Bull. Aust. Math. Soc. (First published online 2025), page 1 of 8*
doi:10.1017/S0004972725100671
*Provisional—final page numbers to be inserted when paper edition is published

A NOTE ON SOME QUADRATICS AND CUBICS OVER FINITE FIELDS

EILEEN X. PAN

(Received 8 July 2025; accepted 3 October 2025)

Abstract

We determine the conditions for the reducibility of some parametrised families of quadratic and cubic polynomials over finite fields, and count the number of irreducible trinomials. The existence of a factorisation of these polynomials plays an important role in studying the finite groups of exceptional Lie types.

2020 *Mathematics subject classification*: primary 11T06.

Keywords and phrases: field theory, polynomials over a finite field, irreducibility of polynomials, trinomials.

1. Introduction

The reducibility of polynomials over finite fields is important for many applications, including coding theory and cryptography. The well-known Berlekamp Algorithm [2] provides a method for factorising such polynomials. A more challenging problem is to decide reducibility for parametrised families of polynomials. For example, Dickson [5] determined for which nonzero parameters α, β, in the finite field $\mathbb{F}_{p^n}$ with $p > 3$ a prime, the polynomial $x^3 + \alpha x + \beta$ is reducible over $\mathbb{F}_{p^n}$. The analogous characterisation was obtained by Williams [9] for finite fields of characteristic 2 and 3. Polynomials of this form are trinomials as they have exactly three nontrivial terms. Von zur Gathen [8] has considered the irreducibility of trinomials over finite fields and formulated some conjectures on their distribution. This line of research was continued by Ahmadi in [1], who solved some of these conjectures and also proved irreducibility results for trinomials of the form $x^d + \alpha x^k + \beta$, where $\alpha, \beta \in \mathbb{F}_q^\times$ with even degree d.

Results of this flavour have applications in group theory. For example, in the course of classifying the conjugacy classes of the simple group of Lie type $G_2(q)$, Chang [4]

This work forms part of the author's PhD thesis at Warwick University and Monash University; the author was supported by Monash–Warwick Alliance Joint PhD Scholarships (Warwick).

required knowledge of the parameters $\zeta \in \mathbb{F}_q$ for which $x^3 - 3x - \zeta$ is irreducible over $\mathbb{F}_q$. Similarly, the determination of the conjugacy classes in $F_4(2^n)$ required Shinoda [7] to classify those parameters $\zeta \in \mathbb{F}_{2^n}$ for which $x^3 + x + \zeta$ is irreducible and, at the same time, $x^2 + \zeta x + \zeta^2 + 1$ is reducible.

This note is also motivated by a problem in group theory (see [6]): the suborbit classification of the (primitive) actions of $G_2(q)$ requires a detailed analysis of the reducibility of $x^2 + \zeta x - \zeta$ and $x^3 - 3x^2 - \zeta$ with parameter $\zeta \in \mathbb{F}_q$. We consider a slightly more general case and state our main result as follows.

Theorem 1.1. *Let q be a prime power, $\gamma \in \mathbb{F}_q, \zeta \in \mathbb{F}_q^\times$, and*

$$P = x^2 + \zeta x - \zeta \quad \text{and} \quad Q = x^3 - \gamma x^2 - \zeta.$$

For $q \equiv 0, 1 \bmod 3$, if $\gamma = 3$ or $\gamma^2 + 3\gamma + 9 = 0$, then at least one of P and Q is reducible. If $q \equiv 2 \bmod 3$ and $\gamma = 3$, then there are $\frac{1}{3}(q+1)$ elements $\zeta \in \mathbb{F}_q^\times$ such that both P and Q are irreducible.

2. Proof of Theorem 1.1

Throughout, let $q = p^n$ be a prime power. If $p = 3$, then, by assumption, we have $\gamma = 0$ and Q always has a root since $c \mapsto c^3$ is a Frobenius automorphism of $\mathbb{F}_{3^n}$. For $p \neq 3$, by construction, P and Q are trinomials over $\mathbb{F}_q$.

