

# On the Minimal Distance of Binary Self-Dual Cyclic Codes

Bas Heijne and Jaap Top

**Abstract**—In this paper, an explicit construction of binary self-dual cyclic codes of length  $n$  going to infinity with a minimal distance at least half the square root of  $n$  is presented. The same idea is also used to construct more general binary cyclic codes with a large minimal distance. Finally, in the special case of self-dual cyclic codes, a simplified version of a proof by Conway and Sloane is given, showing an upper bound for the distance of binary self-dual codes.

**Index Terms**—BCH bound, binary code, cyclic code, minimal distance, self-dual code.

## I. RESULTS

THE main result proven in this paper (see Section III) is the following.

*Theorem 1.1:* Given a positive integer  $\delta$ , there exists a binary cyclic self-dual code with length  $n < 4\delta^2 - 2$  and minimal distance  $d \geq \delta$ .

The proof, which is constructive, uses the BCH-bound, which we recall and slightly extend in the first paragraphs of Section III. It should be noted that MacWilliams, Sloane, and Thompson [8] provided a nonconstructive proof for the existence of binary self-dual  $[n_i, k_i = n_i/2, d_i]$ -codes with  $(n_i)_{i \geq 1}$  strictly increasing and such that  $d_i/n_i$  converges to a nonzero constant. Concerning explicit examples, it is well known (see, for example, [12, Section 8.4]) that for any prime number  $p \equiv \pm 1 \pmod{8}$ , the (binary) extended quadratic residue code of length  $p + 1$  is self-dual and has minimal distance  $\geq \sqrt{p}$ . However, these codes are not cyclic.

It is an open problem (compare [14]) whether there is a family of cyclic codes such that both  $d_i/n_i$  and  $k_i/n_i$  converge to nonzero constants, while  $n_i$  is strictly increasing. Much weaker than this, we give an example (Proposition 3.6) of a family of cyclic codes with strictly increasing lengths, such that 0 is not a limit point of one of the arrays  $d_i \log(n_i)/n_i$  and  $k_i/n_i$ .

The second subject of this paper is a significant simplification of the proof of the following theorem by Conway and Sloane, in the special case of cyclic self-dual codes.

Manuscript received December 10, 2008; revised July 10, 2009. Current version published October 21, 2009. This work was supported by the Netherlands Organization for Scientific Research (NWO).

The authors are with the Department of Mathematics and Computer Science (IWI), University of Groningen, 9700AK Groningen, The Netherlands (e-mail: b.l.heijne@rug.nl; j.top@rug.nl).

Communicated by T. Etzion, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2009.2030484

*Theorem 1.2 (Conway and Sloane):* Let  $\mathcal{C}$  be a  $[n, k, d]$  binary self-dual code, with  $n \notin \{2, 8, 12, 22, 24, 32, 48, 72\}$ . Then

$$d \leq 2 \left\lfloor \frac{n+6}{10} \right\rfloor.$$

The special properties of cyclic codes allow us to circumvent the rather deep analysis that was needed in the original proof. An upper bounds for  $d$  in the finite set of exceptions is in fact  $2 \lfloor \frac{n+6}{10} \rfloor + 2$ ; see [2] and also [3]. For cyclic self-dual codes, there is no need to consider a finite set of exceptions: the only assumption we use on the length  $n$  of the cyclic code is that  $n \neq 2$ .

We note that stronger general bounds on  $d$  are known for general self-dual codes; see [9] and [11].

In particular, for binary self-dual  $[n, n/2, d]$ -codes, one has

$$d \leq \begin{cases} 4 \left\lfloor \frac{n}{24} \right\rfloor + 4, & \text{if } n \not\equiv 22 \pmod{24} \\ 4 \left\lfloor \frac{n}{24} \right\rfloor + 6, & \text{if } n \equiv 22 \pmod{24}. \end{cases}$$

Whether even stronger bounds exist, when one restricts to the special case of self-dual cyclic codes, seems unknown. Our exposition in Section IV indicates that at least some arguments are simpler for this subclass.

## II. NOTATION AND DEFINITIONS

An  $[n, k, d]$ -code (or  $[n, k]$ -code) is as usual in coding theory as  $k$ -dimensional linear subspace of  $\mathbb{F}^n$ . Here  $\mathbb{F}$  is a finite field. Moreover,  $d$  is the minimal distance of the code.

