On the Triple-Error-Correcting Cyclic Codes with Zero Set $\{1, 2^i + 1, 2^j + 1\}$

Vincent Herbert[1] and Sumanta Sarkar[2]

[1]CRI INRIA Paris-Rocquencourt
Domaine de Voluceau - Le Chesnay - 78153 - B.P. 105 - France

[2]Department of Computer Science
University of Calgary, Canada
Vincent.Herbert@inria.fr sarkas@ucalgary.ca

Abstract. We consider a class of 3-error-correcting cyclic codes of length $2^m - 1$ over the two-element field $\mathbb{F}_2$. The generator polynomial of a code of this class has zeroes α, α^{2^i+1} and α^{2^j+1}, where α is a primitive element of the field $\mathbb{F}_{2^m}$. In short, $\{1, 2^i + 1, 2^j + 1\}$ refers to the zero set of these codes. Kasami in 1971 and Bracken and Helleseth in 2009, showed that cyclic codes with zeroes $\{1, 2^\ell + 1, 2^{3\ell} + 1\}$ and $\{1, 2^\ell + 1, 2^{2\ell} + 1\}$ respectively are 3-error correcting, where $\gcd(\ell, m) = 1$. We present a sufficient condition so that the zero set $\{1, 2^\ell + 1, 2^{p\ell} + 1\}$, $\gcd(\ell, m) = 1$ gives a 3-error-correcting cyclic code. The question for $p > 3$ is open. In addition, we determine all the 3-error-correcting cyclic codes in the class $\{1, 2^i + 1, 2^j + 1\}$ for $m < 20$. We investigate their weight distribution via their duals and observe that they have the same weight distribution as 3-error-correcting BCH codes for $m < 14$. Further our experiment shows that these codes are not equivalent to the 3-error-correcting BCH code in general. We also study the Schaub algorithm which determines a lower bound of the minimum distance of a cyclic code. We introduce a pruning strategy to improve the Schaub algorithm. Finally we study the cryptographic property of a Boolean function, called spectral immunity which is directly related to the minimum distance of cyclic codes over $\mathbb{F}_{2^m}$. We apply the improved Schaub algorithm in order to find a lower bound of the spectral immunity of a Boolean function related to the zero set $\{1, 2^i + 1, 2^j + 1\}$.

Keywords: Cyclic codes; Weight enumerator; Zero set; Dual codes; Schaub algorithm; Cyclotomic cosets; Spectral immunity.

1 Introduction

The family of cyclic codes is a well known class of error-correcting codes. We deal with 3-error-correcting binary cyclic codes and their duals. Let $\mathbb{F}_{2^m}$ be the extension field of degree m of the two-element field $\mathbb{F}_2$ and n be an odd integer. Consider a binary cyclic code C of length n and let α be a primitive n-th root of

unity in $\mathbb{F}_{2^m}$. One can describe C as a principal ideal, in the ring $\mathbb{F}_2[X]/(X^n-1)$, with a so-called *generator polynomial* g over $\mathbb{F}_2$, where $n \mid (2^m-1)$. Therefore, the zeroes of g can be used to define C. The *zero set* Z of C is the set of exponents i of the primitive element α such that α^i is a root of g. Note that if z is a root of g, so is z^{2^i} for all i. In other words, Z is a union of 2-cyclotomic cosets modulo n. Most of the time, Z is shortly described by the list of distinct representatives of these cyclotomic cosets. If the length of the code is 2^m-1, *i.e.* α is a primitive element of $\mathbb{F}_{2^m}$, then the code is said to be *primitive*.

BCH codes form an important class of cyclic codes. A cyclic code generated by $g(X) = \mathrm{lcm}(\{M^{(i)}(X)\}_{i\in I})$ where $M^{(i)}(X)$ is the minimal polynomial of α^i with respect to $\mathbb{F}_2$ and where I is a set of $\delta-1$ consecutive integers is a BCH code with a *designed distance* δ. In particular, if $I = \{1, 2, \ldots, \delta-1\}$, then the BCH code is said to be *narrow sense*.

Kasami [Kas71] introduced some classes of primitive binary 3-error-correcting cyclic codes (*i.e.* their minimum distance is 7) similar to 3-error-correcting BCH codes, in the sense that their zero set consists of the union of 3 cyclotomic cosets. These codes have a dimension $k \geq n-3m$. This also means that, these codes asymptotically have a high information rate and moreover, their minimum distance is optimal. Indeed, Hamming bound implies that long cyclic codes defined by τ distinct cyclotomic cosets have an error-correcting capacity $t \leq \tau$. One of those classes is $\{1, 2^\ell+1, 2^{3\ell}+1\}$ with $\gcd(\ell, m) = 1$ and m odd. Later Bracken and Helleseth in [BH09] discovered the class $\{1, 2^\ell+1, 2^{2\ell}+1\}$ with $\gcd(\ell, m) = 1$.

In this article, we investigate the class $\{1, 2^i+1, 2^j+1\}$ for $i, j > 1$, $i \neq j$. We attempt to generalize the subclass $\{1, 2^\ell+1, 2^{3\ell}+1\}$ and $\{1, 2^\ell+1, 2^{2\ell}+1\}$ with $\gcd(\ell, m) = 1$ to $\{1, 2^\ell+1, 2^{p\ell}+1\}$ with $\gcd(\ell, m) = 1$ and $p > 1$.

Another class of 3-error-correcting cyclic codes with zero set $\{1, 2^{\ell-1}+1, 2^\ell+1\}$ for $m = 2\ell+1$ was introduced in [MS83]. A question was raised whether these codes have the same weight distribution as the BCH code. Later it was proved to be true in [vDV96]. They showed that these dual of these codes have the same weight distribution as the dual of the BCH codes. This motivates us to study the weight distribution of the general class $\{1, 2^i+1, 2^j+1\}$. By computation up to $m < 14$, we check that the dual of all the 3-error-correcting cyclic codes that has zero $\{1, 2^i+1, 2^j+1\}$ and which are not BCH, have the same weight distribution as the dual of the 3-error-correcting BCH code.

Further we study the minimum distance of their duals over $\mathbb{F}_2$ and over $\mathbb{F}_{2^m}$. In the literature, numerous theoretical lower bounds on the minimum distance of cyclic codes are known (*e.g.* [BR60,HT72,Roo83,vLW86,Wol89]). Schaub [Sch88] has investigated an algorithmic approach to compute a lower bound on the minimum distance of a given cyclic code. This idea is particularly efficient for the codes which have few cyclic subcodes. We improve time-complexity of the Schaub algorithm using a *pruning criteria* based on BCH bound in order to be able to manage codes with more cyclic subcodes. We compare the Schaub bound with the Hartmann-Tzeng bound and the true minimum distance of duals of codes with the zero set $\{1, 2^i+1, 2^j+1\}$. Augot and Levy-dit-Vehel [AL96] had also applied the Schaub algorithm to find a lower bound of the minimum distance

of the dual of BCH codes and found this algorithm gives better results than Ross bound and Weil bound on the dual of BCH codes. Our numerical results show a similar behavior of the minimum distance of the duals of 3-error-correcting cyclic codes in the class $\{1, 2^i + 1, 2^j + 1\}$ for $i, j > 1$, $i \neq j$.

