ALGEBRAIC COMBINATORICS

Santana F. Afton & Eric Swartz
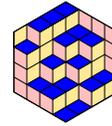
On prime order automorphisms of generalized quadrangles

Santana F. Afton & Eric Swartz

ABSTRACT In this paper, we study prime order automorphisms of generalized quadrangles. We show that, if $\mathcal{Q}$ is a thick generalized quadrangle of order (s,t), where $s > t$ and $s+1$ is prime, and $\mathcal{Q}$ has an automorphism of order $s+1$, then

$$s \left\lceil \left\lceil \frac{t^2}{s+1} \right\rceil \left(\frac{s+1}{t} \right) \right\rceil \leqslant t(s+t),$$

with a similar inequality holding in the dual case when $t > s$, $t+1$ is prime, and $\mathcal{Q}$ is a thick generalized quadrangle of order (s,t) with an automorphism of order $t+1$.

In particular, if $s+1$ is prime and if there exists a natural number n such that

$$\frac{t^2}{n+1} + t \leqslant s+1 < \frac{t^2}{n},$$

then a thick generalized quadrangle $\mathcal{Q}$ cannot have an automorphism of order $s+1$, and hence the automorphism group of $\mathcal{Q}$ cannot be transitive on points. These results apply to numerous potential orders for which it is still unknown whether or not generalized quadrangles exist, showing that any examples would necessarily be somewhat asymmetric. Finally, we are able to use the theory we have built up about prime order automorphisms of generalized quadrangles to show that the automorphism group of a potential generalized quadrangle of order $(4, 12)$ must necessarily be intransitive on both points and lines.

1. INTRODUCTION

Following [26], a *finite generalized quadrangle* $\mathcal{Q}$ is an incidence structure $(\mathcal{P}, \mathcal{L}, \mathrm{I})$, where $\mathcal{P}$ is the set of *points*, $\mathcal{L}$ is the set of *lines* (which is disjoint from $\mathcal{P}$), and I is a symmetric point-line incidence relation satisfying the following axioms:

Point-line incidence: Each point is incident with $t+1$ lines and each line is incident with $s+1$ points, where $s, t \in \mathbb{N}$, and two distinct points (respectively, lines) are mutually incident with at most one line (respectively, point).

GQ Axiom: Given a point P and a line ℓ not incident with P, there is a unique pair $(P', \ell') \in \mathcal{P} \times \mathcal{L}$ such that $P \mathrm{\ I\ } \ell' \mathrm{\ I\ } P' \mathrm{\ I\ } \ell$.

A generalized quadrangle with $s+1$ points incident with a given line and $t+1$ lines incident with a given point is said to have *order* (s,t), and such a generalized quadrangle is said to be *thick* if both $s > 1$ and $t > 1$. Much like the situation with projective planes, there are some arithmetical restrictions on the possible order (s,t) of a generalized quadrangle; see Lemma 2.1. However, these restrictions leave a large number of cases about which absolutely nothing is known, and, while projective planes are only known to exist when their order is a prime power, there exist generalized

quadrangles of orders (q, q), (q, q^2), (q^2, q), (q^2, q^3), (q^3, q^2), $(q - 1, q + 1)$, and $(q + 1, q - 1)$, where q is a prime power [26]. The existence of generalized quadrangles of orders $(q - 1, q + 1)$ and $(q + 1, q - 1)$ especially make it entirely unclear whether generalized quadrangles of other orders will exist.

Generalized quadrangles (and, more generally, *generalized n-gons*) were invented by Jacques Tits [29] to help better understand certain classical groups by providing natural geometric objects on which the groups act. The *automorphism group* of a finite generalized quadrangle is the set of permutations of the point set that preserve collinearity. While the definition of a generalized quadrangle is purely combinatorial, the known examples of generalized quadrangles all have nontrivial (and, typically, quite robust) automorphism groups and often arise from algebraic constructions; see [13, 23, 25, 26]. Moreover, many examples of generalized quadrangles of order $(q-1, q+1)$ and $(q+1, q-1)$ have automorphism groups that are point-transitive and line-transitive, respectively. For this reason, given a hypothetical order (s, t) of a generalized quadrangle $\mathcal{Q}$, it is natural to study the possible automorphisms of $\mathcal{Q}$ in the same spirit that the possible automorphisms of the "missing" Moore graph have been studied; see [10, pp. 89–91] and [21]. Toward this end, we prove the following result:

THEOREM 1.1. *Let $\mathcal{Q}$ be a thick generalized quadrangle of order (s, t), where $s > t$ and $s + 1$ is prime. If $\mathcal{Q}$ has an automorphism of order $s + 1$, then*

$$s \left\lceil \left\lceil \frac{t^2}{s+1} \right\rceil \left(\frac{s+1}{t} \right) \right\rceil \leqslant t(s+t).$$

If $\mathcal{Q}$ is a generalized quadrangle of order (s, t), where s, t satisfy both the hypotheses and the inequality of Theorem 1.1, then we cannot say much. The real strength of this result arises in the situation where s, t satisfy all of the numerical constraints of Theorem 1.1 except for the inequality, in which case we can make the following conclusion:

COROLLARY 1.2. *Let $\mathcal{Q}$ be a thick generalized quadrangle of order (s, t), where $s > t$ and $s + 1$ is prime. If*

$$s \left\lceil \left\lceil \frac{t^2}{s+1} \right\rceil \left(\frac{s+1}{t} \right) \right\rceil > t(s+t),$$

then $\mathcal{Q}$ does not have an automorphism of order $s + 1$ and the automorphism group of $\mathcal{Q}$ cannot be point-transitive.

The *dual* of a generalized quadrangle $\mathcal{Q}$ with point set $\mathcal{P}$ and line set $\mathcal{L}$ comes from switching the roles of points and lines to create a new generalized quadrangle $\mathcal{Q}'$ with point set $\mathcal{L}$ and line set $\mathcal{P}$. Viewed through the lens of the dual quadrangle, Corollary 1.2 can be rephrased to obtain results about the line-transitivity of the automorphism group of certain potential generalized quadrangles.

COROLLARY 1.3. *Let $\mathcal{Q}$ be a thick generalized quadrangle of order (s, t), where $t > s$ and $t + 1$ is prime. If*

$$t \left\lceil \left\lceil \frac{s^2}{t+1} \right\rceil \left(\frac{t+1}{s} \right) \right\rceil > s(s+t),$$

then $\mathcal{Q}$ does not have an automorphism of order $t + 1$ and the automorphism group of $\mathcal{Q}$ cannot be line-transitive.

At first glance, the inequalities listed above seem to be rather weak. However, the following corollaries show the power of the result when one parameter is (relatively speaking) much bigger than the other.

COROLLARY 1.4. *Let $\mathcal{Q}$ be a thick generalized quadrangle of order (s, t). If $s + 1$ is a prime and if there exists a natural number n such that*

$$\frac{t^2}{n+1} + t \leqslant s + 1 < \frac{t^2}{n},$$

then $\mathcal{Q}$ cannot have an automorphism of order $(s + 1)$ and cannot have a point-transitive group of automorphisms.

COROLLARY 1.5. *If $\mathcal{Q}$ is a generalized quadrangle of order $(q^2 - nq, q)$, where n and q are positive integers with $2n < q$ and $q^2 - nq + 1$ is prime, then $\mathcal{Q}$ cannot have an automorphism of order $q^2 - nq + 1$, and, moreover, $\mathcal{Q}$ does not have a point-transitive group of automorphisms.*

For thick generalized quadrangles, when $s < t^2$, the current best theoretical upper bound is $s \leqslant t^2 - t$ (see Lemma 2.1), and, for this reason, hypothetical generalized quadrangles of order $(q^2 - q, q)$ (and, dually, $(q, q^2 - q)$) have been the subject of recent investigation [1, 22], although still very little is known about such (potential) generalized quadrangles. In particular, Corollary 1.5 shows that the automorphism group of a generalized quadrangle of order $(q^2 - q, q)$, where $q^2 - q + 1$ is prime, is not point-transitive.

