On the Burst-Covering Radius of Binary Cyclic Codes

Gabriel Sac Himelfarb* and Moshe Schwartz*†
* Department of Electrical and Computer Engineering, McMaster University, Hamilton, ON L8S 4K1, Canada
† School of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Beer Sheva 8410501, Israel
Emails: sachimeg@mcmaster.ca, schwartz.moshe@mcmaster.ca

2026 IEEE International Symposium on Information Theory (ISIT) | 979-8-3315-8004-9/26/$31.00 ©2026 IEEE | DOI: 10.1109/ISIT62367.2026.11653718

***Abstract*—We define and study burst-covering codes. We provide some general bounds connecting the code parameters with its burst-covering radius. We then provide stronger bounds on the burst-covering radius of cyclic codes, by employing linear feedback shift register (LFSR) sequences. We prove a new bound on pattern frequencies in LFSR sequences, which is of independent interest. Using this tool, we can bound the burst-covering radius of binary primitive BCH codes and Melas codes.**

I. Introduction

Error-correcting codes and their geometric counterparts, covering codes, have a long and rich history of research (e.g., [7], [13]). From a geometric perspective, while the former pack the space with error balls, the latter cover it. In their intersection lie perfect codes, that manage to tile the space with error balls.

Many families of codes have been studied both for the their error-correction capabilities, as well as their covering parameters. A partial list of those contains MDS codes, cyclic codes (including BCH, dual BCH, Melas and Zetterberg codes), Reed-Muller codes, and of course, perfect codes (for details, see for example [7], [13]).

However, one family of codes is conspicuously missing from this list – codes for burst errors. A b-burst error is an error pattern all of whose erroneous symbols are confined to a contiguous block of b positions. Burst-correcting codes have been studied in [1]–[3], [8], [9]. In this work, we introduce and study *burst-covering codes* for the first time, the natural geometric counterpart to burst-error-correcting codes in the context of covering problems. We are not aware of any previous works in the literature addressing this gap.

Burst-covering codes do not only fill a void in the theory of binary codes, but may also find use in data storage scenarios. Many applications require the implementation of database queries whose return value is a linear combination of database items with coefficients supplied by the user. Private information retrieval (PIR) protocols [6], partial-sum queries [5] and more recently, certain machine learning inference implementations [15], among others, all employ such queries.

Traditionally, the answer of queries requiring linear combinations of items are implemented with linear covering codes. So far, these implementations have not considered spatial locality constraints: many storage devices perform best when accessing contiguous blocks of data, as opposed to a scattered random access pattern. As we will see, the parity-check matrix H of a linear b-burst covering code satisfies the property that any column vector can be obtained as a linear combination of a window of at most b consecutive columns of H. Thus, employing a burst-covering code can address locality issues.

Our main contributions are as follows: We first define burst-covering codes and derive basic bounds on their parameters. We then focus on the study of the burst-covering radius of binary cyclic codes. As we later show, the study of cyclic burst-covering codes is closely related to the analysis of pattern frequencies in linear feedback shift-register (LFSR) sequences. We employ classic known bounds for the number of occurrences of subwords in these sequences, but for the relevant case of BCH codes we show that these fail to provide significant results. We thus prove a new result on pattern frequencies which is meaningful for BCH codes, and is of independent interest for the study of LFSR sequences. We use this to bound the burst-covering radius of binary BCH codes, and the closely related Melas codes. It is also possible to show that our analysis gives rise to efficient covering algorithms for binary cyclic codes. However, due to space limitations, this and other results, as well as many proofs, are omitted and are available in the full version of this paper [16].

This work is organized as follows. Section II gives the necessary notation and known results to be used later. In Section III we define general linear burst-covering codes, and provide some bounds on their parameters. We then study cyclic burst-covering codes in Section IV, and further focus on the burst-covering radius of BCH codes in Section V. We conclude in Section VI with a summary of the results and some open questions.

II. Preliminaries

Let $\mathbb{F}_q$ denote the finite field of size q, and $\mathbb{F}_q^* \triangleq \mathbb{F}_q \setminus \{0\}$. The support of a vector $v \in \mathbb{F}_q^n$ is defined as $\mathrm{supp}(v) \triangleq \{0 \leqslant i \leqslant n-1 : v_i \neq 0\}$.

An $[n, n-r]_q$ linear code, $\mathcal{C}$, is an $(n-r)$-dimensional space, $\mathcal{C} \subseteq \mathbb{F}_q^n$. We say r is the redundancy of the code.

