On the kernel and rank of $\mathbb{Z}_4$-linear Preparata-like and Kerdock-like codes*

J. Borges, K.T. Phelps†, J. Rifà‡, V.A. Zinoviev§

July 1, 2002

Abstract

We say that a binary code of length n is additive if it is isomorphic to a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, where the quaternary coordinates are transformed to binary by means of the usual Gray map and hence $\alpha + 2\beta = n$.

In this paper we prove that any additive extended Preparata-like code always verifies $\alpha = 0$, i.e. it is always a $\mathbb{Z}_4$-linear code. Moreover, we compute the rank and the dimension of the kernel of such Preparata-like codes and also the rank and the kernel of the $\mathbb{Z}_4$-dual of these codes, i.e. the $\mathbb{Z}_4$-linear Kerdock-like codes.

*Research partially supported by Spanish CICYT Grant TIC2000-0739-c04-01, by Catalan DURSI Grant 2001SGR 00219 and also by Ministerio de educación, cultura y deporte Grant SAB 2000-0058.

†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 Science Department, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain. E-mail: {joaquim.borges, josep.rifa}@uab.es.

§V.A. Zinoviev is with the Institute for Problems of Information Transmission of the Russian Academy of Sciences, Bol'shoi Karetnyi per. 19, GSP-4, Moscow, 101447, Russia. E-mail: zinov@iitp.ru.

1 Introduction.

Let $\mathbb{F}^n$ denote the set of all binary vectors of length n. As usual $d(\cdot,\cdot)$ denotes the *Hamming distance* and $\mathrm{wt}(\cdot)$ denotes the *Hamming weight*. Let e_i denote the vector of weight one with the nonzero coordinate at the i-th position for $i = 1, \ldots, n$. For any vector $v \in \mathbb{F}^n$ we denote by $supp(v)$ the set of coordinate positions in which v has nonzero entries.

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

$$d(x \star v,\, x \star u) = d(v,\, u), \quad \forall x, v, u \in \mathbb{F}^n. \tag{1}$$

As can be seen in [2], $(\mathbb{F}^n, \star) \cong (\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta, +)$ where $\alpha + 2\beta = n$ and '+' is the usual addition modulo 2 for the $\mathbb{Z}_2$ coordinates and modulo 4 for the $\mathbb{Z}_4$ coordinates. An isomorphism between $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ and $\mathbb{F}^n$ is given by the map

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

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

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

Let x^{-1} denote the inverse element of x, that is, the unique vector x^{-1} such that $x \star x^{-1} = \mathbf{0}$, where $\mathbf{0}$ denotes the all zero vector. Note the following property.

Lemma 1.1 *For any vectors $x, y \in \mathbb{F}^n$ we have*

$$d(x,y) = wt(x^{-1} \star y) = wt(x \star y^{-1}).$$

Proof: From equation (1) we have

$$d(x,y) = d(x^{-1} \star x,\, x^{-1} \star y) = d(\mathbf{0},\, x^{-1} \star y) = \mathrm{wt}(x^{-1} \star y)$$

or

$$d(x,y) = d(y^{-1} \star x,\, y^{-1} \star y) = d(y^{-1} \star x,\, \mathbf{0}) = \mathrm{wt}(y^{-1} \star x).$$

∎

A *(binary) additive code* (see [2, 4]) $(D, \star)$ of length $n = \alpha + 2\beta$ is a subgroup of $(\mathbb{F}^n, \star)$. An additive code is a particular case of the more general class of *translation-invariant propelinear codes* [2, 13]. Note that the case $\beta = 0$ corresponds to a linear code and the case $\alpha = 0$ corresponds to a $\mathbb{Z}_4$-linear code. In this last case (see [13]) $(D, \star)$ is a group, where each codeword x is associated with a coordinate permutation $\pi_x \in \mathcal{S}_n$ such that $x \star y = x + \pi_x(y)$ for any $y \in D$.

Define $D_\pi = \{z \in D \mid \pi_z = \pi\}$ 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 transpositions permuting the two binary coordinates, corresponding to each $\mathbb{Z}_4$ cordinate. In this paper we will refer to the group of binary coordinate permutations $\pi : D \to D$ as $aut(D)$, the automorphism group of the code.

In order to differentiate codes over $\mathbb{Z}_4$ from codes over $\mathbb{Z}_2$ we use letters $\mathcal{C}, \mathcal{D}, \mathcal{H}, \mathcal{P}, \mathcal{K}$ and so on for the codes over $\mathbb{Z}_4$. For the corresponding codes over $\mathbb{Z}_2$, obtained by the Gray map, we use the corresponding letters $C = \phi(\mathcal{C})$, $D = \phi(\mathcal{D})$, $H = \phi(\mathcal{H})$, $P = \phi(\mathcal{P})$, $K = \phi(\mathcal{K})$, and so on.

We use also $(x, y)_4$ to denote the inner product of vectors over $\mathbb{Z}_4$, and $x \bullet y$ to denote the componentwise product of two or more such vectors. We denote by $\mathbf{1}$ the vector over $\mathbb{Z}_4$ with all the coordinates 1, and by $\mathbf{1}_2$ the vector over $\mathbb{Z}_2$ with all the coordinates 1. We also denote by $\mathbf{2}$ the vector over $\mathbb{Z}_4$ such that $\phi(\mathbf{2}) = \mathbf{1}_2$.

Recall that the rank of any code D is the dimension of the linear span of D, which we denote here $< D >$, and the kernel of D, denoted here by $ker(D)$, is defined by $ker(D) = \{v \in D \,|\, v + D = D\}$.

In this paper we denote by P a binary extended $\mathbb{Z}_4$-linear Preparata-like code with parameters $(n+1, d, M) = (2^{2m}, 6, 2^{n-4m})$, obtained by the Gray

map from an arbitrary linear Preparata-like code $\mathcal{P}$ over $\mathbb{Z}_4$ [8]. The corresponding binary code with $d = 5$, obtained from P by deleting any position, is denoted by P^*. Denote by K a binary extended $\mathbb{Z}_4$-linear Kerdock-like code with parameters $(n+1 = 2^{2m}, (n+1)/2 - \sqrt{n+1}/2, 2^{4m})$, obtained by the Gray map from $\mathcal{K}$, the $\mathbb{Z}_4$-dual of $\mathcal{P}$:

$$\mathcal{K} \ = \ \{x \in \mathbb{Z}_4^{(n+1)/2} : \ (x,p)_4 = 0, \ \ \forall p \in \mathcal{P}\}.$$

We denote by C an extended binary perfect $\mathbb{Z}_4$-linear code with parameters $(n+1 = 2^{2m}, d = 4, M = 2^{n-2m-1})$ and by H its $\mathbb{Z}_4$-dual, a binary Hadamard code with parameters $(n+1 = 2^{2m}, d = (n+1)/2, M = 2\,(n+1))$.

Preparata-like codes are not linear. Concerning to their possible algebraic structure, we remark that the original Preparata codes [12] have a group propelinear structure [13] and the extended Preparata-like codes defined in [8] are $\mathbb{Z}_4$-linear and so, according to [13], they are propelinear codes.

In this paper we prove the nonexistence of extended Preparata-like codes with other additive structures different of the $\mathbb{Z}_4$-linear ones. Given a Preparata-like code P^*, it is well known [17] that the code C^* obtained as the union of P^* and the vectors at maximum distance from P^* is a perfect single error correcting code or *1-perfect code*. If P^* is a standard Preparata code, then C^* is linear i.e. a Hamming code. If P is an extended Preparata-like code, then C is an extended 1-perfect code. We show that if P is $\mathbb{Z}_4$-linear, then C is also $\mathbb{Z}_4$-linear. This allows us to compute the ranks and kernels of P and its $\mathbb{Z}_4$-dual, the Kerdock-like code K.

The paper is organized as follows. In Section 2 we give the basic definitions and properties of Preparata-like codes. In Section 3 we give the main result of the paper: any additive Preparata-like code is $\mathbb{Z}_4$-linear. In Section 4 we compute the rank of any $\mathbb{Z}_4$-linear Preparata-like code P and its $\mathbb{Z}_4$-dual Kerdock-like code K. In Section 5 we find the kernels of both these codes. Note that the kernel of known $\mathbb{Z}_4$-linear Preparata-like codes given in

[8] have been considered also in [9]. Finally, in Section 6 we point out some conclusions.

