(case $n_{d+2} = 1$) will never occur. Rather, for all practical codes, B will typically fall midway between the two extreme bounds in (6.5), thus offering even greater storage savings. In comparison, direct implementations of the enumeration schemes by Gu and Fuja [9] as well as Patrovics and Immink [10] require a table size proportional to Rn^2. For the large values of n required for near-capacity-achieving codes, a table size of tRn is (in many cases) feasible, whereas Rn^2 is not.

As an alternative to a direct implementation of [10], Immink [7] suggests the use of a floating-point representation of the weights. At the cost of a small loss in code rate, this alternate representation reduces the table size from Rn^2 to sn, where s is the number of bits used to represent both the mantissa and exponent of each weight. Despite this storage reduction, a straightforward application of the permutation code enumeration will still have smaller memory requirements than even this new floating-point scheme if $tR < s$ (again, assuming worst possible conditions on B). And, since B will typically be much smaller than tRn, the likelihood of improved memory requirements over those of [7] is extremely high. Consequently, there is an acceptable "window" by which we can increase the permutation code block length n in order to achieve the same efficiencies as the constructions in [7], [9], and [10] while maintaining lower complexity memory requirements. In cases where this window is exceeded, Immink's method [7] may be preferred.

Another option is to implement a floating-point version of the permutation code enumeration. Although this would incur a small loss in code rate, the memory requirements would be drastically improved. Specifically, the table size B would be reduced to $B = pt = p[4(k-d)-1]$ where p is the precision of the new numbering system. As such, the "window" by which n can be increased is tremendously larger than that associated with a direct, fixed-point implementation. Hence, this option offers even greater potential for improvements in storage requirements over the enumeration scheme of [7].

VII. Conclusions

We have introduced an enumeration scheme which encodes and decodes high-efficiency runlength-limited permutation codes with very low complexity. Unlike other enumerative techniques, the permutation codes offer error detection and correction capabilities as well as a significant savings in storage requirements. As an example, a 99.2% efficient, rate 496/528, $(0, 6/3)$ code has been presented.

Acknowledgment

The authors wish to thank Kees A. Schouhamer Immink whose comments allowed for a more balanced presentation of this work.

References

[1] E. Zehavi and J. K. Wolf, "On runlength codes," *IEEE Trans. Inform. Theory*, vol. 34, pp. 45–55, Jan. 1988.

[2] J. K. Wolf, "Permutation codes, (d, k) codes and magnetic recording," in *Proc. 1990 IEEE Colloq. in South America. Argentina, Brazil, Chile, Uruguay*, W. Tompkins, Ed., Sept. 1990.

[3] N. S. Szabo and R. I. Tanaka, *Residue Arithmetic and its Application to Computer Technology.* New York: McGraw-Hill, 1967.

[4] D. H. Lehmer, "The machine tools of combinatorics," in *Applied Combinatorial Mathematics*, E.F. Beckenbach, Ed. New York: Wiley, 1964, pp. 5–31.

[5] W. G. Bliss, "Circuitry for performing error correction calculations on baseband encoded data to eliminate error propagation," *IBM Tech. Discl. Bul.*, vol. 23, pp. 4633–4634, 1981.

[6] M. Mansuripur, "Enumerative modulation coding with arbitrary constraints and post-modulation error correction coding and data storage systems," *Proc. SPIE*, vol. 1499, pp. 72–76, 1991.

[7] K. A. S. Immink, "A practical method for approaching the channel capacity of constrained channels," *IEEE Trans. Inform. Theory*, vol. 43, pp. 1389–1399, Sept. 1997.

[8] J. L. Fan and A. R. Calderbank, "A modified concatenated coding scheme, with applications to magnetic data storage," *IEEE Trans. Inform. Theory*, submitted for publication Dec. 1997.

[9] J. Gu and T. Fuja, "A new approach to constructing optimal block codes for runlength-limited channels," *IEEE Trans. Inform. Theory*, vol. 40, pp. 774–785, May 1994.

