The Cyclic Model for $PG(n, q)$ and a Construction of Arcs

GIORGIO FAINA, GYÖRGY KISS, STEFANO MARCUGINI AND
FERNANDA PAMBIANCO

The $n$-dimensional finite projective space, $PG(n, q)$, admits a cyclic model, in which the set of points of $PG(n, q)$ is identified with the elements of the group $\mathbb{Z}^{q^n+q^{n-1}+\cdots+q+1}$. It was proved by Hall (1974, Math. Centre Tracts, 57, 1–26) that in the cyclic model of $PG(2, q)$, the additive inverse of a line is a conic. The following generalization of this result is proved:

In the cyclic model of $PG(n, q)$, the additive inverse of a line is a $(q+1)$-arc if $n+1$ is a prime and $q+1 > n$.

It is also shown that the additive inverse of a line is always a normal rational curve in some subspace $PG(m, q)$, where $m+1 | n+1$.

© 2002 Academic Press

1. Introduction

Let $PG(n, q)$ be the $n$-dimensional projective space over the finite field $GF(q)$. A $k$-arc in $PG(n, q)$ is a set $K$ of $k$ points with $k \geq n+1$ such that no $n+1$ points lie in a hyperplane. The subject of arcs in $PG(n, q)$ is vast and we will introduce only the concepts and the results that we need in this paper. For more details, one can refer to [3] and [5]. The $n$-dimensional finite projective space, $PG(n, q)$ admits a cyclic model ([3] pp. 95–98), in which the set of points of $PG(n, q)$ is identified with the elements of the group $\mathbb{Z}^{q^n+q^{n-1}+\cdots+q+1}$. Let this identification be given by the bijection $\phi$. We define the additive inverse of a set of points of $PG(n, q)$ using this identification. Let $R$ be any point of $PG(n, q)$ and let $r = \phi(R)$ be the corresponding element of the group $\mathbb{Z}^{q^n+q^{n-1}+\cdots+q+1}$. Then let us denote by $-R$ that point of $PG(n, q)$ which corresponds to $-r$, where $-r$ is the additive inverse of $r$ in the group $\mathbb{Z}^{q^n+q^{n-1}+\cdots+q+1}$. Finally if $S = \{P_1, P_2, \ldots, P_k\}$ is any set of points of $PG(n, q)$, then we call the set $-S := \{-P_1, -P_2, \ldots, -P_k\}$ the additive inverse of $S$. It was proved by Hall [2] that in the cyclic model of $PG(2, q)$, the additive inverse of a line is a conic. The intent of this paper is to produce a generalization of this result for any dimension.

The remainder of this article is organized as follows. Section 2 contains the detailed description of the cyclic model of $PG(n, q)$. In Section 3 the geometric properties of the additive inverse of a hyperplane and a line are discussed and the generalization of Hall’s result is proved.

2. The Cyclic Model for $PG(n, q)$

The following non-classical embedding of $PG(n, q)$ into $PG(n, q^{n+1})$ is a generalization of the known embedding of $PG(2, q)$ into $PG(2, q^3)$ (see e.g. [1, 4]). Let $a$ be a generator in the multiplicative group formed by the $(q^n + q^{n-1} + \cdots + q + 1)$-th roots of unity in $GF(q^{n+1})$. Let $q[i]$ be a shorthand notation for $q^i + q^{i-1} + \cdots + q + 1$, and
let $A$ be the $(n + 1) \times (n + 1)$ diagonal matrix

$$A = \begin{pmatrix} a^{q[n-1]} & 0 & 0 & \ldots & 0 \\ 0 & a^{q[n-2]} & 0 & \ldots & 0 \\ 0 & 0 & a^{q[n-3]} & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & a \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix}$$

Then $A$ has order $q[n]$. The points of $PG(n, q)$ are those points $P_k$ of $PG(n, q^{n+1})$ which have a coordinate vector of the form

$$A^k(1, 1, \ldots, 1)^T$$

where $k \in \{0, 1, \ldots, q^n + q^{n-1} + \cdots + q\}$.

