On components of a Kerdock code and the dual of the primitive double-error-correcting BCH code [⋆]

I. Yu. Mogilnykh and F. I. Solov'eva

Sobolev Institute of Mathematics, Russian Academy of Sciences and Novosibirsk
State University, Novosibirsk, Russia
`ivmog@math.nsc.ru, sol@math.nsc.ru`

Abstract. The structure of i-components of Kerdock codes and the duals of the linear codes with distance 5 of length $n = 2^m - 1$, for odd m related to AB-functions is investigated. It is proved that for any admissible length a punctured Kerdock code consists of two i-components and the dual of any linear uniformly packed code with parameters of primitive double-error-correcting BCH code is an i-component for any i. An alternative proof for the fact presented by De Caen and van Dam in 1999 that the restriction of the Hamming scheme to a doubly shortened Kerdock code is an association scheme is given.

Keywords Kerdock code, BCH code, uniformly packed code, AB function, association scheme, i-component

1 Introduction

In this paper we show that a punctured Kerdock code has two i-components for any coordinate position i, while the dual of a linear uniformly packed code with parameters of primitive double-error-correcting BCH code B is an i-component for any coordinate position i.

By $\mathbb{F}^n$ we denote the vector space of dimension n over the Galois field $GF(2)$. The main definitions and notions can be found in [2]. The *kernel* $Ker(C)$ of a code C is $\{x : x + C = C, x \in \mathbb{F}^n\}$. From the definition it is clear that the code C is a union of cosets of $Ker(C)$. The code obtained from a code C by deleting one coordinate position is called the *punctured code* and is denoted by C^*, the code doubly punctured is denoted by C^{**}. The *shortened code* of C is obtained by selecting the subcode of C having zeros at a fixed position and deleting this position. Such code is denoted by C'. Doubly shortened code is denoted by C''. For a code C denote by $I(C)$ the set of distances between its codewords: $I(C) = \{d(x, y) : x, y \in C\}$ and by C_i denote the set of its codewords of weight i: $C_i = \{x \in C : w(x) = i\}$.

[⋆] This work was funded by the Russian Science Foundation under grant 18-11-00136.

Given a code C with minimum distance d consider the graph $G_i(C)$ with the set of codewords as the set of vertices and the set of edges $\{(x, y) : d(x, y) = d, x_i \neq y_i\}$. A connected component of the graph $G_i(C)$ is called an *i-component* of the code. If the minimum distance is greater than 2 then changing the values in the ith coordinate position in all vectors of any i-component by the opposite one in the code leads to a code with the same parameters: length, size and code distance. Therefore, we can obtain an exponential number (as a function of the number of i-components in the code) of different codes with the same parameters. Such approach was earlier successfully developed for the class of perfect codes. The method of i-components allowed to construct a large class of pairwise nonequivalent perfect codes and was used to study various code properties, see the survey [11].

Punctured Preparata codes, perfect codes with code distance 3 and the primitive cyclic BCH code with designed distance 5 of length $2^m - 1$, odd m are known to be uniformly packed [13], [7]. Therefore, the fixed weight codewords of the extensions of these codes form 3-designs, which was proved by Semakov, Zinov'ev and Zaitsev in [13]. An analogous property holds for the duals of these codes. Let $C^\perp$ be a formally dual code to a code C with code distance d, i.e. their weight distributions are related by McWilliams identities [2]. By Theorem 9, Ch. 9, [2] the set of codewords of any fixed weight in $C^\perp$ is $(d - \bar{s})$-design, where $\bar{s}$ denotes the number of different nontrivial (not equal to 0 and n) weights of the codewords of $C^\perp$. It is well-known that a Kerdock code and a Preparata code of the same length are formally dual. Therefore, the fixed weight codewords of a Kerdock code are 3-designs and the fixed weight codewords of the code orthogonal to primitive double-error-correcting BCH code of length $2^m - 1$, m-odd are 2-designs.

