Bull. Aust. Math. Soc. (First published online 2024), page 1 of 8*
doi:10.1017/S0004972724000698
*Provisional—final page numbers to be inserted when paper edition is published

ON CONSECUTIVE RESIDUES AND NONRESIDUES UNDER A LINEAR MAP IN A FINITE FIELD

EMILY BERGMAN, ROBERT S. COULTER✉ and BRADLEY FAIN

(Received 8 June 2024; accepted 11 June 2024)

Abstract

For fixed m and a, we give an explicit description of those subsets of $\mathbb{F}_q$, q odd, for which both x and $mx + a$ are quadratic residues (and other combinations). These results extend and refine results that date back to Gauss.

2020 *Mathematics subject classification*: primary 11T30; secondary 11A07.

Keywords and phrases: quadratic residues, finite fields.

1. Introduction

Let p be an odd prime and q a power of p. We use $\mathbb{F}_q$ to denote the finite field of order q. Throughout, ζ denotes a primitive element of $\mathbb{F}_q$, so that $\langle\zeta\rangle = \mathbb{F}_q^\star$, the set of nonzero elements of $\mathbb{F}_q$. We also use $\square_q$ and $\boxslash_q$ to denote the squares and nonsquares, respectively, of $\mathbb{F}_q$. The *quadratic character* η over $\mathbb{F}_q$ is the finite field extension of the Legendre symbol:

$$\eta(x) = \begin{cases} 1 & \text{if } x \in \square_q^*, \\ -1 & \text{if } x \in \boxslash_q, \\ 0 & \text{if } x = 0. \end{cases}$$

The problem of considering when an element and a linear translate of that element are both quadratic residues dates back at least to Gauss. Davenport comments in [2, page 63] that Gauss determined the number of pairs $x, x+1 \in \mathbb{F}_p^\star$ for which x and $x+1$ had prescribed characters. Of course, these results have since been extended to arbitrary fields: for example, Dickson gives the generalisation for square x in [3, Theorem 67]. Davenport ascribes the full enumeration over arbitrary fields to Dickson also. More modern treatments of this count were given by Raber [8] and Ralston [9] in the 1970s. In 2002, Sun [10] gave an explicit description of those x in $\mathbb{F}_p$ for which x and $x+1$ were both squares or both nonsquares, thereby extending the original

The second author gratefully acknowledges a bequest from the Estate of Francisco 'Pancho' Sayas, which partially supported this research.

results of Gauss. In this note, we extend Sun's results to all finite fields and all possible prescribed character values, and for any linear translate.

To be more precise, let us fix $m, a \in \mathbb{F}_q^\star$. We define four subsets of $\mathbb{F}_q^\star$:

$$\begin{aligned}
K_1(a, m) &= \{x : \eta(x) = \eta(mx + a) = 1\},\\
K_2(a, m) &= \{x : \eta(x) = \eta(mx + a) = -1\},\\
K_3(a, m) &= \{x : \eta(x) = -1,\ \eta(mx + a) = 1\},\\
K_4(a, m) &= \{x : \eta(x) = 1,\ \eta(mx + a) = -1\}.
\end{aligned}$$

The historical results described above all relate to the sets $K_i(1, 1)$. As mentioned, Sun gave explicit descriptions of the sets $K_1(1, 1)$ and $K_2(1, 1)$ over prime fields in [10]. Here, we provide an explicit description of each of the sets $K_i(a, m)$ for any nonzero a, m in any finite field. To do so, we first show how to relate each of these sets to an explicit description of $K_i(1, 1)$ and then give a complete description of the sets $K_i(a, m)$. The reduction to $K_i(1, 1)$ is shown in the next section. The explicit descriptions of the sets $K_i(a, m)$ over an arbitrary finite field of odd order are given in Section 3. As shall be seen, the main tool used to obtain these descriptions is the 'S-set' representation of a finite field (see Lemma 3.1), which allows for a uniform treatment of all the sets $K_i(a, m)$.

2. Reduction process

Our first step is to reduce our problem to dealing with the sets $K_i(1, 1)$. The reduction step is completely reversible so that having complete descriptions of the sets $K_i(1, 1)$ suffices for our purposes.

