The Generalized Preparata Codes Over $GF(2^l)$ *

Kuzmin A.S., Markov V.T., Nechaev A.A., Neljubin A.S.
Center of New Information Technologies
of Lomonosov Moscow State University
119992, Main building of MSU, Vorobjevy Gory, Moscow, Russia
e-mail: nechaev@cnit.msu.ru

Abstract

For any $q = 2^l > 2$ and any m such that $(m, \text{q-1}) = 1$ a nonlinear code $P_q(m)$ over the field $F = GF(q)$ with parameters $(q(\Delta+1), q^{2(\Delta-m)}, d \geq 3q)$, where $\Delta = \frac{q^m-1}{q-1}$, is constructed. If $d = 3q$ this set of parameters generalizes that of the classical binary Preparata code. The equality $d = 3q$ is established in the following cases: (1) for a series of initial admissible values q and m such that $q^m < 2^{100}$; (2) for $m = 3, 4$ and any admissible q, and (3) for admissible q and m such that there exists a number m_1 with $m_1|m$ and $d(P_q(m_1)) = 3q$. We apply the approach of [8]: the code P is a Reed–Solomon representation of a linear over the Galois ring $R = GR(q^2, 4)$ code $\mathcal{P}$ dual to a linear code $\mathcal{K}$ with parameters near to those of generalized linear Kerdock code over R.

1 Basic notions

Here we continue investigations of the paper [11]. Let $R = GR(q^2, 4)$ be a Galois ring with identity e of characteristic 4 and cardinality q^2, $q = 2^l$, $l \geq 1$. Then (see e.g. [5, 9]) the top-factor $\overline{R} = R/2R$ of the ring R is a field of q elements, the set

$$, (R) = \{r \in R\colon\ r^q = r\} = \{r \in R\colon\ r^{|\overline{R}|} = r\}$$

has cardinality q and is called the *(Teichmueller) coordinate set* of the ring R. Any element $r \in R$ is a unique sum $r = r_0 + 2r_1$, where $r_t = \gamma_t(r) \in , (R)$, $t = 0, 1$. If we define $\oplus$ on $, (R)$ by the rule $u \oplus v = \gamma_0(u + v)$ then $(, (R), \oplus, \cdot)$ is a field $GF(q)$. In the following we denote $F = , (R)$.

Let

$$F = , (R) = \{\omega_0 = 0, \omega_1 = e, \ldots, \omega_{q-1}\}$$

and $\gamma_*\colon\ R \to F^q$ be the map acting on an element $r = r_0 + 2r_1 \in R$ by the rule

$$\gamma_*(r) = (r_1, r_1 \oplus \omega_1 r_0, \ldots, r_1 \oplus \omega_{q-1} r_0). \tag{1}$$

Then $\gamma_*(R)$ is a $[q, 2, q-1]_q$ Reed–Solomon code over $F = GF(q)$ and therefore the map γ_* is called *RS-map* [8]. Note that if $q = 2$, i.e. if $R = \mathbb{Z}_4$, then γ_* is the so called Gray map from [7].

* The work was partially supported by RFFR grants 99-01-00941, 99-01-00382.

With any h-code $\mathcal{P} \subseteq R^h$ over the ring R we can associate an *RS-representation* $P = \gamma_*^h(\mathcal{P}) \subseteq F^{qh}$. It is a code of the length qh over F, consisting of all words

$$\gamma_*^h(\vec{u}) = (\gamma_*(u(0)), \dots, \gamma_*(u(h-1)), \quad \vec{u} \in \mathcal{P}. \tag{2}$$

So P is a concatenation of the code $\mathcal{P}$ over R and a linear over F code $\gamma_*(R)$. Note that if $\mathcal{P}$ is a subgroup of the group $(R^h, +)$ then P is distance invariant [2]. In this case the Hamming distance $d(P)$ of the code P equals to the minimum of Hamming weights of nonzero words of P [8, 9].

