Matrices in $\mathbb{M}_2[\mathbb{F}_q[T]]$ with quadratic minimal polynomial.[×]

J.V. van Zyl[a,b,*]

[a] *Department of Mathematical Sciences, University of Stellenbosch, 7600 Stellenbosch, South Africa*
[b] *Department of Mathematics and Applied Mathematics, University of Pretoria, 0002 Pretoria, South Africa*

Abstract

By a result of Latimer and MacDuffee, there are a finite number of equivalence classes of $n \times n$ matrices over $\mathbb{F}_q[T]$ with minimum polynomial $p(X)$, where p is an n^{th} degree polynomial, irreducible over $\mathbb{F}_q[T]$. In this paper, we develop an algorithm for finding a canonical representative of each matrix class, for $p(X) = X^2 - \Gamma X - \Delta \in \mathbb{F}_q[T][X]$.

Keywords: ideal classes, matrix classes, Latimer-MacDuffee theorem
2010 MSC: 15B33
2010 MSC: 11T55

1. Introduction

Let $p(X) \in R[X]$ be a monic, irreducible polynomial of degree n over a principal ideal domain R. If $C \in \mathbb{M}_n[R]$ is a matrix solution to the equation $p(X) = 0$, then the solution set of this equation is exactly

$$\{S^{-1}CS \ : \ S \in \mathrm{GL}_n[R']\} \cap \mathbb{M}_n[R],$$

where R' is the field of fractions of R. For brevity, we will refer to matrices in this set simply as "solutions (to $p(X) = 0$)" if no confusion can arise.

Definition 1. *We call two solutions A and B* equivalent *if $B = S^{-1}AS$ for some $S \in GL_n[R]$.*

Latimer and MacDuffee showed in [1] that there is a bijection between equivalence classes of matrix solutions to $p(X) = 0$ and ideal classes of $R[\beta]$, where β is a root of $p(X)$ in the algebraic closure of R'.

[×] Declarations of interest: none

[*] Corresponding author. Tel.: +31 68 556 8775
Email address: jv.vanzyl@gmail.com (J.V. van Zyl)

Definition 2. *Two ideals* $\mathfrak{a}$ *and* $\mathfrak{b}$ *of* $R[\beta]$ *are equivalent if there exist* $a, b \in R$ *such that* $a\mathfrak{a} = b\mathfrak{b}$.

In their paper, Latimer and MacDuffee make the correspondence explicit, as follows: if A is a matrix solution to $p(X) = 0$, let $\mathbf{w}$ be an eigenvector of A corresponding to β; associate with A the ideal of $R[\beta]$ generated by the entries of $\mathbf{w}$. However, they don't provide a method for constructing representatives in each class. In [2], Behn and Van der Merwe give an algorithm for constructing representatives in the case when $p(X)$ is quadratic and $R = \mathbb{Z}$. It would be useful to have an algorithm for constructing representatives of each equivalence class of solutions for the case where $p(X)$ is quadratic and $R = \mathbb{F}_q[T]$: via the Latimer-MacDuffee correspondence, these give rise to representatives of ideal classes in a quadratic extension of $\mathbb{F}_q[T]$, which may be used to improve the results by Breuer in [3], section 3, on estimating the heights of CM-points of certain Drinfeld modules. In Breuer's paper, he uses the fact that ideal classes correspond to elements in a so-called *quadratic fundamental domain* (Definition 3.4 in the paper), but is limited by the fact that different elements in the quadratic fundamental domain may correspond to the same ideal class.

In this paper we develop such an algorithm for constructing representatives of matrix solutions to $p(X) = 0$ when $R = \mathbb{F}_q[T]$; conversion to representatives of ideal classes is made explicit in chapter 4 of [4]. When $p(X)$ is reducible, the methods in this paper break down; the neat result over the integers presented in [2] certainly does not translate to $\mathbb{F}_q[T]$, so we omit the reducible case in this paper.

2. Preliminaries

Let the polynomial $p(X) = X^2 - \Gamma X - \Delta \in \mathbb{F}_q[T][X]$ be irreducible. Note that if $p(X)$ is the minimal polynomial of a matrix A over $\mathbb{F}_q[T]$ and $k \in \mathbb{F}_q[T]$, then the polynomial $p(X + k)$ is the minimal polynomial of the matrix $B = A - kI_2$, where I_2 is the 2×2 identity matrix.

By replacing X with $X + k$ for some $k \in \mathbb{F}_q[T]$ if necessary, we may assume that the degree of Δ is minimal. Specifically, if $d = \min\{\deg(p(x)) \,|x \in \mathbb{F}_q[T]\}$, where $\deg(x)$ denotes the degree of x as a polynomial in T, and k is an element of $\mathbb{F}_q[T]$ for which this minimum is attained, we may replace $p(X)$ with $p(X+k)$ (in which case $\deg(\Delta) = d$). Further, by replacing X with $\operatorname{sgn}(\Gamma)X$ and dividing the equation $p(X) = 0$ through by $\operatorname{sgn}(\Gamma)^2$, we may assume that Γ is monic in T.

Remark. In odd characteristic, it is natural to transform the polynomial $p(X)$ by completing the square and eliminating Γ. Unfortunately, this leaves the characteristic 2 case with non-vanishing Γ to be solved by different means. It turns out that in even characteristic with $\Gamma = 0$, the largest odd integer d such that T^d occurs in Δ plays a crucial role and this observation motivated the transformation used in this paper, which works for all characteristics.

