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

\[
q \mid \binom{q}{i} \text{ for } i = 1, \ldots, q - 1.
\]

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

\[
f(x)^q \equiv f(rx) \pmod{E(x)}.
\]

**Proof.** We are done if

\[
(f(x^q) - f(rx) \equiv 0 (\text{mod} E(x))
\]

\[
\iff x^q - rx \equiv 0 (\text{mod} E(x))
\]

\[
\iff E(x) \mid x^{q-1} - rx.
\]

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

We can extend the result to general \( s \),

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

Observe that the proof goes true even if \( \alpha_i \)'s are not \( r^{im} \). We can further improve the result to

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

$$
t' > s^+\sqrt{N'k^s\Pi_j=1(1 + \frac{j}{r})}
\iff t(m - s + 1) > s^+\sqrt{(m - s + 1)Nk^sB(r, s)}
\iff \frac{t}{N} > s^+\sqrt{\frac{k^s}{N^s(m - s + 1)^s}B(r, s)}
\iff \frac{t}{N} > s^+\sqrt{\frac{K^s m^s}{N^s(m - s + 1)^s}B(r, s)}.
$$

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

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