Decoding BCH Codes Using the Euclidean Algorithm for Finding Greatest Common Divisors

In 1975 Sugiyama[1], *et. al.*, published an article describing how to use Euclid's gcd algorithm to solve the key equations for decoding BCH codes. A matrix formulation of Euclid's algorithm is presented in these notes first. Then the method for solving the key BCH decoding equation is presented.

1 A Matrix Formulation of Euclid's Algorithm for Finding Greatest Common Divisors

Euclid's algorithm for finding the greatest common divisor (gcd) of two polynomials can be expressed as a matrix recursion. Suppose we want to find the gcd of $s(D)$ and $t(D)$ where $\deg s(D) \geq \deg t(D)$. Let $s^{(0)}(D) = s(D)$ and $t^{(0)}(D) = t(D)$. As a first step the Euclidean division algorithm can be used to express $s^{(0)}(D)$ as

$$s^{(0)}(D) = Q^{(0)}(D)t^{(0)}(D) + t^{(1)}(D) \tag{1}$$

where $Q^{(0)}(D)$ is the quotient and $t^{(1)}(D)$ is the remainder which has a degree less than the degree of the divisor $t^{(0)}(D)$. From (1) it is clear that the remainder is

$$t^{(1)}(D) = s^{(0)}(D) - Q^{(0)}(D)t^{(0)}(D) \tag{2}$$

The $\gcd(s^{(0)}(D), t^{(0)}(D))$ divides the right-hand side of (2), so it also divides the remainder $t^{(1)}(D)$. Let $s^{(1)}(D) = t^{(0)}(D)$. Then

$$\begin{bmatrix} s^{(1)}(D) \\ t^{(1)}(D) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -Q^{(0)}(D) \end{bmatrix} \begin{bmatrix} s^{(0)}(D) \\ t^{(0)}(D) \end{bmatrix} = \mathbf{B}^{(1)} \begin{bmatrix} s(D) \\ t(D) \end{bmatrix} \tag{3}$$

Let

$$\mathbf{G}^{(0)} = \begin{bmatrix} 0 & 1 \\ 1 & -Q^{(0)}(D) \end{bmatrix} \tag{4}$$

and

$$\mathbf{B}^{(0)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{5}$$

Clearly $\mathbf{B}^{(1)} = \mathbf{G}^{(0)}\mathbf{B}^{(0)}$.

If the remainder $t^{(1)}(D)$ is not zero, the division process can be repeated with $s^{(1)}$ and $t^{(1)}(D)$ to get

$$s^{(1)}(D) = Q^{(1)}(D)t^{(1)}(D) + t^{(2)}(D) \tag{6}$$

with $\deg\, t^{(2)}(D) < \deg\, t^{(1)}(D)$. Also,

$$t^{(2)}(D) = s^{(1)}(D) - Q^{(1)}(D)t^{(1)}(D) \tag{7}$$

[1]Sugiyama, Y., M. Kasahara, and T. Namekawa, "A Method for Solving Key Equation for Decoding Goppa Codes," *Information and Control*, Vol. 27, 1975, pp. 87–99.

The gcd must also divide $t^{(2)}(D)$. Let $s^{(2)}(D) = t^{(1)}(D)$. In matrix form

$$\begin{bmatrix} s^{(2)}(D) \\ t^{(2)}(D) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -Q^{(1)}(D) \end{bmatrix} \begin{bmatrix} s^{(1)}(D) \\ t^{(1)}(D) \end{bmatrix} = \mathbf{G}^{(1)}\mathbf{B}^{(1)} \begin{bmatrix} s(D) \\ t(D) \end{bmatrix} = \mathbf{B}^{(2)} \begin{bmatrix} s(D) \\ t(D) \end{bmatrix} \tag{8}$$

where

$$\mathbf{G}^{(1)} = \begin{bmatrix} 0 & 1 \\ 1 & -Q^{(1)}(D) \end{bmatrix} \tag{9}$$

and

$$\mathbf{B}^{(2)} = \mathbf{G}^{(1)}\mathbf{B}^{(1)} = \mathbf{G}^{(1)}\mathbf{G}^{(0)}\mathbf{B}^{(0)} \tag{10}$$