The polynomial $p(X)$ now has the following property:

Proposition 1. *Let $p(X) = X^2 - \Gamma X - \Delta$ be an irreducible polynomial over $\mathbb{F}_q[T]$ such that Γ is monic in T and $\deg(p(x)) \geq \deg(\Delta)$ for all $x \in \mathbb{F}_q[T]$. If $\deg(\Gamma) = g$ and $\deg(\Delta) = d$, then one of the following holds:*

- *$d > 2g$ and d is odd;*
- *$d > 2g$, d is even and $\operatorname{sgn}(\Delta)$ is not a square in $\mathbb{F}_q$;*
- *$d = 2g$ and $\operatorname{sgn}(\Delta)$ is not of the form $\alpha^2 - \alpha$ for some $\alpha \in \mathbb{F}_q$, or*
- *$d < g$.*

Proof. We prove the contrapositive of the proposition by making use of the following observation: if $\deg(x^2 - \Gamma x) = d$ and $\operatorname{sgn}(x^2 - \Gamma x) = \operatorname{sgn}(\Delta)$, then $\deg(p(x)) < d$, contradicting that $\deg(\Delta)$ is minimal. We consider several cases:

- Suppose that $d > 2g$, $d = 2D$ is even and $\operatorname{sgn}(\Delta) = \alpha^2$ for some $\alpha \in \mathbb{F}_q^\times$. Set $x = \alpha T^D$. Then $\deg(x^2) = 2D > g + D = \deg(\Gamma x)$ and so $\deg(x^2 - \Gamma x) = 2D = d$ and $\operatorname{sgn}(x^2 - \Gamma x) = \operatorname{sgn}(x)^2 = \alpha^2 = \operatorname{sgn}(\Delta)$.
- Suppose that $d = 2g$ and $\operatorname{sgn}(\Delta) = \alpha^2 - \alpha$ for some $\alpha \in \mathbb{F}_q$. Set $x = \alpha T^g$. Then $\deg(x^2) = d = \deg(\Gamma x)$, so $\deg(x^2 - \Gamma x) = d$ (since $\alpha^2 - \alpha \neq 0$) and $\operatorname{sgn}(x^2 - \Gamma x) = \operatorname{sgn}(x)^2 - \operatorname{sgn}(x) = \alpha^2 - \alpha = \operatorname{sgn}(\Delta)$.
- Suppose that $g \leq d < 2g$ and set $x = -\operatorname{sgn}(\Delta) T^{d-g}$. Then we have that $\deg(x^2) = 2d - 2g < d = \deg(\Gamma x)$, hence $\deg(x^2 - \Gamma x) = d$ and $\operatorname{sgn}(x^2 - \Gamma x) = -\operatorname{sgn}(x) = \operatorname{sgn}(\Delta)$.

□

Let $\deg(\Gamma) = g$ and $\deg(\Delta) = d$ for the remainder of the article. We will consider the 2×2 matrices over $\mathbb{F}_q[T]$ which satisfy the equation

$$X^2 - \Gamma X - \Delta = 0. \tag{1}$$

In section 3 we'll introduce the concept of a reduced matrix to limit the matrix solutions of (1) that we need to consider to a finite set. However, not all these matrices necessarily give rise to different solution classes (akin to how different elements in the quadratic fundamental domain in [3] may correspond to the same ideal class) and in section 4 we develop a method for grouping these matrices into distinct equivalence classes.

3. Reduced matrices

Every matrix solution to (1) has the form $\begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$ with $\Delta = b^2 - \Gamma b - ac$, $ac \neq 0$.

Definition 3. *A matrix solution* $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$ *to* (1) *is said to be* reduced *if* $\deg(b) < \deg(a) < \max\{\frac{1}{2}d, g\}$*, and is said to be* almost reduced *if* $\deg(b) < \deg(a) = \max\{\frac{1}{2}d, g\}$.

In a reduced matrix, the degrees of a and b are bounded from above, and the field of coefficients $\mathbb{F}_q$ is finite. Also, given a and b, c is uniquely determined from $b^2 - \Gamma b - \Delta = ac$, so there is only a finite number of reduced matrices.

We have the following:

Proposition 2. *Every matrix solution to* (1) *is equivalent to a reduced matrix or an almost reduced matrix.*

Proof. We use the following algorithm to reduce a matrix $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$.

Step 1. If $\deg(b) \geq \deg(a)$, write $b = aq + r$ in the unique way such that $q,\ r \in \mathbb{F}_q[T]$ and $\deg(r) < \deg(a)$. Replace A with the equivalent matrix

$$\begin{bmatrix} 1 & -q \\ 0 & 1 \end{bmatrix} A \begin{bmatrix} 1 & q \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} r & -c' \\ a & \Gamma - r \end{bmatrix}$$

where $c' = -aq^2 + (\Gamma - 2r)q + c$.

Step 2. If $\deg(a) > \max\{\frac{1}{2}d, g\}$, replace A with the equivalent matrix

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} A \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \Gamma - b & -a \\ c & b \end{bmatrix},$$

and go back to step 1.

If this algorithm terminates, the resulting matrix will be reduced or almost reduced, by construction. It remains to show that the algorithm always terminates.