We are further able to use the theory that we have built up to study the automorphism group of a potential generalized quadrangle of order $(4, 12)$. The best known result thus far comes from [1], which states that if such a generalized quadrangle contains an *ovoid*, a set of $st + 1$ pairwise noncollinear points, then its automorphism group cannot be point-transitive. We are able to say considerably more:

THEOREM 1.6. *If $\mathcal{Q}$ is a generalized quadrangle of order $(4, 12)$, then the automorphism group of $\mathcal{Q}$ cannot be transitive on either points or lines.*

While there are certainly "regular" combinatorial structures that are asymmetric, Theorem 1.6 makes it much more unlikely that such a generalized quadrangle exists. Moreover, it is likely that the techniques used in the proof of Theorem 1.6 can be used to prove that the automorphism groups of generalized quadrangles of other potential orders cannot be point- or line-transitive.

It is possible that the only generalized quadrangles that have a point-transitive automorphism group either arise from classical groups or have order $(q-1, q+1)$, where q is a prime power; see [26]. On the other hand, unlike the case for projective planes [17, 18], other than what is known about specific families of generalized quadrangles, there is a much smaller body of knowledge when it comes to point-transitive generalized quadrangles: the results either involve conditions that are much stronger than mere point-transitivity [2, 3, 4, 5, 6, 7] or involve groups G that act *regularly* on the point set, i.e. G is transitive on the point set, but the stabilizer in G of each point is trivial [12, 14, 16, 28, 30]. The possible orders ruled out by Corollaries 1.2, 1.4, 1.5 and Theorem 1.6 appear to be among the first combinatorially feasible parameters (in the sense of the results contained in Lemma 2.1) that can a priori be ruled out from admitting generalized quadrangles with point-transitive automorphism groups.

This paper is organized as follows. In Section 2, we provide the background material necessary for the rest of the paper. In Section 3, we prove various preliminary results about automorphisms of prime order of generalized quadrangles. Section 4 is dedicated to the proof of Theorem 1.1, and Section 5 is dedicated to the consequences of Theorem 1.1 and, in particular, contains proofs of Corollaries 1.2, 1.4, and 1.5. Section 6 contains results that apply specifically to generalized quadrangles of order $(4, 12)$, culminating in the proof of Theorem 1.6. Finally, we include in Appendix A some tables which list all possible orders (s, t) with $t \leqslant 100$ to which Corollary 1.2 applies.

2. BACKGROUND

Let $\mathcal{Q}$ be a generalized quadrangle with point set $\mathcal{P}$ and line set $\mathcal{L}$. We say that two points P, P' are *collinear* if there is a line incident with both P and P', in which case we write $P \sim P'$. Similarly, we say that two lines ℓ, ℓ' are *concurrent* if there is a point incident with both ℓ and ℓ', and we write $\ell \sim \ell'$. Our convention here will be that $P \sim P$. Given a set X of points,

$$X^{\perp} := \{P \in \mathcal{P} : P \sim Q \text{ for all } Q \in X\}.$$

We define $Z^{\perp}$ for a set Z of lines analogously. If the role of "point" and of "line" (as well as the values of s and t) are interchanged for $\mathcal{Q}$, then the result is also a generalized quadrangle and is called the *dual* of $\mathcal{Q}$.

A *grid* is an incidence structure $(\mathcal{P}, \mathcal{L}, \mathrm{I})$ such that for some integers $s_1, s_2 \in \mathbb{N}$ we have

$$\mathcal{P} = \{P_{i,j} : 0 \leqslant i \leqslant s_1, 0 \leqslant j \leqslant s_2\}, \ \mathcal{L} = \{\ell_0, \dots, \ell_{s_1}, \ell'_0, \dots, \ell'_{s_2}\}$$

with incidence defined by $P_{i,j} \mathrm{I} \ell_k$ if and only if $i = k$ and $P_{i,j} \mathrm{I} \ell'_k$ if and only if $j = k$. A *dual grid* is the point-line dual of a grid, and, instead of s_1 and s_2, it is defined in terms of parameters t_1 and t_2. It is easy to see that a grid is a generalized quadrangle if and only if $s_1 = s_2$, and the generalized quadrangles with $t = 1$ are precisely the grids with $s_1 = s_2 (= s)$. The dual result holds for dual grids.

The following omnibus lemma contains basic results about the parameters s and t.

LEMMA 2.1 ([26, 1.2.1, 1.2.2, 1.2.3, 1.2.5]). *Let $\mathcal{Q}$ be a finite generalized quadrangle of order (s, t). Then the following hold:*

(i) $|\mathcal{P}| = (s+1)(st+1)$ *and* $|\mathcal{L}| = (t+1)(st+1)$;
(ii) $s + t$ *divides* $st(s+1)(t+1)$;
(iii) *if* $s, t > 1$, *then* $t \leqslant s^2$ *and* $s \leqslant t^2$;
(iv) *if* $1 < s < t^2$, *then* $s \leqslant t^2 - t$, *and if* $1 < t < s^2$, *then* $t \leqslant s^2 - s$.

The following result of Payne is an application of the so-called Higman–Sims technique and is crucial to the proof of Theorem 1.1. A more general result is actually proved in [24], and a proof of just Lemma 2.2 is given in [26, 1.4.1].

LEMMA 2.2 ([24, Theorem I.2]). *Let X and Y be disjoint sets of pairwise noncollinear points of a generalized quadrangle $\mathcal{Q}$ of order (s, t) with $s > 1$ such that $|X| = m$, $|Y| = n$, and $X \subseteq Y^{\perp}$. Then $(m-1)(n-1) \leqslant s^2$. Dually, if X and Y are disjoint sets of pairwise nonconcurrent lines of a generalized quadrangle $\mathcal{Q}$ of order (s, t) with $t > 1$ such that $|X| = m$, $|Y| = n$, and $X \subseteq Y^{\perp}$, then $(m-1)(n-1) \leqslant t^2$.*

Let x be an automorphism of $\mathcal{Q}$. Given a point P of $\mathcal{Q}$, there are three possibilities:

(i) $P^x = P$,
(ii) $P^x \neq P$ but $P^x \sim P$,
(iii) $P^x \not\sim P$.

With this in mind, we define $\mathcal{P}_0(x)$ to be the set of points fixed by x, $\mathcal{P}_1(x)$ to be the set of points that are not fixed by x but are sent to collinear points, and $\mathcal{P}_2(x)$ to be the set of points sent to noncollinear points by x. For each i, we define $\alpha_i(x) := |\mathcal{P}_i(x)|$. For the lines of $\mathcal{Q}$, we define $\mathcal{L}_0(x)$, $\mathcal{L}_1(x)$, and $\mathcal{L}_2(x)$ analogously, and for each i we define $\beta_i(x) := |\mathcal{L}_i(x)|$.

The following result is known as Benson's Lemma and is a fundamental result regarding automorphisms of generalized quadrangles. Although we state the result here only in terms of generalized quadrangles, it should be noted that Benson's Lemma is a special case of a more general idea, which allows the character of an automorphism group of an association scheme to be calculated on one of its eigenspaces. This

technique, attributed to Graham Higman, is described in [10, pp. 89–91] and has been applied to both distance-regular and strongly regular graphs; see, for instance [11, 15, 21].

LEMMA 2.3 ([8, Lemma 4.3]). *If x is an automorphism of a finite generalized quadrangle of order (s,t), then*

$$(t+1)\alpha_0(x) + \alpha_1(x) \equiv (st+1) \pmod{s+t}.$$

The following result relates the total number of points sent to collinear points by x to the total number of lines sent to collinear lines by x.

LEMMA 2.4 ([26, 1.9.2]). *If x is an automorphism of a finite generalized quadrangle of order (s,t), then*

$$(1+t)\alpha_0(x) + \alpha_1(x) = (1+s)\beta_0(x) + \beta_1(x).$$

Given an automorphism x of $\mathcal{Q}$, the substructure $\mathcal{Q}_x$ fixed by x must have one of a few types. The following result lists these possible types. For convenience, our delineation into types is slightly different than what is listed in [26].

