Duality of additive codes*

J. Borges and C. Fernandez
Dept. d'Informàtica, Universitat Autònoma de Barcelona
08193-Bellaterra, Spain (e-mail: {jborges, cfernandez}@ccd.uab.es)

July 2003

Abstract

We study duality of additive codes. Given two nonequivalent binary additive codes, it is possible that they have the same binary additive dual code. This is a consequence of the fact that the same binary code can have more than one additive structure. An interesting case is that of the duals of the Hamming and extended Hamming codes.

1 Introduction and definitions

An *additive code* $\mathcal{C}$ *of type* (α, β) is an additive subgroup of $(\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta, +)$, where α and β are nonnegative integers and addition is modulo 2 for the binary coordinates and modulo 4 for the quaternary coordinates [1]. An element x of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ can be denoted by (x_b, x_q), where x_b is the binary part with α coordinates and x_q is the quaternary part with β coordinates. By the *binary image* of x we shall mean the binary vector $\Phi(x) = (x_b, \phi(x_q))$ of length $n = \alpha + 2\beta$, where ϕ is the usual Gray map (that sends 0 to 00, 1 to 01, 2 to 11 and 3 to 10).

The binary image of an additive code $C = \Phi(\mathcal{C})$ is also called (binary) additive code. Such binary codes are a particular case of *translation-invariant propelinear codes* (see [4, 1]). Note that the case $\beta = 0$ corresponds to binary linear codes, whereas the case $\alpha = 0$ corresponds to binary $\mathbb{Z}_4$-linear codes.

Given $x, y \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, we write $x +_b y = \Phi^{-1}(\Phi(x) + \Phi(y) \bmod 2) \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$.

*Research partially supported by Spanish CICYT Grant TIC2000-0739-C04-01 and by Catalan DURSI Grant 2001SGR 00219.

In Section 2 we define additive duality between codes. In Section 3 we study the different additive structures of the binary dual codes of the Hamming and extended Hamming codes. Finally, in Section 4 we point out some further research on the topic.

2 Additive duality

Following [4], we define the inner product between two vectors $x, y \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ as:

$$x \cdot y = 2 < x_b, y_b > + < x_q, y_q > \in \mathbb{Z}_4,$$

where $< \cdot, \cdot >$ is the sum of the coordinatewise product modulo 2 for binary vectors and modulo 4 for quaternary vectors. We say that two vectors $x, y \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ are *orthogonal* if $x \cdot y = 0$. Given a set $\mathcal{X} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, we define the *orthogonal code* to $\mathcal{X}$ as the set of vectors which are orthogonal to all the vectors in $\mathcal{X}$:

$$\mathcal{X}^\perp = \{z \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \mid x \cdot z = 0, \ \forall x \in \mathcal{X}\}.$$

It is readily verified that $\mathcal{X}^\perp$ is an additive code. If $\mathcal{C}$ is an additive code, then $(\mathcal{C}^\perp)^\perp = \mathcal{C}$ and we say that $\mathcal{C}$ and $\mathcal{C}^\perp$ are *dual codes*. Note that, in this case, $|\mathcal{C}||\mathcal{C}^\perp| = |\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta|$ (see [4]).

Given a binary additive code $C = \Phi(\mathcal{C})$, we define its additive dual code to be $C_\perp = \Phi(\mathcal{C}^\perp)$.

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\Phi} & C = \Phi(\mathcal{C}) \\ {\scriptstyle dual}\downarrow & & \\ \mathcal{C}^\perp & \xrightarrow{\Phi} & C_\perp = \Phi(\mathcal{C}^\perp) \end{array}$$

Note that $C_\perp$ is not orthogonal to C, in general, in the usual binary sense. In fact, neither C nor $C_\perp$ are linear codes, in general.

The *Lee weight* of a vector $x = (x_b, x_q) \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is defined in a natural way:

$$w_L(x) = w_H(x_b) + w_L(x_q),$$

where $w_H(\cdot)$ is the Hamming weight of a binary vector (which coincides with the Lee weight) and $w_L(\cdot)$ is the Lee weight of a quaternary vector ([2]). Clearly, $w_L(x) = w_H(\Phi(x))$. Of course, the *Lee distance* between two vectors $x, y \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is defined as $d_L(x, y) = w_L(x - y)$ and then, Φ is an isometry from ($\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, Lee distance) to ($\mathbb{Z}_2^n$, Hamming distance), where $n = \alpha + 2\beta$.

Recall that the *weight distribution* of a binary code C of length n is the set of nonnegative integers $\{A_i\}_{i=0}^n$, where A_i is the number of codewords in C of Hamming weight i. If C contains the zero vector, then it is *distance invariant* if the Hamming weight distributions of its translates $v + C$ are the same for all $v \in C$.