The first and simplest reductions are those reductions involving m. As might be expected, these reductions split based on the value of $\eta(m)$.

LEMMA 2.1. *Let $\mathbb{F}_q$ be a finite field and $a, m \in \mathbb{F}_q^\star$.*

(i) *If $\eta(m) = 1$, then*

$$K_i(a, m) = m^{-1}K_i(a, 1).$$

(ii) *If $\eta(m) = -1$, then*

$$\begin{aligned}
K_1(a, m) &= m^{-1}K_3(a, 1),\\
K_2(a, m) &= m^{-1}K_4(a, 1),\\
K_3(a, m) &= m^{-1}K_1(a, 1),\\
K_4(a, m) &= m^{-1}K_2(a, 1).
\end{aligned}$$

PROOF. Suppose $\eta(m) = 1$. Then, $\eta(x) = \eta(mx)$ for all $x \in \mathbb{F}_q$. So, if $x \in K_i(a, m)$, then $mx \in K_i(a, 1)$ and *vice versa*. Thus, $K_i(a, m) = m^{-1}K_i(a, 1)$ for $i = 1, 2, 3, 4$.

For the remainder, assume $\eta(m) = -1$. If $x \in K_1(a, m)$, then $\eta(x) = 1 = \eta(mx + a)$. Since $\eta(m) = -1$, $\eta(mx) = -1$. Hence, $mx \in K_3(a, 1)$. Thus, $K_1(a, m) = m^{-1}K_3(a, 1)$. The other three cases follow similarly. □

https://doi.org/10.1017/S0004972724000698 Published online by Cambridge University Press

We now deal with the reduction of the a. In light of the previous lemma, we may restrict ourselves to reducing the sets $K_i(a, 1)$. For ease of notation, we denote $K_i(a, 1)$ by $K_i(a)$ for $i = 1, \ldots, 4$.

LEMMA 2.2. *Let $a \in \mathbb{F}_q^\star$. The following statements hold.*

(i) *If $\eta(a) = 1$, then*

$$K_i(a) = aK_i(1).$$

(ii) *If $\eta(a) = -1$, then*

$$\begin{aligned} K_1(a) &= aK_2(1), \\ K_2(a) &= aK_1(1), \\ K_3(a) &= aK_4(1), \\ K_4(a) &= aK_3(1). \end{aligned}$$

PROOF. First, notice that $\eta(x) = \eta(a)\eta(a^{-1}x)$ and $\eta(x + a) = \eta(a)\eta(a^{-1}x + 1)$.

If $\eta(a) = 1$, then $x \in K_i(a)$ implies $a^{-1}x \in K_i(1)$ as $\eta(x) = \eta(a^{-1}x)$ and $\eta(x + a) = \eta(a^{-1}x + 1)$.

Now suppose $\eta(a) = -1$. As with the previous lemma, we prove one equality, with the others following nearly identically. Let $x \in K_3(a)$. Then, $\eta(x) = -1$ and $\eta(x + a) = 1$. So $\eta(a^{-1}x) = 1$ and $\eta(a^{-1}x + 1) = -1$ and hence, $a^{-1}x \in K_4(1)$. □

3. Explicit representations

We now move to providing the explicit representations of the sets $K_i(1)$. Our results make use of the following useful partition of a finite field. We provide a proof for completeness.

LEMMA 3.1. *Let q be an odd prime power and $a \in \mathbb{F}_q^\star$.*

(1) *If $a \in \square_q^*$, then $\mathbb{F}_q = S_0(a) \cup S_1(a) \cup S_2(a)$, where*

$$\begin{aligned} S_0(a) &= \{\pm 2\sqrt{a}\}, \\ S_1(a) &= \{u + au^{-1} : u \in \mathbb{F}_{q^2} \text{ and } u^{q-1} = 1 \text{ and } u \neq \pm\sqrt{a}\}, \\ S_2(a) &= \{u + au^{-1} : u \in \mathbb{F}_{q^2} \text{ and } u^{q+1} = a \text{ and } u \neq \pm\sqrt{a}\}. \end{aligned}$$