A code  $\mathcal{C}$  is cyclic if it is invariant under the shift operator.

*Note:* We allow  $n$  to be divisible by the characteristic of  $\mathbb{F}$ . Under the identification  $\mathbb{F}^n = \mathbb{F}[X]/(X^n - 1)$  cyclic codes correspond to ideals in the principal ideal ring  $\mathbb{F}[X]/(X^n - 1)$ . We will use this identification freely in this text. A monic generator  $f|(X^n - 1)$  of such an ideal is called the generating polynomial of the code.

Let  $\mathcal{C}$  be a code then the dual code  $\mathcal{C}^\perp$  of  $\mathcal{C}$  is the code given by  $\mathcal{C}^\perp = \{x \in \mathbb{F}^n : x \cdot c = 0 \ \forall c \in \mathcal{C}\}$ . Here  $\cdot$  denotes the standard bilinear form. A code satisfying  $\mathcal{C} = \mathcal{C}^\perp$  is called *self-dual*. If  $\mathcal{C}$  is an  $[n, k]$  code, then  $\mathcal{C}^\perp$  is an  $[n, n - k]$  code, hence obviously a necessary condition for the existence of a self-dual code is that  $n = 2k$  is even.

If  $\mathcal{C}$  is a cyclic code with generating polynomial  $f(X)|(X^n - 1)$ , then  $\mathcal{C}^\perp$  is cyclic with generating polynomial  $g^*$ , where  $X^n - 1 = f(X)g(X)$ . Here  $g^*$  stands for the reciprocal polynomial of  $g$ .

As an immediate consequence, one observes the following.

*Proposition 2.1:* Cyclic self-dual codes only exist in characteristic 2.

*Proof:* Suppose that  $\mathcal{C}$  is a cyclic self-dual code of length  $n$  over a finite field  $\mathbb{F}$  with  $\text{char}(\mathbb{F}) = p$ . This means that the generating polynomial  $f$  of  $\mathcal{C}$  satisfies  $f^* \cdot f = X^n - 1$ . Since  $f^*(X) = X^k f(1/X)$  (for  $k = n/2 = \text{deg}(f)$ ), the multiplicity  $\mu$  of the factor  $(X - 1)$  is the same in  $f$  and in  $f^*$ . So  $2\mu$  is the multiplicity of  $(X - 1)$  in  $X^n - 1$ .

Now write  $n = p^e m$  for integers  $e \geq 0$  and  $m$ , with  $\text{gcd}(p, m) = 1$ . One has  $X^n - 1 = (X^m - 1)^{p^e}$  over  $\mathbb{F}$  and  $(X^m - 1) = (X - 1)(X^{m-1} + X^{m-2} + \dots + X + 1)$ . Since  $m \neq 0$  in  $\mathbb{F}$ , this shows that the multiplicity of  $(X - 1)$  in  $X^m - 1$  equals 1, and therefore, the multiplicity of  $(X - 1)$  in  $X^n - 1$  equals  $p^e$ . As a consequence,  $2\mu = p^e$  which implies that  $p = 2$ .  $\square$

From now on we will assume  $\mathbb{F} = \mathbb{F}_2$ .

### III. ARBITRARY LARGE DISTANCE

One of the few general tools to find information on the minimal distance of cyclic codes is the BCH-bound. This bound is usually proven under the condition  $\text{gcd}(n, \text{char}(\mathbb{F})) = 1$  (see, for example, [5]). Since this condition is not satisfied for cyclic self-dual codes, we will use a slight adaption of the BCH-bound.

*Proposition 3.1:* Let  $\mathcal{C}$  be a cyclic  $[n, k, d]$ -code defined over  $\mathbb{F}_2$ , with generating polynomial  $f$  and  $n \equiv 2 \pmod 4$ . Fix  $\zeta \in \overline{\mathbb{F}_2}$  a primitive  $n/2$ th root of unity. Assume that we have  $a, b$ , and  $\delta$  such that  $\zeta^a, \zeta^{a+1}, \dots, \zeta^{a+\delta-2}$  are zeroes of  $f$  and  $\zeta^b, \zeta^{b+1}, \dots, \zeta^{b+\epsilon-2}$  are zeroes of  $f$  with multiplicity 2. Then,  $d \geq \min\{\delta, 2\epsilon\}$ .

