Journal der mathematischen Ablehnungen
Paper No.30 (2014)

On expressing elements as a sum of squares where one square is restricted to a subfield

Robert S. Coulter[1] and Pamela Kosick[2]

[1]Department of Mathematical Sciences, University of Delaware, Newark, DE, 19716, USA.
[2]School of Natural Sciences and Mathematics, The Richard Stockton College of New Jersey, 101 Vera King Farris Drive, Galloway, NJ, 08205, USA.

AMS Subject class: 11T06

Keywords: squares, finite field structure

R.S. Coulter and P. Kosick, *On expressing elements as a sum of squares where one square is restricted to a subfield*, Finite Fields Appl. **26** (2014), 116–122.

Abstract

Let q be a prime power and fix $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. In this note it is proved that, provided $q > 5$, the set

$$\mathcal{S}_a = \{a - \alpha^2 : \alpha \in \mathbb{F}_q^*\}$$

contains both a square and a non-square of $\mathbb{F}_{q^2}^*$. In particular, every $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ can be written as a sum of a square of $\mathbb{F}_{q^2}$ and a square of $\mathbb{F}_q$.

§ 1. The problem and the main result

Throughout we use $\mathbb{F}_q$ to denote the finite field of q elements and $\mathbb{F}_q^*$ to denote the non-zero elements of the field. We also use $\square_q$ and $\boxslash_q$ to denote the squares and non-squares, respectively, of $\mathbb{F}_q$.

In this note we are interested in a specific instance of the following type of problem:

> Let A be a subset of $\mathbb{F}_q^*$ of order $O(q)$. What is the minimum order of a subset S of $\mathbb{F}_q^*$ so that for all $a \in A$, the set $\{a - s : s \in S\}$ contains both a square and non-square element of $\mathbb{F}_q^*$?

Since there are no non-square elements in a finite field of even characteristic, we assume q is an odd prime power throughout.

There are variants of the problem. For example, one can insist that S be a subgroup of $\mathbb{F}_q^*$ instead of simply a subset; or that $A = \mathbb{F}_q^*$; or that q be a square, and so on. We now discuss two such variations. In either of these examples, the lower bounds on q avoid degenerate cases.

For $q \geq 7$, fix $A = \mathbb{F}_q^*$. It is well known that any non-zero element of $\mathbb{F}_q$ can be expressed as the difference of two non-zero squares of the field in many ways. Similar results can be obtained for sums of squares. Together, these show that $S = \square_q^*$ or $S = \boxslash_q$ suffices.

Now fix $A = \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Then it is relatively easy to show that for $q \geq 5$, $S = \mathbb{F}_q^*$ suffices. Let $a \in A$. Then $\{1, a\}$ forms a basis for $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. If $\{a - s : s \in \mathbb{F}_q^*\}$ only contained elements of $\square_{q^2}^*$, then $\{\alpha a - \alpha s : \alpha, s \in \mathbb{F}_q^*\} = \mathbb{F}_{q^2} \setminus \{\alpha a, \alpha : \alpha \in \mathbb{F}_q^*\}$ would only contain elements of $\square_{q^2}^*$ as well. Consequently, $\boxslash_{q^2} \subseteq \{\alpha a : \alpha \in \mathbb{F}_q^*\}$, implying $(q^2-1)/2 \leq q-1$, a contradiction. Thus $\{a - s : s \in \mathbb{F}_q^*\}$ must contain a non-square. Now suppose it contains only non-squares, implying $\mathbb{F}_{q^2} \setminus \{\alpha a, \alpha : \alpha \in \mathbb{F}_q^*\}$ contains only non-squares. Hence $\square_{q^2} \subseteq \{\alpha a, \alpha : \alpha \in \mathbb{F}_q\}$, giving the inequality

$$\frac{q^2-1}{2} \leq \begin{cases} 2q-1 & \text{if } a \in \square_{q^2}, \\ q & \text{if } a \in \boxslash_{q^2}. \end{cases}$$

This yields a contradiction if $q \geq 5$. Thus $S = \mathbb{F}_q^*$ suffices when $q \geq 5$ and $A = \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. (Note that it is trivial to refine this argument to obtain exact counts for $|\{a - s : s \in \mathbb{F}_q^*\} \cap \square_{q^2}^*|$ and $|\{a - s : s \in \mathbb{F}_q^*\} \cap \boxslash_{q^2}^*|$.)

