Reconstructing simple group actions

William M. Kantor and and Tim Penttila***

Abstract. Let G be a simple primitive subgroup of S_n, specified in terms of a set of generating permutations. If $|G| \geq n^5$, efficient algorithms are presented that find "the most natural permutation representation" of G. For example, if G is a classical group then we find a suitable projective space underlying G. A number of related questions are considered. Our notion of "efficiency" takes into account many existing notions, ranging from practical to theoretical ones.

1991 Mathematics Subject Classification: 20B40, 20D08, 20G40, 51N30.

1. Introduction

During the algorithmic study of subgroups of S_n, one often comes across a subgroup G known to be simple [Lu2;Neu;Ka3-5;Ma;Mo]. It is then natural to ask that the given permutation domain be replaced by another one closely related to the structure of G, such as an r–element set on which an alternating group A_r acts. Such a replacement result was, indeed, obtained in [Ka3,4] as an essential ingredient of an algorithm for finding Sylow subgroups in polynomial time (compare [Ma;Mo;KLM]); but this result suffered from the fact that the replacement algorithm relied on additional permutation domains of size $\Theta(n^2)$. The purpose of this note is to provide procedures that are more efficient, avoiding such increased space usage while attempting to limit the use of potentially "costly" algorithms. Specifically, when given a simple primitive subgroup $G \ncong M_{23}, M_{24}$ of S_n of order $\geq n^5$, we will find a set of one of the following sorts upon which G acts faithfully in the "natural" manner:

(i) *An r–set, if $G \cong A_r$*; or

(ii) *The set of 1–spaces of a vector space suitably related to the definition of G, if G is a classical group.*

The assumption that $|G| \geq n^5$ eliminates all exceptional simple groups of Lie type, all but the stated two sporadic simple groups, and all but the most familiar types of primitive permutation representations of the alternating or classical groups. It is hoped that groups satisfying $|G| < n^5$ can be viewed as "very small"

* Research supported in part by the NSF and NSA.

** Research supported in part by the NSF while visiting the University of Oregon.

relative to n, and hence manageable in more direct manners (however, see Section 9).

Most of the arguments used here are geometric and fairly elementary. We do not claim that the algorithms presented are in any sense optimal, or the last word along these lines. In Section 8 we will also indicate how one can go much further: constructing a vector space, basis, form and matrices [Ka3]. Throughout, we have dealt only with deterministic algorithms.

2. Statement of results

We assume that groups are always input using a set of generating permutations. Let G be a subgroup of $S_n = \mathrm{Sym}(\Omega)$.

Hypothesis 2.1. *The action of the simple primitive group G is permutation isomorphic to one of the following*:

(a) *The action on the set of all k–sets of an r–set, when $G \cong A_r$, $r > 9$;*

(b) *The action on the set of all partitions of an r–set into blocks of size k, when $G \cong A_r$, $r > 9$; or*

(c) *The action on an orbit of k–spaces of the vector space V involved in the definition of G when G is a simple classical group; and either $G \cong \mathrm{PSL}(V)$ with $\dim V \geq 3$, or $G \not\cong \mathrm{PSL}(V)$ and V has Witt index > 1.*

We refer to [Di;Ta] for the standard terminology and basic properties concerning the finite classical groups, and to [Ta, Ch. 1;Wi] for the elementary notions concerning permutation groups, especially primitivity and block systems. The justification for considering such a small class of permutation representations in Hypothesis 2.1 is the following observation, which is based on the classification of finite simple groups:

Proposition 2.2. *Let G be a simple primitive subgroup of S_n.*

(i) *If $|G| \geq n^5$ then either* Hypothesis 2.1 *holds or G is a Mathieu group M_n with $n = 23$ or 24.*

(ii) *If G is an alternating group A_r and if $|G| \geq n^3$, then* Hypothesis 2.1 *holds.*

(iii) *If G is a classical group and if $|G| \geq 4n^3$, then either* Hypothesis 2.1(c) *holds or $G \cong \mathrm{PSU}(3,7)$ and $n = 50$; moreover, if $G \not\cong \mathrm{PSL}(d,q)$ for all d, q, then the subspaces referred to in* Hypothesis 2.1(c) *are totally isotropic, totally singular or nonsingular.*

Some care is needed here. For example $\mathrm{PSp}(d,q) \cong \mathrm{P\Omega}(d+1,q)$ when q is even, and for these groups the bound in (iii) allows Ω to be an orbit of nonsingular hyperplanes of the orthogonal space, but there is no way to view this permutation representation in terms of an orbit of subspaces in the symplectic space. Also, instead of $\mathrm{PSp}(4,3)$ we usually consider the isomorphic groups $\mathrm{PSU}(4,2)$ or

$P\Omega^-(6,2)$, where more instances of Hypothesis 2.1 occur; but the various views of this group are allowed in the proposition.

Proof. (Compare [Ka3], which uses the bound $|G| > n^8$ based on [Ka1] and [LaS] instead of bounds in [Li] and [LiS].) When G is an alternating group, bounds on the orders of subgroups [PS] yield (ii). [Maz] takes care of the sporadic groups. In view of the classification of finite simple groups, it remains only to consider the groups of Lie type.

Bounds on the degrees of permutation representations of exceptional groups of Lie type are given in [LiS]. Those results imply that the minimal degree of a faithful permutation representation occurs for the permutation representation determined by some parabolic subgroup. It is then easy to check that the condition $|G| \geq n^5$ never holds (compare Section 9 below).

Suppose that G is a classical group with associated vector space V. If the stabilizer G_x of a point x of Ω is reducible on V, then Hypothesis 2.1 holds, and it is easy to see that the associated subspaces behave as in (iii). If G_x is irreducible then an upper bound on its order is given in [Li] (compare [KlLi]). A calculation shows that the condition $|G| \geq 4n^3$ does not hold except in the single instance mentioned in (iii). However, it should be noted that [Li] only gives the *largest* irreducible subgroup. One must check the proof in [Li] in order to see that, in those cases where a subgroup of index $< |G|^{1/3}$ is listed, there is no slightly smaller subgroup satisfying this bound. Moreover, when G is $\Omega(7,q)$ the bounds in [Li] are inadequate for our purposes, and it is necessary to go through the derivation of those bounds in order to check that no example arises (compare [Kl]). □

Remark. If the assumption $|G| \geq 4n^3$ in (iii) is weakened to $|G| \geq n^3$, then the only additional pairs (G, G_x) are as follows: $(\mathrm{PSU}(6,2), \mathrm{PSU}(4,3)\cdot 2)$, and $(P\Omega(7,q), G_2(q))$ with q odd. Incidentally, the cases in which G is $\mathrm{PSL}(4,q)$ or $\mathrm{PSU}(4,q)$ and G_x is the normalizer of $\mathrm{PSp}(4,q)$ also occur here, but they really occur in the context of other vector spaces, namely, within the framework of $(P\Omega^{\pm}(6,q), \mathrm{PO}(5,q))$; the same is true for $(P\Omega^-(6,2) \cong \mathrm{PSp}(4,3), 2^4A_5)$. See the additional remarks following Theorem 2.3.

Throughout the remainder of this paper we will assume that Hypothesis 2.1 holds. We have framed our treatment so as to apply *even if G is not as large as required in the preceding Proposition*; only rarely does this lead to any additional complications. On the other hand, the simple classical groups of Witt index 1 have been excluded since these are standard and elementary 2–transitive groups; while for $r \leq 9$, A_r is even easier to handle.

For purposes of our main result (Theorem 2.3), we will *assume that procedures* (or oracles) *are available for the following* "**basic**" *types of problems*:

(B1) Find the orbits of a group on a given (small) set; moreover, find an element taking one point to another in the same orbit.

(B2) Find $|G|$. Test whether or not a given permutation belongs to G.

(B3) Find all minimal block systems of a transitive group; given a block of a transitive group, find the block system it determines. (Of course, procedures for both of these may have to be iterated a number of times in order to replace a given transitive action by a primitive one; but this number will always be ≤ 3 in our procedures.)

(B4) Find the pointwise stabilizer of several objects (at most 5 points or blocks, though usually at most 3). This requires some clarification. First, finding a pointwise stabilizer of the form $H_{x_1 \ldots x_j}$ will presuppose that the stabilizers $H_{x_1 \ldots x_i}$ have been found at the same time for $i = 1, \ldots, j$; here H denotes a subgroup of G that has already been constructed, and $j \leq 5$ for the situations we will encounter. Second, if x and y are points in any current permutation domain for G, then we also assume that we have available an element of G_x moving y to any given point in y^{G_x} (so we will have a set of representatives of the cosets of G_{xy} in G_x).

(B5) Pass to a new permutation representation of G whose degree usually is less than that of G and in all cases is never much larger than that of G—in particular, never larger than the size of the target set we seek (see the remarks after the statement of the following theorem). Finding such a new permutation representation is accomplished by finding a subgroup H of G such that $|G : H|$ is small (at most the size of the permutation domain), and then finding the action of G on the corresponding set G/H of right cosets.

Procedures for such problems are (special cases of) standard tools in many existing approaches to permutation group algorithms: practical (CAYLEY/Magma [Ca;BC]; GAP [Sch]), deterministic polynomial time [FHL;Lu2], Monte Carlo polynomial time [CF] and parallel (complexity class NC) [LM;Lu1;Lu3;KLM]. However, no procedure is known for **(B5)** in the context of "nearly linear time" computation, so that only a few of our results apply to that model of computation (cf. [Mo]).

In addition to **(B1-5)** we presuppose various other simple procedures, such as working with subsets of our permutation domain and factoring the order of a group into primes.

In Section 6 we will prove our main result:

Theorem 2.3. *There is an algorithm* NATURAL_ACTION *using only procedures for the above "***basic***" problems which, when given $G \leq S_n$ as in* Hypothesis 2.1, *outputs a new set Π on which G acts either as the full alternating group, or as it does on the set of all 1–spaces of a vector space underlying G if G is a classical group. Moreover, on any input,* NATURAL_ACTION *uses at most* 40 *calls to such procedures; no procedure is called for a set of size $> |\Pi|$.*

In most situations, $|\Pi|$ is at most n; and it is never much larger than n. The boundedness of the number of calls within NATURAL_ACTION seems to be different from other algorithms in print for the same sorts of problems [BKL; Ka3; BLS]. Note, in particular, that not even normal closures or derived groups are used in the algorithm in the theorem. Furthermore, we do not reconstruct recursively;

for example, we pass directly from the set of k–sets of an r–set to the elements of the r–set, rather than passing to the set of $(k-1)$–sets (see Section 7 for alternative approaches that do proceed recursively in some cases). Of course, the standard procedures for some of the problems **(B1-5)** are themselves recursive. Moreover, a significant amount of computation is needed to produce the new permutation action of G on Π (note that this action is, in general, intransitive: there can be as many as three orbits). On the one hand, when new permutation representations are produced for G or subgroups of G, these are *always* of degree at most the size of the target domain Π; on the other hand, cosets of stabilizers are needed, and hence so are tests to distinguish cosets. We have chosen to view these tests as all lumped together (as one big test **(B5)**) each time a new permutation representation is produced.

Theorem 2.3 mentions "a vector space underlying V". This may be a deceptive phrase. There may be vector spaces such that a given group can be considered in different ways as a classical group defined on each of them, and *each such vector space can be thought of as "underlying" G*; the given permutation representation will not indicate which of these vector spaces is desired in a given context. The most familiar instance of this ambiguity occurs when G is $\mathrm{PSL}(d,q) \cong \mathrm{PSL}(V)$ with $d > 2$, in which case there is no "significant" difference between the projective space underlying V and that underlying its dual space V^*. (See Section 8(B) for a brief discussion of the passage from one of these permutation representations to the other.) If G is $\mathrm{PSU}(4,q) \cong \mathrm{P}\Omega^-(6,q)$, or $\mathrm{PSp}(4,q) \cong \mathrm{P}\Omega(5,q)$ with q odd, then we produce whichever incarnation of this group seems to arise most naturally from the given permutation representation (see Remark 5.1 in order to pass between two such equally "natural" permutation representations of G). The case $\mathrm{PSL}(4,q) \cong \mathrm{P}\Omega^+(6,q)$ is handled similarly. When $G \cong \mathrm{P}\Omega^+(8,q)$ there is no readily discernible difference between the vector space defining G and its 8–dimensional half-spin modules, since each of these spaces comes equipped with a quadratic form preserved projectively by G; and in fact a triality automorphism of G transitively permutes this set of three vector spaces. Perhaps the most significant of these ambiguities arises when $G \cong \mathrm{P}\Omega(2m+1,q) \cong \mathrm{PSp}(2m,q)$ with q even, but here we always reconstruct the symplectic space, which is both smaller and "more natural".

Sections 3-5 present algorithms for various possibilities allowed by Hypothesis 2.1. Section 6 glues these together. Throughout the paper, especially in Section 7, we have indicated alternative algorithms. Section 9 contains remarks about other simple groups. Section 8 indicates further aspects of "linear algebra" associated with the Hypothesis: reducing permutation group computations to linear algebra ones. Here we must be willing to increase the size of the set Ω, since the underlying vector space always is slightly larger than Ω. Moreover, we use recursion in order to introduce coordinates: a given point is labeled using what can be almost $\log n$ field elements. We also reconstruct all elements of "the" field. Nevertheless, the introduction of coordinates and linear transformations seems reasonably efficient, and is certainly straightforward. Incidentally, our algorithms and proofs were de-

vised in terms of simple-minded pictures of various situations, and we urge readers to draw while reading.

The following procedure gives an indication of the general methodology in the case of classical groups and provides a rough flow chart. In Section 6 we will prove that this procedure is correct. The end of the present section contains notation and terminology appearing in this algorithm or in later ones.

NATURAL_ACTION

Input: A simple primitive group $G \leq \mathrm{Sym}(\Omega)$ of known order satisfying Hypothesis 2.1.

Output: A set and an action of G as required in Theorem 2.3.

Call ALT_ORDER. If $G \cong A_r$ for some r, call ALT1 and then ALT2.

Let p be the prime contributing the largest prime power to $|G|$, except when $|G| = |\mathrm{PSU}(4,2)|$ and $n \neq 40$, in which case let $p = 2$. (Then p is the characteristic of G [Ar].)

If $p|n$ call CLASSICAL_NS (Section 5), producing a new set Ω'. (Here Ω is a G–orbit of nonsingular subspaces, and CLASSICAL_NS produces the set Ω' of isotropic or singular points of an underlying vector space.)

Now $p \not| n$. Call PSL_ORDER (Section 4). If $G \cong \mathrm{PSL}(d,q)$ for some d, q, call PSL (Section 4).