[10] L. Patrovics and K. A. S. Immink, "Encoding of $dklr$-sequences using one weight set," *IEEE Trans. Inform. Theory*, vol. 42, pp. 1553–1554, Sept. 1996.

[11] D. Slepian, "Permutation modulation," *Proc. IEEE*, vol. 53, pp. 228–236, Mar. 1965.

[12] B. Marcus, P. Siegel, and J. Wolf, "Finite state modulation codes for data storage," *IEEE J. Select. Areas Commun.*, vol. 10, pp. 5–36, Jan. 1992.

[13] T. Berger, F. Jelinek, and J. K. Wolf, "Permutation codes for sources," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 160–169, Jan. 1972.

Representing Group Codes as Permutation Codes

Ezio Biglieri, *Fellow, IEEE*, John K. Karlof, *Senior Member, IEEE*, and Emanuele Viterbo, *Member, IEEE*

***Abstract*—Given an abstract group $\mathcal{G}$, an N-dimensional orthogonal matrix representation $\boldsymbol{G}$ of $\mathcal{G}$, and an "initial vector" $\boldsymbol{x} \in \boldsymbol{R}^N$, Slepian defined the group code generated by the representation $\boldsymbol{G}$ to be the set of vectors $\boldsymbol{Gx}$. If $\boldsymbol{G}$ is a group of permutation matrices, the set $\boldsymbol{Gx}$ is called a "permutation code." For permutation codes a "stack algorithm" decoder exists that, in the presence of low noise, produces the maximum-likelihood estimate of the transmitted vector by using far fewer computations than the standard decoder. In this correspondence, a new concept of equivalence of codes of different dimensions is presented which is weaker than the usual definition of equivalent codes. We show that every group code is (weakly) equivalent to a permutation code and we discuss the minimal degree of this permutation code.**

***Index Terms*—Gaussian channel, group codes, permutation codes.**

I. Introduction

Group codes, as defined by Slepian (see [10] and references therein) are defined as follows.[1] Consider a group $\boldsymbol{G}$ of $N \times N$ orthogonal matrix which forms an injective representation of an

Manuscript received September 28, 1997; revised April 9, 1999. This work was sponsored by CNR under "Progetto Finalizzato Trasporti."

E. Biglieri and E. Viterbo are with Dipartimento di Elettronica, Politecnico di Torino, I-10129 Torino, Italy.

J. K. Karlof is with the Mathematical Sciences Department, University of North Carolina, Wilmington, NC 28403 USA.

Communicated by A. M. Barg, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(99)06141-6.

[1] The reader is warned that the term "group code" is being used of late with a different meaning, i.e., to denote block or convolutional codes defined over an alphabet forming a group. Accordingly, some authors use a different term (e.g., "orbit codes" [8]) instead of Slepian's "group codes." We use here the original definition to be consistent with our references.

abstract group $\mathcal{G}$ with M elements, and an "initial vector" $\boldsymbol{x} \in \boldsymbol{R}^N$, $\boldsymbol{R}^N$ the Euclidean N-dimensional space. A group code $\mathcal{X}$ is the orbit of $\boldsymbol{x}$ under $\mathcal{G}$, i.e., the set of vectors $\boldsymbol{Gx}$. By assuming that the only solution of the equation $G\boldsymbol{x} = \boldsymbol{x}$, $G \in \boldsymbol{G}$, is $G = I$ (the identity matrix), the code $\mathcal{X}$ has M elements. We say $\mathcal{X}$ is an $[M, N]$ group code and denote $\boldsymbol{x}_g$ the code vector associated with $g \in \mathcal{G}$.

