Introduction to MaxDim

R. Keith Dennis and Ravi Fernando

June 21, 2017

1 Motivation

This note provides some background information on the finite group invariant MaxDim, for participants in the 2017 SPUR program at Cornell. The second author's paper [4] (based on work that began in the 2013 REU) has more details and proofs of some statements mentioned here; however, here we provide some examples and questions not discussed there.

Let G be a finite group, and recall the invariants $r(G) \leq m(G) \leq i(G)$, which respectively measure the sizes of the smallest generating sequence, the largest irredundant generating sequence, and the largest irredundant sequence in G. Before defining $\mathrm{MaxDim}(G)$, let's motivate why the invariants we already care about, particularly m and i, might have something to do with maximal subgroups.

Suppose we are interested in r, m, and i of $G = S_7$. Since G is generated by (12) and (234567)—check this if you haven't seen it before!—we have $r(G) = 2$. We also have the irredundant generating sequence $(12), (23), \ldots, (67)$, which shows that $m(G) \geq 6$. We might then suspect that $m(G) = 6$. But it's not clear why there can't be an irredundant generating set of length 7,[1] and it's far too computationally expensive to check all $\binom{7!}{7}$ candidates. We need a better way.

Notice that a subset of G generates G if and only if it isn't contained in any proper subgroup. So any 7-element irredundant generating set $\{g_1, \ldots, g_7\}$ has the property that each 6-element subset $\{g_j : j \neq i\}$ is contained in a proper subgroup $H_i < G$. We can even enlarge these H_i to maximal subgroups M_i, while keeping the property that each M_i contains all of the g_j except for g_i. Then to search for irredundant generating sequences $\{g_i\}$, it suffices to search through large families of maximal subgroups $\{M_i\}$, look for elements $g_i \in \cap_{j \neq i} M_j$, and check whether the g_i generate G.

Crucially, there aren't too many maximal subgroups of G, and we can understand them all reasonably well: all of them are conjugate to either A_7 (order 2520), S_6 (order 720), $S_5 \times S_2$ (order 240), $S_4 \times S_3$ (order 144), or $(\mathbb{Z}/7\mathbb{Z}) \rtimes (\mathbb{Z}/7\mathbb{Z})^\times$ (order 42). (This isn't obvious to a human—at

[1] In fact, one may wonder whether the irredundant generating sequences could "skip" length 7 but reappear at some larger number. Fortunately, Tarski's theorem prevents this.

least not any human I know—but a computer algebra system like GAP or Magma can calculate it very quickly.) We would then show that the last of these is too small to occur as an M_i, by showing that the chain of subgroups $G > M_{i_1} > M_{i_1} \cap M_{i_2} > M_{i_1} \cap M_{i_2} \cap M_{i_3} > \cdots$ is strictly decreasing for any choice of indices. (This is easier than it looks: just look at which of these subgroups contain each g_i.) Finally, we would examine how the remaining maximal subgroups can intersect with each other, and eventually show that a length-7 irredundant generating sequence cannot exist. The conceptual overhead of looking at 7-tuples of maximal subgroups instead of 7-tuples of elements pays off in the fact that there are far fewer of the former than the latter, and what was previously an intractable calculation has become potentially doable. In fact, this approach is essentially the best general-purpose method we have to compute m of a finite group.

If we were Julius Whiston in 2000, we would apply the same approach to all S_n, using the O'Nan-Scott theorem to classify the maximal subgroups of S_n. We would rule out the "small" cases (which depend on the classification of finite simple groups!), and examine the rest, using strong induction on n, to show that $m(S_n)$ is $n-1$ and no greater. We would even show more in the process: that $i(S_n) = n-1$, that $m(A_n) = n-2$, and that every irredundant set in S_n of maximal size actually generates the group.

2 Definition and basic properties

We will now formalize the discussion of the subgroups M_i in the preceding example (or H_i, since maximality isn't needed in the definition), and then explain the precise connection to $m(G)$ and $i(G)$ and the role of the elements g_i.

