 10, Amer. Math. Soc., 1960, 201–209.
14. Ju. L. Vasilev, *On non-group close-packed codes*, Probl. Kibernet. 8 (1962), 337–339 (in Russian), Transl. in Probleme der Kybernetik 8 (1965), 375–378.
15. S. K. Zaremba, *Covering problems concerning abelian groups*, J. London Math. Soc. (2) 27 (1952), 242–246.

[1] Added in proof: The paper is withdrawn. For a substitute see S.W. Colomb and E.C. Posner, *Rook domains, latin squares, affine planes and error-distributing codes*, IEEE Trans. Information Theory, vol. IT-10 (1964), 196–208.

UNIVERSITY OF STOCKHOLM, SWEDEN