On the (2,1)-Separating Weight of the Kerdock Code

Tor Helleseth *Fellow, IEEE,*
Hans Georg Schaathun *Member, IEEE,*

***Abstract*— Separating codes find applications in many fields including automata theory and digital fingerprinting. It is known that the Kerdock code of sufficient order is $(2,1)$- and $(2,2)$-separating, but the separating weight is only known by a lower bound due to Sagalovich. In this paper we prove that the lower bound on the $(2,1)$-separating weight is met with equality.**

***Index Terms*— Fingerprinting, Kerdock code, linear codes over Z_4, separating systems**

I. Introduction

In recent years there has been an increasing interest in problems of digital fingerprinting [2]. When a vendor sells copies of some copyrighted work, each copy may be marked with a unique fingerprint. If illegal copies subsequently appear, the fingerprint enables the vendor to trace them back to a legal copy and a guilty buyer. If two or more users collude they can compare their copies. Any differing bit must be part of the fingerprint, and these detected bits may be changed to produce a hybrid copy. A t-collusion-secure fingerprinting code enables the vendor to trace at least one pirate when a collusion of at most t users is guilty.

Separating codes are used in some constructions of collusion secure codes [1], and for certain constructions [7], the separating weight is an important parameter.

Consider three codewords a_1, a_2, and b in an (n, M, d) code, i.e., a code of length n with M codewords and minimum Hamming distance d. We say that a coordinate position i separates $\{a_1, a_2\}$ and b if both a_1 and a_2 are different from b in this position. A code is $(2,1)$-separating if any pair of codewords is separated from any other codeword in at least one position. The $(2,1)$-separating weight is the greatest number θ such that any pair of codewords is separated from any other codeword in at least θ coordinates.

That $\theta \geq d_1 - m_1/2$ holds for any code with minimum distance d_1 and maximum distance m_1, is well known [6], [4]. Just observe that the number of positions N separating a_1 and a_2 from b is given as

$$N \geq \frac{1}{2}(d(a_1,b) + d(a_2,b) - d(a_1,a_2)) \geq \frac{1}{2}(2d_1 - m_1)$$

where the first bound holds with equality for binary codes. It is evident that $\theta = d_1 - m_1/2$ if and only if there are three codewords a_1, a_2, b such that $d(a_1,a_2) = m_1$ and $d(a_1,b) = d(a_2,b) = d_1$.

The binary Kerdock code is a nonlinear $(2^{m+1}, 2^{2(m+1)}, 2^m - 2^{\lfloor m/2 \rfloor})$ code where m is odd. Due to the all-one and all-zero codewords, the binary Kerdock code cannot itself be $(2,1)$-separating. However, by shortening the code, we obtain a $(2^{m+1} - 1, 2^{2m+1}, 2^m - 2^{\lfloor m/2 \rfloor})$ binary code. A lower bound on θ for the shortened Kerdock code is a simple consequence of the bound above due to Sagalovich [6] and was explicitly stated for the shortened Kerdock code in Krasnopeev and Sagalovich [4].

Theorem 1 *[4] Let m be odd. The $(2^{m+1} - 1, 2^{2m+1}, 2^m - 2^{\lfloor m/2 \rfloor})$ shortened binary Kerdock code has $(2,1)$-separating weight*

$$\theta \geq \max\{0, 2^{m-1} - 3 \cdot 2^{\lfloor m/2 \rfloor - 1}\}.$$

The main result in this paper (see Theorem 3) is to prove that this bound on θ *is always met with equality*, and that it holds for the family of $(2^{m+1} - 1, 2^{2m+1}, 2^m - 2^{\lfloor m/2 \rfloor})$ binary codes obtained by shortening the Gray map of the Kerdock codes over Z_4 defined for all integers m. For m odd these codes coincide with the codes in Theorem 1.