2 Preparata-like codes.

A *Preparata-like code* P^* has length $n = 2^{2m} - 1$ ($m \geq 2$), minimum distance $d = 5$ and $|P^*| = M = 2^{n+1-4m}$ codewords. Such a code satisfies the Johnson bound and therefore it is nearly perfect [7, 15] and strongly uniformly packed and so, completely regular [15] (in particular, distance invariant). If we assume P^* contains the zero codeword, then the codewords of weight 5 form a $2-(n,5,\lambda)$-design [14] with $\lambda = (n-3)/3$.

Let P be an extended Preparata-like code. From [15] we know that the binary all one vector $\mathbf{1}_2$ belongs to P and, therefore, to P^*.

Define $P_i^* = \{c \in \mathbb{F}^n \mid d(c, P^*) = i\}$ for $i = 0, 1, 2, 3$, and $P_i = \{c \in \mathbb{F}^n \mid d(c, P) = i\}$ for $i = 0, 1, 2, 3, 4$. Then we have:

Proposition 2.1 ([17]) *Let P^* be any Preparata-like code and let $C^* = P^* \cup P_3^*$, then C^* is a 1-perfect code.*

Proof: We give our own proof which differs from the one given in [17]. Since P^* is a 2-error-correcting quasi-perfect code, we have that

$$|P_3^*| = |F^n| - |P^*| - |P_1^*| - |P_2^*| = 2^n - |P^*|(1 + n + n(n-1)/2) = |P^*|(2^{2m-1} - 1)$$

Thus $|C^*| = |P^*| + |P_3^*| = |P^*| \cdot 2^{2m-1} = 2^{n-2m}$, which is the correct number of codewords of a 1-perfect code of length $n = 2^{2m} - 1$. It remains to prove that the covering radius of C^* is equal to 1. Let $x \in \mathbb{F}^n$. If $d(x, P^*) = 0$ or $d(x, P^*) = 3$, then $x \in C^*$. If $d(x, P^*) = 1$, then $d(x, C^*) = 1$. Assume that $d(x, P^*) = 2$. Since P^* is distance invariant [15], we may assume, without loss of generality, that x has weight 2. The number of codewords of weight 5 in P^*, containing the support of x, is equal to $\lambda = (n-3)/3$ (these vectors

have only the two nonzero coordinates of x in common). Hence the support J of all these codewords has $n-1$ coordinates. Let i be the coordinate position not in J and consider the vector $y = x + e_i$. It is clear that $d(y, P^*) = 3$, so $y \in C^*$ and $d(x, C^*) = 1$. ∎

Proposition 2.2 *Let P^* be any Preparata-like code and let $C^* = P^* \cup P_3^*$. Then the rank of P^* is equal to the rank of C^*.*

Proof: Since $P^* \subset C^*$ we have that $< P^* > \subset < C^* >$. Let x be a codeword of C^* not in P^*, then $d(x, P^*) = 3$ and without loss of generality we may assume that x has weight 3 because P^* is distance invariant. If we prove that $x \in < P^* >$, then we will have that $< C^* > \subset < P^* >$ and hence $< C^* > = < P^* >$. Therefore we only have to show that given a codeword x of weight 3, this codeword can be obtained as a linear combination of codewords of P^*. Let $x = e_i + e_j + e_k$ be such a codeword. Consider, as in the proof of Proposition 2.1, the set $\{c_\ell\}_{\ell=1}^{\lambda}$ of $\lambda = (n-3)/3$ codewords of weight 5 in P^* that have the coordinates i and j in their support. Let $J = \cup_{\ell=1}^{\lambda} supp(c_\ell)$. Then, taking into account that λ is even and $\mathbf{1}_2 \in P^*$, we obtain that $\sum_{\ell=1}^{\lambda} c_\ell + \mathbf{1}_2 = x$. ∎

Clearly, an extended Preparata-like code P has minimum weight 6 and covering radius 4.

Lemma 2.3 ([17]) *Let P be any extended Preparata-like code. Then the code $P \cup P_4$ is an extended 1-perfect code.*

Proof: As before, let $C^* = P^* \cup P_3^*$, then it is clear that the extended code of C^* is $C = P \cup P_4$, because P_4 is the extension of P_3^*. ∎

All known Preparata-like codes induce a partition of C^* by taking appropriate translates (see [1, 6, 8, 17]). It is possible to generalize this partition to the case when P^* is a propelinear code. In this last case there is a partition which consists of orbits in C^* under the action of P^*.

Proposition 2.4 *If P is an additive extended Preparata-like code, then $C = P \cup P_4$ is partitioned into cosets of P of weight four.*

Proof: Let $D = P \star w$ be a coset of P with minimum weight 4. As it follows from [2], any vector v of D is at distance 4 from P, hence $v \in C$. In the opposite side, if E is a coset with minimum weight less than 4, any vector z in E is at distance less than 4 from P, therefore $z \notin C$. ∎

The rank of any code is equal to the rank of the extended code. Hence, by Proposition 2.2 we have that the ranks of P^*, P, C^* and C are all equal.

3 Any additive Preparata-like code is $\mathbb{Z}_4$-linear.

For any (extended) Preparata-like code P, let C be the corresponding (extended) 1-perfect code, i.e. $C = P \cup P_4$.

Lemma 3.1 *Let P be an additive extended Preparata-like code and let $e \in \mathbb{F}^n$ be a vector such that $d(e, P) = 4$. Then $d(e^{-1}, P) = 4$.*

Proof: Since $(P, \star)$ is a group we know that $e^{-1} \notin P$. Suppose that $d(e^{-1}, P) < 4$. That is, there should be a codeword $x \in P$ such that $d(e^{-1}, x) < 4$. But, by Lemma 1.1, we would have $\mathrm{wt}(e \star x) < 4$ and, again by Lemma 1.1, $d(e, x^{-1}) < 4$ implying that $d(e, P) < 4$, getting a contradiction. ∎

Proposition 3.2 *If P is an additive code then so is $C = P \cup P_4$.*

Proof: Assume that P is an additive code. By Proposition 2.4, C is the union of P with cosets of P, each one with minimum weight 4. Given any word $x \in C$, we have that $x = c \star e$ for some $c \in P$ and for some vector e of weight 4 or 0. In any case, by Lemma 3.1, the inverse element $x^{-1} = c^{-1} \star e^{-1}$ of x is also in C. The identity element (the all zero vector) is in C too.

Therefore we only have to show that for any given $x, y \in C$, the element $x \star y \in C$ belongs to C also. Let $x = c \star e$ and $y = c' \star e'$ where $c, c' \in P$ and e and e' be vectors such that $\mathrm{wt}(e), \mathrm{wt}(e') \in \{0, 4\}$, . Thus,

$$x \star y = c \star e \star c' \star e' = d \star e \star e',$$

where $d = c \star c' \in P$. Denote $a = d \star e \star e'$. If e or e' (or both) has weight 0, then it is clear that $a \in C$. Assume now that $\mathrm{wt}(e) = \mathrm{wt}(e') = 4$ and consider the distance $d(a, P)$ (which should be even). Since the covering radius of P is 4, we have that $d(a, P) \in \{0, 2, 4\}$. For the case $d(a, P) \in \{0, 4\}$ it follows directly that $a \in C$. For the case $d(a, P) = 2$, there would exist $b \in P$ such that $d(a, b) = 2$, implying by Lemma 1.1 that $\mathrm{wt}(a \star b^{-1}) = 2$, that is, $\mathrm{wt}(d \star e \star e' \star b^{-1}) = 2$. If we denote now $d' = d \star b^{-1} \in P$, we would have $\mathrm{wt}(d' \star e \star e') = 2$, implying again by Lemma 1.1 that $d(d' \star e', e^{-1}) = 2$. Clearly $d' \star e' \in C$ and, by Lemma 3.1, e^{-1} is also in C. Since the minimum distance of C is equal to 4, we obtain a contradiction. ∎

Now, we are going to prove that any additive Preparata-like code P should be $\mathbb{Z}_4$-linear.