If, after performing step 1, the algorithm doesn't terminate, it means that $\deg(b) < \deg(a)$ and $\deg(a) > \max\{\frac{1}{2}d, g\}$ and step 2 has to be performed. In this case, since $ac = b^2 - \Gamma b - \Delta$, we have

$$\begin{aligned}
& \deg(c) \\
= \ & \deg(b^2 - \Gamma b - \Delta) - \deg(a) \\
\leq \ & \max\{2\deg(b), g + \deg(b), d\} - \deg(a) \\
= \ & \max\{\deg(b) - [\deg(a) - \deg(b)], g - [\deg(a) - \deg(b)], d - \deg(a)\} \\
< \ & \max\{\deg(b), g, \tfrac{1}{2}d\} \\
< \ & \deg(a).
\end{aligned}$$

Thus, performing step 2 strictly decreases the degree of a. Since step 1 leaves the degree if a unchanged, it means that step 2 can only be performed a finite number of times, and so the process terminates. □

Proposition 2 shows that there are only a finite number of equivalence classes of matrix solutions to (1).

Note that if $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$ is reduced and $d \geq 2g$ (that is to say, $\deg(b) < \deg(a) < \frac{1}{2}d$), then

$$\begin{aligned} \deg(c) &= \deg(b^2 - \Gamma b - \Delta) - \deg(a) \\ &= d - \deg(a) \\ &> \tfrac{1}{2}d, \end{aligned}$$

hence $\deg(a) < \frac{1}{2}d < \deg(c)$ and $\deg(a) + \deg(c) = d$.

Similarly, if $d < g$, then $\deg(b) < \deg(a) < g$ and so

$$\begin{aligned} & \deg(c) \\ = \ & \deg(b^2 - \Gamma b - \Delta) - \deg(a) \\ = \ & \deg(\Gamma b) - \deg(a) \quad (\text{since } \deg(b^2), \deg(\Delta) < g + \deg(b) = \deg(\Gamma b)) \\ = \ & g - [\deg(a) - \deg(b)] \\ < \ & g. \end{aligned}$$

Hence $\deg(c) < g$ in this case, but $\deg(a) < \deg(c)$ does not necessarily hold.

Also note that in this case, if $\deg(a)$, $\deg(b)$, $\deg(c) < g$, then the matrix is automatically reduced. Indeed, the above equations show that

$$\deg(a) + \deg(c) = \deg(b^2 - \Gamma b - \Delta) = g + \deg(b).$$

Hence $\deg(b) = \deg(a) + \deg(c) - g < \min\{\deg(a), \deg(c)\}$ since both $\deg(a)$ and $\deg(c)$ are less than g.

Example. Let's reduce the matrix

$$A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix} = \begin{bmatrix} T^3 + 3T^2 + 4T & T^4 + 2T^3 + 3T + 4 \\ 4T^2 + 2T + 2 & 4T^3 + 3T^2 + T + 1 \end{bmatrix},$$

which is a solution to (1) over $\mathbb{F}_5[T]$, with $\Gamma = T^2 + 1$ and $\Delta = 3$ (hence $g = 2$ and $d = 0$). We see that $\deg(b) > \deg(a)$, so we apply step 1: write

$$b = T^3 + 3T^2 + 4T = (4T)(4T^2 + 2T + 2) + T,$$

so $q = 4T$ and $r = T$ and hence

$$c' = -(4T^2 + 2T + 2)(4T)^2 + (T^2 + 1 - 2T) - (T^4 + 2T^3 + 3T + 4) = T + 1.$$

Thus A is equivalent to

$$A' = \begin{bmatrix} r & -c' \\ a & \Gamma - r \end{bmatrix} = \begin{bmatrix} T & 4T + 4 \\ 4T^2 + 2T + 2 & T^2 + 4T + 1 \end{bmatrix}.$$

This matrix satisfies $\deg(b) < \deg(a) = \max\{g, \frac{1}{2}d\}$ and hence is almost reduced, terminating the algorithm.

Note, however, that $\deg(c') < \deg(a)$ and so we can reduce $\deg(a)$ by applying step 2 of the algorithm again; we see that A' is equivalent to $\begin{bmatrix} T^2+4T+1 & T^2+3T+3 \\ T+1 & T \end{bmatrix}$ and writing

$$T^2 + 4T + 1 = (T+1)(T+3) + 3$$

and applying step 1, this matrix reduces to $\begin{bmatrix} 3 & 3T+2 \\ T+1 & T^2+3 \end{bmatrix}$, which is reduced.

In this case the resulting degrees of a and c are equal, so let's see what happens if we apply step 2 again and reducing: we obtain the matrix $\begin{bmatrix} T^2+3 & 4T+4 \\ 2T+3 & 3 \end{bmatrix}$, and applying step 1 again, with $T^2 + 3 = (2T+3)(3T+3) + 4$, we obtain $\begin{bmatrix} 4 & 2T+2 \\ 2T+3 & T^2+2 \end{bmatrix}$, which is also reduced.

This illustrates that reduced and almost reduced matrices may be equivalent to each other, which we will now investigate.

4. Equivalence of (almost) reduced matrices

For this section, let

$$\begin{bmatrix} b' & -c' \\ a' & \Gamma - b' \end{bmatrix} = \begin{bmatrix} x & w \\ y & z \end{bmatrix}^{-1} \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix} \begin{bmatrix} x & w \\ y & z \end{bmatrix},$$

where matrices $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$ and $A' = \begin{bmatrix} b' & -c' \\ a' & \Gamma - b' \end{bmatrix}$ are almost reduced, with $\deg(a') \leq \deg(a)$, and $\begin{bmatrix} x & w \\ y & z \end{bmatrix} \in \mathrm{SL}_2[\mathbb{F}_q[T]]$. Multiplying out the right hand side, we get

$$\begin{aligned} a' &= ax^2 + (\Gamma - 2b)xy + cy^2, && (2) \\ b' &= b - (awx + (\Gamma - 2b)wy + cyz), && (3) \\ c' &= aw^2 + (\Gamma - 2b)wz + cz^2. && (4) \end{aligned}$$

If $\alpha \in \mathbb{F}_q^\times$, then

$$\begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix}^{-1} \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix} \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix} = \begin{bmatrix} b & -\alpha^{-2}c \\ \alpha^2 a & \Gamma - b \end{bmatrix},$$

so for simplicity, we will consider a and a' to be equal if they are equal modulo $(\mathbb{F}_q^\times)^2$ (that is, we consider the matrix $S = \begin{bmatrix} x & w \\ y & z \end{bmatrix}$ to be an element of $\mathrm{PSL}_2[\mathbb{F}_q[T]]$, the projective special linear group).