Note that the $(2^{m+1} - 1, 2^{2m+1}, 2^m - 2^{\lfloor m/2 \rfloor})$ shortened Kerdock code is a binary three-weight code with weights $d_1 = 2^m - 2^{\lfloor m/2 \rfloor}$, 2^m, and $m_1 = 2^m + 2^{\lfloor m/2 \rfloor}$. Theorem 3 implies that the shortened binary Kerdock code is $(2,1)$-separating if and only if $m \geq 3$, in which case the separating weight is exactly equal to $d_1 - m_1/2$.

So to prove that the bound on θ in Theorem 1 is met with equality, it remains only to prove that the code contains three codewords a_1, a_2, b such that $d(a_1,a_2) = m_1$ and $d(a_1,b) = d(a_2,b) = d_1$.

We present two proofs of our main result. The first proof that we present was suggested to us by an anonymous referee and this proof works directly for the binary Kerdock code defined for odd m. This proof is presented in Section II.

The second proof is based on the algebraic description of the codes over Z_4 that define the binary Kerdock codes via the Gray map. This method can in principle be applied to other codes with a nice algebraic construction. In Section III we describe the Kerdock codes over Z_4 for all integers m and provide the basic results needed in order to give the algebraic proof of the main result of Theorem 3.

II. Separating weight of the binary Kerdock code

In this section we present the proof due to the anonymous referee, implying the main result for the binary $(2^{m+1}, 2^{2(m+1)}, 2^m - 2^{\lfloor m/2 \rfloor})$ Kerdock codes for odd m.

Theorem 2 *Let K be the binary (n, M, d) Kerdock code where $n = 2^{m+1}$, $M = 2^{2(m+1)}$, $d = \frac{n - \sqrt{n}}{2}$ and $m \geq 3$ is odd. There exist at least one pair a_1, a_2 of codewords with minimal weights $(n - \sqrt{n})/2$ such that their distance is $(n + \sqrt{n})/2$.*

Proof: It is known that the Kerdock code can be described as a union of the first order Reed-Muller code, denoted by R, and $n/2 - 1$ cosets of R contained in the second order Reed-Muller code of the same length. The cosets correspond to quadratic bent functions and the sum of two cosets is also a bent function. It is known that any such coset (except the zero coset R) consists of n vectors of minimum

T. Helleseth and H. G. Schaathun are at The Selmer Centre, Department of Informatics, University of Bergen, PB 7800, N-5020 Bergen, Norway (emails: tor.helleseth@ii.uib.no and georg@ii.uib.no)

The authors were supported by the Norwegian Research Council and the AURORA program.

weight $(n-\sqrt{n})/2$ and the same number of vectors of weight $(n+\sqrt{n})/2$. Consider any two such cosets and define the subsets L_α and L_β of R such that $\alpha+L_\alpha$ and $\beta+L_\beta$ are the subsets of vectors of minimum weight $(n-\sqrt{n})/2$ in the cosets $\alpha+R$ and $\beta+R$ respectively, and let α and β have minimum weight i.e., $0\in L_\alpha$ and $0\in L_\beta$.

Consider any two cosets $\alpha+R$ and $\beta+R$ in the Kerdock code. Then the coset $\alpha+\beta+R$ (which does not necessarily have to be in the Kerdock code) is also known to have n vectors of minimum weight $(n-\sqrt{n})/2$ and the same number of vectors of weight $(n+\sqrt{n})/2$.

We will show that there exist two vectors a_1 and a_2 in the Kerdock code of minimum weight $(n-\sqrt{n})/2$ such that their distance is $(n+\sqrt{n})/2$. If there is no such pair of vectors among $a_1\in\alpha+L_\alpha$ and $a_2\in\beta+L_\beta$ then a_1+a_2 has weight $(n-\sqrt{n})/2$ and hence $L_\alpha+L_\beta\subset L_{\alpha+\beta}$. Since $|L_\alpha|=|L_\beta|=|L_{\alpha+\beta}|$, we have that $L_\alpha=L_\beta=L_{\alpha+\beta}$, and therefore $L_\alpha=L$ is an additive subgroup, i.e. an $(m+1)$-dimensional linear code.

