Error Correcting Codes: Combinatorics, Algorithms and Applications **(Fall 2007)**

Lecture 42: Achieving List-Decoding Capacity

December 7, 2007

Lecturer: Atri Rudra *Scribe: Sandipan Kundu*

1 Introduction

$Q(X,Y,Z) \underset{\text{factoring out (E(X))}}{\rightarrow} Q_0(X,Y,Z) \underset{Q_0 \text{ is poly over } \mathbb{F}_q[X]}{\rightarrow} T_0(Y,Z) \underset{\text{mod (E(X))}}{\rightarrow} T(Y,Z) \neq 0$ as $E(X)|Q_0(X,Y,Z)$.
If $f(x)$ is such that $f(\alpha_i)$ and $f(\gamma\alpha_i)$ for at least t values of i, which implies $T(f(x), f(\gamma X)) \equiv 0$.
Find the roots of $T(Y, y^q)$ over $\mathbb{F}_{q^{q-1}}$.

Lemma 1.1. *There exists a irreducible polynomial E(X) such that* $f(x)^q = f(\gamma X)\ mod E(X)$,

$f(x)^q = f(\gamma X) mod E(X), Q(\alpha_i, y_i, z_i) = 0 \Longleftrightarrow Q_0(\alpha_i, y_i, z_i) = 0$
If $f(\alpha_i) = y_i$ and $f(\gamma\alpha_i) = z_i$, then it implies $Q_0(\alpha_i, f(\alpha_i), f(\gamma\alpha_i) = 0$ which in turn implies
$R(X) \stackrel{\triangle}{=} Q_0(X, f(X), f(\gamma X))$ has $\geq rt$ roots.
We know $deg(R) \leq (1,k,k) of Q \leq D$ as $t > \frac{D}{r}$. (Done)
In other words, $Q_0(X, f(X), f(\gamma X)) = 0$ which implies $T_0(f(X), f(\gamma X)) = 0$.
If $f(X)$ is a root of $S(X) \stackrel{\triangle}{=} T(Y, Y^q)$ over $F_{q^{q-1}}$ for general m we have, $\langle f(\gamma^{m_i}), f(\gamma^{m_i+1}, \ldots, f(\gamma^{m_i+m-1})\rangle$.
$Q_0(f(\gamma^{m_i}), f(\gamma^{m_i+1}, \ldots, f(\gamma^{m_i+m-1})) \equiv 0$
Find roots of $T(Y, Y^q, \ldots, Y^{q^{m-1}})$ over $\mathbb{F}_q^{q-1}$ maximum number of roots $\leq Dq^{m-1}$ of degree $q-1$.

Lemma 1.2. *There exists a irreducible polynomial E(X) such that* $f(x)^q = f(\gamma X)\ mod E(X)$,

$S(Y)$ needs to be non-zero or $Z - Y^q$ does't divide $T(Y,Z)$.

$$\text{degree of Y in} T(Y,Z) \leq \text{degree of Y in} Q(X,Y,Z) \tag{1}$$

$$\leq \frac{D}{R} < q \text{by choice of D} \tag{2}$$

In fact for constant rate code, $\frac{D}{R} is \bigcirc(1)$

Lemma 1.3. *$E(X) = X^{q-1} - \gamma$ is irreducible over $\mathbb{F}_q$.*

Exact characterization of irreducible polynomial of the form $X^b - c$.

Lemma 1.4. *$f(X)^q \equiv f^{X^q}$ for $f(X) \in \mathbb{F}_q[X]$*

Proof. Hint: Show $(aX + bY)^q = aX^q + bY^q$ □

Proof. Proof of lemma (1.1) using (1.4)
Done if

$$f(X)^q - f(\gamma X) \equiv 0\ mod\ E(X) \tag{3}$$

$$\Leftarrow X^q - \gamma X \equiv 0\ mod\ E(X) \tag{4}$$

$$\Leftarrow\ E(X) divides X(X^{q-1} - \gamma) \tag{5}$$

True if $E(X) - X^{q-1} - \gamma$ □

In for number of folds, m general, $t > (wk^s \prod_{i=1}^{s} (1 + \frac{j}{r}))$