$\mathcal{Z}_4$-linearity cannot be strictly extended to Hamming spaces

Marcelo Muniz and Sueli Costa

October 23, 2001

Abstract

The concept of $\mathbb{Z}_4$-linearity arises from the labeling of the Hamming Space $(\mathbb{Z}_2^2, d_h)$ by the rotation group $\mathbb{Z}_4$ and its coordinate-wise extension to $\mathbb{Z}_2^{2n}$ [4]. This labeling establishes a correspondence between several well-known classes of good non-linear binary codes and submodules of $\mathbb{Z}_4^n$. A natural question should be if $\mathbb{Z}_4$-linearity can be extended to other Hamming spaces. A partial and negative answer to this question have been done [5]: there is no cyclic labeling of $\mathbb{Z}_p^n$ for p prime. In this paper we extend this result showing that there is no cyclic labeling for general Hamming spaces. This points out to how special $\mathbb{Z}_4$-linearity is and also means that any extension of this concept to Hamming spaces must consider other kinds of labeling groups.

1 Introduction

Since the appearance of $\mathbb{Z}_4$-linearity in [4] several papers have dealt with possible extensions of this concept/technique to other alphabets. This question has been addressed in [7] for binary Hamming spaces; this was further developed in [5], where the author proves that there is no possible extension for Hamming spaces $(\mathbb{Z}_p^n, d)$, with p prime. In order to address this question we should explain what we mean by an extension of $\mathbb{Z}_4$-linearity.

The Gray map $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2^2$ given by $\phi(0) = 00$, $\phi(1) = 01$, $\phi(2) = 11$, $\phi(3) = 10$ is the source of $\mathbb{Z}_4$-linear codes. This map is induced by a quarter-of-turn rotation on the vertices of the square $\mathbb{Z}_2^2$ and its coordinate-wise extension is an action of $\mathbb{Z}_4^n$ in $\mathbb{Z}_2^{2n}$, which is also an isometry between lee space $(\mathbb{Z}_4^n, d_{lee})$ and the Hamming space $(\mathbb{Z}_2^{2n}, d)$[4].

In [5], the extension problem is considered by showing that there is no invariant metric d' (weight) on the cyclic group $\mathbb{Z}_{p^k}$ such that $(\mathbb{Z}_{p^k}, d')$ and the Hamming space $(\mathbb{Z}_p^k, d)$ are isometric, for p prime. Here we translate $\mathbb{Z}_4$-linearity and the possibility of extensions of $\mathbb{Z}_4$-linearity in terms of group actions and extend the previous result for any number p and in fact to general Hamming spaces.

To consider a generic situation, let X be a finite set. The Hamming space (X^n, d) is the metric space over X^n with metric

$$d((p_1, ..., p_n), (q_1, ..., q_n)) = \text{the number of distinct coordinates.}$$

Let G be a group which acts as a group of isometries in the metric space (X^n, d). For each point $p \in X^n$ we have an evaluation map $ev_p : G \to X^n$ given by $ev_p(g) = g(p)$. When G acts freely, this induces a metric on G given by $d_p(g, h) = d(g(p), h(p))$. This metric is also left-invariant, $d_p(g, h) = d_p(h^{-1}g, id)$. $\mathbb{Z}_4$-linearity follows this pattern, and the Lee distance on $\mathbb{Z}_4^n$ is just the induced metric d_p with $p = 0$. So, in this context, the search for an extension of $\mathbb{Z}_4$-linearity can be translated in terms of group actions: is there a cyclic group G acting sharply transitively (freely and transitively) on (X^n, d) as a group of isometries? Such a group should is called a labeling group. The labeling maps are the ev_p's defined above.

The answer unfortunately is no (Theorem 1). One may ask then if it is possible to use, for instance, abelian labeling groups instead of cyclic ones, and still get good "linearizing" results for codes. This is still an open question for Hamming spaces. For Lee spaces $(\mathbb{Z}_m^n, d_{lee})$ there is no cyclic [1] neither abelian labeling group [6]. Anyway, the result obtained here shows once more that $\mathbb{Z}_4$-linearity is quite a special phenomenon in coding theory.

2 There is no cyclic labeling for Hamming spaces

The proof only makes use of some basic geometric features of Hamming spaces and a characterization of cyclic groups.