(2) *If $a \in \boxtimes_q$, then $\mathbb{F}_q = S_1(a) \cup S_2(a)$, where*

$$\begin{aligned} S_1(a) &= \{u + au^{-1} : u \in \mathbb{F}_{q^2} \text{ and } u^{q-1} = 1\} \\ S_2(a) &= \{u + au^{-1} : u \in \mathbb{F}_{q^2} \text{ and } u^{q+1} = a\}. \end{aligned}$$

PROOF. We first show that for fixed $a \in \mathbb{F}_q^\star$, any $x \in \mathbb{F}_q$ can be written as $x = u + au^{-1}$ for some $u \in \mathbb{F}_{q^2}^\star$ with $u^{q-1} = 1$ or $u^{q+1} = a$. To see this, consider the quadratic polynomial $Y^2 - xY - a$ over $\mathbb{F}_q$. This factorises completely in $\mathbb{F}_{q^2}$. Let $u \in \mathbb{F}_{q^2}$ be a root of $Y^2 - xY - a$, that is to say, $u^2 - xu + a = 0$ and note that $u \neq 0$ as $a \neq 0$. Isolating x,

https://doi.org/10.1017/S0004972724000698 Published online by Cambridge University Press

we have $x = u + au^{-1}$, where $u \in \mathbb{F}_{q^2}$. As $x \in \mathbb{F}_q$, we have $x^q = x$, from which we obtain $u^q + au^{-q} = u + au^{-1}$, and rearranging yields

$$0 = u^{2q+1} - u^{q+2} - au^q + au = u(u^{q-1} - 1)(u^{q+1} - a).$$

Thus, $u^{q-1} = 1$ or $u^{q+1} = a$.

Now suppose $a \in \square_q$. We have $x = u + au^{-1}$ for $u \in \mathbb{F}_{q^2}^\star$. If $x \in S_0$, then $x = \pm 2\sqrt{a}$. Therefore, $\pm 2\sqrt{a} = u + au^{-1}$, or multiplying through by u and rearranging, $u^2 - \pm 2\sqrt{a}u + a = 0$. Factoring gives $(u - \pm\sqrt{a})^2 = 0$, or in other words, $u = \pm\sqrt{a}$. It follows that S_0 is disjoint from both S_1 and S_2.

It remains to show S_1 and S_2 are disjoint. Suppose $x \in S_1 \cap S_2$. Then, $x = u + au^{-1}$ for some $u \in \mathbb{F}_{q^2}^\star$ with $u^{q-1} = 1$ and where $u \neq \pm\sqrt{a}$. Also, $x = v + av^{-1}$ for some $v \in \mathbb{F}_{q^2}^\star$ with $v^{q+1} = a$ and where $v \neq \pm\sqrt{a}$. So we have $u + au^{-1} = v + av^{-1}$, or multiplying through by uv and rearranging, $uv(u - v) = a(u - v)$. So $u = v$ or $uv = a$. If $u = v$, then $1 = u^{q-1} = v^{q-1}$. Therefore, $v^{q+1} = v^2 = a$, which implies $v = \pm\sqrt{a}$, so that $x \in S_0$, which is a contradiction. If $uv = a$, then we again find $v^{q-1} = 1$, which we know produces a contradiction. So, $S_1 \cap S_2 = \varnothing$ and $\mathbb{F}_q = S_0 \cup S_1 \cup S_2$ where the S-sets are pairwise disjoint. The case where $a \in \boxslash_q$ is almost the same, except that we no longer have the set S_0 to contend with. $\square$

The S-set representation of a finite field is certainly not new and has been used in a number of places over time. While it may appear so, it is not necessary to work in the quadratic extension, as you can compute S_0 (when required) and S_1 from within $\mathbb{F}_q$ as $u \in \mathbb{F}_q^\star$ for S_1. One can then obtain S_2 as the complement. A specific and important instance of their application has been in the study of the Dickson polynomials of the first and second kind. The functional behaviour of both polynomial classes is intimately tied to the S-sets. Indeed, practically all of the permutation polynomial results for either class have relied specifically on the S-sets. (See Nöbauer [7] for a full classification of permutation polynomials among the Dickson polynomials of the first kind, and Henderson [4], Henderson and Matthews [5, 6] and Coulter and Matthews [1] for establishing classes of permutation polynomials among the Dickson polynomials of the second kind.) We note, in passing, that Henderson and Matthews made a conjecture in [6] concerning permutation polynomials among the Dickson polynomials of the second kind that remains unresolved.

