A Computer Algebraic Approach for the Classification of a Family of Cyclic Codes over Finite Fields via Hamming Distance

Nhan T.V. Nguyen[1] and Nghia T.H. Tran[2]
[1]Vietnam National University, Ho Chi Minh City, Vietnam
[2]Ho Chi Minh City University of Education, Vietnam
24N21102@student.hcmus.edu.vn and nghiatth@hcmue.edu.vn

May 8, 2026

Abstract

The classification of minimum Hamming distances of cyclic codes over finite fields is a central problem in algebraic coding theory. In this paper, we study cyclic codes associated with prime lengths in the modular setting. More precisely, let $n \neq p$ be primes and let m be a positive integer. We consider cyclic codes $C = \langle g \rangle \subseteq \mathbb{F}_{p^m}[x]/\langle x^n - 1 \rangle$, where g is a monic divisor of $x^n - 1$. The classification of the minimum Hamming distances of such codes was previously known only for the small prime values $n = 2, 3, 5, 7$, and remained open for prime lengths $n \geq 11$. We address this problem for arbitrary prime n. Our main result shows that, for each prime n, apart from a finite explicitly computable set of exceptional primes p, every nontrivial cyclic code $C = \langle g \rangle$ over $\mathbb{F}_{p^m}$ satisfies $d_H(C) = \deg(g) + 1$. This gives a uniform generic classification of the minimum Hamming distance for all prime lengths n, extending the previously known classifications for $n = 2, 3, 5, 7$. The proof combines algebraic properties of roots of unity with a computer-algebraic construction that produces the finite exceptional set.

1 Introduction

Cyclic codes are fundamental objects in algebraic coding theory. A linear code of length n over a finite field $\mathbb{F}$ is cyclic if it is invariant under cyclic shifts of coordinates.

Identifying a codeword $(a_0, \ldots, a_{n-1})$ with $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$, cyclic codes are precisely the ideals of $\mathbb{F}[x]/\langle x^n - 1\rangle$. Hence every nonzero cyclic code is generated by a unique monic divisor $g(x)$ of $x^n - 1$.

We study cyclic codes of prime length n over $\mathbb{F}_{p^m}$, where $n \neq p$ are primes. The main problem is to determine the minimum Hamming distance of $C = \langle g(x)\rangle \subseteq \mathbb{F}_{p^m}[x]/\langle x^n - 1\rangle$ from its generator polynomial $g(x)$. This problem is known only in several small cases $n \leq 7$ (see [1] and references therein).

Our main contribution is a generic classification for arbitrary prime length n. For each prime n, we construct an explicit finite set $\mathcal{A}_n$ of exceptional primes such that, for every prime $p \notin \mathcal{A}_n$, $p \neq n$, every nontrivial cyclic code $C = \langle g(x)\rangle \subseteq \mathbb{F}_{p^m}[x]/\langle x^n - 1\rangle$ satisfies $d_H(C) = \deg(g) + 1$. Thus, outside a finite computable exceptional set, every nontrivial cyclic code of prime length n reaches its maximal possible Hamming distance (which is called MDS codes). The construction of $\mathcal{A}_n$ uses determinants of generator matrices, resultants, and Chebotarev's theorem on roots of unity [4, 5].

2 Codes and cyclic codes in $\mathbb{F}_{p^m}[x]/\langle x^n - 1\rangle$

Let $C \subseteq \mathbb{F}_{p^m}^n$ be a linear $[n, k, d]$-code. Recall the Singleton bound $d \leq n - k + 1$. A code attaining this bound is called maximum distance separable, or MDS. Such codes are important in coding theory and in applications including secret sharing and secure communication [2, 3].

Under the polynomial representation of codewords, multiplication by x in $\mathbb{F}_{p^m}[x]/\langle x^n - 1\rangle$ corresponds to a cyclic shift. Thus cyclic codes are precisely ideals of this quotient ring. Since $\mathbb{F}_{p^m}[x]$ is a principal ideal domain, every nonzero cyclic code is of the form $C = \langle g(x)\rangle$, where $g(x)$ is the unique monic divisor of $x^n - 1$ generating C.

Let $g(x) = g_0 + g_1 x + \cdots + g_r x^r$ be a monic divisor of degree r. The usual generator matrix of $C = \langle g(x)\rangle$ is

$$G_g = \begin{bmatrix} g_0 & g_1 & \cdots & g_r & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{r-1} & g_r & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & g_0 & g_1 & \cdots & g_r \end{bmatrix},$$

an $(n-r) \times n$ matrix. Hence $\dim C = n - r$, and the Singleton bound gives $d_H(C) \leq r + 1$.

