A PROPERTY OF THE INVERSE OF A SUBSPACE OF A
FINITE FIELD

SANDRO MATTAREI

Abstract. We prove a geometric property of the set $A^{-1}$ of inverses of the
nonzero elements of an $F_q$-subspace $A$ of a finite field involving the size of its
intersection with two-dimensional $F_q$-subspaces. We give some applications,
including a new upper bound on $|A^{-1} \cap B|$ when $A$ and $B$ are $F_q$-subspaces of
different dimension of a finite field, satisfying a suitable natural assumption.

1. Introduction

The inversion map $x \mapsto x^{-1}$ in a finite field has been the object of various
studies in recent years. In particular, its interaction with the operation of addi-
tion is of interest for cryptographic applications. The best-known example is
that inversion in the finite field of $2^8$ elements (patched by sending zero to it-
self) is the nonlinear transformation employed in the S-boxes in the Advanced
Encryption Standard (Rijndael, see [FIP01]). A study of an AES-like cryptosys-
tem in [CDVS09] required, in the special case of finite fields, the determina-
tion of the additive subgroups of a field which are closed with respect to inverting
nonzero elements, which was provided by the author in [Mat07]. (The more
general question in division rings was independently answered in [GGSZ06].) A
small variation of this fact was required in [KLS12] for a different crypto-
graphic application, and a more substantial generalization was studied in [Csa13],
to which we will return later in this Introduction. All those studies involve a set
$A^{-1} = \{x^{-1} : 0 \neq x \in A\}$, where $A$ is an $F_q$-subspace of a finite field.

In this note we prove a geometric property of $A^{-1}$. Because the specific ambi-
et finite field plays no role in our result, it will be equivalent, but notationally
simpler, to rather work inside an algebraic closure $\overline{F_q}$ of $F_q$. Our result then
reads as follows.

Theorem 1. Let $A$ be an $F_q$-subspace of $\overline{F_q}$, of dimension $d$. Let $U$ be a two-
dimensional $F_q$-subspace of $\overline{F_q}$, and suppose $|A^{-1} \cap U| > d(q-1)$. Then $U^{-1} \subseteq A$,
and the $F_q$-span of $U^{-1}$ is a one-dimensional $F_q$-subspace of $\overline{F_q}$, for some $e$.

Because set $A^{-1}$ is closed with respect to scalar multiplication by elements of
$F_q^*$, it is natural to interpret its properties in a projective space $\mathbb{P}V$, where $V$ is an

2000 Mathematics Subject Classification. Primary 11T30; secondary 51E20.
Key words and phrases. finite field, subspace, inverse, arc, cap.
$\mathbb{F}_q$-linear subspace of $\mathbb{F}_q$ containing $A^{-1}$. (To resolve possible ambiguities, in this paper the operator $\mathbb{P}$ will only be applied to vector spaces over the field $\mathbb{F}_q$.) From this geometric viewpoint, the two-dimensional space $U$ of Theorem 1 represents a line in a projective space, and the condition on the integer $|A^{-1} \cap U|/(q - 1)$, which clearly equals $|A \cap U^{-1}|/(q - 1)$, can be read in terms of caps or arcs according as whether we focus our attention on $A^{-1}$ or $U^{-1}$. We present some applications of our result which exploit, in turn, one or the other interpretation.

Our first application of Theorem 1 is a simpler proof of the main result of [FKMP02], which is their Theorem 3.3, and generalizes the following result of M. Hall [Hal74]: in the cyclic model of the projective plane $\text{PG}(2, q)$, the inverse of a line is a conic. We will explain this terminology, and state and prove the main result of [FKMP02] in Section 2, after proving Theorem 1.

Our next application, which we formalize in Theorem 3, uses Theorem 1 to deduce an upper bound on $|A^{-1} \cap B|/(q - 1)$ from any available general bounds on (higher) caps, where $A$ and $B$ are finite-dimensional subspaces of $\mathbb{F}_q$. Theorem 1 is the special case of this where $B$ has dimension two. Of course a non-trivial bound can only be obtained provided one steers away from some special configurations, such as the extreme case $A^{-1} \subseteq B$. By employing a general bound on caps our result yields $|A^{-1} \cap B| \leq (d - 1)|B|/q + q - d$, where $|A| = q^d$, under the assumption that $A$ does not contain any nonzero $\mathbb{F}_q$-subspace of $\mathbb{F}_q$ with $e > 1$.