When a codeword $\boldsymbol{x}_g$ of $\mathcal{X}$ is transmitted over the additive white Gaussian noise channel, the optimum (i.e., maximum-likelihood) decoder, upon receiving the noisy vector $\boldsymbol{r} = \boldsymbol{x}_g + \boldsymbol{n}$, chooses as the most likely transmitted vector the one that yields

$$\min_{h \in \mathcal{G}} \|\boldsymbol{r} - \boldsymbol{x}_h\|^2. \tag{1}$$

If $\mathcal{G}$ is not endowed with any special structure, decoding (i.e., the solution of (1)) is obtained by an exhaustive search among all the candidates $g \in \mathcal{G}$. This requires a number of calculations $\nu_C = NM$ (in fact, M scalar products of N terms each must be computed) and a storage of $\nu_S = NM$ real numbers (M vectors of N components each). Define the number of bits per dimension carried by the constellation as

$$r = \frac{\log_2 M}{N}$$

then we have $\nu_C = \nu_S = N2^{rN}$, which shows that the complexity of the decoder grows exponentially with the number of dimensions and with the number of bits per dimension. A *permutation code* is a group code obtained by applying to the initial vector $\boldsymbol{x}$ a group $\boldsymbol{G}$ of permutations (i.e., $\boldsymbol{G}$ is a group of permutation matrices). If $\mathcal{X}$ is a permutation code, then a less complex decoder that is equivalent to maximum likelihood is available.

Slepian [9] has studied permutation codes with $\mathcal{G}$ the full symmetric group $\mathcal{S}_n$. In this case, a very simple decoder exists that is equivalent to maximum likelihood. Karlof [4] has described a "stack algorithm" decoder for arbitrary permutation codes that, in the presence of low noise, produces the maximum-likelihood vector using fewer calculations than the standard maximum-likelihood decoder.

Two $[M, N]$ codes $\mathcal{X}_1$ and $\mathcal{X}_2$ are defined to be *equivalent* if there exists an orthogonal $N \times N$ matrix O such that $O\mathcal{X}_1 = \mathcal{X}_2$. Equivalent codes have congruent Voronoi regions and thus have the same error performance over the Gaussian channel. We extend the definition of equivalence to codes in different dimensions with the same number of elements. In this case, we say the two codes are equivalent if they have the same *configuration matrix*, i.e., the Gram matrix of their scalar products. Then the two codes have the same set of distances between codewords as in the case of equivalent codes of the same dimension. We note that this definition is weaker than the usual definition since the codes are not, in general, orthogonal transformations of each other. It what follows it should be clear from the context which definition of equivalence is being used.

In this correspondence, using the fact that every group is isomorphic to a permutation group, we find the minimum degree of this permutation group, show that every group code is (weakly) equivalent to a permutation code, and describe how to find the minimum degree of the equivalent permutation code.

II. Finding an Equivalent Permutation Code

Let $\mathcal{G}$ be a group. A *permutation representation* of degree n [6, Ch. 7] of $\mathcal{G}$ is a homomorphism of $\mathcal{G}$ into $\mathcal{S}_n$, or the image of $\mathcal{G}$ under the homomorphism. If the homomorphism is an isomorphism, we say that the representation is *faithful*.

In general, every group $\mathcal{G}$ with order $|\mathcal{G}|$ is isomorphic to a subgroup of $\mathcal{S}_{|\mathcal{G}|}$. Let $\mathcal{H}$ denote a subgroup of $\mathcal{G}$ and let $\mathcal{R}$ be the set of right cosets of $\mathcal{H}$ in $\mathcal{G}$. Then

$$\mathcal{G} = \bigcup_{\mathcal{H}r \in \mathcal{R}} \mathcal{H}r$$

is the decomposition of $\mathcal{G}$ into right cosets of $\mathcal{H}$. To every $g \in \mathcal{G}$ assign the permutation

$$\pi_g: \mathcal{R} \to \mathcal{R} \text{ where } \pi_g(\mathcal{H}r) = \mathcal{H}rg.$$

The set $\Gamma = \{\pi_g | g \in \mathcal{G}\}$ is a transitive permutation group of degree $n = |\mathcal{G}|/|\mathcal{H}|$ and is the permutation representation of $\mathcal{G}$ induced by $\mathcal{H}$ [6]. Every transitive permutation representation of $\mathcal{G}$ can be obtained in this way. When $\mathcal{H} = \{e\}$, the identity of $\mathcal{G}$, the representation induced by $\mathcal{H}$ is called the *right regular representation* of $\mathcal{G}$. The left regular representation can be defined in a similar way.

