Research Article

Construction of Two-Dimensional Cyclic Codes via Cyclotomic Idempotents

Jean Charles Ramanandraibe[1], **Ramamonjy Andriamifidisoa**[1]

1. University of Antananarivo, Antananarivo, Madagascar

This article presents an innovative method for constructing two-dimensional cyclic codes based on the use of primitive idempotents defined via cyclotomic orbits. Our approach exploits the decomposition of the quotient ring $R = \mathbb{F}_q[x,y]/\langle x^s - 1, y^\ell - 1\rangle$ into a direct product of copies of $\mathbb{F}_q$ using central primitive idempotents. This decomposition enables the explicit construction of vector space bases and optimized generator matrices for two-dimensional codes.

The method incorporates spectral analysis via the discrete Fourier transform, establishing a fundamental link between combinatorial (cyclotomic orbits) and algebraic (primitive idempotents) representations of generator idempotents. We demonstrate that the set $B = \{x^m y^n e(x,y) \mid 0 \le m < k, 0 \le n < \ell'\}$ forms a basis of the two-dimensional cyclic code, with parameters $[s\ell, k\ell', (s-k+1)(\ell-\ell'+1)]$.

The results are validated by explicit examples and generator matrix constructions, offering precise control over code parameters and effectively generalizing BCH-type bounds to the two-dimensional context. This systematic approach fills an important gap in the design of high-performance multidimensional codes.

Correspondence: papers@team.qeios.com — Qeios will forward to the authors

1. Introduction

Error-correcting codes play a fundamental role in information theory, ensuring the reliability of modern communication systems [1][2]. One-dimensional cyclic codes, defined as ideals in univariate polynomial rings, benefit from efficient encoding and decoding algorithms. However, contemporary applications demand more powerful codes capable of handling complex dependencies, hence the emergence of multidimensional cyclic codes [3][4].

These codes are modeled as ideals in the quotient ring

$$R = \mathbb{F}_q[x, y]/\langle x^s - 1, y^\ell - 1\rangle,$$

where $\mathbb{F}_q$ satisfies $q \equiv 1 \pmod{s}$ and $q \equiv 1 \pmod{\ell}$. Their construction presents significant challenges, particularly the efficient decomposition of ideals into vector space bases and the design of optimized generator matrices [5].

This article proposes an original method for constructing two-dimensional cyclic codes by exploiting generator idempotents defined via cyclotomic orbits. Our main contributions are:

- **Definition 3.1.** The introduction of two-dimensional primitive idempotents $e_{i,j}(x, y)$ providing an explicit decomposition of the quotient ring R into a direct product of copies of $\mathbb{F}_q$.
- **Proposition 3.2.** The proof that R is semi-simple and isomorphic to $\bigoplus_{i=0}^{s-1} \bigoplus_{j=0}^{\ell-1} \mathbb{F}_q[x, y]e_{i,j}$, establishing the algebraic foundation of our construction.
- **Definition 3.3.** The combinatorial definition of two-dimensional generator idempotents via cyclotomic orbits $C_{j,k}$, providing a systematic method for code construction.
- **Proposition 3.4.** The establishment of the fundamental equality between combinatorial (cyclotomic orbits) and algebraic (primitive idempotents) representations of generator idempotents, connected via the discrete Fourier transform.
- **Theorem 3.6.** The explicit construction of bases for two-dimensional codes of the form $B = \{x^m y^n e(x, y) \mid 0 \leq m < k, 0 \leq n < \ell'\}$, enabling efficient vector space representation.
- **Theorem 3.7.** The complete determination of code parameters $[s\ell, k\ell', (s - k + 1)(\ell - \ell' + 1)]$ and the construction of optimized generator matrices, offering precise control over code characteristics.
- The generalization of BCH-type bounds to the two-dimensional context through the product bound $(s - k + 1)(\ell - \ell' + 1)$ for the minimum distance.

Unlike existing approaches based on univariate idempotents [6] or row decompositions [5], our method provides a unified framework combining idempotents, cyclotomic orbits, and discrete Fourier transforms. This approach ensures precise control over code parameters and effective generalization of BCH-type bounds to the two-dimensional context, filling an important gap in the design of high-performance multidimensional codes [3][4].

The explicit examples and practical constructions demonstrate the effectiveness of our approach, offering new perspectives for applications in advanced communication systems and cryptographic

protocols [7][8].

2. Preliminaries

Notations. Let $\mathbb{F}_q$ be a finite field with q elements. The multiplicative group $\mathbb{F}_q^\times$ is cyclic of order $q-1$. For integers $s, \ell \geq 1$ such that $q \equiv 1 \pmod{s}$ and $q \equiv 1 \pmod{\ell}$, we consider the quotient ring

$$R = \mathbb{F}_q[x,y]/\langle x^s - 1, y^\ell - 1\rangle.$$

The ring R consists of bivariate polynomials modulo the relations $x^s = 1$ and $y^\ell = 1$.

2.1. **Definition (One-dimensional cyclic code).** A cyclic code C of length n over $\mathbb{F}_q$ is an ideal of the ring $R_n = \mathbb{F}_q[x]/\langle x^n - 1\rangle$.

2.2. **Proposition.** *Every cyclic code $C \subseteq R_n$ is a principal ideal, generated by a unique monic polynomial $g(x)$ of minimal degree in C. Moreover, $g(x)$ divides $x^n - 1$.*

2.3. **Definition (Idempotent element).** Let R be a ring. An element $e \in R$ is said to be *idempotent* if $e^2 = e$.