In this note we give an improvement of this second variation; our result is somewhat related to the first variation. We shall prove that, if $A = \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $q \geq 7$, then $S = \square_q^*$ suffices. More specifically, fix $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and consider the set

$$\mathcal{S}_a = \{a - \alpha : \alpha \in \square_q^*\}.$$

Our main statement is the following.

Theorem 1. *For $q \geq 7$ and any $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, $\mathcal{S}_a$ intersects both $\square_{q^2}$ and $\boxslash_{q^2}$ non-trivially. More specifically, for $q \geq 5$, the following statements hold.*

(i) $\mathcal{S}_a \cap \square_{q^2} = \varnothing$ if and only if $q = 5$ and a satisfies one of $a^2 = 3$, $a^2 = 2a + 1$, or $a^2 = 3a + 1$.

(ii) $\mathcal{S}_a \cap \boxslash_{q^2} = \varnothing$ if and only if $q = 5$ and a satisfies $a^2 = 2$.

As with the earlier examples, there is a degenerate case. When $q = 3$, $|\mathcal{S}_a| = 1$, so that $\mathcal{S}_a \subset \square_{q^2}^*$ or $\mathcal{S}_a \subset \boxslash_{q^2}$ must hold. The proof is mostly elementary; it relies on the regularity of both the sums and differences of squares in a field, but in one instance we also invoke Weil's bound on the number of $\mathbb{F}_q$-rational points on an absolutely irreducible curve over a finite field. Theorem 1 also resolves a problem related to Dickson semifields that arose in work of the second author, see [4].

Before proceeding to the proof, we note that the problem considered in the second variation example and Theorem 1 can be restated as a problem concerning the (ir)reducibility of quadratics over $\mathbb{F}_{q^2}$. Theorem 1 is equivalent to showing that for any $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, there exists elements $\alpha, \beta \in \square_q^*$ for which $a(a - \alpha) \in \boxslash_{q^2}$ and $a(a - \beta) \in \square_{q^2}^*$. This yields the following corollary.

Corollary 2. *Let $q \geq 7$ be an odd prime power. Then for any $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, there exist elements $\alpha, \beta \in \square_q^*$ for which $X^2 - aX + a\alpha$ is irreducible over $\mathbb{F}_{q^2}$ and $X^2 - aX + a\beta$ is reducible over $\mathbb{F}_{q^2}$.*

§ 2. Difference sets and sum sets

We shall need two results concerning sums and differences of squares. For completeness, we recall the following definitions.

Definition 3. *Let G be a group of order v and let $D \subset G$ with $|D| = k$. If there exists non-negative integers λ and μ such that every non-identity element of D can be written in precisely λ ways as a quotient in D while every non-identity element of $G \setminus D$ can be written in μ ways as a quotient in D, then D is called a* (v, k, λ, μ) partial difference set. *If $\lambda = \mu$, then D is called a* (v, k, λ) difference set.

Definition 4. *Let G be a group of order v and let $D \subset G$ with $|D| = k$. If there exists non-negative integers λ and μ such that every non-identity element of D can be written in precisely λ ways as a product in D while every non-identity element of $G \setminus D$ can be written in μ ways as a product in D, then D is called a* (v, k, λ, μ) partial sum set. *If $\lambda = \mu$, then D is called a* (v, k, λ) sum set.

While difference sets and partial difference sets have been studied for quite some period of time [1], an in-depth systematic treatment of sum sets and partial sum sets was only initiated recently by Gutekunst [3], see also the papers [2, 5, 6, 8, 10].

