Turkish Journal of Mathematics
http://journals.tubitak.gov.tr/math/
Research Article

Turk J Math
(2018) 42: 1 – 11
© TÜBİTAK
doi:10.3906/mat-1612-20

Restriction of a quadratic form over a finite field to a nondegenerate affine quadric hypersurface

Edoardo BALLICO*
Department of Mathematics, University of Trento, Povo, Trentino, Italy

Received: 05.12.2016 • **Accepted/Published Online:** 24.02.2017 • **Final Version:** 22.01.2018

Abstract: Let $h, h_M : \mathbb{F}_q^n \to \mathbb{F}_q$ be quadratic forms with h not degenerate. Fix $k \in \mathbb{F}_q$ and set $C_n(k,h)_{\mathbb{F}_q} := \{h(x_1,\dots,x_n) = k\} \subset \mathbb{F}_q^n$. We compute (in many cases) the image of $h_{M|C_n(k,h)_{\mathbb{F}_q}}$. This question is related to a question on the numerical range of matrices over a finite field.

Key words: Quadratic form, finite field

1. Introduction

For any field K let $M_{n,n}(K)$ denote the set of all $n \times n$ matrices with coefficients in K. Take a field K, a nondegenerate quadratic form $h : K^n \to K$, and an $n \times n$ matrix $M = (m_{ij}) \in M_{n,n}(K)$, $i,j = 1,\dots,n$. For any $(x_1,\dots,x_n) \in K^n$ set $h_M(x_1,\dots,x_n) := \sum_{ij} m_{ij}x_ix_j$. For any $k \in K$ set $C_n(k,h)_K := \{(x_1,\dots,x_n) \in K^n \mid h(x_1,\dots,x_n) = k\}$. Let $\mathrm{Num}_k(M)_{h,K} \subseteq K$ be the set of all $h_M(x_1,\dots,x_n)$ with $(x_1,\dots,x_n) \in C_n(k,h)_K$. We came to this topic in [1], motivated to a similar set-up related to the numerical range of a matrix over a finite field introduced in [2]. We consider the case in which K is a finite field $\mathbb{F}_q$ and prove the following result.

Theorem 1 *Take $n \ge 2$, any nondegenerate quadratic form $h : \mathbb{F}_q^n \to \mathbb{F}_q$, any $k \in \mathbb{F}_q$, and any $M \in M_{n,n}(\mathbb{F}_q)$.*

(a) Assume $k = 0$. Either $\mathrm{Num}_0(M)_{h,\mathbb{F}_q} = \{0\}$ or $\mathrm{Num}_0(M)_{h,\mathbb{F}_q} = \mathbb{F}_q$ or q is odd, $\sharp(\mathrm{Num}_0(M)_{h,\mathbb{F}_q}) = (q+1)/2$ and there is $c \in \mathbb{F}_q^*$ such that $\mathrm{Num}_0(M)_{h,\mathbb{F}_q}$ is the union of $\{0\}$ and all $g \in \mathbb{F}_q^*$ such that g/c is a square.

(b) Assume $n \ge 3$ and $q \ne 2$. $\sharp(\mathrm{Num}_k(M)_{h,\mathbb{F}_q}) = 1$ for some $k \in \mathbb{F}_q$ if and only if h_M is a multiple of h.

(c) Assume $\sharp(\mathrm{Num}_k(M)_{h,\mathbb{F}_q}) \ne 1$. If $n = 2$, then $\sharp(\mathrm{Num}_k(M)_{h,\mathbb{F}_q}) \ge \lceil (q-1)/4 \rceil$. If $n \ge 3$, then $\sharp(\mathrm{Num}_k(M)_{h,\mathbb{F}_q}) \ge \lceil q/2 \rceil$.

See Example 1 for a discussion on the strength of parts (a) and (c) of Theorem 1.

See [3, Ch. 5] and [4, §22.1] for the classification of nondegenerate quadratic forms. In [1, §3] we considered the case $k = 0$ of a similar problem with instead of h the quadratic form $\sum_{i=1}^n x_i^2$, which is nondegenerate if q is odd, but it has rank 1 if q is even. For any $k \in \mathbb{F}_q$ set $C_n(k)_q := \{(x_1,\dots,x_n) \in \mathbb{F}_q^n \mid x_1^2 + \cdots + x_n^2 = k\}$.

*Correspondence: ballico@science.unitn.it
The author was partially supported by MIUR and GNSAGA of INdAM (Italy).

Let $\mathrm{Num}_k(M)_q$ be the set of all $h_M(u)$ with $u \in C_n(k)_q$. In Section 3 we consider the case in which we take $x_1^2+\cdots+x_n^2$ instead of h. We improve in this case part (c) of Theorem 1 (see Proposition 3 for q odd). We give very precise descriptions of $\mathrm{Num}_k(M)_q$ when M is the matrix with a unique Jordan block (see Propositions 4, 5, and 6 for the cases $n = 2, 3, 4$, respectively). We get $\mathrm{Num}_k(M)_q = \mathbb{F}_q$ for all $n \geq 4$ for these matrices (Proposition 6 and Remark 6). In each case standard lemmas or reduction steps compute $\mathrm{Num}_k(M)_q$ for many matrices related to direct sums of Jordan blocks.

2. Proof of Theorem 1

For any field K set $K^* := K \setminus \{0\}$. Let $e_1 = (1, 0, \dots, 0), \dots, e_n = (0, \dots, 0, 1)$ be the standard basis of $\mathbb{F}_q^n$. For each $n > 0$ let $\mathbb{I}_{n\times n}$ denote the $n \times n$ identity matrix.

Remark 1 *Fix $M = (m_{ij}), N = (n_{ij}) \in M_{n,n}(\mathbb{F}_q)$ such that $m_{ii} = n_{ii}$ for all i and $m_{ij} + m_{ji} = n_{ij} + n_{ji}$ for all $i \neq j$. Then $h_M = h_N$.*

Remark 2 *Fix $k \in \mathbb{F}_q$, positive integers n, m, $A \in M_{n,n}(\mathbb{F}_q)$, and $B \in M_{m,m}(\mathbb{F}_q)$. Set $M := A \oplus B \in M_{n+m,n+m})(\mathbb{F}_q)$. We have*

$$\mathrm{Num}_k(M)_q = \cup_{k_1,k_2\in\mathbb{F}_q,k_1+k_2=k}\mathrm{Num}_{k_1}(A)_q + \mathrm{Num}_{k_2}(B)_q.$$

For any nondegenerate h we also have

$$\mathrm{Num}_k(M)_{h,\mathbb{F}_q} = \cup_{k_1,k_2\in\mathbb{F}_q,k_1+k_2=k}\mathrm{Num}_{k_1}(A)_{h,\mathbb{F}_q} + \mathrm{Num}_{k_2}(B)_{h,\mathbb{F}_q}.$$

Lemma 1 *For any $n \geq 2$, any nondegenerate quadratic form h, and any $k \in \mathbb{F}_q$ we have $\mathrm{Num}_k(M)_{h,\mathbb{F}_q} \neq \emptyset$.*

Proof We have $\mathrm{Num}_k(M)_{h,\mathbb{F}_q} \neq \emptyset$ if and only if $h : \mathbb{F}_n^q \to \mathbb{F}_q$ has k in its image. Thus, $\mathrm{Num}_k(M)_{h,\mathbb{F}_q} \neq \emptyset$ for all k if and only if h is surjective. If q is odd, then h is surjective by [6, Theorem 4.12]. If q is even, then h is surjective by [6, Theorem 4.16]. □

Lemma 2 *Assume $n \geq 3$ and $q \neq 2$. The following conditions are equivalent:*

(a) h_M is proportional to h;

(b) there is $k \in \mathbb{F}_q$ such that $\sharp(\mathrm{Num}_k(M)_{h,\mathbb{F}_q}) = 1$;

(c) $\sharp(\mathrm{Num}_k(M)_{h,\mathbb{F}_q}) = 1$ for all $k \in \mathbb{F}_q$.

