Cyclic codes with low minimum distance

José Gustavo Coelho
Fabio Enrique Brochero Martinez

Universidade Federal de Minas Gerais

josegustavocoelho@gmail.com
fbrochero@ufmg.br

Instituto de Matemática Pura e Aplicada

Abstract

Let $\mathbf{GF}(q)$ be a finite field with q elements. Consider a cyclic code of length $n = q^m - 1$, where m is a positive integer, and the elements are in $\mathbf{GF}(q)$. We determine the conditions under which the code achieves a minimum distance of 2, based on the parameters of the code's generator polynomial. We also determine sufficient criteria for the cyclic code to have minimum distance 3. In particular, when $q = 2$ we demonstrate that the problem of determining when some specific cyclic codes have minimum distance 3 is equivalent to the problem of factoring a polynomial in $\mathbf{GF}(2)[X]$.

Introduction

Error-correcting codes are data encodings designed to add redundancy to a message to enable the detection and correction of errors that may occur during transmission or storage. Linear codes are codes where the codewords form a linear space, and as such every codeword can be represented as a vector.

A cyclic code of length n over a finite field $\mathbf{GF}(q)$ is a linear code with the interesting property that words can be represented as classes of polynomials in the quotient ring $\mathbf{GF}(q)[X]/(X^n - 1)$, and determining if a particular codeword is in the code can be done through a simple polynomial evaluation.

While some aspects of cyclic codes are very simple, it is a difficult problem to determine the weight distribution, and consequently the minimum distance of these codes. In particular, the problem of determining when the minimum distance of cyclic codes is low is still mostly open.

Objectives

Let $\mathbf{GF}(q)$ be a finite field with q elements, m a positive integer and γ a generator of $\mathbf{GF}(q)^*$. Let us define $C_{t_1,t_2,\ldots,t_s}$ as the cyclic code over $\mathbf{GF}(q)$ with length $n = q^m - 1$ and generator polynomial $g(X) = \mathbf{m}_{t_1}(X) \cdots \mathbf{m}_{t_s}(X)$, where $\mathbf{m}_t(X)$ is the minimal polynomial of γ^t over $\mathbf{GF}(q)$. Our objective is to determine criteria for when $C_{t_1,t_2,\ldots,t_s}$ has low minimum distances, such as 2 and 3.

Results

Let us describe a codeword in a code either by the representative $c(X)$ of its class in $\mathbf{GF}(q)[X]/(X^n - 1)$, or by the n-length vector $\mathbf{c}$ over $\mathbf{GF}(q)$. The codeword is in $C_{t_1,\ldots,t_s}$ if the $g(X) \mid c(X)$, which happens if and only if $c(\gamma^{t_i}) = 0$ for $0 \leq i \leq s$. Thus, the codeword is in the code if and only if $H\mathbf{c}^T = \overline{0}$, where H is the matrix

$$H = \begin{bmatrix} 1 & \gamma^{t_1} & \gamma^{2t_1} & \cdots & \gamma^{(n-1)t_1} \\ 1 & \gamma^{t_2} & \gamma^{2t_2} & \cdots & \gamma^{(n-1)t_2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \gamma^{t_s} & \gamma^{2t_s} & \cdots & \gamma^{(n-1)t_s}. \end{bmatrix}$$

Using this we obtain a straightforward criterion for when a cyclic code has minimum distance 2:

Theorem 1. *The cyclic code $C_{t_1,\ldots,t_s}$ of length $n = q^m - 1$ has minimum distance 2 if and only if the greatest common divisor*

$$D(t_1, \ldots, t_s) := \gcd(q^m - 1, t_1(q-1), t_2 - t_1, t_3 - t_1, \ldots, t_s - t_1)$$

is greater than 1. In that case, the number of codewords with weight 2 is $\frac{n(D(t_1,\ldots,t_s)-1)}{2}$.