2.4. **Definition (One-dimensional central primitive idempotents).** Let k be a positive integer with $q \equiv 1 \pmod{k}$, and let $\omega \in \mathbb{F}_q$ be a primitive k-th root of unity. In the ring $\mathbb{F}_q[x]/\langle x^k - 1\rangle$, the central primitive idempotents are defined by

$$\zeta_t(x) = \prod_{\substack{i=0 \\ i \neq t}}^{k-1} \frac{x - \omega^i}{\omega^t - \omega^i}.$$

2.5. **Proposition.** These idempotents satisfy

$$\sum_{t=0}^{k-1} \zeta_t(x) = 1, \zeta_t(x)\zeta_{t'}(x) = \delta_{t,t'}\zeta_t(x),$$

where $\delta_{t,t'}$ is the Kronecker delta function.

2.6. **Definition (Cyclotomic coset modulo n in base q).** Let n be a positive integer and q a prime power. For each integer $j \in \{0, \ldots, n-1\}$, the *cyclotomic coset modulo n in base q* containing j is defined by

$$C_j = \{j, jq, jq^2, \ldots, jq^{m_j - 1}\} \pmod{n},$$

where m_j is the smallest positive integer such that $jq^{m_j} \equiv j \pmod{n}$.

2.7. **Definition (One-dimensional generator idempotent).** Let $R_n = \mathbb{F}_q[x]/\langle x^n - 1\rangle$, with $q \equiv 1 \pmod{n}$, and C a cyclic code of length n over $\mathbb{F}_q$. The generator idempotent of C is given by

$$e(x) = \sum_{j \in S(q)} a_j \sum_{i \in C_j} x^i,$$

where $a_j \in \mathbb{F}_q$.

2.8. **Theorem.** *Let $R_n = \mathbb{F}_q[x]/\langle x^n - 1 \rangle$, and C a cyclic code of dimension k in R_n, generated by a generator idempotent $e(x)$. Then, the elements $\{e(x), xe(x), \ldots, x^{k-1}e(x)\}$ form a basis of C.*

3. Construction of Two-Dimensional Codes

We now present our main results concerning the construction of two-dimensional cyclic codes. Our first contribution is the definition of two-dimensional primitive idempotents which form the cornerstone of our approach.

3.1. **Definition (Two-dimensional primitive idempotent).** Let $R = \mathbb{F}_q[x,y]/\langle x^s - 1, y^\ell - 1 \rangle$, where $q \equiv 1 \pmod{s}$ and $q \equiv 1 \pmod{\ell}$, and let $S = \mathbb{F}_q[x]/\langle x^s - 1 \rangle$ and $S' = \mathbb{F}_q[y]/\langle y^\ell - 1 \rangle$. Consider the central primitive idempotents defined by:

$$\zeta_i(x) = \frac{1}{s} \sum_{m=0}^{s-1} \gamma^{(s-i)m} x^m, \eta_j(y) = \frac{1}{\ell} \sum_{n=0}^{\ell-1} \gamma^{(\ell-j)n} y^n,$$

where γ is a primitive s-th root and α is a primitive ℓ-th root of unity in $\mathbb{F}_q$. We define the two-dimensional primitive idempotent $e_{i,j}(x,y)$ by:

$$e_{i,j}(x,y) = \zeta_i(x)\eta_j(y) = \frac{1}{s\ell} \sum_{m=0}^{s-1} \sum_{n=0}^{\ell-1} \gamma^{(s-i)m} \alpha^{(\ell-j)n} x^m y^n.$$

Our second result establishes the fundamental algebraic structure of the quotient ring, demonstrating its semi-simplicity and decomposition into primitive idempotents.

3.2. **Proposition.** *Let $R = \mathbb{F}_q[x,y]/\langle x^s - 1, y^\ell - 1 \rangle$, where $q \equiv 1 \pmod{s}$ and $q \equiv 1 \pmod{\ell}$. Let $S = \mathbb{F}_q[x]/\langle x^s - 1 \rangle$ and $S' = \mathbb{F}_q[y]/\langle y^\ell - 1 \rangle$. Then the ring R is semi-simple and isomorphic to $\bigoplus_{i=0}^{s-1} \bigoplus_{j=0}^{\ell-1} \mathbb{F}_q[x,y]e_{i,j}$, where each $\mathbb{F}_q[x,y]e_{i,j} \cong \mathbb{F}_q$.*

Proof. Let $\gamma \in \mathbb{F}_q$ be a primitive s-th root of unity ($\gamma^s = 1$, $\gamma^k \neq 1$ for $0 < k < s$) and $\delta \in \mathbb{F}_q$ be a primitive ℓ-th root of unity ($\delta^\ell = 1$, $\delta^k \neq 1$ for $0 < k < \ell$). Since $q \equiv 1 \pmod{s}$ and $q \equiv 1 \pmod{\ell}$, the field $\mathbb{F}_q$ contains these roots, and $\gcd(s,q) = 1, \gcd(\ell,q) = 1$.

- Dimension. The ring $R = \mathbb{F}_q[x,y]/\langle x^s - 1, y^\ell - 1 \rangle$ is a vector space over $\mathbb{F}_q$ with basis $\{x^i y^j \mid 0 \leq i \leq s-1, 0 \leq j \leq \ell - 1\}$. Thus, $\dim_{\mathbb{F}_q} R = s \cdot \ell$.