If $y = 0$, then $a' = ax^2$ which forces $x \in \mathbb{F}_q^\times$ and $\deg(a') = \deg(a)$. Then, if $w \neq 0$, we have that $\deg(b') = \deg(b - awx) = \deg(awx) \geq \deg(a) = \deg(a')$, contradicting that A' is reduced. Hence $w = 0$ and so $A' = A$. In the sequel we may assume that $y \neq 0$. We will treat the four cases in Proposition 1 separately.

4.1. Case: d is odd and $d > 2g$.

From the remarks following the proof of Proposition 2 it follows that in this case, $\deg(b) < \deg(a) \leq \frac{1}{2}d \leq \deg(c)$ and in fact, all three inequalities are strict since d is odd. Note also that

$$\deg(\Gamma - 2b) \leq \max\{g, \deg(b)\} \leq \max\{g, \deg(a)\} < \tfrac{1}{2}d.$$

Since we are assuming that $y \neq 0$, $\deg(cy^2) \geq \deg(c) > \deg(a) \geq \deg(a')$. If $\deg(x) \leq \deg(y)$, then $\deg(ax^2) < \deg(cy^2)$ and

$$\deg((\Gamma - 2b)xy) < \tfrac{1}{2}d + \deg(x) + \deg(y) \leq \tfrac{1}{2}d + 2\deg(y) < \deg(cy^2)$$

which leads to $\deg(a') = \deg(cy^2) > \deg(a)$, a contradiction. Thus we conclude that $\deg(x) > \deg(y)$.

To obtain equality in (2), at least two terms on the right hand side must have equal degree. However, since d is odd and $\deg(a) + \deg(c) = d$, we have that $\deg(ax^2)$ and $\deg(cy^2)$ have opposite parity. This means that we have one of the following situations:

$$\begin{aligned} \deg(ax^2) &= \deg((\Gamma - 2b)xy) > \deg(cy^2) \quad \text{or} \\ \deg(ax^2) &< \deg((\Gamma - 2b)xy) = \deg(cy^2). \end{aligned}$$

The former leads to

$$\deg(\Gamma - 2b) - \deg(a) = \deg(x) - \deg(y) > \deg(c) - \deg(\Gamma - 2b),$$

which implies $\deg(\Gamma - 2b) > \frac{1}{2}d$ (since $\deg(a) + \deg(c) = d$), a contradiction. The latter leads to

$$\deg(c) - \deg(\Gamma - 2b) = \deg(x) - \deg(y) < \deg(\Gamma - 2b) - \deg(a),$$

which also implies $\deg(\Gamma - 2b) > \frac{1}{2}d$. We conclude that in this case, no two reduced matrices are equivalent. Together with Proposition 2, this gives us

Theorem 1. *If $\deg(\Delta)$ is odd and $\deg(\Delta) > 2\deg(\Gamma)$, then every matrix solution to (1) is equivalent to a unique reduced matrix.*

4.2. Case: d is even, $d > 2g$ and $\operatorname{sgn}(\Delta)$ is not a square in $\mathbb{F}_q$.

As in the previous section, we have that $\deg(b) < \deg(a) \leq \frac{1}{2}d \leq \deg(c)$ and $\deg(\Gamma - 2b) < \frac{1}{2}d$. We first assume that $\deg(a) < \deg(c)$ (that is, the matrix A is reduced) or that $\deg(x) > 0$. As before, to obtain equality in (2), at least two terms on the right hand side must have equal degree. If $\deg(ax^2) = \deg((\Gamma - 2b)xy)$, then $\deg(y) = \deg(a) + \deg(x) - \deg(\Gamma - 2b)$ and so

$$\begin{aligned} \deg(cy^2) &= \deg(c) + \deg(y) + (\deg(a) + \deg(x) - \deg(\Gamma - 2b)) \\ &= \deg(x) + \deg(y) + d - \deg(\Gamma - 2b) \\ &> \deg(x) + \deg(y) + \deg(\Gamma - 2b) \\ &= \deg((\Gamma - 2b)xy), \end{aligned}$$

a contradiction.

Similarly, $\deg(cy^2) = \deg((\Gamma - 2b)xy)$ leads to $\deg(ax^2) > \deg((\Gamma - 2b)xy)$. Hence we must have that $\deg(ax^2) = \deg(cy^2) > \deg((\Gamma - 2b)xy)$ and that $\operatorname{sgn}(ax^2) + \operatorname{sgn}(cy^2) = 0$ which is equivalent to $\operatorname{sgn}(ac) = -(\frac{\operatorname{sgn}(ax)}{\operatorname{sgn}(y)})^2$. However, from the equation $ac = b^2 - \Gamma b - \Delta$ and $d > 2g$, we see that $\operatorname{sgn}(ac) = -\operatorname{sgn}(\Delta)$, which then implies that $\operatorname{sgn}(\Delta) = (\frac{\operatorname{sgn}(ax)}{\operatorname{sgn}(y)})^2$, contradicting that $\operatorname{sgn}(\Delta)$ is not a square in $\mathbb{F}_q$. This shows that no reduced matrix is equivalent to another reduced matrix, or an almost reduced matrix.