LEMMA 2.5 ([26, 2.4.1]). *Let x be an automorphism of a generalized quadrangle $\mathcal{Q}$. The substructure $\mathcal{Q}_x$ fixed by x is one of the following:*

(0) *The substructure $\mathcal{Q}_x$ is empty; that is, there are no fixed points and there are no fixed lines.*

(1) *At least one point is fixed, all fixed points are noncollinear, and no lines are fixed.*

(1') *At least one line is fixed, all fixed lines are nonconcurrent, and no points are fixed.*

(2) *There exists some fixed point P such that $P \sim P'$ for each fixed point P', there exists at least one fixed line, and every fixed line is incident with P.*

(2') *There exists some fixed line ℓ such that $\ell \sim \ell'$ for each fixed line ℓ', there exists at least one fixed point, and every fixed point is incident with ℓ.*

(3) *The substructure $\mathcal{Q}_x$ is a grid with $s_1 < s_2$.*

(3') *The substructure $\mathcal{Q}_x$ is a dual grid with $t_1 < t_2$.*

(4) *The substructure $\mathcal{Q}_x$ is a generalized subquadrangle of order (s',t').*

Note that we allow in (4) the possibility that $\mathcal{Q}_x$ is a *grid* or a *dual grid*, i.e. we allow either $s' = 1$ or $t' = 1$.

Finally, we introduce some terminology from permutation group theory that will be used in Section 6. The action of a group G on a set Ω is said to be *quasiprimitive* if every nontrivial normal subgroup of G is transitive on Ω. Quasiprimitive groups are a generalization of primitive permutation groups, since, if G acts on Ω and G contains a normal subgroup N that is intransitive on Ω, then the set of orbits of N on Ω is a G-invariant partition of Ω. For a characterization of quasiprimitive permutation groups, see [27, Section 2].

3. AUTOMORPHISMS OF PRIME ORDER

In this section, we collect a number of basic results about prime order automorphisms of generalized quadrangles. Throughout this section, $\mathcal{Q}$ will refer to a generalized quadrangle of order (s,t) with point set $\mathcal{P}$ and line set $\mathcal{L}$. For a given automorphism x of $\mathcal{Q}$, the *type* of $\mathcal{Q}_x$ refers to its designation in Lemma 2.5.

Lemma 3.1. *Let x be an automorphism of $\mathcal{Q}$ with order p, where p is a prime. For $i = 1, 2$, we have*

$$\alpha_i(x), \beta_i(x) \equiv 0 \pmod{p}.$$

Moreover,

$$\alpha_0(x) \equiv (s + 1)(st + 1) \pmod{p}$$

and

$$\beta_0(x) \equiv (t + 1)(st + 1) \pmod{p}.$$

Proof. The set $\mathcal{P}_1(x)$ can be partioned into orbits of $\langle x \rangle$, and, since none of these points are fixed, each orbit has size p. This implies that $\alpha_1(x) \equiv 0 \pmod{p}$. By duality, $\beta_1(x) \equiv 0 \pmod{p}$, and analogous arguments show that $\alpha_2(x), \beta_2(x) \equiv 0 \pmod{p}$. The results for $\alpha_0(x), \beta_0(x)$ follow from

$$(s + 1)(st + 1) = |\mathcal{P}| = \alpha_0(x) + \alpha_1(x) + \alpha_2(x)$$

and

$$(t + 1)(st + 1) = |\mathcal{L}| = \beta_0(x) + \beta_1(x) + \beta_2(x). \qquad \square$$

Lemma 3.2. *Let x be an automorphism of $\mathcal{Q}$ of order p, where p is a prime, and assume that $\mathcal{Q}_x$ has type (0). Then either $t + 1 \equiv s + 1 \equiv 0 \pmod{p}$ or $st + 1 \equiv 0 \pmod{p}$. If p is an odd prime, then $s + 1 \equiv t + 1 \equiv 0 \pmod{p}$ if and only if $st + 1 \not\equiv 0 \pmod{p}$.*

Proof. Since $\mathcal{Q}_x$ has type (0), it follows that $\alpha_0(x) = \beta_0(x) = 0$, implying that $p \mid (s + 1)(st + 1)$ and $p \mid (t + 1)(st + 1)$. If $p \nmid (st + 1)$, then $p \mid (s + 1)$ and $p \mid (t + 1)$ by Euclid's Lemma. Finally, if p is an odd prime and $s + 1 \equiv t + 1 \equiv 0 \pmod{p}$, then

$$st + 1 \equiv (-1)(-1) + 1 \equiv 2 \not\equiv 0 \pmod{p}. \qquad \square$$

Lemma 3.3. *Let x be an automorphism of $\mathcal{Q}$ of order p, where p is a prime. If $\mathcal{Q}_x$ has type (1), then $t + 1 \equiv 0 \pmod{p}$. If $\mathcal{Q}_x$ has type $(1')$, then $s + 1 \equiv 0 \pmod{p}$.*

Proof. We will prove the result for $\mathcal{Q}_x$ of type (1); the analogous result for type $(1')$ follows by duality. Since $\mathcal{Q}_x$ has type (1), there are no fixed lines, but there is at least one fixed point. Let P be any fixed point, and let $\mathcal{L}(P)$ be the lines incident with P. Since x is an automorphism, if $\ell \in \mathcal{L}(P)$, then $\ell^x \in \mathcal{L}(P)$. Since no line is fixed by x, $|\mathcal{L}(P)| = t + 1$, and $\mathcal{L}(P)$ can be partitioned into orbits of $\langle x \rangle$, it follows that $t + 1 \equiv 0 \pmod{p}$. $\qquad \square$

Lemma 3.4. *Let x be an automorphism of $\mathcal{Q}$ of order p, where p is a prime.*
   (i) *If $\mathcal{Q}_x$ has type (2) and $\alpha_0(x) = 1$, then $s + 1 \equiv 1 \pmod{p}$.*
   (ii) *If $\mathcal{Q}_x$ has type (2) and $\alpha_0(x) \geqslant 2$, then $t + 1 \equiv 1 \pmod{p}$.*
   (iii) *If $\mathcal{Q}_x$ has type $(2')$ and $\beta_0(x) = 1$, then $t + 1 \equiv 1 \pmod{p}$.*
   (iv) *If $\mathcal{Q}_x$ has type $(2')$ and $\beta_0(x) \geqslant 2$, then $s + 1 \equiv 1 \pmod{p}$.*

Proof. We will prove the results for $\mathcal{Q}_x$ of type (2) and note that the analogous results for type $(2')$ follow by duality. Assume first that $\alpha_0(x) = 1$, and let P be this unique fixed point. By assumption, there is at least one fixed line ℓ incident with P, and the s remaining points of ℓ are partitioned into orbits of size p of $\langle x \rangle$, proving that $s + 1 \equiv 1 \pmod{p}$.

Now assume that $\alpha_0(x) \geqslant 2$. Let P, Q be two distinct fixed points, where we may assume by hypothesis that $P \sim P'$ for every $P' \in \mathcal{P}_0(x)$. Hence $P \sim Q$, and so x also fixes the unique line ℓ with which P and Q are mutually incident. Since none of the other t lines incident with Q are fixed by x, these t lines are partitioned into orbits of size p, proving that $t + 1 \equiv 1 \pmod{p}$. $\qquad \square$

