The $p$-rank of the $Sp(4,p)$ Generalized Quadrangle

D. de Caen$^1$ and G. E. Moorhouse$^2$

Abstract. We determine the $p$-rank of the point-line incidence matrix of the generalized quadrangle of type $Sp(4,p)$ where $p$ is prime.

Keywords: $p$-rank, generalized quadrangle

1. Introduction

Let $P$ be a finite generalized quadrangle of order $s$ (i.e. with parameters $s = t$), and let $N$ be a point-line incidence matrix of $P$. Thus $N$ is a square $(0,1)$-matrix of size $(s^2+1)(s+1)$, and

$$NN^\top = (s + 1)I + A,$$

where $A$ is the adjacency matrix of the collinearity graph of $P$. We recall that the latter graph is strongly regular and

$$A^2 = s(s+1)I + (s - 1)A + (s+1)(J - I - A)$$

where $J$ is the all-1 matrix, from which we find that $A$ has eigenvalues $s(s + 1)$, $s - 1$, $-s - 1$ with multiplicities $1$, $\frac{1}{2}s(s + 1)^2$, $\frac{1}{2}s(s^2 + 1)$ respectively, and $NN^\top$ has eigenvalues $(s + 1)^2$, $2s$, $0$ with these same multiplicities. This proves

1.1 Lemma. $\text{rank}_Q N = \frac{1}{2}s(s + 1)^2 + 1$. In particular, $\text{rank}_K N \leq \frac{1}{2}s(s + 1)^2 + 1$ for any field $K$.

We are interested in a determination of $\text{rank}_F N$ for a finite classical GQ (i.e. one of type $Sp(4,F)$; or its dual, of type $O(5,F)$), which is to say, the rank of $N$ in the natural characteristic. In this direction, Sastry and Sin [6] have obtained

$$\text{rank}_2 N = 1 + \left(1 + \sqrt{17}/2\right)^{2e} + \left(1 - \sqrt{17}/2\right)^{2e}$$

for every classical GQ of order $q = 2^e$. Our main result, proved in Section 3, is that for classical GQ’s of prime order, the upper bound of Lemma 1.1 is attained:

---

$^1$ Dept. of Mathematics and Statistics, Queen’s University, Kingston, Ontario, Canada.

$^2$ Dept. of Mathematics, University of Wyoming, Laramie WY, U.S.A.
1.2 Theorem. If $N$ is the incidence matrix of a generalized quadrangle of type $Sp(4,p)$ or $O(5,p)$ where $p$ is prime, then $\text{rank}_p N = \frac{1}{2}p(p+1)^2 + 1$.

We remark that for classical GQ’s of odd order $q$, Bagchi, Brouwer and Wilbrink show that

$$\text{rank}_2 N = \frac{1}{2} q(q+1)^2 + 1;$$

see [1, Thm.9.4(ii)]. Note that this is the rank in characteristic 2 rather than the natural characteristic. It is therefore reasonable to expect that for a classical GQ of prime order $p$, the invariant factors of $N$ should probably consist of $\frac{1}{2}p(p+1)^2+1$ ones and $\frac{1}{2}p(p^2+1)$ zeroes; and this we have verified for $p = 2, 3, 5$ by computer.

We remark that the incidence matrices of nonclassical objects typically have higher rank (in the natural characteristic) than their classical counterparts. For example, one nonclassical GQ of order 8 is known, denoted $T_2(O)$ where $O$ is the essentially unique oval in $PG(2,8)$ other than a conic; see [7, p.393]. Its 2-rank is 310, which lies between 298 (the 2-rank of the $Sp(4,8)$ quadrangle) and 325, the upper bound of Lemma 1.1.

No nonclassical GQ’s of odd order are known. If a nonclassical GQ of odd prime order $p$ exists, which seems unlikely, its $p$-rank cannot exceed that of a classical GQ of the same order.

2. Polynomials

(DOM: HERE I GIVE MORE GENERAL NOTATION AND RESULTS THAN REQUIRED IN SECTION 3, ANTICIPATING A GENERALIZATION OF THEOREM 1.2 TO PRIME POWERS)

Following the notation of [2] and [5], let

- $X = (X_0, X_1, \ldots, X_n)$, an $(n+1)$-tuple of indeterminates $(n \geq 1)$;
- $F$ a finite field of order $q = p^e$;
- $F[X]$ the ring of polynomials in $X_0, X_1, \ldots, X_n$ with coefficients in $F$;
- $F_d[X]$ the $d$-homogeneous component of $F[X]$. 

