On the isometries between $\mathbb{Z}_{p^k}$ and $\mathbb{Z}_p^k$ *

Ana Sălăgean–Mandache †

February 1, 1999

Abstract

We prove that, except for the well-known case $p = k = 2$, it is not possible to construct a weight function on $\mathbb{Z}_{p^k}$ for which $\mathbb{Z}_{p^k}$ is isometric to $\mathbb{Z}_p^k$ with the Hamming metric.

Keywords: Hamming metric, isometry, Gray map.

The Gray map ϕ from $\mathbb{Z}_4$ to $\mathbb{Z}_2^2$ is defined by $\phi(0) = 00$, $\phi(1) = 10$, $\phi(2) = 11$ and $\phi(3) = 01$. It is an isometry between $\mathbb{Z}_4$ with the Lee metric and $\mathbb{Z}_2^2$ with the Hamming metric. This fact played an important role in proving that many important non-linear binary codes are in fact the images under the Gray map of linear codes over $\mathbb{Z}_4$ (see [3] and the references therein). The minimum Lee distance and the Lee weight enumerator of a $\mathbb{Z}_4$-linear code equal the minimum Hamming distance and the Hamming weight enumerator of the binary image of the code under the Gray map. This explained the formal duality of certain pairs of non-linear binary codes that turned out to be the images of dual $\mathbb{Z}_4$-linear codes.

Let $p \geq 2$ be a prime and let $k \geq 2$. The existence of a weight on $\mathbb{Z}_{p^k}$ for which $\mathbb{Z}_{p^k}$ is isometric to $\mathbb{Z}_p^k$ with the Hamming metric would allow the construction of not necessarily linear codes of length kn over $\mathbb{Z}_p$ with the same minimum Hamming distance and Hamming weight enumerator as the

*Research supported by the U.K. Engineering and Physical Sciences Research Council under Grant L07680.

†Algebraic Coding Research Group, Centre for Communications Research, University of Bristol, U.K., e-mail : Ana.Maria.Mandache@bristol.ac.uk

minimum distance and the weight enumerator of $\mathbb{Z}_{p^k}$-linear codes of length n.

We prove that such a weight and isometry do not exist except for the case $p = k = 2$ discussed above. (We excluded the trivial case $k = 1$ from the start). A similar result for the Lee metric on $\mathbb{Z}_p^k$ instead of the Hamming metric is proved in [4] by determining the symmetry group. Our proof is elementary. For codes over $\mathbb{Z}_p$, the commonly used metric is the Hamming metric. It coincides with the Lee metric when $p = 2$ or $p = 3$. A distance-preserving map from $\mathbb{Z}_{2^k}$ to $\mathbb{Z}_2^{2^{k-1}}$ is constructed in [1, 2].

We recall briefly some basic definitions.

Definition 1 *Let A_1, A_2 be two commutative groups in additive notation and $G : A_1 \to A_2$ a map. For $i = 1, 2$ let wt_i be a weight function defined on A_i and let d_i, defined by $\mathrm{d}_i(x, y) = \mathrm{wt}_i(x - y)$ for all $x, y \in A_i$, be the corresponding distance function. Then*

(i) G is a weight-preserving *map if $\mathrm{wt}_2(G(x)) = \mathrm{wt}_1(x)$ for all $x \in A_1$.*

(ii) G is a distance-preserving *map if $\mathrm{d}_2(G(x), G(y)) = \mathrm{d}_1(x, y)$ for all $x, y \in A_1$.*

(iii) G is an isometry *if G is a one-to-one distance-preserving map. If an isometry exists then A_1 and A_2 are called* isometric.

The following facts are easy to verify.

Lemma 2 *Let $G : A_1 \to A_2$ be a distance-preserving map. Then*

(i) G is weight-preserving iff $G(0) = 0$.

(ii) The map $G' : A_1 \to A_2$ defined as $G'(x) = G(x) - G(0)$ is weight-preserving and distance-preserving. If G is an isometry then G' is a weight-preserving isometry.

