Representing Group Codes as Permutation Codes

Ezio Biglieri, John K. Karlof and Emanuele Viterbo

Dipartimento di Elettronica • Politecnico di Torino • I-10129 Torino (Italy)
Mathematics and Statistics Department • University of North Carolina • Wilmington, NC 28403 (USA)
Dipartimento di Elettronica • Politecnico di Torino • I-10129 Torino (Italy)

Consider a group $\mathbf{G}$ of $N \times N$ orthogonal matrices which forms a faithful representation of an abstract group $\mathcal{G}$ with M elements, and an "initial vector" $\mathbf{x} \in \mathbf{R}^N$. A *group code* [3] $\mathcal{X}$ is the orbit of $\mathbf{x}$ under $\mathcal{G}$, i.e., the set of vectors $\mathbf{Gx}$. By assuming that the only solution of the equation $G\mathbf{x} = \mathbf{x}$, $G \in \mathbf{G}$, 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 $\mathbf{x}_g$ the code vector associated with $g \in \mathcal{G}$.

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

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

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 $g \in \mathcal{G}$. In fact, 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 $\mathbf{x}$ a group $\mathbf{G}$ of permutations (i.e. $\mathbf{G}$ 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 [2] 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 [1] 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 by 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.

In this paper, 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 equivalent to a permutation code, and describe how to find the minimum degree of the equivalent permutation code.

A *permutation representation* of degree n of $\mathcal{G}$ is a homomorphism of $\mathcal{G}$ into $\mathcal{S}_n$, or the image of $\mathcal{G}$ under the homomorphism. 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 $\mathcal{H}$. The minimum n of a faithful permutation representation is $|\mathcal{G}|/|\mathcal{H}'|$ where $\mathcal{H}'$ denotes the largest non-normal subgroup of $\mathcal{G}$ that does not include normal subgroups of $\mathcal{G}$ other than the identity.
We prove the following results.

Theorem 1 *Suppose $\mathcal{G}$ is a finite abstract group with irreducible real characters $\chi_1, \chi_2, \ldots, \chi_p$. Consider a faithful representation $\rho : \mathcal{G} \to \mathbf{G}$ where $\mathbf{G}$ 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 $\mathbf{x} \in \mathbf{R}^N$ and form the group code $\mathcal{X} = \mathbf{Gx} = \{\rho(g)\mathbf{x} : g \in \mathcal{G}\}$. Suppose $\mathcal{H}$ is a subgroup of $\mathcal{G}$ and form the permutation representation $\phi : \mathcal{G} \to \Gamma = \{\pi_g | g \in \mathcal{G}\}$ of degree n 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 $\mathcal{X}$.*

Corollary 1 *Every group code is equivalent to at least one permutation code.*

In practice, it is often difficult to find the orthogonal matrices that are necessary to show the equivalence of the codes in the previous theorem. Also, the degree 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 *Suppose Γ is doubly transitive. Then ρ is irreducible, $\phi = 1 \oplus \rho$ (here, we use 1 to denote the identity representation of $\mathcal{G}$), and $n = N + 1$.*

Given an irreducible representation $\rho : \mathcal{G} :\to \mathbf{G}$, 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.

References

[1] J. K. Karlof, "Decoding spherical codes for the Gaussian channel," *IEEE Trans. Inform. Theory*, Vol. 39, No. 1, pp. 60–65, January 1993.

[2] D. Slepian, "Permutation modulation," *IEEE Proc.*, pp. 228–236, March 1965.

[3] D. Slepian, "Group codes for the Gaussian channel," *Bell System Technical Journal*, Vol. 47, pp. 575–602, April 1968.