Proof By Lemma 1 we have $\mathrm{Num}_k(M)_{h,\mathbb{F}_q} \neq \emptyset$. For each $t, w \in \mathbb{F}_q$ the system $h(x_1, \dots, x_n) - k = h_M(x_1, x_2, \dots, x_m) - w = 0$ has a solution if and only $h(x_1, \dots, x_n) - k = h_M(x_1, x_2, \dots, x_n) - th(x_1, \dots, x_n) - (w - tk) = 0$ has a solution. Hence, if h_M is a multiple of h, then $\sharp(\mathrm{Num}_k(M)_{h,\mathbb{F}_q}) = 1$ for all $k \in \mathbb{F}_q$. Now assume $\sharp(\mathrm{Num}_k(M)_{h,\mathbb{F}_q}) = 1$ for some $k \in \mathbb{F}_q$. Set $Z := \{(x_1, \dots, x_n) \in \mathbb{F}_q^n \mid h(x_1, \dots, x_n)\}$. We take $x_1, \dots, x_n, z$ as homogeneous coordinates of $\mathbb{P}^n$ and set $Z' := \{(x_1 : \cdots : x_n : z) \in \mathbb{P}^n(\mathbb{F}_q) \mid h(x_1, \dots, x_n) = kz^2\}$. If $k = 0$, then Z' is a quadric cone with vertex $(0 : \dots, 0 : 1) \notin Z$ and with as a basis the smooth quadric $\{h(x_1, \dots, x_n) = 0\}$ of $\mathbb{P}^{n-1}(\mathbb{F}_q)$. If $k \neq 0$ and q is odd, then Z' is a smooth quadric hypersurface, because the partial derivative ∂/∂_z of $h(x_1, \dots, x_n) - kz^2$ is $-2kz$, which vanishes only if $z = 0$, while the partial derivatives of $h(x_1, \dots, x_n)$ vanish simultaneously only at $x_1 = \cdots = x_n = 0$, because h is assumed to be nondegenerate. If q is even, then Z' is nondegenerate for n even, while it has corank 1 if n is odd (use the canonical forms in [3, Theorem 5.1.7] or [4, §22.1]).

Claim 1: Assume q odd, $k \neq 0$, and $n = 3$. Then Z' is a hyperbolic quadric.

Proof of Claim 1: Take $a \in \mathbb{F}_q^*$ such that $-a$ is a square in $\mathbb{F}_q$. Since all smooth conics over $\mathbb{F}_q$ are projectively equivalent ([3, Theorem 5.1.6]), there is a linear change of coordinates such that $h(y_1, y_2, y_3) = y_1y_2 + aky_3^2$, where y_1, y_2, y_3 are the new linear coordinates. Hence, $h(y_1, y_2, y_3) - kz^2 = y_1y_2 - k(z^2 + ay_3^2)$. By the choice of a we have $z^22 + ay_3^2 = w_3w_4$ with w_3, w_4 a linear combination of y_3 and z. Since Z' is nondegenerate, w_3 and w_4 are not proportional. In the coordinates y_1, y_2, w_3, w_4 the quadric Z' has the canonical form of a hyperbolic quadric.

Claim 2: For each $u \in Z'$ there is a line $\ell \subset Z'$ with $u \in \ell$.

Proof of Claim 2: If $k = 0$, then Claim 2 is true, because Z' is a cone. If $n \geq 4$, then Claim 2 is true for an arbitrary quadric hypersurface. If $n = 3$, $k \neq 0$, and q is even, then Claim 2 is true, because Z' is a cone. If $n = 3$, $n \neq 0$, and q is odd, then Claim 2 is equivalent to Claim 1.

If $h_M(u) = 0$ for all $u \in \mathbb{F}_q^n$, then it is a multiple of h, because for $n \geq 3$ no homogeneous degree 2 polynomial vanishes at all points of $\mathbb{F}_q^n$. Hence, we may assume that the quadratic function h_M induces a nonconstant map $u : \mathbb{F}_q^n \to \mathbb{F}_q$. Since u is not constant, for each $t \in \mathbb{F}_q$ the set $u^{-1}(t)$ is an affine quadric hypersurface of $\mathbb{F}_q^n$ defined over $\mathbb{F}_q$. By assumption the affine quadric hypersurface $C_n(k,h)_{\mathbb{F}_q} = \{h(x_1, \dots, x_n) = k\}$ is one of the fibers of u, say $C_n(k,h)_{\mathbb{F}_q} = u^{-1}(t)$. Set $W := \{(x_1 : \cdots : x_n : z) \in \mathbb{P}^n(\mathbb{F}_q) \mid h_M(x_1, \dots, x_n) - tz^2 = 0\}$. Let $H \subset \mathbb{P}^n(\mathbb{F}_q)$ be the hyperplane $\{z = 0\}$. Take $u \in Z$ and call L a line defined over $\mathbb{F}_q$, contained in Z' and with $u \in L$ (Claim 2). We have $\sharp(L \cap Z) = q$. By assumption $W \setminus W \cap H \supseteq L \cap Z$. Since $\sharp(L \cap W) \geq q \geq 3 > \deg(h_M)$, we have $L \subset W$. Hence, we see that W contains all lines of Z' intersecting Z. By Claim 2 this implies first that W has the same rank as Z' and then that $Z' = W$. Since $n \geq 3$, there is $c \in \mathbb{F}_q^*$ such that $h_M(x_1, \dots, x_m) - t = c(h(x_1, \dots, x_m) - k)$. □

Proof of Theorem 1. We have $\mathrm{Num}_k(M)_{h,\mathbb{F}_q} \neq \emptyset$ by Lemma 1.

Lemma 2 gives part (b). We take Z and Z' as in the proof of Lemma 2.

(a) Take $k = 0$. Taking $0 \in \mathbb{F}_q^n$ we get $0 \in \mathrm{Num}_k(M)_{h,\mathbb{F}_q}$. Assume the existence of $c \in \mathbb{F}_q^* \cap \mathrm{Num}_k(M)_{h,\mathbb{F}_q}$ and take $(a_1, \dots, a_n) \in \mathbb{F}_q^n$ such that $h_M(a_1, \dots, a_n) = c$. Note that for any $t \in \mathbb{F}_q$ we have $(ta_1, \dots, ta_n) \in Z$ and $h_M(ta_1, \dots, ta_m) = t^2c$. Hence, $\mathrm{Num}_k(M)_{h,\mathbb{F}_q}$ contains all elements $x \in \mathbb{F}_q^*$ such that c/x is a square. If q is even we get that either $\mathrm{Num}_k(M)_{h,\mathbb{F}_q} = \{0\}$ or $\mathrm{Num}_k(M)_{h,\mathbb{F}_q} = \mathbb{F}_q$. If q is odd we get that $\sharp(\mathrm{Num}_k(M)_{h,\mathbb{F}_q}) \in \{1, (q+1)/2, q\}$ and the description in part (a).