The aforementioned codes are related to association schemes. Let X be a set, and there are $n + 1$ relations R_i, $i \in I$ that partition $X \times X$. The pair $(X, \{R_i\}_{i \in I})$ is called an *association scheme*, if there are numbers $\delta^k_{i,j}(X)$, such that

- The relation $\{(x, x) : x \in X\}$ is R_j for some $j \in I$.
- For any i, the relation $R_i^{-1} = \{(y, x) : (x, y) \in R_i\}$ is R_j for some $j \in I$.
- For any $i, j, k \in I$ and x, y in X, $(x, y) \in R_i$ the following holds:

$$\delta^k_{i,j}(X) = |\{z : z \in X, (x, z) \in R_j, (y, z) \in R_k\}|.$$

The numbers $\delta^k_{i,j}(X)$, $i, j, k \in I$ are called the *intersection numbers* of the association scheme.

Let C be a binary code. Consider the partition of the cartesian square $C \times C$ into distance relations, i.e. two pairs of codewords are in the same relation if and only if the Hamming distances between the pairs coincide. Such partition is called *the restriction* of the Hamming scheme to the code C, see [9]. There are several cases where the restriction gives an association scheme. In this case, the code with this property is called distance-regular, see [12]. The duals of linear completely regular codes are known to be distance-regular (Theorem 6.10, [9]). In particular, the dual of the primitive double-error-correcting BCH code of length $n = 2^m - 1$ produces an association scheme in case of odd m. Using linear programming bound, Delsarte in [9] showed that the restriction of the Hamming scheme to a shortened Kerdock code is an association scheme. An analogous fact for Kerdock codes was proved in [12] by finding the intersection numbers of the restricted scheme directly. In work [14], see also [15], it is shown that the restriction of the Hamming scheme to a doubly shortened Kerdock code is also an association scheme. The latter fact contributes to a significant part of the current paper concerning components of a Kerdock code, however we give an alternative combinatorial proof for this fact as we essentially need a convenient approach to calculating the intersection numbers of the scheme.

2 Components of Kerdock code

In the section we fix n to be 2^m, for even m, $m \geq 4$. Denote by $\mathbf{0}^n$ and $\mathbf{1}^n$ the all-zero and all-one vectors in $\mathbb{F}^n$ respectively. A *Kerdock code* K is a binary code of length n and minimum distance $d = (n - \sqrt{n})/2$, consisting of the first order Reed–Muller code RM$(1, m)$ and $2^{m-1} - 1$ its cosets such that the weights of the codewords in any coset are d or $n - d$. These codes were firstly constructed in [5] and further generalizations were obtained in [6], [10].

The weight distribution of a Kerdock code is well-known and is related with the weight distribution of a Preparata code via McWilliams identities [2].

i	The number of codewords of weight i
0	1
d	$n(n-2)/2$
$\frac{n}{2}$	$2n-2$
n-d	$n(n-2)/2$
n	1

In order to prove that a punctured Kerdock code consists of two i-components we use the following properties of the code, that come from its definition. Without loss of generality, the all-zero vector $\mathbf{0}^n$ is in a Kerdock code.

(K1) Any code K is a union of $n/2$ cosets of RM$(1, m)$.

(K2) It is true that $K_{n/2} \bigcup \{\mathbf{0}^n, \mathbf{1}^n\} =$ RM$(1, m)$.

(K3) The distance between codewords from different cosets of RM$(1, m)$ in the code K is either d or $n - d$.

(K4) Nonzero distances between codewords in any coset are either $n/2$ or n.

(K5) RM$(1, m) \subseteq Ker(K)$.

The property below follows from (K2)–(K5):

(K6) If for $x, y \in K$ we have $w(x + y) = n/2$ then $x + y \in K$.

Theorem 1. *[2][Theorem 9, Ch. 9] Let C be a code of length n and minimum distance d, $C^{\perp}$ be a code which is formally dual to C, $\bar{s} = |I(C^{\perp}) \setminus \{0, n\}|$. Then the set of codewords of any fixed nonzero weight in $C^{\perp}$ is $(d - \bar{s})$-design.*

Theorem 1 applied to Preparata and Kerdock codes implies the following:
(K7) (See [2]) K_d, $K_{n/2}$, K_{n-d} are 3-designs.