In the end we study the spectral immunity of a Boolean function which is a cryptographic property. High value of spectral immunity is a necessary condition in order to resist algebraic cryptanalysis of filter generators. In [HR11] the connection between spectral immunity and minimum distance of a cyclic code was shown. The spectral immunity of a Boolean function f over $\mathbb{F}_{2^m}$ (in univariate form) is equal to the minimal weight of the 2^m-ary cyclic code of length $n = 2^m - 1$ generated by $\gcd(f(z), z^n + 1)$ or $\gcd(f(z) + 1, z^n + 1)$. In this paper, we find a lower bound on the spectral immunity of the Boolean function $\mathrm{Tr}(g)$ using the Schaub algorithm, where g is the generator polynomial of the code with the zero set $\{1, 2^i + 1, 2^j + 1\}$.

In summary, we have two major contributions in this paper. First, we present a sufficient condition for which the zero set $\{1, 2^\ell+1, 2^{p\ell}+1\}$, where $gcd(\ell, m) = 1$ will give a 3-error-correcting code of length $2^m - 1$. Secondly, we improve the Schaub algorithm which determines a lower bound of the minimum distance of a cyclic code.

2 Triple-error-correcting cyclic code with the zero set $\{1, 2^i + 1, 2^j + 1\}$

Let $Z = \{a, b, c\}$ be the zero set of a cyclic code C, where a, b and c are the representatives of distinct 2-cyclotomic cosets. Then, the parity check matrix of C is a $(3m \times n)$ matrix over $\mathbb{F}_2$ of form:

$$\mathcal{H} = \begin{pmatrix} 1 & \alpha^a & \alpha^{2a} & \dots & \alpha^{(n-1)a} \\ 1 & \alpha^b & \alpha^{2b} & \dots & \alpha^{(n-1)b} \\ 1 & \alpha^c & \alpha^{2c} & \dots & \alpha^{(n-1)c} \end{pmatrix},$$

where each entry in the matrix is represented as an m-bit column vector with respect to a fixed $\mathbb{F}_2$-basis of $\mathbb{F}_{2^m}$. Then, the code corresponding to Z is the binary kernel of $\mathcal{H}$.

In Table 1, we present the list of known zero sets that correspond to 3-error-correcting cyclic codes of length $2^m - 1$.

2.1 Triple-error-correcting cyclic code with the zero set $\{1, 2^\ell + 1, 2^{p\ell} + 1\}$

The zero sets considered in [Kas71] and [BH09] are of the form $\{1, 2^\ell + 1, 2^{p\ell} + 1\}$, where $p = 3$ and $p = 2$ respectively. Therefore, it will be interesting to characterize p for which the zero set $\{1, 2^\ell + 1, 2^{p\ell} + 1\}$ always gives a 3-error-correcting cyclic code.

In this section, we present a sufficient condition for the zero set $Z = \{1, 2^\ell + 1, 2^{p\ell} + 1\}$ with $\gcd(\ell, m) = 1$ corresponds to a 3-error-correcting cyclic code.

Zero Set	Conditions	References
$\{1, 2^\ell + 1, 2^{3\ell} + 1\}$	$\gcd(\ell, m) = 1$ m odd	[Kas71]
$\{2^\ell + 1, 2^{3\ell} + 1, 2^{5\ell} + 1\}$	$\gcd(\ell, m) = 1$ m odd	[Kas71]
$\{1, 2^{\ell-1} + 1, 2^\ell + 1\}$	$m = 2\ell + 1$ m odd	[MS83]
$\{1, 2^\ell + 1, 2^{\ell+2} + 3\}$	$m = 2\ell + 1$ m odd	[CGG$^+$00]
$\{1, 2^\ell + 1, 2^{2\ell} + 1\}$	$\gcd(\ell, m) = 1$ any m	[BH09]

Table 1. Known classes of 3-error-correcting cyclic codes of length $2^m - 1$

Lemma 1. *Let d be the minimum distance of the cyclic code C given by the zero set $Z = \{1, 2^\ell + 1, 2^{p\ell} + 1\}$ with $\gcd(\ell, m) = 1$ of length $n = 2^m - 1$. Then $d = 5$ or $d = 7$ and there exists a codeword of weight $d + 1$.*

Proof. It is known from [Cha98, Theorem 4.2] that cyclic codes with $Z = \{1, a\}$ have minimum distance 5 if and only if the mapping $x \mapsto x^a$ is almost perfect nonlinear (APN). Consequently, if $Z = \{1, a, b\}$ and if $x \mapsto x^a$ is APN, then the code has minimum distance at least 5 since it is a subcode of code with zero set $\{1, 2^\ell + 1\}$. The mapping $x \mapsto x^{2^\ell+1}$ is APN (*e.g.* [Dob99]) if and only if $\gcd(\ell, m) = 1$. Therefore, the minimum distance of C is at least 5. Further, the code C contains the cyclic Reed-Muller code $\mathcal{R}^*(m-3, m)$ (cf. [Bla02]). Indeed, $\mathcal{R}^*(m-3, m)$ has zero set $\cup_{i\in\mathbb{N}}\{2^i + 1\}$. $\mathcal{R}^*(m-3, m)$ has minimum distance $2^{m-(m-3)} = 7$. Hence, we are ensured that $5 \leq d \leq 7$.

Moreover, by Corollary 17 of [MS83, page 237], the minimum distance d is necessarily odd and there is a codeword of weight $d + 1$. □

Theorem 1. *Consider C, the cyclic code of length $2^m - 1$ with zero set $Z = \{1, 2^\ell + 1, 2^{p\ell} + 1\}$ where $\gcd(\ell, m) = 1$. The minimum distance of C is 7 if for all $\beta \in \mathbb{F}_{2^m}^*, \gamma \in \mathbb{F}_{2^m}$,*

$$x^{2^{p\ell}+1} \sum_{i=0}^{p-1} (\beta x^{-(2^\ell+1)})^{2^{i\ell}} = \gamma \tag{1}$$

have less than or equal to 5 solutions for x in $\mathbb{F}_{2^m}^*$.