The following two properties are proven in [2] for $\mathbb{Z}_4$-linear codes and are generalized in [4] for additive codes:

Theorem 1 *Let C be a binary additive code. Then*

(i) C and $C_\perp$ are distance invariant codes.

(ii) The weight distributions of C and $C_\perp$ are MacWilliams transforms of one another.

Note that, in general, a binary vector of length n can be expressed as the binary image of different vectors in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ for different values of α and β such that $\alpha + 2\beta = n$. For instance, the vector $u = (0, 1, 0, 1, 1, 0)$ is the binary image of $(1, 1, 3) \in \mathbb{Z}_4^3$, but also it is the binary image of $(0, 1, 1, 3) \in \mathbb{Z}_2^2 \times \mathbb{Z}_4^2$. In the second interpretation, it follows that u is a self-orthogonal vector (orthogonal to itself), but this is not true for the first interpretation. These possible different interpretations for binary vectors lead to the following interesting phenomenon:

Given two nonequivalent binary additive codes of length n, C and D, it is possible that $C_\perp = D_\perp$. Obviously, a necessary condition will be that C and D must have the same weight distribution (see Theorem 1). Also, this can happen only if $C_\perp$ has different additive structures. In the following section we study these different structures for the binary duals of Hamming and extended Hamming codes, $H^\perp$ and $(H')^\perp$.

3 Additive duality of $H^\perp$ and $(H')^\perp$

Let H be the Hamming code of length $n = 2^t - 1 \geq 7$. H' is the extended code by adding overall parity check. $H^\perp$ is the dual of the Hamming code and it is called the *simplex code*. A generator matrix of $H^\perp$, G, is a parity check matrix of H and it is a $t \times n$ matrix whose columns are all non-zero t-tuples. The parity check matrix of H' is obtained from G as:

$$\left(\begin{array}{c|c} 0 & \\ \vdots & G \\ 0 & \\ \hline 1 & 111\cdots111 \end{array}\right) \tag{1}$$

Assume $H^\perp$ has nonlinear additive structure. We denote $\mathcal{H}^\perp = \Phi^{-1}(H^\perp) \subset \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. All nonzero codeword in $H^\perp$ has Hamming weight $\frac{n+1}{2}$. Since Φ is an isometry from ($\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, Lee distance) to ($\mathbb{Z}_2^n$, Hamming distance), all nonzero codeword in $\mathcal{H}^\perp$ has Lee weight $\frac{n+1}{2}$.

Lemma 2 *Let C be a binary linear code of length $n \geq 3$ and minimum distance $d \geq 3$. Let $C^\perp$ be its binary dual code. Let $i, j \in \{1, \cdots, n\}$, $i \neq j$. Then, it is not possible that $x_i = x_j$ for all $x = (x_1, x_2, \cdots, x_n) \in C^\perp$.*

Proof: Assume there exist $i, j \in \{1, \cdots, n\}$, $i < j$, such that $x_i = x_j \; \forall x \in C^\perp$. Let $y \in C$ and let y' be equal to y in all coordinates up to i, j, and $y'_i = y_i + 1$, $y'_j = y_j + 1$. As $x \cdot y = 0$, $x_i = x_j$ and $y'_i + y'_j = y_i + y_j$ then, $x \cdot y' = 0$ and $y' \in C$. Hence, y and y' are in C and $d(y, y') = 2$, that is a contradiction. ∎

Lemma 3 *If $H^\perp$ has a nonlinear additive structure, then there exists a codeword in $\mathcal{H}^\perp$ of order 4.*

Proof: If $\mathcal{H}^\perp$ has no codeword of order 4, then it has quaternary coordinates all of them of order 2. If i, j correspond to a quaternary coordinate in $H^\perp$ then, $x_i = x_j = 0$ or $x_i = x_j = 1 \; \forall x \in H^\perp$, that is a contradiction with Lemma 2. ∎

Lemma 4 *If $H^\perp$ has a nonlinear additive structure, then any codeword $x \in \mathcal{H}^\perp$ of order 4 has exactly $\frac{n+1}{4}$ quaternary coordinates of order 4.*

Proof: Recall that all nonzero codewords of $\mathcal{H}^\perp$ have Lee weight $\frac{n+1}{2}$. Let $x \in \mathcal{H}^\perp$ of order 4 and let k be the number of quaternary coordinates of order 4. Since $\mathcal{H}^\perp$ is an additive code, $2x = x + x = (\mathbf{0}, 2x_q)$ belongs to the code. x has order 4, then $w_L(x) = \frac{n+1}{2}$ and $w_L(2x) \geq 2$. Therefore, $w_L(2x) = \frac{n+1}{2} = 2k$ and (x_b, x_q) has exactly $k = \frac{n+1}{4}$ quaternary coordinates of order 4. ∎

