A Formula for Solving the Quintic over GF(256)

Christopher Wayne Walker
University of Southern California and TRW[1]

July 2001

Abstract

In algebraic decoding of certain codes, such as BCH codes, an error locator polynomial is constructed whose roots point to where errors have been detected in the received codeword. Formulas for solving the degree 2 error locator polynomial (and consequently degree 3 and degree 4 polynomials) are available in the literature. In this paper an explicit formula is given for solving the quintic with coefficients and five distinct roots in GF(256).

1 Introduction

Formulas for solving the degree 2 error locator polynomial are readily available (Walker [7], Berlekamp [1], Chen [3]). The degree 3 and degree 4 polynomials can be solved by solving certain degree 2 polynomials just as over the rational field. For the degree 5 polynomial, explicit algebraic formulas cannot exist for the roots, in general, over the rational field. However, the quintic is solvable over finite Galois fields since the corresponding Galois groups are solvable. In this paper an explicit formula is given for solving the

[0]cwwalker@cwwphd.com

[0]Key words and phrases: Finding roots, polynomials, quintic equations.

[0]This paper was presented at the *Sixth International Symposium on Communication Theory and Applications* in Ambleside, Lake District, UK, July 15-20, 2001.

[1]Now Northrop Grumman Aerospace Systems.

quintic with coefficients and five distinct roots (error locator polynomial) in GF(256). Specifically, an algebraic formula is given for one of the roots and the remaining roots can be found by solving the resulting quartic factor. Due to the computational complexity of the formula approach developed in this study, this analysis may be of more theoretical than practical interest.

2 Background

In December 1786, the mathematician E.S. Bring showed how to utilize a Tschirnhaus(en) transformation to reduce the general quintic defined over the rationals to the form $h(x) = x^5 + ex + f$. This technique is described in Harley [4] (the reader can also consult Cayley [2]). We will specialize this method for our finite fields and reduce the general quintic to a trinomial form. Incidentally, the motivation back in Bring's day for performing such a reduction was to hopefully reduce the quintic to a pure form $f(x) = x^5 + f$, thus solving the quintic. Thanks to Abel and later Galois we now know that Bring's goal was impossible to achieve for a quintic over the rationals (see, for example, Holmboe [5] and Rotman [6]). However, the quintic, and any degree polynomial, is theoretically solvable over finite fields.

3 Formula Development

Consider the 5th degree polynomial

$$f_1(x_1) = x_1^5 + b_1 x_1^4 + c_1 x_1^3 + d_1 x_1^2 + e_1 x_1 + f_1$$

with coefficients and five distinct roots in $GF\,(2^m)$.

Step 1: If $c_1 = 0$ then skip to Step 3. Else, let $x_1 = x_2 + d_1/c_1$ to obtain

$$f_2(x_2) = x_2^5 + b_2 x_2^4 + c_2 x_2^3 + e_2 x_2 + f_2$$

where,

$$b_2 = \frac{d_1}{c_1} + b_1,\ c_2 = c_1,\ e_2 = \frac{d_1^4}{c_1^4} + \frac{d_1^2}{c_1^2} + e_1,\ f_2 = \frac{d_1^5}{c_1^5} + b_1\frac{d_1^4}{c_1^4} + e_1\frac{d_1}{c_1} + f_1.$$

Step 2: If $f_2 = 0$ then 0 is a root of $f_2(x_2)$ and the remaining roots can be found by solving the resulting quartic. Else, let $x_2 = 1/x_3$ and clear

denominators to get

$$f_3(x_3) = a_3x_3^5 + b_3x_3^4 + d_3x_3^2 + e_3x_3 + f_3$$

where,

$$a_3 = f_2,\ b_3 = e_2,\ d_3 = c_2,\ e_3 = b_2,\ f_3 = 1.$$

Step 3: Let $x_3 = z + b_3/a_3$ to get

$$f_4(z) = z^5 + pz^2 + qz + r$$

where,

$$p = \frac{d_3}{a_3},\ q = \frac{b_3^4}{a_3^4} + \frac{e_3}{a_3},\ r = d_3\frac{b_3^2}{a_3^2} + e_3\frac{b_3}{a_3^2} + \frac{f_3}{a_3}.$$