The case when $\deg(a) = \deg(c) = \frac{1}{2}d$ (that is, A is almost reduced) and $x \in \mathbb{F}_q$ remains. In this case $y \in \mathbb{F}_q$ is forced. Equation (4) now shows, using a similar argument as above, that $w, z \in \mathbb{F}_q$. From this, w and z are uniquely determined. Indeed, equations (2) and (3) imply $b'x + a'w = bx - cy$ and so $w = \frac{-\operatorname{sgn}(c)y}{\operatorname{sgn}(a')}$ (since $\deg(bx - b'x) < \deg(c)$). Using (2), this simplifies to

$$w = \frac{\operatorname{sgn}(\Delta)y}{(\operatorname{sgn}(a)x)^2 - \operatorname{sgn}(\Delta)y^2}$$

and $z = \frac{1+wy}{x} = \frac{\operatorname{sgn}(a)^2 x}{(\operatorname{sgn}(a)x)^2 - \operatorname{sgn}(\Delta)y^2}$ now follows from $xz - wy = 1$. (Note that w is well-defined since $(\operatorname{sgn}(a)x)^2 - \operatorname{sgn}(\Delta)y^2 \neq 0$ unless $x = y = 0$.)

Therefore, there are $q^2 - 1$ matrices S such that $S^{-1}AS$ is again almost reduced, namely

$$S \in \left\{ \begin{bmatrix} x & \frac{\operatorname{sgn}(\Delta)y}{\tau} \\ y & \frac{\operatorname{sgn}(a)^2 x}{\tau} \end{bmatrix} : \quad (x,y) \in \mathbb{F}_q \times \mathbb{F}_q - (0,0),\ \tau = (\operatorname{sgn}(a)x)^2 - \operatorname{sgn}(\Delta)y^2 \right\}.$$

Not all of them result in distinct matrices, however. Since we are considering equations modulo $(\mathbb{F}_q^2)^\times$, we may mod out the action of this set of q^2-1 matrices by the set of $q-1$ matrices of the form $\begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix}$ which leaves us with $\frac{q^2-1}{q-1} = q+1$ possibilities. We now investigate when these $q+1$ possible matrices $S^{-1}AS$ are not distinct. It suffices to find S for which $S^{-1}AS = A$ and $y \neq 0$.

Now, if $S^{-1}AS = A$, then $x \times (4) + w \times (3)$ yields

$$(\Gamma - 2b)w + c(z - x) = 0.$$

Since $\deg(\Gamma - 2b) = g < \frac{d}{2} = \deg(c)$, we find that $x = z$ and $(\Gamma - 2b)w = 0$. Since we're assuming that $y \neq 0$, it follows that $w \neq 0$ and $\Gamma = 2b$. Substituting this back into (2), we find that $c = \frac{1-x^2}{y^2}a$. But then we have (noting that since $\deg(\Delta)$ is even, the characteristic is necessarily odd)

$$\Delta = b^2 - \Gamma b - ac = -\frac{1}{4}\Gamma^2 + \frac{x^2 - 1}{y^2}a^2,$$

and so

$$\Gamma^2 + 4\Delta = (x^2 - 1)\left(\frac{2a}{y}\right)^2.$$

So x^2-1 must be non-square (since $p(X)$ is irreducible), and also, since $\operatorname{sgn}(c) = -\frac{\operatorname{sgn}(\Delta)}{\operatorname{sgn}(a)}$, we see that $\frac{x^2-1}{y^2} = \frac{\operatorname{sgn}(\Delta)}{\operatorname{sgn}(a)^2}$.

Thus, A is of the form $\begin{bmatrix} \frac{1}{2}\Gamma & \frac{\operatorname{sgn}(\Delta)}{\operatorname{sgn}(a)^2}a \\ a & \frac{1}{2}\Gamma \end{bmatrix}$. Substituting back into equations (2)-(4), we find that any almost reduced matrix equivalent to A must take the form $\begin{bmatrix} \frac{1}{2}\Gamma & \frac{\operatorname{sgn}(\Delta)}{\beta\operatorname{sgn}(a)^2}a \\ \beta a & \frac{1}{2}\Gamma \end{bmatrix}$, where $\beta \in \mathbb{F}_q^\times$. Hence the only almost reduced matrices equivalent to A are A itself and $\begin{bmatrix} \frac{1}{2}\Gamma & \frac{a}{\operatorname{sgn}(a)^2} \\ \operatorname{sgn}(\Delta)a & \frac{1}{2}\Gamma \end{bmatrix}$

4.3. Case: $d = 2g$ and $\operatorname{sgn}(\Delta)$ is not of the form $\alpha^2 - \alpha$, $\alpha \in \mathbb{F}_q$.

A similar argument as in the previous section shows that no two reduced matrices are equivalent, and an almost identical argument shows that there are $q+1$ almost reduced matrices equivalent to any given almost reduced matrix, unless the matrix is of the form $\begin{bmatrix} b & \frac{\operatorname{sgn}(\Delta)}{\operatorname{sgn}(a)^2}a \\ a & b + \frac{a}{\operatorname{sgn}(a)} \end{bmatrix}$. In this case the only almost reduced matrices equivalent to A are A itself and $\begin{bmatrix} b & \frac{\operatorname{sgn}(\Delta)}{\tau\operatorname{sgn}(a)^2}a \\ \tau a & b + \frac{a}{\operatorname{sgn}(a)} \end{bmatrix}$, where τ is a non-square element of $\mathbb{F}_q$.