The special case of this bounding problem where $|A| = |B|$ was studied in [Csaj13], and then in [Mat]. In particular, in the former Csajbók proved the general bound $|A^{-1} \cap B| \leq 2|B|/q - 2$, for any subspaces $A$ and $B$ of $\mathbb{F}_q$, of the same (finite) dimension, such that $A^{-1} \not\subseteq B$. This surpasses the bound given by our Theorem 3 when $|A| = |B| = q^d > q^3$. However, the method of [Csaj13], which expands on a polynomial argument of the author in [Mat07], seems unsuited to deal with the case $|A| > |B|$, where our Theorem 3 provides the only known nontrivial bound. (Note that our bound is larger than $|B| - 1$ when $|A| < |B|$, and hence trivial.)

Furthermore, Theorem 3 produces a contribution to the case $|A| = |B| = q^3$, where a slightly better available bound on caps yields $|A^{-1} \cap B| < 2|B|/q - 2$ apart from a special situation. Our final application of Theorem 3 is then the determination, in Theorem 5 of an exceptional geometric configuration which occurs when equality is attained in Csajbók’s bound for $|A| = |B| = q^3$: the image of $A^{-1} \cap B$ in $\mathbb{P}B$ is then the union of a conic and an external line. As we explain in Section 3, that result is included in a more general investigation in [Mat], but the short proof given here bypasses longer and more demanding arguments employed there.

The author is grateful to Bence Csajbók for interesting discussions on this topic.
A PROPERTY OF THE INVERSE OF A SUBSPACE OF A FINITE FIELD

2. A PROOF OF THEOREM 1 AND AN APPLICATION INVOLVING ARCS

Proof of Theorem 1. Our hypothesis means that there exist \( \xi, \eta \in \mathbb{F}_q \) with \( U = \mathbb{F}_q \xi + \mathbb{F}_q \eta \), and \( d \) distinct \( \alpha_1, \ldots, \alpha_d \in \mathbb{F}_q \), such that \( \eta, \xi, \eta, \ldots, \xi + \alpha_{d-1} \eta \in A^{-1} \).

The inverses of those elements must then be linearly dependent over \( \mathbb{F}_q \), because \( A \) has dimension \( d \). Consider a shortest linear dependence relation among them. Possibly after permuting those elements, which may include redefining \( \eta \), the relation takes the form

\[
\frac{1}{\eta} + \sum_{i=1}^{e} \frac{\beta_i}{\xi + \alpha_i \eta} = 0,
\]

for some \( \beta_1, \ldots, \beta_e \in \mathbb{F}_q^* \), with \( 2 \leq e \leq d \). Clearing the denominators we find that the pair \( (\xi, \eta) \) is a zero of a homogeneous polynomial of degree \( e \) with coefficients in \( \mathbb{F}_q \) and, consequently, \( \xi/\eta \in \mathbb{F}_q^* \) for some \( t \leq e \). Because \( \xi/\eta, \xi/(\xi + \alpha_1 \eta), \ldots, \xi/(\xi + \alpha_{e-1} \eta) \) belong to \( \mathbb{F}_q^* \) are linearly independent over \( \mathbb{F}_q \), we have \( t = e \), and they form a basis of \( \mathbb{F}_q^* \) over \( \mathbb{F}_q \). Hence the elements \( 1/\eta, 1/(\xi + \alpha_1 \eta), \ldots, 1/(\xi + \alpha_{e-1} \eta) \) of \( A \cap U^{-1} \) span the one-dimensional \( \mathbb{F}_q^* \)-subspace \( \mathbb{F}_q^* \xi^{-1} \) of \( \mathbb{F}_q^* \). Because \( \eta \) and \( \xi + \alpha_1 \eta \) belong to \( (\mathbb{F}_q^* \xi^{-1})^{-1} \cup \{0\} = \mathbb{F}_q^* \xi \) and their \( \mathbb{F}_q^* \)-span equals \( U \), we have \( U \subseteq \mathbb{F}_q^* \xi \), and hence \( U^{-1} \subseteq \mathbb{F}_q^* \xi^{-1} \subseteq A \). \( \square \)

In order to formulate our first application of Theorem 1, we need to introduce some terminology. The cyclic model of \( PG(n, q) \) is the \( n \)-dimensional projective space \( \mathbb{P} \mathbb{F}_{q^{n+1}} \), with the added cyclic group structure induced by the multiplicative group \( \mathbb{F}_{q^{n+1}}^* \). The inverse (called the additive inverse in [FKMP02]) of a subset of the cyclic model of \( PG(n, q) \) must be intended with respect to the group operation. An arc in \( PG(n, q) \) is a set of \( k \geq n + 1 \) points of which no \( n + 1 \) lie on the same hyperplane. We use our Theorem 1 to prove the main result of [FKMP02], which reads as follows.

