Quadratic Equations in Finite Fields of Characteristic 2

Klaus Pommerening

May 2000 – english version February 2012

Quadratic equations over fields of characteristic \( \neq 2 \) are solved by the well known quadratic formula that up to rational operations reduces the general case to the square root function, the inverse of the square map \( x \mapsto x^2 \). The solvability of a quadratic equation can be decided by looking at the discriminant—essentially the argument of the square root in the formula.

The situation in characteristic 2 is somewhat different.

1 The general solution

Let \( K \) be a field of characteristic 2. We want to study the roots of a quadratic polynomial
\[
 f = aT^2 + bT + c \in K[T] \quad \text{with} \ a \neq 0.
\]

The case \( b = 0 \)—the degenerate case—is very simple. We have
\[
 a \cdot f = (aT)^2 + ac = g(aT) \quad \text{with} \ g = T^2 + ac \in K[T].
\]

The squaring map \( x \mapsto x^2 \) is an \( \mathbb{F}_2 \)-linear monomorphism of \( K \), an automorphism if \( K \) is perfect, for example finite. Therefore \( ac \) has at most one square root in \( K \), and exactly one square root in the algebraic closure \( \bar{K} \). Let \( ac = d^2 \). Then \( g \) has exactly the one root \( d \), and \( f \) has exactly the one root \( \frac{d}{a} \) in \( \bar{K} \). For an explicit determination we have to extract the square root from \( ac \) in \( K \) or in an extension field \( L \) of degree 2 of \( K \), i. e. to invert the square map in \( K \) or \( L \). Remember that the square map is linear over \( \mathbb{F}_2 \). For examples see Section 3 below.

Now let \( b \neq 0 \). Because the derivative \( f' = b \) is constant \( \neq 0 \), \( f \) has two distinct (simple) roots in the algebraic closure \( \bar{K} \). The transformation
\[
 \frac{a}{b^2} \cdot f = (\frac{a}{b} T)^2 + \frac{a}{b} T + \frac{ac}{b^2} = g(\frac{a}{b} T) \quad \text{with} \ g = T^2 + T + d, \ d = \frac{ac}{b^2} \in K,
\]
reduces our task to the roots of the polynomial \( g \). Let \( u \) be a root of \( g \) in \( \bar{K} \). Then \( u + 1 \) is the other root by VIETA’s formula, and \( u(u + 1) = d \), that is \( d = u^2 + u \). Therefore the problem for the general quadratic polynomial is reduced to the ARTIN-SCHREIER polynomial \( T^2 + T + d \), and thereby to inverting the ARTIN-SCHREIER map \( K \rightarrow K \), \( x \mapsto x^2 + x \). Note that this map also is linear. However in general it is neither injective
nor surjective. Its kernel is the set of elements \( x \) with \( x^2 = x \), that is the prime field \( \mathbb{F}_2 \) inside of \( K \). The preimages \( u \) and \( u + 1 \) of a given element \( d \in K \) may be found in \( K \) or in a quadratic extension \( L = K(u) \) of \( K \). To get the roots of \( f \) we set \( d = \frac{ac}{b^2} \) and determine a preimage \( u \) of \( d \) under the Artin-Schreier map. Then a root of \( f \) is \( x = \frac{bu}{a} \); the other root is \( x + \frac{b}{a} \).

2 The case of a finite field

Now we consider the case where \( K \) is finite. Then \( K \) has \( 2^n \) elements for some \( n \), and coincides with the field \( \mathbb{F}_{2^n} \) up to isomorphism. The trace of an element \( x \in K \) is given by the formula
\[
\text{Tr}(x) = x + x^2 + \cdots + x^{2^{n-1}}.
\]
It is an element of the prime field \( \mathbb{F}_2 \), i.e., 0 or 1, and \( \text{Tr}(x^2) = \text{Tr}(x) \).

**Lemma 1** Let \( K \) be a finite field with \( 2^n \) elements. Then the polynomial \( g = T^2 + T + d \in K[T] \) has a root \( u \) in \( K \), if and only if \( \text{Tr}(d) = 0 \). In this case \( g = h(T + u) \) with \( h = T^2 + T \).