If $\mathcal{P}$ is a linear code over R i.e. $\mathcal{P} \leq {}_RR^h$ (is a submodule of the R-module ${}_RR^h$), we call P an (R, γ_*)-*linear code* (and sometimes briefly an R-*linear code*). An R-linear code P is distance invariant but may be nonlinear.

2 Main construction and results

Here we suppose that $q = 2^l, l \geq 1$. Let $S = GR(q^{2m}, 4)$ be a Galois extension of the degree m of the Galois ring $R = GR(q^2, 4)$ with Teichmueller coordinate set

$$, (S) = \{\beta \in S\colon\ \beta^{q^m} = \beta\} = \{\beta \in S\colon\ \beta^{|\overline{S}|} = \beta\}.$$

Any element $\beta \in S$ is a unique sum $\beta = \beta_0 + 2\beta_1$, where $\beta_t = \gamma_t(\beta) \in , (S)$, $t = 0, 1$. If we define a new operation $\oplus$ on $, (S)$ by the rule $u \oplus v = \gamma_0(u + v)$ then $(, (S), \oplus, \cdot)$ is a field $GF(q^m)$ and the field $F = , (R) = \{\beta \in S\colon\ \beta^q = \beta\}$ is a subfield of $Q = , (S)$.

Let us take an element $\xi \in Q^*$ of order $\operatorname{ord}\xi = \Delta = \frac{q^m-1}{q-1}$ and define $\mathcal{P}_R(m)$ as a linear code of the length $h = \Delta + 1$ over the ring R with check matrix

$$H = H_q(m) = \begin{pmatrix} e & e & e & \dots & e \\ 0 & e & \xi & \dots & \xi^{\Delta-1} \end{pmatrix}.$$

It is easy to see that this code is a free R-module of the rank $\Delta - m$. We shall call its RS-representation $P_q(m) = \gamma_*^h(\mathcal{P}_R(m))$ the *generalized Preparata code*. Note that if $q = 2$ then ξ is a primitive element of the field Q and if m is odd then $P_2(m)$ is the original binary Preparata code in the form of the paper [7] with parameters expressed as

$$(2^{m+1}, 2^{2(2^m-1-m)}, 6) = (q(\Delta+1), q^{2(\Delta-m)}, 3q).$$

If $q \geq 4$ then the following statement gives a necessary condition for the equality $d(P_q(m)) = 3q$.

Proposition 1 *If* $q \geq 4$, $(m, q-1) > 1$ *then* $d(P_q(m)) = 3(q-1)$.

Proof. The condition $(m, q-1) > 1$ is equivalent to the condition $(\Delta, q-1) > 1$ and means that $\xi^k = a \in F \setminus \{0, e\}$ for some $k \in \overline{1, \Delta-1}$. Then the elements ξ^k and e are roots of the polynomial $G(x) = x^2 - (a+e)x + e \in R[x]$ with invertible coefficients. Now it is not difficult to see that the word $\vec{v} \in R^h$ with the only 3 nonzero coordinates $e, -(a+e), e$ in the appropriate places belongs to the code $\mathcal{P}$. Thus $d(P_q(m)) \leq ||\gamma_*(\vec{v})|| = 3(q-1)$. □

One of our main results is

Theorem 2 *If $q = 2^l \geq 4$ and $(m, q-1) = 1$ then the generalized Preparata code $P_q(m)$ is a $(q(\Delta+1), q^{2(\Delta-m)}, d \geq 3q)$-code over the field $F = GF(q)$. Moreover, if $q \geq 4$ and m is even then $d(P_q(m)) \in \{3q, 4(q-1)\}$.*