(b) From now on we fix $k \in \mathbb{F}_q^*$ and we assume $\sharp(\mathrm{Num}_k(M)_{h,\mathbb{F}_q}) > 1$. First assume $n = 2$. In this case Z is a nonempty affine conic whose degree 2 part has rank 2 and hence $\sharp(Z) \geq q - 1$. Since h_M is induced by a degree 2 polynomial and $Z \nsubseteq h_M^{-1}(t)$ for any $t \in \mathbb{F}_q$, each fiber of $h_{M|Z}$ has cardinality ≤ 4 and hence the image of $h_{M|Z}$ has cardinality $\geq \lceil (q-1)/4 \rceil$.

Now assume $n \geq 3$. By assumption $h_{M|Z}$ is not a constant. Take a line $L \subset Z'$ such that $L \cap Z \neq \emptyset$. We have $\sharp(L \cap Z) = q$. Since $h_{M|L\cap Z}$ is induced by a polynomial of degree ≤ 2, either $h_{M|L\cap Z}$ is constant or each fiber of $h_{M|L\cap Z}$ has cardinality at most 2. In the latter case the image of $h_{M|Z\cap L}$ has cardinality $\geq q/2$. Thus, to conclude the proof of Theorem 1, it is sufficient to find a line $L \subset Z'$ such that $L \cap Z \neq \emptyset$ and $h_{M|L\cap Z}$ is not a constant. We assume that no such a line exists. By assumption $m := h_{M|Z} : Z \to \mathbb{F}_q$ is not constant.

Take $o, o' \in Z$ such that $m(o) \neq m(o')$. By Claim 2 of the proof of Lemma 2 there are lines $L, L' \subset Z'$ such that $o \in L$ and $o' \in L'$. Our assumptions on the lines of Z' meeting Z imply that $m_{|L\cap Z}$ and $m_{|L'\cap Z}$ are constant. Let $R \subset \mathbb{P}^n(\mathbb{F}_q)$ be the line spanned by $\{o, o'\}$. Since $o, o' \in Z$ and $m(o) \neq m(o')$, our assumption on the lines contained in Z' and intersecting Z implies $R \nsubseteq Z'$.

(b1) Assume $L \cap L' = \emptyset$. In this case the linear span $E \subset \mathbb{P}^n(\mathbb{F}_q)$ of $L \cup L'$ has dimension 3. First assume $E \subset Z'$. In this case the line R joining o and o' is contained in Z', a contradiction. Now assume $E \nsubseteq Z'$ and so $E \cap Z'$ is a quadric hypersurface of E defined over $\mathbb{F}_q$. Since $E \cap Z'$ contains two disjoint lines (L and L') either $Z' \cap E$ is a smooth hyperbolic quadric surface or it is the union of two different planes ([4, page 4]).

(b1.1) Assume that $Z' \cap E$ is a smooth hyperbolic quadric surface. Since $L \cap L' = \emptyset$, L and L' are in the same ruling of $Z' \cap E$ (call it the first ruling of $E \cap Z$). Since $Z \cap E \neq \emptyset$, $Z' \cap E \cap H$ is a divisor of bidegree $(1,1)$, i.e. either a reducible conic or a smooth conic. For any $a \in L$ let R_a be the line of the second ruling of $E \cap Z'$ containing a. The set $R_a \cap L'$ is a unique point, b_a, and the map $a \mapsto b_a$ induces a bijection $L \to L'$. Since $\sharp(L \cap Z) = \sharp(L' \cap Z) = q > 2$, there is $a \in L \cap Z$ with $b_a \in L' \cap Z$. Since $m_{|Z\cap R_a}$ is not constant, we get a contradiction.

(b1.2) Assume that $Z' \cap E = H_1 \cup H_2$ with H_1 and H_2 planes. Note that this case does not occur if $n = 3$, because h is nonsingular. Each H_i is defined over $\mathbb{F}_q$, because $Z' \cap H$ contains 2 disjoint lines defined over $\mathbb{F}_q$. Fix $b \in H_1 \cap H_2 \subset \mathbb{P}^n(\mathbb{F}_q)$. There are lines $L_1 \subset H_1$, $L_2 \subset H_2$ defined over $\mathbb{F}_q$, with $L_i \neq H_1 \cap H_2$, $L_i \cap Z \neq \emptyset$ for all i and $\{b\} = L_1 \cap L_2$. Since $m_{|Z\cap D}$ is constant for every line $D \subset Z'$ with $D \cap Z \neq \emptyset$, we get $H_1 \cap H_2 \subset H$. Hence, $H_i \setminus H_1 \cap H_2 \subset Z$. By step (b1.1) we get that this is the case for all lines L, L' with $Z \cap L \neq \emptyset$, $Z \cap L' \neq \emptyset$, and $L \cap L' = \emptyset$. In particular, for every line $D \subset Z'$ with $L \cap D = \emptyset$ and $D \cap Z \neq \emptyset$, we have $D \cap H_1 \cap H_2 \neq \emptyset$ and the plane U_D spanned by $D \cup (H_1 \cap H_2)$ is contained in Z'. Fix one such line D not contained in E. In the same way we check that $T \cap H_1 \cap H_2 \neq \emptyset$ for each line $T \subset Z'$ with $T \cap Z \neq \emptyset$ and either $T \cap L' = \emptyset$ or $T \cap D = \emptyset$ or $T \cap L = \emptyset$. Every line J with $J \cap L \neq \emptyset$ and $J \cap L' \neq \emptyset$ is contained in E. If $D \cap E = \emptyset$ (we are always in this case if $n \geq 5$), then we get that every line T contained in Z' and intersecting Z (i.e. not contained in H) meets the line $H_1 \cap H_2$, which is obviously false since Z' has rank at least $n \geq 4$ and every point of Z' is contained in a line contained in Z'. If $D \cap E$ is a point, u, then we take instead of D a line D' with $u \notin D'$, $D' \subset Z'$, $D' \cap Z \neq \emptyset$, and $L \cap D' = \emptyset$. We get $T \cap D' = \emptyset$ if $T \subset E$ and $u \in T$, and conclude using D' instead of D.

(b2) Assume q odd and $L \cap L' \neq \emptyset$. Since $m_{|L\cap Z}$ and $m_{|L'\cap Z}$ are constant and different functions, we have $L \cap L' \in H$. Let $F \subset \mathbb{P}^n(\mathbb{F}_q)$ be the plane spanned by $L \cup L'$. F is defined over $\mathbb{F}_q$. We have $R \subset F$. If $F \subset Z'$, then $R \subset Z'$, a contradiction. Hence, $F \cap Z' = L \cup L'$. For any $a \in \mathbb{P}^n(\mathbb{F}_q) \setminus F$ let W_a be the 3-dimensional linear space spanned by $F \cup \{a\}$. W_a is defined over $\mathbb{F}_q$ and $W_a \cap Z'$ is a quadric surface defined over $\mathbb{F}_q$ and containing 2 intersecting lines and at least another point not in the plane they spanned. Hence, $W_a \cap Z$ is either a hyperbolic quadric surface or an irreducible quadric cone with vertex the point $L \cap L'$ or the union of two different planes, each of them defined over $\mathbb{F}_q$. Since q is odd, Z' is not a cone. Since Z' is not a cone with vertex $L \cap L'$, we may find $a \in Z$ such that $W_a \cap Z'$ is not a cone with vertex containing the point $L \cap L'$. Now assume $W_a \cap Z' = H_1 \cup H_2$ with each H_i a plane defined over $\mathbb{F}_q$. Since $F \nsubseteq Z'$, H_1 contains one of the lines L, L' (say, it contains L) and H_2 contains the other one, L'. Hence, $L \cap L' \in H_1 \cap H_2$. Thus, $W_a \cap Z'$ is a cone with vertex containing $L \cap L'$.