Since all vectors in the coset $\alpha+L$ have weight $(n-\sqrt{n})/2$, we can obtain a contradiction by computing the sum of the weights of the vectors in the coset in two ways, one by computing the sum of the weights of the rows and one by computing the sum of the weights of the columns. Since all vectors in the coset have minimum weight and each nonzero column of L contributes a weight 2^m to the coset, we obtain:

$$2^{m+1}(n-\sqrt{n})/2\geq 2^m n_e$$

where n_e is the number of nonzero columns in L. Hence $n_e\leq n-\sqrt{n}$. Since L is contained in the first order Reed-Muller code of minimum distance 2^m it follows by the Griesmer bound that $n_e\geq 2^{m+1}-1=n-1>n-\sqrt{n}$, a contradiction. ■

Because the sum of the Hamming weights $w(a_1)+w(a_2)+w(a_1+a_2)<2n$ for the vectors selected by the theorem above, there is a position where both a_1 and a_2 are zero. This means that codewords a_1, a_2 and $b=0$ with the required properties exist in a shortened code of the Kerdock code. Since the Kerdock code is invariant under a double transitive group such codewords exist for any shortening of the Kerdock code. It therefore follows that equality holds in Theorem 1.

III. Kerdock codes over Z_4

Let Z_4 be the ring of integers modulo 4. In this section we will study codes over Z_4 and the Gray map that can be used to construct binary codes from codes over Z_4. We will describe a family of $(2^{m+1}-1, 2^{2m+1}, 2^m-2^{\lfloor m/2\rfloor})$ binary codes obtained by shortening the Gray map of the Kerdock codes over Z_4 defined for all integers m. For m odd these codes coincides with the codes in Theorem 1. Further, this section gives basic results needed in order to give the algebraic proof of the main result in this paper (cf. Theorem 3).

A linear code over Z_4 with block length n is an additive subgroup of Z_4^n. The Lee weights of the elements 0, 1, 2, 3 of Z_4 are 0, 1, 2, 1, respectively. The Lee weight of a vector $a\in Z_4^n$ is defined to be the sum of the Lee weights of its components. The Gray map is defined such that 0, 1, 2, and 3 are mapped into 00, 01, 11, and 10, respectively. The Hamming distance between two vectors under the Gray map equals their Lee distance. In [3], it was shown that efficient nonlinear codes such as Kerdock, Preparata, etc., can easily be constructed as binary images under the Gray map of linear codes over Z_4.

The Galois ring $R=GR(4,m)$ is an extension of Z_4 of degree m. The ring R is a local ring having a unique maximal ideal $M=2R$ and the quotient ring R/M is isomorphic to F_{2^m} where F_{2^m} is a finite field with 2^m elements (see [3], [5] for details).

As a multiplicative group, the set R^* of units of R has the following structure

$$R^*\cong Z_{2^m-1}\times\underbrace{Z_2\times Z_2\times\cdots\times Z_2}_{m\text{ times}}.$$

Let $\beta\in R^*$ be a generator for the multiplicative cyclic subgroup $\cong Z_{2^m-1}$ contained within R^*. Let $\mathcal{T}=\{0,1,\beta,\ldots,\beta^{2^m-2}\}$. It can be shown that every element $z\in R$ can be expressed uniquely as

$$z=a+2b,\quad a,b\in\mathcal{T}.$$

It can be also shown that $\alpha=\beta\pmod 2$ is a primitive element in F_{2^m}. The Frobenius map σ from R to R is defined by

$$\sigma(z)=a^2+2b^2$$

and the trace map from R to Z_4 is defined by

$$T(z)=\sum_{j=0}^{m-1}\sigma^j(z).$$

Using the facts that $(a+2b)^{2^m}=a$ and $T(a)=T(a^2)$, we can show that for all $\gamma,\delta\in\mathcal{T}$, we have that $\gamma+\delta+2\sqrt{\gamma\delta}\in\mathcal{T}$ and

$$T\left(\gamma+\delta+2\sqrt{\gamma\delta}\right)=T\left([\gamma+\delta]^2\right).$$

