Extended 1-perfect additive codes*

J.Borges, K.T.Phelps †, J.Rifà‡

7/05/2002

Abstract

A binary extended 1-perfect code of length $n+1=2^t$ is additive if it is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. The punctured code by deleting a $\mathbb{Z}_2$ coordinate (if there is someone) gives a perfect additive code. 1-Perfect additive codes were completely characterized in [1] and by using that characterization we compute the possible parameters k, rank and dimension of the kernel for extended 1-perfect additive codes. A very special case is that of extended 1-perfect $\mathbb{Z}_4$-linear codes.

1 Introduction

Let $\mathbb{F}=\mathbb{Z}/2$ and let $\mathbb{F}^n$ denote the set of all binary vectors of length n. Let $\star$ be a binary operation such that $(\mathbb{F}^n,\star)$ is a translation invariant abelian group, that is, a group with the property that

$$d(x\star v, x\star u)=d(v,u)\ \ \forall x,v,u\in\mathbb{F}^n$$

As can be seen in [1], $(\mathbb{F}^n,\star)\cong(\mathbb{Z}_2^\alpha\times\mathbb{Z}_4^\beta,+)$ where $\alpha+2\beta=n$. An isomorphism between $\mathbb{Z}_2^\alpha\times\mathbb{Z}_4^\beta$ and $\mathbb{F}^n$ is given by the map

$$\Phi(x_1,\ldots,x_\alpha\mid y_1,\ldots,y_\beta)=(x_1,\ldots,x_\alpha\mid \phi(y_1),\ldots,\phi(y_\beta))$$

*Research partially supported by Spanish CICYT Grants TIC00-0232-P4-02, TIC2000-0739-c04-01 and also supported by Catalan DURSI grant 2001SGR 00219

†K.T.Phelps is with the Discrete & Statistical Sciences, Auburn University, Auburn, Al 36849-5307. USA. E-mail: phelpkt@dms.auburn.edu

‡J.Borges and J.Rifà are with the Computer Sciences Department, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain. E-mail: {joaquim.borges,josep.rifa}@uab.es

where $\phi(0) = (0,0), \phi(1) = (0,1), \phi(2) = (1,1)$ and $\phi(3) = (1,0)$ is the usual Gray map from $\mathbb{Z}_4$ onto $\mathbb{Z}_2^2$. Now, it is clear that

$$x \star y = \Phi(\Phi^{-1}(x) + \Phi^{-1}(y)) \ \ \forall x, y \in \mathbb{F}^n.$$

A *(binary) additive code* (see [1], [2]) $(C, \star)$ of length n is a subgroup of $(\mathbb{F}^n, \star)$. For the rest of the paper we assume that all codes are binary. An additive code is a particular case of the more general class of *translation-invariant propelinear codes* [5] and [1]. Note that the case $\beta = 0$ corresponds to a linear code and the case $\alpha = 0$ corresponds to a $\mathbb{Z}_4$-linear code. The single-error correcting perfect additive codes (or 1-perfect additive codes) were completely characterized in [1]. In this case, there is exactly one 1-perfect additive code of length $n = 2^t - 1$, up to coordinate permutation, for any r such that $2 \leq r \leq t \leq 2r$, where $\alpha = 2^r - 1$ and $\beta = 2^{t-1} - 2^{r-1}$.

We will refer to the group of coordinate permutations $\pi : C \to C$ as $Aut(C)$, the automorphism group of the code. Define $C^{\perp}$ as the dual of the span of C and the kernel of code C as $K = \{a \in C | \, a + C = C\}$. In this paper we study extended 1-perfect additive codes, we compute some invariants, namely, the rank (dimension of the linear span of the code) and dimension of the kernel (set of vectors that leave invariant the code under translation). We put special attention to the case of extended perfect $\mathbb{Z}_4$-linear codes.

The paper is organized as follows. In Section 2 we give a characterization for extended 1-perfect additive codes in the non $\mathbb{Z}_4$-linear case and we compute the rank and the kernel. In Section 3 we do the same for the special case of $\mathbb{Z}_4$-linear codes.

2 Extended 1-perfect additive non $\mathbb{Z}_4$-linear codes

Let C be a binary additive code, that is to say $(C, \star)$ is a subgroup of $(\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}, +)$, where $+$ means the usual additive operation on $\mathbb{Z}_2$ and $\mathbb{Z}_4$. Code C has length $n = \alpha + 2\beta$ as a binary code, after doing the Gray map in its $\mathbb{Z}_4$ coordinates. We say that C is an additive code of type (α, β).