Find all orbits $\Delta(X)$ of G_X such that $|\Delta(X)|_{p'}$ is minimal subject to not being 1. Choose the largest such $\Delta(X)$.

Find all maximal block systems $\overline{\Delta}(X)$ of $G_X^{\Delta(X)}$ of p'–length.

Suppose that G has rank 3. If $n = (q^4+1)(q^3+1)(q^2+1)(q+1)$, use Ω^+_MAX (Section 5) to find a new set Ω'. If $n = (q^3+1)(q^2+1)$, use CLASSICAL_TS (Section 5) to find a new set Ω'. Otherwise, let $\Omega' = \Omega$.

Find a new set Ω' by using CLASSICAL_TS if $G_X^{\overline{\Delta}(X)}$ is 2–transitive and Ω^+_MAX otherwise.

Replace Ω by Ω' and call PROJECTIVE_SPACE (Section 6; this finds all remaining points of the underlying projective space if G is an orthogonal or unitary group.) $\diamondsuit$

Conventions: Throughout all of our algorithms we will tend to use notation suggestive of the nature of the "points" being permuted. For example, elements of Ω will be denoted by capital letters, since they frequently "are" subsets or subspaces. Similarly, when proving correctness (or making remarks within algorithms) we will tend to view the objects produced as actually *being inside* the underlying r–set or vector space. In other words, whereas we will have a permutation representation of G that is only permutation isomorphic to a familiar one, we will tend to identify these representations. Nevertheless, it is essential to distinguish the two permutation representations to some extent: some subspaces implicit in an algorithm may not have been reconstructed in the algorithm. Consequently, we will have to refer to corresponding features of the two permutation representations, leading to a corresponding overuse of terms such as "corresponding".

Terminology: If H is a group acting on a set T, then H^T denotes the induced action. If the action is transitive, we will consider block systems. A block system is *minimal* if it is nontrivial and each block contains no nontrivial block; it is *maximal* if the induced permutation representation of H is primitive. Whenever $U \subseteq T$ let H_U denote the set-stabilizer of U; as indicated in the preceding paragraph, we will be viewing subsets of some set other than Ω as the objects being permuted, and we will want to be able to consider both actions simultaneously.

If $G > H$ then G/H denotes the set of right cosets of H in G, which we always view as coming equipped with the usual permutation representation of G on this set.

If k is an integer and p is a prime, then k_p denotes the largest power of p dividing k, and $k_{p'} = k/k_p$.

Suborbits: When G is transitive, we will need to consider orbits of G_X on Ω for $X \in \Omega$ (the "suborbits" of G); the number of such orbits is the *rank* of G. Given an orbit $\Delta(X)$ of one stabilizer G_X, an orbit $\Delta(Y)$ of any other stabilizer G_Y is *always assumed to be obtained as* $\Delta(Y) = \Delta(X)^g$, where $X^g = Y$. This amounts to being given a (directed) graph on which G acts edge-transitively. However, once G_X is in hand, there may be no need to store the entire set orbit $\Delta(X)$, since it can specified by means of a single one of its members (i.e., $\Delta(X) = Y^{G_X}$ if $Y \in \Delta(X)$). Frequently, an element g such that $X^g = Y$ can be used to translate questions about $\Delta(Y)$ back to $\Delta(X)$ without dealing directly with $\Delta(Y)$. Note, however, that such a simple-minded method may not work if we need to consider sets such as $\Delta(X) \cap \Delta(Y)$. Similarly, when we consider a block system $\overline{\Delta}(X)$ for $G_X^{\Delta(X)}$, we can specify it either using one block or the stabilizer in G_X of a block; and the above element g again can be used to translate suitable questions about $\overline{\Delta}(Y)$ back to $\overline{\Delta}(X)$.

We write $\Delta^+(X) = \Delta(X) \cup \{X\}$.

3. Alternating groups

We begin with an arithmetic procedure:

ALT_ORDER

Input: A group G as in Hypothesis 2.1.

Output: Whether or not G is isomorphic to an alternating group; and if it is, the integer r such that $G \cong A_r$.

Find $|G|_2 = 2^{k-1}$. Test whether $|G| = r!/2$ for $9 < r = k+1, \ldots, 2k$. If it is not then G is not an alternating group, otherwise $G \cong A_r$. $\diamondsuit$

Proof of correctness of ALT_ORDER. If $m = [\log_2 r]$ then $(r!)_2 = \Sigma_{i=1}^m [r/2^i] < r\Sigma_{i=1}^\infty 1/2^i = r$ and $(r!)_2 \geq \Sigma_{i=1}^m (r-(2^i-1)/2^i) = r+1-(r+1)2^{-m}-m \geq r-m-1$. Thus, if $G \cong A_r$ then $k = |G|_2 + 1$ is between $r-1$ and $r - \log_2 r - 1$, and the indicated procedure finds r.

Suppose that the procedure determines that $|G| = r!/2$ for some r. By [Ar], G is isomorphic to A_r or $\mathrm{PSL}(3,4)$. If $|G| = |\mathrm{PSL}(3,4)| = |A_8|$ then $G \ncong A_8$ by Hypothesis 2.1(a,b), and the procedure correctly decides that G is not an alternating group. □

ALT1

Input: $G \leq \mathrm{Sym}(\Omega)$ permutation isomorphic to the action of A_r, $r > 9$, on the set of all subsets of some fixed size of the r–set.

Output: An r–set an action of G on that set as the alternating group.

If G is imprimitive, replace Ω by a nontrivial block system and call ALT2.
Find k such that $k+1$ is the rank of G and $|\Omega| = \binom{r}{k}$.
If $k = 1$ then output Ω.
Let $X \in \Omega$. Let $\Delta(X)$ be an orbit of G_X on Ω of length $k(r-k)$.
Find all minimal block systems of $G^{\Delta(X)}$ (there are two of them), and let $\overline{\Delta}(X)$ be the one having k blocks. Let X' and Y be distinct elements of the same member of $\overline{\Delta}(X)$, and let $Y' \in \Delta(X') \cap \Delta(Y) - \Delta(X)$.
Output $G/\langle G_{XY}, G_{X'Y'}\rangle$. ♢

Proof of correctness of ALT1. If Ω consists of all k–sets of Ω then we may assume that $k \leq r/2$. Our permutation representation is imprimitive if and only if $k = r/2$, in which case there is a unique nontrivial block system, and G acts on it as it does on the set of partitions into two blocks of size k. Hence, ALT2 can be used in this case. From now on we may assume that $r > 2k$. We may also assume that $k > 1$.

If $Y \in \Omega$ then $|Y^{G_X}| = \binom{k}{i}\binom{r-k}{k-i}$ where $i = |X \cap Y|$. When $1 < i < k-1$, the first factor is at least $k(k-1)/2$ and the second factor is at least $(r-k)(r-k-1)/2$, so no such orbit has length $k(r-k)$. If $i = 0$, then $|Y^{G_X}| = (r-k)!/(r-2k)!k! \neq k(r-k)$ (recall that $r \neq 7$). If $i = 1$ then $|Y^{G_X}| = k(r-k)!/(r-2k+1)!(k-1)! > k(r-k)$ (since $r > 2k \geq 4$). If $i = k-1$ then $|Y^{G_X}| = k(r-k)$. This shows that $\Delta(X)$ exists as required in the algorithm, and corresponds to $i = k-1$.

Moreover, in this case G_X is imprimitive on Y^{G_X}: if V denotes an r–set on which G acts as the full alternating group, then the block systems for $G_X^{\Delta(X)}$ correspond to fixing a member of the k–set X or of the $(r-k)$–set $V - X$. These block systems have sizes k and $r-k$, respectively.

Let $Z = X \cap Y$ (of size $k-1$), $\{x\} = X - Z$ and $\{y\} = Y - Z$. Then the member of $\overline{\Delta}(X)$ containing Y consists of the elements of $\Omega - \{X\}$ containing Z. In particular, $X' \supset Z$ and $Y' \not\supseteq Z$. If $\{x'\} = X' - Z$, it follows that $x' \in Y'$ as $|X' \cap Y'| = k-1$; similarly $y \in Y'$. Then $Y' \subset X' \cup \{y\}$ implies that $Y' = (Z - \{u\}) \cup \{x', y\}$ for some $u \in Z$, so that $X' - Y' = \{u\}$ and $Z' := X' \cap Y'$ is $(Z \cup \{x'\}) - \{u\} = X' - \{u\}$. Note that $\{y\} = Y' - X'$ since $X' \neq Y$.

Now $G_{XY} = (G_y)_{xZ}$ and $G_{X'Y'} = (G_y)_{uZ'}$, where $x \notin Z \cup Z'$ and $u \in Z - Z'$. Thus, $\langle G_{XY}, G_{X'Y'}\rangle = G_y$, and it is clear that $|G/\langle G_{XY}, G_{X'Y'}\rangle| = r < \binom{r}{k} = n$. □

We now turn to an alternating group A_r acting on the set of partitions of an r–set into blocks of size k. It would, perhaps, be desirable to reconstruct the r–set directly—and we do so when $r = 2k$, which is comforting in view of the fact

that ALT1 calls ALT2 in the case of A_r acting on $r/2$–sets. However, in general we merely output the action of A_r on k–sets, after which ALT1 can be used to reconstruct the underlying r–set, as is done in NATURAL_ACTION in Section 2.

ALT2

Input: $G \leq \mathrm{Sym}(\Omega)$ permutation isomorphic to the action of A_r, $r > 9$, on the set of all partitions of an r–set into blocks all of the same size.

Output: An r–set and an action of G on that set as the alternating group.

Let $X \in \Omega$. Let $\Delta(X)$ be the shortest G_X–orbit on $\Omega - \{X\}$.

Let $Y \in \Delta(X)$.

Find $\Delta(X) \cap \Delta(Y)$. Let $k = (|\Delta(X) \cap \Delta(Y)| + 2)/2$. Find s such that $|\Delta(X)| = \binom{s}{2}k^2/\varepsilon$, where ε is 1 if $k > 2$ and 2 otherwise.

Let $Z \in \Delta(X) \cap \Delta(Y)$.

Let $H := \langle G_{XY}, G_{XZ}, G_{YZ} \rangle$ if $k > 2$; let $H := \langle G_{XY}, g_1, g_2 \rangle$ if $k = 2$, where $g_1 \in G_X$ interchanges Y and Z and $g_2 \in G_Y$ interchanges X and Z.

If $s = 2$, use **(B5)** to find and output G/H.

If $s = 3$, find G/H using **(B5)**. Find the smallest maximal block system Ω' of G on G/H. Output Ω'.

Let W be in an $H_X^{\Delta(X)-\{Y\}}$–orbit that is also a $G_{XY}^{\Delta(X)-\{Y\}}$–orbit.

Let $g \in G_X$ with $Y^g = W$. Let $I := H^g$.

Let $J := \langle I_{XY}, I_{XZ}, I_{YZ} \rangle$ if $k > 2$; let $J := \langle I_{XY}, i_1, i_2 \rangle$ if $k = 2$, where $i_1 \in I_X$ interchanges Y and Z and $i_2 \in I_Y$ interchanges X and Z.

Find G/J using **(B5)**. Find the smallest maximal block system Ω' of G on G/J. Output Ω'. $\diamondsuit$

Proof of correctness of ALT2. We begin by identifying $\Delta(X)$:

Lemma 3.1. $\Delta(X) = \Big\{ Y \in \Omega \;\Big|\; Y = (X - \{A, B\}) \cup \{A', B'\}$ *where* $A' = (A - \{a\}) \cup \{b\}, B' = (B - \{b\}) \cup \{a\}$ *for some* $a \in A \in X, b \in B \in X \Big\}$.

Proof. Note that the G_X–orbit described in the lemma has length $\binom{s}{2}k^2/\varepsilon$, where ε is defined in the algorithm. Consider any $Y \in \Omega - \{X\}$, and assume that exactly i blocks of X are not blocks of Y, so $i \geq 2$; let $A(1), \ldots, A(i)$ denote these blocks of X. Then Y induces a partition $Y(j)$ on $A(j)$ having at least two parts.

If $k = 2$ then $|Y^{G_X}| \geq \binom{s}{i}(2i - 2)$. If $i = 2$ the lemma is clear. Let $i \geq 3$, so that $|Y^{G_X}| > s(s-1) = \binom{s}{2}2^2/2$ since $s \geq 5$, unless i is s. Note that $X \cup Y$ produces a bivalent graph on $r = 2s$ vertices. If there is a cycle of length > 4 then $|Y^{G_X}| \geq (2s-2)(2s-4) > s(s-1)$. Otherwise, s is even and $|Y^{G_X}| \geq (2s-2)(2s-8) > s(s-1)$. We may now assume that $k \geq 3$.

Suppose that $Y(1)$ consists of k singletons. Then k members of Y meet $A(1)$ (so that $i \geq k$); each of them meets some other $A(j)$, and the intersection has at least k images under $\mathrm{Sym}(A(j))$. Thus, we obtain at least k^k members of Y^{G_X}

using elements of G_X fixing each of the $A(j)$'s. We can fix X, Y and all members of $A(1)$ while moving the remaining $A(j)$'s to $\binom{s-1}{i-1}$ different $i-1$–subsets of X. Thus, $|Y^{G_X}| \geq \binom{s-1}{i-1}k^k$. Since $r = sk > 9$ and $s \geq i \geq k \geq 3$, it is easy to check that $|Y^{G_X}| > \binom{s}{2}k^2$, as required. (N.B.—When $r = 9$ and $s = k = 3$, the lemma no longer holds.)

Now

$$|Y^{G_X}| \geq \binom{s}{i} \prod_j |Y(j)^{\mathrm{Sym}(A(j))}| \geq k_0^i \cdot s!/(s-i)!i!,$$

where k_0 denotes the smallest length of a nontrivial S_k–orbit of partitions, so that $k_0 = k$ except when $k = 4$ and $k_0 = 3$. Then $|Y^{G_X}| > s(s-1)k^2/2$ except, perhaps, in the following cases:

(i) $i = 2$,

(ii) $k = 3$, $s = i = 3$,

(iii) $k = 4$, $s = i = 3$ or 4.

A straightforward case analysis shows that $|Y^{G_X}| > s(s-1)k^2/2$ in each of these situations—except for the desired one, in which $i = 2$ and each $Y(j)$ consists of a 1–set and a $(k-1)$–set. □

We now return to the proof of the correctness of ALT2. Let $Y \in \Delta(X)$ arise from A, B, a, b, A', B' as in Lemma 3.1.

The set $\Delta(X) \cap \Delta(Y)$ consists of those $Z \in \Omega$ arising as in Lemma 3.1 from A, B, a, b^* or A, B, a^*, b for some $a^* \in A - \{a\}$, $B^* \in B - \{b\}$. Then $|\Delta(X) \cap \Delta(Y)| = 2k-2$, so the algorithm correctly finds k and s. We may assume that Z arises from some A, B, a, b^*.