Though the two types of objects are similarly defined, their behaviour is generally quite distinct. However, in one particular case, there is a very strong connection. The following result is well known.

Lemma 5. *If $q \equiv 1 \bmod 4$, the set $\square_q^*$ forms a $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$ partial difference set. If $q \equiv 3 \bmod 4$, the set $\square_q^*$ forms a $(q, \frac{q-1}{2}, \frac{q-3}{4})$ difference set.*

Gutekunst noted [3, Lemma 1.5] the following.

Lemma 6. *If $q \equiv 1 \bmod 4$, the set $\square_q^*$ forms a $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$ partial sum set. If $q \equiv 3 \bmod 4$, the set $\square_q^*$ forms a $(q, \frac{q-1}{2}, \frac{q-3}{4}, \frac{q+1}{4})$ partial sum set.*

Let $a \in \mathbb{F}_q^*$. We denote by sn_a the number of ways in which a can be written as $x - y$ with $x \in \square_q^*$ and $y \in \boxslash_q$. Similarly, we use ns_a to denote the number of ways in which a can be written as $y - x$ with $x \in \square_q^*$ and $y \in \boxslash_q$. One can use the previous two lemmas to prove the following.

Lemma 7. *If $q \equiv 1 \bmod 4$, then $sn_a = ns_a = \frac{q-1}{4}$. If $q \equiv 3 \bmod 4$, then*

$$sn_a = \begin{cases} \frac{q-3}{4} & \text{if } a \in \square_q^*, \\ \frac{q+1}{4} & \text{if } a \in \boxslash_q; \end{cases} \qquad \text{and} \qquad ns_a = \begin{cases} \frac{q+1}{4} & \text{if } a \in \square_q^*, \\ \frac{q-3}{4} & \text{if } a \in \boxslash_q. \end{cases}$$

These counts will prove crucial in our proof of Theorem 1

§ 3. Proof of Theorem 1

We proceed to establishing our main result. Fix $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q\}$. Define the set $\mathcal{T}$ by

$$\begin{aligned} \mathcal{T} &= \{\beta a - \alpha \,:\, (\alpha, \beta \in \mathbb{F}_q) \wedge (\beta\alpha \in \square_q^*)\} \\ &= \{\beta(a - \alpha) \,:\, \beta \in \mathbb{F}_q^* \wedge \alpha \in \square_q^*\}. \end{aligned}$$

Note that if $a - \alpha, a - \beta \in \mathbb{F}_q^* b$ for some $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and $\alpha, \beta \in \mathbb{F}_q$, then $\alpha = \beta$ is forced. Consequently, every coset of $\mathbb{F}_q^*$ in $\mathbb{F}_{q^2}^*$, apart from $\mathbb{F}_q^*$ itself, contains a unique element $a - \alpha$ with $\alpha \in \mathbb{F}_q$. This also means

$$\mathcal{T} = \bigcup_{\alpha \in \square_q^*} \mathbb{F}_q^*(a - \alpha). \tag{1}$$

Lemma 8. *Fix $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.*

(i) If $\mathcal{S}_a \cap \square_{q^2} = \varnothing$, then $\mathcal{T} \subset \boxslash_{q^2}$. Furthermore, if $a \in \boxslash_{q^2}$, then

$$\boxslash_{q^2} = \mathcal{T} \cup \mathbb{F}_q^* a \quad \text{and} \quad \square_{q^2}^* = \{\beta a - \alpha \,:\, (\alpha, \beta \in \mathbb{F}_q) \wedge (\beta\alpha \in \boxslash_q)\} \cup \mathbb{F}_q^*;$$

and if $a \in \square_{q^2}$, then there exists a unique $\beta \in \boxslash_q$ for which

$$\boxslash_{q^2} = \mathcal{T} \cup \mathbb{F}_q^*(a - \beta).$$

(ii) If $\mathcal{S}_a \cap \boxslash_{q^2} = \varnothing$, then $a \in \boxslash_{q^2}$, $\square_{q^2}^* = \mathcal{T} \cup \mathbb{F}_q^*$ and $\boxslash_{q^2} = \mathcal{T} a \cup \mathbb{F}_q^* a$.

