CUBO, A Mathematical Journal
Vol. 24, no. 01, pp. 95–103, April 2022
DOI: 10.4067/S0719-06462022000100095

A characterization of $\mathbb{F}_q$-linear subsets of affine spaces $\mathbb{F}_{q^2}^n$

Edoardo Ballico[1]

[1] *Department of Mathematics, University of Trento, 38123 Povo (TN), Italy.*
edoardo.ballico@unitn.it

ABSTRACT

Let q be an odd prime power. We discuss possible definitions over $\mathbb{F}_{q^2}$ (using the Hermitian form) of circles, unit segments and half-lines. If we use our unit segments to define the convex hulls of a set $S \subset \mathbb{F}_{q^2}^n$ for $q \notin \{3, 5, 9\}$ we just get the $\mathbb{F}_q$-affine span of S.

RESUMEN

Sea q una potencia de primo impar. Discutimos posibles definiciones sobre $\mathbb{F}_{q^2}$ (usando la forma Hermitiana) de círculos, segmentos unitarios y semi-líneas. Si usamos nuestros segmentos unitarios para definir las cápsulas convexas de un conjunto $S \subset \mathbb{F}_{q^2}^n$ para $q \notin \{3, 5, 9\}$ simplemente obtenemos el $\mathbb{F}_q$-generado afín de S.

Keywords and Phrases: Finite field, Hermitian form.

2020 AMS Mathematics Subject Classification: 15A33; 15A60; 12E20.

Accepted: 27 December, 2021
Received: 17 May, 2021

1 Introduction

Fix a prime p and a p-power q. There is a unique (up to isomorphism) field $\mathbb{F}_q$ with $\#\mathbb{F}_q = q$. The field $\mathbb{F}_{q^2}$ is a degree 2 Galois extension of $\mathbb{F}_q$ and the Frobenius map $t \mapsto t^q$ is a generator of the Galois group of this extension. This map allows the definition of the Hermitian product $\langle\ ,\ \rangle : \mathbb{F}_{q^2}^n \times \mathbb{F}_{q^2}^n \longrightarrow \mathbb{F}_{q^2}$ in the following way: if $u = (u_1, \dots, u_n) \in \mathbb{F}_{q^2}^n$ and $v = (v_1, \dots, v_n) \in \mathbb{F}_{q^2}^n$, then set $\langle u, v\rangle = \sum_{i=1}^n u_i^q v_i$. The degree $q+1$ hypersurface $\{\langle (x_1, \dots, x_n),\ (x_1, \dots, x_n)\rangle = 0\}$ is the famous full rank Hermitian hypersurface ([11, Ch. 23]).

In the quantum world the classical Hermitian product over the complex numbers is fundamental. The Hermitian product $\langle\ ,\ \rangle$ is one of the tools used to pass from a classical code over a finite field to a quantum code ([17, pp. 430–431], [14, Introduction], [20, §2.2]).

The Hermitian product was used to define the numerical range of a matrix over a finite field ([1, 2, 3, 4, 8]) by analogy with the definition of numerical range for complex matrices ([9, 12, 13, 21]). Over $\mathbb{C}$ a different, but equivalent, definition of numerical range is obtained as the intersection of certain disks ([5, §15, Lemma 1]). It is an important definition, because it was used to extend the use of numerical ranges to rectangular matrices ([7]) and to tensors ([16]). This different definition immediately gives the convexity of the numerical range of complex matrices. Motivated by that definition we look at possible definitions of the unit disk of $\mathbb{F}_{q^2}$. It should be a union of circles with center at 0 and with squared-radius in the unit interval $[0, 1] \subset \mathbb{F}_q$.

For any $c \in \mathbb{F}_q$ and any $a \in \mathbb{F}_{q^2}$ set

$$C(0, c) := \{z \in \mathbb{F}_{q^2} \mid z^{q+1} = c\}, \quad C(a, c) := a + C(0, c).$$

We say that $C(a, c)$ is the *circle of* $\mathbb{F}_{q^2}$ *with center* a *and squared-radius* c. Note that $C(a, 0) = \{a\}$ and $\#C(a, c) = q + 1$ for all $c \in \mathbb{F}_q \setminus \{0\}$.