**Theorem 2** (Theorem 3.3 of [FKMP02]). If \( q + 1 > n \), then in the cyclic model of \( PG(n, q) \) the inverse of any line is an arc in some subspace \( PG(m, q) \), where \( m + 1 \) divides \( n + 1 \).

Proof. A line in the cyclic model of \( PG(n, q) \) is the image in \( \mathbb{P} \mathbb{F}_{q^{n+1}} \) of a two-dimensional \( \mathbb{F}_q \)-subspace \( U \) of \( \mathbb{F}_{q^{n+1}} \). Fix such a line and let \( V \) be the \( \mathbb{F}_q \)-span of \( U^{-1} \). If \( V \) has dimension \( m + 1 \) then \( \mathbb{P} V \) is a projective geometry \( PG(m, q) \). Any hyperplane in \( \mathbb{P} V \), which is the image of an \( m \)-dimensional \( \mathbb{F}_q \)-subspace \( A \) of \( V \), meets the image of \( U^{-1} \) in \( \mathbb{P} V \) in at most \( m \) points, otherwise Theorem 1 would be contradicted because \( U^{-1} \not\subseteq A \). Hence the image of \( U^{-1} \), which is the inverse of our line, is an arc in \( \mathbb{P} V \).

It remains to show that \( m + 1 \) divides \( n + 1 \), and to this purpose we may assume \( m < n \). Because \( |V \cap U^{-1}|/(q - 1) = |U^{-1}|/(q - 1) = q + 1 > m + 1 \), an application of Theorem 1 with \( V \) in place of \( A \) shows that \( V \) is a one-dimensional
\( \mathbb{F}_{q^e} \)-subspace of \( \mathbb{F}_q \), whence \( e = m + 1 \). Because \( V \subseteq \mathbb{F}_{q^{n+1}} \) it follows that 
\( \mathbb{F}_{q^{m+1}} \subseteq \mathbb{F}_{q^{n+1}} \), and hence \( m + 1 \) divides \( n + 1 \). \( \square \)

If \( n + 1 \) is a prime in Theorem 2, one concludes with [FKMP02] that the inverse of a line is an arc in \( PG(n, q) \), and for \( n = 2 \) one recovers the result of M. Hall mentioned in the introduction.

3. Applications involving caps

Our next application of Theorem 1 concerns caps rather than arcs. A \((k, r)\)-cap in the projective geometry \( PG(n, q) \) is a set of \( k \) points, of which no \( r + 1 \) are collinear. (A variant of this definition requires that the set contains at least one set of \( r \) collinear points, but this difference is immaterial here.) The largest size \( k \) of a \((k, r)\)-cap in \( PG(n, q) \) is denoted by \( m_{r}(n, q) \).

**Theorem 3.** Let \( A \) and \( B \) be \( \mathbb{F}_q \)-subspaces of \( \mathbb{F}_q \) of size \( q^d \) and \( q^{d'} \), respectively. Suppose that \( A \) does not contain any nonzero \( \mathbb{F}_q^e \)-subspace of \( \mathbb{F}_q \) with \( e > 1 \). Then \( |A^{-1} \cap B|/(q-1) \leq m_d(d'-1,q) \).

**Proof.** Suppose for a contradiction that the desired conclusion is violated, that is, \( |A^{-1} \cap B|/(q-1) = k > m_d(d'-1,q) \). Then the image of \( A^{-1} \cap B \) in \( \mathbb{P}B \cong PG(d'-1, q) \) is not a \((k, d)\)-cap, and hence it meets a line in \( \mathbb{P}B \) in more than \( d \) points. According to Theorem 1 the preimage \( U \) in \( B \) of that line is contained in some one-dimensional \( \mathbb{F}_q^e \)-subspace \( \mathbb{F}_q^e \xi \) of \( \mathbb{F}_q \) with \( e > 1 \), which in turn is contained in \( A^{-1} \cup \{0\} \). But then \( A \) contains \( \mathbb{F}_q^e \xi^{-1} \), contradicting our hypotheses. \( \square \)