LEMMA 3.5. *Let x be an automorphism of $\mathcal{Q}$ of order p, where p is a prime. If $\mathcal{Q}_x$ has type* (2), *then*

$$\alpha_0(x) \equiv 1 + s\beta_0(x) \pmod{p}.$$

If $\mathcal{Q}_x$ has type (2′), *then*

$$\beta_0(x) \equiv 1 + t\alpha_0(x) \pmod{p}.$$

Proof. We will prove the result for $\mathcal{Q}_x$ of type (2); the result when $\mathcal{Q}_x$ is of type (2′) follows by duality. Let P be the distinguished point with which all fixed lines of x are incident and all fixed points of x are collinear. For any fixed line ℓ, let $s_0(\ell)$ be the number of fixed points incident with ℓ other than P and let $s_1(\ell)$ be the number of points incident with ℓ not fixed by x. Noting that the $s_1(\ell)$ points of ℓ that are not fixed by x are partitioned into orbits of size p of $\langle x \rangle$, we have $s_1(\ell) \equiv 0 \pmod{p}$, which implies that $s_0(\ell) \equiv s \pmod{p}$ since $s_0(\ell) + s_1(\ell) = s$. If the $\beta_0(x)$ lines fixed by x are $\ell_1, \ldots, \ell_{\beta_0(x)}$, then

$$\alpha_0(x) = 1 + \sum_{i=1}^{\beta_0(x)} s_0(\ell_i) \equiv 1 + \sum_{i=1}^{\beta_0(x)} s \pmod{p},$$

and so

$$\alpha_0(x) \equiv 1 + s\beta_0(x) \pmod{p},$$

as desired. $\qquad\square$

LEMMA 3.6. *Let x be an automorphism of $\mathcal{Q}$ of order p, where p is a prime. If $\mathcal{Q}_x$ has type* (3), *then $t + 1 \equiv 2 \pmod{p}$ and $s_1 \equiv s_2 \equiv s \pmod{p}$. If $\mathcal{Q}_x$ has type* (3′), *then $s + 1 \equiv 2 \pmod{p}$ and $t_1 \equiv t_2 \equiv t \pmod{p}$. In particular, if $\mathcal{Q}_x$ has type* (3) *or type* (3′), *then $p < \max\{s, t\}$, and, if $\mathcal{Q}$ is a thick generalized quadrangle and $\mathcal{Q}_x$ has either type* (3) *or type* (3′), *then $p < \min\{s, t\}$.*

Proof. We will prove the result for $\mathcal{Q}_x$ of type (3); the result when $\mathcal{Q}_x$ is of type (3′) follows by duality. Let P be a fixed point of the grid. Since exactly two lines incident with P are fixed by x, the remaining lines incident with P must be partitioned into $\langle x \rangle$-orbits of size p, and hence $t + 1 \equiv 2 \pmod{p}$. Now, there are two types of lines in the grid: those containing $s_1 + 1$ fixed points and those containing $s_2 + 1$ fixed points. For a line ℓ of $\mathcal{Q}$ fixed by x containing $s_1 + 1$ fixed points in $\mathcal{Q}_x$, the remaining $(s + 1) - (s_1 + 1)$ points incident with ℓ are partioned into $\langle x \rangle$-orbits, and so $s_1 \equiv s \pmod{p}$. Analogously, we have $s_2 \equiv s \pmod{p}$. Finally, the prime p divides $(t + 1) - 2 = t - 1$, so $p \leqslant t - 1$ if $t > 1$, and, since $s_1 < s_2 \leqslant s$, p divides $s - s_1 > 0$ and $p \leqslant s - s_1$. The result follows. $\qquad\square$

LEMMA 3.7. *Let x be an automorphism of $\mathcal{Q}$ of order p, where p is a prime. If $s + 1 \not\equiv 0, 1, 2 \pmod{p}$ and $t + 1 \not\equiv 0, 1, 2 \pmod{p}$, then either $\mathcal{Q}_x$ has type* (0) *and $st + 1 \equiv 0 \pmod{p}$, or $\mathcal{Q}_x$ has type* (4).

Proof. We will proceed through the types listed in Lemma 2.5. If $\mathcal{Q}_x$ has type (0), then since p divides neither $s + 1$ nor $t + 1$, it follows that $st + 1 \equiv 0 \pmod{p}$ by Lemma 3.2. If $\mathcal{Q}_x$ has type (1) or (1′), then either $s + 1 \equiv 0 \pmod{p}$ or $t + 1 \equiv 0 \pmod{p}$ by Lemma 3.3, contrary to our hypotheses. If $\mathcal{Q}_x$ has type (2) or (2′), then either $s + 1 \equiv 1 \pmod{p}$ or $t + 1 \equiv 1 \pmod{p}$ by Lemma 3.4, a contradiction to our hypotheses. Finally, if $\mathcal{Q}_x$ has type (3) or type (3′), then either $s + 1 \equiv 2 \pmod{p}$ or $t + 1 \equiv 2 \pmod{p}$ by Lemma 3.6, again a contradiction. $\qquad\square$

LEMMA 3.8. *Let x be an automorphism of $\mathcal{Q}$ of order p, where p is a prime. If $\mathcal{Q}_x$ has type* (4) *and is a subquadrangle of order (s', t'), then $s' \equiv s \pmod{p}$ and $t' \equiv t \pmod{p}$.*

Proof. Let ℓ be any line fixed by x. By hypothesis, there are exactly $s' + 1$ points fixed by x on ℓ, and hence there are $(s + 1) - (s' + 1) = (s - s')$ points on ℓ that are not fixed by x. These remaining $(s - s')$ points are partitioned into orbits of $\langle x \rangle$ of size p, and hence $s' \equiv s \pmod{p}$. By duality, $t' \equiv t \pmod{p}$. $\square$

LEMMA 3.9. *Let x be an automorphism of $\mathcal{Q}$ of order p, where p is a prime. If $\mathcal{Q}_x$ has type (4) and is a proper subquadrangle of order (s, t'), then*

$$\alpha_0(x) = (s + 1)(st' + 1)$$
$$\alpha_1(x) = 0$$
$$\alpha_2(x) = s(s + 1)(t - t')$$

and

$$\beta_0(x) = (t' + 1)(st' + 1)$$
$$\beta_1(x) = (t - t')(s + 1)(st' + 1)$$
$$\beta_2(x) = (t + 1)(st + 1) - (t(s + 1) - st' + 1)(st' + 1).$$

Proof. First, $\alpha_0(x) = (s + 1)(st' + 1)$, since $\mathcal{Q}_x$ is a subquadrangle of order (s, t'). Similarly, $\beta_0(x) = (t' + 1)(st' + 1)$. We will now show that $\alpha_1(x) = 0$. Let P be a point that is not fixed by x. If ℓ is a line fixed by x, then, since $\mathcal{Q}_x$ is a subquadrangle of order (s, t'), all points incident with ℓ are fixed by x. This means that P is not incident with ℓ, and so, by the GQ Axiom, there exists a unique point Q on ℓ with which P is collinear. Let ℓ' be the line incident with both P and Q. Since Q is incident with ℓ, Q is fixed. The line ℓ' cannot be fixed, since P is not fixed by x. However, $(\ell')^x$ is also incident with Q, and, by the GQ Axiom, there are no triangles, which means $P \not\sim P^x$ and $\alpha_1(x) = 0$. The value of $\beta_1(x)$ now follows from Lemma 2.4, and the values of $\alpha_2(x)$ and $\beta_2(x)$ follow from

$$|\mathcal{P}| = \alpha_0(x) + \alpha_1(x) + \alpha_2(x)$$

and

$$|\mathcal{L}| = \beta_0(x) + \beta_1(x) + \beta_2(x),$$

respectively. $\square$

LEMMA 3.10. *Let x be an automorphism of $\mathcal{Q}$ of order p, where p is a prime. If $\mathcal{Q}_x$ has type (4) and $s' = s$, then $s + t$ divides $st'(st + 1)$.*

Proof. By Lemmas 2.3 and 3.9,

$$(t + 1)(s + 1)(st' + 1) \equiv st + 1 \pmod{s + t}.$$

The result follows after simplification of this expression. $\square$

LEMMA 3.11. *Let p be a prime such that $p \geqslant s$, and suppose x is an automorphism of $\mathcal{Q}$ of order p such that $\mathcal{Q}_x$ has type (4). Then $s' = s$, $t' < t$, $t' \equiv t \pmod{p}$, and $s + t$ divides $st'(st + 1)$.*

Proof. By Lemma 3.8, $s' \equiv s \pmod{p}$, and, since $p \geqslant s \geqslant s'$, we have $s' = s$. The result now follows from Lemmas 3.8 and 3.10. $\square$

LEMMA 3.12. *Let $\mathcal{Q}$ be a generalized quadrangle of order (s,t), where $s > t$ and $s + 1$ is prime. If x is an automorphism of $\mathcal{Q}$ of order $s+1$, then $\mathcal{Q}_x$ has type $(1')$.*

Proof. Assume first that $\mathcal{Q}_x$ has type (0). Since $s > t$, $(s+1) \nmid (t+1)$, and hence $st + 1 \equiv 0 \pmod{s+1}$ by Lemma 3.2. However, this implies that

$$s(t-1) \equiv (st+1) - (s+1) \equiv 0 \pmod{s+1}.$$

By Euclid's Lemma, either $(s+1) \mid s$ or $(s+1) \mid (t-1)$, which is impossible since $s + 1 > s, t - 1$. Hence $\mathcal{Q}_x$ cannot have type (0).

