MAC TECHNICAL MEMORANDUM 44

SYMMETRY CODES AND THEIR INVARIANT SUBCODES

Vera Pless

May 1974

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

PROJECT MAC

CAMBRIDGE MASSACHUSETTS 02139

Symmetry Codes and Their Invariant Subcodes

Abstract

We define and study the invariant subcodes of the symmetry codes in order to be able to determine the algebraic properties of these codes. An infinite family of self-orthogonal rate 1/2 codes over GF(3), called symmetry codes, were constructed in [3]. A $(2q + 2, q + 1)$ symmetry code, denoted by $C(q)$, exists whenever q is an odd prime power $\equiv -1$, (mod 3). The group of monomial transformations leaving a symmetry code invariant is denoted by $G(q)$. In this paper we construct two subcodes of $C(q)$ denoted by $R_\sigma(q)$ and $R_\mu(q)$. Every vector in $R_\sigma(q)$ is invariant under a monomial transformation τ in $G(q)$ of odd order s where s divides $(q + 1)$. Also $R_\mu(q)$ is invariant under τ but not vector-wise. The dimensions of $R_\sigma(q)$ and $R_\mu(q)$ are determined and relations between these subcodes are given. An isomorphism is constructed between $R_\sigma(q)$ and a subspace of $W = V_3^{\frac{2q+2}{s}}$. It is shown that the image of $R_\sigma(q)$ is a self-orthogonal subspace of W. The isomorphic images of $R_\sigma(17)$ (under an order 3 monomial) and $R_\sigma(29)$ (under an order 5 monomial) are both demonstrated to be equivalent to the (12, 6) Golay code.

Dr. Vera Pless
Project MAC
Massachusetts Institute of Technology
545 Technology Square, Rm. 830
Cambridge, Massachusetts 02139

Symmetry Codes and Their Invariant Subcodes

by

Dr. Vera Pless
Project MAC

I. Introduction.

This paper defines and studies the invariant subcodes of the symmetry codes which were originally defined in [3]. The purpose of this study is the illucidation of properties of these subcodes in such a manner that these properties can be applied in determining characteristics of the symmetry code itself. For example, maximum length vectors in C(17) and C(29) can be determined from known maximum length vectors in the Golay code C(5). The minimum weights are known for the first five symmetry codes. Estimates of the minimum weights of the larger symmetry codes have been obtained by locating a vector of weight 21 in $R_\sigma(41)$ (under an order 7 monomial) and a vector of weight 27 in $R_\sigma(53)$ (under an order 3 monomial). An (n, k) error correcting code over GF(3) is a k-dimensional subspace of $V_3{}^n = V$. The weight of a vector x, denoted by w(x), is the number of non-zero components it has. Symmetry codes are an infinite family of (2q + 2, q + 1) codes over GF(3) where q is an odd prime power $\equiv -1 \pmod 3$. Each code is given in terms of a basis $[I, S_q]$ where I is the q x q identity matrix and S_q is the matrix described below.

We consider the elements of GF(q) to be ordered in some fixed way, and with this ordering we label the first q + 1 coordinates with the elements of GF(q)$\cup$ $\{\infty\}$ with ∞ taken as the first coordinate. We label the second q + 1 coordinates by the same sequence of elements of

$GF(q) \cup \{\infty\}$ with dashes on them to distinguish them from the first $q + 1$ coordinate labels. When $q = p$ is a prime, for convenience we use the ordering $\infty, 0, 1, \ldots, p-1$ (and hence also $\infty', 0', 1', \ldots, (p-1)'$ for the right side). By definition, S_q is the $(q + 1) \times (q + 1)$ matrix $(s_{i', j'})$, i, j in $GF(q) \cup \{\infty\}$, such that $s_{\infty', \infty'} = 0$ and for $i', j' \neq \infty'$, $s_{i', \infty'} = \chi(-1)$, $s_{\infty', i'} = 1$, and $s_{i', j'} = \chi(j-i)$ where $\chi(0) = 0$, χ (a quadratic residue) $= 1$, χ (a non-residue) $= -1$. We refer to the code generated by $[I, S_q]$ as $C(q)$.

As a concrete example we write the basis for $C(5)$ below.

