On the Apparent Duality of the Kerdock and Preparata Codes *

A. Roger Hammons, Jr.[1], P. Vijay Kumar[2], A. R. Calderbank[3], N.J.A. Sloane[3], Patrick Solé[4]

[1] Hughes Aircraft Company,
8433 Fallbrook Avenue, Canoga Park, CA 91304-0445 U.S.A.
[2] Communication Sciences Institute,
EE-Systems, University of Southern California,
Los Angeles, CA 90089-2565 U.S.A.
[3] Mathematical Sciences Research Center
AT&T Bell Laboratories, Murray Hill, NJ 07974 U.S.A.
[4] CNRS-I3S, 250 rue A. Einstein, bâtiment 4
Sophia - Antipolis, 06560 Valbonne, France

Abstract. The Kerdock and extended Preparata codes are something of an enigma in coding theory since they are both Hamming-distance invariant and have weight enumerators that are MacWilliams duals just as if they were dual linear codes. In this paper, we explain, by constructing in a natural way a Preparata-like code $\mathcal{P}_L$ from the Kerdock code $\mathcal{K}$, why the existence of a distance-invariant code with weight distribution that is the McWilliams transform of that of the Kerdock code is only to be expected. The construction involves quaternary codes over the ring $\mathbb{Z}_4$ of integers modulo 4. We exhibit a quaternary code $\mathcal{Q}$ and its quaternary dual $\mathcal{Q}^\perp$ which, under the Gray mapping, give rise to the Kerdock code $\mathcal{K}$ and Preparata-like code $\mathcal{P}_L$, respectively. The code $\mathcal{P}_L$ is identical in weight and distance distribution to the extended Preparata code. The linearity of $\mathcal{Q}$ and $\mathcal{Q}^\perp$ ensures that the binary codes $\mathcal{K}$ and $\mathcal{P}_L$ are distance invariant, while their duality as quaternary codes guarantees that $\mathcal{K}$ and $\mathcal{P}_L$ have dual weight distributions. The quaternary code $\mathcal{Q}$ is the $\mathbb{Z}_4$-analog of the first-order Reed-Muller code. As a result, $\mathcal{P}_L$ has a simple description in the $\mathbb{Z}_4$-domain that admits a simple syndrome decoder. At length 16, the code $\mathcal{P}_L$ coincides with the Preparata code.

1 Introduction

Recently, a family of nearly optimal four-phase sequences of period $N = 2^r - 1$, r odd, with alphabet $\{1, j, -1, -j\}$, $j = \sqrt{-1}$, was discovered first by Solé [17] and later independently by Boztaş , Hammons, and Kumar [2] (see also [18]). After replacing each complex fourth root-of-unity j^a by its exponent $a \in \{0, 1, 2, 3\}$, this family may be viewed as a linear quaternary code over the ring $\mathbb{Z}_4$ of

* This work was supported in part by the National Science Foundation under Grant NCR-9016077 and by Hughes Aircraft Company under its Ph.D. fellowship program.

integers modulo 4. Since the family has low correlation values, it also possesses large minimum Euclidean distance and thus the potential for excellent error-correcting capability.

A 2-adic (*i.e.*, base 2) expansion of the four-phase sequences is contained in [2]. Interestingly, this bore a striking resemblance to the original expression [12] for the nonlinear binary Kerdock code. A second connection with the Kerdock code arose during attempts to construct good binary codes from the four-phase sequence family using the Gray map. This was a logical step to pursue as the Gray map translates a quaternary code with large minimum Euclidean distance into a binary code of twice the length having large minimum Hamming distance. The codes that resulted were nonlinear and had the same parameters as shortened versions of the Kerdock code.

In exploring these connections, it was discovered that the original quaternary code could be enlarged in a natural way, to a linear quaternary code $\mathcal{Q}$ whose image under the Gray map is *precisely* the Kerdock code. It was only natural to consider whether the interesting link between the Kerdock code and a linear quaternary code could also be used to explain the apparent duality of the Kerdock and Preparata codes.

The new perspective does indeed provide an explanation, although not the one that might first be suspected. We show that the binary images $\mathcal{G}(\mathcal{C})$ and $\mathcal{G}(\mathcal{C}^{\perp})$ under the Gray map of a linear quaternary code $\mathcal{C}$ and its $\mathbb{Z}_4$-dual are always Hamming distance invariant. Furthermore, these binary codes have the property that their weight distributions are always dual under the MacWilliams transform. As a consequence, the Kerdock code possesses a *natural* "quaternary-dual" code $\mathcal{P}_L = \mathcal{G}(\mathcal{Q}^{\perp})$, identical in size, weight, and distance to the extended Preparata code. Although the Preparata and Preparata-like ($\mathcal{P}_L$) codes have similar finite field transform descriptions, they are in general not the same.

Interestingly, at length 16, the Preparata and Preparata-like codes do coincide. In fact, the Kerdock code, the extended Preparata code, and the Preparata-like code all coincide with the Nordstrom-Robinson code $\mathcal{N}_{16}$. Thus, the Nordstrom-Robinson code can be generalized in one way to get the extended Preparata codes, in another way to get the Kerdock codes, and in yet another way to get the Preparata-like codes!