In order to proceed further we need the following lemma.

Lemma 1. *Let x be a vector of weight i, D be $1-(n,j,\lambda_1)$-design. Let the distances between x and vectors of D take values $k_1,\dots,k_s$ with multiplicities $\delta^{k_1},\dots,\delta^{k_s}$ respectively. Then the following formula holds:*

$$\sum_{l=1}^{s}\delta^{k_l}\cdot\frac{i+j-k_l}{2}=i\lambda_1 \tag{1}$$

and $\delta^{k_1},\delta^{k_2}$ are uniquely defined by $\delta^{k_3},\dots,\delta^{k_s}$.

Note that $I(K'')=\{0,d,n/2,n-d\}$, as we exclude the all-one vector in K'. By $\delta^k_{i,j}(x)$ we denote the number of codewords of weight j in K'' at distance k from a codeword x in K'' of weight i. Obviously, the restriction of the Hamming scheme to K'' is an association scheme if $\delta^k_{i,j}(x)$ for all $i,j,k\in I(K'')$ are shown to be independent on the choice of a codeword x of weight i regardless of translation of K'' by any of its codeword.

Lemma 2. *The number $\delta^k_{i,j}(x)$ does not depend on the choice of a codeword x in K''_i if i or j equals to $n/2$.*

Lemma 3. *Let $n/2\in\{i,j,k\}$. Then the number $\delta^k_{i,j}(x)$ does not depend on the choice of a codeword x of weight i.*

Lemma 4. *The number $\delta^k_{i,j}(x)$ does not depend on the choice of a codeword x of weight i for $i,j,k\in I(K'')$.*

Theorem 2. *The restriction of the Hamming scheme to a doubly shortened Kerdock code K'' is an association scheme.*

Proof. The proof follows from properties (K1)–(K7) of a Kerdock code K and lemmas 2–4.

In order to find components of the punctured Kerdock code, we need one more simple lemma.

Lemma 5. *Let C be a code of length n' such that the restriction of the Hamming scheme to its codewords is an association scheme. Let $I(C)$ be such that $I(C)\cap\{n'-i : i\in I(C)\}=\varnothing$. Then the restriction of the Hamming scheme to the code $\overline{C}=C\bigcup(\mathbf{1}^{n'}+C)$ is an association scheme.*

Proof. We have the following equalities:

$$\delta^k_{i',j}(\overline{C})=\delta^k_{i,j'}(\overline{C})=\delta^{k'}_{i,j}(\overline{C})=\delta^{k'}_{i',j'}(\overline{C})=0.$$

$$\delta^k_{i',j'}(\overline{C})=\delta^{k'}_{i',j}(\overline{C})=\delta^{k'}_{i,j'}(\overline{C})=\delta^k_{i,j}(\overline{C})=\delta^k_{i,j}(C). \tag{2}$$

Theorem 3. *Let K^* be a punctured Kerdock code, $i \in \{1, \dots, n-1\}$. The code K^* consists of two i-components and codewords are in the same component if their puncturings in ith position have weights of the same parity.*

Proof. Consider any two different coordinates i, j of a Kerdock code of length n. Denote by K^* the punctured code obtained from the code K by deleting ith coordinate position. The code doubly punctured in ith and jth positions is denoted by K^{**}. Doubly shortened code in ith and jth positions is denoted by C''. Proving that there are just two i-components in K^* is equivalent to showing that the minimum distance graph of the doubly punctured Kerdock code K^{**} has two connected components (which are actually even and odd weight codewords). Recall [1] that the minimum distance graph of a code is the graph with vertex set being codewords and the edgeset being pairs of codewords at code distance. We show the connectedness of the minimum distance graph of the even weight subcode of K^{**} (the latter coincides with $\overline{K''}$). The codewords of the subcodes have weights from $\{0, d-2, d, n/2-2, n/2, n-d-2, n-d, n-2\}$. The proof significatively relies on the fact that the restriction of the Hamming scheme to $\overline{K''}$ is an association scheme which follows from Theorem 2 and Lemma 5. By Lemma 1 we see that certain intersection numbers of the restriction of the Hamming scheme to $\overline{K''}$ are nonzeros.