Theorem 2.1 *If C^* is an extended 1-perfect additive code of length $n+1 = 2^t$, then it is of type $(\alpha + 1, \beta)$, where either $\alpha + 1 = 0$ or $\alpha = 2^r - 1$, $2 \leq r \leq t \leq 2r$.*

Proof: Recall from [1] that any 1-perfect additive code of length $n = 2^t - 1 \geq 15$ is of type $(2^r - 1, 2^{t-1} - 2^{r-1})$, where $2 \leq r \leq t \leq 2r$. If C^* has $\mathbb{Z}_2$ coordinates then puncture it in one of these coordinates preserves the additive structure. Conversely, the gray map preserves parity so adding a parity check bit just increases the number of $\mathbb{Z}_2$ coordinates. ∎

Corollary 2.2 *For any r and $t \geq 4$ such that $2 \leq r \leq t \leq 2r$ there is exactly one extended 1-perfect additive code C^* of type $(2^r, 2^{t-1} - 2^{r-1})$, up to coordinate permutation.*

Proof: The statement follows directly from the previous theorem and the uniqueness of 1-perfect additive codes (see [1]). ∎

Now, given an extended 1-perfect additive code C^* we compute its rank $r(C^*)$ and dimension of the kernel $K(C^*)$.

Theorem 2.3 *Let C^* be an extended 1-perfect additive code of type $(2^r, 2^{t-1} - 2^{r-1})$, where $t > 3$, then*

(i) $dim(K(C^*)) = 2^{r-1} + 2^{t-1} - r$ *if* $t \neq r$ *and* $dim(K(C^*)) = 2^r - r - 1$ *if* $t = r$.

(ii) $r(C^*) = 2^t - r - 1$.

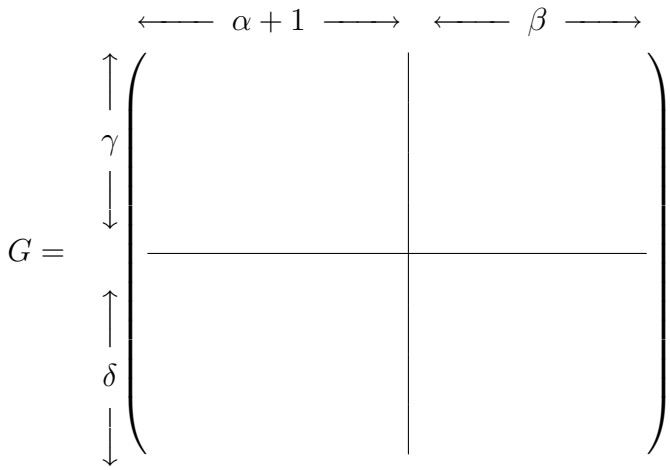
Proof: Let C be the 1-perfect additive code obtained by puncturing a $\mathbb{Z}_2$ coordinate. Let $x \in C$ and let x^* denote the word x with a parity check bit. It is clear that $x \in K(C)$ if and only if $x^* \in K(C^*)$. Also, $x \in < C >$ if and only if $x \in < C^* >$. Hence the dimension of the kernel and the rank are the same for C^* and for C. The values for C are stated in [4] and are those of the statement. ∎

For any allowable parameter r and t, code C^* could be seen as the kernel of a group homomorphism:

$$\mathbb{F}^n = \mathbb{Z}_2^{\alpha+1} \times \mathbb{Z}_4^{\beta} \xrightarrow{\theta} \mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta}$$

where: $\alpha + 1 = 2^r$; $\beta = 2^{t-1} - 2^{r-1}$; $\gamma = 2r - t + 1$; $\delta = t - r$.

This previous homomorphism could be represented by a matrix like:



For instance, in length $n = 31$ (so $t = 5$) there are three different pairs of allowable parameters (see Corollary 2.2): $(r = 3, t = 5)$, $(r = 4, t = 5)$, $(r = 5, t = 5)$ which give us, respectively, code C_1 where $\gamma = 2$ and $\delta = 2$; code C_2 where $\gamma = 4$ and $\delta = 1$; code C_3 where $\gamma = 6$ and $\delta = 0$.

