A Note on Permutation Modulation

W. Wesley Peterson, *Fellow, IEEE*

***Abstract*—Slepian observed that the code points in an n-dimensional variant-1 permutation modulation code actually lie in an $n-1$-dimensional subspace. In this correspondence, a change of coordinates which gives the representation explicitly in $n-1$ dimensions is derived. Slepian's optimum decoding algorithm can be adapted to the codes in this form using an idea of Biglieri.**

***Index Terms*—Permutation modulation, group code, decoding.**

I. Introduction

An n-dimensional group code for the Gaussian channel [1] is a set of N points on an n-dimensional unit sphere defined as follows: There is a group of N orthogonal matrices P_i. Then there is an initial point x_1 on the unit sphere. The N points of the code are the points that are obtained by multiplying x_1 by each of the matrices $P_1, P_2, \cdots, P_N$, and since orthogonal matrices preserve distance, these points will all lie on the unit sphere. Properties of the code depend both on the group of matrices and on the choice of the initial point x_1 and in general are not easy to determine.

A variant-1 permutation modulation code [2] is a group code for which the group of matrices is the set of all permutation matrices, which we will denote P_i. Slepian assumed that the initial point $x_1 = (x_{11}, x_{12}, \cdots, x_{1n})$ satisfies $x_{1i} \geq x_{1j}$ if $i < j$. He considered both the simplest case, in which all the coordinates are distinct, and also the case in which they are not.

It is not difficult to determine the choice of x_1 that maximizes the minimum distance between code points [3], [4]. In the simplest case, when the x_{1i} are all distinct, then

$$x_{1i} = e\left(\frac{n+1}{2} - i\right) \tag{1}$$

where

$$e = \sqrt{\frac{12}{(n+1)n(n-1)}} \tag{2}$$

For example, for $n = 3$, then

$$x_1 = (1/\sqrt{2}, 0, -1/\sqrt{2})$$

and for $n = 4$

$$x_1 = (3/\sqrt{20}, 1/\sqrt{20}, -1/\sqrt{20}, -3/\sqrt{20}).$$

Note also that the sum of the x_{1i} is zero.

With this initial vector, the minimum distance is $e\sqrt{2}$. Slepian [2] found that for the Gaussian channel, the minimum error probability did not occur with exactly the initial point x_1 that maximizes minimum distance, although the x_1 that minimizes error probability and the x_1 that maximizes minimum distance are quite close for the cases that he calculated.

Manuscript received December 26, 1995; revised July 10, 1996.

The author is with the Department of ICS, University of Hawaii, Honolulu, HI 96822 USA.

Publisher Item Identifier S 0018-9448(97)00101-6.

II. Reduced Permutation Codes

Since all code points have coordinates that are permutations of the coordinates of the initial point, the sum of the coordinates for every point in the code is zero. This means that all the points lie on an $n-1$-dimensional hyperplane that passes through the origin. Now we propose to make a change of coordinate axes so that the last coordinate is perpendicular to this plane. A change of coordinate axes can be accomplished by multiplying the vector by an orthogonal matrix. There are many possible choices for this matrix. The matrix A described next is one that seems especially convenient.

Consider the $n \times n$ matrix A which has all elements in the nth row and all the elements in the nth column equal to $1/\sqrt{n}$, all other diagonal elements equal to $1+b$ and all other nondiagonal elements equal to b, where $b = -1/(n-\sqrt{n})$. It is not difficult to verify that A is an orthogonal matrix, i.e., $AA^T = I$ where I is the identity matrix. Note that A is symmetric, so $A^T = A^{-1} = A$. Then A can be used to change the coordinate system. A point x, considered to be an n-component column vector, becomes Ax in the new coordinate system, and since A is an orthogonal matrix, Ax has the same length as x.

For any code point x_i, let us define $x_i' = Ax_i$. Since the elements of the last row of A are all equal to $1/\sqrt{n}$, the last coordinate of x_i' is equal to the sum of the coordinates of x_i divided by $\sqrt{n}$, which is zero, assuming an optimum x_i. Since the coordinates of each of the code points in the original code are permutations of the coordinates of x_1, the sum of the coordinates is zero for every code point. Thus the last coordinate for every x_i' will be zero. Let us define x_i'' to be the point in $n-1$ dimensions obtained by omitting the last coordinate of x_i'.

