9-1992

Divisibility by |G| for Powers of Ordered k-sets

Jeffery Vanderkam
Duke University

DIVISIBILITY BY $|G|$ FOR POWERS OF ORDERED k-SETS

Jeffrey M. Vanderkam

MS TR 92-09

September 1992

Department of Mathematics
Rose-Hulman Institute of Technology
Terre Haute, IN 47803

FAX(812) 877-3198 Phone: (812) 877-8391

Divisibility by $|G|$ for powers of ordered k-sets

Jeffrey M. Vanderkam*

September 16, 1992

Abstract

It is shown that the number of ordered k-sets of a group G whose nth power contains exactly i elements is always a multiple of $|G|$. An elementary proof of the fact that the number of ordered pairs (x, y) such that $x^2 = y^2$ is equal to $k_r|G|$ is also given.

1 Motivation

We define the nth power of an ordered k-set $X = (x_1, \ldots, x_k)$ to be the set $Y = \{x_{i_1} \cdots x_{i_n} \mid x_{i_1}, \ldots, x_{i_n} \in X\}$, where the x_i's need not be distinct. We say that the nth power of X has i elements if $|Y| = i$. While working with cubing ordered pairs and squaring ordered triples, it became apparent that the number of pairs/triples/etc. whose nth power had exactly i elements was always a multiple of the order of the group. It is known [1] that the number of ordered pairs whose square has i elements is always a multiple of the order of the group, but the proof of this uses character theory to show that the number of pairs (x, y) for which $x^2 = y^2$ is a multiple of the order of the group, and does not generalize to larger k-sets or higher powers in any simple fashion. This paper contains an elementary proof of the result that had required character theory as well as a generalization of the entire result to nth powers of ordered k-sets.

*Supported by NSF grant NSF-DMS 9100509.

2 Counting elements with equal squares

Theorem 1 *The number of ordered pairs (x, y) with $x, y \in G$ and $x^2 = y^2$ is equal to $k_r|G|$, where k_r is the number of real conjugacy classes in G.*

PROOF: For notational purposes, we say that a pair (x, y) "works" for q if $q = y^{-1}x$ and $x^2 = y^2$. The strategy for this proof will be to fix an element q, and show that the number of ordered pairs (x, y) which work for q equals $|C(q)|$ if, and only if, q is in a real conjugacy class, and otherwise it must equal zero. Any q for which there is at least one such ordered pair (x, y) must be in a real conjugacy class, because $x^2 = y^2$ implies $q = y^{-1}x = yx^{-1} = yx^{-1}yy^{-1} = y(y^{-1}x)^{-1}y^{-1} = yq^{-1}y^{-1}$. Once this is proven, the proof will be complete, because then the total number of pairs (x, y) such that $x^2 = y^2$ will be equal to

$$\begin{aligned}
\sum_{q \in G} \text{number of pairs working for } q &= \sum_{q \in RC} |C(q)| \\
&= \sum_{RC} |C(q)|(|G|/|C(q)|) \\
&= \sum_{RC} |G| \\
&= k_r|G|,
\end{aligned}$$

where RC denotes the set of real conjugacy classes, $q \in RC$ denotes those elements which are in a real conjugacy class, and $k_r = |RC|$. The proof has three steps:

1. There exists at least one ordered pair (x, y) for a fixed q in a real conjugacy class.

2. If (x, y) works for q, then so does (cx, cy), where $c \in C(q)$.

3. If (x, y) and (a, b) both work for q, then $a = kx$ and $b = ky$, where $k \in C(q)$.

Now we prove them, in the same order as proposed.

1. Since q is in a real conjugacy class, there exists a y such that $q = yq^{-1}y^{-1}$. We pick $x = yq$. Then $y^{-1}x = y^{-1}yq = q$, and

$$\begin{aligned} x^2 &= yqyq \\ &= yyq^{-1}y^{-1}yq \\ &= y^2 \end{aligned}$$

so the pair (x, y) works for q.

2. Say (x, y) works for q, and $c \in C(q)$. Then $(cy)^{-1}(cx) = y^{-1}c^{-1}cx = y^{-1}x = q$, and $cxcx = cyy^{-1}xcx = cycy^{-1}x^2 = cycy^{-1}y^2 = cycy$, as desired. Thus (cx, cy) works for q as well.