Let us denote by $K_g(r)$ the q-cyclotomic coset of r modulo $q^g - 1$, i.e.,

$$K_g(r) = \{rq^k \pmod{q^g - 1} : k = 0, 1, \ldots, g-1\}.$$

We have obtained the following result about codes with minimum distance ≤ 3.

Theorem 2. *Let g be a divisor of m and $0 < t_1 < t_2 < \cdots < t_s < q^m - 1$ be arbitrary integers that do not belong to the same cyclotomic coset modulo $q^m - 1$. If there is an integer r such that $0 < r < q^g - 1$, $\gcd(r, q^m - 1) = 1$ and $t_1, t_2, \ldots, t_s$ are in $K_g(r)$, then $C_{t_1,\ldots,t_s}$ has minimum distance ≤ 3. If additionally $D(t_1, \ldots, t_s) = 1$, then the minimum distance is 3.*

We remark that, unlike Theorem 1, this result only has a *sufficient* condition for dimension 3. However, many examples of codes of minimum distance 3 can be determined from it. For instance, it follows from it that any binary cyclic code $C_{1,t}$ of length $n = 2^m - 1$, where $2 \mid m$, has minimum distance 3.

Let us consider the binary cyclic code $C_{1,t}$, i.e., the cyclic code over $\mathbf{GF}(2)$ of length $n = 2^m - 1$ and generator polynomial $g(X) = \mathbf{m}_1(X)\mathbf{m}_t(X)$. There is a codeword of weight 3 in $C_{1,t}$ if and only if there are indices $1 \leq i < j \leq n - 1$ such that a codeword of the form $c(X) = 1 + x^i + x^j$ is in the code. The fact that the codeword is in the code if and only if its vector form satisfies $H\mathbf{c}^T = \overline{0}$ tells us that the existence of a codeword of weight 3 is equivalent to there being a solution to the system

$$\begin{cases} 1 + \gamma^i + \gamma^j = 0, \\ 1 + \gamma^{it} + \gamma^{jt} = 0, \end{cases}$$

which is equivalent to the polynomial $U_t(x) := 1 + x^t + (1+x)^t$ having a root in $x \in \mathbf{GF}(2^m) \setminus \{0, 1\}$. So the problem of determining if $C_{1,t}$ has minimum distance 3 comes down to factoring $U_t(x)$ over $\mathbf{GF}(2)[x]$. A number of the properties of this polynomial can be determined, as well as conditions under which it has specific irreducible factors (or no factors whose degree divides m), which translate to sufficient conditions for $C_{1,t}$ having minimum distance 3 (respectively minimum distance greater than 3).

For instance, it follows that if we assume that m is a prime and $1 < t < m + 3$, then the roots of $U_t(x)$ different from 0 and 1 are in a finite field not contained in $\mathbf{GF}(2^m)$, and as such $C_{1,t}$ has minimum distance ≥ 4.

Conclusions

There is a very straightforward criterion for when a cyclic code has minimum distance 2; and sufficient conditions, with some assumptions, for the minimum distance to be 3.

In the future we aim to establish sufficient criteria for cases that currently lack any, and also to determine necessary conditions for a cyclic code to have minimum distance 3.

References

[1] Pascale Charpin. Open problems on cyclic codes. 2009.

[2] Pascale Charpin, Aimo Tietäväinen, and Victor Zinoviev. On binary cyclic codes with distance d=3. *Problems Inform. Transmission*, 33(4):287–296, 1998.

[3] Marko Moisio and Kalle Ranto. Kloosterman sum identities and low-weight codewords in a cyclic code with two zeros. *Finite Fields and Their Applications*, 13(4):922–935, 2007.

Acknowledgments

I would like to express my sincere appreciation to IMPA for organizing this event. I am grateful for the guidance and support of my PhD advisor Fabio Brochero, whose expertise guided me in my research. Lastly, I extend my deepest appreciation to my loving mother for her belief in my abilities.