We have $G_{XY} = G_{X\{a,b\}}$ and $G_{XZ} = G_{X\{a,b^*\}}$, which generate G_{XaB} if $k > 2$. If $k = 2$ then $B = \{b, b^*\}$ and g_1 interchanges $\{a, b\}$ and $\{a, b^*\}$, so that $\langle G_{XY}, g_1\rangle = G_{XaB}$. Thus, in any case $H = \langle G_{XaB}, G_{YaB'}\rangle = G_{a,A\cup B,X-\{A,B\}}$.

If $s = 2$ then $H = G_a$, which has index $r < n$ in G.

If $s = 3$ and $X = \{A, B, C\}$, then $H = G_{aC}$, which has index $< n$ in G. The algorithm produces G/G_a.

Let $s \geq 4$. The only $H_X^{\Delta(X)-\{Y\}}$–orbit that is also a $G_{XY}^{\Delta(X)-\{Y\}}$–orbit corresponds (as in Lemma 3.1) to all C, D, c, d with $C, D \in X - \{A, B\}$, $c \in C$ and $d \in D$.

Now $I = G_{ag,C\cup D,X-\{C,D\}}$. As above, $\langle I_{XY}, I_{XZ}, I_{YZ}\rangle$ or $\langle I_{XY}, i_1, i_2\rangle$ is $I_{a,A\cup B,X-\{A,B\}}$. Then $J = \langle G_{a,A\cup B,X-\{A,B\}}, G_{ag,C\cup D,a,A\cup B,X-\{A,B,C,D\}}\rangle$ is $G_{a,A\cup B}$, which has index $< n$ in G. The algorithm produces G/G_a, which clearly has size $< n$. □

Lemma 3.2. *Assume* Hypothesis 2.1(a) *or* (b). *If* ALT1 *does not produce an output, then* ALT2 *does.*

Proof. We only need to check that, if ALT1 does produce an output, then we cannot be in the situation of ALT2. However, in ALT1 we found k such that $k+1$ is the rank of G and $|\Omega| = \binom{r}{k}$. No such k exists in the situation of ALT2. □

It should be clear that the above algorithms work for symmetric groups in place of alternating groups with no change.

4. PSL(V)

Throughout our discussions of classical groups there will be an underlying vector space V (which, of course, we will not have in hand) and an underlying projective space. "Dimension" will always refer to vector space dimension, while "points", "lines" and "not meeting" refer to the projective space.

Once again we begin with an arithmetic procedure:

PSL_ORDER

Input: A classical group G of characteristic p as in Hypothesis 2.1.

Output: Whether or not $G \cong \mathrm{PSL}(d,q)$ for some d, q; and if it is, d and q.

Find $q := (|\Omega| - 1)_p$. Find d such that $|G|_p = q^{d(d-1)/2}$. Test whether $|G| = |\mathrm{PSL}(d,q)|$. If not then $G \ncong \mathrm{PSL}(d,q)$ for any d, q, otherwise $G \cong \mathrm{PSL}(d,q)$. $\diamondsuit$

Correctness is easy to check. $\square$

PSL

Input: $G \leq \mathrm{Sym}(\Omega)$ permutation isomorphic to the action of some projective special linear group on the set of all subspaces of some fixed dimension of the underlying vector space of characteristic p.

Output: A set and an action of G on that set permutation isomorphic to that of G on the set of all 1–spaces of the underlying vector space or its dual.

If G is 2–transitive on Ω then output Ω.
For $X \in \Omega$ let $\Pi(X)$ be the G_X–orbit such that $|\Pi(X)|_p$ is second largest.
Find a maximal block system $\overline{\Pi}(X)$ for $G_X^{\Pi(X)}$ of smallest size.
Let $Y \in y \in \overline{\Pi}(X)$ and $X \in x \in \overline{\Pi}(Y)$.
Output $G/\langle G_{Xy}, G_{Yx} \rangle$ using **(B5)**. $\diamondsuit$

Proof of correctness of PSL. We may assume that Ω consists of the k–subspaces of a d–dimensional vector space V over $GF(q)$, where $2k \leq d$. For $Y \in \Omega - \{X\}$ with $\dim(X \cap Y) = i$, we have $|Y^{G_X}| = |(X \cap Y)^{G_X}| \cdot |\langle X, Y \rangle^{G_X}| \cdot q^{(k-i)^2}$. Here the final term $q^{(k-i)^2}$ is the number of $(k-i)$–spaces in a $2(k-i)$–space that do not meet a given $(k-i)$–space, and $q^{(k-i)^2} = |Y^{G_X}|_p$. Consequently, $\Pi(X)$ corresponds to $i = 1$, in which case $X \cap Y$ is a point.

The nontrivial blocks of $G_X^{\Pi(X)}$ arise from fixing a point w of X, a $(2k-1)$–space W containing X, or a pair w, W. There are fewer points in X than there are $(2k-1)$–spaces containing X, except when $2k = d$, in which case interchanging the underlying space V and its dual interchanges the two maximal block systems. So in any case we may assume that $\overline{\Pi}(X)$ is the block system corresponding to the set of points of X.

Now $X \cap Y = w$ corresponds to both x and y. Then $\langle G_{Xy}, G_{Yx} \rangle = \langle G_{Xw}, G_{Yw} \rangle = G_w$, and this has index $< n$ in G. $\square$

5. Classical groups

We now turn to the most intricate part of this paper. Let V be a d–dimensional vector space over GF(q), equipped with a suitable form (alternating, symmetric, quadratic or hermitian). Let Isom$V$ denote the isometry group of V, and let PIsom$V$ be Isom$V$ modulo scalars; the group G we will study is the derived group (PIsom$V$)$'$ [Di;Ta]. If W is a subspace of V then Isom$W$ will denote the group of isometries of W (where the form on W is inherited from V). We will be concerned with nonsingular subspaces, as well as subspaces on which the relevant form vanishes: totally isotropic subspaces if G is symplectic or unitary, and totally singular subspaces if G is orthogonal. As might be expected, the case of orthogonal groups of characteristic 2 creates some complications. There, V is also a symplectic space—so nonsingular points are perpendicular to themselves—and hence there is a notion of "isotropic" subspaces, but we will never use this term for orthogonal spaces.

If q is even and d is odd then there is a 1–dimensional radical. In this situation, the only subspaces that need to be considered in this paper are the nonsingular hyperplanes: all other relevant subspaces can be more easily handled within the context of the associated $(d-1)$–dimensional symplectic space $V/\mathrm{rad}V$. All new permutation representations we construct occur within the latter symplectic setting. Thus, even when we reconstruct the totally singular points of the orthogonal vector space, we can and will view these as points of the corresponding symplectic space; and it is the latter space we will focus on later in Section 8.

Witt's Lemma [Di;Ta] asserts that all elements of Isom$W$ are induced by elements of Isom$V$. However, we will need to be slightly careful, since sometimes our group G does not induce all elements of PIsom$W$.

Remark 5.1. *Switching between rank* 3 *permutation representations.* Here CLASSICAL sets $\Omega' := \Omega$. However, instead of proceeding in this manner let $\Delta(X)$ be the shortest nontrivial orbit of G_X on Ω, and let $\overline{\Delta}(X)$ be the unique nontrivial block system of $G_X^{\Delta(X)}$. Then the algorithm CLASSICAL_TS given below will produce the rank 3 incarnation of G other than the one we started with. Thus, in this case we can switch between the pairs of isomorphic groups PSp$(4,q)$ and P$\Omega(5,q)$ for q odd, as well as PSU$(4,q)$ and P$\Omega^-(6,q)$.

There is one further isomorphism to consider: PSL$(4,q) \cong$ P$\Omega^+(6,q)$. Converting from the action of PSL$(4,q)$ on points or planes to that of P$\Omega^+(6,q)$ on singular points simply requires finding the lines of the 4–dimensional vector space (cf. Section 8(A)). On the other hand, if we have the set of singular points of a P$\Omega^+(6,q)$–space then calling PSL will produce the points or planes of the 4–dimensional vector space.

The beginning of the next two algorithms already occurs in CLASSICAL. These are included here so that these algorithms can be self–contained.

CLASSICAL_TS

Input: $G \leq \mathrm{Sym}(\Omega)$ permutation isomorphic to the primitive action of some simple symplectic, orthogonal or unitary group, of Witt index > 1, on the set of all totally isotropic or totally singular subspaces of some fixed dimension > 1 of the underlying vector space of characteristic p;
G is neither $\mathrm{PSU}(4,q)$ acting on the set of totally isotropic lines nor $\mathrm{P\Omega}^+(2m,q)$ with m even acting on an orbit of totally singular m–spaces.

Output: A set of size $\leq n$ and an action of G on that set permutation isomorphic to that of G on the set of all totally isotropic or totally singular 1–spaces of the underlying vector space.

Find all orbits $\Delta(X)$ of G_X such that $|\Delta(X)|_{p'}$ is minimal subject to not being 1. Choose the largest such $\Delta(X)$.

Find a block system $\overline{\Delta}(X)$ of $G_X^{\Delta(X)}$ on which G_X is 2–transitive.

Let $Y \in y \in \overline{\Delta}(X)$ and $X \in x \in \overline{\Delta}(Y)$.

Use **(B5)** to find and output $G/\langle G_{Xy}, G_{Yx}\rangle$. $\diamondsuit$

Proof of correctness of CLASSICAL_TS: Let $\dim X = k$. We first identify $\Delta(X)$. Note that $G_X/O_p(G_X)$ is isomorphic to a subgroup of $GL(X)$ containing $SL(X)$.

Lemma 5.2. $\Delta(X) = \{Y \in \Omega \mid \mathrm{rad}\langle X, Y\rangle$ *is a point*$\}$.

Proof. If $Y \in \Omega - \{X\}$ is such that $\mathrm{rad}\langle X, Y\rangle$ is a point w (so $X \cap Y^\perp = w$), then $|Y^{G_X}|_{p'} = |G_X : G_{X,Y}|_{p'} = |G_X : G_w|_{p'} = (q^k - 1)/(q-1)$. Also $|Y^{G_X}|_p$ is the number of totally isotropic or totally singular $k-1$–spaces of $w^\perp/w$ that are opposite X/w (i.e., which, together with X/w, span a nonsingular $2k-2$–space). There always is such a $Y \in \Omega - \{X\}$ since we have excluded the case in which G is $\mathrm{P\Omega}^+(2m,q)$ with m even acting on an orbit of totally singular m–spaces.

Consider any orbit Z^{G_X} with $|Z^{G_X}|_{p'}$ minimal subject to not being 1. Then $X \cap Z^\perp \neq 0$ since $|Z^{G_X}|$ is not a power of p, so that $|Z^{G_X}|_{p'}$ is at least $|(X \cap Z^\perp)^{G_X}|_{p'} \geq (q^k - 1)/(q-1)$. It follows that $|(X \cap Z^\perp)^{G_X}|_{p'} = (q^k-1)/(q-1)$ and $X \cap Z^\perp$ is a point or a hyperplane of X.

We claim that $X \cap Z^\perp = X \cap Z$. For otherwise, $X \cap Z^\perp \not\subset Z$, so that $Z \cap X^\perp \not\subset X$ and $\langle X, Z \cap X^\perp\rangle$ is a totally isotropic or totally singular subspace properly contaning X, and $|\langle X, Z \cap X^\perp\rangle^{G_X}|$ is a factor of $|Z^{G_X}|_{p'}$, whereas we have already accounted for $|Z^{G_X}|_{p'} = |(X \cap Z^\perp)^{G_X}|_{p'} = (q^k-1)/(q-1)$. This proves our claim.

If $X \cap Z^\perp = X \cap Z$ is a point then $Z \in Y^{G_X}$ and we are finished. Suppose that $X \cap Z^\perp = X \cap Z$ is a hyperplane H of X, so $H = \mathrm{rad}\langle X, Z\rangle$; we may assume that $k > 2$ so that H is not a point. This time $|Z^{G_X}|_p$ is the number of totally isotropic or totally singular points of $H^\perp/H$ opposite X/H, so that $|Z^{G_X}| < |Y^{G_X}|$. $\square$

We now return to the proof of correctness of CLASSICAL_TS. We found the block system corresponding to the set of all points of X. Thus, y corresponds to the point $w = X \cap Y$; so does x. It follows that $\langle G_{Xy}, G_{Yx}\rangle = \langle G_{Xw}, G_{Yw}\rangle = G_w$, which has index $< n$ in G. $\square$

Remarks. We assumed primitivity in CLASSICAL_TS. This avoided only one case: the set of totally singular $(m-1)$–spaces when $G = \mathrm{P}\Omega^+(2m,q)$. Of course, in this case one could simply replace Ω by a maximal block system and call MAX_Ω^+.

The case $\mathrm{PSU}(4,q)$ was excluded in CLASSICAL_TS in order to avoid the possibility that Ω is replaced by a much larger set. On the other hand, this permutation group is covered in its incarnation as $\Omega^-(6,q)$ acting on the set of singular points; and this permutation group is also covered within the above procedure if one does not mind having the output set overly large.

Ω^+_MAX

Input: $G \leq \mathrm{Sym}(\Omega)$ permutation isomorphic to the primitive action of $\mathrm{P}\Omega^+(2m,q)$ on an orbit of totally singular m–spaces, where $m \geq 6$ is even.

Output: A set of size $< n$ and an action of G on that set permutation isomorphic to that of G on the set of all totally singular 1–spaces of the underlying vector space.

Find all orbits $\Delta(X)$ of G_X such that $|\Delta(X)|_{p'}$ is minimal subject to not being 1. Choose the largest such $\Delta(X)$. Let $Y \in \Delta(X)$.

Find a maximal block system $\overline{\Delta}(X)$ of $G_X^{\Delta(X)}$ of p'–length.

Use PSL for $G_X^{\overline{\Delta}(X)}$ to find the set Γ of points of X.

Find $x \in \Gamma$ lying in the smallest orbit of $(G_{XY})^\Gamma$. Find $(G_X)_x$.

Find $g \in G$ sending Y to X and $f \in G_X$ sending X^g to Y.

Find $z \in \Gamma$ fixed by $(((G_X)_x)^{gf})_X$. Find $h \in G_{XY}$ with $z^h = x$.