Proof. Let $P = P_q(m)$. To prove the inequality $d(P) \geq 3q$ we note first that P is a distance invariant code and contains the zero word, hence $d(P)$ is equal to the minimal weight of the non zero words $\gamma_*(\vec{v}) \in P$, where $\vec{v} \in \mathcal{P}$. Let $\vec{v} \in \mathcal{P} \setminus \vec{0}$ and $s_i = s_i(v)$ $(i = 0, 1)$ be the number of coordinates of the word $\vec{v}$ that belong, respectively, to $R \setminus 2R$ and $2R \setminus 0$. Then

$$\|\gamma_*(\vec{v})\| = s_0(q-1) + s_1 q = (s_0 + s_1)q - s_0. \tag{1}$$

Note that $s_0 > 2$. Indeed, let $\overline{H}$ be the image of the matrix H under the natural homomorphism $S \to \overline{S} = GF(q^m)$, then $s_0 \neq 1$ since the matrix $\overline{H}$ does not contain zero columns, and $s_0 \neq 2$ since $s_0 = 2$ means that some column of the matrix $\overline{H}$ is equal to another one multiplied by some coefficient from $\overline{R}$ which is also impossible. Then (1) and the condition $q > 4$ imply that the desired inequality is a consequence of the following statement: if $s_0 = 3$ then $s_1 > 0$.

Suppose, on the contrary, that $s_0 = 3$, $s_1 = 0$. Then for some suitable $0 \leq a < b < c < \Delta$ and $v_a, v_b, v_c \in R^*$ we have

$$v_a\xi^a + v_b\xi^b + v_c\xi^c = 0 \quad \text{and} \quad v_a + v_b + v_c = 0. \tag{2}$$

Therefore, multiplying both sides of the first equality by $(v_a\xi^a)^{-1}$ we get

$$e + u\xi^k = (e+u)\xi^l, \quad u \in R^*, \quad 0 < k < l < \Delta. \tag{3}$$

Now we will show that this is impossible. Let $u = u_0 + 2u_1$, where $u_s = \gamma_s(u) \in , (S)$. Then

$$u_0 \neq 0 \quad \text{and} \quad u_0 \neq e \tag{4}$$

since in the latter case (3) implies $\overline{u}\overline{\xi}^k = \overline{e}$ and $\overline{\xi}^k \in \overline{R}^*$ which is invalid because $(q-1, m) = 1$ (i.e. $\langle\overline{\xi}\rangle \cap \overline{R}^* = \{\overline{e}\}$).

Let σ be the automorphism of S over R such that $\sigma(\alpha) = \alpha^2$ for any $\alpha \in , (S)$ [3, 5]). Applying σ to both sides of (3) we obtain

$$e + \sigma(u)\xi^{2k} = (e + \sigma(u))\xi^{2l}. \tag{5}$$

Denote $\xi^k = \alpha$ and $\xi^l = \beta$. The one can rewrite (5) as

$$e + (u_0^2 + 2u_1^2)\alpha^2 = (e + (u_0^2 + 2u_1^2))\beta^2. \tag{6}$$

Taking squares of both sides of (3) we obtain

$$e + 2u_0\alpha + u_0^2\alpha^2 = (e + 2u_0 + u_0^2))\beta^2. \tag{7}$$

Subtracting (6) from (7) we arrive to an equality

$$2(u_0^2\alpha + u_1^2\alpha^2) = 2(u_0 + u_1^2)\beta^2, \tag{8}$$

which is equivalent to the following relation in the field $(, (S), \oplus, \cdot)$:

$$u_0\alpha \oplus u_1^2\alpha^2 = (u_0 \oplus u_1^2)\beta^2. \tag{9}$$

Note now that reducing (3) modulo 2 we get the following:

$$e \oplus u_0\alpha = (e \oplus u_0)\beta$$

and $e \oplus u_0 \neq 0$ in view of (refcondu0). Thus

$$\beta = (e \oplus u_0\alpha)(e \oplus u_0)^{-1}.$$

Then from (9) we deduce

$$(u_0\alpha \oplus u_1^2\alpha^2) = (u_0 \oplus u_1^2)(e \oplus u_0^2\alpha^2)(e \oplus u_0^2)^{-1}.$$

It follows that α is a root of the polynomial

$$(u_0^3 \oplus u_1^2)x^2 \oplus (u_0^3 \oplus u_0)x \oplus (u_0 \oplus u_1^2) \in , (R)[x].$$

It is evident that this polynomial has a root $x = e$, so the its other root α must also belong to , (R), a contradiction.