From the standpoint of decoding, it is not necessary to distinguish between the binary codes and their quaternary parents. An important advantage in working in the $\mathbb{Z}_4$-domain, where the codes are linear, is that it is meaningful to speak of syndromes. Moreover, the codes $\mathcal{Q}$ and $\mathcal{Q}^{\perp}$ are $\mathbb{Z}_4$-analogs of the binary first-order Reed-Muller code $RM(1, r)$ and its dual $RM(r-2, r)$. This connection makes decoding of the Kerdock and Preparata codes, at least conceptually, easier.

Our discussion of these results is organized in the following manner. In Sect. 2, we present the general theory of linear quaternary codes, their duals, and their images as binary codes under the Gray map. We show that the curious linear-like properties of the Kerdock and Preparata codes are true in general for this new class of binary codes. We demonstrate that the Kerdock code is a

member of this class and provide a finite field transform characterization of its Preparata-like pseudo-dual. In Sect. 3, we present simple Galois ring theoretic descriptions of the codes. In Sect. 4, we consider the impact of the new quaternary interpretation on decoding algorithms. Finally, Sect. 5 provides an update on related results by the authors.

2 Theory of Quaternary and Related Binary Codes

2.1 Quaternary Codes

The interest here is in linear block codes over the ring $\mathbb{Z}_4$ of integers modulo 4. By a linear (n, M) quaternary code, we shall mean a set $\mathcal{C}$, consisting of M $\mathbb{Z}_4$-valued n-tuples, that is closed under addition modulo 4. Algebraically, $\mathcal{C}$ is a $\mathbb{Z}_4$-module, *i.e.* a module over the ring $\mathbb{Z}_4$.

Like linear block codes over finite fields, linear quaternary codes possess natural duals. If $\mathcal{C}$ is a linear (n, M) quaternary code, its dual $\mathcal{C}^{\perp}$ is defined to be the set of all $\mathbb{Z}_4$-valued n-tuples $\underline{v} = (v_1, v_2, \ldots, v_n)$ satisfying

$$\underline{u} \cdot \underline{v} = \sum_{t=1}^{n} u_t v_t = 0, \qquad \forall \underline{u} = (u_1, u_2, \ldots, u_n) \in \mathcal{C} \ . \tag{1}$$

To each $\mathbb{Z}_4$-valued codeword $\underline{c} = (c(t) : t \in I)$, we associate the equivalent complex roots-of-unity sequence $\underline{s} = \omega^{\underline{c}} = (\omega^{c(t)} : t \in I)$, where $\omega = i = \sqrt{-1} = e^{2\pi i/4}$. Then, given a set $\mathcal{C}$ of quaternary vectors, we let

$$\Omega\ (\mathcal{C}) = \{\omega^{\underline{c}} : \underline{c} \in \mathcal{C}\} \tag{2}$$

denote the corresponding set of complex sequences. When $\mathcal{C}$ is regarded as a set of quaternary CDMA signature sequences, its effectiveness depends upon the complex correlations (or inner products) of the sequences in $\Omega\ (\mathcal{C})$. When $\mathcal{C}$ is regarded as a quaternary code, its error-correcting capability depends upon the Euclidean distance properties of $\Omega\ (\mathcal{C})$. Note that if $\underline{c}_0 = (c_0(t) : t = 1, 2, \ldots, n)$ and $\underline{c}_1 = (c_1(t) : t = 1, 2, \ldots, n)$ are quaternary vectors with associated complex vectors $\underline{s}_0 = \Omega\ (\underline{c}_0)$ and $\underline{s}_1 = \Omega\ (\underline{c}_1)$, then

$$||\underline{s}_1 - \underline{s}_0||^2 = ||\underline{s}_1||^2 + ||\underline{s}_0||^2 - 2\ \mathrm{Re}\{\underline{s}_1^{\mathrm{H}} \underline{s}_0\} \tag{3}$$

$$= 2n - 2\mathrm{Re}\{\zeta(\underline{c}_1 - \underline{c}_0)\}, \tag{4}$$

where $^{\mathrm{H}}$ denotes the Hermitian inner product and

$$\zeta(\underline{c}_1 - \underline{c}_0) = \sum_{t=1}^{n} \omega^{c_1(t) - c_0(t)} \tag{5}$$

is the *complex correlation* of $\underline{c}_0$ and $\underline{c}_1$. Note that ζ depends only on the difference $\underline{c} = \underline{c}_1 - \underline{c}_0$. By the above, if the nontrivial correlations of $\Omega\ (\mathcal{C})$ are low in magnitude, then the set also possesses large minimum Euclidean distance.