Let $c(u,a)$, where $u\in Z_4, a\in R$, be a vector in Z_4^q indexed by the elements of $\mathcal{T}$ such that $c(u,a)_x=u+T(ax)$ for all $x\in\mathcal{T}$. The Kerdock code $\mathcal{K}$ over Z_4 of length $q=2^m$ is defined by

$$\mathcal{K}=\{c(u,a)\mid u\in Z_4, a\in R\}.$$

Clearly, $\mathcal{K}$ has 4^{m+1} codewords. In this paper, the code $\mathcal{K}$ will be called the Kerdock code over Z_4 for any m.

The Lee weight of $b\in Z_4$ is related to the real part of ω^b via $w_L(b)=1-\mathrm{Re}(\omega^b)$, where $\omega=\sqrt{-1}$. Hence we have

$$w_L(c(u,a))=q-\mathrm{Re}\left[\omega^u\sum_{x\in\mathcal{T}}\omega^{T(ax)}\right].\qquad(1)$$

To find the Lee weight distribution of $\mathcal{K}$, it suffices to determine the distribution of the exponential sum

$$\Gamma(a)=\sum_{x\in\mathcal{T}}\omega^{T(ax)}.\qquad(2)$$

Lemma 1 *Let $q=2^m$ where $m\geq 3$. Let A_i be the number of codewords of Lee weight i. The Lee weight distribution of $\mathcal{K}$ is as follows:*

(i) *If m is odd, then*

$$A_i = \begin{cases} 1 & \text{for } i = 0 \text{ or } 2q, \\ 2q(q-1) & \text{for } i = q \pm \sqrt{q/2}, \\ 4q-2 & \text{for } i = q. \end{cases}$$

(ii) *If m is even, then*

$$A_i = \begin{cases} 1 & \text{for } i = 0 \text{ or } 2q, \\ q(q-1) & \text{for } i = q \pm \sqrt{q}, \\ 2q^2+2q-2 & \text{for } i = q. \end{cases}$$

Proof: If m is odd, the Lee weight distribution can be found in [3]. If m is even, the Lee weight distribution can be determined in a similar way, so we omit the details. ■

For any non-zero $\delta \in \mathcal{T}$, the codeword $c(0, 2\delta)$ is an extended binary m-sequence multiplied by 2 (mod 4), so it has Lee weight $q = 2^m$. In order to identify the minimum Lee weight vectors of the form $c(0,a)$, it is necessary to analyze the exponential sum $\Gamma(a)$ given in (2).

Lemma 2 *Let $a = \gamma + 2\delta$ with $\gamma, \delta \in \mathcal{T}$ and $\gamma \neq 0$. Then*

$$\Gamma(\gamma + 2\delta) = \omega^{-T(\delta/\gamma)}\, \Gamma(1).$$

Lemma 3 *Let ϵ be the primitive 8th root of unity, given by $\epsilon = (1+\omega)/\sqrt{2}$. Then we have*

$$\Gamma(1) = \begin{cases} \sqrt{2^m}\, \epsilon^m & \text{if } m \text{ is odd,} \\ -\sqrt{2^m}\, \epsilon^m & \text{if } m \text{ is even.} \end{cases}$$