In a Hamming space (X^n, d) we consider the "lines" $X_{i,p}$ passing by a point p which are given by

$$X_{i,p}=\{(p_1,\dots,p_{i-1},x,p_{i+1},\dots,p_n)|x\in X\}.$$

Lemma 1 *Let $B_1(p)$ be the unitary ball centered at $p\in X$. For any other point q, we have*
(H1) *$d(p,q)=1$ if and only if $B_1(p)\cap B_1(q)=X_{i,p}=X_{i,q}$ for some i;*
(H2) *$d(p,q)=2$ if and only if $B_1(p)\cap B_1(q)$ is a set of two distinct points.*

These equivalences are important in the results that follow.
We will also the following Lemma:

Lemma 2 *Let G be a group. Then G is cyclic if and only if for any element $g\neq id$ of G, if h is another element and $|h|$ divides $|g|$, then $h\in\langle g\rangle$.*

In what follows, the point $p=(p_1,p_2,\dots,p_n)$ is fixed and we will write X_i instead of $X_{i,p}$, for notational convenience.

Lemma 3 *Let g be an isometry of (X^n,d) ,$m>2$, and G be the subgroup generated by g, $G=\langle g\rangle$. Then*
(i) *If $p,g^t(p)$ and $g^s(p)$ are distinct points, $g^t(p)$ and $g^s(p)$ both lying in the same line X_i, then $g^{t-s}(p)$ also lies on X_i.*
(ii) *Let G act freely in X^n. If $g(p)$ and $g^2(p)$ lie in the same line X_i, then the orbit $G(p)=\{g^k(p)|k=1,2,\dots,|g|\}$ is contained in X_i.If $g(p)$ lies in X_i but $g^2(p)$ does not, the only points in the intersection of the orbit $G(p)$ with X_i are p and $g(p)$.*

Proof (i) By hypothesis, $d(g^t(p),g^s(p))=1$ and $d(g^s(p),p)=1$. Therefore $d(g^{t-s}(p),p)=d(g^t(p),g^s(p))=1$ and $d(g^{t-s}(p),g^t(p))=d(g^{-s}(p),p)=d(p,g^s(p))=1$. This shows that $g^{t-s}\in B_1(p)\cap B_1\,(g^t(p))=X_i$.

(ii.a) Suppose that $g(p)$ and $g^2(p)$ belong to X_i. Since G acts freely, $g^k(p)\neq g^l(p)$ if $k\neq l$ and $0<k,l\leq|g|$. For $k=|g|-1$, we have $g^{|g|-1}(p)=g^{-1}(p)=g^{1-2}(p)\in X_i$ by (i). For all other k we can set by induction that if $g^k(p)\in X_i$, then $g^{k+1}(p)=g^{k-(-1)}(p)\in X_i$.

(ii.b) Now, if $g(p)\in X_i$ and $g^2(p)\notin X_i$, let $t>1$ be the first exponent such that $g^t(p)$ belongs to X_i. We will show that $g^t=id$. Surely $g^t(p)\neq g(p)$, because $g^t(p)=g(p)\Leftrightarrow g^{t-1}(p)=p$, a contradiction with the choice of t. On the other hand, if $g^t(p)\neq p$, then the points $p,g(p),g^t(p)$ are all distinct and lie on X_i, hence $g^{t-1}(p)$ also belongs to X_i (by (i)), another contradiction. Therefore $g^t(p)=p$, which implies that $g^t=id$, and $G(p)\cap X_i=\{p,g(p)\}$.

(ii.a) Suppose that $g(p)$ and $g^2(p)$ belong to X_i. Since G acts freely, $g^k(p)\neq g^l(p)$ if $k\neq l$ and $0<k,l\leq|g|$. For $k=|g|-1$, we have $g^{|g|-1}(p)=g^{-1}(p)=g^{1-2}(p)\in X_i$ by (i). For all other k we can set by induction that if $g^k(p)\in X_i$, then $g^{k+1}(p)=g^{k-(-1)}(p)\in X_i$.

(ii.b) Now, if $g(p)\in X_i$ and $g^2(p)\notin X_i$, let $t>1$ be the first exponent such that $g^t(p)$ belongs to X_i. We will show that $g^t=id$. Surely $g^t(p)\neq g(p)$, because $g^t(p)=g(p)\Leftrightarrow g^{t-1}(p)=p$, a contradiction with the choice of t. On the other hand, if $g^t(p)\neq p$, then the points $p,g(p),g^t(p)$ are all distinct and lie on X_i, hence $g^{t-1}(p)$ also belongs to X_i (by (i)), another contradiction. Therefore $g^t(p)=p$, which implies that $g^t=id$, and $G(p)\cap X_i=\{p,g(p)\}$.