We use the standard rank criterion: for a generator matrix G of a linear $[n, k, d]$-code, one has $d_H(C) \geq \delta$ if and only if deleting any $\delta - 1$ columns of G leaves a

matrix of rank k. Therefore, for $C = \langle g \rangle$, it is enough to show that deleting any $r = \deg(g)$ columns of G_g gives full row rank. This proves $d_H(C) \geq r + 1$, and hence equality by the Singleton bound.

3 Main theorem and algorithm

The main result is the following.

Theorem 1. *Let n be a prime. For each prime $p \neq n$, consider the property $(\mathcal{P}_{n,p})$: for every positive integer m and every nontrivial cyclic code $C = \langle g \rangle \subseteq \mathbb{F}_{p^m}[x]/\langle x^n - 1 \rangle$ generated by a monic divisor g of $x^n - 1$, one has $d_H(C) = \deg(g) + 1$. Let $\mathcal{A}_n$ be the output of Algorithm 1. Then $\mathcal{A}_n$ is finite, and $(\mathcal{P}_{n,p})$ holds for every prime $p \notin \mathcal{A}_n$ with $p \neq n$.*

Algorithm 1 Computation of $\mathcal{A}_n$.

Require: A prime number n
Ensure: The finite exceptional set $\mathcal{A}_n$

```
Set A := ∅.
for each nonempty subset L ⊊ {0, 1, ..., n − 1} do
    Set r := #L and g(t, x) := ∏_{ℓ∈L} (x − t^ℓ).
    Construct the (n − r) × n matrix G_g.
    for each S ⊆ {1, ..., n} with #S = r do
        Let H be obtained from G_g by deleting the columns in S.
        Add c = Res_t(det(H), Φ_n(t)) to A.
    end for
end for
return the set A_n of prime divisors of the nonzero integers in A.
```

The algorithm is finite because there are only finitely many choices of L and S. The key point is that the resultants appearing in the algorithm are nonzero. This follows from Chebotarev's theorem on roots of unity: if n is prime, $\alpha_1, \ldots, \alpha_r$ are distinct n-th roots of unity, and $b_1, \ldots, b_r$ are distinct elements of $\{0, \ldots, n-1\}$, then $\det(\alpha_i^{b_j})_{1 \leq i,j \leq r} \neq 0$.

Using this theorem, one proves that if α is a primitive n-th root of unity and $g(x) \in \mathbb{Z}[\alpha][x]$ is a monic divisor of $x^n - 1$ of degree r, then every matrix obtained from G_g by deleting r columns has nonzero determinant. Indeed, a vanishing determinant would give a nonzero polynomial $h(x) = f(x)g(x)$ with at most r nonzero terms that

vanishes at r distinct n-th roots of unity. Chebotarev's theorem forces all coefficients of h to vanish, a contradiction.

The passage to finite fields is obtained by resultants. If $f(t) \in \mathbb{Z}[t]$ and

$$p \nmid \mathrm{Res}_t(f(t), \Phi_n(t)),$$

then $f(\alpha) \neq 0$ for a primitive n-th root α in $\overline{\mathbb{F}_p}$. Hence, for every $p \notin \mathcal{A}_n$, all the determinants needed in the rank criterion remain nonzero after reduction modulo p. Therefore deleting any $r = \deg(g)$ columns of G_g leaves a full-rank matrix, so $d_H(C) \geq r + 1$. The Singleton bound gives the reverse inequality, and hence $d_H(C) = r + 1 = \deg(g) + 1$.

Example 2. *We implemented Algorithm 1 in Maple and obtained*

$$\mathcal{A}_2 = \mathcal{A}_3 = \mathcal{A}_5 = \emptyset, \qquad \mathcal{A}_7 = \{2\}.$$

These computations recover the known classifications for the cases $n = 2, 3, 5, 7$.

References

[1] H. Q. Dinh, H. V. Ha, N. T. H. Tran, and T. N. Vo, On the Hamming distances of repeated-root constacyclic codes of length $7p^s$, *Finite Fields Appl.* (2024).

[2] J. Pieprzyk and X. M. Zhang, Ideal threshold schemes from MDS codes, LNCS 2587, Springer, 2003, 253–263.

[3] Y. Zhou et al., A secret sharing scheme based on near-MDS codes, *IC-NIDC*, 2009, 833–836.

[4] P. Stevenhagen and H. W. Lenstra Jr., Chebotarëv and his density theorem, *Math. Intelligencer* 18 (1996), 26–37.

[5] T. Tao, An uncertainty principle for cyclic groups of prime order, *Math. Res. Lett.* 12 (2005), 121–127.