The proof is given in Appendix A. We now apply Theorem 1 for $p = 2$ and $p = 3$ to show that $\{1, 2^\ell + 1, 2^{2\ell} + 1\}$ [BH09] and $\{1, 2^\ell + 1, 2^{3\ell} + 1\}$ [Kas71] are

two zero sets that give 3-error-correcting cyclic code in Theorem 2 and Theorem 3 respectively.

Theorem 1 opens up the scope of getting new p for which $\{1, 2^\ell + 1, 2^{p\ell} + 1\}$ gives a 3-error-correcting cyclic code by investigating Equation 1 for $p > 3$ (see Remark 1).

Below we present a consequence of a result given in [Blu04].

Lemma 2. *The equation of the form* $x^{2^\ell+1} + rx^{2^\ell} + tx + s = 0$ *does not have more than three solutions when* $\gcd(\ell, m) = 1$ *for all* $r, s, t \in \mathbb{F}_{2^m}$.

Theorem 2. *For* $p = 2$, *the code* $\{1, 2^\ell + 1, 2^{p\ell} + 1\}$ *with* $\gcd(\ell, m) = 1$ *is a 3-error-correcting cyclic code.*

Proof. For $p = 2$, the equation (1) becomes

$$\begin{aligned}\gamma &= x^{2^{2\ell}+1}(\beta x^{-(2^\ell+1)} + \beta^{2^\ell} x^{-2^\ell(2^\ell+1)}),\\ &= \beta x^{2^{2\ell}-2^\ell} + \beta^{2^\ell} x^{1-2^\ell},\\ &= \beta x^{2^\ell(2^\ell-1)} + \beta^{2^\ell} x^{-(2^\ell-1)}.\end{aligned}$$

Let us remind $\beta \neq 0$. Since $\gcd(\ell, m) = 1$ then $\gcd(2^\ell - 1, 2^m - 1) = 1$ and thus $x \mapsto x^{2^\ell-1}$ is a bijection. Then transforming $x = x^{2^\ell-1}$ we get:

$$\begin{aligned}\beta x^{2^\ell} + \beta^{2^\ell} x^{-1} &= \gamma,\\ x^{2^\ell+1} + \frac{\gamma}{\beta} x + \beta^{2^\ell-1} &= 0. \qquad (2)\end{aligned}$$

Lemma 2 tells that (2) does not have more than three solutions. Therefore, the zero set $\{1, 2^\ell + 1, 2^{2\ell} + 1\}$ gives a 3-error-correcting cyclic code. □

Theorem 3. $\{1, 2^\ell + 1, 2^{p\ell} + 1\}$ *is a 3-error-correcting cyclic code if* $p = 3$, m *is odd and* $\gcd(\ell, m) = 1$.

Proof. For $p = 3$, the equation (1) becomes:

$$\begin{aligned}\gamma = \; & x^{2^{3\ell}+1}(\beta x^{-\left(2^\ell+1\right)} + \beta^{2^\ell} x^{-2^\ell\left(2^\ell+1\right)}\\ & +\beta^{2^{2\ell}} x^{-2^{2\ell}\left(2^\ell+1\right)}),\\ = \; & \beta x^{2^\ell\left(2^{2\ell}-1\right)} + \beta^{2^\ell} x^{\left(2^{2\ell}-1\right)\left(2^\ell-1\right)}\\ & +\beta^{2^{2\ell}} x^{1-2^{2\ell}}.\end{aligned}$$

Since m is odd and $\gcd(\ell, m) = 1$, $\gcd(2^{2\ell} - 1, 2^m - 1) = 1$ and so $x \mapsto x^{2^{2\ell}-1}$ is a bijection. Let us recall $\beta \neq 0$. Now replacing x by $x^{2^{2\ell}-1}$, we obtain:

$$\begin{aligned}\beta x^{2^\ell} + \beta^{2^\ell} x^{(2^\ell-1)} + \beta^{2^{2\ell}} x^{-1} &= \gamma,\\ x^{2^\ell+1} + \beta^{2^\ell-1} x^{2^\ell} + \frac{\gamma}{\beta} x + \beta^{2^{2\ell}-1} &= 0. \qquad (3)\end{aligned}$$

Then, from Lemma 2, we get that (3) can not have more than three solutions. Therefore, $\{1, 2^\ell + 1, 2^{3\ell} + 1\}$ is a 3-error-correcting cyclic code. □

Remark 1. Consider m odd. In that case, $\gcd(2^\ell+1, 2^m-1) = 1$ and so $x \mapsto x^{2^\ell+1}$ is a bijection. If we assume p is odd, then applying the transformation $x \mapsto x^{-(2^\ell+1)}$, (1) becomes :

$$\sum_{i=0}^{p-1} (\beta x)^{2^{i\ell}} = \gamma x^{2^{(p-1)\ell}+2^{(p-2)\ell}+\ldots+1} \tag{4}$$

Then, it is interesting to find out for which values of p, this equation does not have more than 5 nonzero solutions in $\mathbb{F}_{2^m}$.

2.2 Finding 3-error-correcting cyclic codes with the zero set $\{1, 2^i+1, 2^j+1\}$ by computation

We use an implementation of Chose-Joux-Mitton algorithm [CJM02] to look for words of weight $w = 6$ in codes with a zero set $\{1, 2^i+1, 2^j+1\}$ for $m < 20$ and for all i, j. In Table 4, we provide the exhaustive list of triple-error-correcting cyclic codes up to $m = 13$. This algorithm has time complexity $\mathcal{O}(n^{\frac{w}{2}}) = \mathcal{O}(n^3)$ and space complexity $\mathcal{O}(n^{\lceil \frac{w}{4} \rceil}) = \mathcal{O}(n^2)$. From the foundations, this algorithm is employed to find low-weight polynomial multiples in stream cipher cryptanalysis. In our context, it is an efficient algorithm to search codewords of weight smaller than 8. We notice that each of those zero sets $\{1, 2^i+1, 2^j+1\}$ can be written in the form $\{1, 2^\ell+1, 2^{p\ell}+1\}$, where $p = 2$ or $p = 3$ up to $m < 20$. Therefore, the class $\{1, 2^i+1, 2^j+1\}$ of 3-error-correcting cyclic code is completely described by two known classes [Kas71,BH09] for $m < 20$.

2.3 The weight distributions of the 3-error-correcting cyclic codes with the zero set $\{1, 2^i+1, 2^j+1\}$

Weight	# Codewords
0	1
$\frac{N \pm \sqrt{8N}}{2}$	$\frac{(N^2-3N+2)(N \mp \sqrt{8N})}{96}$
$\frac{N \pm \sqrt{2N}}{2}$	$\frac{(5N^2+3N-8)(N \mp \sqrt{2N})}{24}$
$\frac{N}{2}$	$\frac{9N^3-3N^2+10N-16}{16}$

Table 2. Weight distribution of dual of 3-error-correcting BCH code of length 2^m-1, odd m, $N = 2^m$.

