Isometric embeddings of $\mathbb{Z}_{p^k}$ in the Hamming space $\mathbb{F}_p^N$ and $\mathbb{Z}_{p^k}$-linear codes

Marcelo Muniz

Received: 13 March 2003 / Revised: 7 July 2006 / Accepted: 10 July 2006 / Published online: 19 September 2006
© Springer Science+Business Media, LLC 2006

Abstract Isometric embeddings of $\mathbb{Z}_{p^{n+1}}$ into the Hamming space $\left(\mathbb{F}_p^n, w\right)$ have played a fundamental role in recent constructions of non-linear codes. The codes thus obtained are very good codes, but their rate is limited by the rate of the first-order generalized Reed–Muller code—hence, when $n$ is not very small, these embeddings lead to the construction of low-rate codes. A natural question is whether there are embeddings with higher rates than the known ones. In this paper, we provide a partial answer to this question by establishing a lower bound on the order of a symmetry of $\left(\mathbb{F}_p^N, w\right)$.

Keywords Codes over rings · Symmetry group · Isometric embedding · Reed–Muller code

AMS Classifications 94B65

1 Introduction and terminology

In recent years there has been increasing interest in research on codes over modular rings. Starting with the seminal work of Hammons et al. [8] in 1994, where codes over $\mathbb{Z}_4$ provide answers to long-standing questions on binary codes, the applications that were developed in the following years range from methods of construction of non-linear codes in Hamming spaces to the study of unimodular lattices. In the subject of non-linear codes, which is our main concern, the connection between algebraic coding theory over a weighted ring and non-linear codes is made by an isometric embedding...
of $\mathbb{Z}_{p^k}$ in the Hamming space $\left(\mathbb{F}_p^N, w\right)$ (where $\mathbb{F}_p$ is the finite field of $p$ elements). Here we investigate whether it is possible to get better embeddings than the ones already known, at least with respect to the rate $k/N$. In order to state the problem properly, we recall some definitions.

A weight $w$ on a finite ring $R$ is a function $w: R \rightarrow \mathbb{R}$ such that the map $(x, y) \mapsto w(x - y)$ is a distance function on $R$. The pair $(R, w)$ will be called a weighted ring. If $(R, w_1)$ and $(S, w_2)$ are weighted rings, an isometry $\phi: (R, w_1) \rightarrow (S, w_2)$ is an onto map that preserves distances; an isometric embedding is an injective mapping that is an isometry onto its image. Obvious extensions of these concepts are weighted $R$-modules and isometries between weighted modules [in practice, one utilizes mostly the free modules $R^n$ with weight $w_n$ given by $w_n(r_1, \ldots, r_n) = \sum w_R(r_i)$, where $w_R$ is a weight on $R$].

The fundamental example is the Gray map from $\mathbb{Z}_4^n$ to $\mathbb{F}_2^{2n}$. This map takes quaternary codes, i.e., $\mathbb{Z}_4$-submodules of $\mathbb{Z}_4^n$, onto codes in $\mathbb{F}_2^{2n}$, and it does so preserving distances between codewords. The weight considered in $\mathbb{Z}_4^n$ is not the Hamming weight, but the Lee weight. The Lee weight on $\mathbb{Z}_4$ is given by $w_{\text{lee}}(0) = 0$, $w_{\text{lee}}(1) = 1$, $w_{\text{lee}}(2) = 2$, and $w_{\text{lee}}(3) = 1$, and the Lee weight of a vector $(a_1, \ldots, a_n)$ of $\mathbb{Z}_4^n$ is the sum of the Lee weights of its coordinates $a_i$. The Gray encoding $\phi: \mathbb{Z}_4 \rightarrow \mathbb{F}_2$ is given by $\phi(0) = 00$, $\phi(1) = 01$, $\phi(2) = 11$, and $\phi(3) = 10$. Its coordinate-wise extension $\phi: \mathbb{Z}_4^n \rightarrow \mathbb{F}_2^{2n}$ is called the Gray map, and the binary codes that are images of quaternary codes are called $\mathbb{Z}_4$-linear codes. It can be easily checked that this map is really an isometry from $(\mathbb{Z}_4^n, w_{\text{lee}})$ to $(\mathbb{F}_2^{2n}, w)$. This simple fact is a crucial step in all the results obtained in [8], like the description of the Kerdock code as the image by $\phi$ of an extended cyclic quaternary code whose $\mathbb{Z}_4$-dual is equivalent to the Preparata code, which explains why the Kerdock and Preparata codes are formal duals. Not only these and other important problems were solved, but also good non-linear codes were constructed, and the algebraic technique used in these constructions, the Hensel lifting of a cyclic code, can be used for any ring $\mathbb{Z}_{p^k}$. These results motivated the search for generalizations of the Gray encoding to other modular rings. Nevertheless, it was shown in [10] that there is no isometry from $(\mathbb{Z}_{p^k}, w_1)$ to the Hamming space $(\mathbb{F}_p^k, w)$, regardless of the weight $w_1$ being used. Hence, the generalizations of the Gray encoding to the modular rings $\mathbb{Z}_{p^k}$ turn out to be isometric embeddings, rather than isometries.

Starting from the binary case [2], isometric embeddings have been determined for a broad class of weighted rings—namely, finite chain rings with a homogeneous weight [6], which include the rings $\mathbb{Z}_{p^k}$ (see also [1, 4, 5, 7]). In each case the image is the (first-order) Reed–Muller code. The $p$-ary codes obtained as images of $\mathbb{Z}_{p^k}$-submodules of $\mathbb{Z}_{p^k}^n$ are called $\mathbb{Z}_{p^k}$-linear.

Althought several good non-linear codes have been obtained via these embeddings, they are always subcodes of sums of Reed–Muller codes and, therefore, they must have low rate if $k$ is not small. A natural question is whether there exist other extensions of the Gray map that improve on this rate.

It turns out that the existence of an embedding is equivalent to the existence of a symmetry $g$ which has the whole code for its orbit, i.e., $C = \{v, g(v), g^2(v), \ldots, g^{p^k-1}(v)\}$ for any $v$ in $C$ (a symmetry being an isometry from $C$ to itself). Hence, we focus our study on symmetries of codes in $(\mathbb{F}_p^N, w)$. More precisely, we study extendable sym-