Now assume that $Z' \cap E$ is an irreducible hyperbolic quadric. In particular $\sharp(Z' \cap E) = (q+1)^2$. Call I the ruling of $Z' \cap E$ containing L and II the ruling of $Z' \cap E$ containing L'. $Z' \cap E \cap H$ is a curve of bidegree $(1,1)$ of $Z' \cap E$ and hence it is either a reducible conic (with each line defined over $\mathbb{F}_q$ and so of cardinality $2q+1$) or a smooth conic (and so of cardinality $q+1$). For each $a \in Z \cap L$ (resp. $b \in L' \cap Z$) let R_a (resp. D_b) be the line in the ruling II (resp. I) containing a. All lines D_a and R_b are contained in Z', defined over $\mathbb{F}_q$, and each R_a meets hence D_b at exactly one point of $\mathbb{P}^n(\mathbb{F}_q)$. The restriction of m to each $Z \cap R_a$ and to each $Z \cap D_b$ is constant. The set of all $R_a \cap R_b$ is a subset of $Z' \cap H$ with cardinality q^2 and hence at least some of these points must be contained in Z, contradicting the constancy of all $m_{|R_a}$ and all $m_{|D_b}$.

(c) Now assume q even. By the proof in step (b) it is sufficient to do the case $n = 3$. Up to a linear change of coordinates we may take $h = x_1x_2 + x_3^2$. Hence, Z' has equation $x_1x_2 + x_3^2 + kz^2 = 0$. Write $k = c^2$. We have $x_1x_2 + x_3^2 + kz^2 = x_1x_2 + (x_3 + cx_2)^2$ and hence Z' is an irreducible quadric cone with vertex $w = (0 : 0 : c : 1)$. Note that $w \notin H$ and so $w \in Z$. Thus, Z is covered by lines intersecting at a point $w \in Z$. Hence, m is a constant. □

Lemma 3 *Let $C \subset \mathbb{F}_q^2$ be the zero-locus of a polynomial $u \in \mathbb{F}_q[x_1, x_2]$ with degree 2 and whose homogeneous degree 2 part v has rank 2. Then $C \neq \emptyset$.*

Proof Let $J \subset \mathbb{P}^2(\mathbb{F}_q)$ be the zero-locus of the degree 2 form $v(x_1, x_2, z)$ obtained homogenizing v. Either v is a smooth conic (and so $\sharp(J) = q+1$ with at least $q-1 > 0$ points in $\mathbb{F}_q^2$) or it contains a line defined over $\mathbb{F}_q$ (not the line $z = 0$) and so $\sharp(C) \geq q$) or it is the union of two lines defined over $\mathbb{F}_{q^2}$ and exchanged by the map induced by the Frobenius $t \mapsto t^q$. In the latter case $\sharp(J) = 1$, but the point of J lies in C, because v has rank 2 (it is the common point of the 2 irreducible components of J over $\mathbb{F}_{q^2}$). □

Lemma 4 *Let $u \in k[x_1, x_2, x_3]$ be a degree 2 polynomial whose homogeneous part v has rank at least 2. Then u induces a surjection $f : \mathbb{F}_q^3 \to \mathbb{F}_q$.*

Proof There is a linear change of coordinates $\mathbb{F}_q^3 \to \mathbb{F}_q^3$ such that in the new coordinates y_1, y_2, y_3 we have $v(y_1, y_2, y_3) = w(y_1, y_2) + y_3(a_1y_1 + a_2y_2 + a_3y_3)$ with $w(y_1, y_2)$ with rank 2. Write $u(y_1, y_2, y_3) = v(y_1, y_2, y_3) + b_1y_1 + b_2y_3 + b_3y_3 + b_4$. Fix $d \in \mathbb{F}_q$. We need to find $(m_1, m_2, m_3) \in \mathbb{F}_q^3$ with $u(m_1, m_2, m_3) = d$. We take $m_3 = 0$ and apply Lemma 3. □

Lemma 5 *Take $n \geq 4$, a nonzero linear form $\ell : \mathbb{F}_q^n$, and $k \in \mathbb{F}_q$. Then $\ell_{|C_n(k,h)} : C_n(k, h) \to \mathbb{F}_q$ is surjective.*

Proof It is sufficient to do the case $n = 4$. Up to a linear change of coordinates it is sufficient to do the case $\ell = x_4$. Take $d \in \mathbb{F}_q$. We need to find $(x_1, x_2, x_3) \in \mathbb{F}_q^3$ such that $h(x_1, x_2, x_3, d) = k$. Since h has rank 4, the homogeneous degree 2 part of $h(x_1, x_2, x_3, d)$ has at least rank 2. Apply Lemma 4. □

Example 1 *Take a nondegenerate quadratic form $h : \mathbb{F}_q^n \to \mathbb{F}_q$, $n \geq 4$, and a nonzero linear form $\ell : \mathbb{F}_q^n \to \mathbb{F}_q$. Assume $h_M = ch + \ell^2$ for some $c \in \mathbb{F}_q$. Fix any $k \in \mathbb{F}_q$. We claim the following statements:*

(i) If q is even, then $\mathrm{Num}_k(M)_{h,\mathbb{F}_q} = \mathbb{F}_q$;

(ii) If q is odd, then $\sharp(\mathrm{Num}_k(M)_{h,\mathbb{F}_q}) = (q+1)/2$ and $\mathrm{Num}_k(M)_{h,\mathbb{F}_q}$ is the set of all squares in $\mathbb{F}_q$.

Indeed, it is sufficient to prove the case $h_M = \ell^2$, so that it is obvious that all elements of $\mathrm{Num}_k(M)_{h,\mathbb{F}_q}$ *are squares and we only need to prove the opposite containment. Thus, it is sufficient to prove that the map* $\mu = \ell_{|C_n(k,h)_{\mathbb{F}_q}} : C_n(k,h)_{\mathbb{F}_q} \to \mathbb{F}_q$ *is surjective. Apply Lemma 5.*

3. The $\mathbb{F}_q$-numerical range

Remark 3 *Fix* $M \in M_{n,n}(\mathbb{F}_q)$. *Take* $t \in \mathbb{F}_q^*$, $k \in \mathbb{F}_q$. *If* $u = (x_1, \dots, x_n) \in C_n(k)_q$, *then* $tu \in C_n(t^2k)_q$ *and* $h_M(tu) = t^2h_M(u)$. *Hence, to compute the integers* $\sharp(\mathrm{Num}_k(M)_q)$ *for all* k *(and often to get a complete description of* $\mathrm{Num}_k(M)_q$ *for all* $k \in \mathbb{F}_q$*) it is sufficient to do it for* $k = 1$, $k = 0$, *and (if* q *is odd) for a single* k, *which is not a square in* $\mathbb{F}_q$ *(*$\mathbb{F}_q$ *has* $(q-1)/2$ *nonsquares for any odd prime power* q*).*

Remark 4 *For all* $a, b, k \in \mathbb{F}_q$ *and all* $M \in M_{n,n}(\mathbb{F}_q)$ *we have* $\mathrm{Num}_k(aM + b\mathbb{I}_{n,n})_q = a\mathrm{Num}_k(M)_q + kb$. *Write* $M = (m_{ij})$, $i, j = 1, \dots, n$, *and assume that* $k = c^2$ *for some* $c \in \mathbb{F}_q$. *Since* $ce_i \in C_n(c^2)_q$ *and* $h_M(ce_i) = c^2m_{ii}$, *we have* $\{c^2m_{11}, \dots c^2m_{nn}\} \subseteq \mathrm{Num}_{c^2}(M)_q$.

