A FAST ALGORITHM
FOR SOLVING
THE WELCH-BERLEKAMP EQUATIONS
This algorithm was developed jointly by Elwyn Berlekamp, Tze Hua Liu, Po Tong, and Lloyd Welch.

The Key WB Equations are

\[ Q(x_k)\sigma^*_k = P(x_k) \quad \text{for } k \in S^c \quad (1) \]

These equations will be used sequentially in some order depending on auxiliary information such as symbol reliability. We will assume that the \( x_k \)'s are renumbered so that the equations are

\[ Q(x_k)\sigma^*_k = P(x_k) \quad \text{for } k = 1, \ldots, N - M \]
We introduce an auxillary pair of polynomials,
\[ W(Z), V(Z) \]
and recursively compute an integer and four polynomials as follows

\[ J_k, Q_k(Z), P_k(Z), W_k(Z), V_k(Z) \]

The pair
\[ (Q_k, P_k) \]
will constitute a “minimal” solution to the first \( k \) equations

and the pair
\[ (W_k, V_k) \]
will also solve the first \( k \) equations but, in a certain sense, will not be minimal.
Initialization:

\[ J_0 = 0; \]
\[ Q_0(Z) = 1; \quad P_0(Z) = 0; \quad W_0(Z) = 1; \quad V_0(Z) = 1 \]

Since \( k = 0 \), there are
no equations to verify.
When we have generated
\[ Q_k, P_k, W_k, V_k \]
we will have two solutions
to the first \( k \) equations.
\((Q_k, P_k)\) and \((W_k, V_k)\)

However the pair \((W_k, V_k)\) will be
"less suitable" than \((Q_k, P_k)\)
in a certain sense.

But the pair will be useful
in constructing \((Q_{k+1}, P_{k+1})\)
STEP \( k \)

At the beginning of step \( k \) we have \( J_{k-1} \) and 
\( Q_{k-1}(Z), P_{k-1}(Z), W_{k-1}(Z), V_{k-1}(Z) \)

We form 
\[ d_k = Q_{k-1}(x_k)\sigma_k^* - P_{k-1}(x_k) \]

IF \( d_k = 0 \)

\[ J_k = J_{k-1} + 1 \]
\[ Q_k(Z) = Q_{k-1}(Z) \]
\[ P_k(Z) = P_{k-1}(Z) \]
\[ W_k(Z) = (Z - x_k)W_{k-1}(Z) \]
\[ V_k(Z) = (Z - x_k)V_{k-1}(Z) \]

In this case 
\( (Q_{k-1}, P_{k-1}) \) already satisfy the \( k \)'th equation and 

multiplication by \( (Z - x_k) \) 
forces the pair 
\( W_k(Z), V_k(Z) \) 
to satisfy the \( k \)'th equation.
IF $d_k \neq 0$

We form another quantity,

$$c_k = d_k^{-1} \cdot (W_{k-1}(x_k)\sigma_k^* - V_{k-1}(x_k))$$

and set

$$Q_k(Z) = (Z - x_k)Q_{k-1}(Z)$$
$$P_k(Z) = (Z - x_k)P_{k-1}(Z)$$
$$W_k(Z) = W_{k-1} - c_k Q_{k-1}(Z)$$
$$V_k(Z) = V_{k-1} - c_k P_{k-1}(Z)$$

It is readily verified that the two pair of polynomials satisfy the first $k$ equations.

HOWEVER, we are not done with this case.

IF $J_{k-1} = 0$ then

swap the two pair.

$$Q_k(Z) \leftrightarrow W_k(Z)$$
$$P_k(Z) \leftrightarrow V_k(Z)$$

and set $J_k = 0$

OTHERWISE set $J_k = J_{k-1} - 1$

and do not swap pairs.
A MATRIX DESCRIPTION

The four polynomials can be written as components of a matrix.

\[
\begin{pmatrix}
Q_k(Z) & P_k(Z) \\
W_k(Z) & V_k(Z)
\end{pmatrix}
\]