These three codes are given by the following parity check matrices:

Code C_1 is the kernel of the homomorphism $\mathbb{F}^{32} = \mathbb{Z}_2^8 \times \mathbb{Z}_4^{12} \longrightarrow \mathbb{Z}_2^2 \times \mathbb{Z}_4^2$ which is given by:

$$G_1 = \left(\begin{array}{cccccccc|cccccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 & 1 & 1 & 1 & 1 & 0 & 2 & 1 & 1 & 1 & 1 & 0 & 2 \\ 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 1 & 2 & 3 & 1 & 1 & 0 & 1 & 2 & 3 & 1 & 1 \end{array}\right)$$

The rank of this code is $2^t - r - 1 = 28$ and the dimension of its kernel is $2^{r-1} + 2^{t-1} - r = 17$.

Code C_2 is the kernel of the homomorphism $\mathbb{F}^{32} = \mathbb{Z}_2^{16} \times \mathbb{Z}_4^8 \longrightarrow \mathbb{Z}_2^4 \times \mathbb{Z}_4$ which is given by:

$$G_2 = \left(\begin{array}{cccccccccccccccc|cccccccc} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \\ \hline 0&0&0&0&0&0&0&0&2&2&2&2&2&2&2&2&1&3&1&3&1&3&1&3 \end{array}\right)$$

The rank of this code is $2^t - r - 1 = 27$ and the dimension of its kernel is $2^{r-1} + 2^{t-1} - r = 20$.

Code C_3 is the kernel of the homomorphism $\mathbb{F}^{32} = \mathbb{Z}_2^{32} \longrightarrow \mathbb{Z}_2^6$ which is given by the usual parity check matrix for the linear extended Hamming code.

$$G_3 = \left(\begin{array}{cccccccccccccccc} 1&1&1&1&1&1&1&1&\cdots&1&1&1&1&1&1&1&1 \\ 1&1&1&1&1&1&1&1&\cdots&0&0&0&0&0&0&0&0 \\ 1&1&1&1&1&1&1&1&\cdots&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&1&1&1&\cdots&0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1&\cdots&0&0&1&1&0&0&1&1 \\ \hline 0&1&0&1&0&1&0&1&\cdots&0&1&0&1&0&1&0&1 \end{array}\right)$$

The rank of this code is $2^t - r - 1 = 26$ and the dimension of its kernel is $2^{r-1} + 2^{t-1} - r - 1 = 26$.

Notice that all these matrices could be used as parity check matrices for the corresponding codes C_1, C_2 or C_3 and the columns, like in the usual binary extended Hammimg code, are all the possible independent vectors in $\{1 \in \mathbb{Z}_2\} \times \mathbb{Z}_2 \times \mathbb{Z}_4^2$ for code C_1, in $\{1 \in \mathbb{Z}_2\} \times \mathbb{Z}_2^3 \times \mathbb{Z}_4$ for code C_2 and in $\{1 \in \mathbb{Z}_2\} \times \mathbb{Z}_2^5$ for code C_3.

Next section is devoted to consider the case in theorem 2.1 when $\alpha + 1 = 0$.

3 Extended 1-perfect $\mathbb{Z}_4$-linear codes

Let C^* be an extended 1-perfect additive code of length $n+1 = 2^t \geq 16$ and of type $(\alpha + 1, \beta)$ where $\alpha + 1 = 0$. In other words, C^* is a $\mathbb{Z}_4$-linear code of binary length $n + 1 = 2^t \geq 16$.

Consider the quotient group $\mathbb{F}^{n+1}/C^*$ which is isomorphic to $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ where $\gamma + 2\delta = t + 1$ (because the number of cosets is 2^{t+1}). Clearly, the cosets with

leader of weight 1 are elements of order 4 (implying $\delta \geq 1$), whereas the cosets with leader of weight 2 are elements of order 2 or 4. Hence the number of solutions of $\gamma + 2\delta = t + 1$ is $\lfloor (t+1)/2 \rfloor$.

Theorem 3.1 *Let C^* be an extended 1-perfect $\mathbb{Z}_4$-linear code of binary length $n+1 = 2^t \geq 16$, such that $\mathbb{F}^{n+1}/C^*$ is isomorphic to $\mathbb{Z}_2^{t+1-2\delta} \times \mathbb{Z}_4^{\delta}$ for a fixed $\delta \in \{1, \ldots, \lfloor (t+1)/2 \rfloor\}$. Then C^* is unique, up to coordinate permutation.*