∞	0	1	2	3	4	∞'	0'	1'	2'	3'	4'
1	0	0	0	0	0	0	1	1	1	1	1
0	1	0	0	0	0	1	0	1	-1	-1	1
0	0	1	0	0	0	1	1	0	1	-1	-1
0	0	0	1	0	0	1	-1	1	0	1	-1
0	0	0	0	1	0	1	-1	-1	1	0	1
0	0	0	0	0	1	1	1	-1	-1	1	0

$C(5)$ is a $(12, 6)$ code and it is equivalent to the Golay code [2].

In [4] it was shown that each symmetry code is self orthogonal. The transformations on V which preserve the weights of all vectors are the monomial transformations. A monomial transformation can be viewed as a permutation of the coordinate indices of the vectors in V (the same permutation for each vector) coupled with multiplying some (or none) of the coordinates by minus one. The set of monomial transformations which send all the vectors in $C(q)$ onto vectors in $C(q)$ form a group denoted by $G(q)$. In [4] it was shown that $G(q)$ contains $PGL_2(q)$.

In section II of this paper we construct two subcodes of $C(q)$ denoted by $R_\sigma(q)$ and $R_\mu(q)$. Every vector in $R_\sigma(q)$ is invariant under a monomial transformation τ in $G(q)$ of odd order s where s divides $q + 1$. Also $R_\mu(q)$ is invariant under τ but not vector-wise invariant. The dimensions of $R_\sigma(q)$ and $R_\mu(q)$ are determined and relations between these subcodes are given. In section III an isomorphism is constructed between $R_\sigma(q)$ and a subspace of $W = V_3^{\frac{2q+2}{s}}$. It is shown that the image of $R_\sigma(q)$ is a self-orthogonal subspace of W. In section IV the isomorphic images of $R_\sigma(17)$ $(o(\tau) = 3)$ and $R_\sigma(29)$ $(o\ (\tau) = 5)$, are both demonstrated to be equivalent to the (12, 6) Golay code.

II. In this section we construct two subcodes of $C(q)$, $R_\sigma(q)$ and $R_\mu(q)$ with the following properties. Every vector in $R_\sigma(q)$ is invariant under a monomial transformation τ in $G(q)$ where the order of τ is an odd number s dividing $q + 1$. Further, $R_\mu(q)$ is also invariant under but not vector-wise invariant. The dimensions of R_σ and R_μ are determined, and relations between them are given.

In [4] it was shown that the mapping sending a monomial transformation τ in $G(q)$ onto the permutation $\bar{\tau}$ it induces on the coordinate indices is a homomorphism of a subgroup of $G(q)$ onto $PGL_2(q)$ whose kernel has order 2. For the rest of this paper τ denotes a monomial transformation in $G(q)$ of odd order s where s divides $(q + 1)$ such that $\bar{\tau}$ is in $PGL_2(q)$ and the order of τ equals the order of $\bar{\tau}$.

Lemma 1. If s is an odd number dividing $(q + 1)$, then there exists a transformation $\bar{\tau}$ in $G(q)$ or order s. Further $\bar{\tau}$ is in $PGL_2(q)$.

Proof: By [1] it is known that $PGL_2(q)$ contains a cyclic subgroup of order $\frac{(q+1)}{2}$. Hence this subgroup contains an element $\bar{\tau}$ of order s when s is any odd number dividing $(q + 1)$. The monomial τ in $G(q)$ which maps into $\bar{\tau}$ by the homomorphism described above is either of order s or 2s. If it is of order s we are finished. If τ is of order 2s then τ^2 is of order s, $\bar{\tau}^2$ is also of order s (since s is odd), $\bar{\tau}^2$ is in $PGL_q(q)$ and the lemma is demonstrated.

The subcodes $R_\sigma(q)$ and $R_\mu(q)$ are the ranges of two linear transformations σ and μ defined for x in $C(q)$ as follows.

$$x\sigma = x + x\tau + \ldots + x\tau^{s-1}$$

$$x\mu = x - x\tau$$

Even though σ and μ are linear transformations, they are not monomial transformations; they are useful in obtaining information about τ. Let $K_\sigma(q)$ denote the kernel of σ and $K_\mu(q)$ the kernel of μ.