Lemma 6 *Assume* q *odd and take* $k \in \mathbb{F}_q^*$. *Set* $\eta := 0$ *if* $q \equiv 1 \pmod 4$ *and* $\eta := 2$ *if* $q \equiv -1 \pmod 4$. *Then* $\sharp(C_2(k)_q) = q - 1 + \eta$.

Proof Set $T := \{(x_1, x_2, x_3) \in \mathbb{P}^2(\mathbb{F}_q) \mid x_1^2 + x_2^2 = kx_3^2\}$. Since $k \neq 0$ and q is odd, T is a smooth conic defined over $\mathbb{F}_q$. Thus, $\sharp(T) = q + 1$. The line $x_3 = 0$ meets T at two points (resp. no point) defined over $\mathbb{F}_q$ if and only if -1 has (resp. has not) a square-root in $\mathbb{F}_q$, i.e. if and only if $q \equiv 1 \pmod 4$ (resp. $q \equiv -1 \pmod 4$). □

Remark 5 *Assume* q *even and take* $k \in \mathbb{F}_q$. *Since* $\mathbb{F}_q$ *is a perfect field, there is a unique* $c \in \mathbb{F}_q$ *such that* $c^2 = k$. *Take* $u = (x_1, \dots, x_n) \in \mathbb{F}_q^n$. *Since* $(a+b)^2 = a^2 + b^2$ *for all* $a, b \in \mathbb{F}_q$ *we have* $\sum_{i=1} x_i^2 = k$ *(i.e.* $u \in C_n(k)_q$*) if and only if* $x_1 + \cdots + x_n = c$.

Proposition 1 *Assume* q *even. Take* $M \in M_{2,2}(\mathbb{F}_q)$, $M = (m_{ij})$, $i, i = 1, 2$.

(a) We have $\mathrm{Num}_1(M)_q = \{m_{11}\}$ *if and only if* $m_{22} = m_{11}$ *and* $m_{12} = m_{21}$.

(b) We have $\mathrm{Num}_1(M)_q = \mathbb{F}_q$ *if and only if* $m_{12} = m_{21}$ *and* $m_{22} \neq m_{11}$.

(c) If $m_{12} \neq m_{21}$ *and* $m_{11} \neq m_{22}$, *then* $\sharp(\mathrm{Num}_1(M)_q)) = q/2$.

Proof Fix $u = (x_1, x_2) \in C_2(1)_q$, i.e. assume $x_2 = x_1 + 1$ (Remark 5). We have $h_M(u) = (m_{11} + m_{12} + m_{21} + m_{22})x_1^2 + (m_{12} + m_{21})x_1 + (m_{12} + m_{21})$. If $m_{11} + m_{22} = m_{12} + m_{21} = 0$, then $\mathrm{Num}_1(M)_q = \{m_{11}\}$. If $m_{11} + m_{12} + m_{21} + m_{22} = 0$ and $m_{12} + m_{21} \neq 0$, then $\mathrm{Num}_1(M)_q = \mathbb{F}_q$. If $m_{11} + m_{12} + m_{21} + m_{22} \neq 0$ and $m_{12} + m_{21} = 0$, then $\mathrm{Num}_1(M) = \mathbb{F}_q$, because every element of $\mathbb{F}_q$ is a square. If $m_{11} + m_{12} + m_{21} + m_{22} \neq 0$ and $m_{12} + m_{21} \neq 0$, for any $\gamma \in \mathbb{F}_q$ the polynomial $(m_{11} + m_{12} + m_{21} + m_{22})t^2 + (m_{12} + m_{21})t + (m_{12} + m_{21}) + \gamma$ has 2 distinct roots in $\overline{\mathbb{F}}_q$ and either none of both roots are contained in $\mathbb{F}_q$. Thus, $\sharp(\mathrm{Num}_1(M)_q) = q/2$. □

Proposition 2 *Assume* q *even and take* $k \in \mathbb{F}_q^*$. *Take* $M = (m_{ij}) \in M_{n,n}(\mathbb{F}_q)$.

(a) We have $\sharp(\mathrm{Num}_k(M)) = 1$ *if and only if* $m_{ij} + m_{ji} = 0$ *for all* $i \neq j$ *and* $m_{ii} = m_{11}$ *for all* i.

(b) If $\sharp(\mathrm{Num}_k(M)) \neq 1$, *then* $\sharp(\mathrm{Num}_k(M)) \geq q/2$.

Proof By Remark 3 it is sufficient to do the case $k = 1$. By Remark 1 it is sufficient to prove the statements for the matrix $N = (n_{ij})$ with $n_{ii} = m_{ii}$ for all i, $n_{ij} = 0$ if $i > j$ and $n_{ij} = m_{ij} + m_{ij}$ if $i < j$. Take N with $\sharp(\mathrm{Num}_1(N)_q) = 1$. Applying Proposition 1 to all $N_{|\mathbb{F}_q e_i + \mathbb{F}_q e_j}$ we get the "only if" part of (a), while the "if" part is trivial. Proposition 1 also gives part (b). □

Proposition 3 *Assume q odd and take $k \in \mathbb{F}_q^*$ and $M := (m_{ij}) \in M_{2,2}(\mathbb{F}_q)$.*

(a) If k is not a square, assume $q \geq 7$. We have $\sharp(\mathrm{Num}_k(M)_q) = 1$ if and only if $m_{11} = m_{22}$ and either $m_{12} + m_{21} = 0$ or $q = 3, 5$.

(b) Assume $\sharp(\mathrm{Num}_k(M)_q) > 1$. We have $\sharp(\mathrm{Num}_k(M)_q) \geq \lceil (q - 1 + \eta)/4 \rceil$ with $\eta = 0$ if $q \equiv 1 \pmod 4$ and $\eta = 2$ if $q \equiv -1 \pmod 4$.

Proof We have $\mathrm{Num}_k(M)_q \neq \emptyset$. Take $u = (x_1, x_2)$ with $x_1^2 + x_2^2 = k$. By Lemma 6 we have $\sharp(C_2(k)_q) = q - 1 + \eta$. The map $u \mapsto h_M(u)$ induces a surjection $\pi : C_2(k)_q \to \mathrm{Num}_k(M)_q$. The map π is induced by the restriction to $C_2(1, k)$ of a homogeneous quadratic equation of $\mathbb{F}_q^2$. Since $C_2(k)_q$ is irreducible (even over the algebraic closure of $\mathbb{F}_q$), either π is a constant map or each of its fibers have cardinality at most 4, concluding the proof of part (b).

Now assume $\sharp(\mathrm{Num}_k(M)_q) = 1$. We get that the the restriction to $C_2(k)_q$ (i.e. taking $x_2^2 = k - x_{11}^2$) of the function $h(x_1, x_2) := (m_{11} - m_{22})x_{11}^2 + (m_{12} + m_{21})x_1x_2 - km_{22}$ is a constant function, i.e. $(m_{11} - m_{22})x_{11}^2 + (m_{12} + m_{21})x_1x_2$ is constant.

(i) First assume that k is a square in $\mathbb{F}_q$, say $k = c^2$. We have $c \neq 0$. Since $\mathrm{Num}_{c^2}(M)_q = c\mathrm{Num}_1(M)_q$ (Remark 4), it is sufficient to do the case $k = 1$. By the second part of Remark 4 we have $\{m_{11}, m_{22}\} \subseteq \mathrm{Num}_1(M)_q$ and thus $m_{11} = m_{22} = 0$. Taking $M - m_{11}\mathbb{I}_{2,2}$ instead on M we reduce to the case $m_{11} = m_{22} = 0$ by the first part of Remark 4. If $m_{12} + m_{21} = 0$, then $h_M \equiv 0$ and hence $\sharp(\mathrm{Num}_k(M)_q) = 1$. If $m_{12} + m_{21} \neq 0$, then Proposition 4 below gives $\sharp(\mathrm{Num}_k(M)_q) > 1$, unless $q = 3, 5$.