If $p > 3$, then rewriting $x = X + 3^{-1}\gamma$ yields $Q = X^3 - 3^{-1}\gamma^2 X - (\zeta + 2 \cdot 27^{-1}\gamma^3)$. Thus, in this case, [5, Theorems 1 and 3] applies, and P and Q are both irreducible only if we have $\zeta^2 + 4\zeta$ is a nonsquare and $-\zeta(4\gamma^3 + 27\zeta)$ is a square in $\mathbb{F}_q$, and $2^{-1}(\mu\sqrt{-3} + \zeta) + 27^{-1}\gamma^3$ is a noncube in the field extension $\mathbb{F}_q(\sqrt{-3})$, where $\mu \in \mathbb{F}_q$ with $81\mu^2 = -\zeta(4\gamma^2 + 27\zeta)$. This answers the irreducibility question, but it remains to count. Unfortunately, a similar result cannot be easily deduced from Williams' work [9] for $p = 2$. In the following, we present a uniform proof for all p (excluding $p = 3$ as mentioned above). Since P and Q are reducible if and only if they have a root, for a fixed $\gamma \in \mathbb{F}_q^\times$, we consider

$$\mathcal{S}_1 = \{\zeta \in \mathbb{F}_q^\times \mid P \text{ has roots in } \mathbb{F}_q^\times\} \quad \text{and} \quad \mathcal{S}_2 = \{\zeta \in \mathbb{F}_q^\times \mid Q \text{ has roots in } \mathbb{F}_q^\times\}.$$

We will determine the size of these sets separately; then determine $|\mathcal{S}_1 \cup \mathcal{S}_2|$ from $|\mathcal{S}_1 \cup \mathcal{S}_2| = |\mathcal{S}_1| + |\mathcal{S}_2| - |\mathcal{S}_1 \cap \mathcal{S}_2|$.

The polynomial P is reducible if and only if there are $u, v \in \mathbb{F}_q^\times$ such that $P = (x-u)(x-v)$, which is equivalent to $uv = -\zeta$ and $u + v = -\zeta$. Thus, P is reducible if and only if $\zeta = v^2(1-v)^{-1}$ for some $v \in \mathbb{F}_q \backslash \{0,1\}$. If we define $f\colon \mathbb{F}_q \backslash \{0,1\} \to \mathbb{F}_q^\times$ by $f(c) = c^2(1-c)^{-1}$, then $|\mathcal{S}_1| = |\mathrm{Im}\, f|$. Note that $f(s) = f(t)$ with $s, t \notin \{0,1\}$ if and only if $s = t$ or $t = s(s-1)^{-1}$. Since $s = s(s-1)^{-1}$ if and only if q is odd and $s = 2$,

$$|\mathcal{S}_1| = |\mathrm{Im}\, f| = \begin{cases} \frac{1}{2}(q-2) & \text{if } q \equiv 0 \bmod 2, \\ \frac{1}{2}(q-1) & \text{otherwise.} \end{cases}$$

https://doi.org/10.1017/S0004972725100671 Published online by Cambridge University Press

Now, we consider $\mathcal{S}_2$. For a fixed $\gamma \in \mathbb{F}_q^\times$, we know that Q has a root $u \in \mathbb{F}_q$ if and only if $\zeta = u^3 - \gamma u^2$. Since $\zeta \neq 0$, it follows that $|\mathcal{S}_2| = |\mathrm{Im}\, g|$, where $g\colon \mathbb{F}_q \setminus \{0,\gamma\} \to \mathbb{F}_q^\times$ is the map $g(c) = c^3 - \gamma c^2$. Note that $g(s) = g(t)$ for $s, t \notin \{0,\gamma\}$ if and only if $s = t$ or $t = ks$ for some $k \in \mathbb{F}_q\backslash\{0,1\}$ such that

$$g(ks) - g(s) = s^2(k-1)(k^2 s + ks - \gamma k + s - \gamma) = 0.$$

Since $s^2(k-1) \neq 0$, the latter is equivalent to $\ell_s(k) = 0$, where

$$\ell_s(k) = k^2 + r_s k + r_s \quad \text{with} \quad r_s = 1 - \gamma s^{-1} \neq 0.$$