Circles occur in the description of the numerical range of many 2×2 matrices over $\mathbb{F}_{q^2}$ ([8, Lemmas 3.4 and 3.5]). Other subsets of $\mathbb{F}_{q^2}$ (seen as a 2-dimensional vector space of $\mathbb{F}_q$) appear in [6] and are called ellipses, hyperbolas and parabolas, because they are affine conics whose projective closure have 0, 2 or 1 points in the line at infinity.

All these constructions are inside $\mathbb{F}_{q^2}$ seen as a plane over $\mathbb{F}_q$. Restricting to planes we get the following definition for $\mathbb{F}_{q^2}^n$.

Definition 1.1. *A set $E \subset \mathbb{F}_{q^2}^n$ is said to be a circle with center $0 \in \mathbb{F}_{q^2}^n$ and squared-radius c if there is an $\mathbb{F}_q$-linear embedding $f : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_{q^2}^n$ such that $E = f(C(0, c))$. A set $E \subset \mathbb{F}_{q^2}^n$ is said to be a circle with center $a \in \mathbb{F}_{q^2}^n$ and squared-radius c if $E - a$ is a circle with center 0 and squared-radius c. A set $S \subseteq \mathbb{F}_{q^2}^n$, $S \neq \emptyset$, is said to be circular with respect to $a \in \mathbb{F}_{q^2}^n$ if it contains all circles with center a which meet S.*

In the classical theory of numerical range over $\mathbb{C}$ the numerical range of a square matrix which is the orthogonal direct sum of the square matrices A and B is obtained taking the union of all segments $[a,b] \subset \mathbb{C}$ with a in the numerical range of A and b in the numerical range of B ([21, p. 3]). For the numerical range of matrices over $\mathbb{F}_{q^2}$ instead of segments $[a,b]$ one has to use the affine $\mathbb{F}_q$-span of $\{a,b\}$ ([1, Lemma 1], [8, Proposition 3.1]). We wonder if in other linear algebra constructions something smaller than $\mathbb{F}_q$-linear span occurs. A key statement for square matrices over $\mathbb{C}$ (due to Toeplitz and Hausdorff) is that their numerical range is convex ([9, Th. 1.1-2], [21, §3]). Convexity is a property over $\mathbb{R}$ and to define it one only needs the unit interval $[0,1] \subset \mathbb{R}$. Obviously $[0,1] = [0,+\infty) \cap (-\infty,1]$ and $(-\infty,1] = 1 - [0,+\infty)$. As a substitute for the unit interval $[0,1] \subset \mathbb{R}$ (resp. the half-line $[0,+\infty) \subset \mathbb{R}$) we propose the following sets I_q and I_q' (resp. E_q).

Definition 1.2. *Assume q odd. Set $E_q := \{a^2\}_{a\in\mathbb{F}_q} \subset \mathbb{F}_q$, $I_q := E_q \cap (1-E_q)$, $I_q'' := E_q \cap (1+xE_q)$ with $x \in \mathbb{F}_q \setminus E_q$, and $I_q' := I_q'' \cup \{0\}$.*

Note that $I_q' = \{0,1\} \cup (E_q \cap (1+(\mathbb{F}_q \setminus E_q))$. In the first version of this note we only used I_q, but a referee suggested that it is more natural to consider I_q''. We use I_q and I_q' because $\{0,1\} \subseteq I_q \cap I_q'$, while $0 \in I_q''$ if and only if -1 is not a square in $\mathbb{F}_q$, *i. e.* if and only if $q \equiv 3 \pmod 4$ ([10, (ix) and (x) at p. 5], [22, p. 22]). In all statements for odd q we handle both I_q and I_q'.

In the case q even we propose to use $\{a(a+1)\}_{\{a\in\mathbb{F}_q\}}$ as E_q, *i. e.* $E_q := \mathrm{Tr}^{-1}_{\mathbb{F}_q/\mathbb{F}_2}(0)$. Thus E_q is a subgroup of $(\mathbb{F}_q,+)$ of index 2. If q is even we do not have a useful definition of I_q.

Thus we restrict to odd prime powers, except for Propositions 1.8, 2.9 and Remarks 2.1 and 2.2.

We see I_q or I_q' (resp. E_q) as the *unit segment* $[0,1]$ (resp. *positive half-line starting at* 0) of $\mathbb{F}_q \subset \mathbb{F}_{q^2}$. In most of the proofs we only use that $\{0,1\} \subseteq I_q$ and that $\#I_q$ is large, say $\#I_q > (q-1)/4$.

