Error Correcting Codes: Combinatorics, Algorithms and Applications (Spring 2009)

Lecture 24: BCH Codes

March 20, 2009

Lecturer: Atri Rudra *Scribe: Swapnoneel Roy*

1 Introduction

In this lecture we had an introduction to a new family of codes known as BCH codes named after their discoverers, R.C Bose and D.K. Ray-Chaudhuri (1960), and independently by A. Hocquenghem (1959). A lower bound for the BCH code was established in the lecture. The lower bound brings the binary case of the BCH code closer to the Hamming Bound which is $k \leq n - logn + O(n)$. Thus the BCH code *beats* the Gilbert-Varshamov bound which is $k \geq n - (2t)logn$.

2 BCH Codes

Definition 2.1 (BCH Codes). *[1] For prime power q, integer m, and integer d, the BCH code $BCH_{q,m,d}$ is obtained as follows: Let $n = q^m$ and let $\mathbb{F}_{q^m}$ be an extension of $\mathbb{F}_q$ and let C' be the (extended) $[n, n-(d-1), d]_{q^m}$ Reed-Solomon code obtained by evaluating polynomials of degree at most n-1 over $\mathbb{F}_{q^m}$ at all the points of $\mathbb{F}_{q^m}$. Then the code $BCH_{q,m,d}$ is the $\mathbb{F}_q$-subfield subcode of C'. In other words, $BCH_{q,m,d} = C' \cap \mathbb{F}_q^n$.*

If we have $q = 2$ then $BCH_{2,m,d} = C \cap \mathbb{F}_2^{2^n}$ where C is given as a Reed-solomon code $C = RS[n = 2^m, n-(d-1), d]_{\mathbb{F}_{2^m}}$.

The BCH code could be constructed in the following manner: Look at the Reed-Solomon code and only pick up the codewords that are in $\mathbb{F}_2^{2^n}$. Now we argue that the BCH code has dimension at least $n - m(d-1)$.

Conjecture 2.2. *Dimension of BCH code is at least $n - m(d-1)$.*

Proof. [1] We recall that every function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ is a polynomial of over $\mathbb{F}_{2^m}$ of degree at most $n-1$. Thus the space of polynomials from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ is a $\mathbb{F}_2$-linear space of dimension exactly n. We wish to know what is the dimension of the subspace of polynomials of degree at most $n-d$. But now note that the restriction that a polynomial $f(x) = \sum_{i=0}^{n-1} f_i x^i$ has a degree at most $n-d$ is equivalent to saying that the coefficients f_i must equal zero, for $i \in \{n-(d-1), \cdots, n-1\}$. Each such condition is a single linear constraint over $\mathbb{F}_{2^m}$, but this translates into a block of m linear constraints over $\mathbb{F}_2$. Since we have $d-1$ such blocks of constraints, the restriction that the functions have a degree at most $n-d$ place at most $m(d-1)$ linear constraints. Thus the resulting space has dimension at least $n - m(d-1)$. Hence the code $BCH_{2,m,d}$ has dimension at least $2^m - m(d-1)$. $\square$

The general idea of a BCH code is to identify its generating polynomial by the roots (instead of in terms of the coefficients). The code $BSC_{2,m,d}$ implies the evaluation of a "special" polynomial of degree $\leq n-d$ over $\mathbb{F}_{2^m}$.
The term "special" means if $P(x) \in \mathbb{F}_2[x]$ is a "special" polynomial iff $\forall \alpha \in \mathbb{F}_{2^m}, P(\alpha) \in \mathbb{F}_2$. This definition of "special" implies that the polynomials $P(x) = 0$ and $P(x) = 1$ are "special" polynomials.
We can easily see that $BSC_{2,m,d}$ is linear. Because if polynomials $P(x)$ and $Q(x)$ are "special", so is $P(x) + Q(x)$.

3 Bounding the dimension of BCH Codes

We are now ready to prove a stronger bound on the dimension of BCH codes.

Lemma 3.1. *The dimension of the code $BCH_{q,m,d}$ is at least $q^m - 1 - m\left\lceil \frac{(d-2)(q-1)}{q} \right\rceil$.*

Proof. [1] The idea of the proof is to consider the space of all functions from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ which forms an $\mathbb{F}_q$-vector space of dimension n. viewing these funstions as polynomials from $\mathbb{F}_{q^m}[x]$, we then restrict them to have zero as the coefficients of x^i for $i \in \{n-(d-1), \cdots, n-1\}$.
The condition that the coefficients of x^{n-1} is zero imposes one linear constraint and reduces the dimension of the space to $n-1$. The remaining conditions, corresponding to coefficients of x^i for $i \in \{n-(d-1), \cdots, n-2\}$, lead to at most m conditions each. However, we do not need to impose all such conditions. In particular, we can skip every qth condition (starting at $n-2$ and going down) since these are exponents of the form $l = (n-1) - qj$, where j is a positive integer. Now by the property of a polynomial over $\mathbb{F}_{q^m}$ mapping $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, we have $l = q(n-1-j)(mod(n-1))$. Hence the coefficient of $x^{\lessdot}$ equals zero is implied by the condition that the coefficient of x^{n-1-j} equals zero. Thus the constraints corresponding to the coefficients of x^i for $i \in \{n-(d-1), \cdots, n-2\}$, lead to at most $m\left\lceil \frac{(d-2)(q-1)}{q} \right\rceil$ linear constraints. Thus the dimension of the space is at least $q^m - 1 - m\left\lceil \frac{(d-2)(q-1)}{q} \right\rceil$. $\square$

This leads to the following theorem.

Theorem 3.2. *For prime power q, integers m and d, the $BCH_{q,m,d}$ is an $\left[n, n-1-m\left\lceil \frac{(d-2)(q-1)}{q} \right\rceil, d\right]_q$ code, for $n = q^m$.*

In the case of $q = 2$ (binary codes) we have the following corollary:

Corollary 3.3. *For every integer m and t, the code $BCH_{2,m,2t}$ is an $[n, n-1-(t-1)\log n, 2t]$-code, for $n = 2^m$.*

The above k is very close to the Hamming bound for constant d and so is particularly nice.

References

[1] Madhu Sudan. Lecture on bch codes. *Algorithmic Introduction to Coding Theory*, September 2001.