Combining (1) with Lemma 2 and Lemma 3, we have a closed-form expression for the Lee weight of a Kerdock codeword in terms of the coefficients in its trace expansion. That is, for $u \in Z_4$ and $\gamma, \delta \in \mathcal{T}$, we have

$$w_L(c(u, \gamma+2\delta)) = \begin{cases} q - \mathrm{Re}[\omega^{u-T(\delta/\gamma)}\Gamma(1)], & \gamma \neq 0, \\ q, & \gamma = 0, \delta \neq 0, \\ q - \mathrm{Re}(q\,\omega^u), & \gamma = 0, \delta = 0. \end{cases}$$

These relations are the key to identify vectors with minimum Lee weight in the Kerdock code. Note that the codeword $c(0, \gamma + 2\delta)$ has the same Lee weight as the codeword $c(0, 1+2\delta/\gamma)$ for any $\gamma \neq 0$. The codewords of minimum and maximum values, of the form $c(0, 1+2\delta)$, are determined by the values of δ as given in Table I.

[Table 1 about here.]

Consider the codeword $c(u,a)$, where $u \in Z_4, a \in R$. The exponential sum associated with $c(u,a)$ is the exponential sum $\Gamma(a)$ associated with $c(0,a)$, multiplied by ω^u. Hence the effect of u is to rotate $\Gamma(a)$ by a multiple of $\pi/2$.

We will show that we can select two nonzero codewords, $c(0,a)$ and $c(0,b)$, of minimum Lee weight $d_1 = 2^m - 2^{\lfloor m/2 \rfloor}$ in the Kerdock code over Z_4, such that their difference has the maximum Lee weight $m_1 = 2^m + 2^{\lfloor m/2 \rfloor}$ (excluding the all-2 vector of Lee weight 2^{m+1}) in the Kerdock code over Z_4. From now on, the codeword a is assumed to imply the codeword $c(0,a)$.

Let $a = 1 + 2\delta_1$ and $b = \gamma + 2\delta_2$, be two vectors in the Kerdock code with minimum Lee weight. The difference $a-b$ is given as

$$\begin{aligned} a - b &= 1 - \gamma + 2(\delta_1 + \delta_2) \\ &= 1 + \gamma + 2\sqrt{\gamma} + 2(\delta_1 + \delta_2 + \gamma + \sqrt{\gamma}). \end{aligned}$$

If we let a and b correspond to a value s giving a minimum Lee weight d_1 and $a - b$ to a value t giving maximum weight Lee m_1 (less than 2^{m+1}), it follows as an important consequence of the following lemma that we can find nonzero vectors a and b of minimum Lee weight d_1 such that $a-b$ has maximum Lee weight m_1 (less than 2^{m+1}) in the code.

Lemma 4 *Suppose $m \geq 7$. Then, for any $s, t \in Z_4$, there exist $\delta_1, \delta_2, \gamma \in \mathcal{T}$ such that $\gamma \notin \{0,1\}$ and*

$$T(\delta_1) = T\left(\frac{\delta_2}{\gamma}\right) = s$$

and

$$T\left(\frac{(\delta_1 + \delta_2 + \gamma + \sqrt{\gamma})^2}{(1+\gamma)^2}\right) = t.$$

Proof: Consider the three equations

$$\begin{aligned} E_0 &= T(\delta_1) - s, \\ E_1 &= T\left(\frac{\delta_2}{\gamma}\right) - s, \\ E_2 &= T\left(\frac{(\delta_1 + \delta_2 + \gamma + \sqrt{\gamma})^2}{(1+\gamma)^2}\right) - t. \end{aligned}$$

We first select δ_1 such that $T(\delta_1) = s$, and then γ such that $\gamma \notin \{0,1\}$. Let N be the number of $\delta_2 \in \mathcal{T}$ such that $E_1 = E_2 = 0$. Then we have

$$\sum_{\delta_2 \in \mathcal{T}} \sum_{u_1, u_2 \in Z_4} \omega^{u_1 E_1 + u_2 E_2} = 4^2 N.$$