Definition and Lemma 1. We say that a family of subgroups $H_i \leq G$, indexed by a set S, is in *general position* if it satisfies either of the following equivalent conditions:

1. Whenever $\cap_{i\in I} H_i = \cap_{j \in J} H_j$ for $I, J \subseteq S$, we have $I = J$.

2. For every $i \in S$, the intersection $\cap_{j \neq i} H_j$ properly contains $\cap_{j \in S} H_j$.

We let $\mathrm{MaxDim}(G)$ denote the size of the largest family of maximal subgroups of G in general position.

Proof. To show that (1) implies (2), simply take $I = S$ and $J = S \setminus \{i\}$. To show the reverse implication (by contrapositive), suppose we are given $I \neq J \subseteq S$ violating (1), and take $i \in I \setminus J$ without loss of generality. Then we have $\cap_{i \in I} H_i = \cap_{j\in J} H_j$, so

$$\cap_{j \in I \cup J} H_j = \cap_{j \in J} H_j = \cap_{j \in J \cup I \setminus \{i\}} H_j. \tag{1}$$

Intersecting both sides with all H_k for $k \notin I \cup J$ yields $\cap_{j \neq i} H_j = \cap_{\text{all } j} H_j$, contradicting (2). □

Exercise 1. Interpret $\mathrm{MaxDim}((\mathbb{Z}/p\mathbb{Z})^n)$ in terms of linear algebra over $\mathbb{F}_p$, and show that $r = m = i = \mathrm{MaxDim} = n$ for this group.

Now let $(g_1, \ldots, g_n)$ be an irredundant generating sequence of a group G. For each i, let $H_i = \langle g_j : j \neq i \rangle$. Since H_i is a proper subgroup of G, it is contained in some maximal subgroup

M_i. We must have $g_i \notin M_i$, since otherwise M_i contains $\langle g_1, \ldots, g_n \rangle = G$. It follows that the intersection of all M_i contains none of the g_i, while the intersection of any $n-1$ of them contains exactly one g_i. In particular, using criterion (2) above, we have shown that the M_i are in general position. (The same argument applies to the H_i.) Thus, any length-n irredundant generating sequence of a finite group G gives rise to at least one family of n maximal subgroups of G in general position. We have shown:

Proposition 2. *For finite G, we have $m(G) \leq \mathrm{MaxDim}(G)$.*

Next, we might ask whether the correspondence can be reversed. That is, given a family of maximal subgroups of G in general position, can we recover an irredundant generating sequence of the same length? This is not generally possible; in fact, we will see soon that $\mathrm{MaxDim}(G)$ can be strictly greater than $m(G)$. However, we can always recover some irredundant (but not necessarily generating) sequence of the same length, which implies:

Proposition 3. *For finite G, we have $\mathrm{MaxDim}(G) \leq i(G)$.*

Proof. Let $(M_i)_{1 \leq i \leq n}$ be a family of subgroups in general position; they need not even be maximal. By condition (2) of the definition of general position, we can choose elements $g_i \in (\cap_{j \neq i} M_j) \setminus M_i$ for each i. By construction, we have $g_j \in M_i$ if and only if $j \neq i$. So for every i, the subgroup $\langle g_j : j \neq i \rangle$ is contained in M_i and $\langle \text{all } g_j \rangle$ is not, so the elements $g_1, \ldots, g_n$ form an irredundant sequence. Taking $n = \mathrm{MaxDim}(G)$ gives the result. □

In summary, we have $r(G) \leq m(G) \leq \mathrm{MaxDim}(G) \leq i(G)$ for all finite groups G.

Remark 4. Suppose we have a family of subgroups $(H_i)_{i \in S}$ and a family $(g_j)_{j \in S}$ of elements of G indexed by the same set S, and suppose that $g_j \in H_i$ holds exactly when $j \neq i$. Then the argument of Proposition 2 shows that the H_i are in general position. In this case, we say that the g_j *certify* that the H_i are in general position. We can summarize the last two results as saying that every irredundant generating sequence certifies a family of subgroups in general position (which we can choose to be maximal), and every such family is certified by some irredundant sequence.

The MaxDim viewpoint is quite fruitful for calculating m, both theoretically (as in Whiston's theorem) and computationally. Gabe Frieden has written a program in GAP using this idea: it finds all maximal subgroups of G, looks for large families of them in general position, and then checks whether any of these are certified by an irredundant generating sequence.

Exercise 2. Show that $m(G) = \mathrm{MaxDim}(G) = i(G)$ for finite abelian groups G.