Weight distribution of a linear code C and its dual code $C^\perp$ are related by the MacWilliams identity [MS83]. Therefore, knowing the weight distribution of

$C^\perp$ one can obtain the weight distribution of C. The dual code $C^\perp$ of the code C is the annihilator of C. If C is cyclic, then $C^\perp$ is also a cyclic code. We denote the zero set of $C^\perp$ as $Z^\perp$. The generator polynomial of $C^\perp$ is the reciprocal polynomial of $h(X) = (X^n - 1)/g(X)$. Its roots are the inverses of the roots of h. In other words, it is established that $z \in Z^\perp$ if and only if $n - z \notin Z$.

The weight distribution of the dual of 3-error-correcting BCH code for odd m was determined in [Kas69] and we present it in Table 2. However, for even m, explicit formula for the weight distribution of the dual of the BCH code is not known. In [vDV96], it was shown that the dual of the code $\{1, 2^{\ell-1} + 1, 2^\ell + 1\}$ has the same weight distribution as the dual of BCH code. Then from the MacWilliams identity, the code $\{1, 2^{\ell-1} + 1, 2^\ell + 1\}$ has the same weight distribution as the BCH code. This motivated us to find if the code $\{1, 2^i+1, 2^j+1\}$ has the same weight distribution as the BCH code. As shown in [vDV96] we also study the weight distribution of these codes via their duals. Since these duals have fewer codewords, it is possible to compute the weight distribution for higher extension degrees. For this we implement a concurrent algorithm. We first compute the codewords using Gray coding. After that, we determine their Hamming weights with an hardware-accelerated instruction from the SSE4 instruction set.

For $m \leq 13$, we check that duals of the 3-error-correcting cyclic code with zero set $\{1, 2^i + 1, 2^j + 1\}$ have the same weight distribution as the duals of BCH code as given in Table 2. Therefore, we raise the following question.

Problem 1. Prove or disprove that all the 3-error-correcting cyclic codes with the zero set $\{1, 2^i + 1, 2^j + 1\}$ of length $2^m - 1$ have the same weight distribution as the 3-error-correcting BCH code of length $2^m - 1$.

2.4 Non-equivalence of the 3-error-correcting cyclic codes with the zero set $\{1, 2^i + 1, 2^j + 1\}$ with the 3-error-correcting BCH code

In [MS83], it was also asked whether the cyclic code with the zero set $\{1, 2^{\ell-1} + 1, 2^\ell + 1\}$ is equivalent to the 3-error-correcting BCH code. They conjectured that they are not. Since our computational result shows that every 3-error-correcting cyclic codes having the zero set $\{1, 2^i+1, 2^j+1\}$ with $m \leq 13$ have the same weight distribution as the 3-error-correcting BCH codes, we are interested in the question whether these codes are equivalent to the BCH code. We use the MAGMA implementation of Leon's algorithm [Leo82] to prove the non-equivalence for $m = 7$ and $m = 8$. In particular, for $m = 7$, the 3-error-correcting cyclic code with the zero set $\{1, 2^{\ell-1}+1, 2^\ell+1\}$, for $\ell = 3$ is not equivalent to the BCH code $\{1, 3, 5\}$. This supports the conjecture proposed in [MS83]. We employ the support splitting algorithm [Sen00] to prove the non-equivalence for $m = 10$. The weight enumerator of the hull of a code is an invariant by permutation. The hull of a linear code is the intersection of the code with its dual. We notice that the 3-error-correcting cyclic codes with the zero set $\{1, 2^i + 1, 2^j + 1\}$ are self-orthogonal for $m < 20$, *i.e.* the hull of the code is the code itself. If we puncture two equivalent codes in each position, the multiset of weight enumerators of each

punctured code is the same for the two codes. This object is the *signature* of the code that we compute to determine the equivalence of two codes. Cyclic codes have a transitive automorphism group. It implies that if we puncture a cyclic code in any position, we obtain the same weight enumerator for each punctured code. Thus, we puncture the dual codes in one fixed position first. Then we puncture them a second time in each position. We compute the signature of these dual codes. We obtain signatures which are different from the signature of the dual of BCH code $\{1, 3, 5\}$ for $m = 10$. So that we can conclude on the non-equivalence of non-BCH 3-error-correcting cyclic codes with the zero set $\{1, 2^i + 1, 2^j + 1\}$ with BCH. For $m = 9$, we get the same signature as that of BCH code $\{1, 3, 5\}$. This signature is not enough discriminant to collect information on a potential permutation.

We conclude this section by stating that every non-BCH 3*-error-correcting code with the zero set* $\{1, 2^i+1, 2^j+1\}$ *are not equivalent to the* 3*-error-correcting BCH code for* $m = 7$*,* $m = 8$ *and* $m = 10$*. The question remains open for* $m = 9$*.*

3 An algorithmic approach to compute a lower bound on the minimum distance of cyclic codes

While the weight distribution of the code C and its dual $C^\perp$ are directly related by the Pless power moment identity, there is as such no theoretical result known which combines the minimum distance of C and $C^\perp$.

In this section we discuss on the minimum distance of the dual of triple-error-correcting cyclic codes with zero set $\{1, 2^i + 1, 2^j + 1\}$ for i, $j > 1$ and $i \neq j$. Note that these duals are also cyclic. If 0 is in the zero set of C, then C is an even weight code. This implies that dual of the cyclic code with zero set $\{1, 2^i + 1, 2^j + 1\}$, has an even minimum distance.

Theoretical lower bounds on the minimum distance of cyclic codes are known (*e.g.* [BR60,HT72,Roo83,vLW86,Wol89]). They rely either on properties of regular distribution of certain patterns contained in the zero set, or on the number of rational points of algebraic curves over finite fields. Schaub [MS86] has investigated an algorithmic approach to compute a lower bound on the minimum distance of cyclic codes. This idea is particularly efficient for the codes which have few cyclic subcodes.

To find a lower bound of the minimum distance of a given dual code, we apply the Schaub [Sch88] algorithm. We propose an improvement with a pruning criteria based on BCH bound. Then, we compare the tightness of the Schaub bound and Hartmann-Tzeng bound.