We want to show that $N \geq 1$. Setting

$$u_1 E_1 + u_2 E_2 = B(\delta_2) - s u_1 - t u_2,$$

we have

$$\begin{aligned} B(\delta_2) &= T\left(u_1 \frac{\delta_2^2}{\gamma^2} + u_2 \frac{(\delta_1 + \delta_2 + \gamma + \sqrt{\gamma})^2}{(1+\gamma)^2}\right) \\ &= T\left(\delta_2^2 \left[\frac{u_1}{\gamma^2} + \frac{u_2}{(1+\gamma)^2}\right] + 2\delta_2 \left[\frac{u_2(\delta_1 + \gamma + \sqrt{\gamma})}{(1+\gamma)^2}\right] \right. \\ &\qquad \left. + u_2 \frac{(\delta_1 + \gamma + \sqrt{\gamma})^2}{(1+\gamma)^2}\right). \end{aligned}$$

Since $2T(u_i e \delta) = 2u_i T(e\delta) = 2u_i T(e^2\delta^2) = 2T(u_i e^2 \delta^2)$ for any $e \in R$, we have that

$$
\begin{aligned}
B(\delta_2) &= T\Bigg(\delta_2^2\left[\frac{u_1}{\gamma^2}+\frac{u_2}{(1+\gamma)^2}+\frac{2u_2(\delta_1+\gamma+\sqrt{\gamma})^2}{(1+\gamma)^4}\right] \\
&\qquad + u_2\frac{(\delta_1+\gamma+\sqrt{\gamma})^2}{(1+\gamma)^2}\Bigg) \\
&= T(\delta_2^2 B_2 + B_0),
\end{aligned}
$$

where

$$
\begin{aligned}
B_2 &= \frac{u_1}{\gamma^2}+\frac{u_2}{(1+\gamma)^2}+2u_2\frac{(\delta_1+\gamma+\sqrt{\gamma})^2}{(1+\gamma)^4}, \\
B_0 &= u_2\frac{(\delta_1+\gamma+\sqrt{\gamma})^2}{(1+\gamma)^2}.
\end{aligned}
$$

Now we are interested in the cases where $B_2 = 0$. If we write B_2 in 2-adic expression, that is, $B_2 = D_0 + 2D_1$, then $B_2 = 0$ if and only if $D_0 = D_1 = 0$. Since $D_0 = B_2 \bmod 2$, we have

$$
\begin{aligned}
D_0 &= \frac{u_1}{\gamma^2}+\frac{u_2}{(1+\gamma)^2} \pmod 2 \\
&= \frac{u_1+u_1\gamma^2+u_2\gamma^2}{\gamma^2(1+\gamma)^2} \pmod 2 \\
&= \frac{u_1+(u_1+u_2)\gamma^2}{\gamma^2(1+\gamma)^2} \pmod 2.
\end{aligned}
$$

So the only possibility for $D_0 = 0$ is when $u_1 = u_2 = 0 \pmod 2$. In this case, we get

$$B_2 = \frac{u_1}{\gamma^2}+\frac{u_2}{(1+\gamma)^2} \pmod 4.$$

Therefore, since $u_1 = 2v_1$ and $u_2 = 2v_2$, for some $v_1, v_2 \in \{0,1\}$, we can repeat this argument and we obtain $v_1 = v_2 = 0 \pmod 2$. Hence, we have

$$B_2 = 0 \text{ iff } u_1 = u_2 = 0 \pmod 4.$$

Under these conditions we also have that the constant term $B_0 = 0$. Let $q = 2^m$, then by grouping u_1, u_2 into two classes depending on whether the value of B_2 is 0 or not, we have

$$
\begin{aligned}
16N &= \sum_{u_1,u_2\in Z_4}\sum_{\delta_2\in\mathcal{T}}\omega^{u_1E_1+u_2E_2} \\
&= \sum_{(u_1,u_2)=(0,0)}\sum_{\delta_2\in\mathcal{T}}\omega^{T(\delta_2^2B_2+B_0)} \\
&\quad + \sum_{(u_1,u_2)\neq(0,0)}\omega^{-su_1-tu_2}\sum_{\delta_2\in\mathcal{T}}\omega^{T(\delta_2^2B_2+B_0)} \\
&= q + \sum_{(u_1,u_2)\neq(0,0)}\omega^{-su_1-tu_2}\sum_{\delta_2\in\mathcal{T}}\omega^{T(\delta_2^2B_2+B_0)}.
\end{aligned}
$$