Proof: Let $\vartheta : \mathbb{F}^{n+1} \longrightarrow \mathbb{F}^{n+1}/C^*$ be the natural projection and let $\varphi : \mathbb{F}^{n+1}/C^* \longrightarrow \mathbb{Z}_2^{t+1-2\delta} \times \mathbb{Z}_4^{\delta}$ be an isomorphism. Put $\theta = \varphi\vartheta$. We have $C^* = Ker\,\theta$ and if we change θ by θ', note that for all $i \in \{1, \ldots, n+1\}$, $\theta'(e_i) = \theta(e_j)$ for some $j \in \{1, \ldots, n+1\}$. This says that $Ker\,\theta'$ can be obtained as a coordinate permutation of C^*. ∎

Corollary 3.2 *For all $t \geq 4$, there are exactly $\lfloor (t+1)/2 \rfloor$ extended 1-perfect $\mathbb{Z}_4$-linear codes of length $n+1 = 2^t$.*

Proof: This result has been previously stated in [3]. Note that each one of the nonequivalent codes of length $n+1 = 2^t$ corresponds to a different quotient groups $\mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta}$. ∎

As in the previous case of extended 1-perfect additive non-$\mathbb{Z}_4$-linear codes, for any allowable pair of parameters γ and δ we can construct an extended 1-perfect $\mathbb{Z}_4$-linear code (which is unique up to isomorphism) as the kernel of a group homomorphism:

$$\mathbb{F}^{n+1} = \mathbb{Z}_4^{\beta} \xrightarrow{\theta} \mathbb{Z}_2^{\gamma} \times \mathbb{Z}_4^{\delta}$$

where: $n+1 = 2^t$; $\beta = 2^{t-1}$; $t+1 = \gamma + 2\delta$.

For instance, in case of length $n+1 = 32$ ($t = 5$) we have three possible pairs of parameters: ($\gamma = 0$, $\delta = 3$) which leads to code D_1; ($\gamma = 2$, $\delta = 2$) which leads to code D_2 and ($\gamma = 4$, $\delta = 1$) which leads to code D_3.

Code D_1 is the kernel of the homomorphism $\mathbb{F}^{32} = \mathbb{Z}_4^{16} \longrightarrow \mathbb{Z}_4^3$ which is given by:

$$G_1 = \left(\begin{array}{cccccccccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 \\ 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \end{array} \right)$$

Code D_2 is the kernel of the homomorphism $\mathbb{F}^{32} = \mathbb{Z}_4^{16} \longrightarrow \mathbb{Z}_2^2 \times \mathbb{Z}_4^2$ which is given by:

$$G_2 = \left(\begin{array}{cccccccccccccccc} 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 \end{array}\right)$$

Code D_3 is the kernel of the homomorphism $\mathbb{F}^{32} = \mathbb{Z}_4^{16} \longrightarrow \mathbb{Z}_2^4 \times \mathbb{Z}_4^1$ which is given by:

$$G_3 = \left(\begin{array}{cccccccccccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right)$$

Notice that all these matrices could also be used as parity check matrices for the corresponding codes D_1, D_2 or D_3 and the columns, like in the usual binary extended Hammimg code, are all the possible independent vectors in $\mathbb{Z}_4^2 \times \{1 \in \mathbb{Z}_4\}$ for code D_1, in $\mathbb{Z}_2^2 \times \mathbb{Z}_4 \times \{1 \in \mathbb{Z}_4\}$ for code D_2 and in $\mathbb{Z}_2^4 \times \{1 \in \mathbb{Z}_4\}$ for code D_3.

So, in general, we can think of the parity check matrix of C^* as consisting of all column vectors of the form $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^{\delta-1} \times \{1 \in \mathbb{Z}_4\}$.

Lemma 3.3

$$\mathbb{F}^{n+1} = \mathbb{Z}_4^\beta \xrightarrow{\theta} \mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta \xrightarrow{\tau} \mathbb{Z}_2^\gamma \times \mathbb{Z}_2^\delta = \mathbb{Z}_2^{\gamma+\delta}$$

$\psi = \tau\theta$ is a linear mapping form the binary linear space $\mathbb{F}^{n+1}$ to $\mathbb{Z}_2^{\gamma+\delta}$.

Proof: Let π be any involution involving the two coordinates in some $\mathbb{Z}_4$. Let these coordinates be e_i and e_{i+1}. Take $v \in \mathbb{F}^{n+1}$ and note that $\pi(v) = v$ or $\pi(v) = v \star e_i \star e_i$.

Then in both cases $\tau \cdot \theta(\pi(v)) = \tau \cdot \theta(v)$.

We can generalize this result by taking any permutation π_w associated to vector w. We know permutation π_w is a composition of permutations like π, so $\tau \cdot \theta(\pi_w(v)) = \tau \cdot \theta(v)$.