2.2 Equivalent Binary Codes under the Gray Map

In communication systems employing quadrature phase-shift keying (QPSK), the preferred assignment of two information bits to the four possible phases is the one in which adjacent phases differ by only one binary digit. This mapping is called *Gray encoding* and has the advantage that, when a quaternary codeword is transmitted across the additive white Gaussian noise channel, the errors most likely to occur are those causing a single erroneously decoded information bit.

For $c \in \mathbb{Z}_4$, it is natural from an algebraic viewpoint to consider the 2-adic expansion

$$c = 2a + b \tag{6}$$

where $a, b \in \{0, 1\}$. If u, v denote the two binary digits assigned to the complex number ω^c by the Gray encoder, then the pairs (a, b) and (u, v) are related by

$$u = a \tag{7}$$

$$v = a \oplus b. \tag{8}$$

where $\oplus$ denotes addition modulo 2.

Consider the map $g : \Omega\,(\mathbb{Z}_4{}^n) \rightarrow (\mathbb{Z}_2\,)^{2n}$ in which $g(\omega^{\underline{c}}) = (\,\underline{u} \mid \underline{v}\,) = (\,\underline{a} \mid \underline{a} \oplus \underline{b}\,)$. It is easy to see that g maps complex vectors into binary vectors of twice the length in such a way that the squared Euclidean distance between two complex vectors is proportional to the Hamming distance between the corresponding binary vectors.

Thus, given a quaternary code $\mathcal{C}$ whose associated complex sequence set has good Euclidean distance, it is natural to examine the binary code $\mathcal{B}$ obtained by mapping the quaternary codeword $\underline{c} = 2\underline{a} + \underline{b}$ in $\mathcal{C}$ to the binary codeword $(\,\underline{a} \mid \underline{a} \oplus \underline{b}\,)$. In general, if $\mathcal{C}$ is a code of length n, then $\mathcal{B}$ is a nonlinear code of length $2n$. We will use $\mathcal{G} : (\mathbb{Z}_4\,)^n \rightarrow (\mathbb{Z}_2\,)^{2n}$ to denote this *Gray map* transformation, so that $\mathcal{G}(\mathcal{C}) = \mathcal{B}$.

2.3 Weight and Distance Properties

In this section, we discuss the weight and distance properties of the quaternary codes $\mathcal{C}$ and $\mathcal{C}^\perp$ and their respective associated binary codes $\mathcal{B} = \mathcal{G}(\mathcal{C})$ and $\mathcal{B}_\perp = \mathcal{G}(\mathcal{C}^\perp)$. The two principal results to be derived here are the following:

1. $\mathcal{B}$ and $\mathcal{B}_\perp$ are distance invariant.
2. The weight distributions of $\mathcal{B}$ and $\mathcal{B}_\perp$ are MacWilliams transforms of one another.

A binary code $\mathcal{B}$ is said to be *distance invariant* if the Hamming weight distributions of its translates $\underline{c} + \mathcal{B}$ are the same for all $\underline{c} \in \mathcal{B}$.

Theorem 1. *If $\mathcal{C}$ is a linear quaternary code, then its binary Gray representation $\mathcal{G}(\mathcal{C})$ is distance invariant.*

Proof. When $\mathcal{C}$ is a linear quaternary code, the complex signal set $\Omega(\mathcal{C})$ is Euclidean distance invariant, *i.e.* the set of relative Euclidean distances

$$\{||\underline{s} - \underline{s}_0|| \ : \ \underline{s} \in \Omega(\mathcal{C})\} \tag{9}$$

does not depend on the choice of $\underline{s}_0 \in \Omega(\mathcal{C})$. This is clear from (3) and (4). Since Hamming distances in $\mathcal{G}(\mathcal{C})$ are proportional to squared-Euclidean distances in $\Omega(\mathcal{C})$, $\mathcal{G}(\mathcal{C})$ must be Hamming distance invariant. □

Next, we recall from [15], (pp. 141–145), that the *complete weight enumerator* for a binary code $\mathcal{B}$ of block length n is a polynomial in two variables given by

$$W_{\mathcal{B}}(z_0, z_1) = \sum_{\underline{c}=[c_1,c_2,\ldots,c_n]\in\mathcal{B}} z_0^{k_0(\underline{c})} z_1^{k_1(\underline{c})} \ , \tag{10}$$

where $k_i(\underline{c})$ is the number of times the value i appears as an entry in the vector $\underline{c}$. If $\mathcal{B}$ is a linear binary code with dual $\mathcal{B}^{\perp}$, the weight enumerators of the two codes are related by the MacWilliams transform:

$$W_{\mathcal{B}^{\perp}}(z_0, z_1) = \frac{1}{|\mathcal{B}|} W_{\mathcal{B}}(z_0 + z_1, z_0 - z_1) \ . \tag{11}$$

Similarly, the complete weight enumerator for a quaternary code $\mathcal{C}$ is defined by

$$W_{\mathcal{C}}(z_0, z_1, z_2, z_3) = \sum_{\underline{c}=[c_1,c_2,\ldots,c_n]\in\mathcal{C}} z_0^{k_0(\underline{c})} z_1^{k_1(\underline{c})} z_2^{k_2(\underline{c})} z_3^{k_3(\underline{c})} \ . \tag{12}$$

The relationships between the complete weight enumerators of $\mathcal{C}$, its dual $\mathcal{C}^{\perp}$, and their binary representations $\mathcal{G}(\mathcal{C})$ and $\mathcal{G}(\mathcal{C}^{\perp})$ are given by the following theorems.