*Proof:* Write  $f = g^2 h$  for coprime polynomials  $g, h$ . From [7, Th. 1], it is known that  $\mathcal{C} = (g^2 h)$  is equivalent to the  $|u|u + v|$  sum of the cyclic codes  $\mathcal{C}_1, \mathcal{C}_2$  of length  $n/2$ , with generator  $g$  and  $gh$ , respectively. This implies that

$$d(\mathcal{C}) = \min\{2d(\mathcal{C}_1), d(\mathcal{C}_2)\}.$$

Since  $\zeta^a, \zeta^{a+1}, \dots, \zeta^{a+\delta-2}$  are zeroes of  $gh$ , the classical BCH-bound applied to  $\mathcal{C}_2$  yields  $d(\mathcal{C}_2) \geq \delta$ . Similarly,  $\zeta^b, \zeta^{b+1}, \dots, \zeta^{b+\epsilon-2}$  are zeroes of  $g$ , and therefore,  $d(\mathcal{C}_1) \geq \epsilon$ . The result follows.  $\square$

*Remark 3.2:* In practice, Van Lint’s result used in the proof of Proposition 3.1 is very useful for determining the actual distance of certain binary cyclic codes of length  $\equiv 2 \pmod 4$ . Namely, write the generator as  $g^2 h$  for coprime  $g, h$ . The distance  $d_1, d_2$  of the codes of length  $n/2$  generated by  $g$  and by  $gh$  is easier to find, and the distance we look for equals  $\min\{2d_1, d_2\}$ . We exploited this idea to find the minimal distance of some cyclic codes of length roughly 600, using MAGMA.

We will now use Proposition 3.1 in the proof of Theorem 1.1.

*Proof (of Theorem 1.1):* The main idea is to construct a cyclic self-dual code with such properties that the BCH-bound will give us the desired bound on the distance. Take any integer  $\delta > 2$  (the case of smaller  $\delta$  is trivial). Fix  $a \in \mathbb{Z}$  minimal such that  $2^{a+1} \geq \delta$  and put  $k := 2^{2a+1} - 1$ . Fix  $\zeta$  a root of unity of order  $k$ . In order to apply the BCH-bound, we construct  $f$  and  $g$  such that  $X^k - 1 = f f^* g$  and  $f(\zeta^1) = f(\zeta^2) =$

$\dots = f(\zeta^{\delta-1}) = 0$ . Then, applying Proposition 3.1 to the cyclic code of length  $2k$  generated by  $f^2 g$  (using  $a = 0, b = 1$ , and  $\epsilon = \delta - 1$ ), one concludes  $d \geq \delta$ . Clearly, this code is self-dual and has length  $n = 2k < 4\delta^2 - 2$ .

As groups,  $\langle \zeta \rangle \cong \mathbb{Z}/k\mathbb{Z}$ . Take the subset  $G = \{1, \dots, 2^{a+1} - 2\}$  of  $\mathbb{Z}/k\mathbb{Z}$  and put  $S = \bigcup_{i \geq 0} 2^i G$ .

*Claim:*  $f := \prod_{s \in S} (X - \zeta^s) \in \mathbb{F}_2[X]$  satisfies  $\text{gcd}(f, f^*) = 1$ . Moreover, clearly  $\zeta^i$  is a zero of  $f$  for all  $1 \leq i \leq \delta - 2$ .

The fact that  $S = 2S$  implies that indeed  $f \in \mathbb{F}_2[X]$ . Next, we need to show that there is a  $g$  such that  $X^k - 1 = f f^* g$ . This is equivalent to proving that  $f$  and  $f^*$  have no common zeroes. Since the zeroes of  $f$  and  $f^*$  are  $\zeta^S$  and  $\zeta^{-S}$ , respectively, we have to show  $S \cap -S = \emptyset$ .

This can be seen as follows. An element in  $\mathbb{Z}/k\mathbb{Z}$  is represented in binary as

$$c_0 + c_1 2 + \dots + c_{2a} 2^{2a}$$

with all  $c_j \in \{0, 1\}$ . Moreover, this representation is unique except for  $0 = k = 1 + 2 + 2^2 + \dots + 2^{2a}$ . In this notation, multiplication by 2 equals a shift. So multiplying a nonzero element of  $\mathbb{Z}/k\mathbb{Z}$  by 2 fixes the number of nonzero  $c_i$ ’s. Similarly, multiplying a nonzero element by  $-1$  corresponds to  $c_i \mapsto 1 - c_i$  for all  $i$ . Observe that any element in  $G$  has  $\geq a + 1$  coefficients  $c_i = 0$ . Hence, the same is true for the elements of  $S$ . It follows that the elements of  $-S$  have  $\leq a$  coefficients  $c_i = 0$ . So  $S \cap -S = \emptyset$ .