Remark 1.3. *Note that $\#E_q = (q+1)/2$ for all odd prime powers q.*

We prove that $\#I_q = \#I_q' - 1 = (q+3)/4$ if $q \equiv 1 \mod 4$ and $\#I_q = \#I_q' = (q+5)/4$ if $q \equiv 3 \pmod 4$ (Proposition 2.3).

We only use the case $A = E_q$, $A = I_q$ and $A = I_q'$ of the following definition.

Definition 1.4. *Fix $S \subseteq \mathbb{F}_{q^2}^n$, $S \neq \emptyset$, and $A \subseteq \mathbb{F}_q$ such that $0 \in A$. We say that S is A-closed if $a + (b-a)A \subseteq S$ for all $a, b \in S$.*

In the set-up of Definition 1.4 for any $a, b \in \mathbb{F}_{q^2}^n$ the A-segment $[a,b]_A$ of $\{a,b\}$ is the set $a+(b-a)A$. Note that $[a,a]_A = \{a\}$ and that if $b \neq a$ then $b \in [a,b]_A$ if and only if $1 \in A$. If S is a subset of a real vector space and A is the unit interval $[0,1] \subset \mathbb{R}$, Definition 1.4 gives the usual notion of convexity, because $a + (b-a)t = (1-t)a + tb$ for all $t \in [0,1]$.

Remark 1.5. *Take any $A \subseteq \mathbb{F}_q$ such that $0 \in A$. Any translate by an element of $\mathbb{F}_{q^2}^n$ of an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^2}^n$ is A-closed. In particular $\mathbb{F}_q^n$ and $\mathbb{F}_{q^2}^n$ are A-closed. The intersection of A-closed sets is A-closed, if non-empty. Hence we may define the A-closure of any $S \subseteq \mathbb{F}_{q^2}^n$, $S \neq \emptyset$, as the intersection of all A-closed subsets of $\mathbb{F}_{q^2}^n$ containing S.*

In most cases I_q is not I_q-closed. We prove the following result.

Theorem 1.6. *Assume q odd. Then:*

(a) If $q \notin \{3, 5, 9\}$ (resp. $q \neq 3$), then $\mathbb{F}_q$ is the I_q-closure of I_q (resp. the I'_q-closure of I'_q).

(b) If $q \notin \{3, 5, 9\}$ (resp. $q \neq 3$), then the I_q-closed (resp. I'_q-closed) subsets of $\mathbb{F}_{q^2}^n$ are the translations of the $\mathbb{F}_q$-linear subspaces.

Remark 1.7. *Fix $A \subseteq \mathbb{F}_q$ such that $0 \in A$. Assume that $\mathbb{F}_q$ is the A-closure of $\mathbb{F}_q$. Then $S \subseteq \mathbb{F}_{q^2}^n$, $S \neq \emptyset$, is A-closed if and only if it is the translation of an $\mathbb{F}_q$-linear subspace by an element of $\mathbb{F}_{q^2}^n$. Thus part (b) of Theorem 1.6 follows at once from part (a) and similar statements are true for the A-closures for any A whose A-closure is $\mathbb{F}_q$.*

As suggested by one of the referees a key part of one of our proofs may be stated in the following general way.

Proposition 1.8. *Let A, B be subsets of $\mathbb{F}_q$ containing 0. Assume $A \neq \{0\}$ and let G be the subgroup of the multiplicative group $\mathbb{F}_q \setminus \{0\}$ generated by $A \setminus \{0\}$. Assume that B is A-closed. Then $B \setminus \{0\}$ is a union of cosets of G.*

Fix $S \subset \mathbb{F}_{q^2}^n$ and a set $A \subset \mathbb{F}_q$ such that $\{0, 1\} \subseteq A$. Instead of the A-closure of S the following sets $S_{i,A}$, $i \geq 1$, seem to be better. In particular both circles and $S_{1,A}$ appear in some proofs on the numerical range. Let $S_{1,A}$ be the set of all $a + (b - a)A$, $a, b \in S$. For all $i \geq 1$ set $S_{i+1,A} := (S_{1,A})_{1,A}$. Obviously $S_{i,A}$ is A-closed for $i \gg 0$. Note that $\{0, 1\}_A = A$ and hence if we start with $S = \{0, 1\}$ we obtain the A-closure of A after finitely many steps.

We thank the referees for an exceptional job, making key corrections and suggestions.