Use **(B5)** to find and output $G/\langle (G_X)_x, ((G_X)_x)^{gfh}\rangle$. $\diamondsuit$

Proof of correctness of Ω^+_MAX: Suppose that $|Z^{G_X}|_{p'}$ is minimal subject to not being 1 for some $Z \in \Omega - \{X\}$. As in CLASSICAL_TS, we may assume that $X \cap Z \neq 0$; here, $\dim X \cap Z$ is even. Since $|Z^{G_X}|_{p'} \geq |(X \cap Z)^{G_X}|_{p'}$, it follows that $\dim X \cap Z$ is 2 or $m-2$. This gives us two choices for the orbit Z^{G_X}, and the larger one occurs when $X \cap Z$ is a line.

Thus, we chose Y so that $X \cap Y$ is a line. Then x is a point of $X \cap Y$. Since gf interchanges X and Y, it fixes $X \cap Y$. Then $((G_X)_x)^{gf}$ is the stabilizer in G_Y of a point $z = x^{gf}$ of $X \cap Y$, and this is the only point of X fixed by $(((G_X)_x)^{gf})_X = G_{YzX}$. Now $((G_X)_x)^{gfh} = (G_Y)_{(x^{gf})^h} = G_{Yx}$, and hence $\langle (G_X)_x, ((G_X)_x)^{gfh}\rangle = G_x$. $\square$

Remark. Note that not dealing with sets of size $> |\Omega|$ eliminates the following simple procedure for Ω^+_MAX: let $Y \in y \in \overline{\Delta}(X)$, $X \in x \in \overline{\Delta}(Y)$, and $\Omega := G/\langle G_{Xy}, G_{Yx}\rangle$; call CLASSICAL_TS. Namely, here $|G\colon \langle G_{Xy}, G_{Yx}\rangle|$ can be quite a bit larger than the size of our original set Ω.

The next algorithm is perhaps the hardest one in this paper. In it the number of isotropic or singular points is usually—but not always—less than the size of each orbit of nonsingular subspaces.

CLASSICAL_NS

Input: $G \leq \mathrm{Sym}(\Omega)$ permutation isomorphic to the primitive action of some simple symplectic, orthogonal or unitary group, of Witt index > 1, on a G–orbit of nonsingular subspaces of the underlying vector space of characteristic p.

Output: A set of size $\leq 2.5n$ and an action of G on that set permutation isomorphic to that of G on the set of all isotropic or singular 1–spaces of the underlying vector space.

Let $X \in \Omega$. Let $\Delta(X)$ be the union of the nontrivial G_X–orbits on Ω of p'–length. Let $\Delta^+(X) = \{X\} \cup \Delta(X)$.

Find $g \in G$ with $X^g = Y \in \Delta(X)$.

Assume that $(|\Delta^+(X)|_{p'} - 1)_p = |\Delta^+(X)|_p$, or that $|\Delta(X)| = q^2(q^3+1)$ or $q(q^2+1)$ but not $q^2(q^2+1)$ for some prime power q. Find the set w of points of $\Delta(X) \cap \Delta^+(Y)$ fixed by G_{XY}. Find the block system $\overline{\Delta}(X) := w^{G_X}$ of $G_X^{\Delta(X)}$, and then find G_{Xw}. Find $f \in G_X$ moving X^g to Y and let $J := \langle G_{Xw}, gf \rangle$. Let $Z \in \Omega - (\{X\} \cup w)$, chosen with $|Z^{G_{Xw}}|_p$ minimal subject to the following condition: $Z \in \Delta(X)$ if $G_X^{\Delta(X)}$ is not 2–transitive and $Z \notin \Delta(X)$ otherwise. Let $z \in \overline{\Delta}(Z)$ be fixed by J_Z. Output $G/\langle J, G_{Zz} \rangle$ using **(B5)**. (This portion of the algorithm handled the cases in which X has dimension or codimension 1.)

Let $A \in \Delta(X) - \Delta(Y)$, $Z \in \Delta(X) \cap \Delta(Y) \cap \Delta(A)$, and $y := \Delta(X) \cap \Delta^+(Y) \cap \Delta^+(Z)$. If $2|y| < |\Delta(X) \cap \Delta^+(Y)|$ replace Z by an element of $\Delta(X) \cap \Delta^+(Y) - y$ and recompute y.

Let $\Delta'(X)$ be a G_X–orbit in $\Delta(X)$, let $y' = y \cap \Delta'(X)$, and find the stabilizer $G_{Xy'} = G_{Xy}$ of the block y' of $G_X^{\Delta'(X)}$.

Let $x := \Delta^+(X) \cap \Delta(Y) \cap \Delta^+(Z)$. Find $f \in G_X$, with $(x^g)^f = y$.

Let $J := \langle G_{Xy}, gf \rangle$.

Find $\Omega' := G/J$ using **(B5)**.

Let Ω'' be a nontrivial block system for $G^{\Omega'}$ if one exists; otherwise let $\Omega'' := \Omega'$.

If $p \not| |\Omega''|$ output Ω''. If $p || \Omega''|$ then replace Ω by Ω'' and call CLASSICAL_NS. $\diamondsuit$

Remarks. The algorithm only *calls itself at most once* at the end, replacing an orbit Ω of nonsingular lines in an orthogonal space first by an orbit Ω'' of nonsingular points and then by the orbit of singular points.

The suggestion to use a union of G_X–orbits is due to R. Liebler in the case $G = \Omega(5,q)$, $\dim X = 2$, which has the annoying problem that G_{XY} can be 1. Note that $G_X^{\Delta(X)}$ can only be intransitive when G is orthogonal and $\dim X = 2$.

Proof of correctness of CLASSICAL_NS. Let $\dim X = k$. We may assume that either $\mathrm{rad} V = 0$ and $k \leq d/2$, or $\mathrm{rad} V \neq 0$, V is an orthogonal space of odd dimension and characteristic 2 and $k = d-1$. A check of the possible groups G

shows that $X^\perp$ has Witt index ≥ 1 if $\mathrm{rad}V = 0$. Let q be the size of the field underlying V.

We begin with the simplest case:

CASE I. $\mathrm{rad}V = 0$ and $k = 1$.

Here X and Y are nonsingular 1–spaces, and some Sylow p–subgroup P of G_X fixes Y and hence also the line $\langle X, Y\rangle$. It follows that $\langle X, Y\rangle$ contains a unique isotropic or singular point r (this is the radical of $\langle X, Y\rangle$ except when V is an orthogonal space of characteristic 2). Moreover, G_X is transitive on $\Delta(X)$ since P fixes only one isotropic or singular point of $X^\perp$ and $G_{X\langle X,Y\rangle}$ is transitive on the points of $\langle X, Y\rangle - \{X, r\}$. In particular, some element of G interchanges X and Y, and hence gf can be found behaving as indicated in the algorithm.

Now w consists of the points $\neq X, r$ of $\langle X, Y\rangle = \langle X, r\rangle$, and $J = \langle G_{Xw}, gf\rangle = G_{\langle X,Y\rangle}$ since gf interchanges X and Y. (N.B.—The element gf is needed here when $q = 2$.) Then $G_X^{\Delta(X)}$ acts on the block system $\overline{\Delta}(X)$ as it does on the set of isotropic or singular points of $X^\perp$, and hence has rank 3 or is 2–transitive, and always is primitive in CASE I. Moreover, $(|\Delta^+(X)|_{p'} - 1)_p = |\Delta^+(X)|_p = q$ here, except that $|\Delta(X)|$ is $q(\sqrt{q}^3 + 1)$ when $G = \mathrm{PSU}(4, \sqrt{q})$ and $q(q^2 + 1)$ when $G = \mathrm{P\Omega}(5, q)$; and that $|\Delta(X)|$ is not of the form $q^2(q^2 + 1)$.

Subcase Ia. $G_X^{\overline{\Delta}(X)}$ *is not* 2*–transitive.*

Here $X^\perp$ has Witt index > 1. Consider any $Z' \in \Delta(X) - w$. Let $Z' \in w'$ with $w' \in \overline{\Delta}(X) - \{w\}$. Then $|G_{XwZ'}|_p = |G_{Xww'}|_p$ and hence $|Z'^{G_{Xw}}|_p = |w'^{G_{Xw}}|_p$. Since $Z' \in \Delta(X)$, w' corresponds to the isotropic or singular point r' of $\langle X, Z'\rangle$. Depending upon whether r' is or is not in $r^\perp$, $|r'^{G_{Xw}}|_p$ is q or is $> q$, respectively. Since the algorithm chooses $Z = Z' \in \Delta(X) - w$ with $|Z^{G_{Xw}}|_p$ minimal, it follows that $r' \in r^\perp$ and hence that $r^\perp \supseteq \langle X, r'\rangle = \langle X, Z\rangle$. Now $\langle Z, r\rangle$ can be viewed as one of the members of $\overline{\Delta}(Z)$, and is fixed by $G_{\langle X,Y\rangle,Z} = J_Z$.

We claim that *there is just one isotropic or singular point of* $Z^\perp$ *fixed by* J_Z. For, G_{ZL} induces at least $\mathrm{PSL}(2, q)$ on the totally isotropic or totally singular line $L = \langle r, r'\rangle$, and hence G_{ZLr} has a p–element t acting nontrivially on L. All isotropic or singular points of $\langle X, Y, Z\rangle = X \perp L$ lie in L, and t fixes only the point r of L; every point of $Z^\perp$ not in L is moved by G_{XYZ}. This proves the claim.

It follows that $z \in \overline{\Delta}(Z)$ corresponds to r. Then $\langle J, G_{Zz}\rangle = \langle G_{\langle X,Y\rangle}, G_{Zr}\rangle$ properly contains $G_{\langle X,Y\rangle}$, fixes r, and hence is G_r, as required. Usually $|G\colon\langle J, G_{Zz}\rangle| < n$; in all cases a calculation yields that $|G\colon\langle J, G_{Zz}\rangle| < 2n$.

Subcase Ib. $G_X^{\overline{\Delta}(X)}$ *is* 2*–transitive.*

Now $X^\perp$ has Witt index 1, so that G is $\mathrm{PSU}(4, q)$, $\mathrm{P\Omega}^-(6, q)$ or $\mathrm{P\Omega}(5, q)$, where q is odd in the latter case. In particular, $V = X \perp X^\perp$.

This time consider any $Z' \in \Omega - \Delta^+(X)$, so $\langle X, Z'\rangle \cap X^\perp = u$ is nonsingular. Then $|G_{XwZ'}|_p = |G_{Xru}|_p$, so that $|G_{XwZ'}|_p \neq 1$ if $u \in r^\perp$ and $|G_{XwZ'}|_p = 1$ if $u \notin r^\perp$ (recall that $G_X^{X^\perp}$ is either a 3–dimensional unitary or a 3– or 4–dimensional orthogonal group).

We chose $Z := Z' \in \Omega - \Delta^+(X)$ with $|G_{XwZ}|_p$ maximal, so $u \in r^\perp$ and hence $r^\perp \supseteq \langle X, u\rangle = \langle X, Z\rangle$. It follows that J_Z fixes some $z \in \overline{\Delta}(Z)$ (corresponding to

the line $\langle Z, r\rangle$). This is the only fixed point of J_Z in $\overline{\Delta}(Z)$ since r is again the only isotropic or singular point fixed by $J_Z = G_{\langle X,r\rangle,Z}$. Once again this implies that $\langle J, G_{Zz}\rangle = G_r$, where $|G\colon \langle J, G_{Zz}\rangle| < 2n$.

CASE II: $\mathrm{rad}V = 0$ and $k > 1$.

Primitivity excludes the following situations: V is orthogonal over GF(2) or GF(3) and X is a hyperbolic line (since $\mathrm{O}^+(2,2)$ and $\mathrm{O}^+(2,3)$ fix a nonsingular point), as well as the case in which $X^\perp \in \Omega$. Our first task is to determine $\Delta(X)$. We begin with the following simple

Lemma 5.3. *Suppose that W is a subspace of V, and y is an isotropic or singular point of $W^\perp$.*

(i) *The group of all (projective) transvections of $\langle W, y\rangle$ with center y is induced by a subgroup of G. In particular, $G_{\langle W,y\rangle}$ is transitive on the complements to y in $\langle W, y\rangle$.*

(ii) *Assume that, in addition, G is an orthogonal group and W is nonsingular with $\dim W \geq 3$. Then $\langle G_{W,\langle W,y\rangle}, G_{W',\langle W,y\rangle}\rangle = G_{\langle W,y\rangle}$ for any complement $W' \neq W$ to y in $\langle W, y\rangle$.*

Proof. (i) We may assume that $W = y^\perp$. Since all complements to y in $y^\perp$ are isometric, by Witt's Lemma the group T of those transvections of $y^\perp$ with center y is induced by a subgroup $\hat{T}$ of $\mathrm{PIsom}\, V$; also $\mathrm{Isom}\, y^\perp$ is induced by a subgroup of $\mathrm{PIsom}V$. The representation of $\mathrm{Isom}\, y^\perp$ on T is equivalent to that on $y^\perp/y$, and hence is irreducible. It follows that $\hat{T}$ lies in the derived group G of $\mathrm{PIsom}V$.

(ii) The stated conditions on W imply that $G_{W\langle W,y\rangle}$ acts irreducibly on $T/C_T(W)$, and hence is a maximal subgroup of the group induced on $\langle W, y\rangle$ by $\hat{T} \cdot G_{W,\langle W,y\rangle} = G_{\langle W,y\rangle}$. □

Lemma 5.4. *If $Y \in \Omega - \{X\}$ is in a G_X-orbit of p'-length, then $\langle X, Y\rangle = X \perp r$ for an isotropic or singular point r.*

Proof. Recall that $V = X \perp X^\perp$. There is a Sylow p–subgroup P of G_X fixing Y and restricting to Sylow subgroups of both G_X^X and $G_X^{X^\perp}$. Let Y' denote Y or $Y^\perp$, and let U be the projection $\langle X, Y'\rangle \cap X^\perp$ of Y' into $X^\perp$. Then U is fixed by P.

Note that $U \neq 0$, as otherwise $Y \neq X = Y'$ and hence $X^\perp = Y \in \Omega$, which would contradict the primitivity of G on Ω. We will consider two cases; these roughly correspond to the possibilities $k < d/2$ and $k = d/2$.

Case 1. $U \neq X^\perp$.

Since $X^\perp$ has dimension $\geq d/2$ it has nonzero Witt index and is not an $\mathrm{O}^+(2,q)$–space. Then the proper P–invariant subspace U of $X^\perp$ has a nonzero radical containing an isotropic or singular point r fixed by P.

Suppose that $U \neq r$. By Lemma 5.3, P contains an element g inducing a nontrivial transvection of $\langle X, U\rangle$ with center r and axis $A \supset X$. Since g fixes $Y' \subset \langle X, U\rangle$, it follows that Y' must either be contained in A or contain r. The first of these is impossible since $\langle X, Y'\rangle = \langle X, U\rangle \not\subseteq A$. So is the second: $r^\perp$

contains X, as well as U (recall that r is in rad$U$), and hence also Y', so that $r \notin Y'$ since Y' is nonsingular.