Lemma 6. *The following equalities hold:*

$$\delta^{d-2}_{d-2,n/2}(\overline{K''}) = \frac{n^2 - 6n - 2nd + 8d}{4(n-2d)}. \tag{3}$$

$$\delta^{n-d-2}_{d-2,n/2}(\overline{K''}) = \frac{n^2 - 2nd + 2n}{4(n-2d)}. \tag{4}$$

From the values given by (3) and (4) we see that $\delta^{d-2}_{d-2,n/2}(\overline{K''})$ and $\delta^{n-d-2}_{d-2,n/2}(\overline{K''})$ are nonzeros, which is equivalent to

$$\delta^{d-2}_{d-2,n/2}(\overline{K''}) \neq 0, \ \delta^{d-2}_{n/2,n-d-2}(\overline{K''}) \neq 0. \tag{5}$$

Consider the codewords of $\overline{K''}_{d-2}$. Obviously, the codewords cannot be at distance $n/2$ pairwise apart, which follows, for example, from the Plotkin's bound. Therefore there are codewords of weight $d-2$ at distance d apart and $\delta^{d}_{d-2,d-2}(\overline{K''}) \neq 0$, which is equivalent to

$$\delta^{d-2}_{d-2,d}(\overline{K''}) \neq 0. \tag{6}$$

From (5) we see that any codeword of $\overline{K''}_{n/2}$ is at distance $d-2$ from at least one codeword of K_{d-2} and a codeword of $\overline{K''}_{n-d-2}$ is at distance $d-2$ from at least one codeword of $\overline{K''}_{n/2}$. Therefore, $\overline{K''}_{d-2}$, $\overline{K''}_{n/2}$, $\overline{K''}_{n-d-2}$ are in one connected component of the minimum distance graph of $\overline{K''}$. Taking into account the equality (2) this fact is equivalent to the fact that the codewords of $\overline{K''}_{n-d}$, $\overline{K''}_{n/2-2}$ and $\overline{K''}_{d}$ belong to the same component. Finally, the inequality

(6) implies that $\overline{K''}_{d-2}$ and $\overline{K''}_d$ are in the same component, which implies that the codewords of weights $\{0, d-2, d, n/2-2, n/2, n-d-2, n-d, n-2\}$ are in the same connected component, which is exactly the minimum distance graph of $\overline{K''}$.

Remark 1. Theorems 2 and 3 are true for some other Kerdock-related codes. In particular, by considerations similar to those in proof of Theorem 2 one can show that a Kerdock and a shortened Kerdock codes produce association schemes, which gives an alternative (combinatorial) proof for these well-known facts from [9] and [12]. Analogously to the proof of Theorem 3, one can prove that the i-components of a Kerdock code coincide with the Kerdock code or equivalently, the minimum distance graph of a punctured Kerdock code is connected.

Remark 2. According to Theorem 3, new Kerdock codes cannot be constructed by means of traditional switchings. For convenience we set $i = n-1$. By the proof of Theorem 3 we know that two codewords are in the same $(n-1)$-component of the Kerdock code punctured in the nth position if and only if their puncturings in the $(n-1)$th coordinate position have weights of the same parity. Therefore, the codewords of the Kerdock code K could be represented as K^{00}, K^{11}, K^{01}, K^{10}, where $K^{ab} = \{x \in K : x_{n-1} = a, x_n = b\}$, with $K^{00} \cup K^{11}$ corresponding to one $(n-1)$-component of K_n^* and $K^{01} \cup K^{10}$ to the other one. Moreover, the "odd weight" component is the translation of the "even weight" one, i.e. there is a codeword $(x'01)$ of $RM(1, m)$ such that $(K^{01} \cup K^{10}) + (x'01) = K^{00} \cup K^{11}$. Now the switching $K = K^{00} \cup K^{11} \cup ((x'01) + (K^{00} \cup K^{11}))$ to $K' = K^{00} \cup K^{11} \cup ((x'10) + (K^{00} \cup K^{11}))$ gives an equivalent code, which is obtained from K by permuting the $(n-1)$th and the nth coordinate positions.