Denote $\mathbb{F}_q[X]$ the set of polynomials in the unknown X, with coefficients from $\mathbb{F}_q$. With any vector $v \in \mathbb{F}_q^n$ we associate the polynomial $v(X) = \sum_{i=0}^{n-1} v_i X^i$. Using this identification, a cyclic code $\mathcal{C}$ is an ideal in the ring of polynomials $\mathbb{F}_q[X]/(X^n - 1)$. There exists a unique generator polynomial, $g(X) \in \mathbb{F}_q[X]$, $\deg(g(X)) = r$, such that $c(X) \in \mathcal{C}$ if

and only if $c(X) = u(X)g(X)$, for some $u(X) \in \mathbb{F}_q[X]$, $\deg(u(X)) \leqslant n - r - 1$. The roots of $g(X)$ (in its splitting field) are called the roots of the code $\mathcal{C}$. The commonly studied case is that of $g(x)$ having only simple roots (i.e., no repeated root). This is guaranteed, for example, when $\gcd(n, q) = 1$.

A. Linear feedback shift registers (LFSRs)

Definition 1. *Given a polynomial $f \in \mathbb{F}_q[X]$, its* order *(also known as* exponent*) is the least positive integer n such that $f|X^n - 1$.*

Definition 2. *Given a field extension $\mathbb{F}_{q^t}$ of $\mathbb{F}_q$, the* trace *map, $\mathrm{Tr}_{\mathbb{F}_{q^t}/\mathbb{F}_q} : \mathbb{F}_{q^t} \to \mathbb{F}_q$, is defined as $\mathrm{Tr}_{\mathbb{F}_{q^t}/\mathbb{F}_q}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{t-1}}$. If the field extension is clear from the context, we will drop the subscript $\mathbb{F}_{q^t}/\mathbb{F}_q$.*

For simplicity of presentation, we will limit our treatment of LFSRs to binary sequences:

Definition 3. *Given a polynomial of degree r, $g(X) = \sum_{i=0}^{r-1} m_i X^i + X^r \in \mathbb{F}_2[X]$, we define an LFSR sequence of* order r *and* connection polynomial g *(sometimes called characteristic polynomial) as a sequence $(a_k)_{k \geqslant 0}$ which satisfies the linear recurrence $a_k = \sum_{i=0}^{r-1} m_i a_{k-r+i}$ for all $k \geqslant r$. The elements $a_0, \ldots, a_{r-1}$ are called the initial conditions of the sequence. We say g is the* minimal *connection polynomial in case $(a_k)_{k \geqslant 0}$ does not satisfy any linear recursion of smaller order.*

The following theorem summarizes results from [11] and [10]:

Theorem 4. 1) *If $g \in \mathbb{F}_2[X]$ is irreducible over $\mathbb{F}_2$, and $\alpha \in \mathbb{F}_{2^r}$ is a root of g, there exists some $\beta \in \mathbb{F}_{2^r}$, determined by the initial conditions $a_0, \ldots, a_{r-1}$, such that for all $k \geqslant 0$, $a_k = \mathrm{Tr}(\beta \alpha^k)$, where $\mathrm{Tr} : \mathbb{F}_{2^r} \to \mathbb{F}_2$ is the trace map from $\mathbb{F}_{2^r}$ to $\mathbb{F}_2$. The minimal period of the sequence is $\mathrm{ord}(g)$.*

2) *If g factors into distinct irreducible polynomials, $g = \prod_{i=1}^{e} g_i$, of degrees $d_1, \ldots, d_e$ respectively, then for all $k \geqslant 0$,*

$$a_k = \mathrm{Tr}\left(\sum_{i=1}^{e} \gamma_i \alpha_i^k \right),$$

where $\alpha_i \in \mathbb{F}_{2^{d_i}}$ is a root of g_i and $\gamma_i \in \mathbb{F}_{2^{d_i}}$ $1 \leqslant i \leqslant e$, and Tr is the trace function from the splitting field of g to $\mathbb{F}_2$. If g is the minimal polynomial of the sequence, then the minimal period is equal to $\mathrm{lcm}\{\mathrm{ord}(g_i) : 1 \leqslant i \leqslant e\}$.

B. Galois-mode LFSRs

We now introduce Galois-mode linear feedback shift registers. We refer the reader to [11], although our treatment differs slightly.