2 The proofs and related observations

We assume q odd, except in Remarks 2.1 and 2.2, Proposition 2.9 and the proof of Proposition 1.8.

Remark 2.1. *The notions of E_q-closed, I_q-closed and I'_q-closed subsets of $\mathbb{F}_{q^2}^n$ are invariant by translations of elements of $\mathbb{F}_{q^2}^n$ and by the action of $GL(n, \mathbb{F}_q)$.*

Remark 2.2. *Fix any $A \subseteq \mathbb{F}_q$ such that $0 \in A$. Any translate by an element of $\mathbb{F}_{q^2}^n$ of an A-closed set is A-closed. The $\mathbb{F}_q$-closed subsets of $\mathbb{F}_{q^2}^n$ are the translates by an element of $\mathbb{F}_{q^2}^n$ of the $\mathbb{F}_q$-linear subspaces. If $A \subseteq \{0, 1\}$, then any nonempty subset of $\mathbb{F}_{q^2}^n$ is A-closed.*

Proof of Proposition 1.8: Since $\mathbb{F}_q \setminus \{0\}$ is cyclic, G is cyclic. Let $a \in A \setminus \{0\}$ be a generator of G. Fix $c \in B \setminus \{0\}$ and take $t \in \mathbb{F}_q \setminus \{0\}$ such that $c = ta^z$ for some positive integer z. We need to prove that $B \setminus \{0\}$ contains all ta^k, $k \in \mathbb{Z}$. Since $b \in B$, B is A-closed, $a \in A$ and $a = 0 + (a - 0)$, we get $ta^{z+1} \in B$. Iterating this trick we get that B contains all ta^k for large k and hence the coset tG, because G is cyclic. □

Proposition 2.3. *We have $\#I_q = \#I'_q - 1 = (q+3)/4$ if $q \equiv 1 \pmod 4$ and $\#I_q = \#I'_q = (q+5)/4$ if $q \equiv 3 \pmod 4$.*

Proof. Since $A := \{x^2 + y^2 = 1\} \subset \mathbb{F}_q^2$ is a smooth affine conic, its projectivization $B := \{x^2 + y^2 = z^2\} \subset \mathbb{P}^2(\mathbb{F}_q)$ has cardinality $q + 1$ ([10, th. 5.1.8]). Note that the line $z = 0$ is not tangent to B and hence $B \cap \{z = 0\}$ has 2 points over $\mathbb{F}_{q^2}$. It has 2 points over $\mathbb{F}_q$ if and only if -1 is a square in $\mathbb{F}_q$, *i. e.* if and only if $q \equiv 1 \pmod 4$ ([10, (ix) and (x) at p. 5], [22, p. 22]). Hence $\#A = q + 1$ if $q \equiv 3 \pmod 4$ and $\#A = q - 1$ if $q \equiv 1 \pmod 4$. Note that $a \in I_q$ if and only if there is $(e, f) \in \mathbb{F}_q^2$ such that $e^2 + f^2 = 1$ and $a = e^2$. Note that $(e, f) \in A$ and that conversely for each $(e, f) \in A$, $e^2 \in I_q$. Obviously $0 \in I_q$ and $(0, f) \in A$ if and only if either $f = 1$ or $f = -1$. Thus $0 \in I_q$ comes from 2 points of A. Obviously $1 \in I_q$. If either $e = 1$ or $e = -1$, then $(e, f) \in A$ if and only if $f = 0$. Thus $1 \in I_q$ comes from 2 points of A. If $e^2 \notin \{0, 1\}$ and $e^2 \in I_q$, then e^2 comes from 4 points of A.

Fix a non-square $c \in \mathbb{F}_q$ and set $A' := \{x^2 - cy^2 = 1\} \subset \mathbb{F}_q^2$. Let $B' := \{x^2 - cy^2 = z^2\} \subset \mathbb{P}^2(\mathbb{F}_q)$ be the smooth conic which is the projectivization of A'. The line $\{z = 0\}$ is not tangent to B' and $\{z = 0\} \cap A' = \emptyset$. Thus $\#A' = q + 1$. Note that $a \in I''_q$ if and only if there is $(e, f) \in \mathbb{F}_q^2$ such that $a = e^2$ and $e^2 - cf^2 = 1$. The element $1 \in I''_q$ comes from two elements of A'. If $0 \in I''_q$, then it comes from two elements of A'. If $0 \notin I''_q$, *i. e.* if $q \equiv 3 \pmod 4$, we get $\#I''_q = (q + 1)/4$ and $\#I'_q = (q + 5)/4$. If $0 \in I''_q$ we get $\#I''_q = \#I'_q = (q + 7)/4$. □