Denote by wt_H and d_H the Hamming weight and distance functions on $\mathbb{Z}_p^k$. We represent elements of $\mathbb{Z}_p^k$ as k concatenated elements of $\mathbb{Z}_p$ and write b^i for $\underbrace{bb\dots b}_{i}$, where $b \in \mathbb{Z}_p$.

Theorem 3 *There is no weight function on $\mathbb{Z}_{p^k}$ for which $\mathbb{Z}_{p^k}$ is isometric to $\mathbb{Z}_p^k$ with the Hamming metric, except for the case $p = k = 2$.*

Proof. Assume there is a weight function, wt, on $\mathbb{Z}_{p^k}$ such that $\mathbb{Z}_{p^k}$ and $\mathbb{Z}_p^k$ are isometric. Denote by d the corresponding distance function on $\mathbb{Z}_{p^k}$ and by G the isometry. By Lemma 2, we may assume that $G(0) = 0$ and that G is weight-preserving. Hence $\mathrm{d}_H(G(x), G(y)) = \mathrm{d}(x, y) = \mathrm{wt}(x - y) = \mathrm{wt}_H(G(x - y))$ for all $x, y \in \mathbb{Z}_{p^k}$. The main idea of the proof is to use the constraint $\mathrm{d}_H(G(x), G(y)) = \mathrm{wt}_H(G(x - y))$ for showing that G can only exist when $p = k = 2$.

Let $a \in \mathbb{Z}_{p^k}$ be an element of weight 1. We examine the values of $G(ia)$ for $i \in \mathbb{Z}$. We have $\mathrm{d}_H(G((i+1)a), G(ia)) = 1$, so $|\,\mathrm{wt}_H(G((i+1)a)) - \mathrm{wt}_H(G(ia))| \leq 1$. Let j be the integer for which $0 = \mathrm{wt}_H(G(0)) < \mathrm{wt}_H(G(a)) < \mathrm{wt}_H(G(2a)) < \ldots < \mathrm{wt}_H(G(ja)) \not< \mathrm{wt}_H(G((j+1)a))$. Since the weight of $G(ia)$ and of $G((i+1)a)$ differ by at most 1, we have $\mathrm{wt}_H(G(ia)) = i$ for $i = 1, \ldots j$. We have that $1 \leq j \leq k$, as k is the maximum value for the Hamming weight on $\mathbb{Z}_p^k$. After a suitable permutation of the coordinates of $\mathbb{Z}_p^k$ we may assume that $G(ia) = a_1 a_2 \ldots a_i 0^{k-i}$ for $i = 1, \ldots j$, where $a_1, \ldots, a_j \in \mathbb{Z}_p \setminus \{0\}$. Further, let s be the integer for which $j = \mathrm{wt}_H(G(ja)) = \ldots = \mathrm{wt}_H(G((j+s)a)) \neq \mathrm{wt}_H(G((j+s+1)a))$. For any $0 \leq i \leq s-1$, $G((j+i)a)$ and $G((j+i+1)a)$ have the same weight and are at distance 1 from each other, so they must have the same support i.e. all the $G((j+i)a)$, $i = 0, \ldots, s$ have non-zero symbols on the first j positions and zeros on the last $k - j$ positions. Hence $0 \leq s < (p-1)^j$ and $G((j+s)a) = b_1 \ldots b_j 0^{k-j}$ for some $b_1, \ldots, b_j \in \mathbb{Z}_p \setminus \{0\}$. Of course, if $s = 0$ then $a_i = b_i$ for $i = 1, \ldots, j$. Graphically, this looks as follows:

$$
\begin{array}{lclllll}
G(0) & = & & & & & \\
G(a) & = & a_1 & & & & \\
G(2a) & = & a_1 & a_2 & & & \\
G(3a) & = & a_1 & a_2 & a_3 & & \\
\vdots & & \vdots & \vdots & \vdots & & \\
G(ja) & = & a_1 & a_2 & a_3 & \ldots & a_j \\
\vdots & & \vdots & \vdots & \vdots & & \vdots \\
G((j+s)a) & = & b_1 & b_2 & b_3 & \ldots & b_j
\end{array}
$$

with the blanks filled with 0's.