Given a polynomial of degree r, $g(X) = \sum_{i=0}^{r-1} m_i X^i + X^r \in \mathbb{F}_2[X]$, we define the Galois-mode LFSR of length r and connection polynomial g as a sequence generator with states of the form $(f_0, f_1, \ldots, f_{r-1}) \in \mathbb{F}_2^r$, and whose state transition is given by: $(f_0, f_1, \ldots, f_{r-1}) \longrightarrow (m_0 f_{r-1}, f_0 + m_1 f_{r-1}, \ldots, f_{r-2} + m_{r-1} f_{r-1})$. The output of the LFSR is the sequence of elements f_{r-1} from each state.

Theorem 5. *Given a Galois-mode LFSR of length r and connection polynomial g as above,*

1) *If we identify a state $(f_0, \ldots, f_{r-1})$ with the polynomial $f(X) = \sum_{i=0}^{r-1} f_i X^i$, then the sequence of states corresponds to the sequence of polynomials $(X^k f \pmod g)_{k \geqslant 0}$, where f is the initial state.*
2) *The output $(a_k)_{k \geqslant 0}$ satisfies the linear recurrence $a_k = m_{r-1} a_{k-1} + m_{r-2} a_{k-2} + \cdots + m_0 a_{k-r}$ for every $k \geqslant r$, which means that it can also be obtained as the output of an LFSR with connection polynomial g.*

Theorem 6. *Given $g \in \mathbb{F}_2[X]$ of degree r, consider the Galois-mode LFSR with connection polynomial g as above and initial load f. Denote by $(a_k)_{k \geqslant 0}$ the output sequence. Then $\deg(X^k f \pmod g) = r - 1 - \max\{j : a_k = 0, \ldots, a_{k+j-1} = 0\}$, where the maximum is taken to be 0 if $a_k = 1$.*

C. Character sums

Definition 7 ([12, Chapter 5])**.** *An additive character over a finite field $\mathbb{F}_q$ is a function $\chi : \mathbb{F}_q \to \mathbb{C}$ that satisfies $\chi(x + y) = \chi(x) \cdot \chi(y)$. In other words, it is an homomorphism from the additive group of the field to the multiplicative group of modulus-1 complex numbers.*

Most of the results in the following sections are for binary codes. In this case, we shall use the canonical additive character $\chi(x) = (-1)^{\mathrm{Tr}(x)}$.

Theorem 8 (Weil-Carlitz-Uchiyama bound, [4])**.** *Let $f \in \mathbb{F}_q[X]$ be of degree $n \geqslant 1$ with $\gcd(n, q) = 1$, and let χ be a non-trivial additive character of $\mathbb{F}_q$. Then*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \right| \leqslant (n-1) q^{1/2}.$$

III. Burst-Covering Codes

Linear covering codes have several equivalent definitions. In particular, a geometric definition shows how the space is covered by error balls, and an algebraic definition shows how syndromes are covered by linear combinations of columns from a parity-check matrix for the code. We use these two approaches to define burst-covering codes. We begin with a geometric definition:

Definition 9. *Given $x \in \mathbb{F}_q^n$, $b > 0$ an integer, and an index $0 \leqslant i < n$, define:*

$$B_b(x, i) \triangleq \left\{ y \in \mathbb{F}_q^n : \mathrm{supp}(y - x) \subseteq \{i, \ldots, i + b - 1\} \right\},$$

where indices are considered modulo n. In other words, $B_b(x, i)$ is the set of vectors that differ from x inside a window of b consecutive positions starting at i, where indices are viewed cyclically.

We define the b-burst ball *of radius* b*, centered at* $x \in \mathbb{F}_q^n$*, as:*

$$B_b(x) \triangleq \bigcup_{i=0}^{n-1} B_b(x,i)$$

We note that $d(x,y) = \min\{b : y \in B_b(x)\}$ is not a metric, as it does not satisfy the triangle inequality. For example, $3 = d(10100, 00000) > d(10100, 10000) + d(10000, 00000) = 1 + 1 = 2$. Even so, we use the burst balls to provide a geometric definition of burst-covering codes:

Definition 10. *We say* $\mathcal{C} \subseteq \mathbb{F}_q^n$ *is a* b*-burst covering code if*

$$\bigcup_{c \in \mathcal{C}} B_b(x) = \mathbb{F}_q^n.$$

Similarly to what occurs in the case of regular covering codes, we can give an equivalent definition for linear codes based on their parity-check matrix:

Theorem 11. *Let* $\mathcal{C}$ *be a linear* $[n, n-r]_q$ *code, and let* $H \in \mathbb{F}_q^{r \times n}$ *be a parity-check matrix for the code. Then* $\mathcal{C}$ *is a* b*-burst covering code if and only if every column vector* $z \in \mathbb{F}_q^r$ *can be obtained as a linear combination of* b *(cyclically) consecutive columns of* H*. Additionally,* b *does not depend on the choice of* H*.*

Definition 12. *The* burst-covering radius *of a code* $\mathcal{C}$ *is the least integer* b *such that* $\mathcal{C}$ *is a* b*-burst covering code. The burst-covering radius of a full-rank matrix* $H \in \mathbb{F}_q^{r \times n}$*,* $r \leqslant n$*, is the least integer* b *such that any column vector* $z \in \mathbb{F}_q^r$ *can be obtained as a linear combination of* b *consecutive columns of* H*.*

Remark 13. *Unlike other code parameters, the burst-covering radius is not necessarily invariant under permutations of the bit positions.*

Using a usual counting argument, we can give the following bound on the code parameters:

Theorem 14. *Let* $\mathcal{C}$ *be an* $[n, n-r]_q$ b*-burst-covering code with* $b \geqslant 2$*. Then,*

$$n \geqslant \frac{q^{r-b+1} - 1}{q-1} + 1 \tag{1}$$

For binary codes and burst sizes greater than 2, we can improve bound (1):

Theorem 15. *If* $\mathcal{C}$ *is an* $[n, n-r]_2$ b*-burst-covering code with* $b \geqslant 3$ *and* $r \geqslant 2$*, then in the cyclical-burst case we have*

$$n \geqslant 2^{r-b+1} + 1. \tag{2}$$

IV. Burst-Covering Radius of Binary Cyclic Codes

We will restrict our study to binary cyclic codes with no repeated roots. Consider a cyclic code with generator polynomial $g(X) = \prod_{i=1}^{e} g_i(X)$, where $g_i \in \mathbb{F}_2[X]$, $1 \leqslant i \leqslant e$, are distinct irreducible polynomials of degrees $d_1, d_2, \ldots, d_e$ respectively, and $r = \deg(g) = \sum_{i=1}^{e} d_i$ is the redundancy of the code. Let $\alpha_i \in \mathbb{F}_{2^{d_i}}$ be a root of g_i for each i. Then, a possible parity-check matrix for the code is

$$H = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_e & \alpha_e^2 & \ldots & \alpha_e^{n-1} \end{pmatrix}, \tag{3}$$

where the i-th row should be interpreted as d_i rows, after replacing each α_i^j by its binary vector representation over $\mathbb{F}_2^{d_i}$ (after a choice of some basis).

We begin by giving crude upper and lower bounds:

Theorem 16. *The burst-covering radius* b *of a cyclic* $[n, n-r]_q$ *code with generator polynomial* g *as defined above, satisfies:*

$$r - \min_{1 \leqslant i \leqslant e} d_i + 1 \leqslant b \leqslant r.$$

Given a window of t consecutive columns $h_i, h_{i+1}, \ldots, h_{i+t-1}$ in H and a polynomial $f(X) = \sum_{j=0}^{t-1} c_j X^j \in \mathbb{F}_2[X]$, we define the linear combination $\mathrm{LC}(i, f) \triangleq \sum_{j=0}^{t-1} c_j h_{i+j}$. Given a polynomial $f \in \mathbb{F}_2[X]$, we denote by $\mathrm{LC}(f)$ the set $\mathrm{LC}(f) \triangleq \{\mathrm{LC}(i, f) : 0 \leqslant i \leqslant n-1\}$.

Lemma 17. *For* $f_1, f_2 \in \mathbb{F}_2[X]$*,* $\mathrm{LC}(f_1) = \mathrm{LC}(f_2)$ *if and only if* $f_1(X) \equiv X^k f_2(X) \pmod{g(X)}$ *for some* $k \geqslant 0$*.*

From Theorem 16 and Lemma 17 we arrive at the following characterization of the burst-covering radius of cyclic codes:

Corollary 18. *The burst covering radius* b *of a binary cyclic code with no repeated roots satisfies*

$$b = \max_{f \in \mathcal{F}_r} \min_{k \geqslant 0} \deg(X^k f \pmod{g}) + 1, \tag{4}$$

where $\mathcal{F}_r \triangleq \{f \in \mathbb{F}_2[X] : \deg(f) < r\}$*.*

In the Preliminaries section we recalled the connection between the computation of $X^k f \pmod{g}$ and a Galois-mode LFSR with connection polynomial g. By Theorem 6 and (4) we deduce that:

Corollary 19. *The burst covering radius of a binary cyclic code* $\mathcal{C}$ *with no repeated roots, as in* (3)*, is given by:*

$$b = r - \min_{a_0, \ldots, a_{r-1}} Z(g, (a_0, \ldots, a_{r-1})), \tag{5}$$

where $Z(g, (a_0, \ldots, a_{r-1}))$ *denotes the maximum length of a run of zeros in the LFSR sequence with connection polynomial* g *and initial conditions* $a_0, \ldots, a_{r-1}$*. Alternatively,*

$$b = r - \min_{c \in \mathcal{C}^\perp} Z(c),$$

where $Z(c)$ *is the maximum length of a run of zeros in* c*.*

A. Pattern frequencies in LFSR sequences

We begin this section by recalling a previous result on the number of occurrences of patterns in LFSR sequences:

Theorem 20 ([14])**.** *Consider a binary LFSR sequence with minimal period* π*. Let* $g \in \mathbb{F}_2[X]$ *be the minimal polynomial*

of the sequence, and $r = \deg(g)$. Suppose that s is a positive integer less than or equal to the degree of any irreducible factor of g in $\mathbb{F}_2[X]$. Then for any pattern $y \in \mathbb{F}_2^s$, its number of occurrences N in one minimal period of the sequence satisfies

$$\left|N - \frac{\pi}{2^s}\right| \leqslant \left(1 - \frac{1}{2^s}\right) 2^{r/2}. \tag{6}$$

Theorem 20 will allow us to study the burst-covering radius of general cyclic codes. However, there is a notable case for which this result is not useful: if g factors into irreducible polynomials of equal degrees, then the lower bound on N that can be derived from (6) can be negative. This problem arises in the study of relevant codes such as long BCH codes. Thus, we introduce the following new result:

Theorem 21. *Consider a connection polynomial $g(X) = \prod_{i=1}^{e} g_i(X)$, where $g_i \in \mathbb{F}_2[X]$, $1 \leqslant i \leqslant e$, are distinct irreducible polynomials of the same degree m. Let α be a primitive element in the splitting field $\mathbb{F}_{2^m}$ of g, and let $t_i \geqslant 1$ be such that α^{t_i} is a root of g_i for each $1 \leqslant i \leqslant e$. Further assume that all t_i are odd. Under these conditions, the following holds:*

Consider any pattern $y \in \mathbb{F}_2^s$ of length $s \leqslant m$. If $\max_{i=1,\ldots,e} t_i \geqslant 3$, then the number of occurrences N of y in a window of length $2^m - 1$ of any non-zero LFSR sequence with connection polynomial g as above[1], satisfies

$$\left|N - \frac{2^m - 1}{2^s}\right| \leqslant \left(1 - \frac{1}{2^s}\right)\left((\max_i t_i - 1)2^{m/2} + 1\right). \tag{7}$$

Proof: From Theorem 4 we know that the sequence is $(a_k = \mathrm{Tr}(\sum_{i=1}^{e} \gamma_i \alpha^{t_i k}))_{k \geqslant 0}$, where $\gamma_i \in \mathbb{F}_{2^m}$, $1 \leqslant i \leqslant e$, determine the initial conditions, and $\mathrm{Tr} : \mathbb{F}_{2^m} \to \mathbb{F}_2$ is the trace map. We observe that, over the reals, $(1+(-1)^{a+a_k})/2$ is 1 if $a_k = a$ and 0 otherwise. Recalling that $\chi(x) = (-1)^{\mathrm{Tr}(x)}$ is the canonical additive character of the field $\mathbb{F}_{2^m}$, we deduce that $\frac{1+(-1)^a \chi(\sum_{i=1}^{e} \gamma_i \alpha^{t_i k})}{2}$ is an indicator function of the k-th element of the sequence being equal to a.