(ii) Now assume that k is not a square in $\mathbb{F}_q$. Set $E := \{(x_1, x_2, x_3) \in \mathbb{P}^2(\mathbb{F}_q) \mid x_1^2 + x_2^2 = kx_3^2\}$, so that $C_2(k)_q = E \setminus E \cap \{x_3 = 0\}$. Write $\mathrm{Num}_k(M)_k = \{\alpha\}$ and set $Z := \{(x_1, x_2, x_3) \in \mathbb{P}^2(\mathbb{F}_q) \mid m_{11}x_1^2 + m_{22}x_2^2 + (m_{12} + m_{21})x_1x_2 = \alpha x_3^2\}$. If $Z = \mathbb{P}^2(\mathbb{F}_q)$, then $\alpha = 0$ and $m_{11} = m_{22} = m_{12} + m_{21} = 0$ and hence $\mathrm{Num}_k(M)_q = \{0\}$. Hence, we may assume that Z is a conic defined over $\mathbb{F}_q$ (not necessarily a smooth conic). Since E is geometrically irreducible, either $E = Z$ or $\sharp(Z \cap E) \leq 4$. Since $\sharp(C_2(k)_q) > 4$, then $E = Z$. Thus, $m_{11} = m_{22}$ and $m_{12} + m_{21} = 0$. □

Proposition 4 *Take*

$$M = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$$

for some $b \in \mathbb{F}_q^*$.

(a) If q is even then $\sharp(\mathrm{Num}_1(M)_q) = q/2$; we have $\mathrm{Num}_1(M)_2 = \{0\}$ and $\mathrm{Num}_1(M)_q = b\mathbb{F}_{q/2}$ if $q > 2$.

(b) Assume that $q = p^e$ is odd, $e \geq 1$.

(b1) Assume that either e is even or that $(p^2-1)/8$ is even and that $q \equiv 1 \pmod 4$. Then $\sharp(\mathrm{Num}_1(M)_q) = (q + 3)/4$.

(b2) Assume that either e is even or that $(p^2-1)/8$ is even and that $q \equiv -1 \pmod 4$. Then $\sharp(\mathrm{Num}_1(M)_q) = (q+5)/4$.

(b3) Assume that e and $(p^2-1)/8$ are odd and that $q \equiv 1 \pmod 4$. Then $\sharp(\mathrm{Num}_1(M)_q) = (q-1)/4$.

(b4) Assume that e and $(p^2-1)/8$ are odd and that $q \equiv -1 \pmod 4$. Then $\sharp(\mathrm{Num}_1(M)_q) = (q+1)/4$.

Proof Taking $(1/b)M$ instead of M we reduce to the case $b = 1$. Take $u = (x_1, x_2)$ such that $x_1^2 + x_2^2 = 1$. We have $h_M(u) = x_1x_2$. Hence, $0 \in \mathrm{Num}(M)_q$ and $h_M(u) \neq 0$ if and only if $x_1 \neq 0$ and $x_2 \neq 0$.

(a) Assume that q is even and so $x_2 = x_1 + 1$ and $h_M(u) = x_1^2 + x_1$. If $q \geq 4$, the function $t \mapsto t^2 + t$ is a trace-function $\mathbb{F}_q \to \mathbb{F}_{q/2}$, while $t^2 + t = 0$ if $t \in \mathbb{F}_2$. Thus, $\mathrm{Num}_1(M)_2 = \{0\}$ and $\mathrm{Num}_1(M)_q = \mathbb{F}_{q/2}$ if $q > 2$.

(b) Assume that q is odd. Recall that $\sharp(C_2(1)_q) = q - 1$ if $q \equiv -1 \pmod 4$ and $\sharp(C_2(1)_q) = q + 1$ if $q \equiv 1 \pmod 4$ (Lemma 6). If $x_1^2 + x_2^2 = 1 = y_1^2 + y_2^2$ and $x_1x_2 = y_1y_2$, then $(x_1 + x_2)^2 = (y_1 + y_2)^2$ (i.e. either $x_1 + x_2 = y_1 + y_2$ or $x_1 + x_2 = -y_1 - y_2$) and $(x_1 - x_2)^2 = (y_1 - y_2)^2$ (i.e. either $x_1 - x_2 = y_1 - y_2$ or $x_1 - x_2 = y_2 - y_1$) and hence (since 2 is invertible in $\mathbb{F}_q$) either $(y_1, y_2) = (x_1, x_2)$ or $(y_1, y_2) = (x_2, x_1)$ or $(y_1, y_2) = (-x_1, -x_2)$ or $(y_1, y_2) = (-x_2, -x_1)$. If $x_i \neq 0$ for all i, $x_1 \neq x_2$ and $x_1 \neq -x_2$, then the set $A := \{(x_1, x_2), (-x_1, -x_2), (x_2, x_1), (-x_2, -x_1)\}$ has cardinality 4. If $x_1 = 0$, then $x_2 = \pm 1$ and the set A has cardinality 4. The same is true if $x_2 = 0$. If $x_2 = \pm x_1 \neq 0$, then A has cardinality 2. If $x_2 = \pm x_1$ we have $x_1^2 + x_2^2 = 1$ if and only if $x_1^2 = 1/2$ and this is the case for some $x_1 \in \mathbb{F}_q$ if and only if 2 is a square in $\mathbb{F}_q$. Write $q = p^e$ for some $e \geq 1$. 2 is a square in $\mathbb{F}_p$ if and only if $(p^2 - 1)/8$ is even by the Gauss reciprocity law ([5, Proposition 5.2.2]). If e is even, 2 is always a square in $\mathbb{F}_q$, because if a square-root of 2 is not contained in $\mathbb{F}_p$, then it generates $\mathbb{F}_{p^2} \supseteq \mathbb{F}_p$. If e is odd, $\mathbb{F}_q$ has a square-root of 2 if and only if $\mathbb{F}_p$ has a square-root of 2, because $\mathbb{F}_q$ contains $\mathbb{F}_p$, but not $\mathbb{F}_{p^2}$. Note that there is $A \subset C_2(1)_q$ with $x_2 = x_1$ if and only if there is $A \subset C_2(1)_q$ with $x_2 = -x_1$. Thus, we counted the cardinality of the fibers of the surjection $\pi : C_2(1)_q \to \mathrm{Num}(M)_q$ in terms of q (either all fibers have cardinality 4 or 2 have cardinality 2 and the other ones have cardinality 4). □

Proposition 4 shows that part (b) of Proposition 3 is often sharp.

Proposition 5 *Take $b, b' \in \mathbb{F}_q^*$ and set*

$$M = \begin{pmatrix} 0 & b & 0 \\ 0 & 0 & b' \\ 0 & 0 & 0 \end{pmatrix}$$

1. *If q is even and $b = b'$, then $\sharp(\mathrm{Num}_1(M)_q) = q/2$ with $\mathrm{Num}_1(M)_2 = \{0\}$ and $\mathrm{Num}_1(M)_q = b\mathbb{F}_{q/2}$ for all $q \geq 4$.*

2. *If q is even and $b \neq b'$, then $\mathrm{Num}_0(M)_q = \mathbb{F}_q$.*

3. *If $q \equiv 1 \pmod 4$, then $\mathrm{Num}_1(M) = \mathbb{F}_q$.*

Proof Taking b/b' instead of b and $\frac{1}{b'}M$ instead of M we reduce to the case $b' = 1$. Take $u = (x_1, x_2, x_3)$. We have $h_M(x_1, x_2, x_3) = x_2(bx_1 + x_3)$.