Thus, $U = r$, so that $\langle X, Y'\rangle = \langle X, r\rangle$ is a $(k+1)$–space with radical r. Then X and Y' are complements to r in $\langle X, r\rangle$, so that $Y' \in \Omega$ by Lemma 5.3(i). Since $Y \in \Omega$ and $Y^\perp \notin \Omega$ we have $Y' = Y$. This proves the lemma in this case.

Case 2. $U = X^\perp$.

Here $d = 2k$, so since $X^\perp \notin \Omega$ the group G must be orthogonal. There is a singular point r of $X^\perp$ and a line $L \subset X^\perp$ containing r that are fixed by P (here L is totally singular unless $X^\perp$ has Witt index 1). Then $L^\perp$ is a hyperplane of $r^\perp$ containing X, so by Lemma 5.3(i) there is an element $g \in P$ fixing $\langle X, X^\perp \cap L^\perp\rangle$ pointwise. Then $[V, g] \subseteq L$ since $C_V(g) \supseteq L^\perp$.

Since $Y^g = Y$, either Y or $Y^\perp$ meets L; let Y' be one of these meeting L. Then the projection $\langle X^\perp, Y'\rangle \cap X$ of Y' on X is not X. After interchanging the roles of X and $X^\perp$ we find that we are back in Case 1. Consequently, X is a hyperplane of $\langle X, Y'\rangle$. Then $\langle X, Y'\rangle = X \perp y$ for a point $y \in X^\perp$ that is fixed by P and hence is singular. Now $Y' \in \Omega$ by Lemma 5.3(i), while $Y \in \Omega$ and $Y^\perp \notin \Omega$, so $Y' = Y$. □

Lemma 5.5. *Let $\Gamma(X)$ be a nontrivial G_X–orbit of p'–length. Let $Y \in \Gamma(X)$.*

(i) *$r = \mathrm{rad}\langle X, Y\rangle$ is an isotropic or singular point, and $\langle X, Y\rangle = X \perp r$.*

(ii) *If $s = X \cap (X \cap Y)^\perp$, then s is a point and $\langle X^\perp, Y^\perp\rangle = X^\perp \perp s$. Moreover, s is isotropic or singular and is $\mathrm{rad}\langle X^\perp, Y^\perp\rangle$, except that it is nonsingular if G is an orthogonal group and $\dim X = 2$.*

(iii) *Exclude the following case: $(*)$ G is an orthogonal group of odd characteristic, and $\dim X = 2$. Then $\Gamma(X)$ contains all hyperplanes of $\langle X, Y\rangle$ that contain $X \cap Y$ but not r. Moreover, $\Gamma(X)$ is the only nontrivial G_X–orbit of p'–length, and there is an element of G interchanging X and Y.*

(iv) *$\Gamma(X) \cap \Gamma^+(Y)$ is contained in the set of $Z \in \Omega - \{X\}$ such that (α) $Z \subset \langle X, Y\rangle$ or (β) $Z \supset X \cap Y$, and contains all Z of type (α); it also contains all of type (β) if $(*)$ is excluded.*

(v) *Let $\Delta(X)$ be the union of all the nontrivial G_X–orbits of p'–length. Then $|\Delta^+(X)|_p = (|\Delta^+(X)|_{p'} - 1)_p^k$, with the following exceptions: $G \cong \mathrm{PSU}(5, q)$, $k = 2$, $|\Delta^+(X)| = q^4(q^3+1)$; $G \cong \mathrm{P}\Omega^\pm(6, q)$, $k = 2$, $|\Delta^+(X)| = q^2(q^2+1)$.*

Proof. Part (i) is just Lemma 5.4. For the first statement in (ii), note that $X \cap Y = X \cap s^\perp$ for a unique point s of X, and then $\langle X^\perp, Y^\perp\rangle = X^\perp \perp s$.

If V is orthogonal assume temporarily that $k > 2$ (recall that $k > 1$ already). A Sylow p–subgroup P of G_X fixes Y and hence s. This implies (ii). Moreover, G_{Xs} has an element inducing 1 on $X^\perp$ and transitive on the nonzero vectors in r, so that G_{Xrs} is transitive on the hyperplanes $\neq X$ of $\langle X, Y\rangle$ containing $X \cap s^\perp$ but not r. Hence, $\Gamma(X)$ is as described in (iii), and the relation between X and Y is symmetric. Finally, if $Z \in \Gamma(X) \cap \Gamma(Y)$ and $Z \not\supset X \cap Y$ then, since $X \cap Z$ and $Y \cap Z$ are hyperplanes of Z, we must have $Z = \langle Z \cap X, Z \cap Y\rangle \subset \langle X, Y\rangle$. Clearly Y has types (α) and (β). By Lemma 5.3(i), $G_{\langle X,Y\rangle r}$ is transitive on the subspaces of type (α) and $G_{\langle X^\perp Y^\perp\rangle s}$ is transitive on those of type (β).

This proves (i-iv) except when V is an orthogonal space and $\dim X = 2$. In that case, $\dim X^\perp \geq 3$. If $p = 2$ then P fixes a unique point of X, and that point is nonsingular. Thus, s is nonsingular. However, the arguments in the rest of the preceding paragraph remain valid.

Finally, assume that p is odd. Here P is the identity on $\langle X, r\rangle$, so any line of this subspace, not containing r, lies in a G_X–orbit of p'–length. Nevertheless, for the weaker assertions required in (ii-iv), the above arguments remain valid.

In all cases (v) involves a brief calculation. □

We now return to CASE II *of* CLASSICAL_NS.

Let X, Y, r, s be as in the preceding lemma. The members of $\Delta(X) \cap \Delta^+(Y)$ fixed by G_{XY} include the hyperplanes $\neq X$ of $\langle X, Y\rangle$ containing $X \cap Y$ (these are fixed since G_{XY} already fixes three hyperplanes X, Y and $\langle X \cap Y, s\rangle$ of $\langle X, Y\rangle$ containing $X \cap Y$); and these are all of the members of w except, perhaps, when G is orthogonal, $k = 2$, and $w \cup \{X\}$ consists of all q^2 lines of $\langle X, Y\rangle$ not containing $X \cap Y$. In particular, G_{Xw} fixes $\langle X, Y\rangle$ and $X \cap Y$, so that G is imprimitive on $\overline{\Delta}(X)$ in CASE II.

By Lemma 5.5(iv), $\Delta(X) \cap \Delta^+(Y)$ is the union of two subsets, respectively of size $q^k - 1$ (type (α)) and $q^{d-k} - 1$ (type (β)). Hence, we may assume that the algorithm chose Z in (β). (If $\dim X = \dim X^\perp$ then we can replace X by $X^\perp$ if necessary.) Then $y = \Delta(X) \cap \Delta^+(Y) \cap \Delta^+(Z)$ consists of all of (β), and $G_{Xy} = G_{X,X\cap Y} = G_{Xs}$. Similarly, $G_{Yx} = G_{Ys}$. Since x^g is a member of y^{G_X}, f can be found such that $x^{gf} = y$.

By Lemma 5.3(ii), $J = \langle G_{Xy}, gf\rangle = \langle G_{X\langle X^\perp, s\rangle}, G_{Y\langle X^\perp, s\rangle}, gf\rangle = G_{\langle X^\perp, s\rangle}$, so $|\Omega'| = |G\colon J| = |G\colon G_{X^\perp}|\,|s^{G_X}|/|(X^\perp)^{G_{\langle x^\perp, s\rangle}}|$. Here, s^{G_X} is an orbit of points of the nonsingular k–space X.

If s is isotropic or singular then $J = \langle G_{Xy}, gf\rangle = \langle G_{X^\perp\langle X^\perp, s\rangle}, G_{Y^\perp\langle X^\perp, s\rangle}, gf\rangle = G_{\langle X^\perp, s\rangle}$ by Lemma 5.3(ii), so $|\Omega'| = |G\colon J| = |G\colon G_{X^\perp}|\,|s^{G_X}|/|(X^\perp)^{G_{\langle x^\perp, s\rangle}}|$. Here, s^{G_X} consists of all isotropic or singular points of the nonsingular k–space X. Then $|s^{G_X}| < q^k \leq q^{d-k} = |(X^\perp)^{G_{\langle x^\perp, s\rangle}}|$ (using $W = X^\perp$ in Lemma 5.3(i)). Consequently, $|G\colon J| < |G\colon G_{X^\perp}| = n$. Moreover, $J = G_{\langle X^\perp, s\rangle}$ is properly contained in exactly one proper subgroup of G, namely G_s. Thus, Ω'' corresponds to s^G, and CLASSICAL_NS outputs correctly in this situation.

Finally, if s is nonsingular then $k = 2$ and G is orthogonal. This time $\langle X^\perp, s\rangle$ is a hyperplane, and G_{Xs} is a maximal subgroup of $G_{\langle X^\perp, s\rangle}$. Once again $J = \langle G_{Xy}, gf\rangle = \langle G_{X\langle X^\perp, s\rangle}, G_{Y\langle X^\perp, s\rangle}, gf\rangle = G_{\langle X^\perp, s\rangle}$, where $|G\colon J| < |G\colon G_{X^\perp}| = n$ since there are many more than $|s^{G_X}| \leq q + 1$ hyperplanes isometric to $X^\perp$ in $(X^\perp)^{G_{\langle x^\perp, s\rangle}}$. Thus, the algorithm replaces an orbit Ω of nonsingular lines by (what amounts to) an orbit $\Omega' = \Omega''$ of nonsingular points, and then calls CASE I of CLASSICAL_NS.

CASE III: $\mathrm{rad}V \neq 0$ and $k = d - 1$.

Here V is orthogonal, $p = 2$ and d is odd. This case resembles CASE I. In order to emphasize the similarities and facilitate visualization, it seems easiest to view this permutation representation of G from the following slightly different

perspective, using different language to describe the members of Ω. Let $v = \mathrm{rad}V$, and view V as the hyperplane $v^\perp$ in a $(d+1)$–dimensional orthogonal space U. Then Ω can be viewed as a G–orbit of *nonsingular lines* X of U containing v but not contained in V; here $X^\perp$ is a nonsingular hyperplane of V, thereby matching this description with our original one. If $Y \in \Omega - \{X\}$ then $\mathrm{rad}\langle X, Y\rangle$ can be either a singular or a nonsingular point of $X^\perp$. (N.B.—Only singular points can occur if $q = 2$.)

Once again we need to identify $\Delta(X)$ and $\overline{\Delta}(X)$. A Sylow 2–subgroup P of G_X fixes a unique point $r \in X^\perp \subset v^\perp$, and r is singular. It follows that $\Delta(X)$ consists of those $Y \in \Omega$ such that $\mathrm{rad}\langle X, Y\rangle$ is singular. Note that G_{XY} fixes all lines of $\langle X, Y\rangle$ through v but no other lines of U. Once again $(|\Delta^+(X)|_{p'} - 1)_p = |\Delta^+(X)|_p = q$. Once again the block system $\overline{\Delta}(X)$ corresponds to the set of all singular points of $X^\perp$, so that G_X *acts primitively* on it; w corresponds to $\langle X, Y\rangle = \langle X, r\rangle$, and $J = G_{\langle X,r\rangle}$.

Subcase IIIa. $G_X^{\overline{\Delta}(X)}$ *is not* 2*–transitive.*

As in Subcase Ia, this means that $X^\perp$ has Witt index > 1. We chose $Z \in \Delta(X)$ with $|Z^{G_{Xw}}|_2$ minimal, so the radical r' of $\langle X, Z\rangle$ is perpendicular to r. Then r is perpendicular to $\langle X, r'\rangle = \langle X, Z\rangle$. Now $\langle Z, r\rangle$ can be viewed as a member of $\overline{\Delta}(Z)$, and is fixed by J_Z.

As in Subcase Ia, r is the only singular point of $Z^\perp$ fixed by J_Z, and hence there is only one $z \in \overline{\Delta}(Z)$ fixed by J_Z. Once again it follows that $\langle J, G_{Zz}\rangle = G_r$. This time $|G\colon \langle J, G_{Zz}\rangle| \leq 2.5n$ (with equality occurring when G is $\Omega(7,2)$ and G_X is $O^-(6,2)$).

Subcase IIIb. $G_X^{\overline{\Delta}(X)}$ *is* 2*–transitive.*

Here $X^\perp$ has Witt index 1, so that G is $\mathrm{P}\Omega(5,q)$ with $q > 2$. We chose Z in the algorithm with $Z \notin \Delta(X)$ and $|Z^{G_{Xw}}|_2$ minimal subject to $Z \not\subseteq \langle X, r\rangle$. *We claim that* $Z \subset r$.

First consider any $Z' \in \Omega$ with $Z' \subset r^\perp$ but $Z' \notin \Delta(X)$, so $r' = \langle X, Z\rangle$ is nonsingular. Then $G_{XZ'}$ has a normal subgroup $\Omega(3,q)$ in view of its action on $X^\perp \cap r'^\perp$, and this subgroup induces 1 on $\langle X, r'\rangle$. An involution t in this group is 1 on X, fixes r and $\langle X, r\rangle \cap V = \langle v, r\rangle$, and hence induces a transvection of $\langle X, r\rangle$ with center v. In particular, $|G_{XYZ}|_2 \neq 1$.

Conversely, consider any $Z' \in \Omega$, $Z' \not\subseteq \langle X, Y\rangle$, with $|G_{XYZ'}|_2 \neq 1$. Let $w = \langle X, Z'\rangle \cap X^\perp$. Then a Sylow 2–subgroup of $G_{XYZ'}$ fixes the points r and w of $X^\perp$. Since $X^\perp$ is an orthogonal space of Witt index 1, and G_X has a nontrivial 2–subgroup fixing the singular point r and the nonsingular point u, this is only possible if r is perpendicular to w, and hence also to $\langle X, w\rangle = \langle X, Z'\rangle$.

This proves our claim. It follows that J_Z fixes some $z \in \overline{\Delta}(Z)$ (corresponding to $\langle Z, r\rangle$). Once again, there is only one element of $\overline{\Delta}(Z)$ fixed by J_Z, $\langle J, G_{Zz}\rangle = G_r$, and $|G\colon \langle J, G_{Zz}\rangle| \leq 2n$. $\square$

Remark. We emphasize that, even in CLASSICAL_NS, we have never used permutation groups on sets of size greater than that of the output.

6. All points

Before proving Theorem 2.3 we need to be able to reconstruct the set of all points of a projective space from a suitable G–orbit of points:

PROJECTIVE_SPACE

Input: $G \leq \mathrm{Sym}(\Omega)$ permutation isomorphic to the action of some simple classical group on an orbit of 1–spaces of a vector space V underlying G, where $|\Omega|$ is not divisible by the characteristic p and G is not 2–transitive on Ω.