The above arguments, together with Proposition 2 give us

Theorem 2. *If $\deg(\Delta)$ is even, and either $\deg(\Delta) > 2\deg(\Gamma)$ and $\operatorname{sgn}(\Delta)$ is not a square in $\mathbb{F}_q$, or $\deg(\Delta) = 2\deg(\Gamma)$ and $\operatorname{sgn}(\Delta)$ is not of the form $\alpha^2 - \alpha$, $\alpha \in \mathbb{F}_q$, then every matrix solution to (1) is either equivalent to a unique reduced matrix, or to a set of $q+1$ equivalent almost reduced matrices, except when said solution takes one of the following forms:*

- $\begin{bmatrix} \frac{1}{2}\Gamma & \frac{\operatorname{sgn}(\Delta)}{\operatorname{sgn}(a)^2}a \\ a & \frac{1}{2}\Gamma \end{bmatrix}$ *if $\deg(\Delta) > 2\deg(\Gamma)$, or*
- $\begin{bmatrix} b & \frac{\operatorname{sgn}(\Delta)}{\operatorname{sgn}(a)^2}a \\ a & b + \frac{a}{\operatorname{sgn}(a)} \end{bmatrix}$ *if $\deg(\Delta) = 2\deg(\Gamma)$.*

4.4. Case: $d < g$.

First note that if A is an almost reduced matrix, then adapting the remarks following the proof of Proposition 2 we can show that $\deg(c) < \deg(b) < g$. Applying Step 2 of Proposition 2 to the matrix A will yield a reduced matrix equivalent to A (as we noticed in the example following Proposition 2), so we may disregard almost reduced matrices in this section.

To determine which reduced matrices are equivalent, we need to determine when the expression $ax^2 + (\Gamma - 2b)xy + cy^2$ has degree less than g. We first look at this expression when $y = 1$.

Proposition 3. *If* $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$ *is a reduced matrix solution to* (1)*, then the expression* $ax^2 + (\Gamma - 2b)x + c$ *has degree less than* g *for exactly two distinct values of* x*.*

Proof. Since $\deg(c) < g$, a necessary and sufficient condition for the degree of $ax^2 + (\Gamma - 2b)x + c$ to be less than g is $\deg(ax^2 + (\Gamma - 2b)x) < g$. So we need to find x such that $x(ax + \Gamma - 2b)$ has degree less than g. One solution is clearly $x = 0$, so suppose that $x \neq 0$.

In this case, we must have that $\deg(ax) = \deg(\Gamma - 2b) = g$ and so $\deg(x) = g - \deg(a)$. If we let $r = ax + \Gamma - 2b$, it follows that we need $\deg(xr) < g$, i.e. $\deg(r) < g - \deg(x) = \deg(a)$. But since $\deg(a) < g = \deg(\Gamma - 2b)$, there exist unique non-zero x and r with $\deg(r) < \deg(a)$ such that $\Gamma - 2b = -ax + r$. □

We now define a mapping on the (finite) set of reduced matrices.

Define the mapping ϕ to map the reduced matrix $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$ to the matrix $S^{-1}AS$, where $S = \begin{bmatrix} x & -1 \\ 1 & 0 \end{bmatrix}$ and x is the unique non-zero polynomial from Proposition 3. Using the same notation as in Proposition 3, we have

$$\phi(A) = \begin{bmatrix} \Gamma - b + ax & -a \\ ax^2 + (\Gamma - 2b)x + c & b - ax \end{bmatrix} = \begin{bmatrix} b + r & -a \\ rx + c & \Gamma - b - r \end{bmatrix}.$$

I claim that this matrix is reduced. Indeed, we have that $\deg(a) < g$ and by construction, $\deg(ax^2 + (\Gamma - 2b)x + c) < g$. The remarks following the proof of Proposition 2, together with

$$\deg(b + r) \leq \max\{\deg(b), \deg(r)\} < \deg(a) < g$$

now implies that the matrix is reduced.

We now show that the mapping is injective. Suppose that there is a matrix B such that $\phi(B) = \phi(A)$. If $\phi(B) = R^{-1}BR$ with $R = \begin{bmatrix} y & -1 \\ 1 & 0 \end{bmatrix}$, then it follows that

$$B = RS^{-1}ASR^{-1} = \begin{bmatrix} b + ay - ax & -C \\ a & \Gamma - b - ay + ax \end{bmatrix}$$

for some C. Since B is recuced, it follows that $\deg(b + ay - ax) < \deg(a)$ which is only possible if $x = y$, in which case $A = B$. This shows that ϕ is an injective mapping on the finite set of reduced matrices, hence bijective. The inverse of ϕ is the mapping which sends $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$ to the matrix $S^{-1}AS$ where $S = \begin{bmatrix} 0 & -1 \\ 1 & x' \end{bmatrix}$ and x' is the unique non-zero polynomial such that $\deg(\Gamma - 2b - cx') < \deg(c)$.

Since ϕ is injective, it induces a permutation on the set of reduced matrices. Writing the permutation in disjoint cycle notation, we see that all the matrices

in each cycle are equivalent. It remains to show that all equivalent reduced matrices lie in the same cycle.

