New Formulas for Solving Quadratic Equations over Certain Finite Fields

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

January 1999

Abstract

We present new formulas for solving quadratic equations with distinct roots in certain finite fields. We develop in detail formulas for solving such quadratics over $GF(4)$, $GF(16)$ and $GF(256)$ and the approach we take is applicable for solving quadratics over $GF\left(2^k\right)$, with k a power of 2.

1 Introduction

In this study we develop formulas for finding roots of quadratic equations with coefficients and distinct roots in certain finite fields. Previously, Berlekamp *et al.* [1] showed how to construct a matrix that is used to multiply the reduced quadratic (as a vector) to produce its roots. Chen [2] gave a solution of the reduced quadratic in terms of the parameters of the equation, i.e., its coefficients. A formula involving only the coefficients of the reduced quadratic also follows from the constructive proof of the additive version of Hilbert's Theorem 90 given in Kaplansky [4, pp. 40-41]. Chien *et al.* [3] utilized an efficient look-up table approach to read off the roots of the quadratic after it has been put in reduced form. In Section II we define mapping operations

[0] cwwalker@cwwphd.com

[0] Key words and phrases: Quadratic equations, polynomials, finding roots.

[1] Now Northrop Grumman Aerospace Systems.

and discuss their properties which will aid us in developing explicit formulas in Section III for solving quadratics over $GF(4)$, $GF(16)$ and $GF(256)$. The approach we take is applicable for solving quadratics over $GF\left(2^k\right)$, with k a power of 2.

2 Map Definitions and Properties

Let

$$F_m = GF\left(2^{2^m}\right),\ m \geq 0.$$

For $m \geq 1$, let

$$T_m\left(y\right) = y^{2^{2^{m-1}}} + y$$

denote the trace mapping from F_m to F_{m-1}. It follows that

- $T_m(x) \in F_{m-1},\ x \in F_m.$
- $T_m\left(x_1 + x_2\right) = T_m(x_1) + T_m(x_2),\ x_1, x_2 \in F_m.$
- $T_m\left(\alpha x\right) = \alpha T_m\left(x\right),\ x \in F_m,\ \alpha \in F_{m-1}.$
- If $x \in F_m$, then $T_m\left(x\right) = 0 \Leftrightarrow x \in F_{m-1}$.

Now fix $s \in F_m \setminus F_{m-1}$: thus $T_m(s) \neq 0$. Given any $x \in F_m$, evidently $x = \alpha_1 s + \alpha_2$ for some $\alpha_1,\ \alpha_2 \in F_{m-1}$ which depends on x. In fact, applying our trace operator gives $\alpha_1 = T_m(x)/T_m(s)$, so we can write

$$x = \frac{T_m(x)s + \gamma_x}{T_m(s)},\ \gamma_x \in F_{m-1}.$$

Next define the map $G_x^m :\ F_m \rightarrow F_m$ by

$$G_x^m(y) = \frac{T_m(y)s + \gamma_x}{T_m(s)}.$$

Clearly,

$$G_x^m\left(x + \alpha s + \beta\right) = x + \alpha s,\ \alpha, \beta \in F_{m-1}.$$

Thus,

- G_x^m is a $2^{2^{m-1}} \rightarrow 1$ mapping.

- If $S_x^m = \{x + s\alpha,\ \alpha \in F_{m-1}\}$, then S_x^m is both the image set and the set of fixed points of G_x^m.

- For any $z \in S_x^m,\ \gamma_z = \gamma_x = \gamma$ say.

Now we take x to be a root of $f(x) = x^2 + bx + c$ with coefficients and two distinct roots in F_m and set $s = b$. We will assume throughout that $b \notin F_{m-1}$. If this is not so then simply scale x by a suitable field element (such as the generator of the field).

Let a be an arbitrary element of F_m (the simplest expedient is to choose $a = 0$). If $z = G_x^m(a)$, then $x = z + \alpha b\ \ (\alpha \in F_{m-1})$ and α is obtained as the root of a quadratic over F_{m-1}, namely,

$$\alpha^2 + \alpha + \frac{f(z)}{b^2} = 0. \tag{1}$$

In (1), z is expressed in terms of γ, but γ can be expressed in terms of b and c by induction from $x^2 + bx + c$ as

$$x^{2^{2^r}} = b^{2^{2^r}-1}x + c_r,\ r \geq 0 \tag{2}$$

where $c_0 = c$ and

$$c_r = \left(b^{2^{2^r}-2^{2^{r-1}}}\right) c_{r-1} + c_{r-1}^{2^{2^{r-1}}},\ r \geq 1.$$

From (2) with $r = m - 1$ and $G_x^m(x) = x$ it follows that $\gamma = bc_{m-1}$.