Lemma 3.3 *Let P^* be an additive Preparata-like code of length $n = \alpha + 2\beta$ which is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, for some $\alpha, \beta > 0$. Then $\alpha \geq 3$.*

Proof: Clearly, $C^* = P^* \cup P_3^*$ should be a 1-perfect additive code because C can be obtained from $C = P \cup P_4$ by deleting a $\mathbb{Z}_2$ coordinate. Consider the subcode D of C formed by all the codewords with zeroes in all the $\mathbb{Z}_4$ coordinates. This subcode D restricted to the $\mathbb{Z}_2$ coordinates is a 1-perfect code of length $\alpha = 2^r - 1$ for some $r \geq 2$ (see [2]). ∎

Lemma 3.4 *Let P^* be an additive Preparata-like code of length $n = \alpha + 2\beta$ which is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ for some $\alpha, \beta > 0$. Denote by X the set of $\mathbb{Z}_2$ coordinates and fix any two such coordinates $i, j \in X$. Let $V \subset P^*$ be the*

set of all codewords of P^* of weight 5 containing i and j in their supports. Then

(i) For any pair of codewords $x, y \in V$ we have that $supp(x) \cap supp(y) = \{i, j\}$, the set V has a cardinality $|V| = (n-3)/3$, and the union of the supports of all the codewords of V is $\{1, \ldots, n\} \setminus \{k\}$ for some $k \in X \setminus \{i, j\}$.

(ii) For any $x \in V$ there are two possibilities: either $|supp(x) \cap X| \in \{3, 5\}$ and $x = x^{-1}$, or $|supp(x) \cap X| = 2$ and $x \star x$ has weight 6.

Proof: (i) We know from [14] that the set of codewords of P^* of weight 5 form a $2-(n, 5, (n-3)/3)$-design. For any $x, y \in V$ the condition $|supp(x) \cap supp(y)| > 2$ is impossible because we would have $d(x, y) < 5$ and the minimum distance of P^* is 5. This implies that $|V| = (n-3)/3$, and therefore

$$\left| \bigcup_{x \in V} supp(x) \right| = 3 \, \frac{n-3}{3} + 2 = n - 1.$$

Let k be the coordinate which is not in the support of x for any $x \in V$, i.e. $k = supp(P^*) \setminus supp(V)$. We have to show that k belongs to X. In contrary, assume that $k \notin X$. This means that there is some k' which is the inverse coordinate of k such that $e_{k'} = e_k^{-1}$). Now let $y \in V$ be a vector such that $k' \in supp(y)$. Using that for any $x \in V$ the inverse x^{-1} laso belongs to V, we obtain a contradiction because $y^{-1} \in V$ and $k \in supp(y^{-1})$.

(ii) If $|supp(x) \cap X| = 5$, then it is clear that $x = x^{-1}$ (as $x \star x = x + x = \mathbf{0}$). The condition $|supp(x) \cap X| = 4$ is impossible because $x \star x$ would have weight 2. If $|supp(x) \cap X| = 3$, then the two nonzero coordinates of x not in X must be inverses (and $x = x^{-1}$), otherwise $x \star x$ would have weight 4. Finally, if $|supp(x) \cap X| = 2$, then $x \star x \neq \mathbf{0}$ and hence $x \star x$ should have weight 6. ∎

Lemma 3.5 *A (non-extended) Preparata-like code P^* cannot be additive.*

Proof: We know that a Preparata-like code cannot be linear (see [7]). Since the length of P^* is odd it cannot be $\mathbb{Z}_4$-linear. Assume that P^* is an additive code, which is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, where $\alpha, \beta > 0$.

As in the previous lemma, let X be the set of $\mathbb{Z}_2$ coordinates. Let $i, j \in X$ and define V and k as before. Then we obtain that

$$V = \{x_1, \ldots, x_p\} \cup \{y_1, y_1^{-1}, \ldots, y_q, y_q^{-1}\},$$

where $|supp(x_i) \cap X| \in \{3, 5\}$ for all $i = 1, \ldots, p$ and where $|supp(y_j) \cap X| = |supp(y_j^{-1} \cap X| = 2$ for all $j = 1, \ldots, q$. Since $|V| = (n-3)/3 = p + 2\,q$, we note, that p is even because so is $(n-3)/3$.

Let $z = x_1 \star \cdots \star x_p \star y_1 \star y_1 \star \cdots y_q \star y_q$. By assumption z is a codeword of P^*. It is easy to see that $supp(z) = \{1, \ldots, n\} \setminus \{i, j, k\}$. But we know from [15] that the all ones vector $\mathbf{1}_2$ is also in P^*. Therefore we get a contradiction because $d(z, \mathbf{1}_2) = 3$ and the minimum distance of P^* is 5. ∎

Theorem 3.6 *Let P be an extended additive Preparata-like code and let $K = \phi(\mathcal{P}^\perp)$ be the corresponding extended additive Kerdock-like code. Then P and K are both $\mathbb{Z}_4$-linear.*

Proof: Assume that P is an additive but not $\mathbb{Z}_4$-linear code. Puncturing a $\mathbb{Z}_2$ coordinate would give an additive (non-extended) Preparata-like code P^* which is impossible by the previous lemma.

Now assume that the Kerdock code K is additive, i.e. K is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ for some α and β. Then according to [13] its $\mathbb{Z}_4$-dual, which is a Preparata-like code P, should be also additive with the same parameters α and β. But this is impossible by the lemma above. Hence, this last code P should be $\mathbb{Z}_4$-linear. So, we conclude that K is also $\mathbb{Z}_4$-linear. ∎

Let q_i denote the quaternary vector in $\mathbb{Z}_4^{2^{2m-1}}$ with only one nonzero coordinate at the i-th position, the value of which is 2. In other words, $\phi(q_i)$

is a binary vector in $\mathbb{Z}_2^{2^{2m}}$ with two nonzero positions, corresponding to the i-th quaternary position.

As the natural extension of Proposition 2.4, now we can give the evident partition of the extended $\mathbb{Z}_4$-linear 1-perfect code C into the translates of the corresponding $\mathbb{Z}_4$-linear Preparata-like code P.

Theorem 3.7 *Let P be a $\mathbb{Z}_4$-linear extended Preparata-like code of length $n+1 = 2^{2m}$, and let $C = P \cup P_4$ be the corresponding extended 1-perfect $\mathbb{Z}_4$-linear code. Then for any integer $i = 1, 2, ..., (n+1)/2$, the code C is partitioned into the cosets of P of weight 4 as follows:*

$$C = \bigcup_{j=1}^{(n+1)/2} \{P + \phi(q_i + q_j)\}$$

(recall that "+" means addition modulo 2 for binary vectors and modulo 4 for vectors over $\mathbb{Z}_4$).

Proof: From Proposition 2.4 we know that any additive Preparata-like code P partitions the corresponding additive extended 1-perfect code $C = P \cup P_4$. But Theorem 3.6 states that this code P is $\mathbb{Z}_4$-linear. Now we want to show that for any i and j, the binary vector $b_{i,j} = \phi(q_i + q_j)$ belongs to P_4, i.e. it can be used as a leader of the coset. As P has the minimal distance $d(P) = 6$, it is enough to consider the words of P of weight 6 only. To the contrary, assume that for some $p \in P$ of weight 6 we have $d(p, b_{i,j}) = 2$. Clearly this can happen only, if $\phi^{-1}(p)$ contains elements 2 in both i-th and j-th positions. But in this case the vector $\phi(2\,\phi^{-1}(p))$, which belongs to P, will have the weight 4, i.e. a contradiction. Thus, any vector $b_{i,j}$ belongs to P_4 and $P \star b_{i,j} = P + b_{i,j}$ is a coset of P of weight 4, which, according to Proposition 2.4, belongs to C.