Thus $\dim F_d[X] = \binom{n+d}{n}$. Let $\ell(X) = a_0X_0 + a_1X_1 + \cdots + a_nX_n \in F_1[X]$ where $a_k \in F$, and for a fixed exponent $d \geq 0$, consider the multinomial expansion

$$\ell(X)^d = \sum_i \binom{d}{i} a^i X^i$$
where the sum extends over all \((n+1)\)-tuples \(i = (i_0, i_1, \ldots, i_n)\) of nonnegative integers such that \(i_0 + i_1 + \cdots + i_n = d\). Here we abbreviate \(a^i := a_0^{i_0} a_1^{i_1} \cdots a_n^{i_n}\), \(X^i := X_0^{i_0} X_1^{i_1} \cdots X_n^{i_n}\), and the multinomial coefficient

\[
\binom{d}{i} := \binom{d}{i_0, i_1, \ldots, i_n} = \frac{d!}{i_0! i_1! \cdots i_n!}.
\]

Following [2] and [5], we let \(F^+_d[X]\) denote the subspace of \(F_d[X]\) spanned by all monomials \(X^i\) with \(i_0 + i_1 + \cdots + i_n = d\) such that the multinomial coefficient \(\binom{d}{i}\) is not divisible by \(p\). Thus the polynomials \(\ell(X)^d\) for \(\ell(X) \in F_1[X]\) clearly lie in \(F^+_d[X]\). By Lucas’ Theorem (see [2], [3] or [5]), \(\dim F^+_d[X] = \prod_k \binom{n+d_k}{n}\) where \(d = \sum_k d_k p^k\), \(0 \leq d_k \leq p - 1\). Although the following is not new (cf. [2, Cor.3.2]), for the sake of completeness we include a bare-bones proof here, modulo a few details found in [2].

**2.1 Lemma.** Let \(0 \leq d \leq q - 1\). The vector space \(F^+_d[X]\) is spanned by the polynomials \(\ell(X)^d\) for \(\ell(X) \in F_1[X]\). In particular for \(d \leq p - 1\), the polynomials \(\ell(X)^d\) span \(F_d[X]\).

**Proof.** Let \(V\) be the subspace of \(F^+_d[X]\) spanned by the polynomials \(\ell(X)^d\) for \(\ell(X) \in F_1[X]\). Then \(\dim V = p^{n+1} - \dim U\) where \(U\) is the vector space of all \(p^{n+1}\)-tuples \((c_a : a \in F^{n+1})\) with \(c_a = c_{a_0, a_1, \ldots, a_n} \in F\) such that \(\sum_a c_a(a_0 X_0 + a_1 X_1 + \cdots + a_n X_n)^d = 0\). Thus \((c_a)_a \in U\) iff

\[
0 = \sum_a c_a \sum_i \binom{d}{i} a^i X^i = \sum_i \binom{d}{i} \left[ \sum_a c_a a^i \right] X^i.
\]

Thus \((c_a)_a \in U\) iff

\[
(2.1.1) \quad \sum_a a^i c_a = 0
\]

for all \(i = (i_0, i_1, \ldots, i_n)\) such that \(\binom{d}{i}\) is not divisible by \(p\). By the remarks above, the number of such \(i\) is given by \(\prod_k \binom{n+d_k}{n}\) where the \(d_k\) are the \(p\)-ary digits of \(d\), defined as above. Thus (2.1.1) is a linear system of \(\prod_k \binom{n+d_k}{n}\) equations in \(p^{n+1}\) unknowns \(c_a\). Since each \(i_k \leq d \leq q - 1\), the coefficient matrix of this linear system has full rank \(\binom{n+d}{n}\); see [2, Lemma 2.3]. Thus \(\dim U = p^{n+1} - \prod_k \binom{n+d_k}{n}\), whence \(\dim V = \prod_k \binom{n+d_k}{n}\) and \(V = F^+_d[X]\).

The following slight improvement of Lemma 2.1 will be useful later.
2.2 Corollary. Let $0 \leq d \leq q - 1$. The vector space $F_d[X]$ is spanned by the polynomials $\ell(X)^d$ for $\ell(X) \in F_1[X]$ of the form $\ell(X) = X_0 + a_1X_1 + a_2X_2 + \cdots + a_nX_n$, $a_k \in F$.