Theorem 1. $R_\sigma(q)$, $R_\mu(q)$, $K_\sigma(q)$, $K_\mu(q)$ are subcodes of $C(q)$ such that

1) $R_\sigma(q)$ is contained in $K_\mu(q)$ and $R_\mu(q)$ is contained in $K_\sigma(q)$, and
2) τ leaves $R_\mu(q)$ invariant and τ leaves every vector in $R_\sigma(q)$ invariant.

Proof: It is clear that $R_\sigma(q)$, $R_\mu(q)$, $K_\sigma(q)$ are subcodes since they are vector subspaces contained in $C(q)$. If $x\sigma$ is in $R_\sigma(q)$ then $(x\sigma)\mu = (x + x\tau + \ldots + x\tau^{s-1})\mu = (x + x\tau + \ldots x\tau^{s-1}) - (x\tau + x\tau^2 + \ldots + x\tau^{s-1} + x) = 0$ so that $R_\sigma(q)$ is contained in $K_\mu(q)$. Similarly $R_\mu(q)$ is contained in $K_\sigma(q)$. If $x\sigma$ is in $R_\sigma(q)$, then $(x\sigma)\tau = (x + x\tau + \ldots + x\tau^{s-1})\tau = x\tau + x\tau^2 + \ldots x\tau^{s-1} + x = x\sigma$ and we see that τ leaves every vector in $R_\sigma(q)$ invariant. Since $(x\mu)\tau = x\tau - x\tau^2$, τ leaves $R_\mu(q)$ invariant and the theorem is proved.

Remark: When s is divisible by 3, $R_\sigma(q)$ is contained in $K_\sigma(q)$.

Proof: If y is in $R_\sigma(q)$, $y = x\sigma = x + x\tau + \ldots + x\tau^{s-1}$. Hence $y\sigma = (x + x\tau + \ldots x\tau^{s-1})\sigma = sy \equiv 0 \pmod 3$.

Lemma 2. $\bar{\tau}$ is a product of disjoint cycles of length s. Further, if $(i_1, \ldots, i_s)$ is such an s-cycle for the left coordinate indices of V, then $(i_1', \ldots, i_s')$ is such an s-cycle for the right coordinate indices of V.

Proof: By their construction [4] the transformations in $PGL_2(q)$ act on the left coordinate indices (and simultaneously on the right coordinate indices) as transformations on the projective line. Since s is an odd number which divides q + 1, $\bar{\tau}$ is either completely a product of disjoint cycles of length s or a product of disjoint cycles of length s with ks fixed points. But a projective transformation with three fixed points is the identity. Hence $\bar{\tau}$ can have at most two fixed points on each side of coordinate indices. Since s divides q + 1, the number of left coordinate indices (and the number of right coordinate indices), this is only possible for k = 1 and s = 2. The lemma follows from the fact that s is an odd number.

We let J be a set of left coordinate indices with the property that J contains exactly one index from each of these s cycles. Note that $|J| = \frac{(q + 1)}{s}$.

In order to determine the dimension of $R_\sigma(q)$ and $R_\mu(q)$ we introduce the following terminology. We let the vectors in the basis $[I, S_q]$ be denoted by $(e_i, c(e_i))$ where e_i is the $i^{\underline{th}}$ row of I and $c(e_i)$ is the $i^{\underline{th}}$ row of S_q.

Theorem 2. dim $R_\sigma(q) = \frac{(q + 1)}{s}$ and dim $R_\mu(q) = \frac{(q + 1)(s - 1)}{s}$.

Proof: Consider the set of $\frac{(q + 1)}{s}$ vectors $\{(e_j + e_j\tau + \ldots + e_j\tau^{s-1}, c(e_j) + c(e_j)\tau + \ldots + c(e_j)\tau^{s-1})\}$ for $j\varepsilon J$. Since the order of τ equals the order of $\overline{\tau}$, $e_j \neq \pm e_j \tau^i$, $1 \leqq i \leqq s - 1$, so that $(e_j + e_j\tau + \ldots + e_j \tau^{s-1}) \neq 0$ for each $j \in J$. Hence by the definition of J, these vectors are linearly independent. Clearly they span $R_\sigma(q)$, and it thus follows that dim $R_\sigma(q) = |J| = \frac{q + 1}{s}$. Similarly $\{ (e_j\tau^k - e_j\tau^{k+1}), (c(e_j)\tau^k - c(e_j)\tau^{k+1})\}$ for $j\varepsilon J$, $k = 0, \ldots, s - 2$ is a basis of $R_\mu(q)$. Hence dim $R_\mu(q) = \frac{(q + 1)(s - 1)}{s}$.