Now for any fixed i and for all $j = 1, 2, ..., (n+1)/2$, the cosets $P + b_{i,j}$ are all disjoint and

$$C \subset \bigcup_{j=1}^{(n+1)/2} \{P + b_{i,j}\}.$$

Finally, by cardinality argument we obtain the statement. ∎

Corollary 3.8 *Let P be an extended $\mathbb{Z}_4$-linear Preparata-like code, and let $C = P \cup P_4$. Then $2\,\mathcal{P} = 2\,\mathcal{C}$.*

Proof: From Theorem 3.7 above we have that any $c \in C$ can be presented in the form $c = p + \phi(q_i + q_j)$ for some $p \in P$ and i and j. In quaternary notation this means that $\phi^{-1}(c) = \phi^{-1}(p) + q_i + q_j$. Multiplying by 2 we obtain

$$2\,\phi^{-1}(c) = 2\,\phi^{-1}(p) + 2\,(q_i + q_j) = 2\,\phi^{-1}(p).$$

∎

From [17] we know that any Preparata-like code P has the vector $\mathbf{1}_2 = \phi(\mathbf{2})$. For $\mathbb{Z}_4$-linear codes we can say much more. We will see in the next propositions that, after a binary coordinate permutation, the quaternary all ones vector $\mathbf{1}$ is contained, simultaneously, in $\mathcal{P}$, $\mathcal{K}$, $\mathcal{C}$ and $\mathcal{H}$.

First we are going to see whether we have in these codes elements v, which have the associated permutation $\pi_v = \sigma$.

Lemma 3.9 *Let P be an extended $\mathbb{Z}_4$-linear Preparata-like code of length $n + 1 = 2^{2m}$ and let K be its $\mathbb{Z}_4$-dual. Assume $m > 2$, $\mathbf{1} \in \mathcal{K}$ and let $x \in \mathcal{K}$ be any vector with a coordinates 1, b coordinates 2, c coordinates 3 and d coordinates 0. Then $a + 2b + 3c \equiv 0 \pmod 4$.*

Proof: Since the length of binary code K is $n+1$ we can write $a+b+c+d = n + 1$.

It is well known (see [16]) that vectors in K have their weights restricted to five possibilities, exactly, 0, $2^{2m-1}-2^{m-1}$, 2^{2m-1}, $2^{2m-1}+2^{m-1}$ and 2^{2m}. Note that for $m>2$ all these weights are multiples of 4.

Let $x \in \mathcal{K}$ any vector with a coordinates 1, b coordinates 2, c coordinates 3 and d coordinates 0. It is easy to compute the weights of some vectors related to $\phi^{-1}(x)$. Vector $\phi^{-1}(x)$ has weight $a+2b+c$, vector $\phi^{-1}(x+x)$ has weight $2a+2c$, vector $\phi^{-1}(x+1)$ has weight $2a+b+d$ and vector $\phi^{-1}(x-1)$ has weight $2c+b+d$.

We see that $\mathrm{wt}(\phi^{-1}(x+1))+\mathrm{wt}(\phi^{-1}(x-1))=2(n+1)$ so, looking at the weights in K, we have two possibilities, either $\mathrm{wt}(\phi^{-1}(x+1))-\mathrm{wt}(\phi^{-1}(x-1))=0$ or $\mathrm{wt}(\phi^{-1}(x+1))-\mathrm{wt}(\phi^{-1}(x-1))=\pm 2^m$. In the first case $2a=2c$ and in the second one $2a-2c=\pm 2^m$. In all the cases for $m>2$ we have $a \equiv c \pmod 4$ or, the same $a+3c \equiv 0 \pmod 4$.

Hence, to finish the proof of this lemma, we only need to show that $2b \equiv 0 \pmod 4$.

Since K is a $\mathbb{Z}_4$-linear code, vector $\phi(x+x)$ belongs to K, but also to H (see Corollary 3.8). The possible weights in H are even more restrictive that in K, in fact there are only three possibilities: 0, 2^{2m-1}, and 2^{2m} (see reference in [11]). In any case we can conclude that, for $m>2$, the weight of vector $\phi(x+x)$ is a multiple of eight and, hence, $a+c \equiv 0 \pmod 4$. But, for $m>2$, the weight of vector $\phi(x)$, like the other vectors in K, is a multiple of 4 and so $2b \equiv 0 \pmod 4$, which finishes our proof. ∎

Proposition 3.10 *Let P be an extended $\mathbb{Z}_4$-linear Preparata-like code, let C be the corresponding extended 1-perfect code and let K and H be their $\mathbb{Z}_4$-duals. Then there exists a vector $v \in H$ such that $\pi_v = \sigma$. This vector v also belongs to C and to K.*

Proof: In Theorem 3.7 we have seen that the $\mathbb{Z}_4$-linear span of vectors $v_{ij}=q_i+q_j$ is contained in C. According to the remarkable Lloyd Theorem

([11], Chapter 6, Theorem 28), all the nonzero codewords in $C^{\perp}$, apart from vector $\mathbf{1}_2$, have the weight equal to half the length, namely $(n+1)/2 = 2^{2m-1}$. Moreover, following [10] or [3], for any $m > 2$ there exists in H some vector v with $\pi_v \neq id$. Vector $\phi^{-1}(v)$ could have even (i.e. containing 0 and 2) and odd (containing 1 and 3) coordinates. Assume that $\phi^{-1}(v)$ has even and odd coordinates. Let i be one of the odd coordinates and let j be one of the even coordinates. But this is not possible because we can take vector $q_i + q_j \in \mathcal{C}$ (see Theorem 3.7), then we will have that $(\phi^{-1}(v), (q_i + q_j))_4 \neq 0$ and therefore $v \notin H$. Hence, the only possibility is that vector $\phi^{-1}(v)$ has only odd coordinates, which implies that $\pi_v = \sigma$.

For the second part of our proposition assume that this claimed vector v does not belong to C. Then there will exists a vector $w \in C$ at distance at most two from v. Hence, there are two possibilities: either $\phi^{-1}(w) = \phi^{-1}(v)+q_i$ for some q_i or $w = v+e_i+e_j$ for some unit binary vectors e_i, e_j. For the first case $0 = (\phi^{-1}(w), \phi^{-1}(v))_4 = (\phi^{-1}(v), \phi^{-1}(v))_4 + 2 \equiv 2^{2m-1} + 2 \equiv 2 \pmod 4$ which is impossible. For the second case we have $\phi^{-1}(w)+q_i+q_k \in \mathcal{P}$ for some index k, and, since $\mathcal{P}$ is $\mathbb{Z}_4$-linear, $\phi^{-1}(w) + \phi^{-1}(w) + \phi^{-1}(\mathbf{1}_2)$ is in $\mathcal{P}$, but $\phi^{-1}(w) + \phi^{-1}(w) + \phi^{-1}(\mathbf{1}_2) = q_i + q_j$ and this is impossible because the minimum weight in P is 6.

Hence, we have a vector $v \in C$ such that $\pi_v = \sigma$ and also $v \in H \subset K$. ∎

Corollary 3.11 *After a permutation of binary coordinates vector $\phi(\mathbf{1})$ belongs to C, H, P and K.*

Proof: Vector $\phi^{-1}(v)$ in Proposition 3.10 has all the quaternary coordinates 1 or 3. Changing value 3 to 1 is a permutation on the two binary coordinates composing the quaternary component we are treating. Hence, after an appropriate coordinate's permutation, we can assure vector $\phi(\mathbf{1})$ belongs to C, H, and K.

Finally, assuming that $\mathbf{1} \in \mathcal{K}$, let $x \in \mathcal{K}$ any vector with a coordinates 1, b coordinates 2, c coordinates 3 and d coordinates 0. The condition that vector $\phi(\mathbf{1})$ belongs to P is equivalent to the condition $a + 2b + 3c = 0 \pmod 4$, but this is true after Lemma 3.9. ∎

4 The rank of $\mathbb{Z}_4$-linear Preparata-like codes and their dual, $\mathbb{Z}_4$-linear Kerdock-like codes.

Now, we will assume that P is a $\mathbb{Z}_4$-linear code (and so C too). We will see that not all the possible ranks are allowable.