Note that  $0 \notin S \cup -S$ , hence  $X^n - 1 = f \cdot f^* \cdot g$  with  $g(1) = 0$ . This shows that  $f^2 g$  has  $\zeta^0, \zeta^1, \dots, \zeta^{\delta-2}$  as zeroes, which finishes the proof.  $\square$

*Remark 3.3:* The proof presented here constructs a sequence of cyclic self-dual  $[2k, k, d(k)]$ -codes  $\mathcal{C}_k$  such that

$$\limsup_{k \rightarrow \infty} \frac{d(k)}{\sqrt{2k}} \geq \lim_{a \rightarrow \infty} \frac{2^{a+1}}{\sqrt{2^{2a+2} - 2}} = 1.$$

*Remark 3.4:* The code constructed in our proof of Theorem 1.1 depends only on (the  $\text{Gal}(\overline{\mathbb{F}_2}/\mathbb{F}_2)$ -orbit of) the chosen primitive  $k$ th root of unity  $\zeta$ . A different choice results in an equivalent code, with the equivalence given by an automorphism of rings

$$\mathbb{F}_2[X]/(X^n - 1) \xrightarrow{\cong} \mathbb{F}_2[X]/(X^n - 1) : X \mapsto X^m$$

for some integer  $m$  with  $\text{gcd}(m, n) = 1$ .

*Example 3.5:* For  $a = 1, 2, 3$ , we discuss the binary cyclic self-dual codes constructed above.

The case  $a = 1$  yields a  $[14, 7]$ -code. It is shown in [6] that there is (up to equivalence) a unique self-dual code of length 14, and this code has distance 4. This implies that the BCH-bound  $\delta = 4$ , which we have in this case, is sharp.

For  $a = 2$ , we obtain a code of length 62. The minimal distance of any binary self-dual code of length 62 is bounded by 12, and examples of such  $[62, 31, 12]$ -codes were constructed by Harara [4]. Harara’s example is not a cyclic code, and in fact, it follows from the calculations in [10] that the largest minimal distance of a binary cyclic self-dual  $[62, 31]$ -code is 10. Using MAGMA, we found that our example has distance  $d = 8$ , which

is not best possible, but which equals the BCH-bound  $\delta = 8$  in the present case.

For  $a = 3$ , our construction yields a code of length 254, and the BCH-bound gives  $d \geq \delta = 16$ . Using MAGMA and the idea sketched in Remark 3.2, it turns out that in fact the code obtained here is [254, 127, 28]. In particular, the BCH-bound is far from optimal in this example.

The results are summarized in the following table.

$a$	1	2	3
$k$	7	31	127
$n$	14	62	254
$\delta$	4	8	16
$d$	4	8	28

The ideas used above can be used to construct more general (binary) cyclic codes with reasonably large minimal distance. The precise result is as follows.

**Proposition 3.6:** There exist cyclic  $[n_i, k_i, d_i]$ -codes such that  $(n_i)_{i \geq 1}$  is strictly increasing and neither of  $d_i \log(n_i)/n_i$  and  $k_i/n_i$  has 0 as a limit point.

*Proof:* Take an integer  $a > 1$  and put  $n := 2^a - 1$  and  $\delta := \lfloor 2^{a-1}/a \rfloor$ . Let  $\zeta \in \overline{\mathbb{F}_2}$  be a primitive  $n$ th root of unity and identify  $\langle \zeta \rangle \cong \mathbb{Z}/n\mathbb{Z}$ . In  $\mathbb{Z}/n\mathbb{Z}$ , we consider the subset  $G = \{b \bmod n \mid b \text{ odd and } 1 \leq b \leq \delta\}$  and put  $S = \bigcup_{i \geq 0} 2^i G$  as before. By the choice of  $n$ , the order of 2 in the group of units  $(\mathbb{Z}/n\mathbb{Z})^\times$  equals  $a$ . It follows that  $\#S \leq a \cdot \lceil \delta/2 \rceil \leq 2^{a-2}$ . We let  $C_a$  be the binary cyclic code with generator  $f := \prod_{s \in S} (X - \zeta^s) \in \mathbb{F}_2[X]$ . The classical BCH-bound (see, for example, [5]) implies that the distance of  $C_a$  is  $d \geq \delta + 1$ . The dimension  $k = n - \deg(f) = n - \#S$  of this code is then at least  $n - 2^{a-2} = 3 \cdot 2^{a-2} - 1$ . From this, the result follows.  $\square$