3.1 Schaub Algorithm Description

In [Sch88], Schaub introduced an algorithm which computes a lower bound of the minimum distance of a cyclic code. This algorithm iteratively applies a method called Rank bounding on symbolic matrices. Basically, this method computes the linear complexity of the infinite periodic sequence derived from the Discrete

Fourier Transform of an n-length word c over $\mathbb{F}_{q^m}$, where q is a prime power. The Rank bounding method is described in Appendix B. In our instance, $q = 2$ and $n = 2^m - 1$. Its time complexity is $\mathcal{O}(n^3) = \mathcal{O}(2^{3m})$. Blahut's theorem ensures that this quantity is equal to the Hamming weight of c (*e.g.* [Mas98]). In matrix terms, it means that the weight of c is equal to the rank of the circulant matrix $\mathcal{B}_c$ of order n,

$$\mathcal{B}_c = \begin{pmatrix} A_0 & A_1 & \dots & A_{n-2} & A_{n-1} \\ A_1 & A_2 & \dots & A_{n-1} & A_0 \\ \vdots & \vdots & & \vdots & \vdots \\ A_{n-1} & A_0 & \dots & A_{n-3} & A_{n-2} \end{pmatrix},$$

where $(A_i)_{0 \leq i \leq n-1}$ is the family of coefficients of Mattson-Solomon polynomial of c.

Consider an n-length cyclic code C over $\mathbb{F}_2$ with zero set Z. On the one hand, the minimum distance d of C is equal to the minimum rank of $\mathcal{B}_c$, for all $c \in C$. However, it is impractical to employ Berlekamp-Massey algorithm, whose time complexity is $\mathcal{O}(n^2)$, to compute the minimum distance of a cyclic code. On the other hand, since C is cyclic, the coefficients of $\mathcal{B}_c$ satisfy, for all $c \in C$, the property: $A_z = 0$ for all $z \in Z$. In addition, for all $c \in C$, the set of integers i such that $A_i = 0$ forms an union of 2-cyclotomic cosets modulo n. The Schaub algorithm computes a lower bound on the rank of symbolic matrices that we describe below.

Schaub [Sch88] defined an arithmetic with three symbols 0, 1 and X. In this notation, 0 stands for null element of $\mathbb{F}_{2^m}$, 1 stands for any nonzero element of $\mathbb{F}_{2^m}$ and X stands for any element of $\mathbb{F}_{2^m}$ whose nullity or non-nullity is not known.

The commutative semiring $(\{0, 1, X\}, +, *)$ is defined with tables:

$+$	0	1	X
0	0	1	X
1	1	X	X
X	X	X	X

$*$	0	1	X
0	0	0	0
1	0	1	X
X	0	X	X

If κ cyclotomic cosets do not belong to Z, then the Schaub algorithm computes in effect a lower bound on the rank of 2^κ circulant matrices in $M(\{0, 1\})$. These matrices have zero coefficient only in the positions determined by the 2^κ corresponding unions of cyclotomic cosets. Thus, the Schaub algorithm has time complexity $\mathcal{O}(2^{3m+\kappa})$.

3.2 An improved Schaub algorithm

Each matrix can be identified with a non-linear subcode of C. This code is defined by the codewords of C having zeroes only in the form α^i, where i belongs to the set of positions of zeroes coefficients in the first row of the matrix. Each of these codes is of the form $\mathcal{D} \setminus \mathcal{E}$, where $\mathcal{D}$ is a cyclic subcode of C and $\mathcal{E}$ is

the union of all strict cyclic subcodes of $\mathcal{D}$. Let us denominate these non-linear subcodes as *constant-zero codes* of C, since their codewords (as polynomials) all have the same zeroes. Constant-zero codes form a partition of C. In addition, we can associate to each constant-zero subcode of C, the cyclic subcode of C with corresponding zero set. Rank bounding method consists in constructing a set of necessarily independent rows of the matrix and returns its cardinality. This cardinality is a lower bound on the minimum distance of a constant-zero code of C. Thus, the Schaub bound is the minimum cardinality computed among all the considered subcodes.

Note that each circulant matrix of order n over $\{0, 1\}$ can be identified by the integer between 0 and $2^n - 1$ whose binary representation is the first row of the matrix. We assume that the integers are distinct from $2^n - 1$. If two integers are in the same cyclotomic coset modulo $(2^n - 1)$, then the corresponding matrices are row equivalent and thus have the same rank. Thus, it is only necessary to consider one representative of each cyclotomic coset modulo $(2^n - 1)$. Further, if the cyclotomic coset modulo $(2^n - 1)$ of the integer contains p elements, then we have only to consider the submatrix containing the first p rows of the matrix instead of the whole circulant matrix. Indeed, the circulant matrix is a block matrix and can be split by horizontal lines into n/p blocks where each block is the submatrix described above. Note that p necessarily divides n.

A natural data structure to represent the set of the considered subcodes is the tree. A node A of the tree corresponds to a constant-zero code of C or equivalently to a cyclic subcode of C with zero set denoted Z_A. For our purpose, the root node corresponds to the subcode of C which contains the codewords with zeroes exactly in the positions given by Z. A node C is the child of a parent node P if and only if $Z_C \supset Z_P$ and $|Z_C| = |Z_P| + 1$. The number of studied subcodes grows exponentially in the number of cyclotomic cosets which are not in Z. In order to reduce time complexity, our strategy is to prune the tree using the BCH bound which is easily computable. One can think to introduce Hartmann-Tzeng bound in the pruning. However, our empirical analysis shows that Hartmann-Tzeng bound slows down the process and does not give better results than BCH. If, in a node, the Schaub bound is found to be smaller than BCH bound of the associated cyclic subcode of C, it becomes pointless to apply Rank bounding method to the subtree whose root is the considered node. Indeed, in each node of the pruned tree, BCH bound is always greater than Schaub bound and thus the Schaub bound is not be updated in this subtree.

3.3 Schaub algorithm and algebraic cryptanalysis

Boolean functions are important building blocks in the design of stream ciphers. High algebraic immunity [CM03] is a necessary condition to protect the stream cipher from algebraic attack. *Spectral immunity* is a related concept to algebraic immunity [HR11]. If the spectral immunity of a Boolean function is small, then one can find the initial state of a filter generator in which that Boolean function is used. In [HR11] the connection between spectral immunity and minimum distance of a cyclic code was shown which is as follows. The spectral immunity of

a Boolean function f over $\mathbb{F}_{2^m}$ (in univariate form) is equal to the minimal weight of the 2^m-ary cyclic codes of length $n = 2^m - 1$ generated by the polynomials $\gcd(f(z), z^n + 1)$ and $\gcd(f(z) + 1, z^n + 1)$. Therefore, we need an algorithm to efficiently estimate the minimum distance of a cyclic code over $\mathbb{F}_{2^m}$.

We apply the improved Schaub algorithm on cyclic codes of length n over $\mathbb{F}_{2^m}$ with a zero set derived from triple-error-correcting cyclic codes with zero set $\{1, 2^i + 1, 2^j + 1\}$.