Remark: When τ has even order ($\neq 2$) which divides $\frac{(q + 1)}{2}$, all the results of this paper hold when the order of τ equals the order of $\overline{\tau}$. When the order of τ equals twice the order of $\overline{\tau}$, then it is possible that Theorem 2 does not hold since the basis vectors described above can be zero.

Corollary 1. $R_\sigma(q) = K_\mu(q)$ and $R_\mu(q) = K_\sigma(q)$.

Proof: By Theorem 1, $R_\mu(q)$ is contained in $K_\sigma(q)$ and $R_\sigma(q)$ is contained in $K_\mu(q)$. In general, dim $R_\mu(q)$ + dim $K_\mu(q) = q + 1 =$ dim $K_\sigma(q)$ + dim $R_\sigma(q)$. By Theorem 2, dim $R_\sigma(q) = \frac{(q + 1)}{s}$ and dim $R_\mu(q) = \frac{(q + 1)(s - 1)}{s}$. Hence dim $R_\mu(q) =$ dim $K_\sigma(q)$ and dim $R_\sigma(q) =$ dim $K_\mu(q)$ and the corollary is demonstrated.

Note that since 3 divides $(q + 1)$ for every $q \equiv -1 (\text{mod } 3)$, every symmetry code has a monomial transformation of order 3 leaving it invariant.

III. The isomorphic image of R_σ.

In this section we construct a linear transformation φ from V onto $W = V_3^{\frac{2q+2}{s}}$ where s is again an odd number dividing q + 1 with the following properties. The dimension of $\varphi(R_\sigma)$ equals the dimension of R_σ, the weight of $\varphi(x)$ for x in R_σ is the weight of x divided by s, and $\varphi(R_\sigma)$ is a self-orthogonal subspace of W.

In order to do this we let J be as in section II, and let J' be the elements in J with dashes on them. Note that $J \cup J'$ contains $\frac{2(q+1)}{s}$ elements. We consider the elements in J to have the same ordering they had in $GF(q) \cup \{\infty\}$. With this ordering we label the left half of the coordinate indices in W with the elements from J, and the right half with the elements from J'. We denote the unit vectors in W by $\bar{e}_j$, j in J and $\bar{e}_j'$, j' in J'.

Lemma 3. If $x\tau = x$, then the components of x on a cycle of $\bar{\tau}$ are either all zero or all non-zero. Further, if $x\tau = x$ and $y\tau = y$, then on the cycles of $\bar{\tau}$ on which the components of both x and y are non-zero, the components of x equal plus or minus the components of y.

Proof: Let $(i_1,\ldots,i_s)$ be the coordinate indices of a cycle of $\bar{\tau}$. Let x_{i_j} be the $i_j^{\underline{th}}$ component of x. If $x\tau = x$, then all the components of x on this cycle are determined by x_{i_1} and τ. If $y\tau = y$ also, then the components of x on this cycle equal the components of y on this cycle of $x_{i_1} = y_{i_1}$. If $x_{i_1} = -y_{i_1}$ the components of x on this cycle are the negatives of the components of y. Since these are the only possibilities, the lemma is proved.

Theorem 3. There is a linear transformation φ from V onto $W = V_3^{\frac{2q+2}{s}}$ such that 1) $\dim \varphi(R_\sigma(q)) = \dim R_\sigma(q) = \frac{(q+1)}{s}$, and

2) $w(\varphi(x)) = \frac{w(x)}{s}$.

Proof: We let e_i and e_i', $i \in GF(q) \cup \{\infty\}$ denote the unit vectors in V. We define φ on these unit vectors as follows.