In this form the \(k\)'th step can be written
IF $d_k = 0$

$$\begin{pmatrix} Q_k(Z) & P_k(Z) \\ W_k(Z) & V_k(Z) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & (Z - x_k) \end{pmatrix} \begin{pmatrix} Q_{k-1}(Z) & P_{k-1}(Z) \\ W_{k-1}(Z) & V_{k-1}(Z) \end{pmatrix}$$

IF $d_k \neq 0$ and $J_{k-1} \neq 0$

$$\begin{pmatrix} Q_k(Z) & P_k(Z) \\ W_k(Z) & V_k(Z) \end{pmatrix} = \begin{pmatrix} (Z - x_k) & 0 \\ c_k & 1 \end{pmatrix} \begin{pmatrix} Q_{k-1}(Z) & P_{k-1}(Z) \\ W_{k-1}(Z) & V_{k-1}(Z) \end{pmatrix}$$

IF $d_k \neq 0$ and $J_{k-1} = 0$

$$\begin{pmatrix} Q_k(Z) & P_k(Z) \\ W_k(Z) & V_k(Z) \end{pmatrix} = \begin{pmatrix} -c_k & 1 \\ (Z - x_k) & 1 \end{pmatrix} \begin{pmatrix} Q_{k-1}(Z) & P_{k-1}(Z) \\ W_{k-1}(Z) & V_{k-1}(Z) \end{pmatrix}$$
The fact that each pair, 
\((Q_k(Z), P_k(Z))\) and \((W_k(Z), V_k(Z))\)
satisfy the first \(k\) equations 
can be expressed as

\[
\begin{pmatrix}
Q_k(x_i) & P_k(x_i) \\
W_k(x_i) & V_k(x_i)
\end{pmatrix}
\begin{pmatrix}
\sigma^*_i \\
-1
\end{pmatrix}
= \begin{pmatrix}
0 \\
0
\end{pmatrix}
\text{ for } i \leq k
\]
WHAT ABOUT MINIMALITY?

This is the difficult part of the theorem
and I will just outline the proof
with a few comments.

I will pattern this proof after that in
Tze Hwa Liu’s dissertation (1984)
First we are going to replace the decision criterion using \( J_k \) by something more intuitive. (It is equivalent)

Define the length of an ordered pair of polynomials by

\[
L(Q(Z), P(Z)) = \max(\deg(Q), 1 + \deg(P))
\]

and define

\[
L_k = \min L(Q(Z), P(Z))
\]

where the minimum is taken over all pairs of polynomials satisfying the first \( k \) equations.
THEOREM:
The algorithm described above gives a sequence of pairs, $(Q_k(Z), P_k(Z))$
for which

$$L_k = L(Q_k(Z), P_k(Z))$$

That is: $(Q_k(Z), P_k(Z))$ is minimal.

I will just list the lemmas, with a comment about some of them.

Lemma 1
$L_k$ is monotone increasing.

Lemma 2
If $2L_k \leq k$ then there is a unique minimum pair satisfying the first $k$ equations.
Lemma 3
If $2L_k \leq k$ and $d_{k+1} \neq 0$
when computed for a minimal pair at level $k$ then
$L_{k+1} = L_k + 1$

Lemma 4

$$\begin{vmatrix} Q_k(Z) & P_k(Z) \\ W_k(Z) & V_k(Z) \end{vmatrix} = \prod_{i=1}^{k} (Z - x_i)$$

(determinant of product is product of determinants)
Lemmas 5,6

\[ L(Q_k(Z), P_k(Z)) + L(W_k(Z), V_k(Z)) = k + 1 \]

THE SWAP PAIRS DECISION

The swap pairs decision based on the value of \( J_k \) is really the comparison of \( L(Q_k(Z), P_k(Z)) \) and \( L(W_k(Z), V_k(Z)) \) and picking \( L(Q_k(Z), P_k(Z)) \) to be the smaller.
We restate the theorem:

THEOREM:
The algorithm described above gives a sequence of pairs, \((Q_k(Z), P_k(Z))\) for which

\[ L_k = L(Q_k(Z), P_k(Z)) \]

That is: \((Q_k(Z), P_k(Z))\) is minimal.