Since $B_2 = 0$ only if $u_1 = u_2 = 0 \pmod 4$, we can use the bound on the exponential sum [5, Theorem 1] (or Lemma 2 and Lemma 3 above). Since the inner sum is 0 in the case $u_1 = u_2 = 0 \pmod 2$, we have

$$|16N - q| \leq 12\sqrt{q}.$$

Therefore, $q \geq 2^8$ guarantees that $N > 0$.

In the case when m is odd this can be slightly improved, by noting that the 12 sums corresponding to $(u_1,u_2) \neq (0,0) \pmod 2$ can be divided into six pairs. Each pair correspond to (u_1,u_2) and its negative $(-u_1,-u_2) \pmod 4$. Since, each pair contributes two complex conjugate values to the sum, it follows that when m is odd, the bound $12\sqrt{q}$ can be improved to $6\sqrt{2q}$. Hence, for odd m it is sufficient to require $q \geq 2^7$. ■

Lemma 4 and the discussion before this lemma implies the following result.

Lemma 5 *Suppose $m \geq 7$. There exists two codewords $c(0,a)$ and $c(0,b)$ in the Kerdock code over Z_4 of minimum Lee weight $d_1 = 2^m - 2^{\lfloor m/2\rfloor}$ such that their Lee distance is $m_1 = 2^m + 2^{\lfloor m/2\rfloor}$.*

Since the Kerdock code over Z_4 is invariant under a double transitive permutation group we can assume without loss of generality that the code after the Gray map is shortened in the first position. Our main result is to determine the exact (2,1)-separating weight of the resulting binary code.

Theorem 3 *Let m be any integer ≥ 3. Then the $(2^{m+1}-1, 2^{2m+1}, 2^m - 2^{\lfloor m/2\rfloor})$ binary code obtained by shortening the Gray map of the Kerdock code over Z_4 has $(2,1)$-separating weight*

$$\theta = \max\{0, 2^{m-1} - 3\cdot 2^{\lfloor m/2\rfloor - 1}\}.$$

Proof: The theorem says that the code is $(2,1)$-separating if and only if $m \geq 3$, in which case the separating weight is exactly equal to $d_1 - m_1/2$. It is easily verified that the code is not (2,1)-separating for $m = 1$ and $m = 2$. In the case $m = 3$ and $m = 5$ the result has been shown by Krasnopeev and Sagalovich [4] using a computer search. The cases $m = 4$ and $m = 6$ we have settled by a computer search.

It is clear following the remark after Theorem 1 that the result follows if and only if there are three codewords a_1, a_2, b such that $d(a_1,a_2) = m_1$ and $d(a_1,b) = d(a_2,b) = d_1$. So to prove the theorem, it remains only to prove that such codewords exist for $m \geq 7$.

It follows as a consequence of Lemma 5 above that there are codewords $a_1 = c(0,a)$, $a_2 = c(0,b)$ and $b = 0$ with these properties. Since all these codewords are zero in position $x = 0$, the Gray map of all these vectors will after shortening in the first position, also belong to the shortened binary Kerdock code and have the required properties. ■

IV. Acknowledgement

The authors would like to thank Gerard Cohen for bringing the problem to the authors attention and the referee for valuable comments and for suggesting the proof of Theorem 2.