This procedure can be repeated as long as the remainder is not zero. The general form of the recursion at step r is

$$Q^{(r)}(D) = \left\lfloor \frac{s^{(r)}(D)}{t^{(r)}(D)} \right\rfloor \tag{11}$$

$$\mathbf{B}^{(r+1)} = \begin{bmatrix} 0 & 1 \\ 1 & -Q^{(r)}(D) \end{bmatrix} \mathbf{B}^{(r)} = \mathbf{G}^{(r)}\mathbf{B}^{(r)} = \mathbf{G}^{(r)}\mathbf{G}^{(r-1)} \cdots \mathbf{G}^{(0)} \tag{12}$$

$$\begin{bmatrix} s^{(r+1)}(D) \\ t^{(r+1)}(D) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -Q^{(r)}(D) \end{bmatrix} \begin{bmatrix} s^{(r)}(D) \\ t^{(r)}(D) \end{bmatrix} = \mathbf{B}^{(r+1)} \begin{bmatrix} s(D) \\ t(D) \end{bmatrix} \tag{13}$$

Since the degree of the remainder decreases at each step, the remainder must become zero at some point, say, $r + 1 = R$, and (13) becomes

$$\begin{bmatrix} s^{(R)}(D) \\ 0 \end{bmatrix} = \mathbf{B}^{(R)} \begin{bmatrix} s(D) \\ t(D) \end{bmatrix} \tag{14}$$

The first row of (14) is equivalent to

$$s^{(R)}(D) = \mathbf{B}_{11}^{(R)} s(D) + \mathbf{B}_{12}^{(R)} t(D) \tag{15}$$

Since $\gcd(s, t)$ divides $s(D)$ and $t(D)$ it also must divide $s^{(R)}(D)$.

The inverse of $\mathbf{B}^{(R)}$ exists since $\det \mathbf{B}^{(R)} = \Pi_{i=0}^{R-1} \det \mathbf{G}^{(i)} = (-1)^R \neq 0$. Therefore,

$$\begin{bmatrix} s(D) \\ t(D) \end{bmatrix} = \left[B^{(R)}\right]^{-1} \begin{bmatrix} s^{(R)}(D) \\ 0 \end{bmatrix} = \left[\mathbf{G}^{(0)}\right]^{-1} \left[\mathbf{G}^{(1)}\right]^{-1} \cdots \left[\mathbf{G}^{(R-1)}\right]^{-1} \begin{bmatrix} s^{(R)}(D) \\ 0 \end{bmatrix} \tag{16}$$

with

$$\left[\mathbf{G}^{(r)}\right]^{-1} = \begin{bmatrix} Q^{(r)} & 1 \\ 1 & 0 \end{bmatrix} \tag{17}$$

So

$$s(D) = \left[\mathbf{B}^{(R)}\right]_{11}^{-1} s^{(R)}(D) \quad \text{and} \quad t(D) = \left[\mathbf{B}^{(R)}\right]_{21}^{-1} s^{(R)}(D) \tag{18}$$

Since $s^{(R)}(D)$ divides both $s(D)$ and $t(D)$, it is a common divisor of $s(D)$ and $t(D)$. However, it was demonstrated in the previous paragraph the $\gcd(s(D), t(D))$ divides $s^{(R)}$. Therefore,

$$\gcd(s(D), t(D)) = \alpha s^{(R)}(D) \tag{19}$$

where α is some scale factor. In other words, the last non-zero remainder is proportional to the gcd.

Finally, the terms in (18) will be expressed directly in terms of the elements of $\mathbf{B}^{(R)}$. Since $\det \mathbf{B}^{(R)} = (-1)^R$

$$\left[\mathbf{B}^{(R)}\right]^{-1} = \frac{1}{\det \mathbf{B}^{(R)}} \text{ adj } \mathbf{B}^{(R)} = (-1)^R \begin{bmatrix} \mathbf{B}_{22}^{(R)} & -\mathbf{B}_{12}^{(R)} \\ -\mathbf{B}_{21}^{(R)} & \mathbf{B}_{11}^{(R)} \end{bmatrix} \tag{20}$$

Therefore,

$$s(D) = (-1)^R \mathbf{B}_{22}^{(R)} s^{(R)}(D) \quad \text{and} \quad t(D) = (-1)^{R+1} \mathbf{B}_{21}^{(R)} s^{(R)}(D) \tag{21}$$