Proof. Suppose first that $\mathcal{S}_a \cap \square_{q^2} = \varnothing$. Since every coset of $\mathbb{F}_q^*$ in $\mathbb{F}_{q^2}^*$ consists entirely of squares or non-squares of $\mathbb{F}_{q^2}$, it follows from (1) that $\mathcal{T} \subset \boxslash_{q^2}$. Note $a \notin \mathcal{T}$. Straightforward counting shows $|\mathcal{T}| = \frac{(q-1)^2}{2}$ and so $|\boxslash_{q^2} \setminus \mathcal{T}| = q - 1$. Thus, if $a \in \boxslash_{q^2}$, then $\boxslash_{q^2} = \mathcal{T} \cup \mathbb{F}_q^* a$, while if $a \in \square_{q^2}$, then the discussion preceding (1) implies there must exist a unique $\beta \in \boxslash_q$ for which $\boxslash_{q^2} = \mathcal{T} \cup \mathbb{F}_q^*(a - \beta)$.

For (ii), a similar argument to the above establishes $\mathcal{T} \subset \square_{q^2}^*$. Since $\mathbb{F}_q^* \subset \square_{q^2}^*$, we have $\square_{q^2}^* = \mathcal{T} \cup \mathbb{F}_q^*$ and $a \in \boxslash_{q^2}$. □

Lemma 9. *Fix $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Then there exist $c, d \in \mathbb{F}_q$ satisfying $a^2 = ca - d$ with $X^2 - cX + d$ irreducible over $\mathbb{F}_q$. If $c = 0$, then $-d \in \square_q$. Otherwise, $c \neq 0$ and*

$$\begin{cases} cd \in \square_q & \text{if } \mathcal{S}_a \cap \square_{q^2} = \varnothing, \text{ or} \\ cd \in \square_q^* & \text{if } \mathcal{S}_a \cap \square_{q^2} = \varnothing. \end{cases}$$

Proof. Since $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, a must be the root of an irreducible polynomial $X^2 - cX + d$. If $c = 0$ and $-d \in \square_q^*$, then $a \in \mathbb{F}_q$, a contradiction. Now suppose $c \neq 0$. Since $ca - d \in \square_{q^2}^*$, an appeal to Lemma 8 establishes the remaining claims. □

Theorem 1 is established in the following two lemmas.

Lemma 10. *Let $q \geq 5$ and suppose $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ satisfies $a^2 = -d$ for some $-d \in \square_q$. The following statements hold.*

(i) $\mathcal{S}_a \cap \square_{q^2} = \varnothing$ if and only if $q = 5$ and $a^2 = 3$.

(ii) $\mathcal{S}_a \cap \square_{q^2} = \varnothing$ if and only if $q = 5$ and $a^2 = 2$.

Proof. We first note

$$\begin{aligned} \mathcal{T}a &= \{\beta a^2 - \alpha a : (\alpha, \beta \in \mathbb{F}_q) \wedge (\beta\alpha \in \square_q^*)\} \\ &= \{-\alpha a - \beta d : (\alpha, \beta \in \mathbb{F}_q) \wedge (\beta\alpha \in \square_q^*)\} \\ &= \{\beta' a - \alpha' : (\alpha', \beta' \in \mathbb{F}_q) \wedge (\beta'\alpha' \in \square_q)\}. \end{aligned}$$

Hence $\mathcal{T} \cap \mathcal{T}a = \varnothing$.

As $a^2 \in \mathbb{F}_q$ and $a \notin \mathbb{F}_q$, we have $a^{q-1} = -1$. Consequently, $a^{(q^2-1)/2} = (-1)^{(q+1)/2}$, so that $a \in \square_{q^2}$ if $q \equiv 3 \bmod 4$ and $a \in \square_{q^2}$ if $q \equiv 1 \bmod 4$.