Remark 2.4. *If $q \in \{3, 5\}$, then $I_q = \{0, 1\}$ and hence each non-empty subset of $\mathbb{F}_{q^2}^n$ is I_q-closed if $q \in \{3, 5\}$. Since $\{0, 1\} \subseteq I'_q$, Proposition 2.3 gives $I'_3 = I_3$. We have $I'_5 = \{0, 1, 4\} = E_5$, because 3 is not a square in $\mathbb{F}_5$.*

Remark 2.5. *Fix any $t \in \mathbb{F}_q \setminus E_q$. Then $\mathbb{F}_q \setminus E_q = t(E_q \setminus \{0\})$. Obviously $E_qE_q = E_q$.*

The following result characterizes E_{q^2} and hence characterizes all E_r with r a square odd prime power.

Proposition 2.6. *The set of $E_{q^2} \setminus \{0\}$ of all squares of $\mathbb{F}_{q^2} \setminus \{0\}$ is the set of all ab such that $a \in \mathbb{F}_q \setminus \{0\}$ and $b^{q+1} = 1$. We have $ab = a_1b_1$ if and only if $(a_1, b_1) \in \{(a, b), (-a, -b)\}$.*

Proof. Fix $z \in \mathbb{F}_{q^2} \setminus \{0\}$. Hence $z^{q^2-1} = 1$. Thus $z^{(q-1)^{q+1}} = 1$ (and so $z^{(1-q)^{q+1}} = 1$) and $z^{(q+1)^{q-1}} = 1$, *i. e.* $z^{q+1} \in \mathbb{F}_q \setminus \{0\}$. Note that $z^2 = z^{q+1}z^{1-q}$. Assume $ab = a_1b_1$ with a, $a_1 \in \mathbb{F}_q \setminus \{0\}$ *(i.e., with* $a^{q-1} = {a_1}^{q-1} = 1$*) and* $b^{q+1} = {b_1}^{q+1} = 1$*. Taking* $a{a_1}^{-1}$ *and* $b{b_1}^{-1}$ *instead of* a *and* b *we reduce to the case* $a_1 = b_1 = 1$ *and hence* $ab = 1$*. Thus* $a^{q+1}b^{q+1} = 1$*. Hence* $a^2 = 1$*. Since* q *is odd and* $a \neq 1$*, then* $a = -1$*. Thus* $b = -1$*.* □

Proposition 2.7. *Take* $S \subseteq \mathbb{F}_{q^2}^n$*. The set* S *is* E_q*-closed if and only if it is a translation of an* $\mathbb{F}_q$*-linear subspace.*

Proof. Remark 2.2 gives the "if" part. Assume that S is not a translation of an $\mathbb{F}_q$-linear subspace and fix $a, b \in S$ such that $a \neq b$ and the affine $\mathbb{F}_q$-line L spanned by $\{a, b\}$ is not contained in S. By Remark 2.1 it is sufficient to find a contradiction in the case $n = 1$ and $L = \mathbb{F}_q$ with $a = 0$ and $b = 1$. Thus $E_q \subseteq S$. Since S is E_q-closed and $0 \in S$, $c + (-c)E_q \subseteq S$ for all $c \in E_q$. First assume $-1 \in E_q$. In this case $-cE_q = E_q$. Thus S contains all sums of two squares. Thus $S = \mathbb{F}_q$. Now assume $-1 \notin E_q$. In this case we obtained that S contains all differences of two squares. Thus $-E_q \subset S$. Since $-1 \notin E_q$, $-E_q = \{0\} \cup (\mathbb{F}_q \setminus E_q)$ (Remark 2.5). Thus $S \supseteq L$. □

The cases of I_q-closures and I'_q-closures are more complicated, because $I_q = I'_q = \{0, 1\}$ if $q = 3, 5$ and hence all subsets of $\mathbb{F}_{q^2}^n$ are I_q-closed if $q = 3, 5$. The following observation shows that the I_9-closed subsets of $\mathbb{F}_{81}^n$ are exactly the translations of the $\mathbb{F}_3$-linear subspaces and gives many examples with $I_q \nsubseteq I'_q$.