2 Using Euclid's Algorithm to Decode BCH Codes

Suppose the design distance for a BCH code is $d = 2t_0 + 1$. The generator polynomial for the code is the smallest degree polynomial over the symbol field with roots α^{m_0+i} for $i = 0, \ldots, d-2$ and the syndromes for the received word $y(D)$ were defined to be

$$s_i = y(\alpha^{m_0+i}) \quad \text{for} \quad i = 0, \ldots, d-2 \tag{22}$$

which is a sequence of $d - 1 = 2t_0$ field elements. The syndrome polynomial was defined as

$$S(D) = \sum_{i=0}^{d-2} s_i D^i \tag{23}$$

If t errors occur in positions $n_1, \ldots, n_t$, the error locators were defined as

$$U_k = \alpha^{n_k} \quad \text{for} \quad k = 1, \ldots, t \tag{24}$$

and the error locator polynomial was defined to be

$$\sigma(D) = \prod_{k=1}^{t} (1 - U_k D) = 1 + \sigma_1 D + \cdots + \sigma_t D^t \tag{25}$$

The error evaluator polynomial was defined as

$$A(D) = [\sigma(D) S(D)]_0^{d-2} \tag{26}$$

and it was shown that $\deg A(D) \leq t - 1 \leq t_0 - 1$. Therefore, we concluded that $S(D)$ can be found by solving the key equation

$$[\sigma(D) S(D)]_t^{d-2} = 0 \tag{27}$$

which is a set of $d - t - 1 = 2t_0 - t \geq t_0$ equations in t unknowns. Of course, this assumes that no more than the guaranteed number of correctable errors occurred, that is, $t \leq t_0$.

Since $d - 2 = 2t_0 - 1$, the formula for $A(D)$ can also be written as

$$A(D) = \sigma(D) S(D) \mod D^{2t_0} \tag{28}$$

with $\deg \sigma(D) \leq t_0$ and $\deg A(D) \leq t_0 - 1$. The mod operation deletes all powers of D greater than or equal to $2t_0$ in the product which is what the bracket operation does. The solution for $A(D)$ and $\sigma(D)$ is unique for a correctable number of errors.

From (13) for the Euclid gcd recursion, it follows that

$$\begin{bmatrix} s^{(r)}(D) \\ t^{(r)}(D) \end{bmatrix} = \begin{bmatrix} \mathbf{B}_{11}^{(r)} & \mathbf{B}_{12}^{(r)} \\ \mathbf{B}_{21}^{(r)} & \mathbf{B}_{22}^{(r)} \end{bmatrix} \begin{bmatrix} s(D) \\ t(D) \end{bmatrix} \tag{29}$$

so that

$$\begin{aligned} t^{(r)}(D) &= \mathbf{B}_{22}^{(r)} t(D) + \mathbf{B}_{21}^{(r)} s(D) \\ &= \mathbf{B}_{22}^{(r)} t(D) \mod s(D) \end{aligned} \tag{30}$$

This has the form of (28), the equation we wish to solve, if we let $s(D) = D^{2t_0}$ and $t(D) = S(D)$. Then it will be shown that $A(D) = t^{(r)}(D)$ and $\sigma(D) = \mathbf{B}_{22}^{(r)}$ for a specific value of r, say, r', found in the recursion. To solve the key equation, we must find the integer r' such that $\deg \mathbf{B}_{22}^{(r')} \leq t_0$ and $\deg t^{(r')}(D) \leq t_0 - 1$. Since $t^{(r)}(D)$ is the remainder at each step, its degree starts at $\deg S(D) = 2t_0 - 1$ for $r = 0$ and decreases as r increases. As the recursion progresses, let r' be the value of r such that

$$\deg t^{(r'-1)}(D) \geq t_0 \quad \text{and} \quad \deg t^{(r')}(D) \leq t_0 - 1 \tag{31}$$

By the rule for finding r', we have guaranteed that $\deg t^{(r')} \leq t_0 - 1$. It will now be shown that $\deg \mathbf{B}_{22}^{(r')} \leq t_0$. According to (12),

$$\mathbf{B}^{(r')} = \prod_{r=r'-1}^{0} \begin{bmatrix} 0 & 1 \\ 1 & -Q^{(r)}(D) \end{bmatrix} \tag{32}$$

with the factor for $r = r' - 1$ on the left and the factor for $r = 0$ on the right. Since the degrees of successive remainders decrease, the quotients, $Q^{(r)}(D)$, have a degree of at least 1. Forming the products, starting from the left, it can be seen that $\deg \mathbf{B}_{22}^{(r')} > \deg \mathbf{B}_{12}^{(r')}$. In addition, we can conclude that $\deg \mathbf{B}_{22}^{(r)}$ increases with r starting with degree 1 for $r = 1$. Also remember that $s^{(r')}(D) = t^{(r'-1)}(D)$ so $\deg s^{(r')}(D) > \deg t^{(r')}(D)$. Using the inverse formula (20) to solve for $s(D)$ and $t(D)$ gives