- Factorization. In $\mathbb{F}_q[x]$, $x^s - 1 = \prod_{i=0}^{s-1}(x - \gamma^i)$, because γ is a primitive s-th root and $q \equiv 1 \pmod{s}$. Similarly, in $\mathbb{F}_q[y]$, $y^\ell - 1 = \prod_{j=0}^{\ell-1}(y - \delta^j)$. In $\mathbb{F}_q[x,y]$, the ideals $\langle x - \gamma^i \rangle$ and $\langle y - \delta^j \rangle$ are maximal, and for each pair (i,j), the ideal $\langle x - \gamma^i, y - \delta^j \rangle$ is maximal. By the Chinese Remainder Theorem, since the ideals $\langle x - \gamma^i, y - \delta^j \rangle$ are pairwise coprime, we have:
  $R \cong \bigoplus_{i=0}^{s-1} \bigoplus_{j=0}^{\ell-1} \mathbb{F}_q[x,y]/\langle x - \gamma^i, y - \delta^j \rangle$.
  Each quotient $\mathbb{F}_q[x,y]/\langle x - \gamma^i, y - \delta^j \rangle \cong \mathbb{F}_q$, because evaluation at $(x,y) = (\gamma^i, \delta^j)$ gives a field isomorphic to $\mathbb{F}_q$. Thus, $R \cong \mathbb{F}_q^{s \cdot \ell}$.
- Idempotents. Define $e_{i,j}(x,y) = \frac{1}{s\ell} \sum_{m=0}^{s-1} \sum_{n=0}^{\ell-1} \gamma^{(s-i)m} \delta^{(\ell-j)n} x^m y^n \in R$. Verify the properties:
  - Idempotence. Evaluate $e_{i,j}(x,y)$ at $(x,y) = (\gamma^{i'}, \delta^{j'})$:
    $e_{i,j}(\gamma^{i'}, \delta^{j'}) = \frac{1}{s\ell} \sum_{m=0}^{s-1} \sum_{n=0}^{\ell-1} \gamma^{(s-i)m} \delta^{(\ell-j)n} \gamma^{i'm} \delta^{j'n} = \frac{1}{s\ell} \sum_{m=0}^{s-1} \gamma^{m(s-i+i')} \sum_{n=0}^{\ell-1} \delta^{n(\ell-j+j')}$.
    If $i = i'$ and $j = j'$, then $\gamma^{m(s-i+i')} = \gamma^{ms} = 1$, $\delta^{n(\ell-j+j')} = \delta^{n\ell} = 1$, and the sum gives $\frac{1}{s\ell} \cdot s \cdot \ell = 1$. If $i \neq i'$, the sum $\sum_{m=0}^{s-1} \gamma^{m(s-(i-i'))} = 0$, because $\gamma^{s-(i-i')} \neq 1$. Similarly, if $j \neq j'$, $\sum_{n=0}^{\ell-1} \delta^{n(\ell-(j-j'))} = 0$. Thus, $e_{i,j}(\gamma^{i'}, \delta^{j'}) = \delta_{i,i'} \delta_{j,j'}$. Consequently, $e_{i,j}^2 = e_{i,j}$.
  - Orthogonality. For $(i,j) \neq (i',j')$, we have $e_{i,j} e_{i',j'} = 0$, because $e_{i,j}(\gamma^{i''}, \delta^{j''}) e_{i',j'}(\gamma^{i''}, \delta^{j''}) = \delta_{i,i''} \delta_{j,j''} \delta_{i',i''} \delta_{j',j''} = 0$, the indices where $e_{i,j}$ and $e_{i',j'}$ are nonzero being disjoint.
  - Sum. Verify $\sum_{i=0}^{s-1} \sum_{j=0}^{\ell-1} e_{i,j} = 1$. Evaluating at $(\gamma^{i'}, \delta^{j'})$:
    $\sum_{i=0}^{s-1} \sum_{j=0}^{\ell-1} e_{i,j}(\gamma^{i'}, \delta^{j'}) = \sum_{i=0}^{s-1} \sum_{j=0}^{\ell-1} \delta_{i,i'} \delta_{j,j'} = 1$,
    because exactly one term is nonzero (for $i = i', j = j'$). Thus, $\sum_{i=0}^{s-1} \sum_{j=0}^{\ell-1} e_{i,j} = 1$.
  - Centrality. For all $f \in R$, we have $e_{i,j} f = f e_{i,j}$. Evaluating at $(\gamma^{i'}, \delta^{j'})$, $(e_{i,j} f)(\gamma^{i'}, \delta^{j'}) = e_{i,j}(\gamma^{i'}, \delta^{j'}) f(\gamma^{i'}, \delta^{j'}) = \delta_{i,i'} \delta_{j,j'} f(\gamma^{i'}, \delta^{j'})$, and similarly for $f e_{i,j}$. Thus, $e_{i,j}$ is central.
  - Isomorphism. Each ideal $\mathbb{F}_q[x,y] e_{i,j} \cong \mathbb{F}_q$, via the projection $f \mapsto f(\gamma^i, \delta^j)$. Indeed, $e_{i,j} f = f(\gamma^i, \delta^j) e_{i,j}$, so $\mathbb{F}_q[x,y] e_{i,j} \cong \mathbb{F}_q$. By the decomposition of orthogonal idempotents, $R \cong \bigoplus_{i=0}^{s-1} \bigoplus_{j=0}^{\ell-1} \mathbb{F}_q[x,y] e_{i,j}$.
  - Semi-simplicity. Since $R \cong \mathbb{F}_q^{s \cdot \ell}$, a product of fields, R is semi-simple by ring theory.

Thus, R is semi-simple and $R \cong \bigoplus_{i=0}^{s-1} \bigoplus_{j=0}^{\ell-1} \mathbb{F}_q[x,y] e_{i,j}$, where each $\mathbb{F}_q[x,y] e_{i,j} \cong \mathbb{F}_q$. □

We now introduce the combinatorial definition of two-dimensional generator idempotents via cyclotomic orbits, which provides a systematic method for code construction.