We define the *Trace function* as $\mathrm{Tr}(\cdot) : \mathbb{F}_{2^m} \to \mathbb{F}_2$,

$$\mathrm{Tr}(z) \coloneqq z + z^2 + z^{2^2} + \ldots + z^{2^{m-1}}.$$

In Table 3, we provide a lower bound on the spectral immunity of the boolean function $\mathrm{Tr}(g(.))$ in univariate form over $\mathbb{F}_{2^m}$, where g is the generator polynomial of a triple-error-correcting cyclic code with zero set $\{1, 2^i + 1, 2^j + 1\}$ for $m < 9$. We denote G and H, the generator polynomials of the cyclic codes over $\mathbb{F}_{2^m}$ upon which we apply the Schaub algorithm,

$$G(z) \coloneqq \gcd(\mathrm{Tr}(g(z)), z^n + 1),$$

$$H(z) \coloneqq \frac{z^n + 1}{G(z)}.$$

Note that the zero set of G contains the zero set of g since $g(z)$ divides both $\mathrm{Tr}(g(z))$ and $z^n + 1$. In addition, $H(z) = \gcd(\mathrm{Tr}(g(z)) + 1, z^n + 1)$, since $\mathrm{Tr}(g(.))$ is a boolean function.

The polynomial g has coefficients over $\mathbb{F}_2$ since it is the product of minimal polynomials with respect to $\mathbb{F}_2$. Therefore, the boolean function $\mathrm{Tr}(g(.))$ and the generator polynomials G and H have binary coefficients. From Theorem 9 in [vLW86], the minimum distance of these codes over $\mathbb{F}_{2^m}$ is the same as that of their subfield subcodes over $\mathbb{F}_2$. As a consequence, we apply the Schaub algorithm on their binary subfield subcodes, since these one have much less cyclic subcodes.

3.4 Computational results

In Table 4, we give the Hartmann-Tzeng bound and the Schaub bound of every dual codes of triple-error-correcting cyclic codes of length $2^m - 1$ with $5 \leq m \leq 13$ and $Z = \{1, 2^i + 1, 2^j + 1\}$. Some subclasses of codes of this form are well known. We observe the Schaub bound is sharper than Hartmann-Tzeng bound on this class of codes.

Remark 2. As well, we consider the dual of triple-error-correcting cyclic codes defined with the same zero set $\{1, 2^i + 1, 2^j + 1\}$ over the alphabet $\mathbb{F}_{2^m}$ for $m < 9$. It is interesting to note that we obtain the same bound for the codes over $\mathbb{F}_{2^m}$ and their subfield subcodes over $\mathbb{F}_2$ with the Schaub algorithm.

Code Length	Zero Set	Lower Bound for Spectral Immunity
31	$\{1, 3, 5\}$	2
63	$\{1, 3, 5\}$	8
127	$\{1, 3, 5\}$	11
	$\{1, 3, 9\}$	13
	$\{1, 5, 9\}$	12
255	$\{1, 3, 5\}$	14
	$\{1, 5, 9\}$	14

Table 3. Lower bound for spectral immunity of Boolean functions $\mathrm{Tr}(g(.))$ where g is the generator polynomial of binary 3-error-correcting cyclic codes with zero set $\{1, 2^i + 1, 2^j + 1\}$

4 Conclusions

In this work we have discussed on the 3-error-correcting cyclic code that has zero set of the form $\{1, 2^i + 1, 2^j + 1\}$. We have presented a sufficient condition so that $\{1, 2^\ell + 1, 2^{p\ell} + 1\}$ corresponds to a 3-error-correcting cyclic code. Although $p = 2$ and $p = 3$ are known, our result opens the window to obtain a zero set of the form $\{1, 2^\ell + 1, 2^{p\ell} + 1\}$ for $p > 3$. For this one needs to find $p > 3$ such that Equation (1) does not have more than 5 solutions. Remark 1 highlights some reduced form of this equation when p is odd, which may be easier to handle with.

Our experimental result shows that $\{1, 2^i + 1, 2^j + 1\}$ has the same weight distribution as that of 3-error-correcting BCH code. However, these codes are not equivalent to the BCH code in general, this supports the conjecture proposed by Sloane and MacWilliams [MS83].

We have improved the Schaub algorithm that finds a lower bound of the minimum distance of a cyclic code. We have used this algorithm to find a lower bound of the spectral immunity of Boolean function $\mathrm{Tr}(g)$, where g is the generator polynomial of the code with the zero set $\{1, 2^i + 1, 2^j + 1\}$. We would like to see the deployment of this algorithm to find a lower bound of the minimum distance of some other class of cyclic codes in future.

Acknowledgments: The authors are highly grateful to Daniel Augot and Pascale Charpin for their valuable suggestions and comments on this work. The authors also thank the anonymous reviewers for their comments which has improved the editorial quality of this paper. The second author also would like to acknowledge the financial support by the French Agence National de la Recherche under contract ANR-06-SERI-013-RAPIDE that he received during this work.

Code Length	Dual Zero Set	Hartmann-Tzeng Bound	Schaub Bound	Minimum Distance
31	$\{1,3,5\}$	8	8	8
63	$\{1,3,5\}$	16	16	16
127	$\{1,3,5\}$	32	48	48
	$\{1,3,9\}$	32	48	48
	$\{1,5,9\}$	48	48	48
255	$\{1,3,5\}$	64	96	96
	$\{1,5,9\}$	96	96	96
511	$\{1,3,5\}$	128	216	224
	$\{1,3,9\}$	128	212	224
	$\{1,3,17\}$	128	210	224
	$\{1,5,9\}$	192	218	224
	$\{1,5,17\}$	192	212	224
	$\{1,9,17\}$	224	224	224
1023	$\{1,3,5\}$	256	446	448
	$\{1,9,17\}$	448	448	448
2047	$\{1,3,5\}$	512	930	960
	$\{1,3,9\}$	512	906	960
	$\{1,3,17\}$	512	906	960
	$\{1,3,33\}$	512	876	960
	$\{1,5,9\}$	768	936	960
	$\{1,5,17\}$	768	872	960
	$\{1,5,33\}$	768	916	960
	$\{1,9,17\}$	896	902	960
	$\{1,9,33\}$	896	902	960
	$\{1,17,33\}$	960	960	960
4095	$\{1,3,5\}$	1024	1886	1920
	$\{1,5,33\}$	1536	1814	1920
8191	$\{1,3,5\}$	2048	3110	3968
	$\{1,3,9\}$	2048	3588	3968
	$\{1,3,17\}$	2048	3643	3968
	$\{1,3,65\}$	2048	3668	3968
	$\{1,5,17\}$	3072	3594	3968
	$\{1,5,33\}$	3072	3678	3968
	$\{1,5,65\}$	3072	3802	3968
	$\{1,9,17\}$	3584	3912	3968
	$\{1,9,33\}$	3584	3718	3968
	$\{1,9,65\}$	3584	3722	3968
	$\{1,17,33\}$	3840	3844	3968
	$\{1,33,65\}$	3968	3968	3968

Table 4. Bounds on the minimum distance of the dual of the 3-error-correcting cyclic code over $\mathbb{F}_2$ of length $2^m - 1$ with zero set $\{1, 2^i + 1, 2^j + 1\}$

References

[AL96] D. Augot and F. Levy-dit-Vehel. Bounds on the minimum distance of the duals of BCH codes. *IEEE Transactions on Information Theory*, 42(4):1257–1260, 1996.