Exercise 3. Let G be a finite p-group. Then an exercise (6.1.26a) in Dummit & Foote shows that $G/\Phi(G) \cong (\mathbb{Z}/p\mathbb{Z})^n$ for some n. Show that $r(G) = m(G) = \mathrm{MaxDim}(G) = n$, and conclude that $r = m = \mathrm{MaxDim}$ for all finite nilpotent groups. (Reduce to Exercise 1 by showing that all three invariants are insensitive to modding out by $\Phi(G)$.[2] A finite nilpotent group is the direct product of its Sylow subgroups.) On the other hand, show that $i(G)$ need not equal the rest even for nilpotent groups. In particular, setting $G = (\mathbb{Z}/p\mathbb{Z})^p \rtimes (\mathbb{Z}/p\mathbb{Z})$, where $\mathbb{Z}/p\mathbb{Z}$ acts

[2] Your argument should show moreover that every family of n maximal subgroups of G in general position intersects in exactly $\Phi(G)$.

by cyclically permuting the p factors on the left, show that $r(G) = m(G) = \mathrm{MaxDim}(G) = 2$, but $i(G) = p$. The point is that your length-p irredundant sequence will necessarily live in a subgroup "deep inside" G, and adding anything outside of this will cause lots of redundancy.

The equality $\mathrm{MaxDim}(G) = m(G)$ does not hold for all finite groups, or even all solvable groups. However, we show in [4] that it is true for finite supersolvable groups, a class of groups lying between nilpotent and solvable groups.

Question 1. Are there other interesting classes of groups for which $\mathrm{MaxDim}(G) = m(G)$? What about the stronger condition that $m(G) = i(G)$, or that every family of maximal subgroups in general position is certified by a generating sequence?

3 Groups where $\mathrm{MaxDim} > m$

In practice, MaxDim seems to behave more like m than i, and it is surprisingly difficult to find a group G where they are not equal. (Indeed, we know from computations that the smallest group with $\mathrm{MaxDim} > m$ has order 720. In GAP's SmallGroups library, it is identified as `SmallGroup(720, 774)`.) In [4], we discuss a family of finite groups $G = A_5 \wr (\mathbb{Z}/p\mathbb{Z})$, p a prime, where $m(G) \leq 5$ but $\mathrm{MaxDim}(G) \geq 2p$ grows without bound as $p \to \infty$. Detomi and Lucchini [2] have since found similar behavior in a family of solvable groups. Instead of retelling those stories here, we'll describe the first known counterexample, which Gabe Frieden discovered computationally in the 2011 REU. This example is nice because it has a very hands-on interpretation in terms of finite projective geometry, which allows us to see concretely how a family of maximal subgroups in general position can fail to come from an irredundant generating set.

3.1 Gabe Frieden's example

Consider the simple group $\mathrm{PSL}(3, 2)$ of order 168, which acts as the symmetries of the Fano plane $P = \mathbb{P}^2(\mathbb{F}_2)$. Let G be the wreath product $\mathrm{PSL}(3, 2) \wr (\mathbb{Z}/2\mathbb{Z})$; this is the symmetry group of the disjoint union of two Fano planes $P \cup Q$. (We are allowed to apply any two symmetries to the two planes separately, and to switch them with each other, so $|G| = 168^2 \cdot 2 = 56448$.) We will show that G has a set of six maximal subgroups in general position that are not certified by any generating set.

Let's recall some things about the Fano plane and its symmetries. As a projective plane, its "points" are the lines (one-dimensional linear subspaces) in $\mathbb{F}_2^3$, and its "lines" are the two-dimensional linear subspaces. Equivalently, its points are the equivalence classes of nonzero vectors in $\mathbb{F}_2^3$ under nonzero scalar multiplication (which is trivial, because the only nonzero scalar is 1), and its lines are the sets of three nonzero points that lie in a common plane. A symmetry (or automorphism) of P is defined to be any permutation of the seven points that sends lines to lines.