**Example 3.7:** Using MAGMA, we tested the construction in the preceding proof, for  $2 \leq a \leq 9$ . Note that for  $a = 3$ , the cyclic code obtained in this way is the classical [7, 4, 3] Hamming code. The results are presented in the following table.

$a$	$n = 2^a - 1$	$\delta = \lfloor 2^{a-1}/a \rfloor$	$k$	$d$
2	3	1	1	3
3	7	1	4	3
4	15	2	11	3
5	31	3	21	5
6	63	5	45	7
7	127	9	92	11
8	255	16	191	17
9	511	28	385	29

The table shows that for these particular examples the BCH-bound is very close to the actual minimal distance. In the cases with  $n \leq 255$ , MAGMA calculated this distance essentially instantaneously; for  $n = 511$ , it took a few hours.

#### IV. UPPER BOUND

In this section, we prove Theorem 1.2 in the special case of binary cyclic self-dual codes. Basically, we follow the original argument presented in [2]; however, we exploit the extra condition that our codes are cyclic.

Every codeword  $c$  in a self-dual code satisfies  $c \cdot c = 0$ . Hence, in a binary self-dual code,  $\text{wt}(c)$  is even for all  $c$ .

**Lemma 4.1:** A binary cyclic self-dual code is of type I; i.e., it contains a word  $c$  with  $\text{wt}(c) \equiv 2 \pmod 4$ .

*Proof:* Let  $\mathcal{C}$  be a binary cyclic self-dual code. The generator  $f = \sum_{j=0}^k a_j X^j$  satisfies  $f \cdot f^* = X^{2k} + 1$ . Considering all terms of degree  $\leq k$  in the product  $f \cdot f^*$ , this implies

$$\sum_{0 \leq i < j \leq k} a_i a_j X^{k+i-j} = 1.$$

Write  $w := \text{wt}(f)$ , which is an even number since  $f$  generates a self-dual code. In the sum above,  $w(w-1)/2$  products  $a_i a_j = 1$  appear, and since the sum equals 1, it follows that  $w(w-1)/2$  is odd. Hence,  $w \equiv 2 \pmod 4$ .  $\square$

The lemma implies that for a binary cyclic self-dual  $[2k, k]$ -code  $\mathcal{C}$ , the map

$$\mathcal{C} \longrightarrow 2\mathbb{Z}/4\mathbb{Z} \cong \mathbb{F}_2, \quad c \mapsto \text{wt}(c) \pmod 4$$

is surjective. In fact, it is well-known and easily seen that this map is linear. Its kernel is denoted as  $\mathcal{C}^{(0)}$ . This is by construction a binary cyclic  $[2k, k-1]$ -code contained in  $\mathcal{C}$ , so its generator equals  $(X-1) \cdot f$  with  $f$  the generator of  $\mathcal{C}$ . Recall that the shadow  $\mathcal{S}$  of  $\mathcal{C}$  is defined as  $\mathcal{S} := \mathcal{C}^{(0)\perp} \setminus \mathcal{C}$ . The shadow is cyclic, but not linear. Since  $\mathcal{C}^{(0)\perp}$  is the cyclic code with generator  $f/(X-1)$ , the shadow consists of all multiples of  $f/(X-1)$ , which are *not* multiples of  $f$ .

Using the MacWilliams identity and some invariant theory, the following formula for the weight enumerators  $W_{\mathcal{C}}, W_{\mathcal{S}}$  of a binary self-dual  $[n, k]$ -code of type I and its shadow are derived.