Theorem 3. *Two reduced matrix solutions to* (1) *are equivalent if and only if* $B = \phi^k(A)$ *for some integer* k.

Proof. Let $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix}$, $B = \begin{bmatrix} b' & -c' \\ a' & \Gamma - b' \end{bmatrix}$ and let S be a matrix $\begin{bmatrix} x & w \\ y & z \end{bmatrix}$ with $xz - wy = 1$ such that $B = S^{-1}AS$. First assume that $\deg(y) \leq \deg(x)$. As before, $y = 0$ quickly leads to $A = B$ (that is, $k = 0$), so we may assume that $y \neq 0$.

We wish to apply ϕ to the matrix A. Hence we need to find a non-zero polynomial X such that $\deg(aX^2 + (\Gamma - 2b)X + c) < g$. Since $\deg(y) \leq \deg(x)$, we can write $x = x_1 y - Y_1$ with $\deg(Y_1) < \deg(y)$ and x_1 non-zero. We claim that $X = x_1$ will suffice. Indeed,

$$\begin{aligned} & ax_1^2 + (\Gamma - 2b)x_1 + c \\ = \; & a\left(\frac{x + Y_1}{y}\right)^2 + (\Gamma - 2b)\left(\frac{x + Y_1}{y}\right) + c \\ = \; & \frac{1}{y^2}\left[ax^2 + (\Gamma - 2b)xy + cy^2 + 2axY_1 + (\Gamma - 2b)yY_1 + aY_1^2\right] \\ = \; & \frac{1}{y^2}\left[a' + 2axY_1 + (\Gamma - 2b)yY_1 + aY_1^2\right]. \end{aligned}$$

Since $\deg(Y_1) < \deg(y)$ and $\deg(a) < \deg(\Gamma - 2b) = g$, we have that

$$\begin{aligned} & \deg(ax_1^2 + (\Gamma - 2b)x_1 + c) \\ \leq \; & \max\{\deg(a'), \deg(aY_1^2), \deg((\Gamma - 2b)yY_1), \deg(axY_1)\} - 2\deg(y) \\ < \; & \max\{g, g + 2\deg(y), g + 2\deg(y), \deg(ax) + \deg(y)\} - 2\deg(y) \\ = \; & \max\{g, \deg(a) + \deg(x) - \deg(y)\}. \end{aligned}$$

Now, since $\deg(y) \leq \deg(x)$ and $\deg(c) < g = \deg(\Gamma - 2b)$, we have that $\deg(cy^2) < \deg((\Gamma - 2b)xy)$. On the other hand, $ax^2 + (\Gamma - 2b)xy + cy^2$ has degree less than g, so we must have that $\deg(ax^2) = \deg((\Gamma - 2b)xy)$ which leads to $\deg(a) + \deg(x) - \deg(y) = \deg(\Gamma - 2b) = g$ which shows that $\deg(ax_1^2 + (\Gamma - 2b)x_1 + c) < g$.

Applying ϕ to A, we find that $B = S_1^{-1}\phi(A)S_1$, where

$$S_1 = \begin{bmatrix} x_1 & -1 \\ 1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} x & w \\ y & z \end{bmatrix} = \begin{bmatrix} y & z \\ x_1 y - x & x_1 z - w \end{bmatrix} = \begin{bmatrix} X_1 & W_1 \\ Y_1 & Z_1 \end{bmatrix}.$$

Note that $\deg(Y_1) < \deg(y) = \deg(X_1)$, so we may repeat the above process. After a finite number of steps, we obtain $B = S_k^{-1}\phi^k(A)S_k$ with $S_k = \begin{bmatrix} X_k & W_k \\ 0 & Z_k \end{bmatrix}$, which, as before, implies that $\phi^k(A) = B$.

If $\deg(y) > \deg(x)$ but $\deg(y) \leq \deg(z)$, we may exchange the roles of A and B in the above argument. If $\deg(y) > \deg(x)$ and $\deg(y) > \deg(z)$, then apply ϕ^{-1} to A: $\phi^{-1}(A) = \begin{bmatrix} 0 & -1 \\ 1 & q \end{bmatrix}^{-1} A \begin{bmatrix} 0 & -1 \\ 1 & q \end{bmatrix}$. This leads to

$$B = S^{-1}AS = \begin{bmatrix} x & w \\ y & z \end{bmatrix}^{-1} \begin{bmatrix} 0 & -1 \\ 1 & q \end{bmatrix} \phi^{-1}(A) \begin{bmatrix} 0 & -1 \\ 1 & q \end{bmatrix}^{-1} \begin{bmatrix} x & w \\ y & z \end{bmatrix} = S_0^{-1}\phi^{-1}(A)S_0$$

where

$$S_0 = \begin{bmatrix} 0 & -1 \\ 1 & q \end{bmatrix}^{-1} \begin{bmatrix} x & w \\ y & z \end{bmatrix} = \begin{bmatrix} qx+y & qw+z \\ -x & -w \end{bmatrix}.$$

Now $\deg(-x) < \deg(qx+y)$, so we may apply the above argument (which then in fact shows that $\deg(y)$ must have been at most $\deg(x)$ to begin with, or that $x = 0$). □

To summarize, we have

Theorem 4. *If* $\deg(\Delta) < \deg(\Gamma)$*, then every matrix solution to* (1) *is equivalent to the reduced matrices in a unique orbit of* ϕ*.*

Remark. Theorems 1 and 2 are analogous to the positive definite case in [2] (Theorem 3.3); the extra case here is due to the fact that there is a not a unique monic polynomial with given degree, while there *is* a unique positive integer with a given absolute value (making the concept of an almost reduced matrix unnecessary over the integers). Theorem 4 is analogous to the negative definite case in [2] (Theorem 4.3).