**Proof.** "\( \Rightarrow \)" If \( u \in K \), then \( \text{Tr}(d) = \text{Tr}(u^2) + \text{Tr}(u) = 0 \).

"\( \Leftarrow \)" For the converse let \( \text{Tr}(d) = 0 \). Then
\[
0 = \text{Tr}(d) = d + d^2 + \cdots + d^{2^{n-1}} = (u^2 + u) + (u^4 + u^2) + \cdots + (u^{2^n} + u^{2^n-1}) = u + u^{2^n},
\]
hence \( u^{2^n} = u \), and therefore \( u \in K \).

The addendum is trivial. ◊

**Remark** Let \( L \) be a quadratic extension of \( K \), and \( \tilde{\text{Tr}} : L \rightarrow \mathbb{F}_2 \) its trace function. Then \( L \cong \mathbb{F}_{2^{2n}} \) and
\[
\tilde{\text{Tr}}(x) = x + x^2 + \cdots + x^{2^{n-1}} + x^{2n} + \cdots + x^{2^{2n-1}}.
\]
For \( x \in K \) we have \( x^{2^n} = x \), hence \( \tilde{\text{Tr}}(x) = 0 \). This is consistent with the statement of the lemma that \( g = T^2 + T + d \in K[T] \) has a root in \( L \).

**Corollary 1** \( g = T^2 + T + d \in K[T] \) is irreducible, if and only if \( \text{Tr}(d) = 0 \). If this is the case, then \( g = h(T + r) \) with \( h = T^2 + T + e \), where \( e \) is an arbitrarily chosen element of \( K \) with Trace \( \text{Tr}(e) = 1 \), and \( r \in K \) is a solution of \( r^2 + r = d + e \).

**Proof.** \( g \) is irreducible in \( K[T] \), if and only if it has no root in \( K \). The addendum follows because \( d + e \) has trace 0, hence has the form \( r^2 + r \). ◊
Note 1. The lemma is a special case of Hilbert’s Theorem 90, additive form.

Note 2. The Artin-Schreier Theorem generalizes these results to arbitrary finite base fields $\mathbb{F}_q$ instead of $\mathbb{F}_2$, and to polynomials $T^q - T - d$. It characterizes the cyclic field extensions of degree $q$.

We have shown:

**Proposition 1 (Roots)** Let $K$ be a finite field of characteristic 2, and let $f = aT^2 + bT + c \in K[T]$ be a polynomial of degree 2. Then:

(i) $f$ has exactly one root in $K \iff b = 0$.

(ii) $f$ has exactly two roots in $K \iff b \neq 0$ and $\text{Tr}(ac) = 0$.

(iii) $f$ has no root in $K \iff b \neq 0$ and $\text{Tr}(ac) = 1$.

**Proposition 2 (Normal form)** Let $K$ be a finite field of characteristic 2, and $f = aT^2 + bT + c \in K[T]$ be a polynomial of degree 2 i.e. $a \neq 0$. Then there is a $k \in K^\times$ and an affine transformation $\alpha : K \rightarrow K$, $\alpha(x) = rx + s$ with $r \in K^\times$ and $s \in K$, such that

$$k \cdot f \circ \alpha = T^2, \quad T^2 + T, \quad \text{or} \quad T^2 + T + e,$$

where $e \in K$ is a fixed (but arbitrarily chosen) element of Trace $\text{Tr}(e) = 1$. In the case of odd $n = \dim K$ we may chose $e = 1$.

### 3 Examples

As we have seen the key to solving quadratic equations in characteristic 2 is solving systems of linear equations whose coefficient matrix is the matrix of the Artin-Schreier map, or the square map in the degenerate case. To explicitly solve quadratic equations over a finite field $K$ of characteristic 2 we first have to fix a basis of $K$ over $\mathbb{F}_2$. There are several options, and none of them is canonical. One option is to build a basis successively along a chain of intermediate fields between $\mathbb{F}_2$ and $K$.

For this we first consider a field extension $L$ of $K$ of degree 2. If $K$ has $2^n$ elements, then the cardinality of $L$ is $2^{2n}$, and we may construct $L$ from $K$ by adjoining a root $t$ of an irreducible degree 2 polynomial $T^2 + T + d \in K[T]$ where $\text{Tr}(d) = 1$, see Lemma 1. Then a basis of $L$ over $K$ is $\{1, t\}$, and if $\{u_1, \ldots, u_n\}$ is a basis of $K$ over $\mathbb{F}_2$, then $\{u_1, \ldots, u_n, tu_1, \ldots, tu_n\}$ is a basis of $L$ over $\mathbb{F}_2$.