Lemma 4.1 *No codeword of C of weight 6 is fixed by σ.*

Proof: In contrary, assume that $x = e_a + e_{\sigma(a)} + e_b + e_{\sigma(b)} + e_c + e_{\sigma(c)}$ is a codeword. As the covering radius of C is equal to 2, the vector $y = e_a + e_b + e_c$ must be at distance 1 from a codeword z of weight 4. If $z = e_a + e_b + e_c + e_d$ where $d \in \{\sigma(a), \sigma(b), \sigma(c)\}$, then the codeword $z \star z$ has weight 4 but $d(x, z \star z) = 2$ and we get a contradiction. If $d \notin \{\sigma(a), \sigma(b), \sigma(c)\}$, then $z \star z$ has weight 8, but again $d(x, z \star z) = 2$ and thus x is not a codeword of C, i.e. we obtain a contradiction. ∎

Lemma 4.2 *All words of weight 4 fixed by σ are in C.*

Proof: Let v be the vector with support as a quadruple $\{a, \sigma(a), b, \sigma(b)\}$, where $a, b \in \{1, \ldots, n+1\}$. The vector v is in the extended code C or it is at the distance 2 from the unique codeword of the extended Preparata code P. This should be w, with support $\{a, \sigma(a), b, \sigma(b), x, y\}$. However because σ is an automorphism of P (in fact, $\sigma(z) = z^{-1}$ for any $z \in P$), for w be unique we should have $y = \sigma(x)$. But this is not possible by the previous lemma. Therefore v is a codeword of C. ∎

Proposition 4.3 *Let C be the extended 1-perfect code corresponding to an extended $\mathbb{Z}_4$-linear Preparata-like code P, of length $n+1 = 2^{2m}$. Then C is the kernel of a group homomorphism θ from $\mathbb{F}^{n+1}$ onto $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$, where $\gamma + 2\delta = 2m+1$ and $\delta = 1$.*

Proof: Given an extended 1-perfect $\mathbb{Z}_4$-linear code C of length $n+1 = 2^{2m}$, we can consider the quaternary code $\mathcal{C}$ as a subgroup of $\mathbb{Z}_4^{(n+1)/2}$. The quotient group $\mathbb{Z}_4^{(n+1)/2}/\mathcal{C}$ is isomorphic to $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$, where $\gamma + 2\delta = 2m+1$ since the number of cosets is equal to

$$\frac{|\mathbb{Z}_4^{(n+1)/2}|}{|\mathcal{C}|} = \frac{2^{2^{2m}}}{2^{2^{2m}-2m-1}} = 2^{2m+1}.$$

Code $\mathcal{C}$ can be seen as the kernel of a group homomorphism θ from $\mathbb{Z}_4^{(n+1)/2}$ onto $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$.

By Lemma 4.2, all cosets of weight 2 are of order 2, and there are n of such cosets. Moreover, there are $n+1$ cosets of weight one and also one coset of weight zero and there are no more cosets with other weights. On the other hand, in $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$, apart from zero, there are $2^{\gamma+\delta}-1$ elements of order two (those with 0 or 2 in the quaternary part) and the rest $(2^{\gamma+2\delta} - 2^{\gamma+\delta})$ are elements of order four. Hence, equaling the quantity of order two elements, we have $2^{\gamma+\delta}-1 = n = 2^{2m}-1$, but $\gamma+2\delta = 2m+1$, so $\delta = 1$ and $\gamma = 2m-1$. ∎

Corollary 4.4 *Quaternary code $\mathcal{H}$ is generated as a $\mathbb{Z}_4$-modulo by vector $\mathbf{1}$ and vectors of type $2x$.*

Proof: From the above lemma, code $\mathcal{H}$, the $\mathbb{Z}_4$-dual of $\mathcal{C}$, can be seen as a code generated by γ vectors of type $2x$ (i.e., all the quaternary coordinates of such vectors are equal to 0 or 2) and $\delta = 1$ vector which is not of type $2x$. But we know that vector $\mathbf{1}$ is in $\mathcal{H}$ (see Corollary 3.11), then we conclude that the $\mathbb{Z}_4$ generators of $\mathcal{C}^\perp$ are vector $\mathbf{1}$ and γ vectors of type $2x$. ∎

Lemma 4.5 *Let γ and δ be such that the quotient set $\mathbb{F}^{n+1}/C$ is isomorphic to $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Let $\theta : \mathbb{F}^{n+1} \longrightarrow \mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ be the homomorphism such that $C = Ker\,\theta$ and let $\tau : \mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta \longrightarrow \mathbb{Z}_2^{\gamma+\delta}$ be the map defined as*

$$\tau(x_1, \ldots, x_\gamma \mid y_1, \ldots, y_\delta) = (x_1, \ldots, x_\gamma \mid y_1 \pmod 2, \ldots, y_\delta \pmod 2)$$

for all $(x_1, \ldots, x_\gamma \mid y_1, \ldots, y_\delta) \in \mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Then the map $\psi = \tau \cdot \theta$

$$\psi : \quad \mathbb{F}^{n+1} \cong \mathbb{Z}_4^\beta \xrightarrow{\theta} \mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta \xrightarrow{\tau} \mathbb{Z}_2^\gamma \times \mathbb{Z}_2^\delta \cong \mathbb{F}^{\gamma+\delta},$$

is a linear map from $\mathbb{F}^{n+1}$ to $\mathbb{F}^{\gamma+\delta}$.

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 observation by taking any permutation π_w associated to vector w. We know permutation π_w is a composition of permutations like π, so

$$\tau \cdot \theta(\pi_w(v)) = \tau \cdot \theta(v). \tag{2}$$

Now we recall the connection of our two operations "+" and "$\star$". For any $w, v \in (\mathbb{F}^{n+1}, *)$ having in mind that π_w always has the order 2, we obtain that

$$w + v = w \star \pi_w(v) \text{ and } w \star v = w + \pi_w(v). \tag{3}$$

It is easy to see that τ is a linear map, i.e. for any $w, v \in \mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$ we have

$$\tau(w + v) \;=\; \tau(w) \;+\; \tau(v). \tag{4}$$

Hence,

$$\begin{aligned}
\psi(w+v) &= \tau\cdot\theta(w+v) && \text{(by definition of } \psi) \\
&= \tau\cdot\theta(w\star\pi_w(v)) && \text{(by(3))} \\
&= \tau\cdot(\theta(w)+\theta(\pi_w(v))) && \text{(by the property of homomorphism)} \\
&= \tau\cdot\theta(w)+\tau\cdot\theta(\pi_w(v)) && \text{(by(4))} \\
&= \tau\cdot\theta(w)+\tau\cdot\theta(v) && \text{(by(2))} \\
&= \psi(w)+\psi(v) && \text{(by definition of } \psi).
\end{aligned}$$

∎

Theorem 4.6 *Let C be an extended perfect $\mathbb{Z}_4$-linear code. If the length of C is $n+1 = 2^{2m} \geq 16$, then $rank(C) = 2^{2m} - 2m$ for $m > 2$ and $rank(C) = 2^{2m} - 2m - 1$ for $m = 2$.*

Proof: From Proposition 4.3 we know that $\delta = 1$. Consider the following map taking into account Lemma 4.5:

$$\mathbb{F}^{n+1} \xrightarrow{\theta} \mathbb{Z}_2^{2m-1} \times \mathbb{Z}_4 \xrightarrow{\tau} \mathbb{F}^{2m}.$$

Since $\psi = \tau\cdot\theta$ is a linear map, we have that $ker(\psi)$ is a linear space. Thus $< C >$ is contained in $ker(\psi)$ and $dim < C > \leq dim(ker(\psi)) = 2^{2m} - 2m$. On the other hand, $dim < C >$ is at least $2^{2m}-2m-1$ which is the dimension of an extended 1-perfect linear code of length $n+1 = 2^{2m}$. As can be seen in [8], an extended Hamming code of length greater than 8 is $\mathbb{Z}_4$-linear if and only if the length is 16. Hence, the result follows. ∎

Corollary 4.7 *The rank of an extended $\mathbb{Z}_4$-linear Preparata-like code P of length 2^{2m} is equal to $rank(P) = 2^{2m} - 2m$ for $m > 2$ and $rank(P) = 2^{2m} - 2m - 1$ for $m = 2$.*

Proof: Straightforward from Proposition 2.2 and the last theorem. ∎

Theorem 4.8 *The rank of $\mathbb{Z}_4$-linear Kerdock-like code K of length $n+1 = 2^{2m}$ is equal to $rank(K) = 2m^2 + m + 1$.*

Proof: The code which is the $\mathbb{Z}_4$-dual of Preparata-like code is a Kerdock-like code [8]. From the result which we prove in the next section (see Theorem 5.11), any such code K of length $n + 1 = 2^{2m}$ have the kernel of dimension $2m + 1$. This means that K is a union of $(n + 1)/2$ cosets of linear code $ker(K)$.