The points x_i' can be considered to be the same as the points x_i viewed in a different coordinate system. Therefore, the distance between any two points x_i' and x_j' will be the same as the distance between x_i and x_j and the minimum distance will be the same. Since the configuration of points is the same, the error probability for optimum decoding must also be the same. The same statements must be true of the points x_i'' in $n-1$-dimensional space. We will refer to the code consisting of all of the x_i'' as the reduced permutation code.

Slepian found an optimum decoding algorithm for the permutation codes. He found that if P_i^T is the permutation that rearranges the received point y's components into decreasing sequence, then decoding y into x_i is optimum. Biglieri [5] recently found that this decoding algorithm can be used for the reduced code by simply changing coordinates back to the original coordinate system and then applying the original decoding algorithm. Specifically in this case that means 1) add a zero to the end of the $n-1$-dimensional received vector y'' to obtain an n-dimensional vector y'; 2) calculate $y = Ay'$, the received vector viewed in the original coordinate system; and 3) find the permutation P_i^T that rearranges the components of y in decreasing sequence. Then decoding y to x_i is optimum.

III. Reduced Codes as Group Codes

In the new coordinate system defined by A, the orthogonal matrix P_i transforms into $AP_iA^T = AP_iA$. Let us look at AP_iA. P_iA is simply A with its rows permuted by the permutation P_i. Since all the elements in the last column of A are the same $(1/\sqrt{n})$ the last column of P_iA is the same as the last column of A, and therefore the last column of $A(P_iA)$ is the same as the last column of AA, which is $n-1$ zeros followed by a 1 in the last position. Since all the elements in the last row of A are the same $(1/\sqrt{n})$, in calculating

the last row of $A(P_iA)$ the result is the same as the last row of AA, because the permutation of the rows in (P_iA) makes no difference in the result. Again this is $n-1$ zeros followed by a 1 in the last position. Thus AP_iA has the following form:

$$AP_iA = \begin{pmatrix} Q_i & 0 \\ 0 & 1 \end{pmatrix}. \tag{3}$$

Here Q_i in an $(n-1)\times(n-1)$ matrix, the 0 in the first row represents a column of $n-1$ zeros, and the 0 in the second row represents a row of $n-1$ zeros.

Since A and P_i are orthogonal matrices, AP_iA is also. From that, it follows that Q_i is an orthogonal matrix also. Since all the matrices P_i are distinct, then all the matrices AP_iA must be distinct also, because A is nonsingular. But since all the matrices AP_iA have the same last row and column, then all the matrices Q_i must be distinct. Since $(AP_iA)(AP_jA) = AP_iP_jA$, the product Q_iQ_j is a matrix Q_k for some k, so this set of Q_i is closed under multiplication, and being a finite subset of a group (the group of all orthogonal matrices), it is a group. With this group of orthogonal matrices, we can make a group code. Since $x_1' = Ax_1$ by definition, and since A is its own inverse, then $Ax_1' = x_1$. Also, $P_ix_1 = x_i$ by definition, and $Ax_i = x_i'$ by definition. Thus $AP_iAx_1' = x_i'$ and it follows from this by deleting the last component of x_i' and the last row and column of AP_iA that $Q_ix_1'' = x_i''$. Thus the code consisting of the points x_i'' is exactly the $n-1$-dimensional group code generated by the group of matrices Q_i and the initial vector x_1''.

IV. Other Details

It is possible to get expressions for all the matrices Q_i and for all of the code vectors x_i''. The complete derivations are straightforward but somewhat lengthy and uninteresting. Therefore, the results will be stated with a few hints on how they can be derived.

First, let us consider two sets of permutation matrices. Let S_1 consist of all permutation matrices that leave the nth element unchanged, permuting only the first $n-1$ elements. These form a subgroup of all the permutations on n elements. Let S_2 consist of the identity matrix and all of the permutations that simply exchange the nth element and the kth element, $k = 1, \cdots, n-1$. Every permutation can be found as the product of one from S_1 and from S_2. Thus we can find all of the matrices Q_i as products of matrices derived from permutations in S_1 and S_2.

If P_i is a matrix in S_1, then deleting the last row and column of P_i gives an $(n-1)\times(n-1)$ permutation matrix R_i. It turns out that this is equal to the matrix Q_i derived from AP_iA by dropping the last row and column. Note that if the last row and column are dropped from A, the resulting matrix equals $I+B$ where I is an $(n-1)\times(n-1)$ identity matrix and B is an $(n-1)\times(n-1)$ matrix all of whose elements are equal to b. Then $R_iI = R_i = IR_i$ and $R_iB = B = BR_i$, and therefore $R_i(I+B) = (I+B)R_i$. It follows from this that $P_iA = AP_i$ and therefore also $AP_iA = P_i$. Then, dropping the last row and column from both sides here shows that Q_i equals R_i.