$$\begin{bmatrix} s(D) \\ t(D) \end{bmatrix} = (-1)^{r'} \begin{bmatrix} \mathbf{B}_{22}^{(r')} & -\mathbf{B}_{12}^{(r')} \\ -\mathbf{B}_{21}^{(r')} & \mathbf{B}_{11}^{(r')} \end{bmatrix} \begin{bmatrix} s^{(r')}(D) \\ t^{(r')}(D) \end{bmatrix} \tag{33}$$

Therefore,

$$s(D) = (-1)^{r'} \left[\mathbf{B}_{22}^{(r')} s^{(r')}(D) - \mathbf{B}_{12}^{(r')} t^{(r')}(D) \right] \tag{34}$$

From the degree inequalities stated just before these equations, it follows that

$$\deg s(D) = \deg \left[\mathbf{B}_{22}^{(r')} s^{(r')}(D) \right] = \deg \mathbf{B}_{22}^{(r')} + \deg s^{(r')}(D) \tag{35}$$

Rearranging gives

$$\begin{aligned} \deg \mathbf{B}_{22}^{(r')} &= \deg s(D) - \deg s^{(r')}(D) = \deg D^{2t_0} - \deg t^{(r'-1)}(D) \\ &\leq 2t_0 - t_0 = t_0 \end{aligned} \tag{36}$$

For a binary symmetric channel with cross-over probability less than 0.5, error patterns with lower weight are more likely than ones with higher weight. Thus no errors are most likely, then single errors, etc. If the syndromes are all 0, then either no error or an undetectable error occurred. If the syndromes are not all 0, this decoding algorithm has the nice property that it tries to correct the most likely single error patterns first and successively proceeds to higher weight patterns. This follows from the fact that $\deg \mathbf{B}_{22}^{(r)}$ starts at 1 for $r = 1$ and increases with r. Remember that when r' is reached, $\deg \mathbf{B}_{22}^{(r)}$ is equal to the number of errors if a correctable error occurred.

In summary, the steps for solving the key equation using Euclid's gcd algorithm are:

1. Compute the syndrome polynomial $S(D)$.
2. Initialize to $s^{(0)}(D) = D^{2t_0}$, $t^{(0)}(D) = S(D)$, and $\mathbf{B}^{(0)} = \mathbf{I}_{2\times 2}$.
3. Solve the following recursive formulas until $\deg t^{(r')}(D) \leq t_0 - 1$:

$$Q^{(r)}(D) = \left\lfloor \frac{s^{(r)}(D)}{t^{(r)}(D)} \right\rfloor \tag{37}$$

$$\mathbf{B}^{(r+1)} = \begin{bmatrix} 0 & 1 \\ 1 & -Q^{(r)}(D) \end{bmatrix} \mathbf{B}^{(r)} \tag{38}$$

$$\begin{bmatrix} s^{(r+1)}(D) \\ t^{(r+1)}(D) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -Q^{(r)}(D) \end{bmatrix} \begin{bmatrix} s^{(r)}(D) \\ t^{(r)}(D) \end{bmatrix} \tag{39}$$

4. Let $\Delta = \mathbf{B}_{22}^{(r')}|_{D=0}$. Then the solutions are:

$$A(D) = \Delta^{-1} t^{(r')}(D) \tag{40}$$

$$\sigma(D) = \Delta^{-1} \mathbf{B}_{22}^{(r')} \tag{41}$$

The normalization by Δ^{-1} is required to make $\sigma_0 = 1$. A flowchart for this algorithm is shown at the end of this document.

