On subsets of the normal rational curve

Simeon Ball and Jan De Beule

Abstract

A normal rational curve of the $(k-1)$-dimensional projective space over $\mathbb{F}_q$ is an arc of size $q+1$, since any k points of the curve span the whole space. In this article we will prove that if q is odd then a subset of size $3k-6$ of a normal rational curve cannot be extended to an arc of size $q+2$. In fact, we prove something slightly stronger. Suppose that q is odd and E is a $(2k-3)$-subset of an arc G of size $3k-6$. If G projects to a subset of a conic from every $(k-3)$-subset of E then G cannot be extended to an arc of size $q+2$. Stated in terms of error-correcting codes we prove that a k-dimensional linear maximum distance separable code of length $3k-6$ over a field $\mathbb{F}_q$ of odd characteristic, which can be extended to a Reed-Solomon code of length $q+1$, cannot be extended to a linear maximum distance separable code of length $q+2$.

1. *Introduction*

Let $\mathrm{V}_k(\mathbb{F}_q)$ denote the k-dimensional vector space over $\mathbb{F}_q$, the finite field with q elements.

Let $\mathrm{PG}_{k-1}(\mathbb{F}_q)$ denote the $(k-1)$-dimensional projective space over $\mathbb{F}_q$.

An arc S is a set of vectors of $\mathrm{V}_k(\mathbb{F}_q)$ in which every subset of S of size k is a basis of the space, i.e. every k-subset is a set of linearly independent vectors. Equivalently, an arc of $\mathrm{PG}_{k-1}(\mathbb{F}_q)$ is a set of points in which every subset of size k spans the whole space.

The set of columns of a generator matrix of a k-dimensional linear maximum distance separable (MDS) code over $\mathbb{F}_q$ is an arc of $\mathrm{V}_k(\mathbb{F}_q)$ and vice-versa, so arcs and linear MDS codes are equivalent objects. As in coding theory, we define the *weight* of a vector to be the number of non-zero coordinates that it has.

A normal rational curve is a set of $q+1$ vectors of $\mathrm{V}_k(\mathbb{F}_q)$

$$S=\{(1,t,t^2,\dots,t^{k-1}) \mid t\in\mathbb{F}_q\}\cup\{(0,\dots,0,1)\},$$

or equivalently a set of $q+1$ points of $\mathrm{PG}_{k-1}(\mathbb{F}_q)$.

It is easy to see that a normal rational curve is an arc, since taking any k elements of S we can form a $k\times k$ Vandermonde matrix whose determinant is non-zero. Thus, any k vectors of S are linearly independent.

In 1986, Seroussi and Roth [**8**] proved that if $4\leqslant k\leqslant (q+3)/2$ then a normal rational curve cannot be extended to an arc of size $q+2$. In 1992, Storme [**9**] extended this result to $4\leqslant k\leqslant q+2-6\sqrt{q\ln q}$. In this article we will prove that if q is odd then a subset of size $3k-6$ of a normal rational curve cannot be extended to an arc of size $q+2$. Every $(k+2)$-arc is uniquely extendable to a normal rational curve, [**6**, Theorem 27.5.1]. Therefore, an arc G of size $3k-6\geqslant k+2$ which is contained in a normal rational curve, is contained in a unique normal rational curve which, by the results just mentioned, cannot be extended to an arc of

2000 *Mathematics Subject Classification* 51E21, 15A03, 94B05.

The first author acknowledges the support of the project MTM2014-54745-P of the Spanish *Ministerio de Economía y Competitividad.* The second author has been supported by a postdoctoral fellowship of the Research Foundation Flanders (Belgium) – FWO, and by a research grant of the Research Foundation Flanders (Belgium) – FWO, no. 1504514N.

size $q+2$. What we prove here is somehwat stronger, that G does not extend to any arc of size $q+2$.

Lemma 1.1 and Lemma 1.2 follow from [**6**, Theorem 27.5.1 and Lemma 27.5.2]. We include a proof for the sake of completeness.

LEMMA 1.1. *The projection of a normal rational curve of* $\mathrm{PG}_{k-1}(\mathbb{F}_q)$ *from any vector of the normal rational curve is contained in a normal rational curve of* $\mathrm{PG}_{k-2}(\mathbb{F}_q)$.