Remark 2.8. *We always have* $2 \notin 1 + cE_q$*,* c *a non-square, because* 1 *is a square. If* q *is a square, say* $q = s^2$*, then obviously* $\mathbb{F}_s \subseteq E_q \cap (1 - E_q) = I_q$ *and hence* $2 \in I_q$*. Take* $q = 9$*. We get* $\mathbb{F}_3 \subseteq I_9$*. Since* $\#I_9 = 3$ *(Proposition 2.3), we get* $I_q = \mathbb{F}_3$*. Thus the* I_9*-closed subsets of* $\mathbb{F}_{81}^n$ *are exactly the translations of the* $\mathbb{F}_3$*-linear subspaces. Now assume that* q *is not a square. We have* $2 \in 1 - E_q$ *if and only if* -1 *is a square, i. e. if and only if* $q \equiv 1 \pmod 4$*. Since* q *is not a square, we have* $2 \in E_q$ *if and only if* 2 *is a square in* $\mathbb{F}_p$*, i. e. if and only if* $p \equiv -1, 1 \pmod 8$ *([15, Proposition 5.1.3]). Thus for a non-square* q *holds:* $2 \in I_q$ *if and only if* $p \equiv 1 \pmod 8$*.*

Proof of Theorem 1.6: Let Y be the I_q-closure of I_q. By Proposition 1.8, $Y' := Y \setminus \{0\}$ is a union of the cosets of $H := \langle I_q \setminus \{0\} \rangle$. Since $\#(I_q \setminus \{0\}) \geq (q-1)/4$ with equality if and only if $q \equiv 1 \pmod 4$, H is either $\mathbb{F}_q^*$, the set of non-zero squares, the set of non-zero cubes or (only if $q \equiv 1 \bmod 4$), the set of all non-zero 4-powers. Since $I_q \subseteq E_q$, $H \neq \mathbb{F}_q^*$. If H is the set of cubes, then, as all elements of I_q are squares, it would be the set of 6-th powers, contradicting the inequality $\#I_q > (q-1)/4$.

(a) Assume that $H = E_q \setminus \{0\}$. It suffices to show that the I_q-closure of the set of squares contains a non-square. Suppose otherwise. Take an element $a \in I_q$ with $a \notin \{0, 1\}$. Then we obtain that for all squares x, y, $x + (y - x)a$ is also a square. Since a is a non-zero square, this is the same as the statement that for all squares x, z the element $z + (1 - a)x$ is a square. If $1 - a$ is a square we deduce that the set of all squares is closed under addition, a contradiction. If $1 - a$ is not a square we may take $x = 1$, $z = 0$ to obtain a contradiction.

(b) Assume $q \equiv 1 \pmod 4$, $q \neq 9$, and that H is the set of all non-zero 4-powers. We also saw that $H = I_q \setminus \{0\}$. The proof of step (a) works using the word "4-power" instead of "square" with a a 4-power. We get that the set of all 4-powers is closed under taking differences. Thus I_q is closed under taking differences and, since it contains 0, under the multiplication by -1. H is obviously closed under taking products. Thus I_q is a subfield of order $(q+3)/4$, which is absurd if $q \neq 9$.

(c) Now we consider I'_q and set $H' := \langle I_q \setminus \{0\} \rangle$. The cases in which H' is the set of all squares or all cubes are excluded as above. Since $\#(I'_q \setminus \{0\}) > (q-1)/4$, Y is not the set of all 4-th powers. □

Proposition 2.9. *Assume q even and set $E_q := \{a(a+1)\}_{a \in \mathbb{F}_q}$.*

(1) *If $q = 2, 4$, then E_q is the E_q-closure of itself.*

(2) *If $q \geq 8$, then $\mathbb{F}_q$ is the E_q-closure of E_q.*

Proof. We have $E_2 = \{0\}$ and $E_4 = \{0, 1\}$.