Note that any such k satisfies $ks \notin \{0,\gamma\}$ (for otherwise, $r_s = 0$ or $\ell_s = 1$, which is a contradiction). Thus, we are interested in

$$\kappa(s) = |\{k \in \mathbb{F}_q \setminus \{0,1\} \mid \ell_s(k) = 0\}|,$$

which informs us of $\mathrm{Im}\, g$. Suppose $\ell_s(k)$ has roots u, v; note that $u, v \notin \{0,-1\}$. Then, $u + v = -r_s$ and $uv = r_s$, so $r_s = -v^2(1+v)^{-1}$. Moreover, $k = 1$ is a root of $\ell_s(k)$ if and only if q is odd and $r_s = -2^{-1}$. We have $u = v$ if and only if $p = 3$ and $r_s = 1$, or $q \equiv \pm 1 \bmod 6$ and $s \in \{-3^{-1}\gamma, \gamma\}$. With such notation, since $s \neq \gamma$ by assumption,

$$\kappa(s) = \begin{cases} 0 & \text{if } r_s \notin \{-v^2(1+v)^{-1} \mid v \in \mathbb{F}_q\backslash\{0,-1\}\}; \\ 1 & \text{if } q \equiv \pm 1 \bmod 6 \text{ and } r_s \in \{4, -2^{-1}\}; \\ 2 & \text{if } r_s \in \{-v^2(1+v)^{-1} \mid v \in \mathbb{F}_q\backslash\{0,-1\}\} \setminus \{1, 4, -2^{-1}\}; \end{cases}$$

recall that $p = 2$ is allowed, in which case -2^{-1} does not occur. Since the map g restricted to the subset $\mathcal{K}_1 = \{s \in \mathbb{F}_q\backslash\{0,\gamma\} \mid \kappa(s) = 0\}$ is injective, restricted on $\mathcal{K}_2 = \{s \in \mathbb{F}_q\backslash\{0,\gamma\} \mid \kappa(s) = 1\}$ is 2-to-1, restricted to $\mathcal{K}_3 = \{s \in \mathbb{F}_q\backslash\{0,\gamma\} \mid \kappa(s) = 2\}$ is 3-to-1, and $\mathcal{K}_1 \sqcup \mathcal{K}_2 \sqcup \mathcal{K}_3 = \mathbb{F}_q\backslash\{0,\gamma\}$,

$$|\mathrm{Im}\, g| = |\mathcal{K}_1| + \tfrac{1}{2}|\mathcal{K}_2| + \tfrac{1}{3}|\mathcal{K}_3|.$$

More specifically, observe that for any $c \neq 1$, there exists $s = \gamma(1-c)^{-1}$ such that $r_s = c$. Also, by construction, $r_s \neq 1$ and $1 \in \{-v^2(1+v)^{-1} \mid v \in \mathbb{F}_q\backslash\{0,-1\}\}$ if and only if $q \equiv 0, 1 \bmod 3$. Moreover, by symmetry,

$$|\mathcal{K}_1| = |\{-v^2(1+v)^{-1} \mid v \in \mathbb{F}_q\backslash\{0,-1\}\}| = |\mathrm{Im}\, f|$$

and

$$\begin{aligned} |\mathcal{K}_3| &= |\{-v^2(1+v)^{-1} \mid v \in \mathbb{F}_q\backslash\{0,-1\}\} \setminus \{1,4,-2^{-1}\}| \\ &= \begin{cases} \tfrac{1}{2}(q-2) & \text{if } q \equiv 2 \bmod 6, \\ \tfrac{1}{2}(q-2) - 1 & \text{if } q \equiv 4 \bmod 6, \\ \tfrac{1}{2}(q-1) - 3 & \text{if } q \equiv 1 \bmod 6, \\ \tfrac{1}{2}(q-1) - 2 & \text{if } q \equiv 5 \bmod 6. \end{cases} \end{aligned}$$

https://doi.org/10.1017/S0004972725100671 Published online by Cambridge University Press