Theorem 1 *Let (X^n,d) be the Hamming space over X^n, where $|X|=m$. If $(m,n)\neq(2,2)$ and $n>1$, then there is no cyclic labeling of (X^n,d).*

Proof The proof of this statement splits in two cases, $m=2$ and $m>2$. Although the binary case is only a subcase of the results presented in [5], we produce another proof here for the sake of completeness and to see how the $\mathbb{Z}_4$-linearity appears naturally in this context.

We start with $m>2$. Suppose that there is a cyclic group G acting sharply transitively on X^n as a group of isometries, and let g be a generator for G. For each X_i we take k_i as the least positive integer such that $g^{k_i}(p)\in X_i$, and define G_i to be the subgroup of G generated by g^{ki}, $G_i=\langle g^{k_i}\rangle$. We will show that $n=1$.

Suppose that $g^{2k_1}(p)\notin X_1$.

By Lemma 1.ii, $G_1(p)\cap X_1=\{p,g^{k_1}(p)\}$. Since $m>2$, there is a point $q\in X_1$ such that $q\neq p$ and $q\neq g^{k_1}(p)$. By hypothesis there is $t, 0<t<m^n$, such that $g^t(p)=q$. Lemma 1.i assures that $g^{t-k_1}(p)\in X_1$. On the other hand, we also have $d(g^{t-k_1}(p),g^{-k_1}(p))=d(g^t(p),p)=1$. Since $d(g^{-k_1}(p),p)=d(g^{k_1}(p),p)=1$, but $g^{-k_1}(p)\notin X_1$, we must have $g^{-k_1}(p)=(p_1,\dots,p_{j-1},a,p_{j+1},\dots,p_n)$, with $a\neq p_j$ and $j\neq 1$ Therefore $g^{t-k_1}(p)$ belongs to $B_1(g^{-k_i}(p))\cap X_1=\{p\}$. Hence $g^{t-k_1}(p)=p$, what implies $q=g^t(p)=g^{k_1}(p)$, a contradiction. This means that $G(p)\cap X_i=G_i(p)\cap X_i=\{p,g^{k_1}(p)\}$ and we do not have a labeling, contradiction again. Then it must be the case that $g^{2k_1}(p)\in X_1$.

Let's show now that the condition $g^{2k_1}(p)\in X_1$ implies $G_1(p)=X_1$. By Lemma 1.ii we already know that $G_1(p)\subset X_1$.For the converse, let v be any point in X_1 and l be such that $0\leq l<m^n$, $g^l(p)=v$. There is a $s\geq 0$ such that $sk_1\leq l<(s+1)k_1$ or, in other words, $0\leq l-sk_1<k_1$. Suppose that $l\neq sk_1$. Then lemma 1.i guarantees that $g^{l-sk_1}(p)\in X_1$, but the minimality of k_1 implies that $l-sk_1=0$, contradiction. Hence

$g^l = g^{sk_1}$ belongs to G_1. This shows that $G_1(p) = X_1$. This also implies that $|G_1| = m$, because the action of G is free, and then $G_1 = \left\langle g^{m^{n-1}} \right\rangle$ by (CG).

Can n be greater than 1? Certainly not. Suppose that $n > 1$ and let $j \neq 1$. We cannot have $g^{2k_j}(p)$ lying in X_j because this would lead us to $|G_j| = m$ and then $G_j = \left\langle g^{m^{n-1}} \right\rangle = G_1$ ((CG) again). Neither can we have $g^{2k_j}(p) \notin X_j$ (as we have seen above), for we have seen that this leads to $X_j = G(p) \cap X_j = \{p, g^{k_j}(p)\}$, absurd ($|X_j| > 2$). Conclusion: $n = 1$, $G_1 = \langle g \rangle = G \cong \mathbb{Z}_m$.

For the binary case, identify X^n with $\mathbb{Z}_2^n$, p with the origin and let $\{e_1, \ldots, e_n\}$ be the canonical basis of $\mathbb{Z}_2^n$. This is just for notational convenience: we will not use other algebraic structures besides the group structure of G.

Let g and G be as before, and let k be the solution of $g^k(0) = e_1$, $0 < k < 2^n$. We will show that either $n = 2$ and $k = 1$ or 3 (a $\mathbb{Z}_4$ labeling), or $n = k = 1$.