Hence, $\tau \cdot \theta(w+v) = \tau \cdot \theta(w \star \pi_w(v)) = \tau \cdot \theta(w) + \tau \cdot \theta(\pi_w(v)) = \tau \cdot \theta(w) + \tau \cdot \theta(v)$.

∎

Lemma 3.4 *For all $t \geq 4$, $< C^* > \subseteq Ker\ \psi$ and for $t > 4$ or $t = 4$ and specific parameters $\gamma = 1$, $\delta = 2$ then $< C^* > = Ker\ \psi$.*

Proof: The first assertion is easy to verify. $Ker\ \psi$ is generated by vectors of type $(0, 0, \ldots, 2, 0, \ldots, 0)$. The only way such a vector belongs to $< C^* >$ is when there are two binary codewords of weight 4 with share a unique coordinate. This happens for all $t > 4$ and for $t = 4$ in the specific case $\gamma = 1$, $\delta = 2$.

In this last situation the parity check matrix is:

$$H = \left(\begin{array}{cccccccc} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ \hline 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \end{array}\right)$$

and the binary codewords $(1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1)$ and $(1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0)$, which can be written by using the Gray map as $(1, 3, 0, 0, 0, 1, 0, 3)$ and $(1, 0, 3, 0, 3, 0, 1, 0)$, share a unique coordinate, the first one. ∎

Theorem 3.5 *Let C^* be an extended 1-perfect $\mathbb{Z}_4$-linear code of binary length $n + 1 = 2^t > 16$ and assume the quotient set is isomorphic to $G = \mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Then $rank(C^*) = 2^t - t - 1 + \delta$. For the case $t = 4$, either $G = \mathbb{Z}_2^{t-1} \times \mathbb{Z}_4$ and $rank(C^*) = 2^t - t - 1$, i.e. C^* is linear, or $G = \mathbb{Z}_2 \times \mathbb{Z}_4^2$ and $rank(C^*) = 2^t - t - 1 + 2$.*

Proof: From lemma 3.4 in the general case $| < C^* > | = |Ker\ \psi| = \dfrac{|\mathbb{F}^{n+1}|}{|\mathbb{Z}_2^{\gamma+\delta}|} = 2^{n+1-\gamma-\delta} = 2^{2^t-t-1+\delta}$. ∎

After computing the rank of this kind of codes we are interested in the computation of the kernel dimension.

Recall that a $\mathbb{Z}_4$-linear code C is a translation-invariant propelinear code (see [5]). Considering such structure, $(C, \star)$ is a group, where each codeword x has associated a coordinate permutation π_x which verifies that $x \star y = x + \pi_x(y)$, for any $y \in C$. Operation $\star$ can be seen as the additive $\mathbb{Z}_4$ operation and $\pi_x = (a_1 a_1') \cdots (a_\beta a_\beta')$ is the product of all involutions involving the two binary coordinates in every $\mathbb{Z}_4$ coordinate where x is 1 or 3.

Define $A_\pi = \{z \in C^* \mid \pi_z = \pi\}$ and let $\sigma \in \mathcal{S}_n$ be the permutation $\sigma = (a_1 a_1') \cdots (a_\beta a_\beta')$ which is the product of all involutions involving the two coordinates in every $\mathbb{Z}_4$ component. Then $\sigma \in Aut(C^*)$.

Lemma 3.6 *For all $x \in C^*$, the permutation π_x is in $Aut(C^*)$ if and only if x is in the kernel K of C^*.*

Proof: Let x, y be in C^*, as C^* is additive $x \star y \in C^*$ and $x + \pi_x(y) \in C^*$, but $x \in K$ if and only if $x + z \in C^*$ for all $z \in C^*$. ∎

Lemma 3.7 *The $\mathbb{Z}_4$-dual code, $C^{*\perp}$, of an extended 1-perfect $\mathbb{Z}_4$-linear code, C^*, is a sub-code, i.e. $C^{*\perp} \subset C^*$.*

Proof: It is straightforward to verify that rows of the parity check matrix are mutually orthogonal and thus the $\mathbb{Z}_4$-dual code, $C^{*\perp}$, is a sub-code. ∎