Theorem 2 (MacWilliams Transform for Codes over $\mathbb{Z}_4$). *If $\mathcal{C}$ and $\mathcal{C}^{\perp}$ are dual quaternary codes, then*

$$W_{\mathcal{C}^{\perp}}(z_0, z_1, z_2, z_3) = \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}\left(\sum_{i=0}^{3} z_i\omega^{0\cdot i}, \sum_{i=0}^{3} z_i\omega^{1\cdot i}, \sum_{i=0}^{3} z_i\omega^{2\cdot i}, \sum_{i=0}^{3} z_i\omega^{3\cdot i}\right) \ . \tag{13}$$

Proof. The proof is essentially the same as in [15], (Thm. 10, pp. 141–145) for codes over $GF(4)$. □

Lemma 3. *If $\mathcal{C}$ is a quaternary code and $\mathcal{G}(\mathcal{C})$ is its binary Gray representation, then*

$$W_{\mathcal{G}(\mathcal{C})}(z_0, z_1) = W_{\mathcal{C}}(z_0^2, z_0 z_1, z_1^2, z_0 z_1) \ . \tag{14}$$

Proof. Immediate from the definitions. □

Theorem 4. *If $\mathcal{C}$ and $\mathcal{C}^{\perp}$ are dual quaternary codes, then the weight distributions of the nonlinear binary codes $\mathcal{G}(\mathcal{C})$ and $\mathcal{G}(\mathcal{C}^{\perp})$ are related by the binary MacWilliams transform.*

Proof. By the above theorems,

$$W_{\mathcal{G}(\mathcal{C}^{\perp})}(z_0, z_1) = W_{\mathcal{C}^{\perp}}(z_0^2, z_0 z_1, z_1^2, z_0 z_1) \tag{15}$$

$$= \frac{1}{|\mathcal{C}|} W_{\mathcal{C}}((z_0 + z_1)^2, z_0^2 - z_1^2, (z_0 - z_1)^2, z_0^2 - z_1^2) \tag{16}$$

$$= \frac{1}{|\mathcal{G}(\mathcal{C})|} W_{\mathcal{G}(\mathcal{C})}(z_0 + z_1, z_0 - z_1), \tag{17}$$

which is the desired result. □

2.4 Quaternary View of the Kerdock and Preparata-Like Codes

A monic polynomial in $\mathbb{Z}_4\ [x]$ is a *primitive basic irreducible* if its projection modulo 2 is a primitive, irreducible polynomial in $\mathbb{Z}_2\ [x]$. Let $f(x) = f_0 + f_1 x + f_2 x^2 + \ldots + f_{r-1} x^{r-1} + x^r$ be a primitive basic irreducible dividing $x^N - 1$ in $\mathbb{Z}_4\ [x]$, where $N = 2^r - 1$. Let $\mathcal{Q}^-(r)$ denote the set of all $\mathbb{Z}_4$-valued sequences that satisfy the linear recurrence over $\mathbb{Z}_4$ whose characteristic polynomial is $f(x)$. Specifically, the $\mathbb{Z}_4$-valued sequence $c(t)$ is in $\mathcal{Q}^-(r)$ iff

$$c(t) = -\sum_{i=0}^{r-1} f_i\, c(t-i) \qquad \forall t \geq r \ . \tag{18}$$

It is not hard to show that all the sequences in $\mathcal{Q}^-$ have common period N and thus may be regarded as elements of $\mathbb{Z}_4{}^N$. Then, it is clear by construction that $\mathcal{Q}^-(r)$ is a cyclic, linear quaternary code of length N, rank r, and size 4^r.

Let $\mathcal{A}$ denote the family of cyclically distinct sequences obtained from $\mathcal{Q}^-$ by deleting the all-zero sequence and failing to distinguish between a sequence and any of its cyclic shifts. The corresponding collection $\Omega(\mathcal{A})$ of complex-valued sequences has been studied in [2] [17][18] as a family of asymptotically optimal CDMA signature sequences (referred to as Family $\mathcal{A}$ in [2]). Since the sequences of $\Omega(\mathcal{A})$ have low values of auto- and cross-correlation, the set also has large minimum Euclidean distance.

A little experimentation shows that $\mathcal{Q}^-(r)$ can be enlarged while preserving the minimum Euclidean distance of the corresponding complex sequence set. Let $\mathcal{Q}(r)$ denote the following enlarged code:

1. Extend the block length of the code from $N = 2^r - 1$ to $N' = 2^r$ by introducing a leading "0" to each $\mathcal{Q}^-$ codeword.
2. Increase the size of the code from 4^r to 4^{r+1} by adding an arbitrary $\mathbb{Z}_4$-valued constant vector to each lengthened codeword.