The minimum n corresponds to the maximum $|\mathcal{H}|$ such that the representation Γ is faithful, i.e., such that the kernel of the homomorphism of $\mathcal{G}$ onto Γ is the identity. This kernel can be characterized as the maximal normal subgroup of $\mathcal{G}$ contained in $\mathcal{H}$ [6, Ch. 7]. Consequently, if $\mathcal{H}'$ denotes the largest nonnormal subgroup of $\mathcal{G}$ that does not include normal subgroups of $\mathcal{G}$ other than the identity, then n is given by the ratio

$$n = \frac{|\mathcal{G}|}{|\mathcal{H}'|}.$$

Example 2.1—Icosahedral Group [7, p. 32]: Let

$$\mathcal{G} = \langle x, y, z | x^3 = y^2 = z^2 = (xy)^3 = (yz)^3 = (xz)^2 = 1\rangle.$$

Then $\mathcal{G}$ is a simple group of order 60. Let $\mathcal{H} = \langle x, y\rangle$. Then, the order of $\mathcal{H}$ is 12 and since $\mathcal{G}$ has no subgroups of order larger than 12, $\mathcal{H}$ is the largest nonnormal subgroup of $\mathcal{G}$ that does not contain any nontrivial normal subgroups of $\mathcal{G}$. Thus $\mathcal{G}$ is isomorphic to a permutation group, $\Gamma_{\mathcal{H}}$, of degree 5 and of order 60. The set of right cosets is $\mathcal{R} = \{\mathcal{H}, \mathcal{H}z, \mathcal{H}zy, \mathcal{H}zyx, \mathcal{H}zyx^2\}$ and $\Gamma_{\mathcal{H}} = \langle (3, 4, 5), (2, 3)(4, 5), (1, 2)(4, 5)\rangle$. For example, $\pi_z = (1, 2)(4, 5)$ since

$$\begin{aligned}
\pi_z(\mathcal{H}) &= \mathcal{H}z \\
\pi_z(\mathcal{H}z) &= \mathcal{H}z^2 = \mathcal{H} \\
\pi_z(\mathcal{H}zy) &= \mathcal{H}zyz = \mathcal{H}yzy = \mathcal{H}zy \\
\pi_z(\mathcal{H}zyx) &= \mathcal{H}zyxz = \mathcal{H}zyzx^2 = \mathcal{H}yzyx^2 = \mathcal{H}zyx^2 \\
\pi_z(\mathcal{H}zyx^2) &= \mathcal{H}zyx^2z = \mathcal{H}zyxzx^2 = \mathcal{H}zyzx = \mathcal{H}zyx. \qquad \square
\end{aligned}$$

Now if $\mathcal{G}$ is Abelian or a Sylow p-group then all its subgroups are normal. So $|\mathcal{H}'| = 1$, and hence $n = |\mathcal{G}|$. If $\mathcal{G} = \mathcal{S}_m$, $m = 3$, or $m \geq 5$, then its only nontrivial normal subgroup is the alternating group $\mathcal{A}_m$, while $\mathcal{G}$ does admit the subgroup $\mathcal{S}_{m-1}$. Hence

$$n = \frac{|\mathcal{S}_m|}{|\mathcal{S}_{m-1}|} = m.$$

Thus the closer $\mathcal{G}$ is to an Abelian group, the larger is the value of n.