3 Components of duals of BCH codes

In the section we fix $n = 2^m$, m odd. We investigate the i-components of the dual code $B^{\perp}$ of a primitive cyclic BCH code B with zeros α and α^3 with designed distance 5 by i-components, of length $n-1 = 2^m - 1$, m odd, here α is a primitive element of the Galois field $GF(2^m)$. The code shares many similar properties with a Kerdock code. We prove that $B^{\perp}$ is an i-component for any coordinate position i.

Further we use the following properties of the code $B^{\perp}$.

(B1) (See [2].) The minimum distance of the code $B^{\perp}$ is $d = \frac{n-\sqrt{2n}}{2}$. The code $B^{\perp}$ has the following weight distribution:

i	The number of codewords of weight i
0	1
d	$(n-1)(\frac{n}{4} + \sqrt{\frac{n}{8}})$
$\frac{n}{2}$	$(n-1)(\frac{n}{2} + 1)$
n-d	$(n-1)(\frac{n}{4} - \sqrt{\frac{n}{8}})$

The fact below follows from Theorem 1 and the property (B1).

(B2) Any set of fixed weight codewords of $B^{\perp}$ forms a 2-design.

The code B is uniformly packed, see [7]. In [9], Theorem 6.10 it was shown that any code that is dual to a linear completely regular code gives an association scheme.

(B3) (See [9]) The restriction of the Hamming scheme to $B^{\perp}$ is an association scheme.

Lemma 7. *Any codeword of the punctured code of $B^{\perp}$ of weight d is at distance $d-1$ from at least one codeword of weight $d-1$.*

The proof follows from the property (B2) and Lemma 1.

Lemma 8. *The minimum weight codewords of $B^{\perp}$ span the code.*

Proof. The code $B^{\perp}$ is the direct sum of the Hadamard codes H_1 and H_2, both consisting of $n-1$ nonzero codewords having weight $n/2$. The number of codewords of weight d in $B^{\perp}$ is greater then n (see (B1)). Therefore one can find three codewords in the codes H_1 and H_2 with distances d or $n/2$ pairwise, e.g. $x, x' \in H_1$ and $y \in H_2$, such that $d(x,x') = n/2$ and $d(x,y) = d(x',y) = d$. Hence, by the property (B3), we have that the intersection number $\delta^{d}_{d,n/2}(B^{\perp})$ is nonzero, i.e. any codeword of weight $n/2$ is at distance d from at least one codeword of weight d in $B^{\perp}$.

The number of codewords of weight $n-d$ is less than the number of codewords of weight d, therefore any codeword of weight $n-d$ is at distance d from at least one codeword of weight $n/2$ or d. So, the codewords of weight d generate the code $B^{\perp}$.

Theorem 4. *The code $B^{\perp}$ of length $n = 2^m - 1$, m odd, consists of one i-component for any coordinate position i. Equivalently, for any $i \in \{1, \ldots, n\}$ the code $B^{\perp}$ is spanned by minimum weight codewords with ones in ith coordinate.*

Proof. By Lemma 7 any codeword of $B^{\perp}$ of weight d with 0 in the ith coordinate position is at distance d from a codeword of weight d with 1 in the ith coordinate position. By Lemma 8, this implies that the set of all codewords of weight d having 1 in the ith coordinate position generates the code $B^{\perp}$, i.e. the code $B^{\perp}$ is an i-component for any $i \in \{1, 2, \ldots, n-1\}$.

Note that the properties (B1)–(B3) and the proof of Theorem 4 are the same for any code that is dual to a linear uniformly packed code with the same parameters as the BCH code. In particular, the cyclic code $C_{1,2^j+1}$ of length $2^m - 1$, $(j, m) = 1$, m odd, corresponding to the Gold function, as well as the other linear codes obtained from almost bent functions (AB-functions) are uniformly packed [8] and therefore the dual of any such code is an i-component for any i.