Lemma 3.8 *Let C^* be an extended 1-perfect $\mathbb{Z}_4$-linear code. The vectors $v \in K(C^*)$ satisfies the equation $2 \cdot v \cdot c \cdot x = 0$ (for all the vectors $c \in C^*$ and x in the $\mathbb{Z}_4$ dual of C^*), where we take the addition in $\mathbb{Z}_4$ of the componentwise product in $\mathbb{Z}_4$ of three vectors v, c, x.*
Conversely, if $2 \cdot v \cdot c \cdot x = 0$ (for all the vectors $c \in C^*$ and x in the $\mathbb{Z}_4$ dual of C^*) and $v \in C^*$ then $v \in K(C^*)$ and for $v \in C^{*\perp}$ then $v \in K(C^{*\perp})$

Proof: The vectors v in kernel of C^* are such that $v + c \in C^*$ for all $c \in C^*$. This operation $+$ is the binary addition, but if you are using quaternary notation ($\star$ is the quaternary addition) we will have for the elements in $\mathbb{Z}_4$: $a+b = a \star b$ (if $a = 0, 2$ or $b = 0, 2$) or $a + b = a \star b \star 2$ (if $a = 1, 3$ and $b = 1, 3$).

So we can summarize by giving the following equation $a + b = a \star b \star (2ab)$.

Now, for all $e \in \mathbb{Z}_4$ we will have $(a+b) \cdot e = (a \star b \star (2ab)) \cdot e = [(a \star b) \cdot e] \star [2abe]$.

Hence, the vectors v in kernel of C^* are such that $(v + c) \cdot x = 0 \in \mathbb{Z}_4$, for all $c \in C^*$ and x in the $\mathbb{Z}_4$ dual of C^*. But $(v \star c) \cdot x = 0$, so the vectors v in kernel of C^* are the vectors in C^* such that $2 \cdot v \cdot c \cdot x = 0$.

It is straightforward to check the inverse part. ∎

Let $u \in C^*$ be the all 1s quaternary vector with associated permutation σ.

Lemma 3.9 *Let $C^{*\perp}$ be the $\mathbb{Z}_4$ dual of C^*. For $\delta \geq 3$ and any pair of different vectors $v, w \in C^{*\perp}$ which are not of order two and different from u, we have that the componentwise product $2 \cdot v \cdot w \notin C^{*\perp}$.*

Proof: For $\delta \geq 3$ take two vectors, $v, w \in C^{*\perp}$ such that $v \neq u$, $w \neq u$ and its order is not 2. The quarter of the coordinates in v and w are, respectively, 0s, 1s, 2s and 3s and the Hamming distance of the binary representation is $d(v, w) = 2^{t-1}$.

Compare the coordinates in v and w and note that there λ times the two pairs 11, 33 (which give us the componentwise product 1), λ times the two pairs 13, 31 (which give us the componentwise product 3), λ times the four pairs 12, 21, 32, 23 (which give us the componentwise product 2) and λ times the eight pairs 01, 02, ..., 22 (which give us the componentwise product 0). The binary length of the code is $n + 1 = 2^t$ and $\lambda = 2^{t-1}/4^2$.

Now compute $2 \cdot v \cdot w$ and note that we obtain a vector with all the coordinate zeroes except for λ times four coordinates which are 2s. The Hamming weight of this vector is $8\lambda = 2^{t-2}$, which is a contradiction because all the vectors in $C^{*\perp}$ must have Hamming weight 2^{t-1}. ∎

Proposition 3.10 $K(C^{*\perp}) \subset K(C^*)$.

Proof: We know $C^{*\perp} \subset C^*$ (see lemma 3.7). Now the result is straightforward from lemma 3.8. ∎

Proposition 3.11 ([3]) *The dimension of the kernel of* $C^{*\perp}$ *is* $dim\, K(C^{*\perp}) = \gamma + \delta + 1$ *for* $\delta \geq 3$. *Otherwise* $C^{*\perp}$ *is linear and* $dim\, K(C^{*\perp}) = \gamma + 2\delta$.

Proof: It is easy to compute the dimension of $C^{*\perp}$ which is $\gamma + 2\delta = t + 1$.

For the kernel, from lemma 3.8 it is easy to see that all the vectors in $C^{*\perp}$ of order two are in it and the vector u too. This means that in the kernel there are at least $\gamma + \delta + 1$ independent binary vectors. But for $\delta \geq 3$ there are no more vectors in the kernel since lemma 3.8 and 3.9.

When $\delta = 1$ we have $dim(K(C^{*\perp})) = \gamma + \delta + 1 = \gamma + 2\delta$ and when $\delta = 2$ we know $\gamma + \delta + 2$ independent vectors in the kernel, but it is not possible to have a kernel with index 2, so when $\delta = 2$ the code must be linear and $dim(K(C^{*\perp}) = \gamma + \delta + 2 = \gamma + 2\delta$.