If $j \in J$, $\varphi(e_j) = \bar{e}_j$. If $i \notin J$, $\varphi(e_i) = 0$.

If $j' \in J'$, $\varphi(e_j') = \bar{e}_j'$. If $i' \notin J'$, $\varphi(e_i') = 0$.

Define φ on the rest of V linearly. Clearly φ is a linear transformation from V onto W.

Recall that $\{(e_j + e_j\tau + \ldots + e_j\tau^{s-1}, c(e_j) + c(e_j)\tau + \ldots + c(e_j)\tau^{s-1})\}$, $j \in J$ is a basis of $R_\sigma(q)$. Since φ maps these vectors onto linearly independent vectors, $\dim \varphi(R_\sigma(q)) = \dim R_\sigma(q) = \frac{(q+1)}{s}$ by Theorem 2.

Theorem 1 tells us that $x\tau = x$ for all x in $R_\sigma(q)$. By Lemma 3 we know that the components of x on a cycle of $\bar{\tau}$ are either all zero or all non-zero. Since φ projects on precisely one component from each s-cycle of $\bar{\tau}$, $w(\varphi(x)) = \frac{w(x)}{s}$.

It was proven in [4] that C(q) is a self-orthogonal subspace of V so that $R_\sigma(q)$ is certainly a self-orthogonal subspace of V. Even though φ does not preserve the property of self-orthogonality, we can prove that $\varphi(R_\sigma(q))$ is a self-orthogonal subspace of W.

Theorem 4. $\varphi(R_\sigma(q))$ is a self-orthogonal subspace of W.

Proof: Let x and y be vectors in W such that $x = (\alpha_1, \ldots, \alpha_{\frac{2q+2}{s}})$ and $y = (\beta_1, \ldots, \beta_{\frac{2q+2}{s}})$. Then the inner product of x and y, denoted by (x,y), is $\left(\sum_{i=1}^{\frac{2q+2}{s}} \alpha_i \beta_i\right) \pmod 3$. As is usual, x and y are orthogonal to each other if $(x,y) = 0$. In order to prove Theorem 4 we need to show that $(x,y) = 0$ for all x,y in $\varphi(R_\sigma(q))$ (x can also equal y). In order to prove this, we introduce the inner product of x and y over the integers, denoted by $[x,y]$, where $[x,y]$ equals $\sum_{i=1}^{\frac{2q+2}{s}} \alpha_i\beta_i$ by definition. We define $[x,y]$ in a similar fashion for x and y in V.

The proof of Theorem 4 is divided into two cases. The first case is 3 does not divide s. If x and y are in $R_\sigma(q)$, then $x = x_1 + x_1\tau + \dots + x_1\tau^{s-1}$ and $y = y_1 + y_1\tau + \dots + y_1\tau^{s-1}$ for some x_1 and y_1 in $C(q)$. By Lemma 3, all the elements in $R_\sigma(q)$ which are not zero on a particular cycle of $\bar{\tau}$ have the same or opposite components on that cycle. Hence $[x,y] = rs$ where r is the number of s-cycles of $\bar{\tau}$ (in both the left and right coordinates) in which both x and y have non-zero components. Since $(x,y) = 0$, 3 divides rs, but by assumption 3 does not divide s so that 3 divides r. By the definition of φ, $[\varphi(x), \varphi(y)] = r$ so that $(\varphi(x), \varphi(y)) = 0$ for all x,y in $R_\sigma(q)$. Hence $\varphi(R_\sigma(q))$ is self-orthogonal in this situation. We now consider the case that $s = 3j$, i.e., $\tau^{3j} = 1$. We let x and y be in $R_\sigma(q)$, and we have $x = x_1 + x_1\tau + \dots + x_1\tau^{3j-1}$, $y = y_1 + y_1\tau + \dots y_1\tau^{3j-1}$ for x_1, y_1 in $C(q)$. Then

$$[x,y] = \sum_{i=0}^{3j-1} [x_1, y_1\tau^i] + \sum_{i=0}^{3j-1} [x_1\tau, y_1\tau^i] + \dots + \sum_{i=0}^{3j-1} [x_1\tau^{3j-1}, y_1\tau^i]$$