Our main results will make use of the partition of $\mathbb{F}_q$ given in Lemma 3.1 as it allows us to obtain a consistent form for all four sets. Below, when we write $S_i^\star$, we mean the nonzero elements of S_i, though it is not necessarily the case that 0 will lie in the set S_i. We start with the explicit descriptions of the sets $K_i(1)$, which are given in the following two theorems.

THEOREM 3.2. *For arbitrary odd q,*

$$K_1(1) = \{\tfrac{1}{4}\alpha^2 : \alpha \in S_1^\star(-1)\} \quad \text{and} \quad K_4(1) = \{\tfrac{1}{4}\alpha^2 : \alpha \in S_2^\star(-1)\}.$$

https://doi.org/10.1017/S0004972724000698 Published online by Cambridge University Press

PROOF. For ease, define

$$A = \{\tfrac{1}{4}\alpha^2 : \alpha \in S_1^\star(-1)\} \quad \text{and} \quad B = \{\tfrac{1}{4}\alpha^2 : \alpha \in S_2^\star(-1)\}.$$

Lemma 3.1 shows that the sets A and B contain all nonzero squares except for -1 when -1 is a square. So we have $K_1(1) \cup K_4(1) = A \cup B$. Now if $a \in A$, then $a = \frac{1}{4}(u - u^{-1})^2$ for some u such that $u \in \mathbb{F}_q$. So we can rewrite

$$a = \tfrac{1}{4}(\zeta^k - \zeta^{-k})^2$$

for some primitive element ζ of $\mathbb{F}_q$ and integer k. From here, we can see that $a + 1 = \frac{1}{4}(\zeta^k + \zeta^{-k})^2$ which is a square in $\mathbb{F}_q$, so that $A \subseteq K_1(1)$. It now suffices to show that $\#K_1(1) = \#A$. Towards this end, consider $S_1^\star(-1)$. If $q \equiv 1 \pmod 4$, then -1 is a square in $\mathbb{F}_q$ so $\#S_1^\star(-1) = \frac{1}{2}(q-3) - 1$. Similarly, if $q \equiv -1 \pmod 4$, then $\#S_1^\star(-1) = \frac{1}{2}(q-1) - 1$. Since $S_1^\star(-1)$ is closed under negation, we have $\#A = \frac{1}{2}\#S_1^\star(-1)$ and thus $A = K_1(1)$ in each case by [9]. This then gives $B = K_4(1)$ since A and B are disjoint. □

THEOREM 3.3. *Let ζ be a primitive element of $\mathbb{F}_q$. Then,*

$$K_2(1) = \left\{\frac{1}{4\zeta}\alpha^2 : \alpha \in S_1^\star(-\zeta)\right\} \quad \textit{and} \quad K_3(1) = \left\{\frac{1}{4\zeta}\alpha^2 : \alpha \in S_2^\star(-\zeta)\right\}.$$

PROOF. Let

$$A = \left\{\frac{1}{4\zeta}\alpha^2 : \alpha \in S_1^\star(-\zeta)\right\} \quad \text{and} \quad B = \left\{\frac{1}{4\zeta}\alpha^2 : \alpha \in S_2^\star(-\zeta)\right\}.$$

Similar to Theorem 3.2, we can see that $A \cup B = K_2(1) \cup K_3(1)$ and that $A \cap B = \emptyset$. Let $a \in A$. Then, $a = \frac{1}{4\zeta}(\zeta^k - \zeta^{1-k})^2$ for some integer k, and thus,

$$a + 1 = \frac{1}{4\zeta}(\zeta^k + \zeta^{1-k})^2.$$

So we have $A \subseteq K_2(1)$. To finish the proof, we need only show that $\#A = \#K_1(1)$.