Suppose $q \equiv 3 \bmod 4$, so that $a \in \square_{q^2}$. By Lemma 8, we need only consider the case where $\mathcal{S}_a \cap \square_{q^2} = \varnothing$. If this holds, then $\mathcal{T} \cup \mathcal{T}a \subseteq \square_{q^2}$, and $|\mathcal{T}| + |\mathcal{T}a| = (q-1)^2 \leq \frac{q^2-1}{2}$, so that $q \leq 3$, the degenerate case we need not consider.

Now suppose $q \equiv 1 \bmod 4$, so that $a \in \square_{q^2}$. Consider $x^2 - a$ with $x \in \mathbb{F}_q$. Let $\mathsf{N}(x) = x^{1+q}$ denote the norm from $\mathbb{F}_{q^2}$ into $\mathbb{F}_q$. Then

$$\mathsf{N}(x^2 - a) = (x^2 - a)(x^2 - a)^q = (x^2 - a)(x^2 + a) = x^4 - a^2 = x^4 + d.$$

Now $\mathsf{N}(x) \in \square_q^*$ if and only if $x \in \square_{q^2}^*$. Set $f(X, Y) = X^4 + d - Y^2$ and let $\mathcal{C}$ be the number of solutions $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ satisfying $f(x, y) = 0$. By the above argument, we have

$$\mathcal{C} = \begin{cases} 0 & \text{if } \mathcal{S}_a \cap \square_{q^2} = \varnothing, \\ 2(q-1) & \text{if } \mathcal{S}_a \cap \square_{q^2} = \varnothing. \end{cases}$$

However, since $X^4 + d$ is not a square, $f(X, Y)$ is absolutely irreducible, and so by [9, page 70], $|\mathcal{C} - q| < 3\sqrt{q}$. Thus $q = 5$ is forced if $\mathcal{S}_a \cap \square_{q^2} = \varnothing$, while $q \in \{5, 9\}$ if $\mathcal{S}_a \cap \square_{q^2} = \varnothing$. It is easily checked the only cases where either situation arises occurs when $q = 5$, with $d = 2, 3$ leading to the two claimed cases. □

Lemma 11. *Let $q \geq 5$ and suppose $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ satisfies $a^2 = ca - d$ with $c \neq 0$. The following statements hold.*

(i) $\mathcal{S}_a \cap \square_{q^2} = \varnothing$ if and only if $q = 5$ and $(c, d) \in \{(2, -1), (3, -1)\}$.

(ii) $\mathcal{S}_a \cap \square_{q^2} \neq \varnothing$.

Proof. Since $a^2 = ca - d$, we have

$$\begin{aligned}\mathcal{T}a &= \{\beta a^2 - \alpha a : (\alpha, \beta \in \mathbb{F}_q) \wedge (\beta\alpha \in \square_q^*)\} \\ &= \{(\beta c - \alpha)a - \beta d : (\alpha, \beta \in \mathbb{F}_q) \wedge (\beta\alpha \in \square_q^*)\}.\end{aligned}$$

There are two cases, depending on whether or not $a \in \square_{q^2}$.

- *First case:* $a \in \boxslash_{q^2}$

  Let $a \in \boxslash_{q^2}$. If either $\mathcal{S}_a \cap \square_{q^2} = \varnothing$ or $\mathcal{S}_a \cap \boxslash_{q^2} = \varnothing$, then $\mathcal{T} \cap \mathcal{T}a = \varnothing$ follows from Lemma 8. Thus $\beta c - \alpha = 0$ or $(\beta c - \alpha)(\beta d) \in \boxslash_q$ whenever $\beta\alpha \in \square_q^*$. Fix $\alpha \in \boxslash_q$ and consider the set

  $$B_\alpha = \{\beta c - \alpha : \beta \in \boxslash_q\} \setminus \{0\}.$$

  Note that

  $$|B_\alpha| = \begin{cases} \frac{q-3}{2} & \text{if } c \in \square_q^*, \\ \frac{q-1}{2} & \text{if } c \in \boxslash_q. \end{cases}$$