We therefore deduce that

$$|\mathcal{S}_2| = |\mathrm{Im}\, g| = \begin{cases} q-2-\frac{1}{2}(q-2)+\frac{1}{6}(q-2) = \frac{2}{3}(q-2) & \text{if } q \equiv 2 \bmod 6,\\ q-2-\frac{1}{2}(q-2)+1+\frac{1}{6}(q-4) = \frac{2}{3}(q-1) & \text{if } q \equiv 4 \bmod 6,\\ q-2-\frac{1}{2}(q-1)+1+\frac{2}{2}+\frac{1}{6}(q-7) = \frac{2}{3}(q-1) & \text{if } q \equiv 1 \bmod 6,\\ q-2-\frac{1}{2}(q-1)+\frac{2}{2}+\frac{1}{6}(q-5) = \frac{2}{3}(q-2) & \text{if } q \equiv 5 \bmod 6. \end{cases}$$

In summary,

$$|\mathcal{S}_2| = |\mathrm{Im}\, g| = \begin{cases} \frac{2}{3}(q-1) & \text{if } q \equiv 1 \bmod 3,\\ \frac{2}{3}(q-2) & \text{if } q \equiv 2 \bmod 3. \end{cases}$$

It remains to examine $\mathcal{S}_1 \cap \mathcal{S}_2$. With the same setup as above, $\zeta \in \mathcal{S}_1 \cap \mathcal{S}_2$ if and only if there exist $s \in \mathbb{F}_q \backslash \{0, \gamma\}$ and $t \in \mathbb{F}_q \backslash \{0, 1\}$ such that $\zeta = f(t) = g(s)$, where f, g are as defined above. The latter equality is equivalent to $h(t) = 0$, where

$$h(t) = t^2 + (s^3 - \gamma s^2)t - (s^3 - \gamma s^2).$$

When $p \neq 2$, the quadratic equation $h(t) = 0$ in t holds for some $t \in \mathbb{F}_q \backslash \{0, 1\}$ if and only if

$$c(s) = s^2(s-\gamma)(s^3 - \gamma s^2 + 4)$$

is a square in $\mathbb{F}_q$. In particular, given $s \notin \{0, \gamma\}$, we see $c(s) = 0$ if and only if $-4 = s^3 - \gamma s^2$. If $\gamma^2 + 3\gamma + 9 = 0$, then $q \equiv 1 \bmod 3$ and $\gamma = (-3 \pm 3w)2^{-1}$ for $w \in \mathbb{F}_q^\times$ such that $-3 = w^2$, and

$$c(s) = s^2(s-\gamma)(s + 3^{-1}\gamma)(s - 2\cdot 3^{-1}\gamma)^2.$$

Note that when $\gamma = 3$, the same factorisation exists; that is,

$$c(s) = s^2(s-\gamma)(s+1)(s-2)^2.$$

For $p \neq 2$, if $q \equiv 1 \bmod 3$, then let $\gamma \in \{3, (-3+3w)2^{-1}, (-3-3w)2^{-1}\}$; if $q \equiv 2 \bmod 3$, then let $\gamma = 3$. Recall that if $p \neq 2$, then $\kappa(s) = 2$ if and only if the discriminant $s^{-2}(\gamma - s)(\gamma + 3s)$ of $\ell_s(k)$ is a square in $\mathbb{F}_q^\times$, and $\kappa(s) = 0$ if and only if $(\gamma - s)(\gamma + 3s)$ is a nonsquare in $\mathbb{F}_q^\times$. Since -3 is a square in $\mathbb{F}_q^\times$ if $q \equiv 2 \bmod 3$, and is a nonsquare if $q \equiv 1 \bmod 3$ and $-3(s-\gamma)(s + 3^{-1}\gamma) = (\gamma - s)(3s + \gamma)$, it follows that

$$\begin{aligned} \mathcal{S}_1 \cap \mathcal{S}_2 &= \{-4\} \cup \{s^3 - \gamma s^2 \mid s \in \mathbb{F}_q \backslash \{0,\gamma\} \text{ and } c(s) \text{ is a square in } \mathbb{F}_q^\times\} \\ &= \{-4\} \cup \begin{cases} \{s^3 - \gamma s^2 \mid s \in \mathbb{F}_q \backslash \{0,\gamma\} \text{ and } \kappa(s) = 2\} & \text{if } q \equiv 1 \bmod 6,\\ \{s^3 - \gamma s^2 \mid s \in \mathbb{F}_q \backslash \{0,\gamma\} \text{ and } \kappa(s) = 0\} & \text{if } q \equiv 5 \bmod 6. \end{cases} \end{aligned}$$