3.3. **Definition.** Let C be a two-dimensional cyclic code of length $n = s\ell$ over $\mathbb{F}_q$ in $R = \mathbb{F}_q[x,y]/\langle x^s - 1, y^\ell - 1\rangle$, with $q \equiv 1 \pmod{s}$ and $q \equiv 1 \pmod{\ell}$. The generator idempotent $e(x,y)$ is written as:

$$e(x,y) = \sum_{(j,k)\in T} a_{j,k} \sum_{(m,n)\in C_{j,k}} x^m y^n,$$

where $T \subseteq \{0,\dots,s-1\}\times\{0,\dots,\ell-1\}$, $C_{j,k} = \{(jq^r \bmod s, kq^r \bmod \ell) \mid r \geq 0\}$ and $a_{j,k} \in \mathbb{F}_q$.

T is a set of representatives of disjoint cyclotomic orbits $C_{j,k}$, and the coefficients are typically $a_{j,k} = 1$ if $(j,k) \in T$, $a_{j,k} = 0$ otherwise.

A fundamental result of our work is the establishment of the equivalence between combinatorial and algebraic representations of generator idempotents.

3.4. **Proposition.** *Let C be a two-dimensional cyclic code of length $n = s\ell$ over $\mathbb{F}_q$ in $R = \mathbb{F}_q[x,y]/\langle x^s - 1, y^\ell - 1\rangle$, with $q \equiv 1 \pmod{s}$ and $q \equiv 1 \pmod{\ell}$. Then, we have the equality*

$$e(x,y) = \sum_{i=0}^{s-1}\sum_{j=0}^{\ell-1} c_{i,j} e_{i,j}(x,y),$$

where $c_{i,j} = e(\gamma^i, \alpha^j) \in \{0,1\}$, $e_{i,j}(x,y) = \zeta_i(x)\eta_j(y)$, $\zeta_i(x) = \frac{1}{s}\sum_{m=0}^{s-1}\gamma^{-im}x^m$, $\eta_j(y) = \frac{1}{\ell}\sum_{n=0}^{\ell-1}\alpha^{-jn}y^n$, *and γ, α are primitive roots of order s, ℓ.*

Proof. Let C be a two-dimensional cyclic code of length $n = s\ell$ over $\mathbb{F}_q$ in $R = \mathbb{F}_q[x,y]/\langle x^s - 1, y^\ell - 1\rangle$, with $q \equiv 1 \pmod{s}$, $q \equiv 1 \pmod{\ell}$. Let γ be a primitive root of order s, α a primitive root of order ℓ in $\mathbb{F}_q$. Show that

$$e(x,y) = \sum_{(j,k)\in T} a_{j,k} \sum_{(m,n)\in C_{j,k}} x^m y^n = \sum_{i=0}^{s-1}\sum_{j=0}^{\ell-1} c_{i,j} e_{i,j}(x,y),$$

where $T \subseteq \{0,\dots,s-1\}\times\{0,\dots,\ell-1\}$, $C_{j,k} = \{(jq^r \bmod s, kq^r \bmod \ell) \mid r \geq 0\}$, $a_{j,k} \in \mathbb{F}_q$, $c_{i,j} = e(\gamma^i, \alpha^j) \in \{0,1\}$, $e_{i,j}(x,y) = \zeta_i(x)\eta_j(y)$, $\zeta_i(x) = \frac{1}{s}\sum_{m=0}^{s-1}\gamma^{-im}x^m$, $\eta_j(y) = \frac{1}{\ell}\sum_{n=0}^{\ell-1}\alpha^{-jn}y^n$.

Step 1: Coefficients of the first form.

Write $e(x,y) = \sum_{m=0}^{s-1}\sum_{n=0}^{\ell-1} b_{m,n}x^m y^n$, where

$$b_{m,n} = \begin{cases} a_{j,k} & \text{if~} (m,n) \in C_{j,k}, (j,k) \in T, \\ 0 & \text{otherwise.} \end{cases}$$

The discrete Fourier transform gives

$$c_{i,j} = e(\gamma^i, \alpha^j) = \sum_{m=0}^{s-1}\sum_{n=0}^{\ell-1} b_{m,n}\gamma^{im}\alpha^{jn}.$$

Substitute $e(x,y) = \sum_{(j,k)\in T} a_{j,k} \sum_{(m,n)\in C_{j,k}} x^m y^n$:

$$e(\gamma^i, \alpha^j) = \sum_{(j,k)\in T} a_{j,k} \sum_{(m,n)\in C_{j,k}} \gamma^{im}\alpha^{jn}.$$

For $(m,n) = (jq^r \bmod s, kq^r \bmod \ell) \in C_{j,k}$,

$$\sum_{(m,n)\in C_{j,k}} \gamma^{im}\alpha^{jn} = \sum_{r=0}^{|C_{j,k}|-1} \gamma^{i(jq^r \bmod s)}\alpha^{j(kq^r \bmod \ell)}.$$

This sum is nonzero if $(i,j) \in C_{j',k'}$ for some $(j',k') \in T$, in which case it equals $|C_{j',k'}| \cdot a_{j',k'}$ (by properties of roots of unity and orbits). Thus,

$$c_{i,j} = \sum_{(j,k)\in T} a_{j,k} \cdot |C_{j,k}| \cdot 1_{(i,j)\in C_{j,k}}.$$

If $a_{j,k} = 1$ for $(j,k) \in T$, and $c_{i,j} \in \{0,1\}$, then $c_{i,j} = 1$ if $(i,j) \in C_{j,k}$ for some $(j,k) \in T$, otherwise $c_{i,j} = 0$.

Step 2: Second form.