As P is a subset of the corresponding Z_4-linear code C, we conclude, therefore, that $H \subseteq K$. But, according to Lloyd Theorem ([11], Chapter 6, Theorem 28), all the nonzero codewords of H different from $\mathbf{1}_2$ have the weight $(n + 1)/2$. Therefore, the linear subcode of K has the parameters $n+1 = 2^{2m}$, $d = (n+1)/2$ and the dimension $k = 2m+1$, i.e. the parameters of the Reed-Muller code $\mathrm{RM}(1, 2m)$ of the first order. As this code is unique in the class of linear binary codes, we deduce that the linear subcode of K is exactly $\mathrm{RM}(1, 2m)$ code.

Thus, K is the union of $(n+1)/2$ cosets of $\mathrm{RM}(1, 2m)$. One of this coset is the code $\mathrm{RM}(1, 2m)$ itself. It is also known due to [5], that for any such Kerdock code the leaders of the $(n + 1)/2 - 1$ cosets of $\mathrm{RM}(1, 2m)$ form the so called Kerdock set of quadratic forms (these forms have the maximal ranks; they are also called maximal nonlinear bent functions [11]). Any such Kerdock set defines the Kerdock-like code, which is a subcode of the Reed-Muller code $\mathrm{RM}(2, 2m)$, which has the dimension

$$1 + 2m + \binom{2m}{2} = 2m^2 + m + 1.$$

It is also known ([11], Chapter 15, Problem 12), that any such Kerdock-like code generates this code $\mathrm{RM}(2, 2m)$. We conclude, therefore, that $rank(K) = 2m^2 + m + 1$. ∎

5 The kernel of $\mathbb{Z}_4$-linear Preparata-like codes and their dual, $\mathbb{Z}_4$-linear Kerdock-like codes.

After computing the rank of $\mathbb{Z}_4$-linear Preparata-like codes and its dual, $\mathbb{Z}_4$-linear Kerdock-like codes, we are interested in computing the kernel as well.

Recall the definition of $D_\pi = \{z \in D \mid \pi_z = \pi\}$ and $\sigma \in \mathcal{S}_n$ which is the permutation $\sigma = (a_1 a_1') \cdots (a_\beta a_\beta')$ composed by the product of all involutions involving the two coordinates in every $\mathbb{Z}_4$ component.

For any $\mathbb{Z}_4$-linear code $\mathcal{D}$ we have $\sigma \in aut(D)$ since for any $x \in D$ we have $\sigma(x) = x \star x \star x \in D$.

Lemma 5.1 *For all $x \in D$, the permutation π_x is in $aut(D)$ if and only if x is in the kernel $ker(D)$.*

Proof: Recalling that C is a group with operation $\star$, and then using (3), we obtain

$$D \;=\; x \star D \;=\; x + \pi_x(D) \;=\; x + D,$$

which exactly means that the condition $x \in ker(D)$ is equivalent to the condition $\pi_x \in aut(D)$. ∎

Lemma 5.2 *Let $D \subseteq \mathbb{F}^n$ be a $\mathbb{Z}_4$-linear code and let $D^\perp$ be its $\mathbb{Z}_4$-dual, i.e. $D^\perp = \phi(\mathcal{D}^\perp)$. Then $v \in D$ is in $ker(D)$, if and only if the following congruence:*

$$(\phi^{-1}(v) \bullet \phi^{-1}(c),\, \phi^{-1}(x))_4 \equiv 0 \pmod 2$$

is valid for all $c \in D$ and $x \in D^\perp$.

Proof: For any $a, b \in \mathbb{Z}_4$ it is easy to check that $\phi(a) + \phi(b) = \phi(a+b)$ if $a \in \{0,2\}$ or $b \in \{0,2\}$. But if $a, b \in \{1,3\}$, then $\phi(a) + \phi(b) = \phi(a+b+2)$. So we can summarize by giving the following equality:

$$\phi(a) + \phi(b) \;=\; \phi(a + b + 2ab).$$

Clearly this equality can be extended for the vectors over $\mathbb{Z}_4$:

$$\phi(a) + \phi(b) \ = \ \phi(a + b + \mathbf{2} \bullet a \bullet b),$$

which can be rewritten for the binary vectors x, y as follows:

$$x + y \ = \ \phi\left(\phi^{-1}(x) + \phi^{-1}(y) + \mathbf{2} \bullet \phi^{-1}(x) \bullet \phi^{-1}(y)\right). \tag{5}$$

The vectors v from D are in the kernel of D are such that $v + c \in D$ for all $c \in D$. In other words, the vectors v are in kernel of D are such that $(\phi^{-1}(v + c),\, \phi^{-1}(x))_4 = 0$, for all $c \in D$ and $x \in D^{\perp}$. Using the equality (5), we obtain

$$\begin{aligned}(\phi^{-1}(v + c),\, \phi^{-1}(x))_4 &= (\phi^{-1}(v) + \phi^{-1}(c) + \mathbf{2} \bullet \phi^{-1}(v) \bullet \phi^{-1}(c),\, \phi^{-1}(x))_4 \\ &= (\phi^{-1}(v) + \phi^{-1}(c),\, \phi^{-1}(x))_4 + (\mathbf{2} \bullet \phi^{-1}(v) \bullet \phi^{-1}(c),\, \phi^{-1}(x))_4.\end{aligned}$$

But $(\phi^{-1}(v) + \phi^{-1}(c),\, \phi^{-1}(x))_4 = 0$, so the vectors v in kernel of D are the vectors in D such that $(\phi^{-1}(v) \bullet \phi^{-1}(c),\, \phi^{-1}(x))_4 \equiv 0 \pmod 2$.

The inverse part follows similarly. ∎

Lemma 5.3 *Let $D = \phi(\mathcal{D})$ be a $\mathbb{Z}_4$-linear code such that there exists $u \in \mathcal{D}^{\perp}$ such that $\pi_u = \sigma$. Then the condition $v \in ker(D)$ implies the condition $2\,\phi^{-1}(v) \in \mathcal{D}^{\perp}$, i.e.*

$$2\,\phi^{-1}(ker(D)) \ \subseteq \ \mathcal{D}^{\perp}.$$

Proof: In contrary, assume that $v \in ker(D)$ but $2\,\phi^{-1}(v) \notin \mathcal{D}^{\perp}$. This last condition means that there exists $x \in D$ such that $(2\,\phi^{-1}(v),\, \phi^{-1}(x))_4 \neq 0$. But

$$(2\,\phi^{-1}(v),\, \phi^{-1}(x))_4 = (2\,u \bullet \phi^{-1}(v),\, \phi^{-1}(x))_4 = 2\,(u \bullet \phi^{-1}(v),\, \phi^{-1}(x))_4$$

and, taking into account that $u \in \mathcal{D}^{\perp}$, we deduce by Lemma 5.2, that v does not belong to $ker(D)$, i.e. a contradiction. ∎

For the case of the extended 1-perfect $\mathbb{Z}_4$-linear code C, it is possible to say more. Assume that $v \in C$ and $v \notin ker(C)$. Then (see Lemma 5.2), for some $c \in C$ and some vector $x \in H = \phi(\mathcal{C}^{\perp})$ we will have

$$(\phi^{-1}(v) \bullet \phi^{-1}(c),\, \phi^{-1}(x))_4 \not\equiv 0 \pmod 2 \tag{6}$$

But all the vectors in $\mathcal{C}^{\perp}$ are generated by vector $\phi^{-1}(x) = \mathbf{1}$ and vectors $\phi^{-1}(x) = 2y$ (see Corollary 4.4). Hence for the case $\phi^{-1} = 2\,y$ we have $(\phi^{-1}(v) \bullet \phi^{-1}(c), \phi^{-1}(x))_4 \equiv 0 \pmod 2$. The only possibility to fulfill the inequality (6) is when $\phi^{-1}(x) = \mathbf{1}$, so $(\phi^{-1}(v) \bullet \phi^{-1}(c), \mathbf{1})_4 \not\equiv 0 \pmod 2$ and therefore $(\phi^{-1}(v), \phi^{-1}(c))_4 \not\equiv 0 \pmod 2$. This implies that $(2\,\phi^{-1}(v), \phi^{-1}(c))_4 \neq 0$ and, hence, $2\,\phi^{-1}(v) \notin \mathcal{C}^{\perp}$.