This is analogous to the process by which one enlarges the binary maximum-length code to obtain the first-order Reed-Muller code.

Let $\underline{c}^- = (c^-(t) : t \in I)$ denote a $\mathcal{Q}^-$ codeword where $I = \{0, 1, 2, \ldots, N-1\}$. Then, the codewords of $\mathcal{Q}$ are of the form

$$\underline{c} = (c(t) : t \in I^{\star}) \ , \tag{19}$$

where $I^\star \doteq I \cup \{\star\}$, $c(\star) = \delta$ is the arbitrary $\mathbb{Z}_4$-valued constant, and $c(t) = c^-(t) + \delta$ for all $t \in I$.

Theorem 5. *When r is an odd integer, the binary code $\mathcal{G}(\mathcal{Q}(r))$ derived via the Gray map is the Kerdock code $\mathcal{K}(r+1)$.*

Proof. Let $tr(x) = \sum_{i=1}^{r-1} x^{2^i}$ denote the usual binary trace mapping, and define $Q(x) = \sum_{i=1}^{s} tr(x^{1+2^i})$. One may show as in [2] that, when $r = 2s+1$, each codeword of $\mathcal{Q}(r)$ has 2-adic components

$$a(t) = tr(\eta\alpha^t) \oplus Q(\gamma\alpha^t) \oplus A \tag{20}$$

$$b(t) = tr(\gamma\alpha^t) \oplus B \tag{21}$$

$\forall (t \in I^\star)$, where α is a primitive element in the finite field $GF(2^r)$, $\alpha^\star \doteq 0$, and the elements $\eta, \gamma \in GF(2^r)$ and $A, B \in GF(2)$ are arbitrary.

From Kerdock's original construction [12], one finds that $a(t)$ and $a(t) \oplus b(t)$ are also the left and right halves of the codewords of $\mathcal{K}(r+1)$. Thus, $\mathcal{G}(\mathcal{Q}(r)) = \mathcal{K}(r+1)$ as claimed. □

In light of Theorem 5, it is natural to think of the Kerdock codes as linear quaternary codes and wonder about their quaternary duals. Let $\mathcal{P}_L$ denote the binary code that results from applying the Gray map to the quaternary code $\mathcal{Q}^\perp$, *i.e.*, $\mathcal{P}_L = \mathcal{G}(\mathcal{Q}^\perp)$. Then $\mathcal{P}_L$ is a nonlinear binary code of length $2(N+1) = 2^{r+1}$ and size $4^{2^r-(r+1)}$. From Theorems 1 and 4, we have the following corollary.

Corollary 6. *$\mathcal{P}(r)$ is a nonlinear, distance invariant, binary code whose weight distribution is related to that of the Kerdock code $\mathcal{K}(r+1)$ by the MacWilliams transform.*

Thus, $\mathcal{P}(r)$ is a nonlinear code of length $2(N+1) = 2^{r+1}$, size 4^{2^r-r-1}, and minimum Hamming distance 6. Like the extended Preparata code $\mathcal{P}(r+1)$, it is an optimal code capable of simultaneously correcting up to two-bit errors and detecting all three-bit errors. We shall refer to $\mathcal{P}_L$ as the *Preparata-like* code. As we shall see in the next section, the two codes $\mathcal{P}$ and $\mathcal{P}_L$ also share similar finite field transform descriptions.

2.5 Comparing the Preparata and Preparata-Like Codes

We define the finite field transform $\hat{\underline{a}} = (\hat{a}(\lambda) : \lambda \in I^\star)$ of the binary vector $\underline{a} = (a(t) : t \in I^\star)$ as follows:

$$\hat{a}(\lambda) = \sum_{t \in I^\star} a(t)\alpha^{\lambda t}, \qquad \forall \lambda \in I^\star \ , \tag{22}$$

where α is a fixed primitive element in $GF(2^r)$. We define the *half-convolution* of the sequence $\hat{\underline{a}}$ at lag λ by the equation

$$\mathcal{H}(\hat{\underline{a}}, \lambda) = \sum_{\substack{\lambda_1, \lambda_2 \in I \\ \lambda_1 \le \lambda_2 \\ \lambda_1 + \lambda_2 = \lambda}} \hat{a}(\lambda_1)\hat{a}(\lambda_2) \ . \tag{23}$$

The summation is a half, rather than full, convolution because we exclude the cases $\lambda_1 > \lambda_2$.