Proof. Suppose we wish to project

$$S = \{(1,t,\ldots,t^{k-1}) \mid t \in \mathbb{F}_q\} \cup \{(0,\ldots,0,1)\},$$

from the point

$$x = (1,s,s^2,\ldots,s^{k-1}).$$

There is a change of basis matrix of $\mathrm{V}_k(\mathbb{F}_q)$ that maps

$$(1,t,t^2,\ldots,t^{k-1}) \mapsto ((ct+d)^{k-1},(ct+d)^{k-2}(at+b),\ldots,(ct+d)(at+b)^{k-2},(at+b)^{k-1}),$$

where $ad \neq bc$. Hence, we can find a change of basis that changes the coordinates of x to $(0,\ldots,0,1)$ and fixes S set-wise. Projecting from x is equivalent to deleting the last coordinate, so the projection of S is contained in a normal rational curve of $\mathrm{PG}_{k-2}(\mathbb{F}_q)$. □

LEMMA 1.2. *The projection of a normal rational curve of* $\mathrm{PG}_{k-1}(\mathbb{F}_q)$ *from any* $k-3$ *vectors of the normal rational curve is contained in a conic of* $\mathrm{PG}_2(\mathbb{F}_q)$.

Proof. Let $D=\{x_1,\ldots,x_{k-3}\}$ be $k-3$ vectors of the normal rational curve. By Lemma 1.1, the projection of a normal rational curve of $\mathrm{PG}_{k-1}(\mathbb{F}_q)$ from x_1 is contained in a normal rational curve of $\mathrm{PG}_{k-2}(\mathbb{F}_q)$. Projecting this projection from the projection of x_2 we obtain a set contained in a normal rational curve of $\mathrm{PG}_{k-3}(\mathbb{F}_q)$. Continuing in this way we see that the projection from D of the normal rational curve is contained in a normal rational curve (i.e. a conic) of $\mathrm{PG}_2(\mathbb{F}_q)$. □

The aim of this article is to prove the following theorem.

THEOREM 1.3. *Suppose* q *is odd and* G *is an arc of* $\mathrm{PG}_{k-1}(\mathbb{F}_q)$ *of size* $3k-6$. *Suppose that* E *is a subset of* G *of size* $2k-3$ *and that* G *projects to a subset of a conic from every* $(k-3)$*-subset of* E. *Then* G *cannot be extended to an arc of size* $q+2$.

The following theorem follows immediately from Lemma 1.2 and Theorem 1.3.

THEOREM 1.4. *If* q *is odd then a subset of* $3k-6$ *points on a normal rational curve of* $\mathrm{PG}_{k-1}(\mathbb{F}_q)$ *cannot be extended to an arc of size* $q+2$.

Stated in terms of error-correcting codes, Theorem 1.4 says the following.

Theorem 1.5. *A k-dimensional linear maximum distance separable code of length $3k-6$ over a field $\mathbb{F}_q$ of odd characteristic, which can be extended to a Reed-Solomon code of length $q+1$, cannot be extended to a linear maximum distance separable code of length $q+2$.*

Note that some authors refer to the Reed-Solomon code as the cyclic code of length $q-1$, obtained from the normal rational curve by deleting the columns $(1,0,\ldots,0)$ and $(0,\ldots,0,1)$ in the generator matrix, and the code of length $q+1$ as the doubly-extended Reed-Solomon code.

2. *A set of equations associated with an arc*

Let $\det(v_1,\ldots,v_k)$ denote the determinant of the matrix whose i-th row is v_i, a vector of $\mathrm{V}_k(\mathbb{F}_q)$. If $C=\{p_1,\ldots,p_{k-1}\}$ is an ordered set of $k-1$ vectors then we write

$$\det(u,C)=\det(u,p_1,\ldots,p_{k-1}),$$

where we evaluate the determinant with respect to a fixed canonical basis.

Throughout S will be an arbitrarily ordered arc of size $q+k-1-t$ of $\mathrm{V}_k(\mathbb{F}_q)$.

Let C be a subset of S of size $k-1$. There is a non-zero element $\alpha_C\in\mathbb{F}_q$, such that the following lemma holds, see [**2**, Lemma 7.20] or [**3**, Lemma 17].