Finally, as we know that a vector u such that $\pi_u = \sigma$ belongs to P, K, C and to H, we can write (see Lemma 5.3):

$$\left.\begin{array}{rcl} 2\,\phi^{-1}(ker(C)) & = & \mathcal{H} \\ 2\,\phi^{-1}(ker(H)) & \subseteq & \mathcal{C} \\ 2\,\phi^{-1}(ker(P)) & \subseteq & \mathcal{K} \\ 2\,\phi^{-1}(ker(K)) & \subseteq & \mathcal{P}. \end{array}\right\} \tag{7}$$

For Preparata and Kerdock codes we can say a little more.

Lemma 5.4 *Let P be any $\mathbb{Z}_4$-linear Preparata-like code, let C be the corresponding extended 1-perfect $\mathbb{Z}_4$-linear code and let K and H be their $\mathbb{Z}_4$-dual codes. Then*

$$2\,\phi^{-1}(ker(P)) \subset \mathcal{H} \;\; and \;\; 2\,\phi^{-1}(ker(K)) \subset \mathcal{H}.$$

Proof: If $v \in ker(P)$, from Lemma 5.2, we have that $(\phi^{-1}(v) \bullet \phi^{-1}(c), \phi^{-1}(x))_4 \equiv 0 \pmod 2$ for all $c \in P$ and $x \in K$. Clearly we can rewrite it as $(\phi^{-1}(v) \bullet \phi^{-1}(x), \phi^{-1}(c))_4 \equiv 0 \pmod 2$. Take $x \in K$ as the vector with $\pi_x = \sigma$ (see Lemma 3.11). Hence

$$(\phi^{-1}(v) \bullet \phi^{-1}(x), \phi^{-1}(c))_4 \equiv (\phi^{-1}(v), \phi^{-1}(c))_4 \equiv 0 \pmod 2.$$

This implies that

$$(2\,\phi^{-1}(v), \phi^{-1}(c))_4 \;=\; (\phi^{-1}(v),\, 2\,\phi^{-1}(c))_4 \;=\; 0.$$

This last equality is satisfied for any $v \in ker(P)$ and for any $c \in P$. But, by Corollary 3.8, we have $2\,\mathcal{P} = 2\,\mathcal{C}$. Therefore, this equality is fulfilled by all the vectors $x \in C$. We deduce finally, that $2\,\phi^{-1}(ker(P)) \in \mathcal{H}$.

The second statement of the lemma follows by exactly the same arguments. ∎

Lemma 5.5 *Let P be any $\mathbb{Z}_4$-linear Preparata-like code and let $C = P \cup P_4$. Then $ker(P) \subset ker(C)$.*

Proof: We only need to show that, if $x \in ker(P)$, then $x \in ker(C)$. If $x \in ker(P)$ then, for all $v \in P$ we have $x + v \in P$. Take $w \in C$ and let $v \in P$ be such that $w = v \star a = v + \pi_v(a) = v + a$, where $a = \phi(q_1 + q_i)$ and vectors q_i are like in Theorem 3.7. Now, $x + w = x + v + a = (x + v) \star a \in P \star a \subset C$ and, hence, $x \in ker(C)$. ∎

Lemma 5.6 *Let P be any $\mathbb{Z}_4$-linear Preparata-like code of length $n+1 = 2^{2m}$. The linear code P_{id} of all the elements of P, the associated permutation of which is the identity, has dimension $2^{2m-1} - 2m$.*

Proof: The elements in P the associated permutation of which is the identity have in quaternary notation 2's in all the nonzero coordinates. But, according to Lemma 4.1, no codeword of weight 6 is fixed by σ. This means that these kind of elements have weight at least 8. That is to say, they have at least four coordinates with 2's in quaternary notation.

Let the vectors q_i over $\mathbb{Z}_4$ be as in Theorem 3.7. Take three such vectors, say q_i, q_j, q_k and recall (see the proof of Theorem 3.7) that one can see C as the union of P with cosets $P \star \phi(q_i + q_s)$ (for all $s = 1, 2, ..., (n+1)/2$). Now as C is $\mathbb{Z}_4$-linear, $(P \star \phi(q_i + q_j)) \star (P \star \phi(q_i + q_k))$ is a coset, say $P \star \phi(q_i + q_r)$

for some r. This means that $\phi(q_i + q_j + q_k + q_r) \in P$ and that given q_i, q_j, q_k, there exists a unique q_r, such that $\phi(q_i + q_j + q_k + q_r) \in P$. Hence these 4-tuples $\{q_i, q_j, q_k, q_r\}$ of vectors compose a Steiner Quadruple System (SQS) $S((n+1)/2, 4, 3)$ on 2^{2m-1} quaternary coordinates.

Now we can think of the vectors of P_{id} as binary vectors in $(n+1)/2 = 2^{2m-1}$ coordinates, where the coordinate is 1 or 0 depending on q_i is in the support of this vector, or not. Using this binary representation of P_{id} we get a binary linear code of minimum weight 4 and such that the vectors of this minimum weight forms a $S((n+1)/2, 4, 3)$. Now according to the well known result due to Assmus and Mattson ([11], Chapter 6, Problem (14)), the corresponding linear code is a binary extended 1-perfect code of length $(n+1)/2$. Hence, the binary representation of P_{id} is this linear code and so $dim(P_{id}) = 2^{2m-1} - (2m-1) - 1 = 2^{2m-1} - 2m$. ∎

Lemma 5.7 *Let $\mathbf{1} \in \mathcal{H}$ be the quaternary all ones vector. Then $< K_{id}, \phi(\mathbf{1}) >= H$.*

Proof: The elements v in K_{id} are the elements $v \in K$ with the identity as a associated permutation π_v. This means they have in the quaternary notation the element 2 in all the nonzero coordinates, in other words, $\phi^{-1}(v) = 2\,\phi^{-1}(w)$ for some w. Moreover, we have that $(\phi^{-1}(v), \phi^{-1}(x))_4 = 0$ for all $x \in P$. But $2\,\mathcal{C} = 2\,\mathcal{P}$ (see Theorem 3.7). Hence $(\phi^{-1}(w), 2\,\phi^{-1}(x))_4 = (2\,\phi^{-1}(w), \phi^{-1}(x))_4 = 0$ for all $x \in C$, and therefore $2\,\phi^{-1}(w) = \phi^{-1}(v)$ belongs to $\mathcal{H}$, which means that $K_{id} \subset H$.

Now let $v \in H$ and assume $\pi_v \neq \sigma$. So $\phi^{-1}(v) = 2\,\phi^{-1}(w)$ for some vector $w \in \mathbb{Z}_4^{2^{2m-1}}$ (see Corollary 4.4). We will have $(\phi^{-1}(v), \phi^{-1}(x))_4 = 0$ for all $x \in C$. But $x = p \star \phi(q_1 + q_i)$ for some q_i and $p \in P$ (see Theorem 3.7).