A Very Simple Example

As a very simple example, consider the single error correcting Reed-Solomon code with $d = 3$, $t_0 = 1$, and α a primitive element of GF(p^m). Then $d - 2 = 1$ so α^{m_0} and α^{m_0+1} are roots of $g(D)$. Suppose the received word contains a single error of value V in position n so

$$y(D) = x(D) + VD^n \tag{42}$$

The required syndromes are

$$s_0 = y(\alpha^{m_0}) = V\alpha^{m_0 n} \quad \text{and} \quad s_1 = y(\alpha^{m_0+1}) = V\alpha^{(m_0+1)n} \tag{43}$$

Of course, V and n are unknown and must be found. The syndrome polynomial is

$$S(D) = s_0 + s_1 D \tag{44}$$

The key equation is

$$A(D) = [(1 + \sigma_1 D)(s_0 + s_1 D)]_0^1 \tag{45}$$

In this case, $\deg A(D) \leq t_0 - 1 = 0$, so

$$A(D) = [(1 + \sigma_1 D)(s_0 + s_1 D)]_0^0 = s_0 \tag{46}$$

and

$$[(1 + \sigma_1 D)(s_0 + s_1 D)]_1^1 = 0 \tag{47}$$

or

$$\sigma_1 s_0 + s_1 = 0 \tag{48}$$

so

$$\sigma_1 = -s_1 s_0^{-1} \tag{49}$$

Therefore, the error locator polynomial is

$$\sigma(D) = 1 - s_1 s_0^{-1} D \tag{50}$$

In this simple example, it is clear that the single error locator is

$$U = s_1 s_0^{-1} = V\alpha^{(m_0+1)n} V^{-1} \alpha^{-m_0 n} = \alpha^n \tag{51}$$

The error value is

$$V = -U^{1-m_0} A(U^{-1})/\sigma'(U^{-1}) = -\left(s_1 s_0^{-1}\right)^{1-m_0} s_0 \left(-s_1 s_0^{-1}\right)^{-1} = s_0 U^{-m_0} \tag{52}$$

Since $s_0 = V\alpha^{m_0 n}$ and $U = \alpha^n$, this formula gives the correct value for V.

Now the Euclidean algorithm will be used to find $A(D)$ and $\sigma(D)$. The initial values are $s^{(0)}(D) = D^{2t_0} = D^2$ and $t^{(0)}(D) = S(D) = \sigma_0 + \sigma_1 D$. Dividing $s^{(0)}(D)$ by $t^{(0)}(D)$ we find that quotient is

$$Q^{(0)}(D) = s_1^{-1} D - s_1^{-2} s_0 \tag{53}$$

and the remainder is

$$t^{(1)}(D) = s_1^{-2} s_0^2 \tag{54}$$

Notice that $\deg t^{(1)}(D) = 0$ which is equal to $t_0 - 1 = 0$, so we have determined that $r' = 1$. The required transformation matrix is

$$\mathbf{B}^{(1)} = \begin{bmatrix} 0 & 1 \\ 1 & -Q^{(0)}(D) \end{bmatrix} \tag{55}$$

Thus

$$B_{22}^{(1)} = -Q^{(0)}(D) \quad \text{and} \quad \Delta = s_1^{-2} s_0 \tag{56}$$

According to (40) and (41)

$$A(D) = \Delta^{-1} t^{(1)}(D) = s_0 \tag{57}$$

and

$$\sigma(D) = \Delta^{-1} B_{22}^{(1)} = 1 - s_1 s_0^{-1} D \tag{58}$$

exactly as determined previously by direct solution of the key equations. ■

A Slightly More Complicated Example

Now assume the code is a t_0-error correcting Reed-Solomon code corresponding to the root sequence α^{m_0+i} for $i = 0, \ldots, 2t-1$. Suppose a genie tells us that the single error pattern $E(D) = VD^n$ occurred. Then the syndromes are

$$s_i = V\alpha^{n(m_0+i)} \quad \text{for} \quad i = 0, \cdots, 2t_0 - 1 \tag{59}$$

Then $s^{(0)}(D) = D^{2t_0}$ and $t^0(D) = \sum_{i=0}^{2t_0-1} V\alpha^{m_0+i} D^i$. Dividing $t^{(0)}(D)$ into $s^{(0)}(D)$ gives the quotient

$$Q^{(0)}(D) = V^{-1}\alpha^{-n(m_0+2t_0-1)} D - V^{-1}\alpha^{-n(m_0+2t_0)} \tag{60}$$

and remainder

$$t^{(1)}(D) = -\alpha^{-n2t_0} \tag{61}$$

Therefore, in the very first iteration, we have determined that $r' = 1$ since $\deg t^{(1)}(D) = 0 \leq t_0 - 1$. Since $\mathbf{B}_{22}^{(1)} = -Q^{(0)}(D)$, it follows that $\Delta = V^{-1}\alpha^{-n(m_0+2t_0)}$ and

$$\sigma(D) = -\Delta^{-1} Q^{(0)}(D) = 1 - \alpha^n D \tag{62}$$

and

$$A(D) = \Delta^{-1} t^{(1)}(D) = V\alpha^{m_0 n} \tag{63}$$

Therefore, the error locator is $U = \alpha^n$. It is readily verified that $V = -U^{1-m_0} A(U^{-1})/\sigma'(U^{-1})$.
■