Now, consider the case where $p = 2$ and $q = 2^n$. The trace map over $\mathbb{F}_{2^n}$ is defined by

$$\mathrm{tr}\colon \mathbb{F}_{2^n} \to \{0,1\}, \quad s \mapsto \Big(\sum_{i=0}^{n-1} s^{(2^i)}\Big) \bmod 2.$$

https://doi.org/10.1017/S0004972725100671 Published online by Cambridge University Press

It follows that $\mathrm{tr}(x) = \mathrm{tr}(x^2)$ and $\mathrm{tr}(x) + \mathrm{tr}(y) = \mathrm{tr}(x + y)$ for all $x, y \in \mathbb{F}_{2^n}$. We now consider $\gamma = 1$ or $\gamma^2 + \gamma + 1 = 0$. Note that there exists $\gamma \in \mathbb{F}_q^\times$ such that $\gamma^2 + \gamma + 1 = 0$ if and only if $q \equiv 1 \bmod 3$ and $\gamma^3 = 1$. Moreover, it is well known that $x^2 + \alpha x + \beta$ for $\alpha, \beta \in \mathbb{F}_q^\times$ is reducible over $\mathbb{F}_q$ if and only if $\mathrm{tr}(a^{-2}b) = 0$ (see [3, Theorem 6.69]). Thus, $h(t) = 0$ has:

- two solutions if and only if $\mathrm{tr}(s^{-2}(s + \gamma)^{-1}) = 0$ and
- no solution if and only if $\mathrm{tr}(s^{-2}(s + \gamma)^{-1}) = 1$.

However, when $p = 2$, the quadratic $\ell_s(k) = 0$ has two solutions if and only if $\mathrm{tr}(s(s + \gamma)^{-1}) = 0$ and no solution if and only if $\mathrm{tr}(s(s + \gamma)^{-1}) = 1$. Observe that if $\gamma^3 = 1$, then $1 + s^3 = \gamma^3 + s^3 = (\gamma + s)(\gamma^2 + s^2 + \gamma s)$ and so

$$\mathrm{tr}(s^{-2}(s + \gamma)^{-1}) + \mathrm{tr}(s(s + \gamma)^{-1}) = \mathrm{tr}(\gamma^2 s^{-2}) + \mathrm{tr}(\gamma s^{-1}) + \mathrm{tr}(1) = \mathrm{tr}(1).$$

Since $\mathrm{tr}(1) = 0$ if and only if $q \equiv 1 \bmod 3$, and $\mathrm{tr}(1) = 1$ if and only if $q \equiv 2 \bmod 3$, it follows that

$$\begin{aligned}\mathcal{S}_1 \cap \mathcal{S}_2 &= \{s^3 + \gamma s^2 \mid s \in \mathbb{F}_q \backslash \{0, \gamma\} \text{ and } \mathrm{tr}(s^{-2}(s + 1)^{-1}) = 0\} \\ &= \begin{cases} \{s^3 + \gamma s^2 \mid s \in \mathbb{F}_q \backslash \{0, \gamma\} \text{ and } \kappa(s) = 2\} & \text{if } q \equiv 4 \bmod 6, \\ \{s^3 + \gamma s^2 \mid s \in \mathbb{F}_q \backslash \{0, \gamma\} \text{ and } \kappa(s) = 0\} & \text{if } q \equiv 2 \bmod 6. \end{cases}\end{aligned}$$