The hyperplanes of $PG(n, q)$ are formed by those points of type $P_k$ which are contained in the hyperplanes of $PG(n, q^{n+1})$ having equation

$$b^{q[n-1]-q[n-2]}X_0 + b^{q[n-1]-q[n-3]}X_1 + \cdots + b^{q[n-1]}X_{n-1} + X_n = 0$$

where $b$ is a $q[n]$-th root of unity in $GF(q^{n+1})$. Let us denote by $\pi_b$ the hyperplane corresponding to $b$. The elements $a^k$ for any $k$ are $q[n]$th roots of unity in $GF(q^{n+1})$, hence they are non-zero $(q^n-1)$-st powers in $GF(q^{n+1})$. Thus for any $a^k$ and $b$ there are elements $c, d$ such that $a^k = c^{q^n-1}$ and $b = d^{q^n-1}$. It means that the expression

$$b^{q[n-1]-q[n-2]}a^{kq[n-1]} + b^{q[n-1]-q[n-3]}a^{kq[n-2]} + \cdots + b^{q[n-1]}a^k + 1$$

can be written as

$$\frac{d^{q^n}}{c}\left(\frac{c^{q^n}}{d^{q^n-1}} + \frac{c^{q^n-1}}{d^{q^n-2}} + \cdots + \frac{c^q}{d^{q-1}} + \frac{c}{d}\right) = \frac{d^{q^n}}{c} \cdot Tr\left(\frac{c}{d}\right)$$

where $Tr : GF(q^{n+1}) \to GF(q)$ is the trace function $Tr(x) = x^{q^n} + x^{q^{n-1}} + \cdots + x^q + x$. Thus the points of type $P_k$ on any hyperplane $\pi_b$ correspond to points on an $n$-dimensional subspace through the origin when $GF(q^{n+1})$ is interpreted as an $(n + 1)$-dimensional vector space over $GF(q)$. Hence the points $P_k$ form a cyclic model of $PG(n, q)$.

Let $m+1$ be a divisor of $n+1$. Then $GF(q^{m+1})$ is a subfield of $GF(q^{n+1})$, and $GF(q^{n+1}/q[m])$ is a generator element in the multiplicative group formed by the $q[m]$-th roots of unity in $GF(q^{m+1}) \subset GF(q^{n+1})$. The projective space $PG(m, q)$ can be embedded into $PG(n, q^{m+1})$ as it was described previously, and $PG(m, q^{m+1})$ can be considered as a subspace of $PG(n, q^{n+1})$. Now the projective space $PG(n, q)$ contains a special $m$-dimensional subspace, $P_m$. The points of $P_m$ are those points of $PG(n, q^{n+1})$ whose coordinate vector have the form