Proof. We use the well-known fact that

$$\sum_{\lambda \in F} \lambda^d = \begin{cases} 0, & 0 \leq d \leq q - 2; \\ -1, & d = q - 1. \end{cases}$$

In order to prove the corollary, it suffices to show that for $0 \leq d \leq q - 1$, the polynomial $f(X)^d$ is a linear combination of the polynomials $(X_0 + \lambda f(X))^d$ for $\lambda \in F$, where $f(X) = a_1X_1 + a_2X_2 + \cdots + a_nX_n$. Indeed

$$\sum_{\lambda \in F} \lambda^{q-1-d}(X_0 + \lambda f(X))^d = \sum_{\lambda \in F} \sum_{k=0}^{d} \binom{d}{k} \lambda^{q-1-k} X_k f(X)^{d-k}$$

$$= \sum_{k=0}^{d} \binom{d}{k} \left[ \sum_{\lambda \in F} \lambda^{q-1-k} \right] X_k f(X)^{d-k} = -f(X)^d. \quad \square$$

3. Codes Spanned by Lines of $PG(3,p)$

We now specialize the notation of Section 2 to the case $n = 3$ and $F$ is a field of prime order $p$. Let $P_1, P_2, \ldots, P_N$ be the $N = (p^2 + 1)(p + 1)$ points of $PG(3,F)$. For every polynomial $f(X) \in F[X]$, all of whose homogeneous components have degree divisible by $p - 1$, the values $f(P_i)$ are well-defined and so we may define

$$\phi(f) := (f(P_1), f(P_2), \ldots, f(P_N)) \in F^N.$$ 

The code spanned by the (characteristic vectors of the) planes of $PG(3,F)$ is simply

$$C_2 := \langle \phi(1 - \ell(X)^{p-1}) : \ell(X) \in F_1[X] \rangle_F \leq F^N.$$ 

Note that for nonzero $\ell(X) \in F_1[X]$, the vector $\phi(1 - \ell(X)^{p-1})$ is the characteristic vector of the plane on which $\ell(X)$ vanishes. For $\ell(X) = 0$ we obtain $\phi(1) = (1, 1, \ldots, 1)$, which is the sum of the characteristic vectors of all planes. The code spanned by the lines is

$$C_1 := \langle \phi((1 - \ell(X)^{p-1})(1 - m(X)^{p-1})) : \ell(X), m(X) \in F_1[X] \rangle_F \leq F^N.$$ 

Note that if $\ell(X)$ and $m(X)$ are linearly independent, then the line on which they vanish simultaneously has characteristic vector $\phi((1 - \ell(X)^{p-1})(1 - m(X)^{p-1}))$. If $\ell(X)$ and $m(X)$ are linearly dependent, then the resulting vector $\phi((1 - \ell(X)^{p-1})(1 - m(X)^{p-1})) \in C_2 \subseteq C_1$. 

4
It follows easily from Lemma 2.1 that the polynomials $(1 - \ell(X)p^{-1})(1 - m(X)p^{-1})$ span the space of polynomials 

$$V := F \oplus F_{p-1}[X] \oplus F_{2p-2}[X].$$

Moreover, the map $\phi : V \rightarrow C_1$ is linear and surjective. Its kernel is $V_0 \oplus V_1 \oplus V_2 \oplus V_3$ where $V_k = (X_k^p - X_k)F_{2p-2}[X]$. Thus

$$\dim C_1 = 1 + \binom{p+2}{3} + \binom{2p+1}{3} - 4\binom{p+1}{2} = \frac{1}{6}(p+1)(5p^2 - 2p + 6),$$

in agreement with Hamada’s formula; see [3, Thm.4.8]. We remark that this argument shows that as an $FG$-module for $G = GL(n+1,p)$, $C_1$ has a filtration with quotients given by $F, F_{p-1}[X],$ and $F_{2p-2}[X]/F^\dagger_{2p-2}[X]$; this is because $F^\dagger_{2p-2}[X]$ is spanned by the monomials of degree $2p - 2$ divisible by some $X_k^p$.

We now prove Theorem 1.2, considering only a generalized quadrangle of type $Sp(4,p)$. (The GQ of type $O(5,p)$ is its dual.) We may choose

$$B(u,v) = u_0v_2 + u_1v_3 - u_2v_0 - u_3v_1$$

for our nondegenerate alternating bilinear form. The code spanned by the (characteristic vectors of the) totally isotropic lines with respect to $B$ is $C := \phi(U)$ where $U \leq V$ is the subspace spanned by all polynomials of the form $(1 - \ell(X)p^{-1})(1 - m(X)p^{-1})$ such that the simultaneous zeroes of $\ell(X)$ and $m(X)$ form a totally isotropic line.