If $\mathcal{Q}_x$ has type (1), then $t + 1 \equiv 0 \pmod{s+1}$ by Lemma 3.3, which is impossible since $s > t$. If $\mathcal{Q}_x$ has either type (2) or type $(2')$, then either $s+1 \equiv 1 \pmod{s+1}$ or $t + 1 \equiv 1 \pmod{s+1}$ by Lemma 3.4, again a contradiction. If $\mathcal{Q}_x$ has either type (3) or type $(3')$, then either $s + 1 \equiv 2 \pmod{s+1}$ or $t + 1 \equiv 2 \pmod{s+1}$ by Lemma 3.6, another contradiction. Finally, if $\mathcal{Q}_x$ has type (4), then by Lemma 3.11 we have $s = s'$ and $(s+1)$ divides $(t - t')$. However, $t - t'$ is both smaller than $s + 1$ and nonzero, a contradiction. □

LEMMA 3.13. *Let p be a prime that divides the order of the automorphism group of a finite generalized quadrangle $\mathcal{Q}$ of order (s,t). If $p \nmid (st+1)$, then $p \leqslant \max\{s+1, t+1\}$.*

Proof. First, if $t = 1$, then $\mathcal{Q}$ is a grid with automorphism group isomorphic to the wreath product $\mathrm{Sym}(s+1) \, \mathrm{wr} \, 2$, and so $p \leqslant s + 1$, with an analogous result holding in the dual grid case. Hence we may assume that $\mathcal{Q}$ is a thick generalized quadrangle. Assume $p > (s+1)$ and $p > (t+1)$. Let x be an automorphism of $\mathcal{Q}$ of order p. Since $\mathcal{Q}$ is thick, we have $s + 1 \not\equiv 0, 1, 2 \pmod{p}$ and $t + 1 \not\equiv 0, 1, 2 \pmod{p}$. By Lemma 3.7, if $p \nmid (st + 1)$, then $\mathcal{Q}_x$ has type (4). However, since $p > s + 1$, by Lemma 3.11 we have that $s = s'$ and $p \mid (t - t')$, a contradiction since $p > s + 1 > t - t' > 0$. The result follows. □

It should be noted that this last lemma yields a definitive list of primes that could be orders of automorphisms of a generalized quadrangle $\mathcal{Q}$ without knowing any information about $\mathcal{Q}$ other than its order (s,t).

4. PROOF OF THE INEQUALITY

This section is devoted to the proof of Theorem 1.1.

Proof of Theorem 1.1. Let $\mathcal{Q}$ be a thick generalized quadrangle of order (s,t), where $s > t$ and $s+1$ is prime, and let $\mathcal{Q}$ have an automorphism x of order $s+1$. By Lemma 3.12, $\mathcal{Q}_x$ has type $(1')$, thus no points are fixed by x and at least one line is fixed by x. Let ℓ be a line fixed by x. Since $\mathcal{Q}_x$ has type $(1')$, no points incident with ℓ are fixed and all fixed lines are pairwise nonconcurrent, and so the lines concurrent with ℓ are divided into t distinct orbits of $\langle x \rangle$ of size $s + 1$. If ℓ' is any other fixed line, then $|\{\ell, \ell'\}^{\perp}| = s + 1$, i.e. there is a unique $\langle x \rangle$-orbit of lines concurrent with ℓ that is also concurrent with ℓ'. By the Pigeonhole Principle, one of the t different $\langle x \rangle$-orbits of lines concurrent with ℓ, which we name X, is also concurrent with at least $\lceil (\beta_0(x) - 1)/t \rceil$ fixed lines other than ℓ. If Y is the set of $\lceil (\beta_0(x) - 1)/t \rceil + 1$ lines that are all nonconcurrent, fixed by x, and incident with each line in X, then, by Lemma 2.2,

$$s \left\lceil \frac{\beta_0(x) - 1}{t} \right\rceil \leqslant t^2.$$

To finish the proof, we provide a lower bound on $\beta_0(x)$. Since $s+1$ is prime, by Lemma 3.1 we have

$$\beta_0(x) \equiv (t+1)(st+1) \pmod{s+1},$$

which equivalently implies that

$$\beta_0(x) \equiv -(t^2-1) \pmod{s+1}.$$

Thus, there exists some $k \in \mathbb{N}$ such that

$$\beta_0(x) = k(s+1) - (t^2-1).$$

If $k < t^2/(s+1)$, then

$$\beta_0(x) = k(s+1) - (t^2-1) < \frac{t^2}{s+1}(s+1) - (t^2-1) = 1,$$

which implies that $\beta_0(x) < 1$, a contradiction, since $\mathcal{Q}_x$ has type $(1')$. Thus $k \geqslant \left\lceil \frac{t^2}{s+1} \right\rceil$, and so

$$\left\lceil \frac{t^2}{s+1} \right\rceil (s+1) - (t^2-1) \leqslant \beta_0(x).$$

This means

$$s\left(\left\lceil \left\lceil \frac{t^2}{s+1} \right\rceil \cdot \frac{s+1}{t} \right\rceil - t \right) = s \left\lceil \frac{\left(\left\lceil \frac{t^2}{s+1} \right\rceil (s+1) - (t^2-1) \right) - 1}{t} \right\rceil$$

$$\leqslant s \left\lceil \frac{\beta_0(x) - 1}{t} \right\rceil$$

$$\leqslant t^2.$$

Simplifying, we have

$$s \left\lceil \left\lceil \frac{t^2}{s+1} \right\rceil \left(\frac{s+1}{t} \right) \right\rceil \leqslant t(s+t),$$

as desired. $\qquad \square$

5. CONSEQUENCES OF THE INEQUALITY

In this section, we present some consequences of Theorem 1.1. First, we have immediately Corollary 1.2, which says that a generalized quadrangle of order (s,t), where $s > t$, $s+1$ is prime, and

$$s \left\lceil \left\lceil \frac{t^2}{s+1} \right\rceil \left(\frac{s+1}{t} \right) \right\rceil > t(s+t),$$

is not point-transitive.

Proof of Corollary 1.2. Assume that $\mathcal{Q}$ has order (s,t), where $s > t > 1$ and $s+1$ is prime. If $\mathcal{Q}$ has an automorphism group G that is transitive on points and P is a point of $\mathcal{Q}$, then

$$|G| = |\mathcal{P}||G_P| = (s+1)(st+1)|G_P|.$$

Since the prime $(s+1)$ divides $|G|$, G must have an element of order $s+1$, which means s and t must satisfy the hypotheses of Theorem 1.1. The result follows. $\qquad \square$

We can also now prove Corollary 1.3.

Proof of Corollary 1.3. This follows immediately from point-line duality and Corollary 1.2. □

At first glance, the inequality

$$s\left\lceil\left\lceil\frac{t^2}{s+1}\right\rceil\left(\frac{s+1}{t}\right)\right\rceil \leqslant t(s+t)$$

does not seem like much of a restriction. However, as we will see, when s is much larger than t, there are often situations when the ceiling functions contained in the inequality make a drastic difference. Corollary 1.4 shows that one implication of Theorem 1.1 is that, if $s+1$ is prime and if there exists a natural number n such that

$$\frac{t^2}{n+1}+t \leqslant s+1 < \frac{t^2}{n},$$

then a generalized quadrangle of order (s,t) cannot have an automorphism of order $s+1$ and cannot be point-transitive.