Lemma 2.1. *Let E be a subset of S of size $k+t$. For any subset A of E of size $k-2$,*

$$\sum_C \alpha_C \prod_{z\in E\setminus C} \det(z,C)^{-1}=0,$$

where the sum runs over the subsets C of E of size $k-1$ containing A.

It is important to note that α_C does not depends on E or A, so Lemma 2.1 gives us a lot of equations involving the same quantity, α_C. This is what we are going to exploit.

In this article we will use the following set of equations, which are deduced from the equations in Lemma 2.1.

Lemma 2.2. *Suppose that q is odd. Let E be a subset of S of size $k+t-1$ and let $e\in S\setminus E$. For any subset D of E of size $k-3$,*

$$\sum_C \alpha_C \prod_{z\in (E\cup\{e\})\setminus C} \det(z,C)^{-1}=0,$$

where the sum runs over the subsets C of E of size $k-1$ containing D.

Proof. Let us call the equation in Lemma 2.1, eq(A). Then for any D which is a subset of E of size $k-3$, consider

$$-\mathrm{eq}(D\cup\{e\})+\sum_{a\in E\setminus(D\cup\{e\})}\mathrm{eq}(D\cup\{a\}).$$

The terms for which $e\in C$ cancel and the terms for which $e\notin C$ appear twice. Since q is odd we obtain the equation stated in the lemma. □

Lemma 2.2 demonstrates that the set of equations we obtain from Lemma 2.1 for q odd, behaves very differently from the set of equations we obtain from Lemma 2.1 for q even. Indeed, for q odd, the equations in Lemma 2.2 imply that for a fixed subset E of size $k+t-1$, all the elements of $S \setminus E$ must satisfy the some set of equations, one equation for each subset D of E of size $k-3$.

Since S is an arc, every $(k-1)$-subset $C = \{p_1, \ldots, p_{k-1}\}$ of S spans a hyperplane. In the dual space this hyperplane is a vector. To explicitly work with this vector we set up a duality between $\mathrm{V}_k(\mathbb{F}_q)$ and its dual space. Let

$$x_j = (-1)^{j+1} \det(p_1, \ldots, p_{k-1}),$$

where the j-th coordinate of $p_1, \ldots, p_{k-1}$ has been deleted.

This allows us to write

$$\det(u, C) = u \cdot x,$$

where $x = (x_1, \ldots, x_k)$ and $\cdot$ is the standard scalar product, which by abusing notation slightly, we will write as $u \cdot C$.

We will use the word *point* for a 1-dimensional subspace of $\mathrm{V}_k(\mathbb{F}_q)$ and *line* for a 2-dimensional subspace of $\mathrm{V}_k(\mathbb{F}_q)$ and likewise for the dual space. Thus, in the dual space, the subspace spanned by a set C of $(k-1)$ vectors of S is a point and the subspace spanned by a set A of $k-2$ vectors of S is a line. Again, we will abuse notation slightly and refer to C as a point of the dual space and A as a line of the dual space.

In the following lemma, $X = (X_1, \ldots, X_k)$.

LEMMA 2.3. *Suppose that A and U are disjoint subsets of an arc of $\mathrm{V}_k(\mathbb{F}_q)$ of sizes $k-2$ and $n+1$ respectively. If*

$$\psi(X) = \sum_{w \in U} \lambda_w \prod_{u \in U \setminus \{w\}} (u \cdot X),$$

for some $\lambda_w \in \mathbb{F}_q$, is zero at $n+1$ points on the line A, then $\psi \equiv 0$.

Proof. The polynomial ψ is of degree n. By choosing a basis which includes the elements of A, we see that its restriction to the line A is a homogeneous polynomial in two variables. If it is zero at $n+1$ distinct points then it is identically zero on the line A. Explicitly, suppose $A = \{a_1, \ldots, a_{k-2}\}$ and that we choose a basis of $\mathrm{V}_k(\mathbb{F}_q)$ in which the last $k-2$ vectors are the elements of A. Then, in the dual space, a vector x on the line A has coordinates $(x_1, x_2, 0, \ldots, 0)$, for some $x_1, x_2 \in \mathbb{F}_q$, and so $u \cdot x = u_1 x_1 + u_2 x_2$.