Now let us look at permutations from the set S_2. If we denote by P_k the permutation that permutes elements n and k, and by Q_k the $(n-1)\times(n-1)$ matrix derived from AP_kA, then the elements q_{kij} of Q_k are as follows:

$$\begin{aligned} q_{kkk} &= -c^2 + 2c \\ q_{kii} &= -c^2 + 1 \quad \text{if } i \neq k \\ q_{kij} &= -c^2 + c \quad \text{if } i = k \text{ and } j \neq k \\ &\qquad\qquad \text{or } i \neq k \text{ and } j = k \\ q_{kij} &= -c^2 \quad \text{otherwise} \end{aligned} \tag{4}$$

where $c = 1/\sqrt{n} - b = 1/(\sqrt{n}-1)$. In deriving this, it helps to define $W = P_kA - A$. W has only two nonzero rows, row k and row n, and they are equal but opposite in sign. Then $P_kA = A + W$ and $AP_kA = AA + AW = I + AW$.

The complete group of matrices Q_i consists of all the $(n-1)\times(n-1)$ permutation matrices, including the identity matrix, and the matrices Q_k for $k = 1\cdots n-1$, and finally all products of a permutation matrix with one of these $n-1$ matrices. In other words, the complete group consists of all the $(n-1)\times(n-1)$ permutation matrices, the $n-1$ matrices Q_k, and all matrices that can be obtained from the Q_k by permuting rows. In fact, since you can multiply any element of the group either on the right or on the left by any other element of the group and obtain another element of this group, any matrix derived from a matrix in this group by a permutation of rows and/or columns results in a matrix in the group.

Finally, consider the code vectors. The initial vector is obtained by omitting the last component from $x_1' = Ax_1$, where x_1 is given in (1). A direct calculation gives

$$x_{1i}'' = e(i - (n - \sqrt{n})/2). \tag{5}$$

Then from the matrices Q_k derived from the set S_2 of permutations, $n-1$ more code vectors $x_k'' = Q_kx_1''$ can be derived, and again by direct calculation, here are their values.

$$\begin{aligned} x_{ki}'' &= -ei - cek + \frac{ce\sqrt{n}}{2}(n+1) \quad \text{if } i \neq k \\ x_{kk}'' &= -cek - \frac{ce\sqrt{n}}{2}(n - 2\sqrt{n} - 1). \end{aligned} \tag{6}$$

These with the initial vector total n vectors. The rest can be found by taking all permutations of each of these vectors—there are $(n-1)!$ permutations of each of n vectors, to give a total of $n(n-1)! = n!$ vectors, which is the number of matrices Q_i in the group and hence the number of code points.

Mathematically, the group of all permutation matrices is a representation of the abstract group of all permutations. It is the direct sum of the identity representation, which maps every permutation into 1, and the representation made up of the Q_i. It is known that the representation by the Q_i is irreducible. More generally, the matrix A can be used with any group of $n \times n$ permutation matrices to display it as the direct product of the identity representation and a $(k-1)\times(k-1)$ representation, which will be irreducible if the subgroup is doubly transitive [4], [6, example 2.6, p. 17].

V. Conclusion

Slepian observed that the code points for the variant-1 permutation modulation codes of dimension n actually lie in a subspace of dimension $n-1$. This correspondence carries out explicitly the change of coordinates required to represent these codes in $n-1$ dimensions. Biglieri [3] discovered how to adapt Slepian's optimum decoding algorithm to the codes represented in $n-1$ dimensions. Biglieri's paper gave me important new insights into these codes beyond just how to decode them.

References

[1] D. Slepian, "Group codes for the gaussian channel," *Bell Syst. Tech. J.*, vol. 47, pp. 575–602, Apr. 1968.

[2] ——, "Permutation modulation," *Proc. IEEE*, vol. 53, pp. 228–236, Mar. 1965.

[3] E. Biglieri and M. Elia, "Optimum permutation modulation codes and their asymptotic performance," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 751–753, Nov. 1976.

[4] 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.

[5] E. Biglieri, "Permutation decoding of group codes," in *Proc. 1995 Int. Symp. on Information Theory* (Whistler, BC. Canada), p. 306.

[6] J.-P. Serre, *Linear Representations of Finite Groups*. New York: Springer-Verlag, 1977.