Now let

$$y = z^4 + dz^3 + cz^2 + bz + a.$$

Multiplying this last equation by successive powers of z and reducing using $z^5 + pz^2 + qz + r = 0$, we can form the following system of equations:

$$\begin{aligned}
(y+a) + bz + cz^2 + dz^3 + z^4 &= 0,\\
r + (y+a+q)z + (b+p)z^2 + cz^3 + dz^4 &= 0,\\
dr + (r+dq)z + (y+a+q+dp)z^2 + (b+p)z^3 + cz^4 &= 0,\\
cr + (dr+cq)z + (r+dq+cp)z^2 + (y+a+q+dp)z^3 + (b+p)z^4 &= 0,\\
(b+p)r + (cr+bq+pq)z + (dr+cq+bp+p^2)z^2 + (r+dq+cp)z^3 &\\
+(y+a+q+dp)z^4 &= 0.
\end{aligned}$$

We can write the above system of equations in matrix form $A\underline{z} = 0$. The determinant of A set equal to zero then gives us a quintic in y. We get

$$y^5 + \alpha y^4 + \beta y^3 + \gamma y^2 + \delta y + \epsilon = 0,$$

where,

$$\alpha = a + dp, \quad \beta = bcp + cp^2 + d^2p^2 + dpq + br + cdr,$$

$$\begin{aligned}
\gamma \ = \ & b^3p + abcp + b^2p^2 + acp^2 + c^3p^2 + bcdp^2 + ad^2p^2 + bp^3\\
& + cdp^3 + d^3p^3 + p^4 + adpq + c^2dpq + bd^2pq + d^2p^2q + dpq^2\\
& + abr + bc^2r + b^2dr + acdr + bdpr + cd^2pr + dp^2r + bqr\\
& + d^3qr + cr^2 + d^2r^2,
\end{aligned}$$

$$\begin{aligned}\delta &= a^4 + a^2bcp + a^2cp^2 + a^2d^2p^2 + b^4q + b^3pq + bc^3pq + a^2dpq \\ &\quad + b^2cdpq + b^2p^2q + bcdp^2q + bd^3p^2q + bp^3q + c^4q^2 + bcpq^2 \\ &\quad + c^2dpq^2 + bd^2pq^2 + cd^3pq^2 + cp^2q^2 + d^4q^3 + dpq^3 + q^4 \\ &\quad + a^2br + b^3cr + a^2cdr + b^2cpr + b^2d^2pr + bc^2qr + b^2dqr \\ &\quad + c^3dqr + bcd^2qr + cd^2pqr + d^4pqr + dp^2qr + bq^2r + cdq^2r \\ &\quad + d^3q^2r + b^2r^2 + c^3r^2 + bcdr^2 + c^2d^2r^2 + bd^3r^2 + bpr^2 \\ &\quad + d^2qr^2 + dr^3,\end{aligned}$$