(a) Assume q even and take $x_3 = x_1 + x_2 + 1$, i.e. we compute $\mathrm{Num}_1(M)_q$. We get $h_M(x_1, x_2, x_3) = x_2((b-1)x_1 + x_2 + 1)$. First assume $b = 1$. In this case $h_M(x_1, x_2, x_3) = x_2^2 + x_2$ and hence $\mathrm{Num}_1(M)_q$ is the image of the trace map $x_2 \to x_2^2 + x_2$. Hence, $\sharp(\mathrm{Num}_1(M)_q) = q/2$ with $\mathrm{Num}_1(M)_2 = \{0\}$ and

$\mathrm{Num}_1(M)_q = b\mathbb{F}_{q/2}$ for all $q \ge 4$. Now assume $b \ne 1$. For any $c \in \mathbb{F}_q$ take $x_2 = 1$, $x_1 = c/(b-1)$, and $x_3 = x_1 + x_2 + 1$.

(b) Assume q even and take $x_3 = x_1 + x_2$, i.e. we compute $\mathrm{Num}_0(M)_q$. We have $h_M(x_1, x_2, x_3) = x_2((b+1)x_1 + x_2)$. Fix $c \in \mathbb{F}_q$. Since c is a square, say $c = s^2$, we take $x_2 = s$ and $x_1 = 0$.

(c) Assume $q \equiv 1 \pmod 4$. Hence, there is $\epsilon \in \mathbb{F}_q$ with $\epsilon^2 = -1$. Take $x_2 = 1$ and $x_3 = \epsilon x_1$, so that for any x_1 we have $x_1^2 + x_2^2 + x_3^2 = 1$. We have $h_M(x_1, x_2, x_3) = x_1(b+\epsilon)$ and hence $h_{M|C_3(1)_q}$ is surjective, i.e. $\mathrm{Num}_1(M) = \mathbb{F}_q$, if $b \ne -\epsilon$. Now assume $b = -\epsilon$. In this case we take $x_2 = 1$ and $x_3 = -\epsilon x_1$, so that for any x_1 we have $x_1^2 + x_2^2 + x_3^2 = 1$ and $h_M(x_1, x_2, x_3) = -2\epsilon x_1$. Hence, $h_{M|C_3(1)_q}$ is surjective. □

Proposition 6 *Fix $k \in \mathbb{F}_q$ and $b \in \mathbb{F}_q^*$. Set*

$$M = \begin{pmatrix} 0 & b & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & 0 & 0 & b \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Then $\mathrm{Num}_k(M)_q = \mathbb{F}_q$.

Proof Taking $\frac{1}{b}M$ instead of M we reduce to the case $b = 1$. If $u = (x_1, x_2, x_3, x_4)$, then $h_M(u) = x_1x_2 + x_2x_3 + x_3x_4$.

(a) Assume q even. Since $x_4 = k + x_3 + x_2 + x_1$, we get $h_M(u) = x_1x_2 + x_3^2 + x_1x_3 + kx_3$. For any $c \in \mathbb{F}_q$, take $x_3 = 0$, $x_1 = c$, and $x_2 = 1$.

(b) Assume q odd.

(b1) Assume that k is a nonzero square in $\mathbb{F}_q$. By Remark 3 we may assume $k = 1$. Taking $x_1 = 1$ and $x_2 = x_3 = x_4 = 0$ we see that $0 \in \mathrm{Num}_1(M)_q$. Set $x_2 = 1$ and hence $h_M(u) = x_1 + x_3(x_4 + x_3)$. Take $c \in \mathbb{F}_q^*$. We need to find $(x_1, x_3, x_4) \in \mathbb{F}_q^3$ with $x_1^2 + x_3^2 + x_4^2 = 0$ and $c = x_1 + x_3(x_4 + x_3)$, i.e. $(x_3, x_4) \in \mathbb{F}_q^2$ with $(c - x_3(x_4+x_3))^2 + x_3^2 + x_4^2 = 0$. The latter is the equation of an affine degree 4 curve $T \subset \mathbb{F}_q^2$. Call $J \subset \mathbb{P}^2(\mathbb{F}_q)$ the projective completion of its defining equation, i.e. the curve with $(cz^2 - x_3(x_4 + x_3))^2 + z^2x_3^2 + z^2x_4^2 = 0$ as its equation. If $T \ne \emptyset$, then we are done. Hence, we may assume $T = \emptyset$. The line at infinity $\{z = 0\}$ intersects J in the points $\{(0:1:0), (1:-1:0)\}$, which are singular points of J with multiplicity 2 and on them lie at most 4 points over the normalization of the reduced curve J; if J is geometrically irreducible with geometric genus 1, then there are at most 3 because at $(0:1:0)$ the tangent cone has z^2 as its equation.

Claim 1: Over $\overline{\mathbb{F}}_q$ J is not a union of lines (counting multiplicities) defined over $\overline{\mathbb{F}}_q$.

Proof of Claim 1: The singular points of J are its multiple components and the intersection of its components defined over $\overline{\mathbb{F}}_q$. At $(0:1:0)$ the equation of J has z^2 as its leading part and hence the tangent cone to J at $(0:1:0)$ is $\{z = 0\}$ counted with multiplicity 2. Hence, z^2 divides the equation of J, which is false.

Claim 2: J is not a union of two smooth conics defined over $\mathbb{F}_{q^2}$, but not over $\mathbb{F}_q$.

Proof of Claim 2: Assume that this is the case with $J = C_1 \cup C_2$. We have $\sigma(C_1) = C_2$ and $\sigma(C_2) = C_1$, where σ is induced by the Frobenius map $t \mapsto t^q$. The singular points of J are the points $C_1 \cap C_2$ and $(0:1:0)$, $(1:-1:0)$ are two of these points, both defined over $\mathbb{F}_q$. As in the proof of Claim 1 we get that

$\{z=0\}$ is the tangent line to both C_1 and C_2 at $(0:1:0)$. Writing $y=x_3+x_4$, the multiplicity 2 part at $(1:-1:0)$ of the equation of J is $x_3^2(y^2+z^2)$ and so C_1 and C_2 have different tangents at $(1:-1:0)$. We get that $C_1\cap C_2$ has exactly one point (call it o) outside the line $\{z=0\}$. Since $\sigma(C_i)=C_{3-i}$, $i=1,2$, and σ fixes $\{(0:1:0),(1:-1:0)\}$, we have $\sigma(o)=o$, i.e. $o\in\mathbb{F}_q^2$, i.e. $T\neq\emptyset$, a contradiction, concluding the proof of Claim 2.

An irreducible conic defined over $\mathbb{F}_q$ has $q+1$ points ([3, Table 7.2]). Since over $J\setminus T$ the normalization of J has at most 4 points, the Hasse–Weil lower bound for the number of points of a curve of genus ≤ 1 (applied if J is reducible to the connected components of its normalization) gives $T\neq\emptyset$ if $q+1>2\sqrt{q}+3$, i.e. if $q\geq 9$. All cases with $q\equiv 1\pmod 4$ are covered by Proposition 5. Take $q=3$; $u=(1,1,1,1)$ gives $0\in\mathrm{Num}_1(M)_3$; $u=(2,2,1,1)$ gives $1\in\mathrm{Num}_1(M)_q$; $u=(2,1,1,2)$ gives $2\in\mathrm{Num}(M)_3$. Take $q=7$; $u=(0,0,0,1)$ gives $0\in\mathrm{Num}_1(M)_7$; $u=(4,2,1,1)$ gives $4\in\mathrm{Num}_1(M)_7$; $u=(2,4,1,1)$ gives $6\in\mathrm{Num}_1(M)_7$; $u=(2,5,0,0)$ gives $3\in\mathrm{Num}_1(M)_7$; $u=(3,0,2,3)$ gives $1\in\mathrm{Num}_1(M)_7$; $u=(4,3,3,4)$ gives $5\in\mathrm{Num}_1(M)_7$; $u=(5,1,1,3)$ gives $2\in\mathrm{Num}_1(M)_7$.

