L.R.Welch

WELCH-BERLEKAMP DECODING
OF
REED-SOLOMON CODES

TWO VIEWS
OF
REED-SOLOMON CODES

THE ORIGINAL VIEW

[Polynomial Codes over Certain Finite Fields,
I.S.Reed and G. Solomon,
Journal of SIAM, June 1960]

Parameters:
Let GF(2^n) be the field with 2^n elements.
The number of message symbols encoded into a codeword is M.
The number of code symbols transmitted is
N $= 2^n$.
Message symbols are elements of GF(2^n).

The original view is that the symbols of a codeword are the values of a polynomial whose coefficients are the message symbols.

MATHEMATICALLY:

Let $(x_1, x_2, \cdots, x_N)$ be an enumeration of the elements of the field.
Let $(m_1, m_2, \cdots, m_M)$ be a message where
$m_i \in GF(2^n)$.
Define a polynomial by

$$P(Z) = m_1 + m_2 Z + m_3 Z^2 + \cdots + m_M Z^{M-1}$$

Then the codeword is

$$(P(x_1), P(x_2), \ldots, P(x_N))$$

The enumeration used by Reed and Solomon was as follows.
Let β be a primitive element in GF(2^n). Then the enumeration is

$$(x_1, x_2, \cdots, x_N) = (0, \beta, \beta^2, \cdots, \beta^{N-2}, 1)$$

THE CLASSICAL VIEW

Reed Solomon Codes are view
as a sub type of BCH Codes

Parameters:
Let GF(2^n) be the field with 2^n elements.
Let β be a primitive element in GF(2^n).
The number of message symbols encoded into a codeword is M.
The number of code symbols transmitted is
$N = 2^n - 1$.
Let $G(Z)$ be the polynomial whose roots are

$$(\beta, \beta^2, \cdots, \beta^{N-M})$$

Message symbols are elements of GF(2^n).

The BCH view is that the symbols of a codeword are the coefficients of a polynomial in Z which is divisible by G.

MATHEMATICALLY:

Let

$$G(Z) = \prod_{i=1}^{N-M} (Z - \beta^i)$$

Let $(m_1, m_2, \cdots, m_M)$ be a message where $m_i \in GF(2^n)$.

Define a polynomial by

$$P(Z) = m_1 + m_2 Z + m_3 Z^2 + \cdots + m_M Z^{M-1}$$

and define

$$\begin{aligned} C(Z) &= P(Z)G(Z) \\ &= \sum_{i=0}^{N-1} c_i Z^i \end{aligned}$$

Then the codeword is

$$(c_0, c_1, \cdots, c_{N-1})$$

Alternatively, dividing $Z^{N-M}P(Z)$ by $G(Z)$ to get

$$Z^{N-M}P(Z) = Q(Z)G(Z) + R(Z)$$

Then

$$C(Z) = Z^{N-M}P(Z) - R(Z)$$

is divisible by $G(Z)$ and its coefficients form a systematic codeword.

DECODING PRESENTED
IN
THE REED-SOLOMON PAPER

Reed and Solomon described the following decoding procedure.

Receive $(r_1, r_2, \cdots, r_N)$

Select M indices in all possible ways

(Lagrange Interpolation)For each selection,
find $P(Z)$ with $\deg(P) = M - 1$
$P(x_i) = r_i$ at these indices.

The coefficients of P form a potential message.

As all possible selections are made, the message which gives a codeword closest to the received word occurs more often than any other.

An alternative is to form a codeword corresponding to each potential message and stop when the result disagrees with the received message in at most $(N-M)/2$ places. If none is found, failure to decode occurs.

These procedures are very inefficient.

Let us return to the first step of Reed-Solomon Decoding

We begin in the same way
Reed and Solomon did
by selecting a set of M indices, S,
and finding $P(Z)$ for which
degree of P is at most $M-1$
and $P(x_i) = r_i$ for $i \in S$

The tool is Lagrange interpolation.

We ask what is the effect of errors
at the selected indices.

LAGRANGE INTERPOLATION

For each $i \in S$ we need a polynomial, $\phi_i(Z)$, of degree $M-1$ which has the value 1 at x_i and the value 0 at x_j for $j \in S, j \neq i$

With these, the solution for P is

$$P(Z) = \sum_{i \in S} r_i \phi_i(Z)$$

If r_i includes an error e_i then $e_i\phi_i(Z)$ is added to the correct $P(Z)$.