and

$$\begin{aligned}\epsilon &= a^5 + a^2b^3p + a^3bcp + a^4dp + a^2b^2p^2 + a^3cp^2 + a^2c^3p^2 + a^2bcdp^2 \\ &\quad + a^3d^2p^2 + a^2bp^3 + a^2cdp^3 + a^2d^3p^3 + a^2p^4 + ab^4q + ab^3pq + abc^3pq \\ &\quad + a^3dpq + ab^2cdpq + a^2c^2dpq + a^2bd^2pq + ab^2p^2q + abcdp^2q \\ &\quad + a^2d^2p^2q + abd^3p^2q + abp^3q + ac^4q^2 + abcpq^2 + a^2dpq^2 + ac^2dpq^2 \\ &\quad + abd^2pq^2 + acd^3pq^2 + acp^2q^2 + ad^4q^3 + adpq^3 + aq^4 + a^3br + b^5r \\ &\quad + ab^3cr + a^2bc^2r + a^2b^2dr + a^3cdr + b^4pr + ab^2cpr + b^2c^3pr + a^2bdpr \\ &\quad + b^3cdpr + ab^2d^2pr + a^2cd^2pr + b^3p^2r + a^2dp^2r + b^2cdp^2r + b^2d^3p^2r \\ &\quad + b^2p^3r + a^2bqr + abc^2qr + bc^4qr + ab^2dqr + ac^3dqr + abcd^2qr \\ &\quad + a^2d^3qr + b^2cpqr + bc^2dpqr + b^2d^2pqr + acd^2pqr + bcd^3pqr \\ &\quad + ad^4pqr + bcp^2qr + adp^2qr + abq^2r + acdq^2r + ad^3q^2r + bd^4q^2r \\ &\quad + bdpq^2r + bq^3r + ab^2r^2 + a^2cr^2 + b^2c^2r^2 + ac^3r^2 + c^5r^2 \\ &\quad + b^3dr^2 + abcdr^2 + bc^3dr^2 + a^2d^2r^2 + b^2cd^2r^2 + ac^2d^2r^2 + abd^3r^2 \\ &\quad + abpr^2 + bc^2pr^2 + b^2dpr^2 + c^3dpr^2 + c^2d^3pr^2 + c^2p^2r^2 \\ &\quad + b^2qr^2 + bcdqr^2 + ad^2qr^2 + bd^3qr^2 + cd^4qr^2 + bpqr^2 \\ &\quad + cdpqr^2 + cq^2r^2 + bcr^3 + adr^3 + c^2dr^3 + bd^2r^3 + cd^3r^3 \\ &\quad + d^5r^3 + d^2pr^3 + dqr^3 + r^4.\end{aligned}$$

We now wish to find conditions that will make $\alpha = \beta = \gamma = 0$. An easy observation shows that $a = dp$ will force $\alpha = 0$ (d is yet to be determined). This value of a can be substituted into the equations $\beta = 0$ and $\gamma = 0$ and then eliminating either b, c or d results in an equation of the sixth degree. This elevation of degree can be avoided by the following technique. Let

$b = \theta d + \lambda$, and $c = d + \tau$. Then, the equation $\beta = 0$ becomes a quadratic in d, viz.,

$$\left(p\theta + p^2 + r\right) d^2 + \left(p\tau\theta + p\lambda + p^2 + pq + r\theta + r\tau\right) d + \left(p\lambda\tau + p^2\tau + r\lambda\right) = 0.$$

We will now make each of the coefficients of this quadratic vanish. We set

$$\theta = \frac{p^2 + r}{p}$$

to cancel the coefficient of d^2. Then with θ determined, we set

$$\begin{aligned} \lambda &= \frac{p\tau\theta + p^2 + pq + r\theta + r\tau}{p} \\ &= \frac{p\theta + r}{p}\tau + \frac{p^2 + pq + r\theta}{p} \end{aligned}$$

to get λ as a linear function of τ. Substituting this result into the expression for the third coefficient gives us a quadratic in τ with known coefficients. Thus, θ, λ and τ have been determined such that the condition $\beta = 0$ is met. Next we substitute $a = dp$, $b = \theta d + \lambda$ and $c = d + \tau$ into the equation $\gamma = 0$ and the resulting equation will be a function of only one unknown, namely, d. An observation of the above expression for γ shows that this last equation in d cannot be greater than the third degree. So, by solving this possible cubic in d we have satisfied the condition $\gamma = 0$ and our quintic equation becomes

$$y^5 + \delta y + \epsilon = 0$$

which is the desired trinomial form. We now normalize the degree one coefficient to one by letting $y = \delta^{1/4} x$ and dividing by the leading coefficient to get

$$x^5 + x + f = 0,$$

where, $f = \epsilon\delta^{-5/4}$. We now offer a formula solution for a root to this equation that is valid in $GF(256)$.