$$= \sum_{i=0}^{3j-1} [x_1\tau^i, y_1\tau^i] + \sum_{i=0}^{3j-1} [x_1\tau^i, y_1\tau^{i+1}] + \dots + \sum_{i=0}^{3j-1} [x_1\tau^i, y, \tau^{i+3j-1}]$$

by rearranging terms. Now $[u,v] = [u\tau^i, v\tau^i]$ for all u and v in V

since τ^{i} is a monomial transformation over GF(3). Hence $[x,y] = 3j[x_1, y_1] + 3j[x_1, y_1\tau] + \ldots + 3j[x_1, y_1\tau^{3j-1}]$. Since x_1 and $y_1\tau^{i}(i=0,..,3j-1)$ are all in C(q) which is self-orthogonal, each $[x_1, y_1\tau^{i}]$ is divisible by 3 so that $[x,y] = 9r$ for some r. Each cycle of $\bar{\tau}$ is a 3j-cycle, and by the definition of φ, φ projects onto one coordinate from each 3j-cycle so that $[\varphi(x), \varphi(y)] = 3r$. Hence $(\varphi(x), \varphi(y)) = 0$, and $\varphi(R_\sigma(q))$ is a self-orthogonal subspace of W for this case also.

IV. Invariant subcodes of C(17) and C(29) are isomorphic to the Golay code.

In this section we apply these ideas to C(17) and C(29). The τ for C(17) has order 3 and the τ for C(29) has order 5. We describe these two monomial transformations explicitly, and exhibit bases for $R_\sigma(17)$ and $\varphi(R_\sigma(17))$.

In order to exhibit these monomial transformations we introduce the following convention. We let $\overline{\chi(i)}$ times a column index mean that we multiply the column by $\chi(i)$ where $\chi(i) = 1$ for i a quadratic residue, and $\chi(i) = -1$ for i a non-residue. This convention is used in order to avoid confusion with negatives in GF(17).

We can represent τ as a monomial transformation on the columns of V as follows.

$$\tau(\infty) = 0, \quad \tau(16) = \infty; \quad \tau(i) = \overline{\chi(i+1)} \ \left(\frac{16}{i+1}\right), \ i \neq \infty, 16;$$

$$\tau(\infty') = 0', \quad \tau(16') = \infty'; \ \tau(i') = \overline{\chi(i'+1)} \left(\frac{16}{i+1}\right), \ i' \neq \infty', 16'.$$

The generators of the subgroup of G(17) which is isomorphic to $PGL_2(17)$ are given in [4, p. 131]. It is easy to verify that τ is a product of two of these generators so that τ is in G(17). A straightforward check shows that τ has order 3. If we rearrange the columns of V to correspond to the cycles of $\bar{\tau}$, the following is a basis of $R_\sigma(17)$.

∞ 0 16	1 8 15	2 11 7	3 4 10	5 14 9	6 12 13	∞' 0' 16'	1' 8' 15'	2' 11' 7'	3' 4' 10'	5' 14' 9'	6' 12' 13'
1 1 1						-1 -1 -1		1 -1 1	1 1 -1	-1 1 1	-1 1 1
	1 1 1						1 1 1	1 -1 1	-1 -1 1	-1 1 1	1 -1 -1
		1 -1 1				1 1 1	1 1 1	1 -1 1	1 1 -1	1 -1 -1	
			1 1 -1			1 1 1	-1 -1 -1	1 -1 1	-1 -1 1		-1 1 1
				1 -1 -1		-1 -1 -1	-1 -1 -1	1 -1 1		1 -1 -1	1 -1 -1
					1 -1 -1	-1 -1 -1	1 1 1		-1 -1 1	1 -1 -1	-1 1 1

From this we get the following basis for $\varphi(R_\sigma(17))$ by choosing $J = \{\infty,1,2,3,5,6\}$.

∞	1	2	3	5	6	∞'	1'	2'	3'	5'	6'
1						-1		1	1	-1	-1
	1						1	1	-1	-1	1
		1				1	1	1	1	1	
			1			1	-1	1	-1		-1
				1		-1	-1	1		1	1
					1	-1	1		-1	1	-1

It is known [4] that the minimum weight of C(17) is 18, so that the minimum weight of $\varphi(R_\sigma(17))$ is 6. It follows from the theorem in [2] that $\varphi(R_\sigma(17))$ is equivalent to the Golay (12, 6) code over GF(3).

