A study of cyclic codes BCH and Reed-Solomon code

Welington Santos

UFPR

January 2015

Cyclic Codes

Definition

A linear (n, k) *code* $\mathbf{C}$ *over* $\mathbb{F}_q$ *is called cyclic if* $(a_0, a_1, \ldots, a_{n-1}) \in \mathbf{C}$ *implies* $(a_{n-1}, a_0, \ldots, a_{n-2}) \in \mathbf{C}$.

But this definition is not good to work, so we will identify a cyclic code with polynomial ring.

Let $(x^n - 1)$ be the ideal generated by $x^n - 1 \in \mathbb{F}_q[x]$. Then all elements of $\mathbb{F}_q[x]/(x^n - 1)$ can be represented by polynomials of degree less than n and clearly this residue class ring is isomorphic to $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$. An isomorphism given by

$$\psi(a_0, a_1, \ldots, a_{n-1}) = \left[a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}\right].$$

Theorem

The linear code $\mathbf{C}$ *is cyclic if only if* $\psi(\mathbf{C})$ *is an ideal of* $\mathbb{F}_q[x]/(x^n - 1)$.

BCH-codes

One particular subclass of cyclic codes are codes known as BCH codes. This codes are defined from an integer b and a n-th root of unity as follows

Definition

Let b be a nonnegative integer and let $\alpha \in \mathbb{F}_{q^m}$ be a primitive n th root of unity,where m is the multiplicative order of q modulo n. A BCH code over $\mathbb{F}_q$ of length n and designed distance δ, $2 \leq \delta \leq n$, is a cyclic code defined by the roots

$$\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$$

of the generator polynomial.

An important property of BCH codes is that, the minimum distance of a BCH code of designed distance d is at least δ.

Reed-Solomon codes

Definition

A Reed-Solomon code is a cyclic BCH code of length $n = q - 1$, and generator polynomial

$$g(x) = (x - \alpha^{b+1})(x - \alpha^{b+2}) \dots (x - \alpha^{b+\delta-1})$$

Where α be a primitive element of $\mathbb{F}_q$, $b \geq 0$ and $2 \leq \delta \leq q - 1$.

Definition

A linear code of parameters $[n, k, d]$ is said MDS (maximum distance separable) if, the equality $d = n - k + 1$ is valid.

Theorem

The Reed-Solomon codes are MDS codes.

My Objectives

We would like to study MDS codes for poset metric.

Definition

The $\mathbb{P}$-weight of a element $x \in \mathbb{F}_q^n$ is the cardinality of ideal of $\mathbb{P}$ generated by the support of x i.e.

$$w_P(x) = | < supp(x) >_{\mathbb{P}} |$$

Where $supp(x) = \{i : x_i \neq 0\}$.

Definition

If $\mathbb{P} = ([n], \preceq)$ is a poset, then the $\mathbb{P}$-distance $d_{\mathbb{P}}(x, y)$ between $x, y \in \mathbb{F}_q^n$ is defined by

$$d_{\mathbb{P}}(x, y) = w_{\mathbb{P}}(x - y).$$

- J.Y. Hyun · H.K. Kim - *Maximum distance separable poset codes* , © Springer Science+Business Media, LLC 2008
- S.T. Dougherty; M. M. Skriganov - *Maximum Distance Separable Codes in the ρ Metric over Arbitrary Alphabets* , Journal of Algebraic Combinatorics 16 (2002), 71–81
- M.M.S. Alves.- *A standard form for generator matrices with respect to the niederreiter-rosenbloom-tsfasman metric*.IEEE Information Theory Workshop- pages 486–489, 2011.
- M.M.S. Alves, L. Panek, and M. Firer.*Error-block codes and poset metrics*. Advances in Mathematics of Communications, 2(1):95–111, 2008