Theorem 2.1: Suppose $\mathcal{G}$ is a finite abstract group with irreducible real characters $\chi_1, \chi_2, \cdots, \chi_p$. Consider a faithful representation ρ: $\mathcal{G} \to \boldsymbol{G}$ where $\boldsymbol{G}$ is a group of orthogonal $N \times N$ matrices. Let χ_ρ be the character of ρ and suppose

$$\chi_\rho = \sum_{i=1}^{p} a_i \chi_i.$$

Let $\boldsymbol{x} \in \boldsymbol{R}^N$ and form the group code

$$\mathcal{X} = \boldsymbol{Gx} = \{\rho(g)\boldsymbol{x}: g \in \mathcal{G}\}.$$

Suppose $\mathcal{H}$ is a subgroup of $\mathcal{G}$ and form the permutation representation ϕ: $\mathcal{G} \rightarrow \Gamma = \{\pi_g | g \in \mathcal{G}\}$ induced by $\mathcal{H}$. Let χ_ϕ be the character of ϕ and suppose

$$\chi_\phi = \sum_{i=1}^{p} b_i \chi_i.$$

If ϕ is faithful and $b_i \geq a_i \, \forall i$, then Γ generates a permutation code equivalent to $\mathcal{X}$.

Proof: Let ψ_i be the irreducible representation of $\mathcal{G}$ afforded by χ_i. Without loss of generality assume that $a_i \neq 0$ for $1 \leq i \leq m$ and $a_i = 0$ for $i > m$. Then there exists an orthogonal $N \times N$ matrix U such that

$$U\rho(g)U^T = \oplus_{i=1}^{m} a_i \psi_i(g), \qquad \forall g \in \mathcal{G}$$

(i.e., $\rho(g)$ is equivalent to the direct sum of a_1 copies of $\psi_1(g) \cdots a_m$ copies of $\psi_m(g)$). Let $\overline{x} = Ux$. Then $\mathcal{X}$ and $\{(\oplus_{i=1}^{m} a_i \psi_i(g))\overline{x} | g \in \mathcal{G}\}$ are equivalent N-dimensional codes.

We will consider Γ as a group of $n \times n$ permutation matrix where $n = |\mathcal{G}|/|\mathcal{H}|$. Then there exists an orthogonal $n \times n$ matrix V such that

$$V\phi(g)V^T = \oplus_{i=1}^{m} a_i \psi_i(g) \oplus_{i=1}^{m} (b_i - a_i)\psi_i(g) \oplus_{i=m+1}^{p} b_i \psi_i(g), \qquad \forall g \in \mathcal{G}.$$

Let x^0 be a zero-padded n-dimensional version of $\overline{x}$ (i.e., $x^0 = (\overline{x}^T, 0 \cdots 0)^T$). Then $\{(\oplus_{i=1}^{p} b_i \psi_i(g))x^0\}$ and $\{\phi(g)(V^T x^0)\}$ are equivalent n-dimensional codes. Clearly, the N-dimensional code $\{\oplus_{i=1}^{m} a_i \psi_i(g)\overline{x}\}$ and the n-dimensional code $\{\oplus_{i=1}^{p} b_i \psi_i(g) x^0\}$ have the same number of elements and the same configuration matrix. Thus Γ generates a permutation code equivalent to $\mathcal{X}$. □

Corollary 2.1: Every group code is equivalent to at least one permutation code.

Proof: Let $\mathcal{H} = \{e\}$. Then ϕ is the right regular permutation representation of $\mathcal{G}$, $\phi(g) = \oplus_{i=1}^{p} b_i \psi_i(g)$ where $b_i = \deg(\psi_i)$ if ψ_i is also irreducible over the complex field (i.e., ψ_i is a complex irreducible representation of the first kind) and $b_i = \frac{1}{2}$ or $\frac{1}{4}$ times $\deg(\psi_i)$ otherwise. If $a_i > b_i$, then more copies of ϕ may be used. □

Example 2.2: The 4-PSK signal set can be generated by the following representation of the cyclic group $\mathcal{G}$ of order four:

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

using the initial vector $\boldsymbol{x} = [1, 0]^T$. The irreducible real representations of this cyclic group are the representation above, denoted $\psi_2(g)$, the identity representation $\psi_1(g)$, associating $+1$ with all the groups elements, and the alternating representation $\psi_{-1}(g)$, associating -1 with the first and third elements of $\mathcal{G}$ and $+1$ with the second and fourth elements. Consequently, letting ϕ denote the right regular representation, an orthogonal matrix V exists such that

$$\psi_1(g) \oplus \psi_{-1}(g) \oplus \psi_2(g) = V\phi(g)V^T.$$

The matrix V is found in [1]

$$V = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ \sqrt{2} & 0 & -\sqrt{2} & 0 \\ 0 & -\sqrt{2} & 0 & \sqrt{2} \end{bmatrix}.$$