3. Say (x, y) and (a, b) both work for q. Certainly there exists a k such that $a = kx$, and certainly there exists a z such that $b = kz$. First we show that $z = y$, then we show that $k \in C(q)$. Now $y^{-1}x = q = b^{-1}a = (kz)^{-1}(kx) = z^{-1}x$, so we have $z = y$. Now we also know that $a^2 = b^2$, so we may write $kxkx = kyky \Rightarrow xkx = yky \Rightarrow y^{-1}xk = kyx^{-1} \Rightarrow y^{-1}x = k(yx^{-1})k^{-1}$. But since $y^2 = x^2$, we know that $yx^{-1} = y^{-1}x$, so we may rewrite this last equation as $y^{-1}x = k(y^{-1}x)k^{-1}$, implying that k commutes with $y^{-1}x$, so $k \in C(q)$.

Since we have shown that the number of pairs (x, y) which work for q is a multiple of $|C(q)|$, the proof is complete. •

3 Divisibility by $|G|$ for all powers

Theorem 2 *The number of ordered k-sets of a group whose n^{th} power has exactly i elements is divisible by the order of the group.*

PROOF: For the sake of notation, we refer to the ordered k-set as a vector with k components: $X = (x_1, \ldots, x_k)$. The elements of the nth power of the k-set must all have the form $x_{i_1} x_{i_2} \ldots x_{i_n}$, where the i's are all integers between 1 and k (not necessarily distinct). We refer to the elements of the nth power of the k-set as an ordered tuple $Y = (y_1, \ldots, y_{k^n})$, rather than as a set, with the understanding that some of the y_i's may also not be distinct. To keep a fixed order on the y_i's, we assign them in lexiographic order by subscripts, that is, $y_1 = x_1^n$, $y_2 = x_1^{n-1} x_2$, and so on up to $y_{k^n} = x_k^n$. As an example, if we are squaring the ordered pair (x_1, x_2), then $(y_1, y_2, y_3, y_4) = (x_1^2, x_1 x_2, x_2 x_1, x_2^2)$, in that order. We consider the $(k^n(k^n-1)/2)$-tuple $S = (y_i y_j^{-1} | j > i)$, where again we put the elements in lexiographical order by subscripts: the first element is $y_1 y_2^{-1}$, and so on. In the same example, we would then have $S = (x_1^2(x_1x_2)^{-1}, x_1^2(x_2x_1)^{-1}, x_1^2(x_2^2)^{-1}, x_1x_2(x_2x_1)^{-1}, x_1x_2(x_2^2)^{-1}, x_2x_1(x_2^2)^{-1})$. Clearly, if all the y_i's are distinct, no element in S is equal to the identity. In addition, the location and frequency of the identity element in S completely determine which elements among the y_i's are equal (and thus, how many distinct elements there are in the nth power of the ordered k-set). We introduce a new array of elements $q_{s,t} = x_s^t x_{s+1}^{-t}$, and another array $r_{s,t} = x_s^{-t} x_{s+1}^t$, for s ranging from 1 to $(k-1)$ and t ranging from 1 to v, where v is to be assigned. The purpose of these is as follows:

Lemma 1 *If $c \in C(q_{s,t})$ for all s and all $t \leq v$, then c commutes with any product of the form $x_{i_1} x_{i_2} \cdots x_{i_w} x_{i_{w+1}}^{-1} \cdots x_{i_{2w}}^{-1}$, where $w \leq v$.*

PROOF: First we note that c must in fact commute with $x_i^t x_j^{-t}$ for any i, j, for any $t \leq v$ since if $i < j$, then $x_i^t x_j^{-t} = (x_i^t x_{i+1}^{-t})(x_{i+1}^t x_{i+2}^{-t}) \cdots (x_{j-1}^t x_j^{-t})$, all of which commute with c, and if $i > j$, then the same argument shows that c commutes with $x_j^t x_i^{-t}$, and thus with $x_i^t x_j^{-t}$. Thus it suffices to write the product in the lemma as

$$x_{i_1} \cdots x_{i_{2w}}^{-1} = (x_{i_1} x_{i_2}^{-1})(x_{i_2}^2 x_{i_3}^{-2}) \cdots (x_{i_w}^w x_{i_{w+1}}^{-w})(x_{i_{w+1}}^{w-1} x_{i_{w+2}}^{1-w}) \cdots (x_{i_{2w-1}} x_{i_{2w}}^{-1}),$$

a product which commutes with c. •

Similarly, we also have

Lemma 2 *If $c \in C(r_{s,t})$ for all s and all $t \leq v$, then c commutes with any product of the form $x_{i_1}^{-1} x_{i_2}^{-1} \cdots x_{i_w}^{-1} x_{i_{w+1}} \cdots x_{i_{2w}}$, with $w \leq v$.*