(b2) Take $k=0$. $u=(0,0,0,0)$ gives $0\in\mathrm{Num}_0(M)_q$. Take $x_4=-x_2$ and so $h_M(u)=x_1x_2$. Fix $c\in\mathbb{F}_q^*$ and take $x_2=c/x_1$. We need to find $(x_1,x_3)\in T$, where $T\subset\mathbb{F}_q^2$ is the affine curve $x_1^4+c^2+x_1^2x_3^2=0$. Assume $T=\emptyset$ and call $J\subset\mathbb{P}^2(\mathbb{F}_q)$ the projective completion of the equation defining T, i.e. the curve with $x_1^4+z^4c^2+x_1^2x_3^2=0$ as its equation. $J\cap\{z=0\}$ contains the points $(0:1:0)$ (which has multiplicity 2 with x_1^2 as its tangent cone) and (over any extension of $\mathbb{F}_q$ on which -1 has a root) two other points at which J is smooth. Take the affine set $J'':=J\cap\{x_3\neq 0\}$. Taking $x_3=1$, $w=cz^2$, and $y=x_1^2$ we see that J is irreducible and that the normalization J' of J is a double covering of the rational curve $y^2+w^2=y$ ramified at at most 4 points. The Hasse–Weil lower bound gives $T\neq\emptyset$ if $q+1>2\sqrt{q}+3$, i.e. if $q\geq 9$. Now assume $q=3$; $u=(1,1,1,0)$ gives $2\in\mathrm{Num}_0(M)_3$; $u=(1,0,1,1)$ gives $1\in\mathrm{Num}_0(M)_3$. Now assume $q=5$; $u=(2,1,0,0)$ gives $2\in\mathrm{Num}_0(M)_5$; $u=(2,1,2,1)$ gives $1\in\mathrm{Num}_0(M)_5$; $u=(3,1,0,0)$ gives $3\in\mathrm{Num}_0(M)_5$; $u=(3,1,3,1)$ gives $4\in\mathrm{Num}_0(M)_5$. Now assume $q=7$; $u=(0,0,0,0)$ gives $0\in\mathrm{Num}_0(M)_7$; to get all squares it is sufficient to prove that $4\in\mathrm{Num}_0(M)_7$: take $u=(6,4,2,0)$; to get all nonsquares it is sufficient to prove that $5\in\mathrm{Num}_0(M)_7$: take $u=(3,1,2,0)$.

(b3) Take as k any nonsquare. Taking $x_2=x_3=0$ and x_1,x_4 with $x_1^2+x_4^2=k$ ([3, Lemma 5.1.4]) we see that $0\in\mathrm{Num}_k(M)_q$. We adapt the proof of step (b1). Set $x_2=1$ and hence $h_M(u)=x_1+x_3(x_4+x_3)$. Fix $c\in\mathbb{F}_q^*$. We need to find $(x_1,x_3,x_4)\in\mathbb{F}_q^3$ with $x_1^2+x_3^2+x_4^2=k-1$ and $c=x_1+x_3(x_4+x_3)$, i.e. $(x_3,x_4)\in\mathbb{F}_q^2$ with $(c-x_3(x_4+x_3))^2+x_3^2+x_4^2=k-1$. The latter is the equation of an affine degree 4 curve $T\subset\mathbb{F}_q^2$. Call $J\subset\mathbb{P}^2(\mathbb{F}_q)$ the projective completion of its equation, i.e. the curve with $(cz^2-x_3(x_4+x_3))^2+z^2x_3^2+z^2x_4^2=(k-1)z^4$ as its equation. If $T\neq\emptyset$, then we are done. Hence, we may assume $T=\emptyset$. The line at infinity $\{z=0\}$ intersects J in the points $\{(0:1:0),(1:-1:0)\}$, which are singular points of J with multiplicity 2 and on them lie at most 4 points over the normalization J' of the reduced curve J (at most 3 if J' is not rational). As in step (b1) we see that J is neither the union of 4 lines not defined over $\mathbb{F}_q$ nor the union of 2 smooth conics not defined over $\mathbb{F}_q$. Then using the Hasse–Weil bound we get $T\neq\emptyset$, unless $q=3,5,7$. Take $q=3$ and so $k=2$; $u=(1,1,0,0)$ gives $1\in\mathrm{Num}_2(M)_3$; $u=(2,1,0,0)$ gives $2\in\mathrm{Num}_2(M)_3$. Now assume $q=5$; we take $k=2$; $u=(1,1,0,0)$ gives $1\in\mathrm{Num}_2(M)_5$; $u=(2,1,1,1)$ gives $4\in\mathrm{Num}_2(M)_5$; $u=(2,2,2,0)$ gives $3\in\mathrm{Num}_2(M)_5$; $u=(4,4,1,2)$ gives $2\in\mathrm{Num}_2(M)_5$. Now assume $q=7$;

we take $k = 3$; $u = (3, 0, 0, 1)$ implies $0 \in \mathrm{Num}_3(M)_7$; $u = (0, 3, 1, 0)$ implies $3 \in \mathrm{Num}_3(M)_7$; $u = (1, 1, 1, 0)$ implies $2 \in \mathrm{Num}_3(M)_7$; $u = (1, 1, 0, 1)$ implies $1 \in \mathrm{Num}_3(M)_7$; $u = (4, 3, 3, 2)$ implies $6 \in \mathrm{Num}_3(M)_7$; $u = (3, 3, 3, 5)$ gives $5 \in \mathrm{Num}_3(M)_q$; $u = (5, 6, 1, 3)$ gives $4 \in \mathrm{Num}_3(M)_7$. □

Remark 6 *Fix an integer $n \geq 5$ and let $M = (m_{ij}) \in M_{n,n}(\mathbb{F}_q)$ be the Jordan matrix with a unique block, i.e. $m_{ij} = 0$, unless $j = i + 1$, $i = 1, \ldots, n - 1$. Taking $u = (x_1, \ldots, x_n) \in C_n(k)_q$ with $x_i = 0$ for all $i > 4$ we see that Proposition 5 implies* $\mathrm{Num}_k(M)_q = \mathbb{F}_q$.

References

[1] Ballico E. The Hermitian null-range of a matrix over a finite field. arXiv: 1611.08840.

[2] Coons JI, Jenkins J, Knowles D, Luke RA, Rault PX. Numerical ranges over finite fields. Linear Algebra Appl 2016; 501: 37-47.

[3] Hirschfeld JWP. Projective Geometries over Finite Fields. Oxford, UK: Clarendon Press, 1979.

[4] Hirschfeld JWP, Thas JA. General Galois Geometries. Oxford, UK: Oxford University Press, 1991.

[5] Ireland K, Rosen M. A Classical Introduction to Modern Number Theory. New York, NY, USA: Springer, 1982.

[6] Small C. Arithmetic of Finite Fields. New York, NY, USA: Marcel & Dekker, 1973.