Order the monomials in $F[X]$ by graded reverse lex order (cf. [4]). This is the total order on monomials specified as follows. We have $X^i < X^j$ whenever $i_0 + \cdots + i_3 < j_0 + \cdots + j_3$. For monomials of the same degree, we have

$$X_0^i_0 X_1^i_1 X_2^i_2 X_3^i_3 < X_0^j_0 X_1^j_1 X_2^j_2 X_3^j_3 \iff \begin{cases} i_3 < j_3, & \text{or} \\ i_2 < j_2 & \text{or} \\ i_1 < j_1 & \text{or} \\ i_2 = j_2 & \text{or} \\ i_3 = j_3. & \end{cases}$$

For each nonzero polynomial $f(X)$, the initial monomial of $f(X)$, denoted $\text{Init}(f(X))$, is the largest monomial appearing in $f(X)$. Gaussian elimination shows that the dimension of $U$ equals the number of initial monomials of the nonzero polynomials in $U$. Moreover since the kernel of $\phi : U \rightarrow C$ equals $U \cap (\sum_k V_k),$

$$\dim C = |\{\text{Init}(f(X)) : 0 \neq f(X) \in U, \text{Init}(f(X)) \text{ is not divisible by any } X_k^p\}|.$$

Clearly $F \oplus F_{p-1}[X] \subseteq U$, so that $\dim C \geq 1 + \binom{p+2}{3}$. In view of the upper bound given by Lemma 1.1, it suffices to find $\frac{1}{2}p(p+1)^2 + 1 - 1 - \binom{p+2}{3} = \frac{1}{6}p(p+1)(2p+1)$ monomials of degree $2p - 2$, none of which are divisible by any $X_k^p$, occurring as initial monomials of polynomials in $U$. 

5
3.1 Lemma. The monomials $X_0^{j_0}X_1^{j_1}X_2^{j_2}X_3^{j_3}$ for $j_0 + \cdots + j_3 = 2p - 2$, $j_0 + j_2 \leq p - 1$, occur as initial monomials of polynomials in $U$.

Proof. Let $\alpha, \beta, \gamma \in F$. Then

$$\langle (-\alpha, 0, 1, \gamma), (\gamma, -1, 0, \beta) \rangle_F$$

is a totally singular line of $PG(3, p)$, equal to the set of common zeroes of

$$\ell(X) = X_0 + \gamma X_1 + \alpha X_2 \quad \text{and} \quad m(X) = \beta X_1 - \gamma X_2 + X_3.$$ 

Two applications of Corollary 2.2 show that

$$U \supseteq \langle [(X_0 + \gamma X_1) + \alpha X_2]^p - 1 [\beta X_1 + (X_3 - \gamma X_2)]^p - 1 : \alpha, \beta, \gamma \in F \rangle_F$$

$$= \langle (X_0 + \gamma X_1)^{i_0}X_1^{i_1}X_2^{i_2}(X_3 - \gamma X_2)^{i_3} : i_0 + i_2 = i_1 + i_3 = p - 1, \gamma \in F \rangle_F.$$ 

Now

$$(X_0 + \gamma X_1)^{i_0}X_1^{i_1}X_2^{i_2}(X_3 - \gamma X_2)^{i_3} = (X_0 + \gamma X_1)^{i_0}X_1^{i_1}X_2^{i_2}X_3^{i_3} + (\text{linear combinations of monomials } < X_0^{i_0}X_1^{i_1}X_2^{i_2}X_3^{i_3} >).$$

Another application of Corollary 2.2 shows that the monomials $X_0^{i_0-k}X_1^{i_1+k}X_2^{i_2}X_3^{i_3}$ for $i_0 + i_2 = i_1 + i_3 = p - 1, 0 \leq k \leq i_0$, occur as initial monomials of members of $U$. These monomials are the same as those listed in the statement of the lemma. \hfill \Box

Among the monomials listed in Lemma 3.1, those which are not divisible by any $X_k^p$ are the monomials

$$X_0^{j_0}X_1^{j_1}X_2^{d-j_0}X_3^{2p-2-d-j_1}, \quad 0 \leq j_0 \leq d \leq p - 1, \quad p - 1 - d \leq j_1 \leq p - 1.$$ 

The number of such monomials is

$$\sum_{d=0}^{p-1} (d + 1)^2 = \frac{1}{6}p(p + 1)(2p + 1).$$

By the preceding arguments, this proves Theorem 1.2.
References