[BH09] C. Bracken and T. Helleseth. Triple-Error-Correcting BCH-like codes. In *Proceedings of the 2009 IEEE international conference on Symposium on Information Theory - Volume 3*, ISIT'09, pages 1723–1725, Piscataway, NJ, USA, 2009. IEEE Press.

[Bla02] R. E. Blahut. *Algebraic Codes for Data Transmission*. Cambridge University Press, 1 edition, July 2002.

[Blu04] A. W. Bluher. On $x^{q+1}+ax+b$. *Finite Fields and Their Applications*, 10(3):285–305, 2004.

[BR60] R. C. Bose and D. K. Ray-Chaudhuri. On a class of error correcting binary group codes. *Information and Control*, 3:68–79, 1960.

[CGG+00] A. Chang, P. Gaal, S. W. Golomb, G. Gong, T. Helleseth, and P. V. Kumar. On a conjectured ideal autocorrelation sequence, a related triple-error correcting cyclic code. *IEEE Transactions on Information Theory*, 46(2):680–687, 2000.

[Cha98] P. Charpin. Open problems on cyclic codes. In V. S. Pless and W. C. Huffman, editors, *Handbook of Coding Theory*, pages 963–1063. Amsterdam: Elsevier, 1998. Volume 1, Part 1, Chapter 11.

[CJM02] P. Chose, A. Joux, and M. Mitton. Fast correlation attacks: An algorithmic point of view. In *EUROCRYPT*, pages 209–221, 2002.

[CM03] N. Courtois and W. Meier. Algebraic attacks on stream ciphers with linear feedback. In *EUROCRYPT*, pages 345–359, 2003.

[Dob99] H. Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: The Welch case. *IEEE Transactions on Information Theory*, 45(4):1271–1275, 1999.

[HR11] T. Helleseth and S. Rønjom. Simplifying algebraic attacks with univariate analysis. In *Information Theory and Applications Workshop (ITA), 2011*, pages 1–7, Feb. 2011.

[HT72] C. R. P. Hartmann and K. K. Tzeng. Generalizations of the BCH bound. *Information and Control*, 20(5):489–498, 1972.

[Kas69] T. Kasami. Weight Distributions of BCH Codes. In *Combinatorial Mathematics and Its Applications*, pages 335–357. Chapell Hill, NC: University of North Carolina Press, 1969.

[Kas71] T. Kasami. The Weight Enumerators for Several Classes of Subcodes of the 2nd Order Binary Reed-Muller Codes. *Information and Control*, 18(4):369–394, 1971.

[Leo82] J. S. Leon. Computing automorphism groups of error-correcting codes. *IEEE Transactions on Information Theory*, 28(3):496–510, 1982.

[Mas98] J. L. Massey. The discrete Fourier transform in coding and cryptography. In *IEEE Information Theory Workshop, ITW 98*, pages 9–11, 1998.

[MS83] F. J. Macwilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes (North-Holland Mathematical Library)*. North Holland, January 1983.

[MS86] J. L. Massey and T. Schaub. Linear complexity in coding theory. In *Coding Theory and Applications*, pages 19–32, 1986.

[Roo83] C. Roos. A new lower bound for the minimum distance of a cyclic code. *IEEE Transactions on Information Theory*, 29(3):330 – 332, May 1983.

[Sch88] T. Schaub. *A linear complexity approach to cyclic codes*. PhD thesis, Swiss Federal Institute of Technology, Zürich, 1988. Diss. ETH No. 8730.

[Sen00] N. Sendrier. Finding the permutation between equivalent codes: the support splitting algorithm. *IEEE Transactions on Information Theory*, 46(4):1193–1203, Jul 2000.

[vDV96] M. van Der Vlugt. Non-BCH Triple-Error-Correcting codes. *IEEE Transactions on Information Theory*, 42(5):1612–1614, 1996.

[vLW86] J. H. van Lint and R. M. Wilson. On the minimum distance of cyclic codes. *IEEE Transactions on Information Theory*, 32(1):23–40, 1986.

[Wol89] J. Wolfmann. New bounds on cyclic codes from algebraic curves. In *Proceedings of the 3rd International Colloquium on Coding Theory and Applications*, pages 47–62, London, UK, 1989. Springer-Verlag.

A Proof of Theorem 1

The parity check matrix of C is of the form:

$$\mathcal{H} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{(n-1)} \\ 1 & \alpha^{2^\ell+1} & \alpha^{2(2^\ell+1)} & \dots & \alpha^{(n-1)(2^\ell+1)} \\ 1 & \alpha^{2^{p\ell}+1} & \alpha^{2(2^{p\ell}+1)} & \dots & \alpha^{(n-1)(2^{p\ell}+1)} \end{pmatrix}.$$

Suppose, for a contradiction, that the minimum distance is five. From Lemma 1, we can consider a codeword of weight six. Thus, there exists a set of six dependent columns over $\mathbb{F}_2$ in $\mathcal{H}$. In other words, there exist six distinct elements x, y, z, u, v, w in $\mathbb{F}_{2^m}^*$ such that:

$$\begin{cases} x + y + z + u + v + w & = 0, \\ x^{2^\ell+1} + y^{2^\ell+1} + \dots + v^{2^\ell+1} + w^{2^\ell+1} & = 0, \\ x^{2^{p\ell}+1} + y^{2^{p\ell}+1} + \dots + v^{2^{p\ell}+1} + w^{2^{p\ell}+1} & = 0. \end{cases} \tag{5}$$