Together with our discussion for odd q above, we have shown that

$$|\mathcal{S}_1 \cap \mathcal{S}_2| = \begin{cases} \frac{1}{6}(q - 1) & \text{if } q \equiv 1 \bmod 6, \\ \frac{1}{2}(q - 1) & \text{if } q \equiv 5 \bmod 6, \\ \frac{1}{6}(q - 4) & \text{if } q \equiv 4 \bmod 6, \\ \frac{1}{2}(q - 2) & \text{if } q \equiv 2 \bmod 6. \end{cases}$$

In summary, applying the Principle of Inclusion-Exclusion, we see that

$$|\mathcal{S}_1 \cup \mathcal{S}_2| = \begin{cases} q - 1 & \text{if } q \equiv 1 \bmod 3 \text{ and } \gamma = 3 \text{ or } \gamma^2 + 3\gamma + 9 = 0, \\ \frac{2}{3}(q - 2) & \text{if } q \equiv 2 \bmod 3 \text{ and } \gamma = 3. \end{cases}$$

This completes the proof. □

3. Further discussion

Although our proof for the main result excludes the case $p = 3$, our discussion for $\mathcal{S}_2$ remains valid for any $\gamma \in \mathbb{F}_q^\times$ in all characteristics. More specifically, from the discussion above, we also obtain the following result.

COROLLARY 3.1. *Let q be a prime power, $\zeta \in \mathbb{F}_q^\times$ and*

$$Q = x^3 - \gamma x^2 - \zeta.$$

Then, for each $\gamma \in \mathbb{F}_q^\times$,

$$|\{\zeta \in \mathbb{F}_q^\times \mid Q \text{ is reducible}\}| = \begin{cases} \frac{1}{3}(2q-3) & \text{if } q \equiv 0 \bmod 3, \\ \frac{2}{3}(q-1) & \text{if } q \equiv 1 \bmod 3, \\ \frac{2}{3}(q-2) & \text{if } q \equiv 2 \bmod 3. \end{cases}$$

The next result is a corollary of [9, Theorem 1] that turns out to be useful in finding suborbit representatives in primitive $G_2(q)$-actions, where $G_2(q)$ is the finite simple group of exceptional Lie type G_2 over $\mathbb{F}_q$. In the case where $p = 2$, setting $x = y + 1$ yields the depressed form of Q, namely, $D = y^3 + \gamma y + \zeta$, which has the same reducibility as Q. In particular, by assumption, we have $\gamma^3 = 1$ if $q \equiv 1 \bmod 3$ and $\gamma = 1$ if $q \equiv 2 \bmod 3$. For the sake of completeness, we include a restatement of [9, Theorem 1].

THEOREM 3.2 [9, Theorem 1]. *Let* $q = 2^n$ *for some positive integer n. Let* $D = x^3 + \gamma x + \zeta$*, where* $\gamma \in \mathbb{F}_q, \zeta \in \mathbb{F}_q^\times$*. Let* t_1, t_2 *denote the roots of* $t^2 + \zeta t + \gamma^3 = 0$*. Then,* t_1, t_2 *lie in* $\mathbb{F}_q$ *if* $\mathrm{tr}(\gamma^3\zeta^{-2}) = 0$ *and in* $\mathbb{F}_{q^2}$ *otherwise.*

(a) *D has three distinct roots in* $\mathbb{F}_q$ *if and only if* $\mathrm{tr}(\gamma^3\zeta^{-2}) = \mathrm{tr}(1)$ *and* $t^2 + \zeta t + \gamma^3$ *has roots* t_1, t_2 *that are cubes in* $\mathbb{F}_q$ *(n even) or in* $\mathbb{F}_{q^2}$ *(n odd).*
(b) *D has precisely one root in* $\mathbb{F}_q$ *if and only if* $\mathrm{tr}(\gamma^3\zeta^{-2}) \neq \mathrm{tr}(1)$.
(c) *D has no root in* $\mathbb{F}_q$ *if and only if* $\mathrm{tr}(\gamma^3\zeta^{-2}) = \mathrm{tr}(1)$ *and* $t^2 + \zeta t + \gamma^3$ *has roots* t_1, t_2 *that are noncubes in* $\mathbb{F}_q$ *(n even) or in* $\mathbb{F}_{q^2}$ *(n odd).*