Theorem. *A quintic equation with five distinct roots in GF(256) and of the form $g(x) = x^5 + x + f$, has as a root, $x = f^2 + 1$.*

Proof: The proof is based on the fact (which is easily verified on a computer) that the only possible values for f under the conditions of the theorem are $\{\sigma^{17},\ \sigma^{34},\ \sigma^{68},\ \sigma^{136}\}$, where σ is a root of $x^8+x^4+x^3+x^2+1$ over $GF(2)$ and a generator of $GF(256)$. In other words, f is a primitive 15th root of unity and a root of x^4+x+1 over $GF(2)$. We now compute

$$\begin{aligned} g\left(f^2+1\right) &= \left(f^2+1\right)^5+\left(f^2+1\right)+f \\ &= \left(f^8+1\right)\left(f^2+1\right)+\left(f^2+1\right)+f \\ &= \left(f^2\right)\left(f^2+1\right)+\left(f^2+1\right)+f \\ &= f^4+f+1 \\ &= 0 \end{aligned}$$

which proves the theorem. □

We may therefore write

$$g(x)=\left(x+f^2+1\right)g_1(x)$$

where,

$$g_1(x)=x^4+\left(f^2+1\right)x^3+\left(f^2+1\right)^2x^2+\left(f^2+1\right)^3x+\left(f^2+1\right)^4+1.$$

In this last equation we can make the substitution $x=(f^2+1)\,x_1$ and equate to zero to get

$$x_1^4+x_1^3+x_1^2+x_1+e=0,$$

where, $e=1+(f^2+1)^{-4}$. Using $f^4+f+1=0$ we can write $e=f^6$. We now make the substitution $x_1=x_2+1$ to get

$$x_2^4+x_2^3+e=0.$$

Now, with the inversion $x_2=1/z$ we can write

$$z^4+e^{-1}z+e^{-1}=0.$$

We can factor this last expression as

$$z^4+e^{-1}z+e^{-1}=\left(z^2+bz+c_1\right)\left(z^2+bz+c_2\right)$$

where,

$$b^3=e^{-1},\quad c_2^2+\frac{e^{-1}}{b}c_2+e^{-1}=0.$$

Now,

$$b = \left(e^{-1}\right)^{1/3} = \left(f^{-6}\right)^{1/3} = f^{-2}.$$

Thus,

$$c_2^2 + \frac{e^{-1}}{b}c_2 + e^{-1} = c_2^2 + f^{-4}c_2 + f^{-6} = 0.$$

Let $c_2 = f^{-4}c$ to get

$$c^2 + c + f^2 = 0.$$

It is easy to verify that $c = f^3$ satisfies this last equation. We then obtain $c_2 = f^{-1}$. Using $c_1 c_2 = e^{-1}$ we find that $c_1 = f^{-5}$. We may now write

$$z^4 + e^{-1}z + e^{-1} = \left(z^2 + f^{-2}z + f^{-5}\right)\left(z^2 + f^{-2}z + f^{-1}\right).$$

These last two factors can be solved by formulas for solving the quadratic. Thus, the quintic over $GF(256)$ is solvable via Tschirnhaus(en) transformations and solutions of equations of degree lower than 5.

Acknowledgments

The author would like to express his appreciation to Professor Solomon Golomb of the University of Southern California for introducing the author to Tschirnhaus(en) transformations.

References

[1] E.R. Berlekamp, H. Rumsey and G. Solomon, "On the Solution of Algebraic Equations over Finite Fields," *Inform. Theory Contr.*, pp. 553-564, 1967.

[2] A. Cayley, "On Tschirnhausen's Transformation," *Royal Society of London Philosophical Transactions*, Vol. 152, pp. 561-578, 1862.

[3] C. Chen, "Formulas for the Solutions of Quadratic Equations over $GF\left(2^m\right)$," *IEEE Trans. on Inform. Theory*, vol. IT-28, pp. 792-794, 1982.

[4] Rev. R. Harley, "Contributions to the History of the Problem of the Reduction of the General Equation of the Fifth Degree to a Trinomial Form," *The Quarterly Journal of Pure and Applied Mathematics*, pp. 38-47, 1864.

[5] B. Holmboe, *Oeuvres Completes de N.H. Abel,* Christiania, 1839.

[6] J. Rotman, *Galois Theory,* Springer-Verlag, 1990.

[7] C.W. Walker, "New Formulas for Solving Quadratic Equations over Certain Finite Fields," *IEEE Trans. on Inform. Theory*, vol. 45, pp. 283-284, Jan. 1999.