Let $w_0 \in U$. Then

$$0 = \psi(A \cup \{w_0\}) = \lambda_{w_0} \prod_{u \in U \setminus \{w_0\}} \det(u, A \cup \{w_0\}),$$

and so $\lambda_{w_0} = 0$. Note that all the determinants are non-zero since $A \cup U$ is an arc. □

3. *Arcs in spaces of odd characteristic*

We will suppose from now on that q is odd and $k \geqslant 5$. Note that Theorem 1.3 holds for $k = 2$, 3 and 4 since there are no arcs of size $q+2$ in these spaces when q is odd, see for example [**6**] or [**5**].

Let n be a non-negative integer such that $n \leqslant |S| - k - t$.

Let G be a subset of S of size $k+t+n$, which will remain fixed and let E be a subset of G of size $k+t-1$, which will also remain fixed. Let $U = G \setminus E$. Let A be a subset of E of size $k-2$ which for the most part will also remain fixed.

We define a matrix P_n whose rows are indexed by the $(k-1)$-subsets C of E which contain a $(k-3)$-subset of A. The columns of P_n are indexed by pairs (D,w), where D is a subset of A of size $k-3$ and $w \in U$. The $(C,(D,w))$ entry of P_n is

$$\prod_{u \in U \setminus \{w\}} \det(u,C),$$

if C contains D and zero otherwise.

Note that, by definition, the matrix P_n depends only on G and not on S.

Lemma 3.1. *There is no vector of weight one in the column space of* P_n.

Proof. Let v be the row vector whose coordinates are indexed by the $(k-1)$-subsets C of E which contain a $(k-3)$-subset of A and whose C entry is

$$\alpha_C \prod_{z \in G \setminus C} \det(z,C)^{-1}.$$

Note that all the coordinates in v are non-zero.

The standard scalar product of v with the (D,w) column of P_n is

$$\sum \alpha_C \prod_{z \in G \setminus C} \det(z,C)^{-1} \prod_{u \in U \setminus \{w\}} \det(u,C) = \sum \alpha_C \prod_{z \in (E \cup \{w\}) \setminus C} \det(z,C)^{-1},$$

where the sum runs over the subsets C of E of size $k-1$ containing D. By Lemma 2.2, this sum is zero.

Therefore, if there is a vector r of weight one in the column space of P_n then $v \cdot r = 0$. This implies one of the coordinates of v is zero, which it is not. □

The aim of the rest of the article will be to prove that if $n = t$ then, under the projection hypothesis, P_{k-3} does have a vector of weight one in its column space. This will then contradict Lemma 3.1. Recall that we are supposing that G extends to an arc of size $q+k-1-t$. Thus, if $n = t = k-3$, then we are supposing the G extends to an arc S of size $q+2$.

Let D be a subset of A of size $k-3$. Since D is a set of $k-3$ linearly independent vectors, the subspace $\langle D \rangle$ has dimension $k-3$ and the quotient space $\mathrm{V}_k(\mathbb{F}_q)/\langle D \rangle$ has dimension 3. Let

$$G/D = \{ g + \langle D \rangle \mid g \in G \setminus D \}$$

denote the set of $t+n+3$ vectors in this quotient space obtained from the vectors of $G \setminus D$.

Let e be a fixed element of $E \setminus A$.

Let M_D be the matrix whose rows are indexed by $(k-1)$-subsets $C = D \cup L$, where L is a 2-subset of $E \setminus A$ and whose $n+1$ columns are indexed by $w \in U$ and whose (C,w) entry is

$$\prod_{u \in U \setminus \{w\}} \det(u,C) = \prod_{u \in U \setminus \{w\}} (u \cdot C).$$

Observe that M_D is a submatrix of P_n.

Lemma 3.2. *If G projects to a subset of a conic from D then the row space of* M_D *is spanned by the rows indexed by $C = D \cup \{e,b\}$, where $b \in E \setminus (A \cup \{e\})$.*

Proof. Since G projects to a subset of a conic from D, we have that G/D is contained in the set of zeros of a homogeneous polynomial f_D in 3 variables and of degree 2.