Now assume $q \geq 8$ and call B the E_q-closure of E_q. Let G be the subgroup of the multiplicative group $\mathbb{F}_q \setminus \{0\}$ generated by $E_q \setminus \{0\}$. By Proposition 1.8 it is sufficient to prove that $G = \mathbb{F}_q \setminus \{0\}$. Since $\#E_q = q/2$, $E_q \setminus \{0\} \neq \emptyset$. Fix $a \in E_q \setminus \{0\}$ and a positive integer k. The E_q-closure of $\{0, a^k\}$ contains a^{k+1}. Thus B contains the multiplicative subgroup of $\mathbb{F}_q \setminus \{0\}$ generated by $E_q \setminus \{0\}$. Since $q \geq 8$, $\#(\mathbb{F}_q \setminus \{0\}) = q - 1$ is odd and $q - 1 < 3(q/2 - 1) = 3\#(\mathbb{F}_q \setminus \{0\})$, we get $G = \mathbb{F}_q \setminus \{0\}$. □

References

[1] E. Ballico, “On the numerical range of matrices over a finite field”, Linear Algebra Appl., vol. 512, pp. 162–171, 2017.

[2] E. Ballico, *Corrigendum* to “On the numerical range of matrices over a finite field” [Linear Algebra Appl., vol. 512, pp. 162–171, 2017], Linear Algebra Appl., vol. 556, pp. 421–427, 2018.

[3] E. Ballico, “The Hermitian null-range of a matrix over a finite field”, Electron. J. Linear Algebra, vol. 34, pp. 205–216, 2018.

[4] E. Ballico, “A numerical range characterization of unitary matrices over a finite field”, Asian-European Journal of Mathematics (AEJM) (to appear). doi: 10.1142/S1793557122500498

[5] F. F. Bonsall and J. Duncan, *Numerical ranges II*, London Mathematical Society Lecture Note Series, no. 10, New York-London: Cambridge University Press, 1973.

[6] K. Camenga, B. Collins, G. Hoefer, J. Quezada, P. X. Rault, J. Willson and R. J. Yates, “On the geometry of numerical ranges over finite fields”, Linear Algebra Appl., vol. 628, pp. 182–201, 2021.

[7] Ch. Chorianopoulos, S. Karanasios and P. Psarrakos, “A definition of numerical range of rectangular matrices”, Linear Multilinear Algebra, vol. 57, no. 5, pp. 459–475, 2009.

[8] J. I. Coons, J. Jenkins, D. Knowles, R. A. Luke and P. X. Rault, “Numerical ranges over finite fields”, Linear Algebra Appl., vol. 501, pp. 37–47, 2016.

[9] K. E. Gustafson and D. K. M. Rao, *Numerical range*, Universitext, New York: Springer-Verlag, 1997.

[10] J. W. P. Hirschfeld, *Projective geometries over finite fields*, Oxford Mathematical Monographs, New York: The Clarendon Press, Oxford University Press, 1979.

[11] J. W. P. Hirschfeld and J. A. Thas, *General Galois geometries*, Oxford Mathematical Monographs, New York: The Clarendon Press, Oxford University Press, 1991.

[12] R. A. Horn and C. R. Johnson, *Matrix analysis*, Cambridge: Cambridge University Press, 1985.

[13] R. A. Horn and C. R. Johnson, *Topics in matrix analysis*, Cambridge: Cambridge University Press, 1991.

[14] L. Jin, “Quantum stabilizer codes from maximal curves”, IEEE Trans. Inform. Theory, vol. 60, no. 1, pp. 313–316, 2014.

[15] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Second Edition, Graduate Texts in Mathematics, 84, New York: Springer-Verlag, 1990.

[16] R. Ke, W. Li and M. K. Ng, "Numerical ranges of tensors", Linear Algebra Appl., vol. 508, pp. 100–132, 2016.

[17] J.-L. Kim and G. L. Matthews, "Quantum error-correcting codes from algebraic curves", in *Advances in algebraic geometry codes*, Ser. Coding Theory Cryptol., vol. 5, Hackensack, NJ: World Sci. Publ., 2008, pp. 419–444.

[18] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, 20, Cambridge: Cambridge University Press, 1997.

[19] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge: Cambridge University Press, 1994.

[20] C. Munuera, W. Tenório and F. Torres, "Quantum error-correcting codes from algebraic geometry codes of Castle type", Quantum Inf. Process., vol. 15, no. 10, pp. 4071–4088, 2016.

[21] P. J. Psarrakos and M. J. Tsatsomeros, "Numerical range: (in) a matrix nutshell", National Technical University, Athens, Greece, Notes, 2004.

[22] C. Small, *Arithmetic of finite fields*, Monographs and Textbooks in Pure and Applied, 148, New York: Marcel Dekker, Inc., 1991.