Theorem 7. *The Preparata-like code $\mathcal{P}_L$ consists of all vectors $(\underline{a} \mid \underline{a} \oplus \underline{b})$ for which $\underline{a}, \underline{b} \in (\mathbb{Z}_2)^{N+1}$ satisfy*

$$\hat{b}(0) + b(\star) = 0 \tag{24}$$

$$\hat{b}(1) = 0 \tag{25}$$

$$\hat{a}(0) + a(\star) = \hat{b}(0)b(\star) + \mathcal{H}(\hat{\underline{b}}, 0) \tag{26}$$

$$\hat{a}(1) = \mathcal{H}(\hat{\underline{b}}, 1). \tag{27}$$

The proof of this theorem requires some knowledge of Galois ring theory, and may be found in [9]. It should be emphasized that this somewhat complicated characterization of the Preparata-like code is given primarily for comparison with a similar description of the extended Preparata code. In practice, one would prefer to work in the $\mathbb{Z}_4$-domain where the code $\mathcal{P}_L$ has a more natural description. Indeed, the dual code $\mathcal{Q}^\perp$ has a parity check matrix very similar to that of the even-weight subcode of the binary extended Hamming code. This is discussed in detail in Sect. 3.

For comparison with the Preparata-like code, a transform theoretic characterization of the extended Preparata codes $\mathcal{P}(r+1)$ can be readily derived from the simple description of the codes given by Baker, Van Lint, and Wilson [1]. In particular, the vector $(\underline{a} \mid \underline{a} \oplus \underline{b})$ is in $\mathcal{P}(r+1)$ iff the binary components $\underline{a} = (a(t) : t \in I^\star)$ and $\underline{b} = (b(t) : t \in I^\star)$ have transforms satisfying

$$\hat{b}(0) + b(\star) = 0 \tag{28}$$

$$\hat{b}(1) = 0 \tag{29}$$

$$\hat{a}(0) + a(\star) = 0 \tag{30}$$

$$(\hat{a}(1))^3 = \hat{b}(3). \tag{31}$$

The similarity in descriptions of the two codes $\mathcal{P}$ and $\mathcal{P}_L$ is evident. Interestingly, in one particular case, the two codes are the same!

Theorem 8. *For $r = 3$, $\mathcal{P}(r) = \mathcal{P}(r+1)$.*

Remark. When $r = 3$, both $\mathcal{K}(4)$ and $\mathcal{P}(4)$ coincide with $\mathcal{N}_{16}$, the Nordstrom-Robinson $(16, 256, 6)$ code. The discovery of $\mathcal{N}_{16}$ was published by Nordstrom and Robinson in 1967. Preparata's analysis of the distance properties of the code and his generalization to the codes that bear his name were both published in 1968. Kerdock's generalization of $\mathcal{N}_{16}$ was published in 1972. Thus, the Nordstrom-Robinson code can be generalized in one way to get the extended Preparata codes, in another way to get the Kerdock codes, and in yet another way to get our Preparata-like codes that are dual (in the quaternary sense) to the Kerdock codes!

3 Galois Ring Theoretic Descriptions

This section has two parts. The first provides a description of the internal structure of the Galois ring, of the trace function acting on the Galois ring, and of a Fourier-like transform defined on n-tuples over the Galois ring. The second part applies this Galois ring theory to derive binary and quaternary descriptions of $\mathcal{Q}$ and $\mathcal{Q}^{\perp}$ (and thus the Kerdock and Preparata-like codes). For a more detailed mathematical development of Galois rings, the reader is referred to [14].

3.1 Galois Rings

A polynomial $f(x) \in \mathbb{Z}_4\ [x]$ is called a *basic irreducible* if its reduction modulo 2 is an irreducible polynomial $\bar{f}(x) \in \mathbb{Z}_2\ [x]$. Similarly, $f(x)$ is a *primitive* basic irreducible if $\bar{f}(x)$ is primitive. The Galois ring $GR(4,r)$ denotes a Galois extension of dimension r over the integer ring $\mathbb{Z}_4$. Every such Galois ring is isomorphic to a quotient ring $\mathbb{Z}_4\ [x]/(f(x))$, where $f(x)$ is a basic irreducible polynomial in $\mathbb{Z}_4\ [x]$. It is convenient, although not essential, to assume that $f(x)$ is a primitive basic irreducible dividing $x^N - 1$ in $\mathbb{Z}_4\ [x]$, where as usual $N = 2^r - 1$. This is analogous to preferring to construct a finite field using a polynomial that is primitive as well as irreducible. Clearly, one can extend the reduction modulo 2 mapping defined on $\mathbb{Z}_4\ [x]$ to a surjective ring homomorphism $\mu : GR(4,r) \rightarrow GF(2^r)$.

Let $R = GR(4,r)$ and $K = GF(2^r)$. The Galois ring R is a local ring whose zero divisors form the unique maximal ideal $2R$. The units of R may be expressed [14] as a direct product of groups $R^* = G_1 \times G_2$, where G_1 is a cyclic group of order N and G_2 is a direct product of r cyclic groups of order 2. Let β be a root of $f(x)$. Then, β has multiplicative order N, cyclically generates G_1, and has modulo 2 projection $\alpha = \mu(\beta)$ that is primitive in K. As a $\mathbb{Z}_4$-module, $R = < 1, \beta, \beta^2, \ldots, \beta^{r-1} >$. It is not hard to show that the Frobenius mapping $\sigma_R : \beta \rightarrow \beta^2$ generates the Galois automorphism group of R over $\mathbb{Z}_4$. For a more detailed discussion of these facts, see Sect. 3 of [2].