Output: A set Π and an action of G on Π permutation isomorphic to that of G on the set of all points of the projective space corresponding to V.

We will separate the procedure into several parts.

1. Let $X \in \Omega$. Let $\Gamma(X)$ and $\Delta(X)$ be the orbits of G_X on $\Omega - \{X\}$, where $\Delta(X)$ is the shorter of these orbits. Let $Y \in \Gamma(X)$ and $\Delta(X,Y) := \Delta(X) \cap \Delta(Y)$.

Let $Z \in \Delta(X,Y)$. Find the unique maximal block system $\overline{\Delta}(Z)$ of $G_Z^{\Delta(Z)}$.

Let $x, y \in \overline{\Delta}(Z)$ with $X \in x$ and $Y \in y$. Let $X' \in x$ and $Y' \in y$ with $X \neq X'$ and $Y \neq Y'$.

Let $q := |x|$ and $K := G_{XYZX'Y'}$.

2. Let $g_1 \in G$ send Y to X and $g_2 \in G_X$ send X^{g_1} to Y. Let $H := \langle G_{XY}, g_1 g_2 \rangle$. Let $\Lambda(X,Y)$ be the union of those H–orbits on Ω having length $< q$.

If $|\Lambda(X,Y)| = q+1$, output Ω.

Find subgroups L and F, as follows:

If $|\Lambda(X,Y)| > 2$ find $g \in G_X$ sending Y to some point of $\Lambda(X,Y) - \{X,Y\}$, and let $L := \langle H, H^g \rangle$ and $F := G_{XYY^g}$;

if $|\Lambda(X,Y)| = 2$ let $h \in H$ move Z, and let $L := H$ and $F := \langle K, K^h \rangle$.

3. Find the L–orbits on $\Omega - (\Lambda(X,Y) \cup \Delta(X,Y))$ of length divisible by p. There is either just one of them, $\Sigma(X,Y)$, or two of them, $\Sigma(X,Y)$ and $\Sigma'(X,Y)$.

Let $W \in \Sigma(X,Y)$.

Let $u := W^F$ (this is a block of $L^{\Sigma(X,Y)}$). Find G_{XYu} and L_{Zu}.

4. If $|\Lambda(X,Y)| > 2$ or $p > 2$, then L_W fixes some $W' \in \Sigma(X,Y) - \{W\}$. Find $f_1 \in G$ sending X to W and $f_2 \in G_W$ sending Y^{f_1} to W'. Find $\Phi := G/\langle G_{XYu}, (G_{XYu})^{f_1 f_2} \rangle$ using **(B5)**.

If $\Sigma(X,Y)$ was the only L–orbit on $\Omega - (\Lambda(X,Y) \cup \Delta(X,Y))$, output $\Omega \cup \Phi$.

Otherwise, replace $\Sigma(X,Y)$ by $\Sigma'(X,Y)$ and repeat, in order to obtain another set Φ' on which G acts. Output $\Omega \cup \Phi \cup \Phi'$.

5. Find $g \in G_{YZx}$ such that $X^g = X'$. Let $J := \langle L_Z, g \rangle$.

Find the $(q-1)st$ powers of the generators of L_{Zu}. Let t be such a power that moves X.

Find $j \in J$ sending X to X' and Y to Y^t.

Find $\Phi := G/\langle G_{XYu}, (G_{XYu})^j \rangle$ using **(B5)**. Output $\Omega \cup \Phi$. $\diamondsuit$

Proof of correctness of PROJECTIVE_SPACE.

1. Since G is not 2–transitive, the Witt index of V is ≥ 2. Then G_X has just two nontrivial orbits, and $Y \in \Gamma(X)$ if and only if X and Y are not perpendicular. In particular, $\langle X, Y\rangle$ is a hyperbolic line, and $\Delta(X,Y) \subseteq \langle X, Y\rangle^\perp$.

The block system $\overline{\Delta}(Z)$ corresponds to the set of all lines in $\{Z\} \cup \Delta(Z)$ through Z, and q is the size of the underlying field. The totally isotropic or totally singular lines $\langle X, Z\rangle$ and $\langle Y, Z\rangle$ are distinct and span the plane $\langle X, Y, Z\rangle$. Since $K = G_{XX'YY'Z}$ fixes three points of each of these lines, it is the pointwise stabilizer of $\langle X, Y, Z\rangle$ in G.

2. We have $H = G_{\{X,Y\}}$ since $g_1 g_2$ interchanges X and Y. Then $\Lambda(X,Y)$ consists of the members of Ω on the hyperbolic line $\langle X, Y\rangle$, so $|\Lambda(X,Y)|$ is 2, $\sqrt{q}+1$ or $q+1$ according to whether G is orthogonal, unitary or symplectic. In particular, the output is correct if $|\Lambda(X,Y)| = q+1$.

We claim that L and F behave as follows: *L is the set–stabilizer $G_{\langle X,Y\rangle}$, and F fixes $\langle X, Y\rangle$ pointwise while inducing at least* $(\mathrm{Isom}\langle X, Y\rangle^\perp)'$ *on* $\langle X, Y\rangle^\perp$.

Namely, if $|\Lambda(X,Y)| > 2$ then $G_{\langle X,Y\rangle}$ is 2-transitive on $\Lambda(X,Y)$. Then g exists in **2**, and $L = \langle H, H^g\rangle$ is $G_{\langle X,Y\rangle}$. Moreover, $F = G_{XYY^g}$ is the pointwise stabilizer of $\langle X, Y\rangle$ in G.

On the other hand, if $|\Lambda(X,Y)| = 2$ then $L = H = G_{\langle X,Y\rangle}$. Moreover, $F = \langle K, K^h\rangle$ fixes all points of $\langle X, Y\rangle$ since K does; the group it induces on $\langle X, Y\rangle^\perp$ contains all p–elements in $(\mathrm{Isom}\langle X, Y\rangle^\perp)'$ that fix Z or Z^g, and hence contains $(\mathrm{Isom}\langle X, Y\rangle^\perp)'$. This completes the proof of our claim.

3. Each G–orbit of nonsingular points has a representative in $\langle X, Y\rangle$. Moreover, L is transitive on the set of nonsingular points of $\langle X, Y\rangle$ unless V is an orthogonal space of odd characteristic, in which case there are exactly two orbits, each of length $(q-1)/2$.

Any $W \in \Omega - (\Lambda(X,Y) \cup \Delta(X,Y))$ lies in a unique line $\langle U, N\rangle$ spanned by points U of $\langle X, Y\rangle$ and N of $\langle X, Y\rangle^\perp$ both or neither of which are nonsingular. Here, $|W^{G_{\langle X,Y\rangle}}|$ is divisible by p if and only if U and N are nonsingular. Conversely, for any nonsingular point U of $\langle X, Y\rangle$ there is a unique G_{XYU}–orbit $N^{G_{XYU}} \subset \langle X, Y\rangle^\perp$ of nonsingular points such that $\langle U, N\rangle$ contains an isotropic or singular point W. *We claim that all such W lie in the same $G_{\langle X,Y\rangle}$–orbit.* To see this, it suffices to check that all members of Ω lying in $\langle U, N\rangle$ belong to the same same $G_{\langle X,Y\rangle UN}$–orbit. If G is orthogonal of characteristic 2, there is only one singular point in $\langle U, N\rangle$, so there is nothing to prove. In all other cases, $\langle X, Y, N\rangle$ is nonsingular, and $G_{\langle X,Y,N\rangle}$ induces $\mathrm{Isom}\langle X, Y, N\rangle$ on $\langle X, Y, N\rangle$. (For, $\langle X, Y, N\rangle^\perp$ is nonzero, and has dimension ≥ 2 if G is orthogonal.) It follows that $G_{\langle X,Y\rangle UN}$ is transitive on the members of Ω lying in $\langle U, N\rangle$, which proves our claim.

In particular, $G_{\langle X,Y\rangle}$ has at most two orbits on $\Omega - (\Lambda(X,Y) \cup \Delta(X,Y))$ of length divisible by p, with two occurring if and only if V is orthogonal and q is odd.

By **2**, F fixes U and has the same orbits as $\mathrm{Isom}\langle X, Y\rangle^\perp$ on the set of nonsingular points of $\langle X, Y\rangle^\perp$. Thus, if $W \in \Sigma(X,Y)$ then $W^{L_U} = W^F$ is a block u of $L^{\Sigma(X,Y)}$, with stabilizer $L_u = L_U$.

4. Here we are assuming that V is either orthogonal of odd characteristic or unitary. As noted in **3**, $\langle U, N\rangle$ contains at least two members W, W' of Ω. Both of these are fixed by L_W, as L_W fixes W, U, N and hence all points of $\langle U, N\rangle$. Since $f_1 f_2$ sends X to W and Y to W', we have $\langle G_{XYu}, (G_{XYu})^{f_1 f_2}\rangle = \langle G_{XYU}, G_{WW'U}\rangle = G_U$.

Then Φ can be identified with the orbit U^G of nonsingular points. If these are all the nonsingular points then the output $\Omega \cup \Phi$ is correct. If there is a second orbit of nonsingular points then Φ' corresponds to that orbit, and the output $\Omega \cup \Phi \cup \Phi'$ is correct.

5. Now G is orthogonal of characteristic $p = 2$. Note that $Z = \mathrm{rad}\langle X, Y, Z\rangle$. By Lemma 5.3(i) there is an element $g \in G_{ZxY}$ sending X to the point X' of $\langle X, Z\rangle$ chosen in **1**. Then $(L_Z)^g$ is the stabilizer in $G_{\langle X,Y,Z\rangle}$ of $\langle X, Y\rangle^g = \langle X, Y'\rangle$, so that $J = \langle G_{\langle X,Y\rangle}, g\rangle = G_{\langle X,Y,Z\rangle}$. (N.B.–Most of **5.** concerns a small permutation action: that of J on the set X^J of size $2q$.)

The group $L_{Zu} = G_{\langle X,Y\rangle ZU}$ acts on $\langle X, Y\rangle$, inducing a group of order 2; it also acts on $\langle X, Y, Z\rangle$, inducing an abelian group of order dividing $2(q-1)$ generated by an involution and transformations inducing the identity on $\langle X, Y\rangle$. Then the element t constructed in **5** exists, and induces an involution on $\langle X, Y, Z\rangle$—in fact, a transvection having center U and axis $\langle U, Z\rangle$. Since t fixes Z, U and $\langle U, X'\rangle$ while interchanging X and Y, it also interchanges x and y and hence $X' = x \cap \langle U, X'\rangle$ and $y \cap \langle U, X'\rangle$.

By Lemma 5.3(i), there is some $j \in J$ sending X to X' and Y to X'^t (namely, a transvection of $\langle X, Y, Z\rangle$ with center Z and axis $\langle U, Z\rangle$). Then $\langle G_{XYu}, (G_{XYu})^j\rangle = \langle G_{XYU}, G_{X'X''U}\rangle = G_U$. As in **4**, the output $\Omega \cup \Phi$ is correct. □

Remarks. Once again we note that we have only used permutation groups on sets of size at most that of the output.

The above ideas can be varied in many ways. With some care, **5** can be modified so as to apply to the situation in **4**. On the other hand, **4** almost applies to the situation in **5**: an element of L_W moving X has exactly $q/2$ 2–cycles on Ω, each determining a line through U, which can be used as in **4** to obtain G_U provided that $q > 2$. The case $q = 2$ can be dealt with similarly by introducing an additional point and dimension, but then this differs little from the approach in **5**.

As noted at the start of Section 5, in the case of orthogonal spaces of odd dimension d and characteristic 2 PROJECTIVE_SPACE does not construct the points of the corresponding projective space, but rather those of the symplectic space of dimension $d-1$.

Proof of Theorem 2.3. In Section 3 we saw that ALT_ORDER, ALT1 and ALT2 correctly decide whether or not G is isomorphic to an alternating group A_r and, if it is, they produce the natural action of G on an r–set.

Assume that G is a classical group. In NATURAL_ACTION, Ω corresponds to a G–orbit of subspaces, each of dimension k, say (cf. Hypothesis 2.1). The characteristic p of G was found correctly [Ar]. Note that, when $G \cong \mathrm{PSp}(4,3) \cong$

PSU$(4,2)$, the only characteristic 3 instances of Hypothesis 2.1 occur when $n = 40$; this explains the exception at the start of NATURAL_ACTION.

If $p|n$ then Ω corresponds to an orbit of nonsingular subspaces. In Section 5 we saw that CLASSICAL_NS outputs correctly.

We may now assume that $p \not| n$. The possibility $G \cong \mathrm{PSL}(d,q)$ is identified and handled by PSL_ORDER and PSL, which obtain the set of all points or hyperplanes of the underlying projective space.

It remains to consider the case in which G is a symplectic, orthogonal or unitary group on V, and Ω is an orbit of totally isotropic or totally singular k–spaces for some $k \geq 1$. In CLASSICAL_TS and Ω^+_MAX we identified $\Delta(X)$ and saw that there is a unique maximal block system of $G_X^{\Delta(X)}$ of p'–length, provided that $k > 1$ (here we do not have to exclude the case $G \cong \mathrm{PSU}(4,q)$ and $k = 2$, since it arises with $G \cong \mathrm{P\Omega}^-(6,q)$ and $k = 1$). When $k = 1$ it is easy to check that $G_X^{\Delta(X)}$ has a unique maximal block system, corresponding to the totally isotropic or totally singular lines through X.

The instances in which G has rank 3 are as follows: (i) Ω is the set of all totally isotropic or totally singular points; (ii) V has Witt index 2 and Ω is the set of all totally isotropic or totally singular lines; (iii) G is $\mathrm{P\Omega}^+(8,q)$, acting on an orbit of totally singular 4–spaces; or (iv) G is $\mathrm{P\Omega}^+(10,q)$, acting on an orbit of totally singular 5–spaces. Since $\mathrm{PSp}(4,q) \cong \mathrm{P\Omega}(5,q)$ and $\mathrm{PSU}(4,q) \cong \mathrm{P\Omega}^-(6,q)$, case (ii) can be viewed as (i) except when G is $\mathrm{PSU}(5,q)$ and $n = (q^3+1)(q^2+1)$. Case (iii) can be viewed as (i) in view of triality. Case (iv) is also singled out in NATURAL_ACTION. The possibility $G \cong \mathrm{P\Omega}^+(6,q) \cong \mathrm{PSL}(4,q)$ in (i) has already been treated as $\mathrm{PSL}(4,q)$. It is straightforward to check that the degrees dealt with separately in NATURAL_ACTION only arise in the desired cases.