Now the square map has the same effect on the $u_i$ in $L$ as in $K$, and

$$(tu_i)^2 = t^2 u_i^2 = (t + d)u_i^2 = t\cdot u_i^2 + d \cdot u_i^2.$$  

If we denote by $Q_n$ resp. $Q_{2n}$ the matrices of the square maps of $K$ or $L$ with respect to the chosen bases, then

$$Q_{2n} = \begin{pmatrix} Q_n & LdQ_n \\ 0 & Q_n \end{pmatrix},$$  

3
where $L_d$ is the matrix of the left multiplication by $d$ in $K$. The $Q_n$ in the right lower corner of the matrix comes from the fact that $t \cdot u_i^2 = t \cdot \sum q_{ij} u_j = \sum q_{ij} t u_j$ where the $q_{ij}$ are the matrix coefficients of $Q_n$.

Note that for odd $n$ we may choose $d = 1$, hence $L_d = 1_n$, the $n \times n$ unit matrix.

The matrix $A_n$ of the ARTIN-SCHREIER map is $1_n + Q_n$, this means that in $Q_n$ we simply have to complement the diagonal entries, i.e. interchange 0 and 1.

**The case $n = 1$**

Let us first consider the simplest case $K = \mathbb{F}_2$. Its $\mathbb{F}_2$-basis is $\{1\}$, and the matrices are the $1 \times 1$-matrices $Q_n = (1)$ and $A_n = (0)$. Solving quadratic equations is trivial.

**The case $n = 2$**

The field $\mathbb{F}_4$ is an extension of $\mathbb{F}_2$ of degree 2. An $\mathbb{F}_2$-basis is $\{1, t\}$ where $t^2 = t + 1$.

The general consideration above gives

$$Q_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}. $$

Solving quadratic equations (in the nondegenerate case) amounts to finding a preimage $x = (x_1, x_2)$ of $b = (b_1, b_2)$ in the 2-dimensional vectorspace $\mathbb{F}_2^2$ under $A_2$. This gives a system of 2 linear equations over $\mathbb{F}_2$:

$$\begin{pmatrix} x_2 \\ 0 \end{pmatrix} = A_2 \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}. $$

This is solvable if and only if $b_2 = 0$, and all (in fact two) solutions are

$x_1$ arbitrary (i.e. 0 or 1) and $x_2 = b_1$.

For later use we note that $\text{Tr}(t) = t + t^2 = 1$ and

$L_t = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$

**The case $n = 3$**

The field $\mathbb{F}_8$ has an $\mathbb{F}_2$-basis $\{1, s, s^2\}$ where $s^3 + s = 1$. The square map maps $1 \mapsto 1$, $s \mapsto s^2$, $s^2 \mapsto s^2 + s$. We have the matrices

$$Q_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}. $$

4
For preimages under the Artin-Schreier map we have the system of 3 linear equations
\[ A_3x = b, \]
or
\[
\begin{pmatrix}
0 \\
x_2 + x_3 \\
x_2
\end{pmatrix}
= 
\begin{pmatrix}
b_1 \\
b_2 \\
b_3
\end{pmatrix}.
\]
It has a solution if and only if \( b_1 = 0 \), and then its two solutions are
\[ x_1 \text{ arbitrary}, \quad x_2 = b_3, \quad x_3 = b_2 + b_3. \]

The case \( n = 4 \)

The field \( \mathbb{F}_{16} \) is an extension of \( \mathbb{F}_4 \) of degree 2 and has an \( \mathbb{F}_2 \)-basis \( \{1, t, u, tu\} \) where \( u^2 + u = t \). We have
\[
Q_4 = \begin{pmatrix} Q_2 & L_tQ_2 \\ 0 & Q_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.
\]
The system of 4 linear equations to solve becomes \( A_4x = b \), or
\[
\begin{pmatrix}
x_2 + x_4 \\
x_3 \\
x_4 \\
0
\end{pmatrix}
= 
\begin{pmatrix}
b_1 \\
b_2 \\
b_3 \\
b_4
\end{pmatrix}.
\]
It is solvable if and only if \( b_4 = 0 \), and then its two solutions are
\[ x_1 \text{ arbitrary}, \quad x_2 = b_1 + b_3, \quad x_3 = b_2, \quad x_4 = b_3. \]