Suppose that $|g^k| > 2$; then $g^{-k} \neq g^k$, so that $g^{-k}(0) = e_j$ for some $j \neq 1$. Let l be such that $g^l(0) = e_1 + e_j$. We have

$$d(g^{l+k}(0), g^l(0)) = d(g^k(0), 0) = 1;$$
$$d(g^{l+k}(0), 0) = d(g^l(0), g^k(0)) = 1.$$

Then we can assert that

$$g^{l+k}(0) \in S_1(0) \cap S_1(g^l(0)) = \{g^k(0), g^{-k}(0)\} \Longrightarrow g^{l+k} = g^{\pm k}.$$

We get either $g^l = g^0 = id$, which means $0 = e_1 + e_j$, nonsense, or $g^l = g^{2k}$, the right answer. The same reasoning applied to g^{l-k} in place of g^{l+k} yields $g^l = g^{-2k}$, i.e., $g^{2k} = (g^{2k})^{-1}$, and therefore g^{2k} has order two. This implies that g^k has order four.

By (CG) we know that any element of order four belongs to $\left\langle g^{2^{n-2}} \right\rangle$, which has only two of such elements, $g^{2^{n-2}}$ and $g^{3 \cdot 2^{n-2}}$. This implies that only two points of $S_1(0)$ can be reached by elements of order greater than 2, e_1 and e_j. If $n > 2$ the other points of the unit sphere must be reached by elements of order two, but the only element of order two $g^{2^{n-1}}$ is exactly our g^l above. Since the action of G is transitive and only two points in $S_1(0)$ are in its orbit, we conclude that $n = 2$, $k = 1$ or 3, and the corresponding actions of $\mathbb{Z}_4$ on $\mathbb{Z}_2^2$ are the generated by a clockwise or counter-clockwise (Gray map) quarter-of-turn rotation, respectively.

To conclude the proof we must examine the case $|g^k| = 2$, i.e., $k = 2^{n-1}$. We claim that this leads to $n = 1$. In fact, any g^t satisfying $d(g^t(0), 0) = 1$ must have order 2 or 4, as seen above. If $|g^t| = 4$, then we have just seen that $g^{2^{n-1}}(0)$ does not belong to $B_1(0)$. Hence $g^t(0) \in B_1(0) \Rightarrow t = 2^{n-1}$. Since G acts transitively, $n = 1$ and $G = \mathbb{Z}_2$, the trivial action.

Corollary 1 *There is no labeling of the Hamming spaces $(GF(q^k)^n, d)$ and $(\mathbb{Z}_{q^k}^n, d)$ by $\mathbb{Z}_{q^{kn}}$, except for $q = 2, k = 1$ and $n = 2$ (and the trivial ones for $n = 1$).*

3 Concluding remarks

In this paper we rule out any possibility of extending $\mathbb{Z}_4$-linear codes to other cyclic group actions in Hamming spaces, thus establishing, in a certain sense, the "uniqueness" of $\mathbb{Z}_4$-linearity. Nevertheless, there are more general open questions related to possible good codes if we allow other kinds of groups. The idea is to consider "linearization" of codes in a wider sense, but still linking codes to isometry groups, to assure geometrical uniformity considering the concept introduced in [4] extended to Hamming spaces.

References

[1] S. I. R. Costa, J. R. Gerônimo, R. Palazzo Jr. and M. M. S. Alves, The Symmetry Group of $\mathbb{Z}_q^n$ in the Lee space and the $\mathbb{Z}_{q^n}$-Linearity. In: Proceedings of the Symposium on Applied Algebra and Error Correcting Codes, series *Lecture Notes in Computer Science*. Springer Verlag, New York, **1255** (1997), 66-77.

[2] G. D. Forney, Geometrically Uniform Codes, *IEEE Trans. Inform. Theory*, **37** **(5)** (1991) 1241-1260.

[3] J. R. Gerônimo, "Extension of the $\mathbb{Z}_4$-linearity via Symmetry Groups". Ph.D. dissertation, FEEC-UNICAMP, 1997. (in Portuguese).

[4] A. R. Hammons Jr., P. V. Kumar,A. R. Calderbank, N. J. Sloane and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inform. Theory*, **40** (**2**) (1994), 301-319.

[5] A. S. Mandache, On The Isometries Between $\mathbb{Z}_{p^k}$ and $\mathbb{Z}_p^k$, *IEEE Trans. Inform. Theory*, vol. (**45**) **6** (1999), 2145-2148.

[6] M.Muniz and S. Costa, Can $\mathbb{Z}_4$-linearity be Extended to Lee Spaces?. In: Proceedings of the VI International Workshop on Algebraic and Combinatorial Coding Theory, Bulgaria, June 2000.

[7] C. Carlet, $\mathbb{Z}_{2^k}$-linear codes, *IEEE Trans. Inf. Theory*, **44** (**6**) (1998), 1543-1547.