$$A^k(1, 1, \ldots, 1)^T$$

where $k \in \{0, q[n]/q[m], 2q[n]/q[m], \ldots, (q[1]-1)q[n]/q[m]\}$. The points of $P_m$ are completely determined by their first $m + 1$ coordinates, because $(a^{q[i]})^{q[n]/q[m]} = (a^{q[i]+(i-1)n})^{q[n]/q[m]}$ for all $i \in \{1, 2, \ldots, q[n]/q[m]-1\}$ and $i \in \{0, 1, \ldots, m\}$. A hyperplane $\pi_b$ is a hyperplane of $P_m$ if and only if $b$ is a $q[m]$-th root of unity. In this case $b^{q[i]-1} - b^{q[i]} = \pi_{b^{q[i]-1}} - \pi_{b^{q[i]-1}}$ for all $i = 1, 2, \ldots, n$, thus the hyperplanes of $P_m$ are also completely determined by their first $m + 1$ coordinates.
Let $S$ and $T$ be two distinct points of $\mathcal{P}_m$ with coordinate vectors $(1, 1, \ldots, 1)^T$ and $(r^{q[n-1]}, r^{q[n-2]}, \ldots, t, 1)^T$, where $t$ is a $q[m]$-th root of unity. The line joining them in $PG(n, q^{m+1})$ contains those points $P_\alpha$ which have coordinate vector of the form
\[(\alpha + (1 - \alpha)r^{q[n-1]}, \alpha + (1 - \alpha)r^{q[n-2]}, \ldots, \alpha + (1 - \alpha)t, 1)^T\]
where $\alpha \in GF(q^{m+1})$. The point $P_\alpha$ is in $\mathcal{P}_m$ if and only if there exists a $q[m]$-th root of unity $c$ such that
\[\alpha = \frac{t - c}{1 - r} = \frac{r^{q+1} - c^{q+1}}{r^{q+1} - 1} = \ldots = \frac{r^{q[m-1]} - c^{q[m-1]}}{r^{q[m-1]} - 1}.
\]
From these equations we get that $c$ is a root of the equations
\[c^q[i] - c(t[i] - 1) - t + r^q[i] = 0 \quad (1, i)\]
for $i = 1, 2, \ldots, m - 1$. The line joining $S$ and $T$ has $q + 1$ points in $\mathcal{P}_m$, and for $i = 1$, Eqn $(1, i)$ has at most $q + 1$ roots. Any point on the line corresponds to a root of the equation. Hence Eqn $(1, i)$ has exactly $q + 1$ distinct roots in $GF(q^{m+1})$, each of the $q + 1$ roots of Eqn $(1, i)$ satisfies the Eqns $(1, i)$ for $i = 2, 3, \ldots, m - 1$, and each root is a $q[m]$-th root of unity. From these equations we can express the coordinate vector of $P_\alpha$ in such a way that the entries contain only linear terms (and not powers) of $c$. The coordinate vector can be written such that the $i$th $(i = 0, 1, \ldots, m - 2)$ entry is
\[(t - 1)(\alpha + (1 - \alpha)r^{q[m-1-i]}) = c(t^{q[m-1-i]} - 1) + t - r^{q[m-1-i]},\]
while the $m$th and $(m + 1)$-st entries are $c(t - 1)$ and $t - 1$, respectively.

### 3. The Additive Inverse of a Line

First we investigate the additive inverse of a hyperplane of $\mathcal{P}_m$.

**Lemma 3.1.** Let $m + 1$ be any divisor of $n + 1$. In the cyclic model of $PG(n, q)$ the additive inverse of a hyperplane of $\mathcal{P}_m$ is contained in a surface of degree $m$.

**Proof.** Consider the cyclic representation of $PG(n, q)$ in $\mathbb{Z}_q[n]$. Now the point $P_k$ corresponds to the element $k$, hence the additive inverse of $P_k$ is $P_{-(q-1)k}$. Thus the additive inverse of $\mathcal{P}_m$ is $\mathcal{S}_m$. If $P_k$ has coordinate vector $(X_0, X_1, \ldots, X_n)^T$, then $-P_k$ has coordinate vector $(\frac{1}{X_0}, \frac{1}{X_1}, \ldots, \frac{1}{X_n})^T$.

Let $\pi_b$ be a hyperplane of $\mathcal{P}_m$. Then the first $m + 1$ coordinates of the points of $-\pi_b$ satisfy the equation
\[b^{q[m-1]-q[m-2]} \frac{1}{X_0} + b^{q[m-1]-q[m-3]} \frac{1}{X_1} + \ldots + b^{q[m-1]} \frac{1}{X_m} = 0.
\]
It means that $-\pi_b$ is contained in the surface $S_b$ of degree $m$ which has equation
\[\sum_{j=0}^{m-2} b^{q[m-1]-q(m-2-i)} \frac{\Pi_{i=0}^m X_j}{X_i} + b^{q[m-1]} \frac{\Pi_{j=0}^m X_j}{X_m} = 0.
\]

**Theorem 3.2.** Let $\ell$ be any line through the point $(1, 1, \ldots, 1)^T$ in the cyclic model of $PG(n, q)$. Let $m$ be the smallest integer for which $\ell$ is contained in $\mathcal{P}_m$. Then $-\ell$ is a $(q + 1)$-arc in $\mathcal{P}_m$ if $q > m$. 