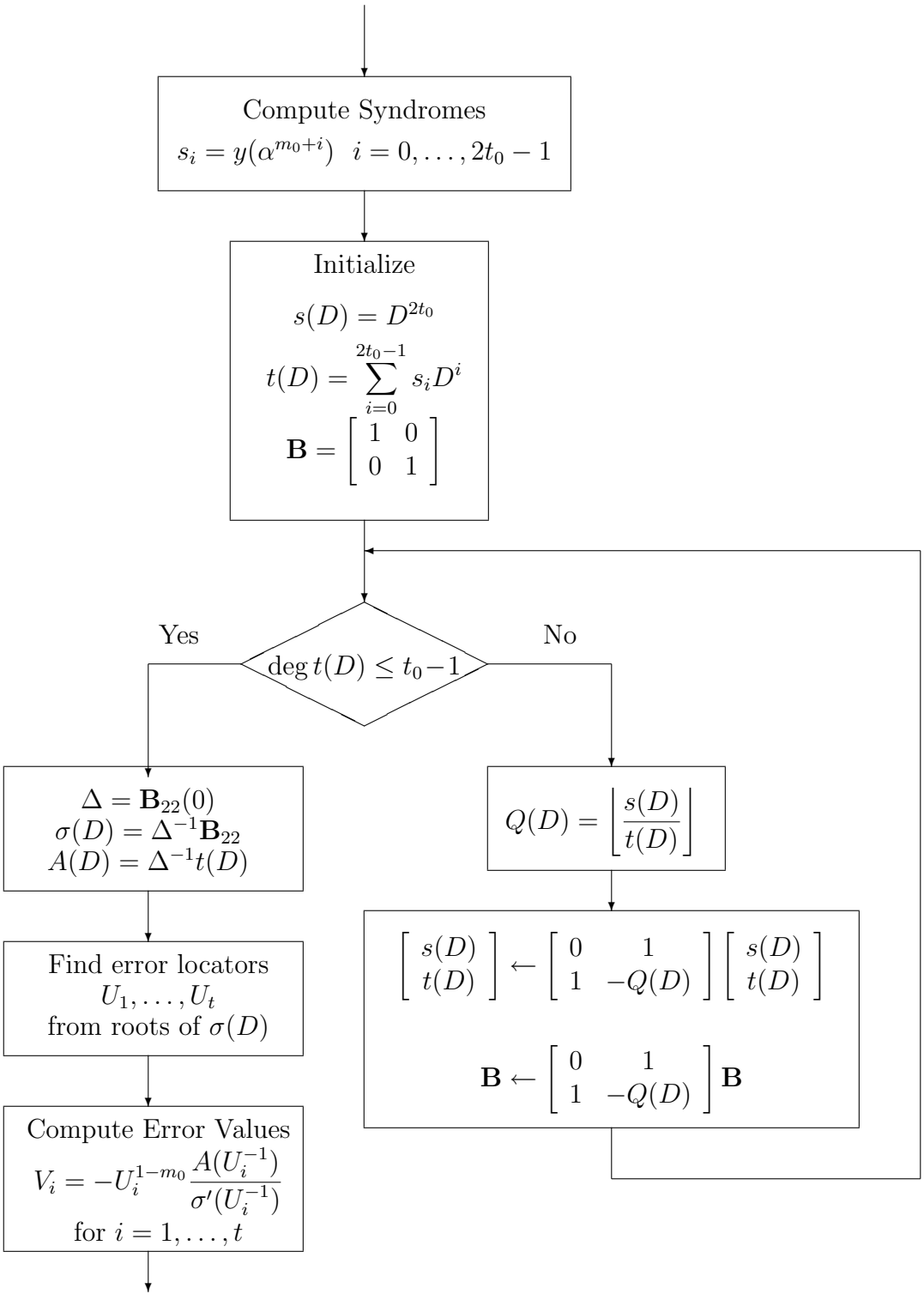

Figure 1: Flowchart for Solving the Key Equation Using the Euclid's GCD Algorithm