Corollary 1. *The dual of a linear uniformly packed code with parameters of the BCH code B of length $n-1 = 2^m$, m-odd is an i-component for any coordinate position i.*

Conclusion. We considered the duals of two such well-known classes of uniformly packed codes as Preparata and 2-error correcting BCH codes. The dual codes have large minimum distance, few nonzero weights and are related to designs and association schemes. We proved that i-components of these codes are maximum. It would be natural to study the structure of i-components of Preparata codes that are formally duals of Kerdock codes. For $n = 15$ these classes meet in the self-dual Nordstrom-Robinson code that has two i-components for any coordinate position i.

By computer-aided investigation we showed that $B^{\perp}$ of length $2^m - 1$ is an i-component for any i for even m also for $m = 6, 8, 10$ and the BCH code B of length $2^m - 1$ consists of two i-components for any coordinate position i for any m: $5 \leq m \leq 8$ as well as $Z4$-linear Preparata code of length $n = 64$. Another challenging problem is finding i-components of the BCH code for any m and their duals for even m. The solution for the problem would directly imply the existence of minimum weight basis for this code. Note that extensions of these codes possess minimum weight basis [3], as well as the extensions of cyclic codes related to Gold functions [4].

References

1. S. V. Avgustinovich. To the Structure of Minimum Distance Graphs of Perfect Binary (n, 3)-Codes. *Diskretn. Anal. Issled. Oper.*, 5(4):3–5, 1998.
2. F. J. MacWilliams, N. J. A. Sloane. *The Theory of Error-Correcting Codes, North-Holland Publishing Company*, pp. 762, 1977.
3. E. Grigorescu, T. Kaufman. Explicit Low-Weight Bases for BCH Codes. *IEEE Trans. Inform. Theory*, (58)2:78–81, 2011.
4. I. Yu. Mogilnykh, F. I. Soloveva. On explicit minimum weight bases for extended cyclic codes related to Gold functions. *Designs, Codes and Cryptography*, (86)11:2619–2627, 2018.
5. A. M. Kerdock. A class of low-rate non-linear binary codes. *Inform. Control*, (20)2:182–187, 1972.
6. W. M. Kantor. An exponential number of generalized Kerdock codes. *Inform. Control*, (53)1-2:74–80, 1982.
7. L. A. Bassalygo, G. A. Zaitsev, V. A. Zinov'ev. Uniformly packed codes. *Probl. Inf. Transm.*, (10)1:6–9, 1974.
8. C. Carlet, P. Charpin, V. A. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Des. Codes Cryptogr.*, (15):125–156, 1998.
9. P. Delsarte. An Algebraic Approach to the Association Schemes of Coding Theory. *Philips Res. Rep. Suppl.*, (10):1–97, 1973.
10. A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Sole. The Z_4-linearity of Kerdock, Preparata, Goethals and related codes. *IEEE Trans. Inform. Theory*, (40):301–319, 1994.
11. F. I. Solov'eva. Survey on perfect codes. *Mathematical Problems of Cybernetics*, (18):5–34, 2013 (in Russian).
12. F. I. Solov'eva, N N. Tokareva. Distance regularity of Kerdock codes. *Siberian Mathematical Journal*, (49)3:539–548, 2008.
13. N. V. Semakov, V. A. Zinov'ev, G. V. Zaitsev. Uniformly Packed Codes. *Probl. Peredachi Inform.*, (7)1:38–50, 1971 (in Russian).

14. D. De Caen, E. R. van Dam. Association schemes related to Kasami codes and Kerdock sets. *Des. Codes. Cryptogr.*, (18):89–102, 1999.
15. K. S. Abdukhalikov, E. Bannai, S. Suda. Association schemes related to universally optimal configurations, Kerdock codes and extremal Euclidean line-sets. *J. Comb. Theory, Ser. A*, (116)2:434–448, 2009.