References

[1] A. Barg, G. R. Blakley, and G.A. Kabatiansky, "Digital fingerprinting codes: Problem statements, constructions, identification of traitors," *IEEE Trans. Inform. Theory*, vol. IT-49, pp. 852-865, Apr. 2003.

[2] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inform. Theory*, vol. IT-44, pp. 1897-1905, Sept. 1998.

[3] A.R. Hammons, Jr., P.V. Kumar, A.R. Calderbank, N. J. A. Sloane, and P. Sole, "The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Inform. Theory*, vol. IT-40, pp. 301-319, Mar. 1994.

[4] A. Krasnopeev and Yu. L. Sagalovich, “The Kerdock codes and separating systems,” in *Proc: Eight International Workshop on Algebraic and Combinatorial Coding Theory*, Sept. 2002, pp. 165-167.

[5] P. V. Kumar, T. Helleseth, and A. R. Calderbank, “An upper bound for Weil exponential sums over Galois rings and applications,” *IEEE Trans. Inform. Theory*, vol. IT-41, pp. 456-468, Mar. 1995.

[6] Yu. L. Sagalovich, “Separating systems,” *Problems of Information Transmission*, vol. 30, pp. 105-123, 1994.

[7] H. G. Schaathun, “Fighting two pirates,” in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, (*Lecture Notes in Computer Science*). Berlin, Germany: Springer-Verlag, 2003,vol. 2643, pp. 71-78.

[8] K. Yang, P. V. Kumar, T. Helleseth, and A. G. Shanbhag, “On the weight hierarchy of Kerdock codes over Z_4,” *IEEE Trans. Inform. Theory*, vol. IT-42, pp. 1587-1593, Sept. 1996.

Tor Helleseth (M’89-SM’96-F’97) received the Cand. Real. and Dr. Philos. degrees in mathematics from the University of Bergen, Bergen, Norway, in 1971 and 1979, respectively.

From 1973 to 1980 he was a Research Assistant at the Department of Mathematics, University of Bergen. From 1981 to 1984 he was at the Chief Headquarters of Defense in Norway. Since 1984 he has been a Professor at the Department of Informatics at the University of Bergen. During the academic years 1977-1978 and 1992-1993 he was on sabbatical leave at the University of Southern California, Los Angeles, and during 1979-1980 he was a Research fellow at the Eindhoven University of Technology, The Netherlands. His research interests include coding theory and cryptology.

From 1991 to 1993 he served as an Associate Editor for Coding Theory for IEEE TRANSACTIONS ON INFORMATION THEORY. He was Program Chairman for Eurocrypt’93 and for the Information Theory Workshop in 1997 in Longyearbyen, Norway. He will also be the Program Chairman for SETA04. In 1997 he was elected an IEEE Fellow for his contributions to coding theory and cryptography.

Hans Georg Schaathun was born in Bergen, Norway, in 1975. He received a Cand.Mag. degree with mathematics from the University of Bergen in 1996. He is Cand.Scient. 1999 and Dr.Scient 2002 from the Department of Informatics at the University of Bergen. During 2002 he was a lecturer, and from 2003 he is a post-doctoral researcher at this university. He has been at research stays at ENST in Paris 2000/2001 and at the Royal Holloway, University of London 2003/2004.

His research interest include codes for digital fingerprinting and higher weights of linear codes.

List of Tables

I The values of $T(\delta)$ which give minimum and maximum weight of $c(0, 1 + 2\delta)$ for the various values of m. . . 7

	$T(\delta)$ for weight	
$m \pmod 8$	Minimum	Maximum
0	2	0
1	0 or 1	2 or 3
2	3	1
3	1 or 2	3 or 0
4	0	2
5	2 or 3	0 or 1
6	1	3
7	3 or 0	1 or 2

TABLE I

THE VALUES OF $T(\delta)$ WHICH GIVE MINIMUM AND MAXIMUM WEIGHT OF $c(0, 1+2\delta)$ FOR THE VARIOUS VALUES OF m.