In order to prove the last statement of the Theorem note that if m is even then the element $\alpha = \xi^k$, where $k = \frac{q^m-1}{q^2-1}$ has the order $q+1$ and is a root of the polynomial $F(x) = (x-\alpha)(x-\alpha^q) = x^2+ax+e \in R[x]$, where $\overline{a} = \overline{\xi}^q + \overline{\xi} \notin \{\overline{0}, \overline{e}\}$ since $q > 2$. Therefore elements α and e are roots of the polynomial $G(x) = (x-e)F(x) = x^3+g_2x^2+g_1x-e \in R[x]$, where $g_1, g_2 \in R^*$. Now it is easy to see that the word $\vec{v} \in R^h$ with only 4 nonzero coordinates $-e, g_1, g_2, e$ in the appropriate places belongs to the code $\mathcal{P}$. Thus $d(P_q(m)) \leq ||\gamma_*(\vec{v})|| = 4(q-1)$. It is enough now to note that according to (1) for any $\vec{v} \in R^h$ the condition $3q \leq ||\gamma_*(\vec{v})|| \leq 4(q-1)$ implies $||\gamma_*(\vec{v})|| \in \{3q, 4(q-1)\}$. □

For the first three initial values of m we can prove the following "exactness property" of the Theorem 2.

Proposition 3 *$d(P_q(2)) = 4(q-1)$ for arbitrary $q = 2^l$.*

Note, by the way, that $d(P_q(2)) = 4(q-1) = 3q$ for $q = 4$ and $d(P_q(2)) > 3q$ in other cases.

Proposition 4 *$d(P_q(m)) = 3q$ for $m = 3, 4$ and any $q = 2^l$ such that $(q-1, m) = 1$.*

Sketch of the proof of Propositions 3, 4. In view of the Theorem 2 in order to prove Proposition 4 (Proposition 3) it is enough to show that the code $\mathcal{P}_R(m)$ (resp. the code $\mathcal{P}_R(2)$) contains (resp. does not contain) a word of the Hamming weight 3 with coordinates in $2R$. The code $\mathcal{P}_R(m)$ contains such a word if and only if there is a linear dependence over the field F between some three columns of the check matrix H defined above and being considered as a matrix over the field F, or, equivalently, that there exist two numbers $k, l \in \overline{1, \Delta-1}$ and an element $\alpha \in P \setminus \{0, 1\}$ such that

$$e + \alpha\xi^k = (e+\alpha)\xi^l. \tag{10}$$

(in this Proof we use for brevity the notation + instead of $\oplus$ for the addition in F.) One can eliminate l by taking Δ-th power of the both sides:

$$(e + \alpha\xi^k)^\Delta = (e+\alpha)^\Delta = (e+\alpha)^m. \tag{11}$$

The left part of (11) has the following expression:

$$\begin{aligned}(e+\alpha\xi^k)^\Delta &= (e+\alpha\xi^k)(e+\alpha\xi^{kq})\dots(e+\alpha\xi^{kq^{k-1}}) = \\ &\alpha^m(\alpha^{-1}+\xi^k)(\alpha^{-1}+(\xi^k)^q)\dots(\alpha^{-1}+(\xi^k)^{q^{k-1}}).\end{aligned} \tag{12}$$

Let $\beta=\alpha^{-1}$ and

$$f_k(x)=\prod_{i=0}^{m-1}(x-(\xi^k)^{q^i}=x^m+f_{m-1}^{(k)}x^{m-1}+\ldots+f_1^{(k)}x+f_0^{(k)}. \tag{13}$$

