Berlekamp-Welch decoding algorithm for error correction with RS codes

C[n,k,d] RS code with defining set $\mathscr{P}=(\alpha_1\alpha_2,\ldots\alpha_n)$
received vector $\mathbf{r}=\mathbf{c}+\mathbf{e}$, $e\in \mathbb{F}_q^n$ is the error vector, $wt(\mathbf{e})\leq \tau=[(n-k)/2]$

Lert $Q(x,y)=Q_0(x)+yQ_1(x)\in \mathbb{F}_q[x,y]$ be a nonzero polynomial such that

$$Q(\alpha_i,r_i)=0,\ i=1,2,\ldots,n$$
$$\deg Q_0 \leq n-1-\tau$$
$$\deg Q_1 \leq n-1-\tau-(k-1)$$

A nonzero polynomial with these properties exists. Indeed, the number of unknown coefficients is
$\#\{(Q_{0,0},\ldots,Q_{0,n-1-\tau}),(Q_{1,0},\ldots,Q_{n-1-\tau-(k-1)})\} = 2n-2\tau-k+1 \geq 2n-n+k-k+1=n+1$
These coefficients satisfy n homogeneous equations, so a nonzero solution exists.

Theorem 13.3: If $wt(\mathbf{e})\leq \tau$ and $\mathbf{c}$=eval (f) then $f=-Q_0/Q_1$.
Proof. $\deg(Q(x,f(x)))\leq \max(n-1-\tau,k-1+n-1-\tau-(k-1))=n-1-\tau$.
$Q(x_i,f(x_i))=0$ if $c_i=r_i$, so $Q(x,f(x))$ has $\geq n-\tau$ zeros. Then $Q\equiv 0$, or $Q_0+f\,Q_1=0$. ▲

Algorithm BW: Given $\mathbf{r}=(r_1,\ldots,r_n)$, $l_0=n-1-\tau$, $l_1=n-1-\tau-(k-1)$

1. Find *any* nonzero solution of the system

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{l_0} & r_1 & r_1\alpha_1 & r_1\alpha_1^2 & \ldots & r_1\alpha_1^{l_1} \\ 1 & \alpha_2 & \alpha_2^2 & \ldots & \alpha_2^{l_0} & r_2 & r_2\alpha_2 & r_2\alpha_2^2 & \ldots & r_2\alpha_2^{l_1} \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \ldots & \alpha_n^{l_0} & r_n & r_n\alpha_n & r_n\alpha_n^2 & \ldots & r_n\alpha_n^{l_1} \end{pmatrix} \mathbf{Q}^T = 0$$

where $\mathbf{Q}=((Q_{0,0},Q_{0,1},\ldots,Q_{0,l_0}),(Q_{1,0},Q_{1,1},\ldots,Q_{1,l_1}))$

(complexity $O(n^3)$)

2. Find $f(x)=-\sum_{i=0}^{l_0} Q_{0,i}x^i / \sum_{i=0}^{l_1} Q_{1,i}x^i$

3. If found $f(x) \in \mathbb{F}_q[x]$, decode as $\mathbf{c}=\text{eval}(f)$

Overall complexity is $O(n^3)$; faster implementations are possible

Remarks.

1.

$$Q(x,y) = Q_1(x)y + Q_0(x) = Q_1(x)\left(y + \frac{Q_0(x)}{Q_1(x)}\right) = Q(x)(y - f(x))$$

$$Q(\alpha_i, r_i) = Q_1(\alpha_i)(r_i - f(\alpha_i)) \equiv 0$$

Either $r_i = f(\alpha_i)$ ($e_i = 0$, no error) or $Q_1(\alpha_i) = 0$.

Hence $Q_1(\alpha_i)=0$ if $e_i \neq 0$. Thus the roots of Q_1 locate errors in **r**, so Q_1 is the error locator polynomial.

2. Given a set of points (α_i, r_i), i=1,…,n in the (x,y) plane over $\mathbb{F}_q$, we need to find a polynomial f(x) of degree $\leq$ k-1 that passes through at least $n-\tau \geq (n+k)/2$ of these points. This task is called interpolation or curve fitting. RS decoding $\equiv$ interpolation.