If G does not have rank 3, then $k > 1$. Except when G is $\mathrm{P\Omega}^+(2k,q)$ with $k \geq 6$ even, in Section 5 we saw that $G_X^{\overline{\Delta}(X)}$ is 2–transitive of degree $(q^k-1)/(q-1)$, and CLASSICAL_TS produces the set Ω' of all isotropic or totally singular points. If G is $\mathrm{P\Omega}^+(2k,q)$ with $k \geq 6$ even, then Ω^+_MAX produces the set Ω' of all isotropic or totally singular points.

Finally, when PROJECTIVE_SPACE is called for Ω' it yields the set of all 1–spaces of the underlying vector space, as required.

This completes the proof of Theorem 2.3, except for the final sentence. The crude estimate of 40 amounts to a fairly straightforward count, and is left to the reader. (The boundedness on any input of the number of calls to procedures for "basic" problems is, of course, somewhat easier to check.) The final part of the theorem has been noted repeatedly in Sections 3–6. □

In practice, point stabilizers are more time-consuming than orbit calculations (all existing algorithms use orbit computations as part of stabilizer computations). The bound at the end of Theorem 2.3 can even be met while also holding down the number of stabilizers used, for example by employing orbit computations to find elements of G that conjugate already computed stabilizers to other ones (see the remark concerning suborbits at the end of Section 2). On the other hand, the count in the theorem has to be viewed with a certain amount of suspicion. When

producing new permutation representations, many tests are needed in order to distinguish cosets; we have chosen to count these tests as all lumped together once for each new permutation representation.

7. Variations

There are many variations on the procedures presented in Sections 3–5. As mentioned in Section 2, we have chosen to avoid recursion when possible, in the sense that we have proceeded directly from the given permutation representation to one on some of the points of an underlying r–set or vector space.

However, some readers may prefer to pass successively from sets or spaces of one size to smaller ones—at least in some situations. In the case of an orbit of nonsingular k–spaces ($k > 1$) of a vector space V it may be tempting to pass to nonsingular $(k-1)$–spaces; but of course this is not possible in the symplectic case, and seems difficult in any event. On the other hand, all remaining situations of Hypothesis 2.1 can be handled in a relatively uniform manner; this resembles, and motivated, part of CLASSICAL_NS.

We leave to the reader the straightforward proof that the following *produces a correct output when G is* $\mathrm{PSL}(V)$*, or when G is a classical group acting on the set of all totally isotropic or totally singular subspaces of dimension* $\leq (d-1)/3$.

PSL+TS

Input: $G \leq \mathrm{Sym}(\Omega)$ permutation isomorphic to a primitive action of one of the following sorts, for some vector space of characteristic p:

(a) the full projective special group of the underlying vector space, in its action on the subspaces of a fixed dimension, or

(b) some simple symplectic, orthogonal or unitary group, of Witt index > 1, on the totally isotropic or totally singular subspaces of a fixed dimension of the underlying vector space.

Output: A set and an action of G on that set permutation isomorphic to that of G on the set of all 1–spaces in (a), or of all isotropic or singular 1–spaces in (b), of an underlying vector space.

If G is 2–transitive on Ω, output Ω.

Let $X \in \Omega$. Let $\Delta(X)$ be an orbit of G_X on $\Omega - \{X\}$ with $|\Delta(X)|_p$ minimal. Let $Y \in \Delta(X)$.

Let $A \in \Delta(X) - \Delta(Y)$, $Z \in \Delta(X) \cap \Delta(Y) \cap \Delta(A)$ and $y := \Delta(X) \cap \Delta^+(Y) \cap \Delta^+(Z)$.

If $y = \Delta(X) \cap \Delta^+(Y)$ then output Ω.

If $|y| < |\Delta(X) \cap \Delta^+(Y) - y|$, replace Z by an element of $\Delta(X) \cap \Delta(Y) - y$ and recompute y.

Find the block system y^{G_X}, and then G_{Xy}.

Let $g \in G$ move Y to X and $f \in G_X$ move X^g to Y.

Find $\Omega' = G/\langle G_{Xy}, gf \rangle$. Recursively replace Ω by Ω'. $\diamondsuit$

Here we have emphasized a very different orbit of G_X than used in CLASSICAL_TS (note that we could have finished as in Ω^+_MAX, using Section 8(A)). Remark 5.1 contains a similar algorithm. Another similar one can be used in place of ALT1:

ALT1′. Same input and output as ALT1.

If G is 2–transitive on Ω, output Ω.

Let $X \in \Omega$. Let $\Delta(X)$ be an orbit of G_X on $\Omega - \{X\}$ with $|\Delta(X)|$ minimal. Let $Y \in \Delta(X)$.

Let $Z \in \Delta(X) \cap \Delta(Y)$ and $y := \Delta(X) \cap \Delta^+(Y) \cap \Delta^+(Z)$. If $|y| < |\big(\Delta(X) \cap \Delta^+(Y)\big) - y|$, replace Z by an element of $\Delta(X) \cap \Delta(Y) - y$ and recompute y.

Find the block system y^{G_X}, and then G_{Xy}.

Let $g \in G$ move Y to X and $f \in G_X$ move X^g to Y.

Find $\Omega' = G/\langle G_{Xy}, gf\rangle$. Recursively replace Ω by Ω. $\diamondsuit$

It is easy to check that the output is correct when $r > 9$.

8. Vector spaces and linear algebra

The results just presented do not quite provide a vector space upon which a classical group G acts. Of course, there may not be such a vector space: a simple classical group arises as the quotient of a group of linear transformations modulo scalars, not necessarily as a group of linear transformations. While this may appear to be a relatively minor distinction, it certainly is not minor in an algorithmic setting. Namely, in addition to reconstructing a projective space and a vector space V one must also produce a group G^* of linear transformations whose quotient, modulo scalars, is G—and such that the group of permutations induced by G^* on the set of all 1–spaces of V is permutation isomorphic to that of G on the set Π constructed in NATURAL_ACTION.

All of this can be found in [Ka3], [Ma] and [Mo] in the sequential, parallel and nearly linear settings, respectively. The approach is fairly simple, and will undoubtedly also work well in practical contexts. There does not seem to be any point in reproducing those algorithms here, so we will simply outline what is involved, frequently using somewhat different methods than in [Ka3] so that the reader has more than one choice to consider. We emphasize that the methodology is straightforward and essentially very classical geometry.

Throughout this section we will assume that G is a simple classical group given as a group of permutations of a set Π in a manner permutation isomorphic to the action of G on the set of all 1–spaces of a vector space V underlying G, as in the output of PROJECTIVE_SPACE. We will identify Π with the set of these 1–spaces. We will always assume that $\dim V \geq 4$, and when $G \ncong \mathrm{PSL}(V)$ that V is a nonsingular space having Witt index > 1 (in particular, Π will never be the set of points of an odd-dimensional orthogonal space of characteristic 2).

There are a number of facets to the conversion from a permutation group to a linear group acting on a vector space. These appear in several subsections: (A) Lines; (B) Subspaces; (C) Frames; (D) Coordinates; (E) Forms; and (F) Linear transformations.

As in CLASSICAL, we may assume that the characteristic p of V is known. Unlike previous sections, members of Π will be denoted by lower case letters: they are points of V.

(A) Lines.

There are at most three G–orbits on Π. Let Ω be the unique orbit of p'–length. If $x \in \Omega$ let $\Delta(x)$ denote the shortest orbit of G_x on $\Omega - \{X\}$. Then there is a unique nontrivial block system $\overline{\Delta}(x)$ of G_x on $\Delta(x)$. Blocks have prime power size q.

The dimension of the desired vector space V is the integer d such that $|\Pi| = (q^d - 1)/(q - 1)$.

If $y \in B \in \overline{\Delta}(x)$ then $B' = (B - \{y\}) \cup \{x\}$ is in $\overline{\Delta}(y)$. Moreover, the group induced by $\langle G_{xB}, G_{yB'} \rangle$ on the set $L = B \cup \{x\}$ contains $\mathrm{PSL}(2, q)$ as a normal subgroup.

Whenever y and z are distinct points of Π, let $[y, z]$ denote the union of all G_{yz}–orbits on Π of length $< q$. This is just a *line* of our projective space. We will assume that, whenever we need a line through two points, we can quickly construct it. This could be accomplished by having access to the set of all lines; but it is probably more practical to create a lookup table consisting of the following: a representative (x, y) of each non-diagonal orbit of G on $\Pi \times \Pi$; the set $[x, y]$; and a complete set of coset representatives of G_{xy} in G.

There can be more that q orbits on $\Pi \times \Pi$. While there are fewer orbits of unordered pairs of points, moving an ordered pair to another can be accomplished easily in at most two stages (cf. CLASSICAL_NS and step **4** of PROJECTIVE_SPACE).

Assume that G is not 2–transitive on Π. Let $x \in \Omega$ and $y \in \Omega - (\{x\} \cup \Delta(x))$, and find $[x, y] \cap \Omega$. Then G is symplectic, orthogonal or unitary according to whether $|[x, y] \cap \Omega|$ is $q + 1$, 2 or $\sqrt{q} + 1$.

(B) Subspaces.

We wish to determine the *subspace spanned by any given nonempty subset* S of Π.

First suppose that G is 2–transitive on Π, so $G \cong \mathrm{PSL}(d, q)$. Construct a d–tuple $x_1 \ldots x_k$ of points, as follows. Let $x_1 \in \Pi$, and for $k = 1, \ldots, d - 1$, let x_{k+1} be any point in the longest orbit $L_{x_1 \ldots x_k}$ of $G_{x_1 \ldots x_k}$ on Π. Note that the complement of $L_{x_1 \ldots x_k}$ is just the set of all 1–spaces of the subspace spanned by $\{x_1, \ldots, x_k\}$. There are exactly $|\Pi|$ images of $\Omega - L_{x_1 \ldots x_{d-1}}$ under G, and these are the *hyperplanes* of Π: we have produced the permutation representation of G on the 1-spaces of the dual V^* of V. Now given *any* subset S of Π, there is an obvious iterative construction for the intersection $[S]$ of all the hyperplanes containing S, using at most $d - 1$ iterations; and this is the subspace spanned by S. However, this seems unnecessarily time-consuming in some situations. For example, if S

consists of the points $x_1, \ldots, x_k$ together with one further point s, then first find $[x_1, \ldots, x_k]$; if $s \notin [x_1, \ldots, x_k]$ then find an element of $G_{x_1 \ldots x_k}$ sending x_{k+1} to s and hence $[x_1, \ldots, x_{k+1}]$ to $[S]$.

Now suppose that G is not 2–transitive on Π. Once again we begin by finding hyperplanes. For $x \in \Pi$ the hyperplane $x^\perp$ is obtained as follows: within each orbit of G on Π find the shortest orbit $\neq \{x\}$ of G_x, and then let $x^\perp$ be the union of these G_x–orbits with the following exceptions:

- If $x \in \Omega$, or if G is orthogonal of characteristic 2 (cf. (A)), then include x in $x^\perp$; and
- If G is orthogonal, $q = 2$ and $|\Omega| = (2^{d/2} + 1)(2^{(d-2)/2} + 1)$, and if $x \in \Pi - \Omega$, then $x^\perp$ consists of $\{x\}$, the shortest G_x–orbit on $\Omega - \{x\}$ and the longest G_x–orbit on $\Pi - \Omega$.

It is straightforward to check that $x^\perp$ is a hyperplane of the underlying projective space. Note that there is no need to compute $x^\perp$ for each $x \in \Pi$, only one such computation is needed for each G–orbit on Π—and there are at most three such orbits.

Now if S is *any* subset of Π, first calculate $S^\perp := \cap\{s^\perp \mid s \in S\}$; then $[S] := S^{\perp\perp}$ is, once again, the subspace spanned by $[S]$.

Remarks. Note that the introduction of hyperplanes is actually easier in the case of the classical groups other than $\mathrm{PSL}(d, q)$, since hyperplanes are nicely tied to orbits of points.

Lines were used in [Ka3] in order to determine subspaces of V. This special case of (B) is given in (A) because lines are especially significant in subsections (D) and (E), and are found more easily using the method of (A) than (B).

(C) Frames.

We next construct a *frame*: a d–tuple $x_1, \ldots, x_d$ of points of Π that will span V (once we actually construct V!). Recall that we already know d.

If G is 2–transitive on Π then we have already done this in (B).

Suppose that G is not 2–transitive. Let $x_1 \in \Omega$ and $x_2 \in \Omega - x_1^\perp$, and recursively let $x_{2k+1} \in \Omega \cap \{x_1, \ldots, x_{2k}\}^\perp$ and $x_{2k+2} \in \Omega \cap \{x_1, \ldots, x_{2k}\}^\perp - x_{2k+1}^\perp$; this produces points $x_1, \ldots, x_{2m}$, where m is the Witt index of V. If $d = 2m + 1$ let x_{2m+1} be any point of $\{x_1, \ldots, x_{2m}\}^\perp$; if $d = 2m + 2$ let x_{2m+1} and x_{2m+2} be any distinct points of $\{x_1, \ldots, x_{2m}\}^\perp$. $\diamondsuit$

This constructs a frame, but in (D) we need slightly more: subspaces such as $[x_1, \ldots, x_i]$ for $i = 1, \ldots, d - 1$. These are readily obtained using (B)—and were obtained in the course of the construction when $G \cong \mathrm{PSL}(d, q)$.

(D) Coordinates.

A straightforward procedure for *introducing coordinates* is given in [Ka3, p. 372], based on [VY]. The frame in (C) and iteration are used to label *all* of the points of the subspaces $[x_1, \ldots, x_i]$ by vectors in $V := \mathrm{GF}(q)^d$ for $i = 2, \ldots, d$.

Here we wish to indicate a variant of that procedure that does not label all of the points of Π by vectors, but instead is designed to label any points one comes across in the course of *using* coordinates.

We will *label* the points of Π by those nonzero vectors of V for which *the last nonzero coordinate is* 1.

(i) *Preprocessing steps.*

For $r = 2, \ldots, d-1$, find $[x_1, \ldots, x_r]$.

For $1 \leq k \leq d$ find $X_k := [x_j \mid j \neq k]$. For $1 \leq k < m \leq d$ find $X_{km} := [x_j \mid j \neq k, m] = X_k \cap X_m$ and $X_{1km} := [x_j \mid j \neq 1, k, m] = X_1 \cap X_k \cap X_m$.

Choose $u \in \Pi - \cup_k X_k$. For $1 \leq k < m$, find $u_{1km} := [u, X_{1km}] \cap [x_1, x_k, x_m]$.