Let σ_K denote the corresponding Galois automorphism of K that maps α to α^2, and let $tr : K \rightarrow \mathbb{Z}_2$ denote the finite field trace mapping. Similarly, let $T : R \rightarrow \mathbb{Z}_4$ denote the Galois ring trace mapping defined by $T(\gamma) = \sum_{i=1}^{r} \sigma_R^i(\gamma)$.

3.2 Galois Ring Transforms

In analogy with finite field transform theory, we define the *Galois ring transform* $\underline{\hat{c}} = (\hat{c}(\lambda) : \lambda \in I^\star)$ of a quaternary sequence $\underline{c} = (c(t) : t \in I^\star)$ as follows:

$$\hat{c}(\lambda) = \sum_{t \in I^\star} c(t) \beta^{\lambda t} \quad , \tag{32}$$

for all $\lambda \in I^\star$, where as usual $\beta^\star = 0$.

The inversion formula

$$c(t) = -\sum_{\lambda \in I^\star} \hat{c}(\lambda)\beta^{-\lambda t} \quad . \tag{33}$$

follows in the usual way from the fact that

$$\sum_{\lambda \in I} \beta^\lambda = \frac{1-\beta^N}{1-\beta} = 0 \quad . \tag{34}$$

Let $c(t)$ have binary 2-adic components $a(t)$ and $b(t)$ satisfying $c(t) = 2a(t)+b(t)$. Since $a(t)$ and $b(t)$ are $\{0,1\}$-valued, we may talk of either their finite field transforms or their Galois ring transforms. In contexts where both are possible, we shall use $\hat{\cdot}$ for the Galois ring transform and $\tilde{\cdot}$ for the finite field transform. Note that $\hat{c}(\lambda) = 2\hat{a}(\lambda) + \hat{b}(\lambda)$.

Theorem 9. *Every sequence in $\mathcal{Q}^-$ has a unique representation as $s_\gamma(t) = T(\gamma\beta^t)$ for some element $\gamma \in R$, where $\beta \in R$ is a fixed root of the characteristic polynomial of the linear recurrence defining $\mathcal{Q}^-$ and $0 \le t \le N-1$. Conversely, every sequence of this form is a member of $\mathcal{Q}^-$.*

Proof. See [2]. □

This trace characterization leads to a simple Galois ring theoretic description of the Kerdock code.

Theorem 10. *The quaternary code $\mathcal{Q}$ consists precisely of the set of all $\mathbb{Z}_4$-valued vectors $\underline{c} = (c(t) : t \in I^\star)$ satisfying*

$$c(t) = T(\gamma\beta^t) + A \quad , \tag{35}$$

where $\gamma \in R$ and $A \in \mathbb{Z}_4$ are arbitrary parameters.

Theorem 11. *The quaternary dual code $\mathcal{Q}^\perp$ consists of all $\mathbb{Z}_4$-valued sequences $\underline{c} = (c(t) : t \in I^\star)$ whose Galois ring transform satisfies*

$$\hat{c}(0) + c(\star) = 0 \tag{36}$$

$$\hat{c}(1) = 0. \tag{37}$$

Based on Theorems 10 and 11, the codes $\mathcal{Q}$ and $\mathcal{Q}^\perp$ may be regarded as quaternary generalizations of the first-order and $(r-2)^{\text{th}}$-order Reed-Muller codes. In fact, all of the Reed-Muller codes have natural quaternary analogs (for more on this, see [9]).

4 Quaternary Decoding Algorithms

Although in the theoretical development, we have made a distinction between the quaternary codes $\mathcal{Q}$ and $\mathcal{Q}^{\perp}$ and their associated nonlinear binary codes $\mathcal{K}$ and $\mathcal{P}_L$, from a practical viewpoint, they are really two different descriptions of the same codes.

It is natural to expect that the simpler quaternary descriptions of the Kerdock and Preparata-like codes would lead to simpler decoding algorithms that work in the $\mathbb{Z}_4$-domain. This is indeed the case for the Preparata-like codes. There is an optimal syndrome decoder that provides correction of all two-bit errors and detection of all three-bit errors. In the case of the Kerdock codes, the quaternary viewpoint leads to a soft-decision decoding algorithm that is comparable in complexity, to previously known binary techniques, derived in a similar fashion from the binary descriptions of the codes.

5 Update

The discoveries about the Kerdock and Preparata codes are in a paper [7] presented by Hammons and Kumar at the IEEE International Symposium on Information Theory (San Antonio January 1993, but submitted in June 1992), in Hammons' dissertation [8], and in a manuscript submitted in early November 1992 to the *IEEE Transactions on Information Theory*, but now replaced by [9]. Hammons and Kumar also realized in June 1992 that the $\mathbb{Z}_4$ Kerdock and 'Preparata' codes could be generalized to give the quaternary Reed-Muller codes $QRM(r, m)$ described in [9].