Proof of Corollary 1.4. Assume that $s+1$ is prime and that

$$\frac{t^2}{n+1}+t \leqslant s+1 < \frac{t^2}{n}$$

for some natural number n. First, since

$$t < \frac{t^2}{n+1}+t \leqslant s+1,$$

$s \geqslant t$. If $s = t$, then $t^2/(n+1) \leqslant 1$, which implies that

$$s+1 < \frac{t^2}{n} = \left(\frac{t^2}{n+1}\right)\left(\frac{n+1}{n}\right) \leqslant 1+\frac{1}{n},$$

a contradiction. Hence $s > t$. On the other hand, since

$$\frac{t^2}{n+1} < \frac{t^2}{n+1}+t \leqslant s+1 < \frac{t^2}{n},$$

we have

$$n < \frac{t^2}{s+1} < n+1,$$

and so

$$\left\lceil\frac{t^2}{s+1}\right\rceil = n+1.$$

Moreover, since $t^2/(n+1)+t \leqslant s+1$

$$(n+1)(s+1) \geqslant t^2+(n+1)t,$$

and, since $t > 1$,

$$(n+1)s \geqslant t^2+(n+1)(t-1) > t^2.$$

Thus,

$$\begin{aligned}
s\left\lceil\left\lceil\frac{t^2}{s+1}\right\rceil\left(\frac{s+1}{t}\right)\right\rceil &= s\left\lceil(n+1)\frac{s+1}{t}\right\rceil \\
&\geqslant s\left\lceil\frac{t^2+(n+1)t}{t}\right\rceil \\
&= s(t+(n+1)) \\
&= ts+(n+1)s \\
&> ts+t^2 \\
&= t(s+t),
\end{aligned}$$

and, by Theorem 1.1 and Corollary 1.2, such a generalized quadrangle cannot have an automorphism of order $s + 1$ and cannot be point-transitive. ☐

One particular application of the inequality is Corollary 1.5, which states that, if $\mathcal{Q}$ is a generalized quadrangle of order $(q^2 - nq, q)$ and $q^2 - nq + 1$ is prime with $q > 2n$, then $\mathcal{Q}$ is not point-transitive. These conditions apply to numerous potential generalized quadrangles whose existence is not known, for instance orders $(12, 4)$, $(30, 6)$, $(42, 7)$, and $(72, 9)$; see Appendix A for many more instances.

Proof of Corollary 1.5. Let $\mathcal{Q}$ be a generalized quadrangle of order $(q^2 - nq, q)$, where $q > 2n$ and $q^2 - nq + 1$ is prime. In this instance,

$$\left\lceil \frac{q^2}{q^2 - nq + 1} \right\rceil = 2,$$

and

$$\left\lceil 2 \frac{q^2 - nq + 1}{q} \right\rceil = \left\lceil 2q - 2n + \frac{2}{q} \right\rceil = 2q - 2n + 1,$$

and so

$$\begin{aligned}
(q^2 - q) \left\lceil \left\lceil \frac{q^2}{q^2 - q + 1} \right\rceil \left(\frac{q^2 - q + 1}{q} \right) \right\rceil &= (q^2 - q)(2q - 2n + 1) \\
&= q\left((q - 1)(2q - 2n + 1)\right) \\
&> q \cdot q^2 \\
&> q\left((q^2 - nq) + q\right)
\end{aligned}$$

when $q > 2n$, and hence by Theorem 1.1 and Corollary 1.2, such a generalized quadrangle cannot have an automorphism of order $q^2 - nq + 1$ and cannot be point-transitive. ☐

It is unknown whether $q^2 - nq + 1$ is prime for infinitely many positive integer values of q for a fixed n. However, the following conjecture from number theory supports this conclusion.

CONJECTURE 5.1 ([9]). *Let $f(x) = a_d x^d + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients. The set $\{k \in \mathbb{Z} : f(k) \text{ is prime}\}$ is infinite if the following three conditions hold:*

(i) *$a_d = 1$,*
(ii) *f is irreducible over $\mathbb{Z}$,*
(iii) *The set of integers $f(\mathbb{Z}) = \{f(n) : n \in \mathbb{Z}\}$ has greatest common divisor* 1.

For $f(x) = x^2 - nx + 1$, it is plain to see that f satisfies conditions (i) and (ii) when $n \neq 2$, and $f(n) = 1$, showing (iii). The numerical evidence in Appendix A lends evidence that there could indeed be infinitely many such pairs where $(s, t) = (q^2 - nq, q)$ that satisfy $s + t \mid st(st + 1)$ where $s + 1$ is prime.

It is an interesting question as to whether generalized quadrangles of such orders actually exist. While the asymmetry of such examples is potential evidence against existence, combinatorial regularity also does not necessitate symmetry.

6. Automorphisms of a generalized quadrangle of order $(4, 12)$

This section is dedicated to analyzing the structure of the automorphism group of a generalized quadrangle of order $(4, 12)$, if one were to exist. Throughout this section, $\mathcal{Q}$ will be a generalized quadrangle of order $(4, 12)$ with point set $\mathcal{P}$, line set $\mathcal{L}$, and automorphism group G. As in the previous sections, for $x \in G$, the *type* of $\mathcal{Q}_x$ refers to its designation under Lemma 2.5.

LEMMA 6.1. *If p is a prime that divides $|G|$, then $p \leqslant 7$.*

Proof. Let p be a prime dividing $|G|$. By Lemma 3.13, $p \leqslant 13$. We know that no automorphism of order 13 exists by Corollary 1.3, and so we assume $p = 11$ and let x be an element of G of order 11. By Lemma 3.2, $\mathcal{Q}_x$ cannot be of type (0); by Lemma 3.3, $\mathcal{Q}_x$ cannot be of type (1) or type $(1')$; by Lemma 3.4, $\mathcal{Q}_x$ cannot be of type (2) or $(2')$; by Lemma 3.6, $\mathcal{Q}_x$ cannot be of type (3) or $(3')$; and, by Lemma 3.11, $\mathcal{Q}_x$ cannot be of type (4). Therefore, if p divides $|G|$, then $p \leqslant 7$. $\square$

LEMMA 6.2. *If $x \in G$ is an element of order 7, then $\alpha_0(x) = 0$.*

Proof. Let x be an element of G of order 7. By Lemma 3.3, $\mathcal{Q}_x$ cannot be of type (1) or of type $(1')$. By Lemma 3.4, $\mathcal{Q}_x$ cannot be of type (2) or of type $(2')$. By Lemma 3.6, $\mathcal{Q}_x$ cannot be of type (3) or of type $(3')$ By Lemma 3.11, $\mathcal{Q}_x$ cannot be of type (4). Therefore, $\mathcal{Q}_x$ is of type (0) and $\alpha_0(x) = 0$. $\square$

LEMMA 6.3. *A Sylow 7-subgroup of G has order at most 49.*

Proof. Let X be a Sylow 7-subgroup of G, and let $y \in X$. If y is not the identity and y fixes any point of $\mathcal{Q}$, then $y^{|y|/7}$ is an element of order 7 that fixes a point of $\mathcal{Q}$, a contradiction to Lemma 6.2. This implies that X acts semiregularly on $\mathcal{P}$, and so $|X|$ divides $|\mathcal{P}| = 245$. The result follows. $\square$

LEMMA 6.4. *If $h \in G$ is an element of order 5, then $\alpha_0(h) = 0$.*

Proof. Let h be an element of G of order 5. By Lemma 3.2, $\mathcal{Q}_h$ cannot be of type (0). By Lemma 3.3, $\mathcal{Q}_h$ cannot be of type (1). By Lemma 3.4, $\mathcal{Q}_h$ cannot be of type (2) or of type $(2')$. By Lemma 3.6, $\mathcal{Q}_h$ cannot be of type (3) or of type $(3')$. By Lemma 3.11, $\mathcal{Q}_h$ cannot be of type (4). Therefore, $\mathcal{Q}_h$ is of type $(1')$ and $\alpha_0(h) = 0$. $\square$

LEMMA 6.5. *A Sylow 5-subgroup of G has order at most 5.*

Proof. Let H be a Sylow 5-subgroup of G, and let $y \in H$. If y is not the identity and y fixes any point of $\mathcal{Q}$, then $y^{|y|/5}$ is an element of order 5 that fixes a point of $\mathcal{Q}$, a contradiction to Lemma 6.4. This implies that H acts semiregularly on $\mathcal{P}$, and so $|H|$ divides $|\mathcal{P}| = 245$. The result follows. $\square$

LEMMA 6.6. *If G is transitive on $\mathcal{P}$, then the action of G on $\mathcal{P}$ is not quasiprimitive, i.e. G must contain a nontrivial normal subgroup that is intransitive on $\mathcal{P}$.*

Proof. Assume that the action of G on $\mathcal{P}$ is quasiprimitive. By [27, Theorem 1], since $|\mathcal{P}|$ is not a prime power, G must have a nonabelian minimal normal subgroup $N = T^k$, where T is a nonabelian finite simple group and $k \in \mathbb{N}$, such that N is transitive on $\mathcal{P}$. Moreover, by Lemma 6.1, no prime greater than 7 divides $|N|$. Assume $k \geqslant 2$. Since the largest power of 5 to divide $|G|$ is 5, in this case $5 \nmid |T|$. However, since N is transitive on $\mathcal{P}$, 5 divides $|N|$, and so 5 divides $|T|$, a contradiction. Hence $N = T$ is a finite nonabelian simple group.

