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

# Lecture 42: Achieving List-Decoding Capacity

Dec. 7, 2007

*Lecturer: Atri Rudra* *Scribe: Yang Wang*

**Lemma 0.1.** $f(x^q) \equiv f(x)^q$ *for* $f(x) \in F_q[x]$.

*Proof.* Note that for any $g(x) \in F_q[x]$,

$$q \cdot g(x) = 0.$$

Hence

$$(g(x) + h(x))^q = \sum_{i=0}^{q} g^i(x)h^{q-i}(x)\binom{q}{i} = g^q(x) + h^q(x)$$

by using

$$q|\binom{q}{i} \; for \; i = 1, \ldots, q-1.$$

Thus we can easily prove the lemma by induction on the degree of $f(x)$. □

Now we can prove the following lemma:

**Lemma 0.2.** *There exists irreducible polynomial* $E(x)$ *of degree* $q-1$ *such that*

$$f(x)^q \equiv f(rx)(\mod E(x)).$$

*Proof.* We are done if

$$\begin{aligned} & f(x^q) - f(rx) \equiv 0(modE(x)) \\ \Leftarrow \quad & x^q - rx \equiv 0(modE(x)) \\ \Leftarrow \quad & E(x)|x^{q-1} - rx. \end{aligned}$$

Thus we just set $E(x) = x^{q-1} - rx$.

□

We can extend the result to general $s$,

$$t > \sqrt[s+1]{NK^s\Pi_{j=1}^s(1 + \frac{j}{r})}.$$

Observe that the proof goes true even if $\alpha_i$'s are not $r^{im}$. We can further improve the result to $1 - (1+\delta)R^{\frac{s}{s+1}}$. For suitable choices of $\delta$ that depends on $R, \delta, \varepsilon$,

$$1 - (1+\delta)R^{\frac{s}{s+1}} \geq 1 - R - \varepsilon.$$

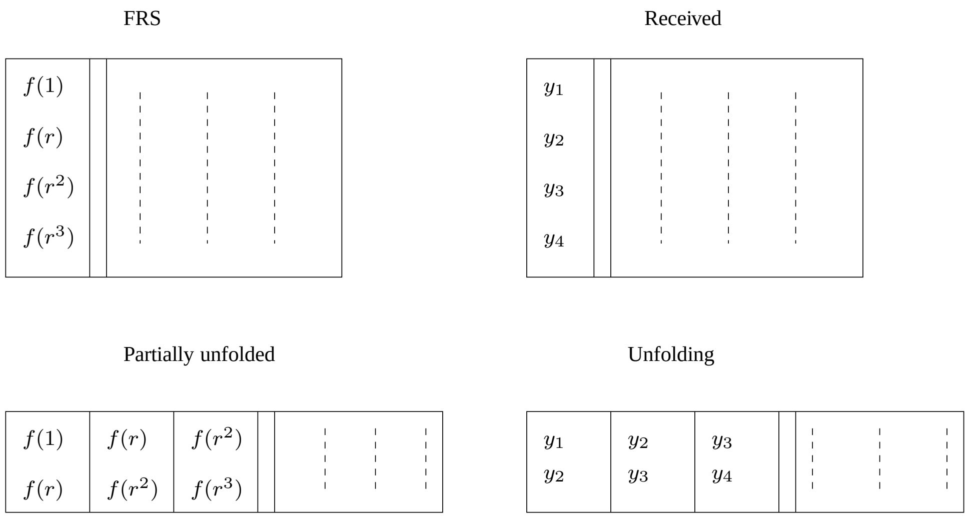


Figure 1: Example of $m = 4, s = 2$

Suppose the block length of the folded Reed-Solomon code is $N$, then the partially unfolded code has $N' = (m - sN)N$. If the received folded word has $t$ agreement with the codeword, then in the unfolded received word there are $t' = t(m - s + 1)$ agreement. Please refer to Fig.1 for an example. We run decoder on unfolded received word for folding parameters. It will be done if

$$
\begin{aligned}
& t' > \sqrt[s+1]{N' k^s \Pi_{j=1}^{s} (1 + \frac{j}{r})} \\
\iff \quad & t(m - s + 1) > \sqrt[s+1]{(m - s + 1) N k^s B(r, s)} \\
\iff \quad & \frac{t}{N} > \sqrt[s+1]{\frac{k^s}{N^s (m - s + 1)^s} B(r, s)} \\
\iff \quad & \frac{t}{N} > \sqrt[s+1]{\frac{K^s m^s}{N^s (m - s + 1)^s} B(r, s)}.
\end{aligned}
$$

We have used the fact that $K = k/m$. Then the alphabet has size $N^{O(\frac{1}{\varepsilon^2})}$. The worst case list decoding size is $N^{O(\frac{\log VR}{\varepsilon}}$. For constant $\varepsilon$ it is $N^{O(1)}$.