We will now determine $G((j+s+1)a)$. We know it must be obtained from $b_1 \dots b_j 0^{k-j}$ by changing one symbol. We have $\mathrm{d}_H(G((j+s+1)a), G(a)) = \mathrm{wt}_H(G((j+s)a)) = j$. If $s = 0$ we also know $\mathrm{wt}_H(G((j+s+1)a)) = j-1$ from the definitions of j and of s, so we must have $G((j+s+1)a)) = 0a_2 \dots a_j 0^{k-j} = 0b_2 \dots b_j 0^{k-j}$. If $s \geq 1$ then $\mathrm{wt}_H(G((j+s+1)a)) = j \pm 1$ from the definition of s. We cannot have $b_1 = a_1$ because $\mathrm{d}_H(G((j+s)a), G(a)) = \mathrm{wt}_H(G((j+s-1)a)) = j$. So the only possibility of achieving $\mathrm{d}_H(G((j+s+1)a), G(a)) = j$ is $G((j+s+1)a)) = 0b_2 \dots b_j 0^{k-j}$.

We prove next, inductively, that $G((j+s+l)a)) = 0^l b_{l+1} \dots b_j 0^{k-j}$ for all $0 \leq l \leq j$. We have seen that this is true for $l = 0, 1$. We assume the assertion is true for a certain l, $0 < l < j$ and prove it for $l+1$. We have to change one of the symbols of $G((j+s+l)a)) = 0^l b_{l+1} \dots b_j 0^{k-j}$ to obtain $G((j+s+l+1)a))$. If we changed one of the first l zeros, then $\mathrm{d}_H(G((j+s+l+1)a), G((j+s)a))$ would be l or $l-1$ instead of being equal to $\mathrm{wt}_H(G((l+1)a)) = l+1$. If we changed one of the last $k-j$ zeros or if we changed one of the elements $b_{l+1}, \dots, b_j$ to another non-zero element of $\mathbb{Z}_p$ then $\mathrm{d}_H(G((j+s+l+1)a), G(la))$ would be j or $j+1$ instead of being equal to $\mathrm{wt}_H(G((j+s+1)a)) = j-1$. Hence one of the elements $b_{l+1}, \dots, b_j$ has to be changed to a zero, and from the condition $\mathrm{d}_H(G((j+s+l+1)a), G((l+1)a)) = \mathrm{wt}_H(G((j+s)a)) = j$ we see this has to be b_{l+1} i.e. $G((j+s+l+1)a) = 0^{l+1} b_{l+2} \dots b_j 0^{k-j}$, which concludes the induction.

We can now fill in the remaining values in the table:

$$
\begin{array}{lcccccc}
G(0) & = & & & & & \\
G(a) & = & a_1 & & & & \\
G(2a) & = & a_1 & a_2 & & & \\
G(3a) & = & a_1 & a_2 & a_3 & & \\
\vdots & & \vdots & \vdots & \vdots & & \\
G(ja) & = & a_1 & a_2 & a_3 & \dots & a_j \\
\vdots & & \vdots & \vdots & \vdots & & \vdots \\
G((j+s)a) & = & b_1 & b_2 & b_3 & \dots & b_j \\
G((j+s+1)a) & = & & b_2 & b_3 & \dots & b_j \\
G((j+s+2)a) & = & & & b_3 & \dots & b_j \\
\vdots & & & & & & \vdots \\
G((2j+s-1)a) & = & & & & & b_j \\
G((2j+s)a) & = & & & & &
\end{array}
$$