**Lemma 4.2:** There are integers  $a_0, \dots, a_{\lfloor \frac{n}{8} \rfloor}$  such that

$$W_{\mathcal{C}}(X, Y) = \sum_{i=0}^{\lfloor \frac{n}{8} \rfloor} a_i (X^2 + Y^2)^{k-4i} (X^2 Y^2 (X^2 - Y^2)^2)^i$$

and

$$W_{\mathcal{S}}(X, Y) = \sum_{i=0}^{\lfloor \frac{n}{8} \rfloor} 2^{k-6i} a_i (XY)^{k-4i} (Y^4 - X^4)^{2i}.$$

*Proof:* See [2] or [13].  $\square$

We now prove Theorem 1.2 for cyclic codes. So suppose  $\mathcal{C}$  is a binary cyclic self-dual  $[n, k, d]$ -code with  $n > 2$ . Fix integers  $\ell$  and  $\delta$  such that  $n = 10\ell + 2\delta$ , with  $-3 \leq \delta \leq 1$ . Note that  $n > 2$  implies  $\ell > 0$ . Our aim is to show that  $d \leq 2\ell$ , so assume this is not the case. Since  $d$  is even, this implies  $d \geq 2\ell + 2$ . Hence

$$W_{\mathcal{C}} = X^n + Y^n + \sum_{i=2\ell+2}^{n-2\ell-2} A_i X^i Y^{n-i}.$$

Applying Lemma 4.2 yields integers  $a_i$  such that

$$\begin{aligned} X^n + Y^n + \sum_{i=2\ell+2}^{n-2\ell-2} A_i X^i Y^{n-i} &= \sum_{i=0}^{\lfloor \frac{n}{8} \rfloor} a_i (X^2 + Y^2)^{k-4i} (X^2 Y^2 (X^2 - Y^2)^2)^i. \end{aligned}$$

To simplify notation take  $X = 1$  and  $Y^2 = y$ . Modulo  $y^{\ell+1}$  the above equality reads

$$1 \equiv \sum_{i=0}^{\lfloor \frac{n}{8} \rfloor} a_i(1+y)^{k-4i}(y(1-y)^2)^i \pmod{y^{\ell+1}}.$$

The Bürmann–Lagrange formula (see [15]) implies in particular

$$a_\ell = -\frac{k}{\ell} \cdot (\text{coeff. of } y^{\ell-1} \text{ in } (1-y^2)^{-\ell-\delta-1}(1-y)^{-\ell+\delta+1}).$$

For  $d = 2$ , the code  $\mathcal{C}$  equals the binary repetition code with generator  $X^k - 1$ ; in this case, the bound follows since we assume  $n > 2$ . We now assume  $d > 2$ . Then, the binary cyclic self-dual codes such that  $\ell \leq 4$  are easily determined (compare [10]) and the theorem holds in these cases. Now assume  $\ell \geq 5$ , which implies that  $-\ell - \delta - 1$  and  $-\ell + \delta + 1$  are negative. Since the Taylor coefficients of  $\frac{1}{1-y^2}$  are nonnegative and of  $\frac{1}{1-y}$  strictly positive, it follows that  $a_\ell < 0$ .

Write

$$W_S(X, Y) = \sum_{i=0}^n B_i X^i Y^{n-i}.$$

Observe that  $B_i = 0$  if  $i < d/2$  since otherwise adding a nonzero word of the shadow of weight  $< d/2$  to its shift would give a word in  $\mathcal{C}$  of weight  $< d$ .

We now distinguish two possibilities. First, if  $d > 2\ell + 2$ , then we have shown  $B_0 = B_1 = \dots = B_{\ell+1} = 0$ , so

$$W_S \equiv 0 \pmod{X^{\ell+2}}.$$

In particular, using the formula for  $W_S$  given in Lemma 4.2 and the fact that  $k - 4\ell \leq \ell + 1$ , it follows that  $a_\ell = 0$ . This contradiction shows that  $d = 2\ell + 2$ .

A word in  $\mathcal{S}$  of weight  $d/2$  would give, by shifting and using that  $\mathcal{C}$  has minimal distance  $d$ , a partition of  $n$  in pairwise disjoint subsets of cardinality  $d/2$ . So if such a word exists, then  $d/2 = \ell + 1$  divides  $n = 10\ell + 2\delta$ . This is not the case if  $n > 144$  and so we get  $B_{d/2} = 0$  whenever  $n > 144$ . So also in this case, one obtains  $B_0 = B_1 = \dots = B_{\ell+1} = 0$ , which as is shown above yields the contradiction  $a_\ell = 0$ .