You can check that P contains seven points and seven lines; each line contains three points; each point lies on three lines; there is a unique line connecting any two points, there is a unique point of intersection of any two lines, and so on.[3] By linear algebra, there exists a unique symmetry of P sending any basis (i.e. set of three points whose corresponding linear subspaces are linearly independent) to any other basis. In particular, $\mathrm{Aut}(P)$ acts 2-transitively, and almost 3-transitively: any ordered triple of non-collinear points can be sent to any other. A nice example of this is if we decide to fix two points on the "line at infinity" (thus all three of them, namely the three nonzero points $[a : b : 0]$ in projective coordinates): we still have four symmetries, acting on the "affine part" of P (i.e. the four points $[a : b : 1]$) by translations in the (a, b)-plane.

We now construct our six maximal subgroups of G. Choose one point p in our first plane P, and three non-collinear points p_1, p_2, p_3 in Q. Dually, choose one line ℓ in Q, and three lines ℓ_1, ℓ_2, ℓ_3 in P not passing through a common point. For $i = 1, 2, 3$, we let $H_i < G$ be the subgroup preserving the set $\{p, p_i\}$, and let $K_i < G$ preserve $\{\ell, \ell_i\}$. So for example an element in H_1 must either fix both p and p_1, or swap the two planes while sending p and p_1 to each other.

Exercise 4. Show that the H_i and K_i are maximal subgroups of G. You will probably need some transitivity properties of $\mathrm{PSL}(3, 2)$ acting on P and Q.

We claim that the intersection of all six subgroups is trivial, but that the intersection of any five is nontrivial. To prove this, note that any element $g \in (H_1 \cap H_2 \cap \cdots)$ must fix $\{p, p_1\}$ and $\{p, p_2\}$, so it fixes p and in particular doesn't swap P and Q. Then g must also fix all three p_i, which forces it to fix Q pointwise. A similar argument with the K_i forces g to fix P pointwise, so $g = 1$.

On the other hand, suppose we intersect all but K_3. This forces us to fix Q pointwise, as well as fixing p and fixing ℓ_1 and ℓ_2 each setwise. Then we must fix the intersection point $p' = \ell_1.\ell_2$, so we fix every point on the line $\ell' = \overline{pp'}$. (I'm ignoring the case $p' = p$, which is easier.) But if we choose coordinates so that ℓ' is the line at infinity, then we can take g to be one of the transpositions from earlier, namely the one parallel to the lines ℓ_1 and ℓ_2. (You may want to draw a picture if you haven't already!) The dual argument works for intersecting all but one of the H_i; this is left as an exercise.

So we've shown that the six subgroups are in general position. But the five-fold intersections are very small; in particular, just by intersecting two of the H_i or two of the K_i, we already get an intersection contained in the index-2 subgroup $(\mathrm{PSL}(3, 2))^2$. So if $\{g_i\}$ is any set certifying that they are in general position, then all $g_i \in (\mathrm{PSL}(3, 2))^2$, so they cannot be a generating set.

We haven't actually proved that $m(G) < 6$, since there could be other sets of six maximal subgroups in general position. But in fact we know computationally that $m(G) = 5$ and $\mathrm{MaxDim}(G) = 6$.

Question 2. Can we say something interesting about generating sequences of other groups

[3] The symmetry between these statements is not a coincidence. In fact, the points and lines are dual to each other: if we define a new plane $P^\vee$ by declaring its points to be the lines of P, declaring its lines to be the points of P, and saying that ℓ lies on p in $P^\vee$ if and only if p lies on ℓ in P, then $P^\vee$ is isomorphic to P.

(e.g. $\mathrm{PSL}(3,p)$, $\mathrm{PSL}(n,q)$, their wreath products with $\mathbb{Z}/2\mathbb{Z}$, etc.) using similar geometric arguments?

The case of $G = \mathrm{PSL}(3,p)$ seems most accessible. In this case, with $p \neq 2$ prime, we can write down some explicit maximal subgroups (stabilizers of certain points and lines) that show $\mathrm{MaxDim}(G) \geq 5$. It might be possible to compute the exact value—is it always 5?—and then say something about $m(G)$ and $i(G)$.

4 Other questions

In the spirit of understanding groups in terms of their Jordan-Hölder decompositions, it would be good to understand how $r(G), m(G), \mathrm{MaxDim}(G), i(G)$, and so on behave for finite simple groups, and how they transform in extensions. The simplest open problem in this direction, and the most embarrassing to not have an answer to, seems to be the following:

Question 3. Is $\mathrm{MaxDim}(G \times H) = \mathrm{MaxDim}(G) + \mathrm{MaxDim}(H)$?