Thus, the following sum counts the number of occurrences of the pattern y in the first $2^m - 1$ bits of the sequence:

$$N = \sum_{k=0}^{2^m-2} \prod_{j=0}^{s-1} \frac{1 + (-1)^{y_j} \chi(\sum_{i=1}^{e} \gamma_i \alpha^{t_i (k+j)})}{2}$$

Making the substitution $x = \alpha^k$, and letting $[s-1] = \{0, 1, \ldots, s-1\}$ we get

$$\begin{aligned} N &= \frac{1}{2^s} \sum_{x \in \mathbb{F}_{2^m}^*} \prod_{j=0}^{s-1} \left(1 + (-1)^{y_j} \chi\left(\sum_{i=1}^{e} \gamma_i \alpha^{t_i j} x^{t_i}\right)\right) \\ &= \frac{1}{2^s} \sum_{x \in \mathbb{F}_{2^m}^*} \left(1 + \sum_{\substack{J \subseteq [s-1] \\ J \neq \emptyset}} (-1)^{\sum_{j \in J} y_j} \chi\left(\sum_{j \in J} \sum_{i=1}^{e} \gamma_i \alpha^{t_i j} x^{t_i}\right)\right) \\ &= \frac{1}{2^s} \left(2^m - 1 + \sum_{\substack{J \subseteq [s-1] \\ J \neq \emptyset}} (-1)^{\sum_{j \in J} y_j} \sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\sum_{i=1}^{e} \gamma_i \sum_{j \in J} \alpha^{t_i j} x^{t_i}\right)\right) \end{aligned}$$

[1]Note that g need not be the minimal polynomial of the sequence.

Thus, we have

$$\left|N - \frac{2^m - 1}{2^s}\right| \leqslant \frac{1}{2^s} \sum_{\substack{J \subseteq [s-1] \\ J \neq \emptyset}} \left|\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\sum_{i=1}^{e} \gamma_i \sum_{j \in J} \alpha^{t_i j} x^{t_i}\right)\right|$$

By considering the polynomial $\sum_{i=1}^{e} \gamma_i \sum_{j \in J} \alpha^{t_i j} x^{t_i}$, we obtain from the Weil-Carlitz-Uchiyama bound

$$\left|\sum_{x \in \mathbb{F}_{2^m}^*} \chi\left(\sum_{i=1}^{e} \gamma_i \sum_{j \in J} \alpha^{t_i j} x^{t_i}\right)\right| \leqslant (\max_i t_i - 1)2^{m/2} + 1,$$

and the desired bound follows. ∎

Corollary 22. *Consider the setting of Theorem 21, and any pattern $y \in \mathbb{F}_2^s$ of length s. If $\max_{i=1,\ldots,e} t_i > 1$ and*

$$s \leqslant \frac{m}{2} - \log_2\left(\max_{i=1,\ldots,e} t_i - 1\right),$$

then any non-zero LFSR sequence with connecting polynomial g as in Theorem 21 contains the pattern y.

By employing a generalized version of the Weil-Carlitz-Uchiyama bound for rational functions, we can extend Theorem 21 as follows:

Theorem 23. *Consider a connection polynomial $g(X) = \prod_{i=1}^{e} g_i(X) \cdot \prod_{i=1}^{d} h_i(X)$, where $g_i \in \mathbb{F}_2[X]$, $1 \leqslant i \leqslant e$, and $h_j \in \mathbb{F}_2[X]$, $1 \leqslant j \leqslant d$, are distinct irreducible polynomials of the same degree m. Let $\alpha \in \mathbb{F}_{2^m}$ be a primitive element, and let $t_i, u_i \geqslant 1$ be odd positive integers such that α^{t_i} is a root of g_i for every $1 \leqslant i \leqslant e$, and α^{-u_i} is a root of h_i for every $1 \leqslant i \leqslant d$. Under these conditions, the following holds:*

Consider any pattern $y \in \mathbb{F}_2^s$ of length $s \leqslant m$. Then, the number of occurrences N of y in a window of length $2^m - 1$ of any non-zero LFSR sequence with connection polynomial g as above, satisfies

$$\left|N - \frac{2^m - 1}{2^s}\right| \leqslant \left(1 - \frac{1}{2^s}\right)(\max t_i + \max u_i)2^{m/2}.$$

Corollary 24. *Consider the setting of Theorem 23, and any pattern $y \in \mathbb{F}_2^s$ of length s. If*

$$s \leqslant \frac{m}{2} - \log_2(\max t_i + \max u_i),$$

then any non-zero LFSR sequence with connecting polynomial g as in Theorem 23 contains the pattern y.