Again, consider $S_1^\star(-\zeta)$. If $q \equiv 1 \pmod 4$, then $-\zeta$ is a nonsquare, so $\#S_1^\star(-\zeta) = \frac{1}{2}(q-1)$ since $S_1^\star(-\zeta) = S_1$. So $\#A = \frac{1}{4}(q-1)$ and $\#B = \frac{1}{4}(q-1)$. If $q \equiv 3 \pmod 4$, then $-\zeta$ is a square and so $\#S_1^\star(-\zeta) = \frac{1}{2}(q-3)$, and so $\#A = \frac{1}{4}(q-3)$ and $\#B = \frac{1}{4}(q-3)$ giving $A = K_2(1)$ and $B = K_3(1)$. □

A nearly identical proof to the two above yields the following corollary, though you could also use Lemma 2.2.

THEOREM 3.4. *Let $\mathbb{F}_q$ be a finite field, ζ a primitive element of $\mathbb{F}_q$, and $a \in \mathbb{F}_q^\star$. Then,*

$$K_1(a) = \{\tfrac{1}{4}\alpha^2 : \alpha \in S_1^\star(-a)\},$$
$$K_2(a) = \left\{\frac{1}{4\zeta}\alpha^2 : \alpha \in S_1^\star(-a\zeta)\right\},$$

https://doi.org/10.1017/S0004972724000698 Published online by Cambridge University Press

$$K_3(a) = \left\{\frac{1}{4\zeta}\alpha^2 : \alpha \in S_2^\star(-a\zeta)\right\},$$
$$K_4(a) = \{\tfrac{1}{4}\alpha^2 : \alpha \in S_2^\star(-a)\}.$$

We now use Lemma 2.1 to get the representations of $K_i(a, m)$.

THEOREM 3.5. *Let $\mathbb{F}_q$ be a finite field, ζ a primitive element of $\mathbb{F}_q$, and $a, m \in \mathbb{F}_q^\star$.*

(i) *If $\eta(m) = 1$, then*

$$K_1(a, m) = \left\{\frac{1}{4m}\alpha^2 : \alpha \in S_1^\star(-a)\right\},$$
$$K_2(a, m) = \left\{\frac{1}{4m\zeta}\alpha^2 : \alpha \in S_1^\star(-a\zeta)\right\},$$
$$K_3(a, m) = \left\{\frac{1}{4m\zeta}\alpha^2 : \alpha \in S_2^\star(-a\zeta)\right\},$$
$$K_4(a, m) = \left\{\frac{1}{4m}\alpha^2 : \alpha \in S_2^\star(-a)\right\}.$$

(ii) *If $\eta(m) = -1$, then*

$$K_1(a, m) = \left\{\frac{1}{4m}\alpha^2 : \alpha \in S_2^\star(-a\zeta)\right\},$$
$$K_2(a, m) = \left\{\frac{1}{4m\zeta}\alpha^2 : \alpha \in S_2^\star(-a)\right\},$$
$$K_3(a, m) = \left\{\frac{1}{4m\zeta}\alpha^2 : \alpha \in S_1^\star(-a)\right\},$$
$$K_4(a, m) = \left\{\frac{1}{4m}\alpha^2 : \alpha \in S_1^\star(-a\zeta)\right\}.$$

Finally, Sun determined in [10] forms for $K_1(1)$ and $K_2(1)$ over prime fields. However, Sun's results do not have the same format as our general results above for $K_1(1)$ and $K_2(1)$, even when we restrict to the prime case. For completeness, we give the representations of $K_i(1)$ in terms similar to Sun's.

COROLLARY 3.6. *Let ζ be a primitive element of $\mathbb{F}_q$. Then,*

$$K_1(1) = \left\{b_k : b_k = \frac{(\zeta^{2k} - 1)^2}{4\zeta^{2k}} \text{ and } k = 1, \ldots, \left\lfloor \frac{q-3}{4} \right\rfloor\right\},$$
$$K_2(1) = \left\{b_k : b_k = \frac{(\zeta^{2k-1} - 1)^2}{4\zeta^{2k-1}} \text{ and } k = 1, \ldots, \left\lfloor \frac{q-1}{4} \right\rfloor\right\},$$
$$K_3(1) = \left\{b_k : b_k = \frac{4\zeta^{2k-1}}{(\zeta^{2k-1} - 1)^2} \text{ and } k = 1, \ldots, \left\lfloor \frac{q-1}{4} \right\rfloor\right\}.$$

https://doi.org/10.1017/S0004972724000698 Published online by Cambridge University Press