\[\square\]
Let $\ell$ be the line $ST$. If $P_m$ contains $\ell$, then it also contains $-\ell$. Suppose that $-\ell$ is not an arc. Then there is a hyperplane $\pi_b$ of $P_m$ which contains more than $m$ points of $-\ell$. Thus the additive inverse of $\pi_b$, which is a surface of degree $m$ by Lemma 3.1, contains more than $m$ points of $\ell$. So this surface contains the whole line $ST$. Hence the coordinates of $P_\alpha$ satisfy the equation of the surface $S_b$. Let us write the coordinates of $P_\alpha$ into this equation. We can consider the left-hand side as a polynomial of $c$. This polynomial has degree $m$ because each coordinate is a linear expression in $c$. Let us write it in the form

$$f(c) = \sum_{i=0}^{m} A_i c^i.$$  

It is easy to calculate the main coefficient $A_m$ of $f(c)$:

$$A_m = (t^{q[m-1]} - 1)(t^{q[m-2]} - 1) \cdots (t - 1).$$

This is not equal to zero, because $m$ is the smallest positive integer for which $t^{q[m]} = 1$ holds by the definition of $m$. Hence the polynomial $f(c)$ of degree $m$ has $q + 1 > m$ distinct roots, because each root of Eqn (1.1) corresponds to a point of the line $ST$. This contradiction means that $-ST$ is an arc in $P_m$. \hfill $\square$

Now it is easy to prove the following.

**Theorem 3.3.** If $q + 1 > n$ then in the cyclic model of $PG(n, q)$ the additive inverse of a line is always an arc in some subspace $PG(m, q)$, where $m + 1$ is a divisor of $n + 1$.

**Proof.** The collineation group generated by $\sigma : P_k \to P_{k+1}$ maps $P_m$ to $P_m$ and is transitive on the points of $PG(n, q)$. Thus any line can be mapped to a line through the point $(1, 1, \ldots, 1)^T$ and then we can apply Theorem 3.2. \hfill $\square$

If $n + 1$ is a prime, then $m + 1|n + 1$ implies $m = n$, thus we proved the following generalization of Hall’s result:

**Theorem 3.4.** In the cyclic model of $PG(n, q)$ the additive inverse of a line is an arc if $n + 1$ is a prime and $q + 1 > n$.

Elementary calculation shows that the additive inverse of any line is always a normal rational curve in the corresponding subspace, because the coordinates of the points of the inverse can be expressed by independent polynomials of degree $m$.

**Acknowledgements**

We are grateful to the referee whose suggestions helped us to improve the proofs of the first version of this paper. The research was supported by the Italian MURST (progetto 40% ‘Strutture Geometriche, Combinatoria e loro Applicazioni’ and progetto 40% ‘Efficienza di Algoritmi e progetto di Strutture Informative’), by CNR (progetto strategico ‘Applicazioni della matematica per la tecnologia e la società’, sottoprogetto ‘Calcolo Simbolico’) and by GNSAGA. The research was also supported by the Hungarian National Foundation for Scientific Research, Grant No. T 0123324, and by the Research Development Foundation of the Hungarian Ministry of Education, Grant No. 0151/1999.
The cyclic model for $PG(n, q)$ and a construction of arcs

REFERENCES


Received 10 July 1999 and accepted 15 May 2001

GIORGIO FAINA
Dipartimento di Matematica,
Università degli Studi di Perugia,
Via Vanvitelli 1,
06123 Perugia,
Italy
E-mail: faina@dipmat.unipg.it

GYÖRGY KISS
Department of Geometry,
Eötvös Loránd University,
H-1088 Budapest,
Rákóczi u. 5,
Hungary
and
Bolyai Institute,
University of Szeged,
H-6720 Szeged,
Aradi vénásút teré 1,
Hungary
E-mail: kissgy@cs.elte.hu

AND

STEFANO MARCUGINI AND FERNANDA PAMBIANCO
Dipartimento di Matematica,
Università degli Studi di Perugia,
Via Vanvitelli 1,
06123 Perugia,
Italy
E-mails: gino@dipmat.unipg.it; fernanda@dipmat.unipg.it