By applying V^T to the zero-padded version of $\boldsymbol{x}$, $\boldsymbol{x}^0 = [0, 0, 1, 0]^T$, we get the initial vector of the permutation code equivalent to 4-PSK: $[\sqrt{2}/2, 0, -\sqrt{2}/2, 0]^T$. □

In practice, it is often difficult to find the matrices U and V in the proof of the previous theorem. Also, the degree n of the permutation representation may be prohibitively large. The procedure is greatly simplified in the case that the image of ϕ is doubly transitive.

Corollary 2.2: Suppose Γ is doubly transitive. Then

1) ρ is irreducible;
2) $\phi = 1 \oplus \rho$ (here, we use 1 to denote the identity representation of $\mathcal{G}$);
3) $n = N + 1$;
4) U is the identity matrix; and
5) V may be taken to be

$$\begin{bmatrix} \gamma & \gamma & \gamma & \cdots & \gamma & \gamma \\ \beta_1 & -\gamma_1 & -\gamma_1 & \cdots & -\gamma_1 & -\gamma_1 \\ 0 & \beta_2 & -\gamma_2 & \cdots & -\gamma_2 & -\gamma_2 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & \beta_{n-1} & -\beta_{n-1} \end{bmatrix}$$

where $n\gamma^2 = 1$, $(n-j)\gamma_j^2 + \beta_j^2 = 1$, $\beta_j - (n-j)\gamma_j = 0$.

Proof: It is well known [3, p. 230] that a doubly transitive permutation representation may be written as the direct sum of the identity representation and an irreducible representation. The matrix V is given in [2]. □

Given an irreducible representation $\rho : \mathcal{G} :\rightarrow \boldsymbol{G}$, a method to find an appropriate $\mathcal{H}$ is to use a computer algebra system such as MAGMA to print out all subgroups of $\mathcal{G}$ of low index and then, if necessary, use the characters of $\mathcal{G}$ to find which of the induced permutation representations contain ρ. This is illustrated in the following example.

Example 2.3: Let $\mathcal{G} =$ the icosahedral group. This group has four nontrivial irreducible orthogonal representations [7, p. 313], two of degree 3, one of degree 4, and one of degree 5. We label these ρ_1, ρ_2, ρ_3, ρ_4 and their characters χ_1, χ_2, χ_3, χ_4, respectively. We use MAGMA to find the low index subgroups of $\mathcal{G}$. There are four of index 12 or less. They are $\mathcal{H}$ of index 5 from Example 2.1, $\mathcal{I} = \langle y, zx^2 \rangle$ of index 6, $\mathcal{K} = \langle x, z \rangle$ of index 10, and $\mathcal{L} = \langle xyz \rangle$ of index 12. Denote the induced permutation representations by $\phi_\mathcal{H}$, $\phi_\mathcal{I}$, $\phi_\mathcal{K}$, and $\phi_\mathcal{L}$, respectively. Only $\phi_\mathcal{H}$ and $\phi_\mathcal{I}$ are doubly transitive. Thus $\phi_\mathcal{H} = 1 \oplus \rho_3$ and $\phi_\mathcal{I} = 1 \oplus \rho_4$ and, by Corollary 2.2, any group codes generated by ρ_3 or ρ_4 can be easily represented by equivalent permutation codes.