Corollary 5 *If $H^\perp$ has a nonlinear additive structure, then all order 4 codewords in $\mathcal{H}^\perp$ have the $\frac{n+1}{4}$ quaternary coordinates of order 4 in the same quaternary positions.*

Proof: Let $x, y \in \mathcal{H}^\perp$ of order 4. Let k be the number of coincident positions in which x and y both have quaternary coordinates of order 4. Clearly, $k \neq 0$; otherwise, $w_L(2x + 2y) = n > \frac{n+1}{2}$. Let v be a vector with entries 2 in these k coordinates and zeroes elsewhere. Let $z = x +_b y$ and $z' = x + y$. $z, z' \in \mathcal{H}^\perp$ and $z + z' = v \in \mathcal{H}^\perp$, then $w_L(z + z') = w_L(v) = 2k$. Since $k \neq 0$, $w_L(z + z') = \frac{n+1}{2}$ and $k = \frac{n+1}{4}$. ∎

Theorem 6 *Let C be a binary linear code of even length. Assume* $\mathbf{1}$*, the all ones vector, is in C and, $\forall x \in C$, $\phi^{-1}(x)$ is a $\frac{n}{2}$ length codeword of order 2 or all quaternary coordinates have order 4. Then, C is a $\mathbb{Z}_4$-linear code.*

Proof: Let $x, y \in C$ and $+_q$ the quaternary sum. If $\phi^{-1}(x)$ has order 2 then, $\phi(\phi^{-1}(x) +_q \phi^{-1}(y)) = x + y \in C$. In the case of $\phi^{-1}(x)$ and $\phi^{-1}(y)$ with all quaternary coordinates of order 4, $\phi(\phi^{-1}(x) +_q \phi^{-1}(y)) = x + y + \mathbf{1} \in C$. ∎

Corollary 7 *Let $C \subset \mathbb{F}^n$ be a binary linear code. Let $X = supp(x) \neq \emptyset$ for some $x \in C$ of even weight. Consider $\mathbb{F}^n$ as the group $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, where $n = \alpha + 2\beta$ and the α $\mathbb{Z}_2$ coordinates are those not in X, i.e. $\beta = |X|/2$. Assume that for all $y \in C$, $\Phi^{-1}(y)$ has order 2 or all the quaternary coordinates of $\Phi^{-1}(y)$ have order 4. Then, C is a binary additive code of type $(n - |X|, \frac{|X|}{2})$.*

Proof: Let $\mathcal{C} = \Phi^{-1}(C)$. Note that $\Phi^{-1}(x) = (\mathbf{0}_b, \mathbf{2}_q)$, in other words, the vector x restricted to the X coordinates is the all ones vector $x|_X = \mathbf{1}$. Hence, by Theorem 6, the code C restricted to the X coordinates, $C|_X$, is a $\mathbb{Z}_4$-linear code.

Let $u, v \in \mathcal{C}$, we must prove that $u + v \in \mathcal{C}$. If u or v is a codeword of order 2, then it is clear that $u + v = u +_b v \in \mathcal{C}$. Now, if both of them have all quaternary coordinates of order 4, then $u + v = u +_b v +_b (\mathbf{0}_b, \mathbf{2}_q) = u +_b v +_b \Phi^{-1}(x)$. Since $\Phi(u), \Phi(v)$ and x are in C, we obtain that $u + v$ is in $\mathcal{C}$.

Hence, $\mathcal{C}$ is an additive code of type $(n - |X|, \frac{|X|}{2})$. ∎

In [1], 1-perfect additive codes are completely characterized. There is exactly one 1-perfect additive code of type $(2^r - 1, 2^{t-1} - 2^{r-1})$ of length $n = 2^t - 1 \geq 7$ for any integer r such that $2 \leq r \leq t \leq 2r$, up to coordinate permutation. Moreover, any 1-perfect additive code is of this type for some r verifying the inequalities. Hence, an extended 1-perfect additive code of length $n+1 = 2^t \geq 8$ must be either of type $(2^r, 2^{t-1} - 2^{r-1})$ or of type $(0, 2^{t-1})$ ($\mathbb{Z}_4$-linear), as can be seen in [5]. All these codes are also characterized and the rank and dimension of the kernel are computed in [5].