3 Formula Development

Let $a = 0$ and define $\lambda = f(z)/b^2$ where as before $z = G_x^m(a)$ (so z depends on m). Also, let $s = b$ unless stated otherwise.

For $m = 1$, $\gamma = bc$. Let $z_1 = z$. Then with $\alpha \in F_0$ we have $\alpha^2 + \alpha = 0$. From (1) it then follows that

$$x = z_1 = \frac{c}{b+1}$$

is a root of $f(x)$.

For $m = 2$, $\gamma = b\,(b^2c + c^2)$. Let $z_2 = z$ and $\lambda_2 = \lambda$. Let $b^* \in F_1 \setminus F_0$ (so that $(b^*)^2 + b^* + 1 = 0$). Set $\alpha = b^*x^*$ in (1). Then,

$$x^{*^2} + \frac{x^*}{b^*} + \frac{\lambda_2}{(b^*)^2} = 0.$$

Using the formula for a quadratic over F_1 then gives

$$x^* = \frac{\lambda_2}{(b^*)^2 + b^*} = \lambda_2$$

and thus a solution of the original equation is $x = z_2 + bb^*\lambda_2$.

For $m = 3$, $\gamma = b\,(b^{14}c + b^{12}c^2 + b^8c^4 + c^8)$. Let $z_3 = z$ and $\lambda_3 = \lambda$. Let $b^{**} \in F_2 \setminus F_1$ such that $(b^{**})^4 + b^{**} + 1 = 0$. Set $\alpha = b^{**}x^{**}$ in (1). Then,

$$x^{**^2} + \frac{x^*}{b^{**}} + \frac{\lambda_3}{(b^{**})^2} = 0.$$

Define $g(u) = u^2 + b_0u + c_0$ where $b_0 = 1/b^{**}$ and $c_0 = \lambda_3/\,(b^{**})^2$. Now, we have $\gamma_u = b_0\,(b_0^2c_0 + c_0^2)$ and we use $s = b_0$. Let $z_3^* = G_u^2\,(a_0)$, where $a_0 \in F_2$ (again , $a_0 = 0$ is desirable). Define $\lambda_3^* = g\,(z_3^*)\,/b_0^2$ and let $b^* \in F_1 \setminus F_0$. Using the formula for the quadratic over F_2 then gives a root of $g(u)$ as $u = z_3^* + b_0b^*\lambda_3^*$ and thus a root of the original quadratic is $x = z_3 + bb^{**}u$ or $x = z_3 + bb^*\lambda_3^* + bb^{**}z_3^*$.

Using the above definitions and notation, we have established the following theorem.

Theorem 3.1: The polynomial

$$f(x) = x^2 + bx + c$$

$b \notin F_{m-1}$, with coefficients and two distinct roots in F_m, has roots x and $x + b$ where for

- $m = 1,\ x = z_1$.
- $m = 2,\ x = z_2 + bb^*\lambda_2$.
- $m = 3,\ x = z_3 + bb^*\lambda_3^* + bb^{**}z_3^*$.

Remarks: To use the above formulas the roots must reside in the defining finite field. If the roots reside in an extension field then the corresponding formulas would have to be applied in an appropriate extension field. Note that the solution of the cubic and quartic equations over these finite fields follows easily from these results since roots of polynomials of degree 3 or 4 can be found through solutions of certain degree 2 polynomials just as over the rational field. For details see Chen [2].

Acknowledgments

The author would like to express his appreciation to Professors Solomon Golomb and Lloyd Welch of the University of Southern California for their guidance during this work and to TRW, Redondo Beach, California for their encouragement and financial support. The author would especially like to thank the referees for their careful review and valuable suggestions that improved this correspondence.

References

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

[2] C. Chen, "Formulas for the Solutions of Quadratic Equations over $GF(2^m)$,", *IEEE Transactions on Information Theory*, pp. 792-794, 1982.

[3] R.T. Chien and B.D. Cunningham, "Hybrid Methods for Finding Roots of a Polynomial,", *IEEE Transactions on Information Theory*, pp. 329-335, 1969.

[4] Irving Kaplansky, *Fields and Rings*, 2nd ed., pp. 40-41, University of Chicago Press, 1969.