Consider

$$e(x,y) = \sum_{i=0}^{s-1}\sum_{j=0}^{\ell-1} c_{i,j} e_{i,j}(x,y), e_{i,j}(x,y) = \zeta_i(x)\eta_j(y).$$

The primitive idempotents are

$$\zeta_i(x) = \frac{1}{s}\sum_{m=0}^{s-1} \gamma^{-im}x^m, \eta_j(y) = \frac{1}{\ell}\sum_{n=0}^{\ell-1} \alpha^{-jn}y^n,$$

with

$$\zeta_i(\gamma^{i'}) = \delta_{i,i'}, \eta_j(\alpha^{j'}) = \delta_{j,j'}.$$

Thus,

$$e_{i,j}(\gamma^{i'}, \alpha^{j'}) = \zeta_i(\gamma^{i'})\eta_j(\alpha^{j'}) = \delta_{i,i'}\delta_{j,j'}.$$

Evaluate

$$e(\gamma^{i'}, \alpha^{j'}) = \sum_{i=0}^{s-1}\sum_{j=0}^{\ell-1} c_{i,j} e_{i,j}(\gamma^{i'}, \alpha^{j'}) = \sum_{i=0}^{s-1}\sum_{j=0}^{\ell-1} c_{i,j}\delta_{i,i'}\delta_{j,j'} = c_{i',j'}.$$

So, $c_{i,j} = e(\gamma^i, \alpha^j)$, as in the proposition.

Step 3: Equivalence.

The coefficients $b_{m,n}$ are related to $c_{i,j}$ by the inverse Fourier transform:

$$b_{m,n} = \frac{1}{s\ell} \sum_{i=0}^{s-1} \sum_{j=0}^{\ell-1} c_{i,j} \gamma^{-im} \alpha^{-jn}.$$

Substitute $c_{i,j} = \sum_{m'=0}^{s-1} \sum_{n'=0}^{\ell-1} b_{m',n'} \gamma^{im'} \alpha^{jn'}$:

$$b_{m,n} = \frac{1}{s\ell} \sum_{i=0}^{s-1} \sum_{j=0}^{\ell-1} \left(\sum_{m'=0}^{s-1} \sum_{n'=0}^{\ell-1} b_{m',n'} \gamma^{im'} \alpha^{jn'} \right) \gamma^{-im} \alpha^{-jn}.$$

Rearrange:

$$b_{m,n} = \sum_{m'=0}^{s-1} \sum_{n'=0}^{\ell-1} b_{m',n'} \left(\frac{1}{s} \sum_{i=0}^{s-1} \gamma^{i(m'-m)} \right) \left(\frac{1}{\ell} \sum_{j=0}^{\ell-1} \alpha^{j(n'-n)} \right).$$

The sums are

$$\frac{1}{s} \sum_{i=0}^{s-1} \gamma^{i(m'-m)} = \delta_{m',m}, \frac{1}{\ell} \sum_{j=0}^{\ell-1} \alpha^{j(n'-n)} = \delta_{n',n}.$$

Thus,

$$b_{m,n} = \sum_{m'=0}^{s-1} \sum_{n'=0}^{\ell-1} b_{m',n'} \delta_{m',m} \delta_{n',n} = b_{m,n}.$$

The two forms are therefore equivalent, because they produce the same coefficients $b_{m,n}$.

Step 4: Idempotence.

For $e^2 = e$, the $c_{i,j}$ must satisfy $c_{i,j}^2 = c_{i,j}$, i.e., $c_{i,j} \in \{0, 1\}$. Since $c_{i,j} = e(\gamma^i, \alpha^j)$, and $e^2 = e$, then

$$e(\gamma^i, \alpha^j)^2 = e(\gamma^i, \alpha^j) \implies c_{i,j}^2 = c_{i,j}.$$

This is satisfied if $c_{i,j} \in \{0, 1\}$. Moreover, T is chosen so that $\bigcup_{(j,k) \in T} C_{j,k}$ is stable under convolution, ensuring idempotence.

Conclusion. The two expressions for $e(x, y)$ are equivalent via the Fourier transform, with $c_{i,j} = e(\gamma^i, \alpha^j) \in \{0, 1\}$. $\square$

We now establish the important property concerning dual representations of elements in the quotient ring.

3.5. **Proposition.** *Let $R = \mathbb{F}_q[x, y] / \langle x^s - 1, y^\ell - 1 \rangle$, with γ a primitive s-th root and α a primitive ℓ-th root in $\mathbb{F}_q$. Every element $f(x, y) \in R$ can be written equivalently as:*

1. $f(x,y) = \sum_{m=0}^{s-1} \sum_{n=0}^{\ell-1} a_{m,n} x^m y^n$, with $a_{m,n} \in \mathbb{F}_q$. Since $x^s = 1$, $y^\ell = 1$, the basis of R is $\{x^m y^n \mid 0 \le m \le s-1, 0 \le n \le \ell-1\}$.
2. $f(x,y) = \sum_{i=0}^{s-1} \sum_{j=0}^{\ell-1} c_{i,j} e_{i,j}(x,y)$, where $c_{i,j} \in \mathbb{F}_q$, $c_{i,j} = f(\gamma^i, \alpha^j)$, and the idempotents are $e_{i,j}(x,y) = \frac{1}{s\ell} \sum_{m=0}^{s-1} \sum_{n=0}^{\ell-1} \gamma^{-im} \alpha^{-jn} x^m y^n$.

Proof. Let $R = \mathbb{F}_q[x,y]/\langle x^s - 1, y^\ell - 1 \rangle$, where $\gamma \in \mathbb{F}_q$ is a primitive s-th root ($\gamma^s = 1$, $\gamma^k \neq 1$ for $0 < k < s$) and $\alpha \in \mathbb{F}_q$ is a primitive ℓ-th root ($\alpha^\ell = 1, \alpha^k \neq 1$ for $0 < k < \ell$). Since $q \equiv 1 \pmod{s}$ and $q \equiv 1 \pmod{\ell}$, these roots exist in $\mathbb{F}_q$.