Thus $f_k(x)$ is a power of the minimal polynomial of the element ξ^k, hence $f_k(x)\in F[x]$ and $f_0^{(k)}=e$. Rewriting (12) we obtain

$$(e+\alpha\xi^k)^\Delta=\alpha^m f_k(\beta)=e+f_{m-1}^{(k)}\alpha+\ldots+f_1^{(k)}\alpha^{m-1}+\alpha^m. \tag{14}$$

Equations (11) and (14) imply that solvability of (10) is equivalent to the equality

$$e+f_{m-1}^{(k)}\alpha+\ldots+f_1^{(k)}\alpha^{m-1}+\alpha^m=\sum_{i=0}^{m}\left(\begin{array}{c}m\\ i\end{array}\right)\alpha^i, \tag{15}$$

i.e. to the equality

$$\sum_{i=1}^{m-1}\left(f_{m-i}^{(k)}+\left(\begin{array}{c}m\\ i\end{array}\right)\right)\alpha^{i-1}=0 \tag{16}$$

for some $\alpha\in F\setminus\{0,e\}$ and $k\in\overline{1,\Delta-1}$. Consider the polynomial

$$h_k(x)=\left(f_{m-1}^{(k)}+m\right)+\left(f_{m-2}^{(k)}+\left(\begin{array}{c}m\\ 2\end{array}\right)\right)x+\ldots+\left(f_1^{(k)}+\left(\begin{array}{c}m\\ m-1\end{array}\right)\right)x^{m-2}. \tag{17}$$

It follows that solvability of (10) is equivalent to existence of such element ξ^k that the polynomial $h_k(x)$ has a root α in $F\setminus 0$.

If $m=2$ then $h_k(x)=f_{m-1}^{(k)}=f_1^{(k)}\neq 0$ has no roots in F. So Proposition 3 is proved.

Consider the case $m=3$. Now we have

$$h_k(x)=(f_2^{(k)}+e)+(f_1^{(k)}+e)x,$$

and it is sufficient to prove that there exists an element $\theta=\xi^k$ such that

$$f_1^{(k)}\neq e \quad\text{and}\quad f_2^{(k)}\neq e. \tag{18}$$

If $f_1^{(k)}=e$ then $f_k(x)=x^3+f_2^{(k)}x^2+x+1$ is irreducible, so the number of such polynomials is not greater than $q-1$ (the polynomial $x^3+x^2+x+e=(e+x)^3$ does not belong to this family), so these polynomials can not have more than $3(q-1)$ roots in the group $\Xi=\langle\xi\rangle$. An analogous argument shows that the number of roots of irreducible polynomials of the form $f_k(x)=x^3+x^2+f_1^{(k)}x+1$ in Ξ is also not greater than $3(q-1)$. Thus there are not more than $6(q-1)$ elements $\theta=\xi^k\in\Xi$ such that the condition (18) is not satisfied. Note finally that

$$|\Xi|-6(q-1)=q^2+q+1-6q+6=q^2-4q+4-(q-3)=(q-2)^2-(q-3)>0$$

for any $q \geq 4$. Hence there are elements in Ξ such that the condition (18) is fulfilled.

Case $m = 4$ can be settled with similar but more elaborate arguments. In this case we have

$$h_k(x) = f_3^{(k)} + f_2^{(k)} x + f_1^{(k)} x^{m-2},$$

and it is sufficient to prove that there exists an element $\theta = \xi^k$ such that

$$f_1^{(k)} = 0, \quad f_2^{(k)} \neq 0, \quad f_3^{(k)} \neq 0.$$

This fact is proved using the properties of quadrics over a field of characteristic 2. □

By computation we have also the following

Proposition 5 *The equality $d(P_q(m)) = 3q$ is true for all values of $q = 2^l \geq 4$ and m such that $q^m < 2^{100}$ and $(q-1, m) = 1$.*

These results allow us to "enlarge" the infinite set of generalized Preparata codes with $d(P_q(m)) = 3q$, using the following properties of the function $d(P_q(m))$.