COROLLARY 3.3. *Let* $q = 2^n$ *for some positive integer n and let* $\zeta \in \mathbb{F}_q^\times$*. Let* ξ *be a primitive element of* $\mathbb{F}_{q^2}^\times$ *and*

$$\epsilon = \begin{cases} 1 & \text{if } q \equiv 1 \bmod 3, \\ -1 & \text{if } q \equiv 2 \bmod 3. \end{cases}$$

Let $D = x^3 + \gamma x + \zeta$*, where* $\zeta \in \mathbb{F}_q^\times$ *and* $\gamma = 1$ *if n is odd, or* $\gamma \in \mathbb{F}_q$ *such that* $\gamma^3 = 1$ *if n is even. Then, the following hold.*

(a) *D is irreducible over* $\mathbb{F}_q$ *if and only if* $\zeta = \eta^{3j+1} + \eta^{-3j-1}$ *for some j with* $0 \leq j < \frac{1}{3}(q - \epsilon)$*, where* $\eta = \xi^{q+\epsilon}$.
(b) *D has precisely one root in* $\mathbb{F}_q$ *if and only if* $\zeta = \nu^k + \nu^{-k}$ *for some k with* $0 < k \leq \lfloor \frac{1}{2}(q + \epsilon) \rfloor$*, where* $\nu = \xi^{q-\epsilon}$.
(c) *If D is irreducible over* $\mathbb{F}_q$*, then* $x^2 + \zeta(\zeta + 1)^{-1}x + \zeta(\zeta + 1)^{-1}$ *is reducible over* $\mathbb{F}_q$.
(d) *If* $r \in \mathbb{F}_q^\times$ *is a root of D, then* $x^2 + \zeta x + \zeta$ *and* $x^2 + rx + r$ *have the same reducibility over* $\mathbb{F}_q$.

PROOF. (a) It follows from Theorem 3.2(c) that D is irreducible if and only if $\mathrm{tr}(\zeta^{-2}) = \mathrm{tr}(1)$ and the roots of $x^2 + \zeta x + 1$ (in $\mathbb{F}_q$ if n is even or in $\mathbb{F}_{q^2}$ if n is odd)

https://doi.org/10.1017/S0004972725100671 Published online by Cambridge University Press

are noncubes. Moreover, $t \neq 0$ is a root of $x^2 + \zeta x + 1$ if and only if t^{-1} is also a root and $t + t^{-1} = \zeta$. Since $\zeta \in \mathbb{F}_q^\times$, it follows that $t^q + t^{-q} = t + t^{-1}$, and so either $t \in \mathbb{F}_q^\times$ or $t \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ and $t^{q+1} = 1$. Such t is a noncube if and only if $t = \eta^{3j\pm 1}$ for some $j \in \mathbb{Z}$, where $\eta = \xi^{q+\epsilon}$. However, if $t = \eta^{3j-1}$, then $t^{-1} = \eta^{-3j+1} = \eta^{3j'+1}$ for some $j' = -j \in \mathbb{Z}$. Thus, the irreducibility criteria in Theorem 3.2(c) is equivalent to $\zeta = \eta^{3j+1} + \eta^{-3j-1}$ for some $j \in \mathbb{Z}$.

Note that if $j - k = \frac{1}{3}(q - \epsilon)$, then $\eta^{3j+1} + \eta^{-3j-1} = \eta^{3k+1} + \eta^{-3k-1}$; thus, for $\zeta \in \mathbb{F}_q^\times$, the trinomial D is irreducible if and only if $\zeta \in \{\eta^{3j+1} + \eta^{-3j-1} \mid 0 \leq j < \frac{1}{3}(q - \epsilon)\}$; there are precisely $\frac{1}{3}(q - \epsilon)$ such irreducible polynomials.