  Suppose first that $d \in \square_q^*$. We must have $B_\alpha \subset \square_q^*$. Consequently, if $c \in \square_q^*$, α can be written in $\frac{q-3}{2}$ ways as a non-square of $\mathbb{F}_q$ subtract a square of $\mathbb{F}_q^*$. Thus, if $c \in \square_q^*$, $ns_\alpha = \frac{q-3}{2}$, and comparing with Lemma 7, we find $q = 3$, the degenerate case. If $c \in \boxslash_q$, α can be written in $\frac{q-1}{2}$ ways as a difference of squares in $\mathbb{F}_q$. Now Lemma 5 shows

  $$\frac{q-1}{2} = \begin{cases} \frac{q-1}{4} & \text{if } q \equiv 1 \bmod 4, \\ \frac{q-3}{4} & \text{if } q \equiv 3 \bmod 4. \end{cases}$$

  Both cases lead to a contradiction.

  Now suppose $d \in \boxslash_q$, so that $B_\alpha \subset \boxslash_q$. If $c \in \boxslash_q$, then α can be written in $\frac{q-1}{2}$ ways as a square of $\mathbb{F}_q^*$ subtract a non-square of $\mathbb{F}_q^*$. Hence $sn_\alpha = \frac{q-1}{2}$. Lemma 7 now implies $q = 3$, which we can ignore. If $c \in \square_q^*$, α can be written in $\frac{q-3}{2}$ ways as a difference of two non-squares of $\mathbb{F}_q$. Again we appeal to Lemma 5 and find $q = 3$ or $q = 5$. Ignoring the former case, for $q = 5$, we find $c \in \{1, 4\}$ and $d = 2$. Direct computation now shows precisely one of $a + 1$ or $a - 1$ is a square and so $|\mathcal{S}_a \cap \boxslash_{q^2}| = |\mathcal{S}_a \cap \square_{q^2}| = 1$.

- *Second case:* $a \in \square_{q^2}$

  Now let $a \in \square_{q^2}$. Note that, by Lemma 8, we cannot have $\mathcal{S}_a \cap \boxslash_{q^2} = \varnothing$, so we may assume $\mathcal{S}_a \cap \square_{q^2} = \varnothing$. Hence $|\mathcal{T} \cup \mathcal{T}a| \leq \frac{q^2-1}{2}$, and an application of the Inclusion/Exclusion principle shows $|\mathcal{T} \cap \mathcal{T}a| \geq \frac{(q-1)(q-3)}{2}$. Thus $(\beta c - \alpha)(\beta d) \in \square_q^*$ for at least $\frac{(q-1)(q-3)}{2}$ choices of $\alpha, \beta \in \mathbb{F}_q^*$ satisfying $\beta\alpha \in \square_q^*$. For $\beta \in \mathbb{F}_q^*$, set

  $$A_\beta = \{\beta a - \alpha : (\alpha \in \mathbb{F}_q) \wedge (\beta\alpha \in \square_q^*) \wedge ((\beta c - \alpha)(\beta d) \in \square_q^*)\}.$$

  Clearly, $|A_\beta| \leq \frac{q-1}{2}$. Since $A_{\beta_1} \cap A_{\beta_2} = \varnothing$ whenever $\beta_1 \neq \beta_2$ and

  $$\bigcup_{\beta \in \mathbb{F}_q^*} A_\beta = \mathcal{T} \cap \mathcal{T}a,$$

  it follows that the average order of A_β is at least $\frac{q-3}{2}$. In particular, there must exist a β_0 for which $|A_{\beta_0}| \geq \frac{q-3}{2}$. In this case, $\beta_0^2 cd = \beta_0\alpha d + s_\alpha$, $s_\alpha \in \square_q^*$, for at least $(q-3)/2$ choices of α satisfying $\beta_0\alpha \in \square_q^*$.