Proposition 6 *Under the conditions of Theorem 2 if $m_1 | m$ then $d(P_q(m)) \leq d(P_q(m_1))$. In particular if $(q-1, m) = 1$, $m_1 | m$ and $d(P_q(m_1)) = 3q$, then $d(P_q(m)) = 3q$.*

Proof. It is enough to note that any column of the matrix $H_q(m_1)$ can be considered as a column of the matrix $H_q(m)$. □

The similar reasons give

Proposition 7 *Under the conditions of Theorem 2 if $k \in \mathbb{N}$, $(q^k - 1, m) = 1$ and*

$$\frac{q^m - 1}{q - 1} \mid \frac{q^{km} - 1}{q^k - 1}$$

then

$$d(P_q(m)) = 3q \Rightarrow d(P_{q^k}(m)) = 3q^k.$$

Proposition 8 *For a prime m the condition $\dfrac{q^m - 1}{q - 1} \mid \dfrac{q^{km} - 1}{q^k - 1}$ is equivalent to $(m, k) = 1$.*

These results allow us to formulate the following

Conjecture. *The equalities $d(P_q(2)) = 4(q-1)$, $d(P_q(m)) = 3q$ hold for any $q = 2^l$, $m > 2$ and*

$$\begin{cases} m \text{ is odd} & \text{if } q = 2, \\ (m, q-1) = 1 & \text{if } q > 2. \end{cases}$$

Note that in order to prove this Conjecture it is sufficient, in according to Propositions 4, 6, to prove it only for prime values of m. For example, using the Proposition 5, we can state that for $q = 4$ the minimal value of m in question is $m = 53$.

3 A code linearly dual to the Preparata code

Let $\mathcal{K}^o$ be the code dual to a linear code $\mathcal{K} \leq {}_RR^h$ relative to the standard scalar product. Then again $\mathcal{K}^o \leq {}_RR^h$ and we shall call the R-linear code

$$K_\perp = \gamma_*^h(\mathcal{K}^o) \subseteq F^{qh}$$

(linearly) R-dual to the (R-linear) code K.

In [4, 5] $\mathbb{Z}_4$-linearity of the classical binary Kerdock $(2^{m+1}, 2^{2(m+1)}, 2^m - 2^\lambda)$-code, where m is odd and $\lambda = [m/2]$ (see [1]), was discovered. Further in [7] it was noted that the classical binary Preparata code with parameters

$$(2^{m+1}, 2^{2(2^m-1-m)}, 6)$$

is $\mathbb{Z}_4$-dual to the binary Kerdock code. Simultaneously in [6] a generalized Kerdock code $K_q(m)$ over any Galois field $F = GF(q)$, $q = 2^l$, $l > 1$ with parameters

$$(n, n^2, ((q-1)/q)(n - \sqrt{n})),\ n = q^{m+1}, m \text{ is odd}$$

was constructed. This code has the form $K_q(m) = \gamma_*^h(\mathcal{K}_R(m))$, where $\mathcal{K}_R(m) \leq {}_RR^h$ is a special linear code of the length $h = q^m$, called the *basic linear code* (see below).

However the attempts to build a generalized Preparata code by analogy with [7] as a code R-dual to $K_q(m)$ were unsuccessful: for $q > 2$ the code $K_q(m)_\perp = \gamma_*^h(\mathcal{K}_R(m)^o)$ has the distance $3(q-1)$ (see [8] and [10] for $R = \mathbb{Z}_{q^2}, q$ — prime, odd). So the distance formula of such "generalization" of Preparata code is not a generalization of the distance of original binary Preparata code: for $q = 2$ we have 3 instead of $6 = 3q$. Nevertheless, this very construction was called in [10] the generalization of Preparata code. We have proposed above some alternative approach to the definition of this notion. Now we compare the parameters of the code R-dual to $P_q(m)$ with those of the generalized Kerdock code.