Label x_i using the ith standard basis vector of $\mathrm{GF}(q)^d$. Label u as $(1^d) = (1, \ldots, 1)$.

Coordinatize the plane $X_{(3)} = [x_1, x_2, x_3]$ using $\mathrm{GF}(q)^3 \times 0^{d-3}$ so that u_{112} and u_{123} are labeled $(1, 1, 0, 0^{d-3})$ and $(1, 1, 1, 0^{d-3})$, respectively. (For this purpose one must first introduce multiplication and addition on a set such as $[x_1, x_2] - \{x_1\}$ in order to recover a field $\mathrm{GF}(q)$ from Π; and then use it to label the points of $[x_1, x_2, x_3]$. This is a standard projective plane coordinatization; cf. [Ka4, p. 372].)

For $m > 3$ label u_{12m} as $(1, 1, 0^{m-3}, 1, 0^{d-m})$.

If $m > 2$ and $y \in [x_1, x_m] - \{x_1, x_m\}$, find the label $(b, 1, 0^{d-2})$ of $[y, u_{12m}] \cap [x_1, x_2]$, and label y as $(1 - b, 0^{m-2}, 1, 0^{d-m})$.

If $1 < k < m$ and $y \in [x_k, x_m] - \{x_k, x_m\}$, find the label $(0^{k-1}, b, 0^{m-k-1}, 1, 0^{d-m})$ of $[y, u_{1km}] \cap [x_1 x_k]$, and label y as $(0^{k-1}, 1 - b, 0^{m-k-1}, 1, 0^{d-m})$. (Now all points of $[x_k, x_m]$ have been labeled for $1 \leq k < m \leq d$.)

(ii) *Coordinatizing arbitrary points.*

Let $x \in \Pi - \{x_1\}$. Find the largest $m \geq 2$ such that $x \notin [x_1, \ldots, x_{m-1}]$.

For $k = 1, \ldots, m-1$ find the label $(0^{k-1}, a_k, 0^{m-1}, 1, 0^{d-m})$ of $[X_{km}, x] \cap [x_k, x_m]$. Let $a_m = 1$.

Label x as $(a_1, \ldots, a_m, 0^{d-m})$. $\diamondsuit$

It is straightforward to check that all of this is consistent and labels the points of Π as in linear algebra.

As far as timing is concerned, note that $d = \dim V$ is $\mathrm{O}(\log n)$. Also, q is small relative to n. Thus, while the number of computations used here is no longer bounded, this procedure is nevertheless in polynomial time (even in the parallel class NC), and should be reasonably fast in practice.

(E) Forms.

Assume that G is not 2–transitive on Π. We now *determine an alternating, symmetric, quadratic or hermitian form* on V such that (i) Ω is its set of isotropic or singular points, and (ii) the relation "$y \in x^{\perp}$" on Π corresponds to perpendicularity. A form of the desired type is unique up to multiplication by a nonzero scalar. We no longer require any group: we are merely trying to find a form that yields (i) and (ii).

Start with the frame in (C). We may assume that $x_1 = \langle e_1 \rangle$ and $x_2 = \langle f_1 \rangle$, where $(e_1, e_1) = (f_1, f_1) = 0$ and $(e_1, f_1) = 1$ (in the orthogonal case we also require that the desired quadratic form Q vanishes on x_i, $1 \le i \le 2m$).

For $1 < i \le m$ write $x_{2i-1} = \langle e_i \rangle$ and $x_{2i} = \langle f_i \rangle$; determine the scalar α such that $\langle e_1 - e_i \rangle^\perp \cap [f_1, f_i] = \langle f_1 + \alpha f_i \rangle$, and replace f_i by αf_i in order to guarantee that $(e_i, f_i) = 1$. (Of course, there are various other ways to go about rescaling f_i in order to ensure this.) This uniquely determines our form on $\langle e_1, f_1, \ldots, e_m, f_m \rangle$, by sesquilinearity.

This leaves us with the possibility that there is a point $\langle u \rangle$ in $\langle e_1, f_1, \ldots, e_m, f_m \rangle^\perp$. If d is odd then test each $\alpha \in \mathrm{GF}(q)$ in order to find one such that $\langle e_1 + \alpha f_1 + u \rangle \in \Omega$, in which case the condition $(e_1 + \alpha f_1 + u, e_1 + \alpha f_1 + u) = 0$ determines (u, u) (namely, -2α if V is orthogonal and $-\alpha - \overline{\alpha}$ if V is unitary). As above, this uniquely determines the form on V by sesquilinearity.

Suppose that $d = 2m + 2$, so that G is an orthogonal group. Choose any two points $\langle u \rangle$, $\langle v \rangle$ in $\langle e_1, f_1, \ldots, e_m, f_m \rangle^\perp$. As above, test all field elements using the conditions $\langle e_1 + \alpha f_1 + u \rangle \in \Omega$, $\langle e_1 + \alpha' f_1 + v \rangle \in \Omega$ and $\langle e_1 + \alpha'' f_1 + u + v \rangle \in \Omega$ in order to uniquely determine the values $Q(u) = -\alpha$, $Q(v) = -\alpha'$ and $Q(u+v) = -\alpha''$. This uniquely determines Q, as required. $\diamondsuit$

Note that the number of computations required here was small: $\mathrm{O}(dq)$, though not $\mathrm{O}(1)$.

Remark. In [Ka3, Section 13] part of the above was accomplished in a slightly different manner, by using the group G^* we are about to construct: G^* is a group of isometries, elements of it can be found moving $\langle u \rangle$, $\langle v \rangle$ or $\langle u + v \rangle$ into $\langle e_1, f_1, e_2, f_2 \rangle$, and this determines the form.

(F) Linear transformations.

At this point we have a vector space V, but G does not act on V. We need a group of linear transformations inducing G. We will find such a group, in fact one that is either perfect or the direct product of a copy of G with $\langle -1 \rangle$.

Let $g \in G$. Find $\langle (1^d) \rangle^g = \langle b_1, \ldots, b_d \rangle$ and $x_i^g = \langle a_{i1}, \ldots, a_{id} \rangle$ for $i = 1, \ldots, d$. Then solve the system of linear equations $\Sigma_i c_i(a_{i1}, \ldots, a_{id}) = (b_1, \ldots, b_d)$ for scalars c_i, and represent g by the matrix with rows $c_i(a_{i1}, \ldots, a_{id})$ for $i = 1, \ldots, d$.

In particular, starting with each of the generators g_k of G we obtain a matrix M_k inducing a linear transformation t_k that produces the same permutation on Π as g_k. Since G arises from matrices of determinant 1, we can multiply M_k by a scalar in order to have $\det M_k = 1$. Now let G^* be the group of linear transformations of V generated by the t_k. Then G^* is a perfect group of linear transformations inducing G on Π, except perhaps when G is orthogonal and -1 has spinor norm -1, in which case $G^* \cong G \ or \ G \times \langle -1 \rangle$. For most purposes this ambiguity is probably insignificant, but of course one could either compute the derived group or else provide a definition for the spinor norm in order to remove the possibility $G \times \langle -1 \rangle$ (e.g., using Wall forms as in [Ta, p. 163].

Once again timing considerations are straightforward since $d = \mathrm{O}(\log n)$.

9. Related questions

We have avoided dealing with exceptional groups of Lie type by starting with a suitable inequality $|G| \geq n^5$. However, it would be interesting to have analogous algorithmic results for those groups as well, under the assumption that the given permutation representation is sufficiently natural (e.g., on a class of maximal parabolic subgroups). This may even be essential if further progress is to be made using "natural" permutation representations of simple groups.

If G is an exceptional simple group of Lie type and acts primitively on an n–set Ω, then $|G| > n^4$ except in the following instances: G is $E_6(q)$ acting on a class of maximal parabolic subgroups of type $D_5(q)$; $E_7(q)$ acting on a class of maximal parabolic subgroups of type $E_6(q)$ or $D_6(q)$; or $E_8(q)$ acting on a class of maximal parabolic subgroups of type $E_7(q)$. The geometry of the permutation representation has been studied in each of these cases [Co]. If one requires only that $|G| > n^3$, then there are further parabolic permutation representations to consider, as well as exactly one non-parabolic one: $F_4(q) > B_4(q)$ [LS].

Sporadic groups also present some inconveniences. As noted earlier, if G is a Mathieu group M_n, $n = 23, 24$, then $|G| > n^5$, and there are no other occurrences of this inequality when G is sporadic. In addition, $|G| > n^4$ precisely for the following cases (cf. [Maz]): $M_{12}, n = 12$; $M_{22}, n = 22$; $Co_2, n = 2300$; $Co_3, n = 2300$; $F_{23}, n = 31671$; $F'_{24}, n = 306936$.

It is natural to ask to what extent simplicity was actually needed in previous sections. If G lies between an alternating or classical group and its automorphism group, then similar results hold, although there are a few more situations to consider (cf. [Ka2]). However, the extra effort required does not seem of sufficient value; and whenever any such result is needed, a version of our results can be deduced from the simple case studied here.

Finally, we note that there are entirely different probabilistic approaches to questions such as those dealt with in Theorem 2.3 (e.g., in [KS]). Moreover, there are algorithms in [Ka6], [Mo] and [KS] that pass directly to the vector space V from the set of isotropic or singular points, with some of the geometry in coordinatization replaced by the use of suitable p–groups.

References

[Ar] E. Artin, The orders of the classical simple groups. Comm. Pure Appl. Math. 8 (1955) 455–472.

[BKL] L. Babai, W. M. Kantor and E. M. Luks, Computational complexity and the classification of finite simple groups, pp. 162–171 in: Proc. IEEE Symp. on Foundations of Computer Science 1983.

[BLS] —, E. M. Luks and Á. Seress, Permutation groups in NC, pp. 409–420 in: Proc. ACM Symp. on Theory of Computing 1987.

[BC] W. Bosma and J. J. Cannon, Handbook of MAGMA functions. Department of Pure Mathematics, Sydney U. 1993.

[Ca] J. J. Cannon, An introduction to the group theory language Cayley, pp. 145–183 in: Computational Group Theory (Ed. M. D. Atkinson), Academic Press 1984.

[Co] A. M. Cohen, Point-line characterizations of buildings, pp. 191-206 in: Buildings and the Geometry of Diagrams: CIME Session, Como 1984 (Ed. L. A. Rosati). Springer Lecture Notes in Mathematics 1181, 1986.

[CCNPW] J. H. Conway, R. T. Curtis, S. P. Norton, R. A Parker and R. A. Wilson, Atlas of finite groups. Clarendon Press, Oxford 1985.

[CF] G. Cooperman and L. Finkelstein, Combinatorial tools for computational group theory, pp. 53–86 in: Groups and Computation (Eds. L. Finkelstein and W. M. Kantor), AMS 1993.

[Di] J. Dieudonné, La géométrie des groupes classiques. Springer, Berlin-Göttingen-Heidelberg 1963.

[FHL] M. Furst, J. Hopcroft and E. Luks, Polynomial-time algorithms for permutation groups, pp. 36–41 in: Proc. 21st I.E.E.E. Symp. Found. Comp. Sci. 1980.

[Ka1] W. M. Kantor, Permutation representations of the finite classical groups of small degree or rank. J. Algebra 60 (1979) 158-168.

[Ka2] — Algorithms for Sylow p–subgroups and solvable groups, pp. 77–90 in: Computers in Algebra (Proc. Conf. Chicago 1985), Dekker, New York 1988.

[Ka3] — Polynomial-time algorithms for finding elements of prime order and Sylow subgroups. J. Algorithms 6 (1985) 478–514.

[Ka4] — Sylow's theorem in polynomial time. J. Comp. Syst. Sci. 30 (1985) 359–394.

[Ka5] — Finding composition factors of permutation groups of degree $n < 10^6$. J. Symb. Comp. 12 (1991) 517–526.

[Ka6] — Geometry in computer algebra systems (unpublished manuscript for the 1993 London Magma Conference).

[KLM] —, E. M. Luks and P. D. Mark, Sylow subgroups in parallel (submitted).

[KS] — and Á. Seress, Black box classical groups (submitted).

[Kl] P. B. Kleidman, The maximal subgroups of the finite 8–dimensional orthogonal groups $P\Omega_8^+(q)$ and of their automorphism groups. J. Algebra 110 (1987) 173–242.

[KlLi] — and M. W. Liebeck, The subgroup structure of the finite classical groups. London Math. Soc. Lecture Note Series 129, Cambridge University Press 1990.

[LaS] V. Landazuri and G. M. Seitz, On the minimal degrees of projective representations of the finite Chevalley groups. J. Algebra 32 (1974) 418–443.

[Li] M. W. Liebeck, On the orders of maximal subgroups of the finite classical groups. Proc. London Math. Soc. 50 (1985) 426–446.

[LiS] — and J. Saxl, On the orders of maximal subgroups of the finite exceptional groups of Lie type. Proc. London Math. Soc. 55 (1987) 299–330.

[Lu1] E. M. Luks, Parallel algorithms for permutation groups and graph isomorphism, pp. 292–302 in: Proc. IEEE Symp. on the Foundations of Comp. Sci. 1986.

[Lu2] — Computing the composition factors of a permutation group in polynomial time, Combinatorica 7 (1987) 87–99.

[Lu3] — Permutation groups and polynomial time computation, pp. 139–175 in: Groups and Computation (Eds. L. Finkelstein and W. M. Kantor), AMS 1993.

[Ma] P. D. Mark, Sylow's theorem and parallel computation. Ph. D. thesis, University of Oregon 1993.

[Maz] V.D.Mazurov, A minimal permutation representation of the Thompson simple group, Algebra and Logic, 27 (1988), 350–361.

[Mo] P. G. Morje, A nearly linear time algorithm for Sylow subgroups of permutation groups. Ph.D. thesis, Ohio State U. 1995.

[Neu] P. M. Neumann, Some algorithms for computing with finite permutation groups, pp. 59–92 in: Proceedings of Groups-St. Andrews 1985 (Eds. E. F. Robertson and C. M. Campbell), London Math. Soc. Lect. Note 121, Cambridge U. Press 1987.

[PS] C. E. Praeger and J. Saxl, On the orders of primitive permutation groups. Bull. Lond. Math. Soc. 37 (1980) 303–307.

[Sch] M. Schönert *et al.*, GAP—Groups, algorithms and programming. RWTH Aachen, Lehrstuhl D für Mathematik 1994.

[Ta] D. E. Taylor, The geometry of the classical groups. Heldermann, Berlin 1992.

[VY] O. Veblen and J. W. Young, Projective geometry. Ginn, Boston 1916.

[Wi] H. Wielandt, Finite permutation groups. Academic Press, New York 1964.

University of Oregon
Eugene, OR 97403

and

University of Western Australia
Nedlands, WA 6907