Let $W = \{w_1, w_2, w_3\}$ be a subset of U of size 3. Consider the 3×3 submatrix M of M_D whose columns are indexed by $w \in W$, and whose rows are indexed by $D \cup \{e, a\}$, $D \cup \{e, b\}$ and $D \cup \{a, b\}$. Define g_D to be the polynomial of degree two, which is the determinant of M where we replace w_1 by X. The C-row in this determinant is

$$(\prod_{u \in U \setminus \{w_1\}} (u \cdot C), \quad (X \cdot C) \prod_{u \in U \setminus \{w_1, w_2\}} (u \cdot C), \quad (X \cdot C) \prod_{u \in U \setminus \{w_1, w_3\}} (u \cdot C)).$$

By changing the basis so that the basis includes the elements of D, $g_D(X)$ will be a homogeneous polynomial in three variables. Clearly $g_D(w_2) = g_D(w_3) = 0$ since the determinant will have repeated columns. Moreover $g_D(a) = 0$, since the determinant will have a 2×2 submatrix of zeros. Similarly, $g_D(b) = 0 = g_D(e) = 0$. Thus g_D is the unique polynomial, up to scalar factor, whose set of zeros contains these five vectors of the quotient space. Hence, g_D is a scalar multiple of f_D. Therefore, $g_D(w_1)$ is also zero and the determinant of M is zero.

Since every 3×3 submatrix M of M_D has rank two, the $3 \times (n+1)$ matrix whose columns are indexed by $w \in U$, and whose rows are indexed by $D \cup \{e, a\}$, $D \cup \{e, b\}$ and $D \cup \{a, b\}$ has rank two. Therefore, in M_D, the row indexed by $D \cup \{a, b\}$ must be a linear combination of the rows indexed by $D \cup \{e, a\}$ and $D \cup \{e, b\}$. □

Lemma 3.3. *If G projects to a subset of a conic from D and $n \geqslant t$ then there exist $\lambda_w \in \mathbb{F}_q$ such that*

$$\psi_D(X) = \sum_{w \in U} \lambda_w \prod_{u \in U \setminus \{w\}} (u \cdot X) \not\equiv 0,$$

is zero at $D \cup L$, for all 2-subsets L of $E \setminus A$.

Proof. By Lemma 3.2, the matrix M_D has rank at most $t \leqslant n$. Since M_D has $n+1$ columns there are elements $\lambda_w \in \mathbb{F}_q$, not all zero, such that

$$\sum_{w \in U} \lambda_w v_w = 0,$$

where v_w is the column of M_D indexed by w. Since it is zero, the C coordinate of this linear combination is zero. However, it is also the evaluation of ψ_D at C. Thus, we have that $\psi_D(C) = 0$ for all $C = D \cup L$, where L is a 2-subset of $E \setminus A$. □

In light of Lemma 3.3, we will now take $n = t$.

Let

$$v_D = \sum_{w \in U} \lambda_w v_{D,w},$$

where $v_{D,w}$ is the column of P_n indexed by (D, w). Note that the C-coordinate of v_D is the evaluation of ψ_D if $C \supset D$ and zero otherwise.

By Lemma 3.3, the C-coordinate in v_D is zero if $C = D \cup L$, for some 2-subset L of $E \setminus A$, so the only possibly non-zero coordinates of v_D are indexed by $(k-1)$-subsets $C = A \cup \{b\}$, for some $b \in E \setminus A$.

Let us define a $(t+1) \times (k-2)$ matrix Q_t, whose rows are indexed by $(k-1)$-subsets $C = A \cup \{b\}$, for some $b \in E \setminus A$ and whose columns are the restriction of v_D to these C coordinates. So the columns are indexed by the $(k-3)$-subsets D of A. The following lemmas follow almost immediately from this discussion and the definition of Q_t.

Lemma 3.4. *The C entry of the D column of Q_t is $\psi_D(C)$.*

Proof. The D column of Q_t is the vector v_D, where we only take the coordinates indexed by $C = A \cup \{b\}$ for some $b \in E \setminus A$. Since D is a subset of A and $C = A \cup \{b\}$ for some $b \in E \setminus A$, we have that $C \supset D$ and as noted above, the C coordinate of v_D in this case, is the evalutaion of ψ_D at C. □

Lemma 3.5. *If there is a vector of weight one in the column space of* Q_t *then there is a vector of weight one in the column space of* P_t*.*

Proof. If we extend a vector in the column space of Q_t with zero entries in the coordinates indexed by $(k-1)$-subsets C, where C does not contain A but C does contain a $(k-3)$-subset of A, then we obtain a vector in the column space of P_t, since we constructed the columns of Q_t by deleting these zero coordinates from a vector in the column space of P_t. □

The aim now will be to show that if $n = t = k - 3$ then there is a $(k-2)$-subset A of G for which Q_{k-3} has a vector of weight one in its column space. Then Lemma 3.5 will imply that P_{k-3} has a vector of weight one in its column space, which contradicts Lemma 3.1. Recall that if $n = t = k - 3$, then we are supposing the G extends to an arc S of size $q + 2$.