∎

Lemma 3.12 *Let* C^* *be an extended 1-perfect* $\mathbb{Z}_4$*-linear code, then* $A_\sigma \neq \emptyset$ *and* $A_\sigma \subset K(C^*)$. *Also* $A_{Id} \subset K(C^*)$.

Proof: From Lemma 3.8 and Proposition 3.10, we know that the all ones quaternary vector $u \in K(C^{*\perp}) \subset K(C^*)$ and $u \in A_\sigma$.

The vectors from A_{Id} are vectors of order two, so in quaternary notation they have coordinates only 0s and 2s. Hence from lemma 3.8 it is direct to see that $A_{Id} \subset K(C^*)$. ∎

Lemma 3.13 *A_π is a coset $A_\pi = A_{Id} \star x = A_{Id} + x$, where $\pi_x = \pi$.*

Theorem 3.14 *Let C^* be an extended 1-perfect $\mathbb{Z}_4$-linear code of binary length $n+1 = 2^t$ and $t+1 = \gamma + 2\delta$. The dimension of A_{Id} is $2^{t-1} - 2^{\delta-1}$.*

Proof: As we have previously seen we can think of the parity check matrix H of C^* as consisting of all column vectors of the form $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^{\delta-1} \times \{1 \in \mathbb{Z}_4\}$. Equivalently, the columns of H consist of cosets of the subgroup $H_2 = \mathbb{Z}_2^\gamma \times \{0,2\}^{\delta-1}$. The codewords $c \in A_{Id}$ of weight 4 correspond to $\mathbb{Z}_4$-codewords having exactly two nonzero coordinates with 2's. Equivalently, there must be two column vectors x, y of H such that,

$$2x + 2y \equiv 0 \pmod 4 \qquad \text{or} \qquad x + y \equiv 0 \pmod 2$$

This occurs if and only if x, y are in the same coset of H_2. There are $2^{\delta-1}$ such cosets each corresponding to a sub-code of dimension $2^{\gamma+\delta-1} - 1$.

It is not hard to see that A_{Id} does not contain any words of weight 6 and thus is generated by codewords of weight 4. Hence the dimension of A_{Id} is $(2^{\gamma+\delta-1}-1)2^{\delta-1} = 2^{t-1} - 2^{\delta-1}$. ∎

The following lemma is easy to prove:

Lemma 3.15 *For any $\pi \in Aut(C)$, C a 1-perfect binary code of length $2^t - 1$, the number of fixed points, i.e., the number of coordinates fixed by π, is $2^s - 1$ for some $0 \le s \le t$.*

Of course for extended 1-perfect codes the number of fixed points in any automorphism is just 2^s.

Proposition 3.16 *Let C^* be an extended 1-perfect $\mathbb{Z}_4$-linear code. For $\delta \ge 3$ we have $K(C^*) = A_{Id} \cup A_\sigma$. For $\delta = 2$ we have $K(C^*) = A_{Id} \cup A_\sigma \cup A_{\pi_\omega} \cup A_{\sigma\circ\pi_\omega}$ for some $w \in C^{*\perp}$ with $\pi_w \neq \sigma$ and $\pi_w \neq Id$.*

Proof:

We know $A_{Id} \cup A_\sigma \subset K(C^*)$ (see lemma 3.12).

So assume we have a vector v in $Ker(C^*)$ such that v is not of order two and also $\pi_v \neq \sigma$.

Let w be a vector in $C^{*\perp}$, such that w is not of order 2 and also $\pi_w \neq \sigma$. This vector w exists when $\delta \geq 2$ and for $\delta \geq 3$ we can take w not in $Ker(C^{*\perp})$. Then $\pi_v \in Aut(C^*)$ and π_v consists of a subset of involutions making up σ. By lemma 3.15, π_v moves at most half of binary coordinates in w, so $d_H(w, \pi_v(w)) < 2^{t-2}$ which is impossible unless $\pi_v = \pi_w$. But in this case $w \in Ker(C^*)$ and, from lemma 3.8, $w \in Ker(C^{*\perp})$ and this contradicts our assumption when $\delta \geq 3$.

For $\delta = 2$, all the vectors $w \in Ker(C^{*\perp})$ we can take so that $\pi_\omega \neq Id$ and $\pi_\omega \neq \sigma$ have the same associated permutation, either π_ω or $\pi_\omega \circ \sigma$, so by using the same argumentation we reach the conclusion that either $v \in A_{Id} + w$ or $v \in A_{Id} + w'$, where $\omega' = u \star \omega$ (u is the all ones vector). Hence $K(C^*) = A_{Id} \cup A_\sigma \cup A_{\pi_\omega} \cup A_{\sigma \circ \pi_\omega}$.