The code $\mathcal{P}_R(m)^0$ dual to the initial linear code $\mathcal{P}_R(m)$ consists of all words $\vec{v} = (v(0) \dots v(h-1))$ of the length $h = \Delta + 1$ such that for some $\alpha \in S$, $c \in R$

$$v(i) = Tr_R^S(\alpha\xi^i) + c, \quad i = \overline{0, h-2}, \quad v(h-1) = c, \tag{19}$$

where $Tr_R^S(x)$ is the *trace-function* from S onto R, $Tr_R^S(x) = \sum_\sigma \sigma(x)$, σ spans the group of automorphisms of S over R). We shall denote it by $\mathcal{K}_R[\xi]$.

Note that if we substitute in (19) the primitive element ξ of the field Q instead of the element ξ of order Δ and take $h = q^m$, then we obtain the *basic linear code* for the generalized Kerdock code: $\mathcal{K}_R[\xi] = \mathcal{K}_R(m)$.

In the considered case we shall call $\mathcal{K}_R[\xi]$ the *reduced basic code* and denote it by $\mathcal{K}_R^{red}(m)$. Correspondingly we shall call the code $K_q^{red}(m) = \gamma_*^h(\mathcal{K}_R^{red}(m))$ the *reduced (generalized) Kerdock code*.

Proposition 9 *If n is the length and C the cardinality of the reduced Kerdock code $K_q^{red}(m)$ then*

$$n = q(\Delta + 1) = \frac{q}{q-1}(q^m + q - 2), \quad C = q^{2(m+1)} = ((q-1)n - q^2 + 2q)^2.$$

If $q = 4, (m, q-1) = 1$, then the distance d of this code satisfies the inequalities

$$4^m - 4^{[\frac{m}{2}]} \geq d \geq 4^m - \frac{17}{3} \cdot 4^{\frac{m}{2}} + 2$$

In comparison with the parameters $(n, n^2, \frac{q-1}{q}(n-\sqrt{n})$ of the generalized Kerdock code over F the cardinality C of our code is greater: $C \simeq (q-1)^2 n^2$, but the distance is less. The last inequalities allow to state that for $q = 4$ there is the equality

$$d = \frac{q-1}{q}(n - c(m)\sqrt{n}), \quad \text{where } 6.54 \geq c(m) \geq 0.577 \cdot 2^{m-2\lambda}, \ \ \lambda = [m/2].$$

Apparently the last estimations are rather rough.

First of all note that in addition to the well known fact that

$$P_2(3) = K_2(3) = K_2^{red}(3)$$

is a $(16, 2^8, 6)_2$-code, we have now that

$$P_4(2) = K_4^{red}(2)$$

is a $(24, 4^6, 12)_4$-code. In particular $c(2) \approx 1.77$.

The following results of calculations for $q = 4$ allow to conjecture that for $m > 4$ really $3 \geq c(m) \geq 2$.

m	n	$4^m - 4^\lambda$	d	$4^m - \frac{17}{3}2^m + 2$	$c(m) = \frac{n - \frac{q-1}{q}d}{\sqrt{n}}$
2	24	12	12	-4	1.77
4	344	240	238	167	1.44
5	1368	1008	962	845	2.31
7	21848	16320	16146	15661	2.17
8	87384	65280	65048	64087	2.21

For the indicated values of m the Hamming weight enumerators of the code $K_4^{red}(m)$ were calculated. The possible values of weights of the codewords are the following.

For $m = 2$:

$$4^m + i \cdot 2^\lambda + 2, \ i \in \{-3, -1, 0, 1\},$$
$$d = 12 = 4^m - 3 \cdot 2^\lambda + 2.$$

For $m = 4$:

$$4^m + i \cdot 2^\lambda + 2, \ i \in \overline{-5, 5};$$
$$4^m + i \cdot 2^{\lambda+1}, \ i \in \overline{-2, 3};$$
$$d = 238 = 4^m - 5 \cdot 2^\lambda + 2.$$