4. *Arcs that extend to arcs of size* $q + 2$

Suppose now that $n = t = k - 3$.

Thus G is an arc of size $3k - 6$ which extends to an arc of size $q + 2$, E is a subset of G of size $2k - 4$, A is a subset of E of size $k - 2$ and D is a subset of A of size $k - 3$.

Lemma 4.1. *If G projects to a subset of a conic from all $(k-3)$-subsets of E then $\psi_D(C) = 0$ for all $C \subseteq E \setminus (A \setminus D)$. Moreover, $\psi_D(E \setminus D) \neq 0$.*

Proof. Let D and D' be $(k-3)$-subsets of $E \setminus \{a\}$, where $\{a\} = A \setminus D$. Suppose that $|D' \cap D| = k - 4$.

By hypothesis, G projects to a subset of a conic from D and D'. By Lemma 3.3, with $A = D \cup \{a\}$ and $A = D' \cup \{a\}$ respectively, there is a ψ_D and $\psi_{D'}$ which are both zero at $D \cup D' \cup \{b\}$, for all $b \in E \setminus (D \cup D' \cup \{a\})$.

There are $n + 1 = t + 1$ coefficients λ_w in the definition of ψ_D and there are t elements in $b \in E \setminus (D \cup D' \cup \{a\})$. So up to scalar multiple, ψ_D is determined by the equations $\psi(D \cup D' \cup \{b\}) = 0$. Note that for each b, the equation $\psi(D \cup D' \cup \{b\}) = 0$ gives an independent condition, since for each b this is a distinct point on the line $D \cup D'$.

However, $\psi_{D'}$ is determined by the same set of equations, so we conclude that ψ_D and $\psi_{D'}$ are scalar multiples of each other.

Since $\psi_{D'}(D' \cup L') = 0$, for all 2-subsets L' of $E \setminus (D' \cup \{a\})$, we have that $\psi_D(D' \cup L') = 0$.

Now, repeating the above with D replaced with D' and D' replaced with D'', where $|D' \cap D''| = k - 4$ and $|D \cap D''| = k - 5$, we have that $\psi_D(D'' \cup L'') = 0$ for all 2-subsets L'' of $E \setminus (D'' \cup \{a\})$. Continuing in this way we conclude that $\psi_D(C) = 0$ for all $(k-1)$-subsets C of $E \setminus \{a\}$.

If $\psi_D(E \setminus D) = 0$ then ψ_D has $t + 1$ zeros on the line $E \setminus A$. By Lemma 2.3, this implies that $\psi_D \equiv 0$, which it is not by Lemma 3.3. Therefore, $\psi_D(E \setminus D) \neq 0$, which completes the proof.

□

Lemma 4.2. *If $n = t = k-3$ and G projects to a subset of a conic from every $(k-3)$-subset D of E then there is a vector of weight one in the column space of Q_t.*

Proof. Since $t = k-3$ the matrix Q_t is a square matrix. By Lemma 3.4, a column of Q_t is the evaluation of $\psi_D(X)$ at the $(k-1)$-subsets C of $A \cup \{b\}$, where $b \in E \setminus A$. If Q_t does not have full rank then there is a linear combination of the columns which is zero. The C coordinate of a linear combination of the columns is the evaluation of

$$\psi_A(X) = \sum \mu_D \psi_D(X),$$

for some $\mu_D \in \mathbb{F}_q$, not all zero, where the sum runs over the $(k-3)$-subsets D of A.

If ψ_A is zero at all points $A \cup \{b\}$, where $b \in E \setminus A$ then it is zero at $t+1$ points on the line A. By Lemma 2.3, $\psi_A \equiv 0$. However, for a subset D of E of size $k-3$,

$$\psi_A(E \setminus D) = \mu_D \psi_D(E \setminus D),$$

and by Lemma 4.1, $\psi_D(E \setminus D) \neq 0$. Therefore $\mu_D = 0$, which implies that the columns of Q_t are linearly independent. Since Q_t is a square matrix there is a vector of weight one in the column space of Q_t. □

We can now prove Theorem 1.3.