∎

Corollary 3.17 *Let C^* be an extended 1-perfect $\mathbb{Z}_4$-linear code of binary length $n + 1 = 2^t$.*

For $\delta = 1$ and $t > 4$ the dimension of the kernel is $dim K(C^*) = 2^{t-1} + t - 1$.

For $\delta = 2$, the dimension of the kernel is $dim K(C^*) = 2^{t-1} - 2^{\delta-1} + 2 = 2^{t-1}$.

For $\delta \geq 3$ the dimension of the kernel is $dim K(C^*) = 2^{t-1} - 2^{\delta-1} + 1$.

Proof: For $\delta \geq 2$ it is straightforward from the previous proposition.

For $\delta = 1$ and $t = 4$ we know code C^* is linear (see Theorem 3.5) so $K(C^*) = C^*$.

For $\delta = 1$ and $t > 4$ take a vector v in $Ker(C^*)$ such that v is not of order two and also $\pi_v \neq \sigma$. We note that since π_v and $\sigma \circ \pi_v$ are automorphisms assumed to be different from the identity, both have to have exactly 2^{t-1} fixed points. We can take as a representative of this vector v a vector with half coordinates zeroes and the other half ones (if we need it we can operate this vector by vectors in A_{Id}).

For each one of these vectors like v, the vector $2 \cdot v$ is in $C^{*\perp}$ so there are at most $t - 1$ of them which be independent. We have seen that the parity check matrix of C^* consists of all column vectors of the form $\mathbb{Z}_2^\gamma \times \{1 \in \mathbb{Z}_4\}$, where $\gamma = t - 1$. The vectors $2 \cdot v$ are the rows of this parity check. For $x \in C^{*\perp}$ we have $2 \cdot v \cdot x$ is

the zero vector or $2 \cdot v \cdot x = 2 \cdot v$. In any case, for all $c \in C^*$ the addition of the componentwise product $2 \cdot v \cdot x \cdot c = 0$ and since Lemma 3.8 $v \in Ker(C^*)$.

∎

As a summary we give the following tables for the case of length $n+1 = 16$ (so $t = 4$), for the case $n+1 = 32$ (so $t = 5$) and for the general case.

Capitals K and R means, respectively, the rank and the dimension of the kernel.

		R	K	R	K	R	K
$t = 4$	Additive non Z_4-linear	11	11	12	9	13	8
	Additive Z_4-linear	*	*	11	11	13	8
γ		4		3		1	
δ		0		1		2	

		R	K	R	K	R	K	R	K
$t = 5$	Additive non Z_4-linear	26	26	27	20	28	17	*	*
	Additive Z_4-linear	*	*	27	20	28	16	29	13
γ		6		4		2		0	
δ		0		1		2		3	

		R	K	R	K	R	K	R	K
t	Additive non Z_4-linear	2^t-t-1	2^t-t-1	2^t-t	$2^{t-2}+2^{t-1}-t+1$	$\cdots$	$\cdots$	$2^t-t-1+\delta$	$2^{t-\delta-1}+2^{t-1}-t+\delta$
	Additive Z_4-linear	*	*	2^t-t	$2^{t-1}+t-1$	$\cdots$	$\cdots$	$2^t-t-1+\delta$	$2^{t-1}-2^{\delta-1}+1$
γ		$t+1$		$t-1$		$\cdots$		γ	
δ		0		1		$\cdots$		δ	

References

[1] J. Borges and J. Rifà, "A characterization of 1-perfect additive codes", *IEEE Trans. on Information Theory*, vol. 45, pp. 1688-1697, 1999.

[2] A.E. Brouwer, A.M. Cohen and A. Neumaier, *Distance Regular Graphs*. Springer-Verlag, 1989.

[3] D.S. Krotov, "$\mathbb{Z}_4$-linear Hadamard and extended perfect codes", *Procs. of the International Workshop on Coding and Cryptography*, Jan. 8-12, 2001, Paris (France), pp. 329-334.

[4] K.T.Phelps, J.Rifà, *Combinatorial structure of binary* 1*-perfect additive codes*, Preprint n.488, December 2001. CRM. Spain.

[5] J. Rifà and J. Pujol, "Translation invariant propelinear codes", *IEEE Trans. Information Theory*, vol. 43, pp. 590-598, 1997.