These equations are symmetric in variables x, y, z, u, v, w. Thus, the system (5) can be written as:

$$\begin{cases} x + y + z & = u + v + w & = a, \\ x^{2^\ell+1} + y^{2^\ell+1} + z^{2^\ell+1} & = u^{2^\ell+1} + v^{2^\ell+1} + w^{2^\ell+1} & = b, \\ x^{2^{p\ell}+1} + y^{2^{p\ell}+1} + z^{2^{p\ell}+1} & = u^{2^{p\ell}+1} + v^{2^{p\ell}+1} + w^{2^{p\ell}+1} & = c, \end{cases}$$

where $a, b, c \in \mathbb{F}_{2^m}$. Note that $b \neq a^{2^\ell+1}$, otherwise we would have:

$$\begin{aligned} x + y + z + a &= 0, \\ x^{2^\ell+1} + y^{2^\ell+1} + z^{2^\ell+1} + a^{2^\ell+1} &= 0, \end{aligned}$$

which means there is a codeword of weight 4 in the code with zero set $\{1, 2^\ell+1\}$ where $\gcd(\ell, m) = 1$. This is impossible since this code has minimum distance 5

from the proof of Lemma 1. Now we consider the equations:

$$\begin{aligned} x+y+z &= a,\\ x^{2^\ell+1}+y^{2^\ell+1}+z^{2^\ell+1} &= b,\\ x^{2^{p\ell}+1}+y^{2^{p\ell}+1}+z^{2^{p\ell}+1} &= c. \end{aligned}$$

We substitute x with $x+a$, y with $y+a$ and z with $z+a$.

$$\begin{aligned} x+y+z &= 0,\\ (x+a)^{2^\ell+1}+(y+a)^{2^\ell+1}+(z+a)^{2^\ell+1} &= b,\\ (x+a)^{2^{p\ell}+1}+(y+a)^{2^{p\ell}+1}+(z+a)^{2^{p\ell}+1} &= c. \end{aligned}$$

Then, expanding the second and third equations and using the relation $x+y+z=0$ we obtain the following:

$$\begin{aligned} x+y+z &= 0,\\ x^{2^\ell+1}+y^{2^\ell+1}+z^{2^\ell+1} &= b+a^{2^\ell+1},\\ x^{2^{p\ell}+1}+y^{2^{p\ell}+1}+z^{2^{p\ell}+1} &= c+a^{2^{p\ell}+1}. \end{aligned}$$

Next, we replace $z=x+y$ and we get:

$$\begin{cases} x^{2^\ell}y+y^{2^\ell}x &= \beta,\\ x^{2^{p\ell}}y+y^{2^{p\ell}}x &= \gamma, \end{cases} \tag{6}$$

where $\beta = b+a^{2^\ell+1}$ and $\gamma = c+a^{2^{p\ell}+1}$. Note $x\neq 0$, since $\beta\neq 0$. We replace y by xy. (6) become:

$$\begin{cases} x^{2^\ell+1}(y+y^{2^\ell}) = \beta, & (7)\\ x^{2^{p\ell}+1}(y+y^{2^{p\ell}}) = \gamma. & (8) \end{cases}$$

From (7), we get:

$$y+y^{2^\ell} = \beta x^{-(2^\ell+1)},$$

and raising to the power 2^ℓ repeatedly, we obtain:

$$\begin{aligned} y^{2^\ell}+y^{2^{2\ell}} &= (\beta x^{-(2^\ell+1)})^{2^\ell},\\ y^{2^{2\ell}}+y^{2^{3\ell}} &= (\beta x^{-(2^\ell+1)})^{2^{2\ell}},\\ \cdots &= \cdots,\\ y^{2^{(p-1)\ell}}+y^{2^{p\ell}} &= (\beta x^{-(2^\ell+1)})^{2^{(p-1)\ell}}. \end{aligned}$$

Adding them all, we get:

$$y+y^{2^{p\ell}} = \sum_{i=0}^{p-1}(\beta x^{-(2^\ell+1)})^{2^{i\ell}}.$$

Then, we get from (8):

$$x^{2^{p\ell}+1} \sum_{i=0}^{p-1} (\beta x^{-(2^\ell+1)})^{2^{i\ell}} = \gamma.$$

If this equation does not have more than 5 solutions over $\mathbb{F}_{2^m}^*$, then for all distinct elements x, y, z, u, v, w in $\mathbb{F}_{2^m}^*$ (5) is not satisfied. Hence there is no word of weight 6. Then, Lemma 1 implies that the minimum distance is 7. □

B Rank Bounding method (Schaub, 1988)

Cases	Sum	Terms [1]	Conclusion
1	0	$0 \dots \overset{a}{X} \dots 0$	$\text{coeff}_a = 0$
2	0	$0 \dots \overset{a}{1} \dots 0$	independent
3	0	$0 \dots \overset{a}{X} \dots \overset{b}{1} \dots 0$	$\text{coeff}_a = 1$
4	1	$0 \dots 0 \dots 0$	independent
5	1	$0 \dots \overset{a}{X} \dots 0$	$\text{coeff}_a = 1$

Fig. 1. Description of fives cases which enable to determine either unknown coefficients, or the independence of considered row, in Rank Bounding method.

[1] The superscripts indicate the position of the element in the table of terms.

Algorithm 1 Rank Bound

Input: a nonzero matrix M of size $n \times n$,
with coefficients over $\{0, 1\}$.
Output: a lower bound on the rank of M.

▶ *Initialization step*
{The first row of M is regarded as independent.}
indep-row[1] $\leftarrow M[1]$;
{RankBound is the number of ensured independent rows.}
RankBound $\leftarrow 1$;
▶ *Search of necessarily independent rows in M*
for $1 \leq j \leq n$ **do**
  for $1 \leq i \leq$ RankBound **do**
    {We suppose the current row $M[j]$ is a linear combination of the certified independent rows of M.}
    coeff[i] $\leftarrow X$
  end for
  {From now, we try to derive a contradiction on the dependence of $M[j]$ with the ensured independent rows.}
  repeat
    $k \leftarrow 1$; change $\leftarrow$ false; independent $\leftarrow$ false;
    while $k \leq n$ **and** independent=false **do**
      ▶ *Construction of the table of terms*
      for $1 \leq i \leq$ RankBound **do**
        term[i] $\leftarrow$ coeff[i]$*$ indep-row[i][j];
      end for
      {The coefficient $M[j][k]$ is the sum of terms.}
      sum $\leftarrow M[j][k]$
      if sum$= 0$ **then**
        {The 5 cases are described in Figure 1.}
        case 1: coeff[a] $\leftarrow 0$; change $\leftarrow$ true;
        case 2: independent $\leftarrow$ true;
        case 3: coeff[b] $\leftarrow 1$; change $\leftarrow$ true;
      else
        case 4: independent $\leftarrow$ true;
        case 5: coeff[a] $\leftarrow 1$; change $\leftarrow$ true;
      end if
      $k \leftarrow k + 1$;
    end while
  until change=false **or** independent=true
  if independent=true **then**
    RankBound $\leftarrow$ RankBound+1;
    indep-row[RankBound] $\leftarrow M[j]$;
  end if
end for
return RankBound;