As mentioned earlier, it is natural to transform the polynomial $p(X)$ to the form $p(X) = X^2 - \Delta$, when the characteristic is odd, by completing the square rather than minimizing the degree of Δ as we have done here. If we rework the results in this paper for this form of $p(X)$, the parallels with [2] are much more obvious. Indeed, the cases we need to consider when $p(X) = X^2 - \Delta$ are:

- $\deg(\Delta)$ is odd,
- $\deg(\Delta)$ is even with non-square $\operatorname{sgn}(\Delta)$,
- $\deg(\Delta)$ is even with square $\operatorname{sgn}(\Delta)$,

with Δ playing a role analogous to the discriminant Δ in [2], the first two cases analogous to the positive definite case and the third case analogous to the negative definite case.

Example. Let's return to the $\mathbb{F}_5[T]$ example following Proposition 2, starting with the reduced matrix $A = \begin{bmatrix} b & -c \\ a & \Gamma - b \end{bmatrix} = \begin{bmatrix} 3 & 3T+2 \\ T+1 & T^2+3 \end{bmatrix}$ with $\Gamma = T^2 + 1$ and $\Delta = 3$. We have $\deg(\Delta) < \deg(\Gamma)$, so let's compute the orbit of A under ϕ.

To apply ϕ to A, we need to find the polynomial x from Proposition 3 such that the degree of $ax^2 + (\Gamma - 2b)x + c$ is less than g: we write

$$\Gamma - 2b = T^2 + 1 - 2(3) = T^2 = (T+1)(T+4) + 1 = -(T+1)(4T+1) + 1 = -ax + r,$$

and so $x = 4T + 1$ and $rx + c = (1)(4T + 1) + (2T + 3) = T + 4$. Hence

$$\phi(A) = \begin{bmatrix} b + r & -a \\ rx + c & \Gamma - b - r \end{bmatrix} = \begin{bmatrix} 4 & 4T + 4 \\ T + 4 & T^2 + 2 \end{bmatrix}.$$

Repeating the process, we write $(T^2+1) - 2(4) = T^2 + 3 = -(T+4)(4T+4) + 4$ and so $\phi^2(A) = \begin{bmatrix} 3 & 4T + 1 \\ 2T + 2 & T^2 + 3 \end{bmatrix}$, and similarly

$$\phi^3(A) = \begin{bmatrix} 4 & 3T + 3 \\ 3T + 2 & T^2 + 2 \end{bmatrix}, \quad \phi^4(A) = \begin{bmatrix} 3 & 2T + 3 \\ 4T + 4 & T^2 + 3 \end{bmatrix}.$$

Recall from the comment following equation 4 that we identify reduced matrices equivalent to each other via a matrix of the form $S = \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix}$, $\alpha \in \mathbb{F}_q^\times$; in this case, we identify A with $\phi^4(A)$ via the matrix $S = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$.

For examples of Theorems 1 and 2, as well as a characteristic 2 example, see chapter 5 in [4].

REMARK. In [2], Behn and Van der Merwe make extensive use of the correspondence between binary quadratic forms and 2×2 matrices, and the results in this paper can be restated in terms of binary quadratic forms. Indeed, in their work on class numbers of quadratic function fields, Gonzáles develops a theory of binary quadratic forms over $\mathbb{F}_q[T]$ in [5] with results analogous to the $d < g$ case in this paper, and Yu uses a correspondence between binary quadratic forms over $\mathbb{F}_q[T]$ and lattices in [6] to derive a class number formula. In chapter 3 of [4] we expand on the ideas of this paper to study the ideal class group.

Acknowledgements

This paper is the result of the author's research towards a doctoral dissertation [4]. The author would like to thank his supervisor, professor Florian Breuer, for his guidance and for proofreading several drafts of this paper, and to professor Cristian D. Gonzalez-Avilés for his input and ideas. The research was made possible by financial support from the Stellenbosch University and the Leiden University. The brunt of the work in this paper was done while the author was a student at the University of Stellenbosch under the supervision of professor Florian Breuer.

References

[1] Latimer, C. G. & MacDuffee, C. C., A Correspondence Between Classes of Ideals and Classes of Matrices. *The Annals of Mathematics* **34**, 313 – 316 (1933). doi:10.2307/1968204

[2] Behn, A. & Van der Merwe, A. B., An algorithmic version of the theorem by Latimer and MacDuffee for 2×2 integral matrices. *Linear Algebra and its Applications* **346**, 1 – 14 (2002). doi:10.1016/S0024-3795(01)00518-3

[3] Breuer, F., The André-Oort conjecture for products of Drinfeld modular curves. *Journal für die Reine und Angewandte Mathematik* **579**, :115 –-144 (2005). doi:10.1515/crll.2005.2005.579.115.

[4] Van Zyl, J. V., On the Latimer-MacDuffee theorem for polynomials over finite fields [dissertation]. *Stellenbosch University*, (2011). hdl:10019.1/6581

[5] González, C. D., Class numbers of quadratic function fields and continued fractions. *Journal of Number Theory*, **40(1)**, 38 – 59 (1992). doi:10.1016/0022-314X(92)90027-M

[6] Yu, J. K., A class number relation over function fields. *Journal of Number Theory*, **54(2)**, 318 – 340 (1995). doi:10.1006/jnth.1995.1122