On the other hand, the only primes that can divide $|T|$ are $2, 3, 5, 7$. Moreover, 5 and 7 all must divide $|T|$, since T is transitive on $\mathcal{P}$, and the largest power of 5 dividing $|T|$ is 5 and the largest power of 7 dividing $|T|$ is 49. By [19, Theorem II], there is no such finite simple group. Hence the action of G on $\mathcal{P}$ cannot be quasiprimitive. $\square$

LEMMA 6.7. *If G is transitive on $\mathcal{P}$, then G contains an element of order 35.*

Proof. Assume that G is transitive on $\mathcal{P}$. It suffices to show that either the normalizer of a 5-subgroup contains an element of order 7 or the normalizer of a 7-subgroup contains an element of order 5, since, in either case, the normalizing element is forced to be in the centralizer of the p-subgroup.

Since G is transitive but not quasiprimitive on $\mathcal{P}$ by Lemma 6.6, G must contain an intransitive normal subgroup N. Let P be a Sylow p-subgroup of N for some prime p. By the Frattini Argument (see, for instance, [20, Theorem 1.13]), $G = N_G(P)N$. This means that $|G|$ divides $|N_G(P)| \cdot |N|$.

Since N is intransitive on $\mathcal{P}$, there are four possibilities:

  (i) there are 5 distinct N-orbits of size 49,
 (ii) there are 7 distinct N-orbits of size 35,
(iii) there are 35 distinct N-orbits of size 7, or
 (iv) there are 49 distinct N-orbits of size 5.

Consider first the case when there are 5 distinct N-orbits of size 49. Since N is transitive on a set of size 49, $49 \mid |N|$. Let P be a Sylow 7-subgroup of N, which has size 49. Since G is transitive on the five N-orbits, $5 \mid |G : N|$. Since G is not divisible by 25, this implies that $5 \nmid |N|$. However, since 5 divides $|G|$, $|G|$ divides $|N_G(P)| \cdot |N|$, and 5 does not divide $|N|$, we have that 5 divides $|N_G(P)|$, and so G contains an element of order 5 that normalizes (and hence centralizes) a Sylow 7-subgroup of G.

We proceed similarly in the remaining cases: if there are 7 distinct N-orbits of size 35, then 7 divides $|N_G(P)|$, where P is a Sylow 5-subgroup of N; if there are 35 distinct N-orbits of size 7, then 5 divides $|N_G(P)|$, where P is a Sylow 7-subgroup of N; and, finally, if there are 49 distinct N-orbits of size 5, then 7 divides $|N_G(P)|$, where P is a Sylow 5-subgroup of N. In any case, if G is transitive on $\mathcal{P}$, then G must contain an element of order 35, as desired. $\square$

We are now ready to prove Theorem 1.6.

Proof of Theorem 1.6. Let $\mathcal{Q}$ be a generalized quadrangle of order $(4, 12)$, and let $G = \operatorname{Aut}(\mathcal{Q})$. By Lemma 6.1, $13 \nmid |G|$, and so G cannot be transitive on lines.

Assume that G is transitive on points. By Lemma 6.7, G must contain an element h of order 35. Since $|h^5| = 7$, by Lemma 6.2, $\alpha_0(h) = 0$. Consider $\mathcal{P}_1(h)$, the set of points sent to distinct collinear points by h. The orbits of $\langle h \rangle$ have size 5, 7, or 35, and $\mathcal{P}_1(h)$ is made up of these orbits. However, since $|h^5| = 7$ and $|h^7| = 5$, both h^5 and h^7 are semiregular on $\mathcal{P}$ by Lemmas 6.2 and 6.4, and so no orbit of $\langle h \rangle$ can have size 5 or 7. Thus $\alpha_1(h) \equiv 0 \pmod{35}$.

On the other hand, by Benson's Lemma (Lemma 2.3), $\alpha_1(h) \equiv 1 \pmod{16}$. By the Chinese Remainder Theorem, this means that $\alpha_1(h) \equiv 385 \pmod{560}$. Since $\alpha_1(h) \leqslant |\mathcal{P}| = 245$, we reach a contradiction, and so G cannot be transitive on $\mathcal{P}$, as desired. $\square$

Finally, we remark that, while the techniques used in this section relied heavily on the exact values of s and t, the ideas used here should be applicable to other relatively small values of s and t.

APPENDIX A. CALCULATIONS

As t increases, there seems to be a steady increase in the proportion of feasible parameters (s, t) of generalized quadrangles that satisfy the hypotheses of Corollary 1.2 and hence cannot be point-transitive if they exist.

Now, we give tables of all possible orders (s, t) of generalized quadrangles with $t \leqslant 100$ that satisfy the hypotheses of Corollary 1.2. The tag $(***)$ denotes that this order (s, t) has the form $s = t^2 - nt$ where $s + 1$ is prime and $2n < t$.

(12, 4) ***	(312, 26)	(946, 44)	(826, 59)
(22, 6)	(442, 26) ***	(1276, 44) ***	(660, 60)
(30, 6) ***	(540, 27) ***	(1408, 44) ***	(672, 60)
(42, 7) ***	(378, 28)	(576, 45)	(1038, 60)
(28, 8)	(756, 28) ***	(630, 45)	(1740, 60)
(40, 8) ***	(270, 30)	(990, 45)	(2136, 60)
(36, 9)	(280, 30)	(1012, 46)	(2380, 60)
(72, 9) ***	(420, 30)	(456, 48)	(3540, 60) ***
(40, 10)	(232, 32)	(540, 48)	(1830, 61)
(60, 12)	(672, 32) ***	(1128, 48)	(1860, 62)
(66, 12)	(330, 33)	(1296, 48) ***	(2542, 62) ***
(78, 13)	(442, 34)	(1666, 49) ***	(3906, 63) ***
(156, 13) ***	(1122, 34) ***	(460, 50)	(576, 64)
(126, 14) ***	(280, 35)	(700, 50)	(768, 64)
(210, 15) ***	(490, 35)	(970, 50)	(976, 64)
(112, 16)	(700, 35) ***	(1200, 50)	(1216, 64)
(240, 16) ***	(396, 36)	(1450, 50) ***	(1600, 64)
(136, 17)	(408, 36)	(612, 51)	(2016, 64)
(96, 18)	(556, 36)	(2550, 51) ***	(760, 65)
(210, 18)	(612, 36)	(796, 52)	(910, 65)
(306, 18) ***	(630, 36)	(1300, 52)	(2080, 65)
(130, 20)	(852, 36)	(1326, 52)	(3510, 65) ***
(148, 20)	(456, 38)	(540, 54)	(1408, 66)
(180, 20)	(546, 39)	(918, 54)	(2112, 66)
(190, 20)	(1482, 39) ***	(936, 54)	(2346, 66)
(280, 20) ***	(616, 40)	(1566, 54) ***	(4422, 67) ***
(316, 20)	(760, 40)	(2376, 54) ***	(1666, 68)
(330, 20)	(820, 41)	(1870, 55) ***	(3060, 68) ***
(126, 21)	(546, 42)	(2970, 55) ***	(1380, 69)
(210, 21)	(732, 42)	(616, 56)	(2346, 69)
(420, 21) ***	(1162, 42)	(742, 56)	(910, 70)
(462, 22) ***	(1722, 42) ***	(856, 56)	(2380, 70)
(136, 24)	(430, 43)	(1008, 56)	(4830, 70) ***
(276, 24)	(316, 44)	(1288, 56)	(1096, 72)
(336, 24) ***	(616, 44)	(2296, 56) ***	(1656, 72)
(456, 24) ***	(676, 44)	(1596, 57)	(2520, 72)
(600, 25) ***	(682, 44)	(3306, 58) ***	(2556, 72)