Proof. (of Theorem 1.3) Let G be an arc of $\mathrm{V}_k(\mathbb{F}_q)$ of size $3k-6$ and suppose that E is a subset of G of size $2k-3$ and that G projects to a subset of a conic from every $(k-3)$-subset of E. Suppose that G extends to an arc of size S of size $q+2$, so $t = k-3$.

By Lemma 4.2, there is a vector of weight one in the column space of Q_{k-3}. By Lemma 3.5, there is a vector of weight one in the column space of P_{k-3}, which contradicts Lemma 3.1. □

5. *Comments*

It is a long-standing conjecture, dating back to the 1950's, that there are no arcs of size $q+2$ for $4 \leqslant k \leqslant q-2$, see [**5**], [**7**] or [**10**] for example. It was proven in [**1**] that the conjecture is true for q prime.

This article can be considered as an example of how the system of equations in Lemma 2.1 can be used to prove results about arcs and try to verify this conjecture when q is not a prime. It is by no means easy, but this article at least demonstrates that it is possible.

With regard to the result itself, the hypothesis that the projections lie on a conic may not be necessary. Indeed, computations of explicit examples indicate that this is in fact the worst-case scenario. In other words, it is only in this case that have to take n so large to prove that P_n has a vector of weight one in its column space, assuming that G extends to a $(q+2)$-arc. For other arcs, it appears that P_n has a vector of weight one in its column space for smaller n. However, Q_n does not have a vector of weight one in its column space, if we remove the projection hypothesis, so one must consider the larger matrix P_n in this case.

In [**4**] it is conjectured that a larger matrix M_n has full rank and in [**3**] that it has a vector of weight one in its column space, for any arc where $k \leqslant p + n(p-2)$ and where p is the characteristic of $\mathbb{F}_q$. Again, we are assuming that G extends to a $(q+2)$-arc. This would imply that there are no arcs of size $q+2$ for $k \leqslant (pq - 2q + 6p - 10)/(2p-3)$. We conjecture that the same is true for the smaller matrix P_n. In other words we conjecture that P_n has a vector of weight one in its column space, for any arc that extends to a $(q+2)$-arc, when $k \leqslant p + n(p-2)$, which would contradict Lemma 3.1 and imply that there are no arcs of size $q+2$ for $k \leqslant (pq - 2q + 6p - 10)/(2p-3)$.

References

1. S. Ball, On sets of vectors of a finite vector space in which every subset of basis size is a basis, *J. Eur. Math. Soc.*, **14** (2012) 733–748.

2. S. Ball, *Finite Geometry and Combinatorial Applications*, London Mathematical Society Student Texts **82**, Cambridge University Press, 2015.

3. S. Ball, Extending small arcs to large arcs, `arXiv:1603.05795`, 2016.

4. A. Chowdhury, Inclusion Matrices and the MDS Conjecture, `arXiv:1511.03623v2`, 2015.

5. J. W. P. Hirschfeld and L. Storme, The packing problem in statistics, coding theory and finite projective spaces: update 2001, in *Developments in Mathematics*, **3**, Kluwer Academic Publishers. *Finite Geometries*, Proceedings of the *Fourth Isle of Thorns Conference*, pp. 201–246.

6. J. W. P. Hirschfeld and J. A. Thas, *General Galois Geometries*, Oxford Mathematical Monographs, Oxford, 1991-

7. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

8. R. M. Roth and G. Seroussi, On MDS extensions of generalized Reed–Solomon codes, *IEEE Transactions on Information Theory*, **32** (1986) 349–354.

9. L. Storme, Completeness of normal rational curves, *J. Algebraic Combin.*, **1** (1992) 197–202.

10. A. Vardy, `http://media.itsoc.org/isit2006/vardy/handout.pdf`, 2006

Simeon Ball
Departament de Matemàtiques,
Universitat Politècnica de Catalunya,
Mòdul C3, Campus Nord,
c/ Jordi Girona 1-3,
08034 Barcelona, Spain

simeon@ma4.upc.edu

Jan De Beule
Vakgroep Wiskunde,
Vrije Universiteit Brussel,
Pleinlaan 2,
B-1050 Brussels,
Belgium

jan@debeule.eu