It remains to consider the cases where  $10\ell + 2\delta = n \leq 144$  is a multiple of  $\ell + 1$ , which is easily done; in fact, all but the cases  $n = 144$  and  $n = 126$  are given in [10]. For  $n = 144$ , the only binary cyclic self-dual code is the repetition code which has  $d = 2$ . In case  $n = 126$ , we have used MAGMA to verify the result (compare the example below).  $\square$

*Example 4.3:* For length  $n = 126$ , any binary cyclic self-dual code has a generator  $f^2g$  in which  $f \cdot f^* \cdot g = X^{63} + 1$ . This

condition implies that  $f$  has degree  $3m$  with  $0 \leq m \leq 9$ . Up to isomorphisms of  $\mathbb{F}_2[X]/(X^{126} - 1)$  given by  $X \mapsto X^a$  for some  $a$  with  $\gcd(a, 126) = 1$ , this yields 86 codes. All these codes turn out to have minimal distance  $\leq 14$ , and all even numbers  $d$  with  $2 \leq d \leq 14$  appear as minimal distance for at least one of these codes.

## REFERENCES

- [1] G. Castagnoli, J. L. Massey, P. A. Schoeller, and N. von Seemann, "On repeated root cyclic codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 2, pp. 337–342, Mar. 1991.
- [2] J. H. Conway and N. J. A. Sloane, "A new upper bound on the minimal distance of self-dual codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 6, pp. 1319–1333, Nov. 1990.
- [3] P. Gaborit, "Tables of self-dual codes," [Online]. Available: [http://www.unilim.fr/pages\\_perso/philippe.gaborit/SD/index.html](http://www.unilim.fr/pages_perso/philippe.gaborit/SD/index.html)
- [4] M. Harada, "Construction of an extremal self-dual code of length 62," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1232–1233, Jul. 1999.
- [5] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.
- [6] V. Pless, "A classification of self-orthogonal codes over  $\text{GF}(2)$ ," *Discrete Math.*, vol. 3, pp. 209–249, 1972.
- [7] J. H. van Lint, "Repeated-root cyclic codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 2, pp. 343–345, Apr. 1991.
- [8] F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, "Good self dual codes exist," *Discrete Math.*, vol. 3, pp. 153–162, 1972.
- [9] G. Nebe, E. M. Rains, and N. J. A. Sloane, *Self-Dual Codes and Invariant Theory*. New York: Springer-Verlag, 2006.
- [10] C.-S. Nedeloaia, "Weight distribution of cyclic self-dual codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 6, pp. 1582–1591, Jun. 2003.
- [11] E. M. Rains and N. J. A. Sloane, "Self-dual codes," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. New York: Elsevier, 1998, pp. 177–294.
- [12] S. Roman, *Coding and Information Theory*. New York: Springer-Verlag, 1992.
- [13] N. J. A. Sloane and J. G. Thompson, "Cyclic self-dual codes," *IEEE Trans. Inf. Theory*, vol. 1-29, no. 3, pp. 364–366, Jun. 1983.
- [14] H. Stichtenoth, "Transitive and self-dual codes attaining the Tsfasman-Vladut-Zink bound," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2218–2224, May 2006.
- [15] E. T. Whittaker and G. N. Watson, *A Course of Modern Analysis*, 4th ed. Cambridge, U.K.: Cambridge Univ. Press, 1963.

**Bas Heijne** studied mathematics at the University of Groningen, Groningen, The Netherlands. He wrote his M.S. thesis on the subject of cyclic self-dual codes in 2007. Currently, he is working towards the Ph.D. degree in mathematics at the University of Groningen, working on a project on elliptic curves over function fields.

**Jaap Top** studied mathematics at the University of Utrecht, Utrecht, The Netherlands. He wrote his M.S. thesis in 1984 on the subject of Néron's construction of elliptic curves of high rank and he received the Ph.D. degree in 1989 with a dissertation on *Hecke L-series related with algebraic cycles or with Siegel modular forms*.

He held positions at Queen's University, Kingston, ON, Canada and at the Erasmus University, Rotterdam, The Netherlands. Since 1992, he has been working in the field of arithmetic algebraic geometry at the Institute for Mathematics and Computer Science (IWI), University of Groningen, Groningen, The Netherlands.