Hence

$$\begin{aligned} 0 &= (\phi^{-1}(v), \phi^{-1}(x))_4 \\ &= (\phi^{-1}(v), \phi^{-1}(p + q_1 + q_i))_4 \\ &= (\phi^{-1}(v), \phi^{-1}(p))_4 + (\phi^{-1}(v), \phi^{-1}(q_1 + q_i))_4 \\ &= (\phi^{-1}(v), \phi^{-1}(p))_4 \end{aligned}$$

and, so, $v \in K$ and therefore $v \in K_{id}$. ∎

Corollary 5.8 *Let K be any $\mathbb{Z}_4$-linear Kerdock-like code. The linear code K_{id} of all the elements in K the associated permutation of which is the identity has dimension $2m$.*

Proof: From Lemma 5.7 we have, that $< K_{id}, \phi(\mathbf{1}) >= H$. As $\phi(\mathbf{2})$ belongs to H and therefore $\phi(\mathbf{2})$ belongs to K_{id} by Lemma 5.7 again, we deduce that $dim(K_{id}) = dim(H) - 1 = 2m$. ∎

Lemma 5.9 *Let π_v be the permutation associated with vector v. Then $\pi_v \in aut(K)$, if and only if $\pi_v \in aut(P)$.*

Proof: For a $\mathbb{Z}_4$-linear code the permutation π_v of binary coordinate means in quaternary notation the identity or a sign change in some quaternary coordinates and this permutation depends only on v, so for any vector $a = (a_1, a_2, \ldots)$ over $\mathbb{Z}_4$ we have $\pi_v(a) = (\pm a_1, \pm a_2, \ldots)$.

For all the elements $p \in \mathcal{P}$ and $w \in \mathcal{K}$ compute the quaternary inner product $(p, w)_4$. Using the quaternary interpretation of π_v, observe that $(\pi_v(p), w)_4 = (p, \pi_v(w))_4$. The statement follows. ∎

Lemma 5.10 *Let P be any $\mathbb{Z}_4$ linear Preparata-like code of length $n + 1 = 2^{2m}$. Let v and w two binary vectors with associated permutation, respectively, π_v and π_w. Let A and B be the sets of binary coordinates moved, respectively, by π_v and π_w and assume that $A \cap B = \emptyset$ and $|A \cup B| = n + 1$. Then π_v or π_w are not in $aut(P)$.*

Proof: Fix two binary coordinates $a, c \in A$ and consider $b = \pi_v(a) \in A$. The binary codewords of weight 6 of an extended Preparata code P form a 3-design [14], so starting from a, b, c we can find $(2^{2m} - 4)/3$ triples which jointed to a, b, c gives us codewords of P. It is not possible that all these triples are in A, so let e, f, g one of the other triples. Let p be the codeword of P of weight 6 with the support $supp(p) = \{a, b, c, e, f, g\}$.

If we assume $e, f, g \in B$ we have $d(p, \pi_v(p)) = 2$.

If we assume that two coordinates $e, f \in B$ we have $d(p, \pi_v(p)) = 4$.

If we assume that only one coordinate $e \in B$ we have $d(p, \pi_w(p)) = 2$.

In any case, π_v or π_w could not be an automorphism of P. ∎

Theorem 5.11 *Let P be any $\mathbb{Z}_4$-linear Preparata-like code of length $n+1 = 2^{2m}$ and let K be its $\mathbb{Z}_4$-dual. Then $dim\,(ker(P)) = 2^{2m-1} - 2m + 1$ and $dim\,(ker(K)) = 2m + 1$.*

Proof: From Lemma 3.11 we know that $\mathbf{1} \in \mathcal{P}$. The associated permutation to $\phi^{-1}(\mathbf{1})$ is σ and, from Lemma 5.1 $\phi(\mathbf{1}) \in ker(P)$. Now we want to show, that apart from this vector $\phi(\mathbf{1}) \in P$, there is no other vector in $ker(P)$ such that the associated permutation be different of the identity. To the contrary, assume that there is some $v \in ker(P)$ such that $\pi_v \neq \sigma$ and $\pi_v \neq id$.

Apart from the vectors from P_{id} and the vector $\phi^{-1}(\mathbf{1}) \in P$, the elements v of $ker(P)$ are such that $2\,\phi^{-1}(v) \in \mathcal{H}$ (see Lemma 5.4). So $2\,\phi^{-1}(v)$ has exactly $(n + 1)/4$ odd quaternary coordinates, and therefore π_v moves half of the binary coordinates, namely $(n + 1)/2 = 2^{2m-1}$. Denote by A this set of binary coordinates.

Let $w \in P$ the vector such that $\phi^{-1}(w) = \mathbf{1} + \phi^{-1}(v)$. Applying Lemma 5.2 observe w is also in the kernel like v. Permutation π_w, like the permutation π_v, moves half of the coordinates, exactly 2^{2m-1}. Denote by B this set of coordinates.

By definition, the positions of the elements 1 and 3 in $\phi^{-1}(v)$ differ from the positions of 1 and 3 in $\phi^{-1}(w)$. We deduce, that $A \cap B = \emptyset$ and also $|A \cup B| = n+1 = 2^{2m}$. Now applying Lemmas 5.1 and 5.10 we conclude that v (and w) are not in $ker(P)$ and this contradicts our assumption.

The same for the second statement of the theorem. In this case, we want to show, that apart from vector $\phi(\mathbf{1}) \in K$, there is no other vector in $ker(K)$ such that the associated permutation be different of the identity. In contrary, if we assume that there is some $v \in ker(P)$ such that $\pi_v \neq \sigma$ and $\pi_v \neq id$ we find sets A and B containing, respectively, all the binary coordinates moved by π_v and π_w, where $w = \phi(1) \star v$. These sets fulfill the requirements in Lemma 5.10 and after Lemma 5.1 and Lemma 5.9 we conclude that v and w are not in $ker(K)$ which contradicts our assumption. ∎

6 Conclusions

The standard Preparata code has a propelinear structure but it is not additive. For the case of additive Preparata-like codes we have seen that the only possibility is that of the extended $\mathbb{Z}_4$-linear Preparata-like codes. In this case, we have computed the rank and the dimension of the kernel for these codes and their duals.

As a summary we have the following table:

$$\begin{array}{lcl} dim(ker(P)) & = & 2^{2m-1} - 2m + 1 \\ dim(ker(K)) & = & 2m + 1 \\ rank(P) & = & 2^{2m} - 2m \quad (\text{and } \; 2^{2m} - 2m - 1 \quad \text{for } \; m = 2) \\ rank(K) & = & 2m^2 + m + 1 \end{array}$$

References

[1] R.D. Baker, J.H. van Lint, R.M. Wilson, "On the Preparata and Goethals codes", *IEEE Trans. Inform. Theory*, vol. 29, n. 3, pp. 342-345, May 1983.

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

[3] J. Borges, K.T. Phelps, J. Rifa, "Extended 1-perfect additive codes", Technical Report Pirdi n.01/2002, Autonomous University of Barcelona, Spain. May 2002. Available: http://pirdi.uab.es.

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

[5] P. Delsarte, J.-M. Goethals, "Alternating bilinear forms over $GF(q)$", *Journal of Combinatorial Theory*, 19-A, pp. 26-50, 1975.

[6] I.I. Dumer, "Some new uniformly packed codes", Proc. of Moscow Institute of Physics and Technology, pp. 72-78. Moscow, 1976.

[7] J.M. Goethals and S.L. Snover, "Nearly perfect binary codes", *Discrete Math.*, vol. 3, pp. 65-88, 1972.

[8] 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.

[9] T. Helleseth, V.A. Zinoviev, "On nonlinear codes from linear codes over Z_4 and their cosets", 2001, under submission.

[10] 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.

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

[12] F.P. Preparata, "A class of optimum nonlinear double-error correcting codes," *Inform. and Control*, vol. 13, pp. 378-400, 1968.

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

[14] N.V. Semakov and V.A. Zinoviev, "Balanced codes and tactical configurations," *Problems Inform. Transmission*, vol. 5, pp. 22-28, 1969.

[15] N.V. Semakov, V.A. Zinoviev and G.V. Zaitsev, "Uniformly packed codes," *Problems Inform. Transmission*, vol. 7, pp. 30-39, 1971.

[16] N.V. Semakov, V.A. Zinoviev and G.V. Zaitsev, "On duality of Preparata and Kerdock codes", in: Fifth All-Union Conf. on Coding Theory, Moscow-Gorkyi, 1972, part 2, pp. 55-58 (in Russian).

[17] N.V. Semakov, V.A. Zinoviev and G.V. Zaitsev, "Interrelation of Preparata and Hamming codes and extension of Hamming codes to new double-error-correcting codes," *Proc. 2nd Internat. Sympos. Inform. Theory*, Tsakhadsor, Armenia, 1971, Academiai Kiado, Budapest, 1973.