B. Improved bounds on the burst-covering radius

We are now able to tighten the bounds in Theorem 16, and under certain conditions we can give the exact value of the burst-covering radius of cyclic codes:

Theorem 25. *Consider an $[n, n-r]_2$ binary cyclic code, $\mathcal{C}$, with generator polynomial $g = \prod_{i=1}^{e} g_i$, where $g_i \in \mathbb{F}_2[X]$, for $1 \leqslant i \leqslant e$, are distinct irreducible factors of degrees $d_1 \leqslant d_2 \leqslant \ldots \leqslant d_e$, respectively, and $r = \sum_{i=1}^{e} d_i$. Then, the burst-covering radius b of $\mathcal{C}$ satisfies:*

1) *If g_1 is non-primitive, $b \geqslant r - d_1 + 2$.*

2) *In the case $e = 2$, suppose both g_1 and g_2 are primitive, $d_1 < d_2$, and that either $\gcd(d_1, d_2) < d_2 - d_1$, or $d_2 - d_1 \leqslant 2$. Then $b = d - d_1 + 1 = d_2 + 1$.*

Proof: 1) Consider all possible LFSR sequences with connection polynomial g_1 (in particular, they also have connection polynomial g). If g_1 is not primitive, then there are at least two distinct non-zero such sequences. The pattern $0 \dots 01$ (with $d_1 - 1$ zeros) can only appear in one of them (since the order of the LFSR is d_1), which means there exists a sequence with connection polynomial g containing no runs of zeros of length $d_1 - 1$. By equation (5), $b > r - d_1 + 1$.

2) Thanks to Equation (5), it suffices to show that any LFSR sequence with connection polynomial g contains a run of at least $d_1 - 1$ zeros. Due to the primitivity assumption, an LFSR sequence with minimal connection polynomial g_i, for $i = 1$ or $i = 2$, is a PN sequence. Thus, it contains a run of $d_i - 1 \geqslant d_1 - 1$ zeros.

If the minimal connection polynomial is g, then by Theorem 20 it suffices to check

$$d_1 - 1 < \log_2 \left(1 + \frac{\mathrm{lcm}(\mathrm{ord}(g_1), \mathrm{ord}(g_2))}{2^{(d_1+d_2)/2}} \right).$$

Careful manipulation shows that it suffices to ask $d_1 - 1 \leqslant (d_1+d_2)/2 - \gcd(d_1, d_2)$, which is true if $\gcd(d_1, d_2) < d_2 - d_1$ or if $d_2 - d_1 \leqslant 2$. ∎

Theorem 25 1) shows that the lower bound from Theorem 16 cannot be attained unless the lowest-degree irreducible factor in the generator polynomial for the code is primitive, and 2) shows that there are codes which attain this lower bound.

V. Burst-Covering Radius of Long BCH Codes and Melas Codes

Recall the definition of the binary primitive BCH code of length $n = 2^m - 1$ and designed distance $2e+1$: given $\alpha \in \mathbb{F}_{2^m}$ primitive, the parity-check matrix is defined as

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{2e-1} & \alpha^{2(2e-1)} & \dots & \alpha^{(2e-1)(n-1)} \end{pmatrix}.$$

The parity-check matrix of a binary primitive Melas codes is given by

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

We denote the two codes as $\mathrm{BCH}(e, m)$ and $\mathrm{Melas}(m)$. In what follows, we will consider BCH codes such that

$$2^{\lceil m/2 \rceil} > 2e - 1, \tag{8}$$

which guarantees that the generator polynomial of $\mathrm{BCH}(e, m)$ is $M(X) \triangleq \prod_{i=1}^{e} M_{2e-1}$, where $M_1, M_3, \dots, M_{2e-1}$ are the minimal polynomials of $\alpha, \alpha^3, \dots, \alpha^{2e-1}$ respectively, and all have degree m.

Theorem 26. *If $e > 1$, the burst-covering radius b of $\mathrm{BCH}(e, m)$ which satisfies* (8)*, is bounded by*

$$b \leqslant m\left(e - \frac{1}{2}\right) + \log_2(e - 1) + 1.$$

Proof: Instantiating Corollary 22 with the generator polynomial of $\mathrm{BCH}(e, m)$, $M(X) = \prod_{i=1}^{e} M_{2i-1}$, we can take $t_i = 2i - 1$ for $1 \leqslant i \leqslant e$. We deduce that for any initial condition, an LFSR sequence with connection polynomial M will contain a run of zeros of any length up to $m/2 - \log_2(2e-2)$. The bound now follows from (5). ∎

We can obtain a similar result for Melas codes:

Theorem 27. *The burst-covering radius b of $\mathrm{Melas}(m)$ satisfies $b \leqslant \frac{3}{2}m + 1$.*

We conjecture that the bound in Theorem 26 is essentially tight. Proving a lower bound requires a result like the following:

Conjecture 28. *Consider any pattern $y \in \mathbb{F}_2^s$ of length s. If $s \geqslant \frac{m}{2}(1 + o(1))$ then there exists a non-zero LFSR sequence with connecting polynomial g as in Theorem 21 that does* not *contain the pattern y.*

We are not aware of any result of this type in the literature, and the techniques we have used so far do not seem to be effective for approaching this problem. However, by employing inequality (1), we can give a slight improvement over the lower bound $b \geqslant (e-1)m + 1$ from Theorem 16:

Theorem 29. *The burst-covering radius b of $\mathrm{BCH}(e, m)$ satisfies $b \geqslant (e-1)m+2$. Similarly, $b \geqslant m+2$ for $\mathrm{Melas}(m)$.*

VI. Conclusion

In this paper we initiated the study over burst covering codes. We focused in particular on the rich family of cyclic codes. We showed how the burst-covering radius of cyclic codes depends on the length of runs of zeros in related LFSR sequences. In some cases we can give the exact burst-covering radius. In the specific case of BCH codes, we developed a new bound on the existence of patterns in LFSR sequences, complementing those already found in the literature.

Many open question remain. The immediate problem arising from the case BCH and Melas codes is the gap between the lower bound (Theorem 29) and the upper bound (Theorem 26 and Theorem 27) on the burst-covering radius. Improving the lower bound requires results on the *nonexistence* of patterns in LFSR sequences. To the best of our knowledge, these results are not known yet.

More generally, an important open question is to derive the burst-covering radius of other known families of codes, as well as developing efficient burst-covering algorithms for them. Finally, it is of interest to determine if bounds (1) and (2) can be improved or attained. We leave these questions for future work.

REFERENCES

[1] K. A. S. Abdel-Ghaffar, "On the existence of optimum cyclic burst correcting codes over $GF(q)$," *IEEE Trans. Inform. Theory*, vol. 34, no. 2, pp. 329–332, Mar. 1988.

[2] K. A. S. Abdel-Ghaffar, R. J. McEliece, A. M. Odlyzko, and H. C. A. van Tilborg, "On the existence of optimum cyclic burst-correcting codes," *IEEE Trans. Inform. Theory*, vol. 32, no. 6, pp. 768–775, Nov. 1986.

[3] N. M. Abramson, "A class of systematic codes for non-independent errors," *IRE Trans. on Inform. Theory*, vol. 5, pp. 150–157, Dec. 1959.

[4] L. Carlitz and S. Uchiyama, "Bounds for exponential sums," *Duke Mathematical Journal*, vol. 24, pp. 37–41, 1957.

[5] B. Chazelle and B. Rosenberg, "Computing partial sums in multidimensional arrays," in *SCG '89*, 1989.

[6] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, "Private information retrieval," *J. of the ACM*, vol. 45, no. 6, pp. 965–981, 1998.

[7] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*. North-Holland, 1997.

[8] B. Elspas and R. A. Short, "A note on optimum burst-error-correcting codes," *IRE Trans. on Inform. Theory*, pp. 39–42, Jan. 1962.

[9] P. Fire, "A class of multiple-error-correcting binary codes for non-independent errors," Sylvania Reconnaissance Systems Laboratory, Mountain View, CA, USA, Tech. Rep. Sylvania Report RSL-E-2, 1959.

[10] S. W. Golomb, *Shift Register Sequences*. Holden-Day, San Francisco, 1967.

[11] M. Goresky and A. Klapper, *Algebraic Shift Register Sequences*. Cambridge University Press, 2012.

[12] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge University Press, 1997.

[13] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. North-Holland, 1978.

[14] H. Niederreiter, "Distribution properties of feedback shift register sequences," *Problems of control and information theory- Problemy upravleniya i toerii informatsii*, vol. 15, no. 1, pp. 19–34, 1986.

[15] V. Ramkumar, N. Raviv, and I. Tamo, "Access-redundancy tradeoffs in quantized linear computations," *IEEE Trans. Inform. Theory*, vol. 70, no. 11, pp. 7723–7739, Nov. 2024.

[16] G. Sac Himelfarb and M. Schwartz, "On the burst-covering radius of binary cyclic codes," *arXiv preprint arXiv:2601.00435*, 2026.