For use with \( \mathbb{F}_{256} \) we note that \( \text{Tr}(tu) = 1 \) and
\[
L_{tu} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \quad L_{tu}Q_4 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}.
\]

The case \( n = 5 \)

The field \( \mathbb{F}_{32} \) has an \( \mathbb{F}_2 \)-basis \( \{1, t, t^2, t^3, t^4\} \) with \( t^5 = t^2 + 1 \). Squaring maps \( 1 \mapsto 1 \), \( t \mapsto t^2 \), \( t^2 \mapsto t^4 \), \( t^3 \mapsto t^3 + t \), \( t^4 \mapsto t^3 + t^2 + 1 \). Therefore
\[
Q_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}, \quad A_5 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.
\]
The system $A_5 x = b$ of 5 linear equations is
\[
\begin{pmatrix}
  x_5 \\
  x_2 + x_4 \\
  x_2 + x_3 + x_5 \\
  x_5 \\
  x_3 + x_5
\end{pmatrix} =
\begin{pmatrix}
  b_1 \\
  b_2 \\
  b_3 \\
  b_4 \\
  b_5
\end{pmatrix}.
\]
It has a solution if and only if $b_1 = b_4$, and then its two solutions are
\[
x_1 \text{ arbitrary}, \quad x_2 = b_3 + b_5, \quad x_3 = b_1 + b_5, \quad x_4 = b_2 + b_3 + b_5, \quad x_5 = b_1.
\]

The case $n = 6$

The field $\mathbb{F}_{64}$ is an extension of $\mathbb{F}_8$ of degree 2. Therefore—after choosing a suitable basis—we have
\[
Q_6 = \begin{pmatrix} Q_3 & Q_3 \\ 0 & Q_3 \end{pmatrix} = \begin{pmatrix}
  1 & 0 & 0 & 1 & 0 & 0 \\
  0 & 0 & 1 & 0 & 0 & 1 \\
  0 & 1 & 1 & 0 & 1 & 1 \\
  0 & 0 & 0 & 1 & 0 & 0 \\
  0 & 0 & 0 & 0 & 0 & 1 \\
  0 & 0 & 0 & 0 & 1 & 1
\end{pmatrix}, \quad A_6 = \begin{pmatrix}
  0 & 0 & 0 & 1 & 0 & 0 \\
  0 & 1 & 1 & 0 & 0 & 1 \\
  0 & 1 & 0 & 0 & 1 & 1 \\
  0 & 0 & 0 & 0 & 0 & 0 \\
  0 & 0 & 0 & 0 & 1 & 1 \\
  0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}.
\]

The system of 6 linear equations to solve becomes $A_6 x = b$, or
\[
\begin{pmatrix}
  x_4 \\
  x_2 + x_3 + x_6 \\
  x_2 + x_5 + x_6 \\
  0 \\
  x_3 + x_6 \\
  x_5
\end{pmatrix} =
\begin{pmatrix}
  b_1 \\
  b_2 \\
  b_3 \\
  b_4 \\
  b_5 \\
  b_6
\end{pmatrix}.
\]
It is solvable if and only if $b_4 = 0$, and then its two solutions are
\[
x_1 \text{ arbitrary}, \quad x_2 = b_3 + b_5, \quad x_3 = b_2 + b_3 + b_6, \quad x_4 = b_1, \quad x_5 = b_6, \quad x_6 = b_5 + b_6.
\]

The case $n = 8$

As a final example we consider $\mathbb{F}_{256}$, a quadratic extension of $\mathbb{F}_{16}$. It has a basis \{1, t, u, tu, v, tv, uv, tuv\} with $t$ and $u$ as in $\mathbb{F}_{16}$ and $v^2 = v + tu$. By the general principle
and knowing $L_{tu}$ we have

\[
Q_8 = \begin{pmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}, \quad
A_8 = \begin{pmatrix}
0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}.
\]

Solving for preimages of $A_8$ runs as before.