In late October 1992, Calderbank, Sloane and Solé submitted a research announcement (now replaced by [3]) to the *Bulletin of the American Mathematical Society*, also containing the discoveries about the Kerdock and Preparata codes, as well as results concerning the existence of quaternary versions of Reed-Muller, Golay and Hamming codes. They discovered the quaternary versions of the Goethals and Delsarte-Goethals codes in early November.

The two teams (Hammons-Kumar and Calderbank-Sloane-Solé) worked independently until the middle of November 1992, when discovering the considerable overlap between their work, they decided to join forces. The common starting point for the two independent discoveries was the formula (page 1107 of [2]) providing a base-2 expansion for the four-phase sequence family, Family $\mathcal{A}$. Ref. [9] is a compositum of the results obtained by the 5 authors.

The discovery that the Nordstrom-Robinson code is a quaternary version of the octacode was made by Forney, Sloane and Trott in early October 1992 and is described in [5]. It can be shown [4] that several of the well-known binary nonlinear single-error-correcting codes also have a simpler description as codes over $\mathbb{Z}_4$ (although here, the corresponding $\mathbb{Z}_4$-codes are nonlinear). Large sequence families for code-division multiple-access (CDMA) that are supersets of the near-optimum four-phase families described above, and which are related to the Delsarte-Goethals codes are investigated in [13]. Some related constructions for lattices may be found in [19].

References

1. R. D. Baker, J. H. Van Lint, and R. M. Wilson: On the Preparata and Goethals Codes, IEEE Trans. on Inform. Theory **IT-29, 3** (May 1983), 342–345.
2. S. Boztaş, A. R. Hammons, and P. V. Kumar: 4-phase Sequences with Near Optimum Correlation Properties, IEEE Trans. on Inform. Theory, **IT-38, 3**, (May 1992), 1101–1113.
3. A. R. Calderbank, A. R. Hammons, P. V. Kumar, N. J. A. Sloane and P. Solé, A Linear Construction for Certain Kedock and Preparata Codes, Bull. Amer. Math. Soc., submitted.
4. J. H. Conway and N. J. A. Sloane, Quaternary Constructions for the Binary Codes of Julin, Best and Others, preprint.
5. G. D. Forney, Jr., N. J. A. Sloane and M. D. Trott, The Nordstrom-Robinson Code is the Binary Image of the Octacode, Proc. DIMACS/IEEE Workshop on Coding and Quantization, 1993, to appear.
6. A. R. Hammons and P. V. Kumar: A Linear Quadriphase Interpretation of the Binary Kerdock Code, Tech. Rep. **CSI-92-04-01**, (April 1992), Comm. Sciences Inst., Univ. of South. Calif., Los Angeles, CA.
7. A. R. Hammons and P. V. Kumar, On the Apparent Duality of the Kerdock and Preparata Codes, IEEE Int. Symp. on Inform. Theory, San Antonio, TX January 1993.
8. A. R. Hammons and P. V. Kumar, On four-phase sequences with low correlation and their relation to Kerdock and Preparata Codes, Ph.D. Diss., Univ. of South. Calif., Los Angeles, CA Nov. 1992.
9. 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, submitted to the IEEE Trans. on Inform. Theory.
10. T. W. Hungerford: Algebra, Grad. Texts in Math., **73**, Springer-Verlag, New York, 1974.
11. W. M. Kantor, On the Inequivalence of Generalized Preparata Codes, IEEE Trans. on Inform. Theory, **IT-29, 3**, May 1983, 345–348.
12. A. M. Kerdock, A Class of Low-Rate Nonlinear Binary Codes, Inform. and Control, **20**, 1972, 182–187.
13. P. V. Kumar, A. R. Hammons and T. Helleseth, Large Sequence families for CDMA, IEEE Trans. on Inform. Theory, to be submitted.
14. B. R. MacDonald: Finite Rings with Identity, Marcel Dekker, Inc., New York, 1974.
15. F. J. MacWilliams and N. J. A. Sloane: The Theory of Error-Correcting Codes, North-Holland Publishing Company, Amsterdam, 1977.
16. F. P. Preparata: A Class of Optimum Nonlinear Double-Error-Correcting Codes, Inform. and Control, **13**, 1968, 378–400.
17. P. Solé, A Quarternary Cyclic Code and a Family of Quadriphase Sequences with Low Correlation Properties, Lec. Notes in Comp. Science. **388**, 1989, 193–201.
18. P. Udaya and M. U. Siddiqi: Large Linear Complexity Sequences over $\mathbb{Z}_4$ for Quadriphase Modulated Communication Systems Having Good Correlation Properties, IEEE Int. Symp. on Inform. Theory, Budapest, Hungary, June 1991.
19. K. Yang, A. R. Hammons, and P. V. Kumar: Constructions for Lattices Based on 4-Phase Sequences, Technical Report **CSI-92-06-02**, (June 1992), Comm. Sciences Inst., Univ. of South. Calif., Los Angeles, CA, June 1992.

This article was processed using the LaTeX macro package with LLNCS style