To find permutation codes equivalent to group codes generated by ρ_1 or ρ_2, we investigate the images and characters of $\phi_\mathcal{K}$ and $\phi_\mathcal{L}$ which we denote by $\Gamma_\mathcal{K}$, $\Gamma_\mathcal{L}$, $\chi_\mathcal{K}$, and $\chi_\mathcal{L}$, respectively. The orders of the five conjugacy classes of $\mathcal{G}$ are $|C_1| = 1$, $|C_2| = 12$, $|C_3| = 12$, $|C_4| = 15$,, and $|C_5| = 20$. The representatives of the corresponding conjugacy classes of $\Gamma_\mathcal{K}$ and $\Gamma_\mathcal{L}$ are

$$(1), (1,2,8,10,6)(3,9,7,5,4), (1,8,6,2,10)(3,7,4,9,5), (1,2)(3,5)(6,8)(7,9), (2,3,5)(4,7,6)(8,10,9)$$

and $(1), (2,11,8,5,7)(3,10,12,4,9), (2,8,7,11,5)(3,12,9,10,4), (1,3)(2,4)(5,11)(6,8)(7,12)(9,10), (1,2,5)(3,7,9)(4,10,6)(8,12,11)$

respectively. The character table of $\mathcal{G}$ is

	C_1	C_2	C_3	C_4	C_5
1	1	1	1	1	1
χ_1	3	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$	-1	0
χ_2	3	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$	-1	0
χ_3	4	-1	-1	0	1
χ_4	5	0	0	1	-1

Since $\chi_{\mathcal{K}}(g)$ and $\chi_{\mathcal{L}}(g)$ equal the number of elements $\phi_{\mathcal{K}}(g)$ and $\phi_{\mathcal{L}}(g)$ fix the following character inner products are easily computed

$$\begin{aligned} 1 &= \frac{1}{|\mathcal{G}|} \sum_{g\in\mathcal{G}} \chi_{\mathcal{K}}(g)\chi_3(g) \\ &= \frac{1}{|\mathcal{G}|} \sum_{g\in\mathcal{G}} \chi_{\mathcal{K}}(g)\chi_4(g) \\ 1 &= \frac{1}{|\mathcal{G}|} \sum_{g\in\mathcal{G}} \chi_{\mathcal{L}}(g)\chi_1(g) \\ &= \frac{1}{|\mathcal{G}|} \sum_{g\in\mathcal{G}} \chi_{\mathcal{L}}(g)\chi_2(g) \\ &= \frac{1}{|\mathcal{G}|} \sum_{g\in\mathcal{G}} \chi_{\mathcal{L}}(g)\chi_4(g). \end{aligned}$$

Now, since every permutation representation contains the identity representation we have, $\rho_{\mathcal{K}} = 1 \oplus \rho_3 \oplus \rho_4$ and $\rho_{\mathcal{L}} = 1 \oplus \rho_1 \oplus \rho_2 \oplus \rho_4$. So we can represent group codes generated by ρ_1 and ρ_2 by equivalent permutation codes but the degree would be 12 and the matrix V would have to be found. □

We conclude with an example which summarizes the main result of the correspondence.

Example 2.4: Let $\mathcal{G}$ be the icosahedral group. Consider the four-dimensional group code $\mathcal{X} = \{\rho_3(g)\boldsymbol{x}\colon g \in \mathcal{G}\}$. The image of ρ_3 can be found in [7, p. 313]. We use a modification of the algorithm in (5) to find the optimal initial vector

$$\boldsymbol{x} = [-0.68222, -0.49471, -0.44657, -0.30070]$$

for this representation. The minimum squared Euclidean distance is $d^2_{\min} = 0.447056$. We are then under the hypothesis of Corollary 2.1. We use the degree 5 permutation representation $\phi_{\mathcal{H}} = 1 \oplus \rho_3$ and transform the zero-padded vector

$$\boldsymbol{x}^0 = [0, -0.68222, -0.49471, -0.44657, -0.30070]$$

to the initial vector

$$V^T\boldsymbol{x}^0 = [-0.61010, -0.27588, -0.06926, 0.26504, 0.69020]$$

for the equivalent permutation code generated by $\Gamma_{\mathcal{H}}$.