When \( d > 3 \) the only general bound on cap sizes available for use in Theorem 1 is \( m_r(t, q) \leq 1 + (r-1) \cdot (q^t-1)/(q-1) \), which is easily proved by considering all lines which pass through a fixed point of the cap. The conclusion of Theorem 1 then reads \( |A^{-1} \cap B| \leq (d-1)q^{d-1} + q - d \). As we noted in the Introduction, this is nontrivial when \( d \geq d' \), and new when \( d > d' \), whereas neither the polynomial method used in [Csa13], nor its more powerful variant employed in [Mat], seem capable to produce any essentially nontrivial bound in the latter case. When \( d' = 3 \) our bound can perhaps be more conveniently written as \( |A^{-1} \cap B|/(q-1) \leq (d-1)q + d \).

When \( d = d' \geq 2 \) the bound we have just given is worse than the bound \( |A^{-1} \cap B| \leq 2q^{d-1} - 2 \) proved by Csajbók in [Csa13]. (They match when \( d = d' = 2 \), an easy case briefly discussed in [Mat, Section 2].) For \( d > 3 \) the author strengthened Csajbók’s bound to \( |A^{-1} \cap B| \leq q^{d-1} + O_d(q^{d-3/2}) \) in [Mat]. However, Csajbók’s bound is sharp when \( d = 3 \), and the following corollary of Theorem 3 provides crucial information on the case where equality is attained.
Corollary 4. Suppose $q > 3$. Let $A$ and $B$ be $\mathbb{F}_q$-subspaces of $\overline{\mathbb{F}}_q$ of size $q^3$, with $A^{-1} \not\subseteq B$. If $|A^{-1} \cap B|/(q - 1) > 2q + 1$, then $(A^{-1} \cap B) \cup \{0\}$ contains a one-dimensional $\mathbb{F}_{q^2}$-subspace of $\overline{\mathbb{F}}_q$.

Proof. The general bound for $m_r(t, q)$ recalled above reads $m_3(2, q) \leq 2q + 3$ in the case of present interest. However, the latter can be improved to $m_3(2, q) \leq 2q + 1$ for $q > 3$, see [Hir98, Corollary 12.11 and Theorem 12.47]. Consequently, under our hypothesis the conclusion of Theorem 3 does not hold, and hence the argument in the proof of Theorem 3 applies. We necessarily have $e = 2$, the one-dimensional $\mathbb{F}_{q^2}$-subspace $\mathbb{F}_{q^2}\xi$ of $\overline{\mathbb{F}}_q$ found there coincides with $U$, and hence it is not only contained in $A^{-1} \cup \{0\}$, but in $B$ as well. □

The information contained in the conclusion of Corollary 3 together with a further appeal to Theorem 3 and to a classical result of B. Segre, is sufficient to determine the geometric structure of the set $A^{-1} \cap B$ for three-dimensional $\mathbb{F}_q$-subspaces which attain equality in Csajbók's bound, as follows.

Theorem 5. Suppose $q$ odd and $q > 3$. Let $A$ and $B$ be $\mathbb{F}_q$-subspaces of $\overline{\mathbb{F}}_q$ of size $q^3$, with $A^{-1} \not\subseteq B$, such that $|A^{-1} \cap B|/(q - 1) = 2q + 2$. Then the image of $A^{-1} \cap B$ in $\mathbb{P}B$ is the union of a line and a conic.

Proof. According to Corollary 3 the set $(A^{-1} \cap B) \cup \{0\}$ contains a one-dimensional $\mathbb{F}_{q^2}$-subspace $\mathbb{F}_{q^2}\xi$ of $\overline{\mathbb{F}}_q$. After replacing the subspaces $A$ and $B$ with $\xi A$ and $\xi^{-1}B$, which changes neither the hypotheses nor the conclusion, we may assume that $(A^{-1} \cap B) \cup \{0\}$ contains the subfield $\mathbb{F}_{q^2}$ of $\overline{\mathbb{F}}_q$. Thus, both $A$ and $B$ contain $\mathbb{F}_{q^2}$. The image of $\mathbb{F}_{q^2}$ in the two-dimensional projective space $\mathbb{P}(B)$ is the required line.