- Representation 1. Every element $f(x,y) \in R$ is a polynomial in x and y modulo $\langle x^s - 1, y^\ell - 1 \rangle$. Since $x^s = 1$ and $y^\ell = 1$ in R, every monomial $x^m y^n$ can be reduced to $x^{m \bmod s} y^{n \bmod \ell}$. Thus, $f(x,y)$ is written as:
  $$f(x,y) = \sum_{m=0}^{s-1} \sum_{n=0}^{\ell-1} a_{m,n} x^m y^n,$$
  where $a_{m,n} \in \mathbb{F}_q$. The family $\{x^m y^n \mid 0 \le m \le s-1, 0 \le n \le \ell-1\}$ forms a basis of R as a vector space over $\mathbb{F}_q$, because the monomials are linearly independent (dimension $s \cdot \ell$).
- Representation 2. Define the idempotents $e_{i,j}(x,y) = \frac{1}{s\ell} \sum_{m=0}^{s-1} \sum_{n=0}^{\ell-1} \gamma^{-im} \alpha^{-jn} x^m y^n$. Verify their properties:
  - Evaluation. Evaluate $e_{i,j}(x,y)$ at $(x,y) = (\gamma^{i'}, \alpha^{j'})$:
    $$e_{i,j}(\gamma^{i'}, \alpha^{j'}) = \frac{1}{s\ell} \sum_{m=0}^{s-1} \sum_{n=0}^{\ell-1} \gamma^{-im} \alpha^{-jn} \gamma^{i'm} \alpha^{j'n} = \frac{1}{s\ell} \sum_{m=0}^{s-1} \gamma^{m(i'-i)} \sum_{n=0}^{\ell-1} \alpha^{n(j'-j)}.$$
    If $i = i'$, then $\gamma^{m(i'-i)} = 1$, and the sum over m gives s. Otherwise, $\sum_{m=0}^{s-1} \gamma^{m(i'-i)} = 0$, because $\gamma^{i'-i} \neq 1$. Similarly for $j = j'$. Thus:
    $$e_{i,j}(\gamma^{i'}, \alpha^{j'}) = \delta_{i,i'} \delta_{j,j'}.$$
  - Idempotence. Since $e_{i,j}(\gamma^{i'}, \alpha^{j'}) = \delta_{i,i'} \delta_{j,j'}$, we have $e_{i,j}^2 = e_{i,j}$, because the evaluation of $e_{i,j}^2$ gives $\delta_{i,i'} \delta_{j,j'} \cdot \delta_{i,i'} \delta_{j,j'} = \delta_{i,i'} \delta_{j,j'}$.
  - Orthogonality. For $(i,j) \neq (i',j')$, $e_{i,j} e_{i',j'} = 0$, because $e_{i,j}(\gamma^{i''}, \alpha^{j''}) e_{i',j'}(\gamma^{i''}, \alpha^{j''}) = \delta_{i,i''} \delta_{j,j''} \delta_{i',i''} \delta_{j',j''} = 0$.
  - Sum. Verify $\sum_{i=0}^{s-1} \sum_{j=0}^{\ell-1} e_{i,j} = 1$:
    $$\sum_{i=0}^{s-1} \sum_{j=0}^{\ell-1} e_{i,j}(\gamma^{i'}, \alpha^{j'}) = \sum_{i=0}^{s-1} \sum_{j=0}^{\ell-1} \delta_{i,i'} \delta_{j,j'} = 1,$$
    because exactly one term is nonzero. Thus, $\sum_{i=0}^{s-1} \sum_{j=0}^{\ell-1} e_{i,j} = 1$.
  - Representation. Every $f(x,y) \in R$ can be written as:
    $$f(x,y) = \sum_{i=0}^{s-1} \sum_{j=0}^{\ell-1} c_{i,j} e_{i,j}(x,y),$$
    where $c_{i,j} = f(\gamma^i, \alpha^j)$. Indeed, evaluate $f(x,y) = \sum_{i,j} f(\gamma^i, \alpha^j) e_{i,j}(x,y)$ at $(\gamma^{i'}, \alpha^{j'})$:

$\sum_{i=0}^{s-1}\sum_{j=0}^{\ell-1} f(\gamma^i,\alpha^j)e_{i,j}(\gamma^{i'},\alpha^{j'}) = \sum_{i=0}^{s-1}\sum_{j=0}^{\ell-1} f(\gamma^i,\alpha^j)\delta_{i,i'}\delta_{j,j'} = f(\gamma^{i'},\alpha^{j'})$.

Since f is completely determined by its values at (γ^i,α^j), the representation is correct.

- Equivalence. To relate the two representations, express the coefficients $a_{m,n}$ in terms of $c_{i,j}$. If $f(x,y) = \sum_{m=0}^{s-1}\sum_{n=0}^{\ell-1} a_{m,n}x^m y^n = \sum_{i=0}^{s-1}\sum_{j=0}^{\ell-1} c_{i,j}e_{i,j}(x,y)$, evaluate at (γ^i,α^j):

  $f(\gamma^i,\alpha^j) = \sum_{m=0}^{s-1}\sum_{n=0}^{\ell-1} a_{m,n}\gamma^{im}\alpha^{jn} = c_{i,j}$.

  Conversely, the $a_{m,n}$ are obtained by the discrete Fourier transform:

  $a_{m,n} = \frac{1}{s\ell}\sum_{i=0}^{s-1}\sum_{j=0}^{\ell-1} f(\gamma^i,\alpha^j)\gamma^{-im}\alpha^{-jn}$.

This shows that the two representations are equivalent, because the $e_{i,j}$ form an orthogonal basis and the $x^m y^n$ form a canonical basis.

Thus, every $f(x,y)\in R$ can be written equivalently in the two given forms. $\square$

A central result of our work is the explicit construction of bases for two-dimensional cyclic codes, which enables efficient vector space representation.