Theorem 8 *$H^\perp$ has exactly two additive structures: $(n, 0)$ (linear structure) and $(\frac{n-1}{2}, \frac{n+1}{4})$. Hence, $H^\perp$ is additive dual of exactly 2 1-perfect additive codes: the linear code and the additive code of type $(\frac{n-1}{2}, \frac{n+1}{4})$.*

Proof: Let us consider $H^\perp$ as a non linear additive code. Let $x \in H^\perp$, $x \neq \mathbf{0}$ and $X = supp(x)$. $x|_X = \mathbf{1}$ of length $\frac{n+1}{2}$. Let be $i, j \in X$. By Lemma 2 there exist $y \in H^\perp$ such that $y_i \neq y_j$; that is, has one quaternary coordinate of order 4. $w_L(2\Phi^{-1}(y)) = w_L(\Phi^{-1}(y) + \Phi^{-1}(y)) \neq \mathbf{0}$, because of the coordinate of order 4, then, $w_L(2\Phi^{-1}(y)) = \frac{n+1}{2}$ and $\Phi^{-1}(y)$ has all

quaternary coordinates of order 4. Hence, $\Phi^{-1}(y)$ $\forall y \in H^{\perp}$ is of order 2 or has all coordinates of order 4. By Corollary 7, $H^{\perp}$ is an additive code of type $(\frac{n-1}{2}, \frac{n+1}{4})$. ∎

Theorem 9 *Let $(H')^{\perp}$ be the Hamming extended dual code of length $n+1 = 2^t$. $(H')^{\perp}$ has exactly three additive structures: $(n+1, 0)$, $(\frac{n+1}{2}, \frac{n+1}{4})$ and $(0, \frac{n+1}{2})$. Hence, it is the additive dual of the following extended 1-perfect codes:*

- *The linear code (extended Hamming code),*
- *extended additive code of type $(\frac{n+1}{2}, \frac{n+1}{4})$,*
- *$\mathbb{Z}_4$-linear code, C, $(0, \frac{n+1}{2})$ such that $\mathbb{F}^{n+1}/C \cong \mathbb{Z}_2^{t-1} \times \mathbb{Z}_4$.*

Proof: By definition $(H')^{\perp}$ is the dual code of the linear code H'. Let us consider the nonlinear structures of $(H')^{\perp}$.

Let $x \in (H')^{\perp}$ such that $w(x) = \frac{n+1}{2}$ (it is possible due to Lemma 2) and let $X = supp(x)$. As in Theorem 8, $(H')^{\perp}|_X$ is a $\mathbb{Z}_4$-linear code of length $\frac{n+1}{4}$. Hence, $(H')^{\perp}$ has additive structure of type $(\frac{n+1}{2}, \frac{n+1}{4})$.

Now, by construction of the parity check matrix of H', we obtain a matrix with the appearance:

$$\begin{pmatrix} 00\cdots\cdots00 & 11\cdots\cdots11 \\ 0\cdots01\cdots1 & 0\cdots01\cdots1 \\ \vdots & \vdots \\ 01\cdots\cdots01 & 01\cdots\cdots01 \\ 11\cdots\cdots11 & 11\cdots\cdots11 \end{pmatrix}. \tag{2}$$

It is clear that $\mathbf{1} \in (H')^{\perp}$ and any codeword has order 2 or it has all coordinates of order 4. Then, by Theorem 6, $(H')^{\perp}$ is a $\mathbb{Z}_4$-linear code of length $\frac{n+1}{2}$. Moreover, such parity check matrix coincides with a parity check matrix of a $\mathbb{Z}_4$-linear code, C, of type $(0, \frac{n+1}{2})$ where $\mathbb{F}^{n+1}/C \cong \mathbb{Z}_2^{t-1} \times \mathbb{Z}_4$ (see [5] for construction of such matrices). ∎

4 Further research

The generalization of the concept 'duality' for nonlinear codes (e.g. additive codes) should give also generalizations of the concept 'rank'. This should give a measure of 'additivity' of nongroup codes over $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$.

Another interesting question is about the possibility of defining different inner products in $\mathbb{Z}_2^{\alpha} \times \mathbb{Z}_4^{\beta}$, although it seems that the defined one in [4] (and used in this paper) is the more suitable one.

We have seen all the additive structures of the simplex codes and the duals of the extended Hamming codes. However, given an extended 1-perfect additive but non-$\mathbb{Z}_4$-linear code C and an extended 1-perfect $\mathbb{Z}_4$-linear code D, it appears a challenging question to know when the binary additive dual codes coincide, even in the case that the quotient groups $\mathbb{F}^{n+1}/C$ and $\mathbb{F}^{n+1}/D$ are isomorphic. An answer to this question would lead to the complete characterization of the additive dual codes of extended 1-perfect additive codes.

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.R. Hammons, 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. on Information Theory*, vol. 40, pp. 301-319, 1994.

[3] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland Publishing Company, 1977.

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

[5] J. Borges, K. P. Phelps J. and Rifà, "The rank and kernel of 1-perfect $\mathbb{Z}_4$-linear codes and additive non-$\mathbb{Z}_4$-linear codes," to appear in *IEEE Trans. on Information Theory*, 2003.