We finally note that in practice the code is transmitted over the additive white Gaussian noise (AWGN) channel using the low-dimensional constellation in order to save on the spectral efficiency. The received vector $\boldsymbol{r}$ is first zero-padded as for the initial vector and then transformed into $\boldsymbol{y} = V^T\boldsymbol{r}^0$. Now, $\boldsymbol{y}$ can be maximum-likelihood (ML) decoded with the permutation code decoder. We note that this is an orthogonal transformation on the received vector which does not modify the additive noise statistics. In the above example the operation is particularly convenient since the code dimension is only increased by one. On the other hand, if we wanted to use the three-dimensioanl codes generated by the representations ρ_1 or ρ_2 we would need to use a degree 12 permutation representation.

References

[1] E. Biglieri and M. Elia, "Cyclic-group codes for the Gaussian channel," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 624–629, Sept. 1976.
[2] I. F. Blake, "Distance properties of group codes for the Gaussian channel," *SIAM J. Appl. Math.*, vol. 23, no. 3, pp. 312–324, Nov. 1972.
[3] C. W. Curtis and I. Reiner, "Representation theory of finite groups and associative algebras," *Interscience*, New York, 1962.
[4] J. K. Karlof, "Decoding spherical codes for the Gaussian channel," *IEEE Trans. Inform. Theory*, vol. 39, pp. 60–65, Jan. 1993.
[5] ——, "Permutation codes for the Gaussian channel," *IEEE Trans. Inform. Theory*, vol. 35, pp. 726–732, July 1989.
[6] R. Kochendörffer, *Group Theory.* London, U.K.: McGraw-Hill, 1965.
[7] J. S. Lomont, *Applications of Finite Groups.* New York: Academic, 1959.
[8] V. M. Sidelnikov, "On a finite group of matrices generating orbit codes on Euclidean sphere," in *Proc. 1997 IEEE Int. Symp. Information Theory* (Ulm, Germany, June 29–July 4, 1997), p. 436.
[9] D. Slepian, "Permutation modulation," *Proc. IEEE*, vol. 53, pp. 228–236, Mar. 1965.
[10] ——, "Group codes for the Gaussian channel," *Bell Syst. Tech. J.*, vol. 47, pp. 575–602, Apr. 1968.

On Double-Byte Error-Correcting Codes

C.-L. Chen

***Abstract*—This correspondence shows that there is a flaw in the results presented in [1]. A large family of the codes constructed in [1] are not double-byte error-correcting codes as originally claimed.**

***Index Terms*—Double-byte error correction, error-correcting code.**

I. Introduction

The authors in [1] claim that a class of double-byte error-correcting codes over GF (q), q a power of 2, has been constructed. These codes have the parameters of code length $n = q^m$ and code redundancy $r \le 2m + \lceil \frac{m}{3} \rceil + 1$, for any integer m equal to or greater than 3. However, a close examination of the paper reveals a flaw in the proofs of theorems that renders the claim invalid. This correspondence is to point out the flaw in [1].

Five constructions of linear codes have been presented in [1]. Each construction has been claimed to have a minimum distance of five and thus have the ability to correct all double-byte errors. Constructions 3.2 and 5.1 are equivalent to cyclic codes extended by one byte. The minimum distance of these codes can be shown to be five or more by counting multiple sets of consecutive roots in their generator polynomials [2]. The codes constructed from Construction 3.1 are shortened codes of those constructed from Construction 3.2. The minimum distance of these codes is at least five. The large family of codes constructed from Constructions 3.3 and 3.4 are not double-byte error-correcting codes as claimed by the authors. Counter examples will be presented in the next section to show that codes constructed according to Constructions 3.3 and 3.4 contain codewords of weight four and thus do not have a double-byte error-correcting ability.

II. Counter Examples

The propositions of Theorems 3.3 and 3.4 in [1] state that the codes obtained from Constructions 3.3 and 3.4 in [1] have a minimum distance of five or more. In this section, two examples of Constructions 3.3 and 3.4 are presented. It will be shown that the

Manuscript received August 25, 1998.
The author is with IBM Corporation, MS P361, Poughkeepsie, NY 12601 USA.
Communicated by A. M. Barg, Associate Editor for Coding Theory.
Publisher Item Identifier S 0018-9448(99)05861-7.