3.6. Theorem. *Let $R = \mathbb{F}_q[x,y]/\langle x^s-1, y^\ell-1\rangle$, with $q \equiv 1 \pmod{s}$ and $q \equiv 1 \pmod{\ell}$, guaranteeing the existence of primitive roots γ of order s and α of order ℓ in $\mathbb{F}_q$. Let C be a two-dimensional cyclic code generated by an idempotent $e(x,y)$ with $e(x,y) = a(x,y)g(x,y)$, where $g(x,y)$ is the monic generator polynomial with degrees $\deg_x g = s-k$, $\deg_y g = \ell - \ell'$, and $h(x,y)$ satisfies $g(x,y)h(x,y) = (x^s-1)(y^\ell-1)$, with $\deg_x h = k$ and $\deg_y h = \ell'$. Then, the set $B = \{x^m y^n e(x,y) \mid 0 \le m < k,\, 0 \le n < \ell'\}$ forms a basis of C over $\mathbb{F}_q$.*

Proof. Show that

$$B = \{x^m y^n e(x,y) \mid 0 \le m \le k-1,\, 0 \le n \le \ell - 1\}$$

is a basis of

$$C = \langle e(x,y)\rangle \subset R = \mathbb{F}_q[x,y]/\langle x^s-1, y^\ell-1\rangle.$$

Linear independence.

Suppose there exist scalars $\beta_{m,n}\in\mathbb{F}_q$ such that

$$\sum_{m=0}^{k-1}\sum_{n=0}^{\ell-1}\beta_{m,n}x^m y^n e(x,y) = 0 \quad \text{in } R.$$

Let

$$l(x,y) = \sum_{m=0}^{k-1} \sum_{n=0}^{\ell-1} \beta_{m,n} x^m y^n \in \mathbb{F}_q[x,y], \deg_x l < k, \deg_y l < \ell.$$

Then,

$$l(x,y)e(x,y) = 0\text{-in-}R \Longrightarrow l(x,y)e(x,y) = u(x,y)(x^s - 1)(y^\ell - 1)$$

for some $u(x,y) \in \mathbb{F}_q[x,y]$. Write

$$e(x,y) = a(x,y)g(x,y), g(x,y)h(x,y) = (x^s - 1)(y^\ell - 1),$$

where g is the generator polynomial and h its check polynomial. We obtain:

$$l(x,y)a(x,y)g(x,y) = u(x,y)g(x,y)h(x,y) \Longrightarrow l(x,y)a(x,y) = u(x,y)h(x,y).$$

Since $\deg_x l < k = \deg_x h$ and $\deg_y l < \ell' = \deg_y h$, the polynomial $u(x,y)$ must be zero for the equality to hold in $\mathbb{F}_q[x,y]$. Thus,

$$l(x,y)a(x,y) = 0 \Longrightarrow l(x,y) = 0$$

because $a(x,y) \neq 0$. We conclude that $\beta_{m,n} = 0$ for all (m,n). Therefore, B is linearly independent.

Generation.

Let $c \in C$. Then $c = p(x,y)e(x,y)$ for some $p(x,y) \in R$. Perform Euclidean division of $p(x,y)$ by $h(x,y)$:

$$p(x,y) = q(x,y)h(x,y) + r(x,y), \deg_x r < k, \deg_y r < \ell'.$$

In R, since $h(x,y)e(x,y) = a(x,y)g(x,y)h(x,y) = a(x,y)(x^s - 1)(y^\ell - 1) = 0$, we have:

$$c = p(x,y)e(x,y) = r(x,y)e(x,y) = \sum_{m=0}^{k-1} \sum_{n=0}^{\ell'-1} \beta_{m,n} x^m y^n e(x,y) \in span(B),$$

where $\beta_{m,n}$ are the coefficients of $r(x,y)$.

Conclusion.

The set B is linearly independent and generates C, so B is a basis of C over $\mathbb{F}_q$. $\square$

The following result provides the complete determination of code parameters and the construction of optimized generator matrices.

3.7. **Theorem.** *Let C be a two-dimensional cyclic code over $R = \mathbb{F}_q[x,y]/\langle x^s - 1, y^\ell - 1 \rangle$, with $q \equiv 1 \pmod{s}$ and $q \equiv 1 \pmod{\ell}$, having basis $B = \{x^m y^n e(x,y) \mid 0 \leq m < k, 0 \leq n < \ell'\}$. Then, the*

parameters of C are $[s\ell, k\ell', (s-k+1)(\ell-\ell'+1)]$, and the generator matrix G of C is a matrix of size $k\ell' \times s\ell$ given by

$$G = \begin{pmatrix} \varphi(e) \\ \varphi(xe) \\ \vdots \\ \varphi(x^{k-1}e) \\ \varphi(ye) \\ \varphi(xye) \\ \vdots \\ \varphi(x^{k-1}ye) \\ \vdots \\ \varphi(x^{k-1}y^{\ell'-1}e) \end{pmatrix},$$

where $\varphi : R \to \mathbb{F}_q^{s\ell}$ is the isomorphism that associates to each polynomial $f(x,y) \in R$ the vector of its coefficients flattened row by row.

Proof. The length of C is $s\ell$ because $C \subseteq R \cong \mathbb{F}_q^{s\ell}$. The dimension is $k\ell'$ because the basis $B = \{x^m y^n e(x,y) \mid 0 \le m < k, 0 \le n < \ell'\}$ contains $k\ell'$ elements. The minimum distance is $(s-k+1)(\ell-\ell'+1)$, because C is isomorphic to the tensor product of the one-dimensional cyclic codes $C_x = \langle g_1(x) \rangle$ with parameters $[s, k, s-k+1]$ and $C_y = \langle g_2(y) \rangle$ with parameters $[\ell, \ell', \ell-\ell'+1]$, with $g(x,y) = g_1(x)g_2(y)$, and the distance of a tensor code is the product of the distances of the component codes [1].