Additionally, if $q \equiv 1 \bmod 4$*, then*

$$K_4(1) = \Big\{b_k : b_k = \frac{-(\zeta^{2k-1}-1)^2}{(\zeta^{2k-1}+1)^2} \text{ and } k = 1, \ldots, \frac{q-1}{4}\Big\}.$$

PROOF. Here, $K_1(1)$ follows from the fact that

$$\frac{(\zeta^{2k}-1)^2}{4\zeta^{2k}} = \frac{1}{4\zeta}(\zeta^k - \zeta^{-k})^2$$

and we have seen that this is exactly the form of $K_1(1)$ from Theorem 3.2. Similarly, $K_2(1)$ follows from the fact that

$$\frac{(\zeta^{2k-1}-1)^2}{4\zeta^{2k-1}} = \frac{1}{4\zeta}(\zeta^k - \zeta^{1-k})^2$$

as seen in Theorem 3.3, and $K_3(1)$ follows from the fact that

$$\frac{1}{x} + 1 = \frac{1+x}{x},$$

and so if $x \in K_2(1)$, then $x^{-1} \in K_3(1)$ and *vice versa*.

To finish, for $K_4(1)$, -1 is a square when $q \equiv 1 \bmod 4$ and we can write

$$\frac{-1}{x} - 1 = \frac{1+x}{x} = \frac{-(-1-x)}{x}.$$

Now, we see $x \in K_4(1)$ if and only if $-1 - x^{-1} \in K_3(1)$ and some simple arithmetic produces the claimed description. □

We note that this second 'explicit' format, as given in Corollary 3.6, is missing the $q \equiv 3 \bmod 4$ case for $K_4(1)$. The tricks we have used here do not work for this last case where $-1 \in \boxslash_q$, as they end up producing another element in K_4. In particular, we find that when $q \equiv 3 \bmod 4$, $x \in K_4(1)$ if and only if $-1 - x^{-1} \in K_4(1)$. While this gives us some structural information about $K_4(1)$, it does not appear to lead to an explicit description of its elements in the format of Corollary 3.6.

Acknowledgement

The authors gratefully acknowledge the contribution of an anonymous referee, whose suggestions both improved the exposition and provided a cleaner explanation of how the representation of $K_4(1)$ just given follows from the results in this paper.

References

[1] R. S. Coulter and R. W. Matthews, 'On the permutation behaviour of Dickson polynomials of the second kind', *Finite Fields Appl.* **8** (2002), 519–530.

[2] H. Davenport, *The Higher Arithmetic*, 8th edn (Cambridge University Press, Cambridge, 2008).

[3] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory* (B. G. Teubner, Leipzig, 1901).

[4] M. Henderson, 'A note on the permutation behaviour of the Dickson polynomials of the second kind', *Bull. Aust. Math. Soc.* **56** (1997), 499–505.

[5] M. Henderson and R. Matthews, 'Permutation properties of Chebyshev polynomials of the second kind over a finite field', *Finite Fields Appl.* **1** (1995), 115–125.
[6] M. Henderson and R. Matthews, 'Dickson polynomials of the second kind which are permutation polynomials over a finite field', *New Zealand J. Math.* **27** (1998), 227–244.
[7] W. Nöbauer, 'Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen', *J. reine angew. Math.* **231** (1968), 215–219.
[8] N. C. Raber, 'A geometric approach to counting distribution of squares in a finite field', *Geom. Dedicata* **4** (1975), 297–303.
[9] T. Ralston, 'On the distribution of squares in a finite field', *Geom. Dedicata* **8** (1979), 207–212.
[10] Z.-H. Sun, 'Consecutive numbers with the same Legendre symbol', *Proc. Amer. Math. Soc.* **130** (2002), 2503–2507.

EMILY BERGMAN,
600 Seena Road, Essex, MD 21221, USA
e-mail: emilybergman2011@gmail.com

ROBERT S. COULTER, Department of Mathematical Sciences,
University of Delaware, Newark, DE 19716, USA
e-mail: coulter@udel.edu

BRADLEY FAIN,
6969 West 90th Ave, Apt 933, Westminster, CO 80021, USA
e-mail: fain.bradley@gmail.com

https://doi.org/10.1017/S0004972724000698 Published online by Cambridge University Press