  If $d \in \square_q^*$, then $\beta_0^2 cd$ can be written as a sum of two squares in at least $\frac{q-3}{2}$ ways. Comparing with Lemma 6, we see $c \in \boxslash_q$ and $q = 5$ must hold. In this case, $cd \in \boxslash_q$ and $X^2 - cX + d$ is irreducible, and combining with Lemma 9 we find $(c, d) \in \{(2, -1), (3, -1)\}$ and $\mathcal{S}_a \cap \square_{q^2} = \varnothing$ in each case.

If $d \in \boxslash_q$, then $\beta_0^2 cd$ can be written as the sum of a square and a non-square of $\mathbb{F}_q$ in at least $\frac{q-3}{2}$ ways. If $q \equiv 3 \bmod 4$, then this is the same as writing $\beta_0^2 cd$ as the difference of two squares, implying $q = 3$ by Lemma 5, the trivial case. If $q \equiv 1 \bmod 4$, then this is the same as writing $\beta_0^2 cd$ as the difference of a square and a non-square, so that $q = 5$ is forced by Lemma 7. One now easily checks that every permissible case leads to precisely one of $a + 1$ or $a - 1$ being a square, so that $|\mathcal{S}_a \cap \boxslash_{q^2}| = |\mathcal{S}_a \cap \square_{q^2}| = 1$.

□

§ 4. Final remarks

There are several points we should mention. Our result is equivalent to showing that the number of solutions $N(a)$ of $x^2 + y^{2(q+1)} = a$ satisfies $N(a) > 0$ if $a \in \boxslash_{q^2}$ and $N(a) > 2$ if $a \in \square_{q^2}$. General methods for estimating the number of solutions of such equations do exist and some are outlined in [7]. However, these methods only appear to yield $N(a) \geq 0$ or $N(a) \geq 2$. It is possible that more careful application of these methods might yield results stronger than our Theorem 1 (indeed, we believe that the intersection of S_a with both $\square_{q^2}^*$ and $\boxslash_{q^2}$ should generally increase as one increases q). Additionally, the number of irreducible polynomials with some coefficients fixed has been studied extensively. These results are, however, generally most effective for polynomials of large degree. One can, of course, argue directly about irreducible quadratic polynomials over fields of odd characteristic, and note that for any choice of $a \in \mathbb{F}_q$, the number of $b \in \mathbb{F}_q^*$ for which $X^2 - aX + b$ is irreducible is $(q-1)/2$. This does not, however, say anything about the existence of an irreducible quadratic where there is a specified, restricted relationship between the constant and linear terms.

We thank the anonymous referee, whose comments significantly improved the exposition, particularly the transparency of the proofs of Lemmas 8 and 10.

References

[1] R.H. Bruck, *Difference sets in a finite group*, Trans. Amer. Math. Soc. **78** (1955), 464–481.

[2] R.S. Coulter and T. Gutekunst, *Subsets of finite groups exhibiting additive regularity*, submitted.

[3] T. Gutekunst, *Subsets of finite groups exhibiting additive regularity*, Ph.D. thesis, Department of Mathematical Sciences, University of Delaware, USA, 2008.

[4] P. Kosick, *Commutative semifields of odd order and planar Dembowski-Ostrom polynomials*, Ph.D. thesis, Department of Mathematical Sciences, University of Delaware, USA, 2009.

[5] C.W.H. Lam, *A generalization of cyclic difference sets I*, J. Combin. Theory Ser. A **19** (1975), 51–65.

[6] ———, *A generalization of cyclic difference sets II*, J. Combin. Theory Ser. A **19** (1975), 177–191.

[7] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983, (now distributed by Cambridge University Press).

[8] A.R. Prince, *Sum uniform subsets of the integers modulo p and an application to finite fields*, Finite Fields Appl. **13** (2007), 793–79.

[9] W.M. Schmidt, *Equations over Finite Fields: An Elementary Approach*, Lecture Notes in Mathematics, vol. 536, Springer-Verlag, 1976.

[10] J.S. Sumner and A.T. Butson, *Addition sets in a finite group*, J. Combin. Theory Ser. A **32** (1982), 350–369.