(3432, 72)	(1092, 84)	(3060, 90)
(5112, 72) ***	(1276, 84)	(3186, 90)
(1776, 74)	(1582, 84)	(3690, 90)
(1050, 75)	(1596, 84)	(5580, 90) ***
(1800, 75)	(1876, 84)	(6210, 90) ***
(4200, 75) ***	(2268, 84)	(8010, 90) ***
(1596, 76)	(2296, 84)	(2002, 91)
(2052, 76)	(2436, 84)	(3796, 91)
(2850, 76)	(2856, 84)	(8190, 91) ***
(5700, 76) ***	(4200, 84) ***	(3082, 92)
(4642, 77)	(4326, 84)	(6256, 92) ***
(936, 78)	(4956, 84) ***	(2790, 93)
(1950, 78)	(6036, 84)	(1692, 94)
(2766, 78)	(6580, 84)	(4512, 96)
(6006, 78) ***	(990, 85)	(4560, 96)
(6162, 79) ***	(1360, 85)	(6112, 96)
(880, 80)	(3570, 85)	(4656, 97)
(1200, 80)	(3612, 86)	(1288, 98)
(1216, 80)	(4902, 86) ***	(3136, 98)
(1360, 80)	(2436, 87)	(4018, 98)
(1720, 80)	(1870, 88)	(2376, 99)
(2080, 80)	(3916, 89)	(2926, 99)
(2620, 80)	(1530, 90)	(3168, 99)
(2800, 80)	(1548, 90)	(4356, 99)
(3120, 80)	(1800, 90)	(5346, 99) ***
(3760, 80) ***	(1860, 90)	(1900, 100) ***
(4240, 80) ***	(2010, 90)	(4950, 100)
(4240, 80) ***	(2016, 90)	(9900, 100) **
(4720, 80) ***	(2178, 90)	
(6480, 81) ***	(2250, 90)	

References

[1] Mohammad Adm, Ryan Bergen, Ferdinand Ihringer, Sam Jaques, Karen Meagher, Alison Purdy, and Boting Yang, *Ovoids of generalized quadrangles of order $(q, q^2 - q)$ and Delsarte cocliques in related strongly regular graphs*, J. Combin. Des. **26** (2018), no. 5, 249–263.

[2] John Bamberg, Michael Giudici, Joy Morris, Gordon F. Royle, and Pablo Spiga, *Generalised quadrangles with a group of automorphisms acting primitively on points and lines*, J. Combin. Theory Ser. A **119** (2012), no. 7, 1479–1499.

[3] John Bamberg, Stephen Peter Glasby, Tomasz Popiel, and Cheryl E. Praeger, *Generalized quadrangles and transitive pseudo-hyperovals*, J. Combin. Des. **24** (2016), no. 4, 151–164.

[4] John Bamberg, Cai Heng Li, and Eric Swartz, *A classification of finite antiflag-transitive generalized quadrangles*, Trans. Amer. Math. Soc. **370** (2018), no. 3, 1551–1601.

[5] _____, *A classification of finite locally 2-transitive generalized quadrangles*, https://arxiv.org/abs/1903.07442, 2019.

[6] John Bamberg, Tomasz Popiel, and Cheryl E. Praeger, *Point-primitive, line-transitive generalised quadrangles of holomorph type*, J. Group Theory **20** (2017), no. 2, 269–287.

[7] _____, *Simple groups, product actions, and generalized quadrangles*, Nagoya Math. J. **234** (2019), 87–126.

[8] Clark T. Benson, *On the structure of generalized quadrangles*, J. Algebra **15** (1970), 443–454.

[9] Victor Bouniakowsky, *Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la composition des entiers en facteurs*, Sc. Math. Phys. **6** (1857), 305–329.

[10] Peter J. Cameron, *Permutation groups*, London Mathematical Society Student Texts, vol. 45, Cambridge University Press, Cambridge, 1999.

[11] Stefaan De Winter, Ellen Kamischke, and Zeying Wang, *Automorphisms of strongly regular graphs with applications to partial difference sets*, Des. Codes Cryptogr. **79** (2016), no. 3, 471–485.

[12] Stefaan De Winter and Koen Thas, *Generalized quadrangles with an abelian Singer group*, Des. Codes Cryptogr. **39** (2006), no. 1, 81–87.

[13] _____, *The automorphism group of Payne derived generalized quadrangles*, Adv. Math. **214** (2007), no. 1, 146–156.

[14] _____, *Generalized quadrangles admitting a sharply transitive Heisenberg group*, Des. Codes Cryptogr. **47** (2008), no. 1-3, 237–242.

[15] Alexander L. Gavrilyuk and Aleksander A. Makhnev, *On automorphisms of a distance-regular graph with intersection array $\{56, 45, 1; 1, 9, 56\}$*, Dokl. Akad. Nauk **432** (2010), no. 5, 583–587.

[16] Dina Ghinelli, *Regular groups on generalized quadrangles and nonabelian difference sets with multiplier -1*, Geom. Dedicata **41** (1992), no. 2, 165–174.

[17] Nick Gill, *Transitive projective planes*, Adv. Geom. **7** (2007), no. 4, 475–528.

[18] _____, *Transitive projective planes and insoluble groups*, Trans. Amer. Math. Soc. **368** (2016), no. 5, 3017–3057.

[19] Bertram Huppert and Wolfgang Lempken, *Simple groups of order divisible by at most four primes*, Proc. F. Scorina Gomel State Univ. **16** (2000), no. 3, 64–75.

[20] I. Martin Isaacs, *Finite group theory*, Graduate Studies in Mathematics, vol. 92, American Mathematical Society, Providence, RI, 2008.

[21] Martin Mačaj and Jozef Širáň, *Search for properties of the missing Moore graph*, Linear Algebra Appl. **432** (2010), no. 9, 2381–2398.

[22] Alexander A. Makhnev, Jr. and Alexander A. Makhnev, *Ovoids and bipartite subgraphs in generalized quadrangles*, Mat. Zametki **73** (2003), no. 6, 878–885.

[23] Christine M. O'Keefe and Tim Penttila, *Automorphism groups of generalized quadrangles via an unusual action of $P\Gamma L(2, 2^h)$*, European J. Combin. **23** (2002), no. 2, 213–232.

[24] Stanley E. Payne, *An inequality for generalized quadrangles*, Proc. Amer. Math. Soc. **71** (1978), no. 1, 147–152.

[25] _____, *The fundamental theorem of q-clan geometry*, Des. Codes Cryptogr. **8** (1996), no. 1-2, 181–202, Special issue dedicated to Hanfried Lenz.

[26] Stanley E. Payne and Joseph A. Thas, *Finite generalized quadrangles*, second ed., EMS Series of Lectures in Mathematics, European Mathematical Society (EMS), Zürich, 2009.

[27] Cheryl E. Praeger, *An O'Nan–Scott theorem for finite quasiprimitive permutation groups and an application to 2-arc transitive graphs*, J. London Math. Soc. (2) **47** (1993), no. 2, 227–239.

[28] Eric Swartz, *On generalized quadrangles with a point regular group of automorphisms*, European J. Combin. **79** (2019), 60–74.

[29] Jacques Tits, *Sur la trialité et certains groupes qui s'en déduisent*, Inst. Hautes Etudes Sci. Publ. Math. **2** (1959), 14–60.

[30] Satoshi Yoshiara, *A generalized quadrangle with an automorphism group acting regularly on the points*, European J. Combin. **28** (2007), no. 2, 653–664.

Santana F. Afton, Department of Mathematics, College of William & Mary, P.O. Box 8795, Williamsburg, VA 23187-8795, USA
School of Mathematics, Georgia Institute of Technology, 686 Cherry Street, Atlanta, GA 30332-0160, USA
E-mail : `santana.afton@gatech.edu`

Eric Swartz, Department of Mathematics, College of William & Mary, P.O. Box 8795, Williamsburg, VA 23187-8795, USA
E-mail : `easwartz@wm.edu`