The behavior of r, m, and i under direct products is well-understood, the latter two being additive. For MaxDim, we have $\mathrm{MaxDim}(G \times H) \geq \mathrm{MaxDim}(G) + \mathrm{MaxDim}(H)$ by considering maximal subgroups of the form $M \times H$ and $G \times N$, with $M < G$ and $N < H$ maximal. In the case where G and H are relatively prime (no nontrivial quotients in common), every maximal subgroup of $G \times H$ has this form, so $\mathrm{MaxDim}(G \times H) = \mathrm{MaxDim}(G) + \mathrm{MaxDim}(H)$.

More generally, the subgroups (and thus the maximal subgroups) of $G \times H$ are classified by Goursat's lemma. (Thévenaz, [7], gives an exposition of this and proves some more general statements.) The maximal subgroups come in two flavors: the "standard" ones described above, and some "diagonal" ones. To construct the latter, suppose we have surjective homomorphisms $\varphi : G \to S$ and $\psi : H \to S$, where S is some group. Then we get a subgroup $M = \{(g,h) \in G \times H : \varphi(g) = \psi(h)\}$, which is maximal if and only if S is simple. So for example if $G = H$ is already a simple group, then taking $S = G$ and $\psi = \mathrm{id}$ gives the twisted diagonal subgroup $\{(g, \varphi(g)) \in G \times G\}$ for each automorphism $\varphi \in \mathrm{Aut}(G)$. These are all of the nonstandard maximal subgroups of $G \times G$ for G simple.

To produce a counterexample to the desired equality, we would need to fit at least one of these diagonal subgroups into a large family of maximals in general position. This seems difficult, partly because the diagonal subgroups tend to be much smaller than the standard ones, and partly because the diagonals may intersect each other in unpredictable ways.

More ambitiously, we might ask:

Question 4. What can be said about m, MaxDim, etc. of a semidirect product? A wreath product? A non-split extension?

On the simple groups side, most of what we know depends on the classification of finite simple groups, which makes things necessarily complicated. It is known that all finite simple groups satisfy $r(G) = 2$ (except those for which $r(G) = 1$!), and even some stronger properties such as so-called $\frac{3}{2}$-generation. (A group G is $\frac{3}{2}$-generated if for all $g \neq 1$, there exists h such that $G = \langle g, h \rangle$.)

But not much is known in general about the other invariants. As far as we are aware, $m(G)$ is known for three infinite families of finite simple groups: $m(\mathbb{Z}/p\mathbb{Z}) = 1$ (trivial); $m(A_n) = n - 2$ (Whiston, [8]); and $m(\mathrm{PSL}(2,p)) = 4$ for $p = 7, 11, 19, 31$, and 3 for other $p > 3$ (Jambor, [5], building on work of Nachman and others). We also have a list of $m(G)$ for all simple groups of order < 126000. Still, there are vast areas of the classification that haven't been touched. It may be possible, for example, to understand the generating sets of some more of the groups $\mathrm{PSL}(n,q)$, other classical groups of Lie type, or some sporadic groups.

Question 5. How do m, MaxDim, and i behave for (some classes of) finite simple groups? For example, are they all equal?

References

[1] Daniel J. Collins, *Generating Sequences of Finite Groups*, 2013.

[2] Eloisa Detomi and Andrea Lucchini, *Maximal subgroups of finite soluble groups in general position*, 2015. Available at `https://arxiv.org/abs/1502.06840`.

[3] David S. Dummit and Richard M. Foote, *Abstract Algebra, Third Edition*, 2004.

[4] Ravi Fernando, *On an Inequality of Dimension-like Invariants for Finite Groups*, 2015. Available at `https://arxiv.org/abs/1502.00360`.

[5] Sebastian Jambor, *The minimal generating sets of PSL(2, p) of size four*, 2013.

[6] Benjamin Nachman, *Generating Sequences of PSL(2, p)*, 2012. Available at `https://arxiv.org/abs/1210.2073`.

[7] Jacques Thévenaz, *Maximal subgroups of direct products*, 1997. Available at `https://arxiv.org/abs/math/9703201`.

[8] Julius Whiston, *Maximal Independent Generating Sets of the Symmetric Group*, 2000.