(b) From Theorem 3.2(b), we see that D has precisely one root in $\mathbb{F}_q^\times$ if and only if $\mathrm{tr}(\zeta^{-2}) \neq \mathrm{tr}(1)$. Since $\mathrm{tr}(1) \equiv n - 1 \bmod 2$, it follows that $\mathrm{tr}(\zeta^{-2}) \neq \mathrm{tr}(1)$ if and only if the quadratic $x^2 + \zeta x + 1$ has two roots $t, t^{-1} \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ if $q \equiv 1 \bmod 3$, or two roots $t, t^{-1} \in \mathbb{F}_q^\times$ if $q \equiv 2 \bmod 3$; in both cases, $t + t^{-1} = \zeta$. As seen above, such roots t satisfy $t^{q+\epsilon} = 1$. That is, D has precisely one root in $\mathbb{F}_q$ if and only if $\zeta = \nu^k + \nu^{-k}$, where $\nu = \xi^{q-\epsilon}$, for some $0 < k < q + \epsilon$. Moreover, if $i + j = q + \epsilon$, then $\nu^i + \nu^{-i} = \nu^j + \nu^{-j}$. From this, we can conclude that $x^2 + \zeta x + 1$ is irreducible over $\mathbb{F}_q$ if and only if $\zeta \in \{\nu^k + \nu^{-k} \mid 0 < k \leq \lfloor (q + \epsilon)/2 \rfloor\}$.

(c) The quadratic $x^2 + \zeta(\zeta + 1)^{-1}x + \zeta(\zeta + 1)^{-1}$ is reducible if and only if $\mathrm{tr}(1 + \zeta^{-1}) = 0$. Since $\mathrm{tr}(\zeta^{-2}) = \mathrm{tr}(1)$ by Theorem 3.2(c) and $\mathrm{tr}(\zeta^{-1}) = \mathrm{tr}(\zeta^{-2})$, the claim follows.

(d) By assumption, we have $r(r + 1)^2 = \zeta$. Since

$$\mathrm{tr}(r^{-1}(r + 1)^{-2}) + \mathrm{tr}(r^{-1}) = \mathrm{tr}((r + 1)^{-1}) + \mathrm{tr}((r + 1)^{-2}) = 0,$$

it follows that $\mathrm{tr}(\zeta^{-1}) = \mathrm{tr}(r^{-1})$, namely, $x^2 + x + r^{-1}$ is reducible over $\mathbb{F}_q$ if and only if $x^2 + x + \zeta^{-1}$ is reducible over $\mathbb{F}_q$, which proves the claim. □

References

[1] O. Ahmadi, 'On the distribution of irreducible trinomials over F_3', *Finite Fields Appl.* **13**(3) (2007), 659–664.

[2] E. R. Berlekamp, 'Factoring polynomials over finite fields'. *Bell System Tech. J.* **46** (1967), 1853–1859.

[3] E. R. Berlekamp, *Algebraic Coding Theory* (McGraw-Hill, New York–Toronto–London, 1968).

[4] B. Chang, 'The conjugate classes of Chevalley groups of type (G_2)', *J. Algebra* **9** (1968), 190–211.

[5] L. E. Dickson, 'Criteria for the irreducibility of functions in a finite field', *Bull. Amer. Math. Soc.* **13**(1) (1906), 1–8.

[6] E. X. Pan, *Some Primitive Actions of* $G_2(q)$, PhD Thesis (Monash University–Warwick University, in preparation).

[7] K. Shinoda, 'The conjugacy classes of Chevalley groups of type (F_4) over finite fields of characteristic 2', *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **21** (1974), 133–159.

[8] J. von zur Gathen, 'Irreducible trinomials over finite fields', *Math. Comp.* **72**(244) (2003), 1987–2000.

[9] K. S. Williams, 'Note on cubics over $GF(2^n)$ and $GF(3^n)$', *J. Number Theory* **7**(4) (1975), 361–365.

https://doi.org/10.1017/S0004972725100671 Published online by Cambridge University Press

EILEEN X. PAN, School of Mathematics,
Monash University, Victoria 3800, Australia and
Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom
e-mail: eileen.pan@monash.edu

https://doi.org/10.1017/S0004972725100671 Published online by Cambridge University Press