SYNDROMES

Let $T(Z)$ be the message polynomial and e_k be the error at position k
Then

$$r_k = T(x_k) + e_k$$

Given an index selection, S, the Lagrange Interpolation polynomial evaluated at x_k will be

$$\begin{aligned} P(x_k) &= \sum_{i \in S} r_i \phi_i(x_k) \\ &= \sum_{i \in S} T(x_i)\phi_i(x_k) + \sum_{i \in S} e_i \phi_i(x_k) \end{aligned}$$

Subtracting the interpolated values from the received values:

$$\begin{aligned} r_k - P(x_k) &= T(x_k) - \sum_{i \in S} T(x_i)\phi_i(x_k) \\ &\quad + e_k - \sum_{i \in S} e_i \phi_i(x_k) \end{aligned}$$

Since T has degree at most $M-1$,

$$T(x_k) = \sum_{i \in S} T(x_i)\phi_i(x_k)$$

and we have

$$\sigma_k = r_k - P(x_k) = e_k - \sum_{i \in S} e_i \phi_i(x_k)$$

$$\text{for } k \in S^c$$

which is a new family of syndromes.

Given σ_k for $k \in S^c$ and assuming the number of errors is within the R-S bound, we would like to solve for the e_j's.

INTERPOLATION POLYNOMIALS

Given S, the ϕ's are constructed as follows:
Let

$$G(Z) = \prod_{j \in S} (Z - x_j)$$

and let $G'(Z)$ be its formal derivative.
Then

$$\phi_i(Z) = \frac{G(Z)}{(Z - x_i)G'(x_i)}$$

It is clear that $\phi_i(x_j) = 0$ for $i, j \in S$ and $j \neq i$. That $\phi_i(x_i) = 1$ follows from the rule of L'Hospital which is valid for ratios of polynomials over any field.

The syndromes can now be expressed as:

$$\sigma_k = e_k - \sum_{i \in S} e_i \frac{G(x_k)}{(x_k - x_i)G'(x_i)}$$

or

$$\frac{\sigma_k}{G(x_k)} = \frac{e_k}{G(x_k)} - \sum_{i \in S} \frac{e_i}{G'(x_i)} \frac{1}{(x_k - x_i)}$$

This looks simpler if we define

$$\sigma_k^* = \frac{\sigma_k}{G(x_k)}$$

$$e_k^* = \frac{e_k}{G(x_k)} \text{ for } k \in S^c$$

and

$$e_i^* = \frac{e_i}{G'(x_i)}$$

then

$$\sigma_k^* = e_k^* - \sum_{i \in S} \frac{e_i^*}{(x_k - x_i)}$$

Not all of the e's are non-zero.
Let E be the set of indices for which $e_i \neq 0$

Define

$$Q_S(Z) = \prod_{i \in E \cap S} (Z - x_i)$$

and

$$Q_C(Z) = \prod_{i \in E \cap S^c} (Z - x_i)$$

The roots of $Q_S(Z)$ are those x_i for which $i \in S$ and $e_i \neq 0$ While the roots of $Q_C(Z)$ are those x_i for which $i \in S^c$ and $e_i \neq 0$

The summation expression in the syndrome equations can now be put over a common denominator to give

$$\sigma_k^* = e_k^* - \frac{A(x_k)}{Q_S(x_k)}$$

where the degree of Q_S is the number of errors at selected indices and the degree of A is less

For $k \in S^c$, either $e_k = 0$ or $Q_C(x_k) = 0$ so the product is 0 for $k \in S^c$. Multiplying the previous syndrome expression by $Q(x_k) \equiv Q_S(x_k)Q_C(x_k)$ gives

$$Q(x_k)\sigma_k^* = Q_C(x_k)A(x_k) \equiv P(x_k)$$

$$\boxed{Q(x_k)\sigma_k^* = P(x_k)}$$

This expression has, as unknowns, the coefficients of Q and P and provides a system of linear equations for their solution.

At first glance this looks the same has the Classical case but is not. The classical equations are statements about the relationship between COEFFICIENTS of polynomials while the above expression is a relation about the VALUES of polynomials.