For $m = 5$:

$$4^m + i \cdot 2^{\lambda+1} + 2,\ i \in \{-8, \overline{-5, 5}\};$$

$$4^m + i \cdot 2^{\lambda+1},\ i \in \{-5, \overline{-3, -1}, \overline{1, 3}, 5\};$$

$$d = 962 = 4^5 - 8 \cdot 2^3 + 2.$$

For $m = 7$:

$$4^m + i \cdot 2^{\lambda} + 2,\ i \in \{-30, -26, -22, -21, \overline{-19, 21}, 23, 25, 29\};$$

$$4^m + i \cdot 2^{\lambda+1} + 8,\ i \in \{\overline{-13, 9}, 11\};$$

$$4^m + i \cdot 4^{\lambda},\ i \in \{-1, 1\};$$

$$d = 16146 = 4^m - 4 \cdot 4^{\lambda} + 18.$$

For $m = 8$:

$$4^m + i \cdot 2^{\lambda+1} + 2,\ i \in \overline{-14, 13};$$

$$4^m + i \cdot 2^{\lambda+1} - 8,\ i \in \{-15, \overline{-12, 12}, 14, 17\};$$

$$4^m + i \cdot 4^{\lambda},\ i \in \overline{-1, 1};$$

$$d = 65048 = 4^m - 2 \cdot 4^{\lambda} + 24.$$

Thus if the Conjecture formulated in the previous section is true then we can say that $\mathbb{Z}_4$-duality of binary Kerdock and Preparata codes is in some sense casual result. In fact the code R-dual to the generalized (in our sense) Preparata code over $GF(2^l)$ is the reduced Kerdock code $K_q^{red}(m)$ which is equal to the generalized Kerdock code $K_q(m)$ only if $q = 2$.

The authors are grateful to Professor A. V. Mikhalev for helpful discussions of the text of this paper.

References

[1] Kerdock A. M. A class of low-rate non-linear codes. *Inform. Control*, **20** (1972), 182–187.

[2] MacWilliams F. J., Sloane N. J. A. The Theory of Error-Correcting Codes, North-Holland Publ. Co., 1977.

[3] Nechaev A. A. Finite principal ideal rings. *Mat. Sb. (N.S.)* , 91 (1973), No 3, 350-366. (English translation in *Math. of the USSR. Sbornik*).

[4] Nechaev A. A. Trace function in Galois ring and noise stable codes (in Russian), *V All-Union Symp. on theory of rings, algebras and modules*, Novosibirsk, p. 97, 1982.

[5] Nechaev A. A. Kerdock code in a cyclic form (in Russian). *Diskr. Math. (USSR)*, 1 (1989), No 4, 123–139. English translation: *Discrete Math. and Appl.*, 1 (1991), No 4, 365–384 (VSP).

[6] Kuzmin A. S., Nechaev A. A. Linearly presented codes and Kerdock code over an arbitrary Galois field of the characteristic 2. *Russian Math. Surveys*, **49** (1994), No 5.

[7] Hammons A. R., Kumar P. V., Calderbank A. R., Sloane N. J. A., Solé P. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inf. Theory*, vol. 40, No 2, pp. 301–319, 1994.

[8] Nechaev A. A., Kuzmin A. S. Linearly presentable codes, *Proceedings of the 1996 IEEE Int. Symp. Inf. Theory and Appl.*, Victoria B. C., Canada, 1996, pp. 31–34.

[9] Nechaev A. A., Kuzmin A. S. Trace-function on a Galois ring in coding theory. *Lecture Notes in Computer Science*, **1255**. Springer, 1997, 277–290.

[10] Bram van Asch, Henk C. A. van Tilborg. Some observations about linear $\mathbb{Z}_{p^2}$ codes. *Third Euro Workshop on Optimal Codes and Related Topics*. 10-17 June, 2001, Sunny Beach, Bulgaria, 5–12.

[11] Nechaev A. A., Neljubin A. S., The codes of type Preparata over $GF(4)$. Proc. of VIII Intern. workshop "Algebraic and Combinatorial Coding Theory" (ACCT-VIII), Tzarskoe Selo, Sept. 2002, 208-211.