Now set $C := (A^{-1} \cap B) \setminus \mathbb{F}_{q^2}$. We claim that any two-dimensional $\mathbb{F}_q$-subspace $U$ of $B$ meets $C$ in at most $2(q - 1)$ elements. Assuming $U \neq \mathbb{F}_{q^2}$ as we obviously may, we have $|U \cap \mathbb{F}_{q^2}| = q$. By way of contradiction, suppose that $|C \cap U| > 2(q - 1)$. Then $|A^{-1} \cap U| > 3(q - 1)$, and hence $U^{-1}$ spans a one-dimensional $\mathbb{F}_{q^2}$-subspace of $\mathbb{F}_q$ according to Theorem 3. This being clearly not the case, we have to concede that $|C \cap U| \leq 2(q - 1)$. Thus, the image of $C$ in the two-dimensional projective space $\mathbb{P}(B)$ is an arc with $q + 1$ points. According to a celebrated result of B. Segre [Hir98, Theorem 8.14], when $q$ is odd any such arc is a conic. □

The very special case of Theorem 3 where $A = B \subseteq \mathbb{F}_{q^2}$ was proved by Csajbók [Csa13, Theorem 4.8, Assertion (3)]. A much more general result than Theorem 3 was proved by the author by different methods in [Mat, Theorem 9], which gives a classification, and with it a precise count in a suitable sense, of all pairs of three-dimensional $\mathbb{F}_q$-subspaces $A, B$ of $\overline{\mathbb{F}}_q$ such that $|A^{-1} \cap B|/(q - 1) = \{2q, 2q + 1, 2q + 2\}$, with no restriction on the parity of $q$ (with $q > 5$ for the two smaller values). It turns out that in all those cases the image of $A^{-1} \cap B$ in $\mathbb{P}B$ is the union of a nonsingular conic and a secant, tangent or external line in
the three cases. The intermediate case occurs only for even $q$, and the other two cases only for odd $q$.

References

[CDVS09] Andrea Caranti, Francesca Dalla Volta, and Massimiliano Sala, *An application of the O’Nan-Scott theorem to the group generated by the round functions of an AES-like cipher*, Des. Codes Cryptogr. 52 (2009), no. 3, 293–301. MR 2506729 (2010a:94053)

[Csa13] Bence Csajbók, *Linear subspaces of finite fields with large inverse-closed subsets*, Finite Fields Appl. 19 (2013), 55–66. MR 2996759

[FIP01] FIPS Publication 197 (NIST), *Advanced Encryption Standard*, 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[FKMP02] Giorgio Faina, György Kiss, Stefano Marcugini, and Fernanda Pambianco, *The cyclic model for PG(n,q) and a construction of arcs*, European J. Combin. 23 (2002), no. 1, 31–35. MR 1878772 (2003b:51017)

[GGSZ06] Daniel Goldstein, Robert M. Guralnick, Lance Small, and Efim Zelmanov, *Inversion invariant additive subgroups of division rings*, Pacific J. Math. 227 (2006), no. 2, 287–294. MR 2263018 (2007i:17041)

[Hal74] M. Hall, Jr., *Difference sets*, Combinatorics, Part 3: Combinatorial group theory (Proc. NATO Advanced Study Inst., Breukelen, 1974), Math. Centrum, Amsterdam, 1974, pp. 1–26. Math. Centre Tracts, No. 57. MR 0457254 (56 #15462)

[Hir98] James W. P. Hirschfeld, *Projective geometries over finite fields*, second ed., Oxford Mathematical Monographs. The Clarendon Press Oxford University Press, New York, 1998. MR 1612570 (99b:51006)

[KLS12] Gábor Korchmáros, Valentino Lanzone, and Angelo Sonnino, *Projective $k$-arcs and 2-level secret-sharing schemes*, Des. Codes Cryptogr. 64 (2012), no. 1-2, 3–15. MR 2914398

[Mat] S. Mattarei, *Inversion and subspaces of a finite field*, arXiv:1311.3644, submitted.

[Mat07] Sandro Mattarei, *Inverse-closed additive subgroups of fields*, Israel J. Math. 159 (2007), 343–347. MR 2342485 (2008j:12008)

E-mail address: mattarei@science.unitn.it

Dipartimento di Matematica, Università degli Studi di Trento, via Sommarive 14, I-38123 Povo (Trento), Italy