The generator matrix G has as rows the vectors $\varphi(x^m y^n e(x,y))$ for $0 \le m < k$, $0 \le n < \ell'$, ordered lexicographically by n then m. This results from the linearity of φ and the fact that B is a basis of C, each element $x^m y^n e(x,y)$ corresponding to a row of G. $\square$

To illustrate our method, we present a concrete example of constructing a two-dimensional cyclic code.

3.8. **Example.** Let $\mathbb{F}_2$, $s = 3$, $\ell = 2$, $q = 2$. Choose $\gamma = 2$ (primitive root of order 3 of unity), $\alpha = 1$ (primitive root of order 2 of unity).

Cyclotomic orbits.

$$C_{0,0} = \{(0,0)\}, C_{1,1} = \{(1,1),(2,0)\}.$$

Set of representatives.

$$T = \{(0,0),(1,1)\}.$$

Primitive idempotents. (Binary coefficients)

$$e_{0,0}(x,y)=1, e_{1,1}(x,y)=xy+x^2.$$

Chosen idempotent by sum over orbits.

$$e(x,y)=\sum_{(j,k)\in T}\sum_{(m,n)\in C_{j,k}} x^m y^n = e_{0,0}(x,y)+e_{1,1}(x,y)=1+xy+x^2.$$

Idempotence verification.

$$e(x,y)^2=(1+xy+x^2)^2=1+x^2+x^4y^2\equiv 1+xy+x^2=e(x,y) \pmod{x^3-1,y^2-1}.$$

Choice of degrees for the basis.

$$k_x=2, k_y=2.$$

Code basis.

$$B=\{e, xe, ye, xye\}.$$

Explicit expressions.

$$xe=x+x^2y+x^3\equiv x+x^2y+1, ye=y+xy^2+x^2y\equiv y+x+x^2y,$$

$$xye=xy+x^2y^2+x^3y\equiv xy+x^2+xy.$$

Associated vectors (lexicographic order (i,j), $i=0..2$, $j=0..1$).

$$\varphi(e)=(1,0,1,0,1,0), \varphi(xe)=(1,1,0,0,1,0), \varphi(ye)=(0,1,1,0,1,0), \varphi(xye)=(0,1,0,1,0,1).$$

Generator matrix.

$$G=\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \in \mathbb{F}_2^{4\times 6}.$$

Code parameters.

$$n=s\ell=6, \dim_{\mathbb{F}_2} C=k_xk_y=4, d_{\min}=2.$$

Conclusion.

$$[n,k,d]_2=[6,4,2].$$

4. Conclusion

This article has presented a systematic method for constructing two-dimensional cyclic codes based on the use of primitive idempotents and cyclotomic orbits. The main contributions include:

- The definition of two-dimensional primitive idempotents $e_{i,j}(x,y)$ (Definition 3.1) enabling the decomposition of the quotient ring $R = \mathbb{F}_q[x,y]/\langle x^s - 1, y^\ell - 1\rangle$ into a direct product of copies of $\mathbb{F}_q$
- The establishment of the fundamental equality between combinatorial and algebraic representations of generator idempotents (Proposition 3.4), connecting cyclotomic orbits to primitive idempotents via the discrete Fourier transform
- The explicit construction of bases for two-dimensional codes of the form $B = \{x^m y^n e(x,y) \mid 0 \leq m < k, 0 \leq n < \ell'\}$ (Theorem 3.6)
- The complete determination of code parameters $[s\ell, k\ell', (s-k+1)(\ell-\ell'+1)]$ and the construction of optimized generator matrices (Theorem 3.7)
- The generalization of BCH-type bounds to the two-dimensional context through the product bound $(s-k+1)(\ell-\ell'+1)$

The explicit example (Example 3.8) and practical constructions demonstrate the effectiveness of our approach. The proposed method offers precise control over code parameters and fills an important gap in the design of high-performance multidimensional codes [3][4].

Research perspectives include extending this approach to higher dimensions ($s > 2$), developing efficient decoding algorithms adapted to these vector bases, and optimizing cyclotomic orbits to maximize the minimum distance. This method also opens the way to new applications in advanced communication systems and cryptographic protocols [7][8].

Notes

MSC (2025): 13F20, 16D25, 94B60.

References

1. [a], [b] *MacWilliams FJ, Sloane NJA (1977). The Theory of Error-Correcting Codes. North-Holland Publishing Company.*
2. [A] *Blahut RE (2003). Algebraic Codes for Data Transmission. Cambridge University Press.*

3. a, b, c *Bhardwaj M, Raka M (2022). "Construction of Multicyclic Codes Using Gröbner Bases." Des Codes Cryptogr.* ***90****(2):387–406. doi:10.1007/s10623-022-01036-8.*
4. a, b, c *Andriamifidisoa R (2019). "Multicyclic Codes and Gröbner Bases." J Symb Comput.* ***90****:100–120. doi:10.1016/j.jsc.2018.04.008.*
5. a, b *Sepasdar Z (2017). "Generator Matrix for Two-Dimensional Cyclic Codes of Arbitrary Length." arXiv preprint. arXiv:1704.08070.*
6. ^ *Han S (2022). "Cyclotomic Cosets and Coding Theory." J Algebra.* ***600****:50–70. doi:10.1016/j.jalgebra.2022.02.015.*
7. a, b *McEliece RJ (1978). "A Public-Key Cryptosystem Based on Algebraic Coding Theory." DSN Progress Report. Jet Propulsion Laboratory.*
8. a, b *Lalasoa RM (2019). "Multicyclic Codes and Quantum Perspectives with McEliece Cryptosystems." PhD Thesis. University of Antananarivo, Madagascar.*

Declarations

Funding: No specific funding was received for this work.

Potential competing interests: No potential competing interests to declare.