A monomial transformation τ of order 5 in G(29) is given by the following.

$$\tau(\infty) = 0,\ \tau(24) = \infty;\quad \tau(i) = \overline{\chi(i+5)}\left(\frac{28}{i+5}\right),\ i \neq \infty,\ 24,$$

$$\tau(\infty') = 0',\quad \tau(24') = \infty';\quad \tau(i') = \overline{\chi(i'+5)}\left(\frac{28}{i'+5}\right),\ i' \neq \infty',\ 24'.$$

As in the previous case it can be verified that τ is a product of generators of the subgroup of $G(29)$ which is isomorphic to $PGL_2(29)$. Given τ, a basis of $R_\sigma(29)$ can be computed similar to the basis of $R_\sigma(17)$. The minimum weight in $C(29)$ is 18 and since the weight of every vector in $R_\sigma(29)$ is divisible by 5, the minimum weight of $R_\sigma(29)$ must be at least 30. It is exactly 30 since the basis vectors have weight 30. Hence the minimum weight of $\varphi(R_\sigma(29))$ is 6. It then follows as above that $\varphi(R_\sigma(29))$ is equivalent to the Golay Code.

I wish to thank Jean-Marie Goethals for pointing out to me that the results of this paper are applicable to a wider class of monomials than I originally stated.

Bibliography

1. Dickson, L. E. (1901, 1958) "Linear Groups with an Exposition of the Galois Field Theory", reprinted by Dover Publications, New York.

2. V. Pless, "On the uniqueness of the Golay codes", J. of Combinatorial Theory, 5 (1968), 215-228.

3. V. Pless, "On a new family of symmetry codes and related new five-designs", Bulletin of the American Mathematical Society, Vol. 75, No. 6 (1969), 1339-1342.

4. V. Pless, "Symmetry codes over GF(3) and new five-designs", J. of Combinatorial Theory, 12 (1972), 119-142.

BIBLIOGRAPHIC DATA SHEET

1. Report No. MAC TM-44	2.	3. Recipient's Accession No.	

4. Title and Subtitle

Symmetry Codes and their Invariant Subcodes

5. Report Date : Issued May 1974

6.

7. Author(s)

Vera Pless

8. Performing Organization Rept. No. MAC TM- 44

9. Performing Organization Name and Address

PROJECT MAC; MASSACHUSETTS INSTITUTE OF TECHNOLOGY:

545 Technology Square, Cambridge, Massachusetts 02139

10. Project/Task/Work Unit No.

11. Contract/Grant No.

N00014-70-A-0362-0006

12. Sponsoring Organization Name and Address

Office of Naval Research
Department of the Navy
Information Systems Program
Arlington, Va 22217

13. Type of Report & Period Covered: Interim Scientific Report

14.

15. Supplementary Notes

16. Abstracts : The paper defines and studies the invariant subcodes, $R_\sigma(q)$ and $R_\mu(q)$, of the symmetry code $C(q)$ in order to be able to determine the algebraic properties of these codes. Every vector in $R_\sigma(q)$ is invariant under a monomial transformation τ, of odd order dividing $(q + 1)$, in the group of $C(q)$. Also $R_\mu(q)$ is invariant under τ but not vector-wise. The dimensions of $R_\sigma(q)$ and $R_\mu(q)$ are determined and relations between these subcodes are given. Also $R_\sigma(q)$ is shown to be isomorphic to a self-orthogonal subspace of $V_3^{\frac{2q+2}{s}}$. The isomorphic images of $R_\sigma(17)$ and $R_\sigma(29)$ are both demonstrated to be equivalent to the (12,6) Golay code.

17. Key Words and Document Analysis. 17a. Descriptors

17b. Identifiers/Open-Ended Terms

17c. COSATI Field/Group

18. Availability Statement

Approved for Public Release;
Distribution Unlimited

19. Security Class (This Report) UNCLASSIFIED

20. Security Class (This Page UNCLASSIFIED

21. No. of Pages 16

22. Price