Decoding RS codes

$d = n-k+1$, $2t+1 \le d$, wish to decode t errors, $\underline{\alpha}$ known

$\underline{u} = \underline{c} + \underline{e}$ is received, $\underline{c} = V_{\underline{\alpha}}(f)$, $\deg(f) < k$, $w(\underline{e}) \le t$

$\underline{u}$: known; $\underline{e}$: not known

Let the non-zero coord.'s of $\underline{e}$ be $i_1, \dots i_t$ (not known)

Let $h(x) = (x-\alpha_{i_1})(x-\alpha_{i_2})\cdots(x-\alpha_{i_t})$ error-locator poly, $\deg(h) = t$

Let $\underline{x} = V_{\underline{\alpha}}(h)$ ← not known. Then

$\underline{x} \circ \underline{u} = \underline{x} \circ (\underline{c} + \underline{e}) - \underline{x} \circ \underline{c} = V_{\underline{\alpha}}(hf) = \underline{y}$ ← not known, $\deg(hf) < k+t$

What we know is $V_{\underline{\alpha}}(h) \in RS_{t+1}$, $\underline{y} \in RS_{k+t}$.

We get a system of lin. equations: (hom. lin., $2n$ unknowns)

$$(*)\begin{cases} \underline{x} \circ \underline{u} = \underline{y} & \leftarrow n \text{ equations} \\ \underline{x} \in RS_{t+1} & (\underline{x} \cdot H_{t+1}^T = \underline{0}) \leftarrow n-(t+1) \text{ equations} \\ \underline{y} \in RS_{k+t} & (\underline{x} \cdot H_{k+t}^T = \underline{0}) \leftarrow n-(k+t) \text{ equations} \end{cases}$$

Thm. If $2t+1 \le d$, then for **every** sol.'n of $(*)$ we have $\underline{x} \circ \underline{c} = \underline{x} \circ \underline{u}$ ($\Rightarrow c_i = u_i$ for $\forall i$ s.t. $x_i \ne 0$)

$\ge n-(t+1)+1$ such i!

Pf. $\underline{x} \circ \underline{c} = V_{\underline{\alpha}}(hf) \in RS_{k+t}$, $\underline{x} \circ \underline{u} = \underline{y} \in RS_{k+t} \Rightarrow$

$\underline{x} \circ \underline{u} - \underline{x} \circ \underline{c} = \underline{x} \circ (\underline{u} - \underline{c}) \in RS_{k+t}$ ← has min. dist $\ge n-(k+t)+1$

($\underline{u} - \underline{c} = \underline{e}$; has wt $\le t$)

$t \ge w(\underline{x} \circ \underline{u} - \underline{x} \circ \underline{c})$ and we give $n-(k+t)+1 \le t \Rightarrow d \le 2t+1$. So $\underline{x} \circ \underline{u} - \underline{x} \circ \underline{c} = \underline{0}$.

Decoding

1) Solve $(*)$
2) Consider $\underline{u}$ for those i s.t. $x_i \ne 0$ ($\ge n-t$ such "i")
3) Choose k of these "i"-s and write f by LAGRANGE interpolation ($\deg(f) \le k-1$) and put $\underline{c} = V_{\underline{\alpha}}(f)$
4) Check if $u_i = c_i$ for the other "i"-s

Remark: Best decoding alg. works in $O(n \log^2 n \log\log n)$ time.