In particular, we have $G((2j+s)a) = 0$ i.e. $(2j+s)a \equiv 0 \bmod p^k$. So for the ideal (a) we have $(a) = \{ia | i \in \mathbb{Z}\} = \{xa | x \in \mathbb{Z}_{p^k}\} = \{ia | i = 0, \dots, 2j+s-1\}$. Let $\mathcal{U} = \{x \in \mathbb{Z}_{p^k} | \operatorname{wt}(x) = 1\}$. We want to determine how many elements are in $(a) \cap \mathcal{U}$. As G is weight-preserving, $(a) \cap \mathcal{U} = \{x \in (a) | \operatorname{wt}_H(G(x)) = 1\}$. If $j \geq 2$ then $(a) \cap \mathcal{U} = \{a, (2j+s-1)a\}$. If $j = 1$ then $(a) \cap \mathcal{U} = \{a, 2a, \dots, (s+1)a\}$ and $s+1 \leq (p-1)^j = p-1$. So $|(a) \cap \mathcal{U}| \leq \max\{2, p-1\}$.

As $a \in \mathcal{U}$ was chosen arbitrarily, we have proved that for any $x \in \mathcal{U}$ there are at most $\max\{2, p-1\}$ elements in in $(x) \cap \mathcal{U}$.

Recall that any element $x \in \mathbb{Z}_{p^k}$ can be written as $x = p^i u$ for some $0 \leq i \leq k-1$ and u a unit in $\mathbb{Z}_{p^k}$. The integer i is unique and will be denoted by $\log_p x$. Choose an element $b \in \mathcal{U}$ with $\log_p b$ minimal. For any other element $c \in \mathcal{U}$, $\log_p c \geq \log_p b$ i.e. $b | c$ and therefore $c \in (b)$. Hence $\mathcal{U} \subseteq (b)$. The number of elements of weight 1 in $\mathbb{Z}_p^k$, and therefore in $\mathbb{Z}_{p^k}$, is $k(p-1)$. So $k(p-1) = |\mathcal{U}| = |(b) \cap \mathcal{U}| \leq \max\{2, p-1\}$. When $k \geq 2$, the inequality $k(p-1) \leq \max\{2, p-1\}$ is satisfied only for $p = k = 2$. (The other solution, $k = 1$ and p arbitrary, corresponds to the trivial isometry between $\mathbb{Z}_p$ and $\mathbb{Z}_p$.) $\square$

We have proved, in particular, that for $p = 2$ and $k > 2$ none of the Gray maps is an isometry. Recall that a Gray map from $\mathbb{Z}_{2^k}$ to $\mathbb{Z}_2^k$ is a one-to-one map G having the property that $G(x)$ and $G(x+1)$ differ by exactly one bit. For weights on $\mathbb{Z}_{2^k}$ with $\mathrm{wt}(1) = 1$ any isometry would in particular be a Gray map.

Acknowledgement. This paper was prompted by the question of C. Carlet (in his presentation of [2]) as to whether there are distance-preserving one-to-one maps from $\mathbb{Z}_8$ to $\mathbb{Z}_2^3$. Financial support from the U.K. Engineering and Physical Sciences Research Council (EPSRC) under grant L07680 is gratefully acknowledged.

References

[1] C. Carlet. $\mathbb{Z}_{2^k}$-linear codes. *IEEE Trans. Inform. Theory*, 44(4):1543–1547, 1998.

[2] C. Carlet. $\mathbb{Z}_{2^k}$-linear codes. In *Proceedings of the 1998 IEEE International Symposium on Information Theory*. IEEE, 1998.

[3] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé. The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes. *IEEE Trans. Inform. Theory*, 40:301–319, 1994.

[4] S. Rodrigues Costa, J. Roberto Gerônimo, R. Palazzo Jr., J. Carmelo Interlando, and M. Muniz Silva Alves. The symmetry group of ${\mathbb{Z}_q}^n$ in the Lee space and the $\mathbb{Z}_{q^n}$-linear codes. In T. Mora and H. Mattson, editors, *Proceedings of the 12th International Symposium, AAECC-12*, number 1255 in LNCS, pages 66–77. Springer Verlag, 1997.