We also define $\overline{C}$ to be the intersection of all of the $C(q_{s,t})$'s and the $C(r_{s,t})$'s, and note that if $c \in \overline{C}$, then c satisfies the conditions of Lemmas 1 and 2. With the notation out of the way, we may proceed with the proof. We wish to show that the number of ordered k-sets which yield a given subsequence of identity elements in S is a multiple of the order of the group. This is actually a more general result than that stated in Theorem 2, since two different sequences of identity elements could easily yield the same number of distinct y_i's. To prove this more general result, we will show that the number of ordered k-sets which yield a given value for $q_{1,1}$ as well as a fixed sequence of identity elements in S is always a multiple of $|C(q_{1,1})|$. This will complete the proof, since any conjugate of the given value of $q_{1,1}$ will have the same number of ordered k-sets that yield the given sequence of identity elements in S (for all i, just conjugate x_i by the same element $q_{1,1}$ had been conjugated by), so the total number of ordered k-sets yielding that sequence and with a $q_{1,1}$ conjugate to the original $q_{1,1}$ is a multiple of $|C(q_{1,1})|[G : C(q_{1,1})] = |G|$. Summing over all conjugacy classes then shows that the total number of ordered k-sets yielding that sequence of identity elements in S is also a multiple of the order of the group, as desired.

With all this in mind, we fix a sequence of identity elements in S and fix values not just for $q_{1,1}$ but also for $q_{s,t}$ and $r_{s,t}$ for all s and all t up to v, where $n = 2v$ or $n = 2v + 1$ (depending on the parity of n). Our goal will be first to show that the number of ordered k-sets X which yield the given values for all the q's and r's as well as the given sequence of identity elements in S is a multiple of $|\overline{C}|$. We will prove this by showing that, if we choose any $c \in \overline{C}$, then

1. the q's and the r's are fixed when we send X to cX, and

2. the ordered set X yields the identity for a specific element in S if, and only if, cX does as well.

First we prove part (1). This, just like everything else in this proof, will consist only of eliminating a c and a c^{-1} every time they appear on opposite sides of an expression of the form given in the first Lemma.

$$\begin{aligned}(cx_s)^t(cx_{s+1})^{-t} &= cx_s \cdots cx_s(cx_{s+1})^{-1} \cdots (cx_{s+1})^{-1} \\ &= cx_s \cdots cx_s x_{s+1}^{-1}c^{-1} \cdots x_{s+1}^{-1}c^{-1} \\ &= x_s^t x_{s+1}^{-t}.\end{aligned}$$

We could make this last step because conjugating $x_s^m x_{s+1}^{-m}$ with c does not change its value for any $m \leq v$, so that none of the c's changed the value of the expression. The argument that the $r_{s,t}$ values are also fixed proceeds in exactly the same manner.

Now we prove part (2). First we must show that if an element in the S created by X is the identity, then that same element in the S created by cX is also the identity. Let that element be written as $x_{i_1} \cdots x_{i_n} x_{i_{n+1}}^{-1} \cdots x_{i_{2n}}^{-1}$. The element we wish to show equal to the identity can then be written as $(cx_{i_1}) \cdots (cx_{i_n})(cx_{i_{n+1}})^{-1} \cdots (cx_{i_{2n}})^{-1}$. Again we may make repeated use of Lemma 1, since in the middle of this expression we find the product $cx_{i_n}x_{i_{n+1}}^{-1}c^{-1}$, which we know to equal $x_{i_n}x_{i_{n+1}}^{-1}$. But upon eliminating this innermost c and c^{-1}, we find that the new innermost c and c^{-1} are in the product $cx_{i_{n-1}}x_{i_n}x_{i_{n+1}}^{-1}x_{i_{n+2}}^{-1}c^{-1}$. Again using Lemma 1, we see that we may cancel the c and the c^{-1}. We may repeat this process until there are $2v+2$ elements between the innermost c and c^{-1}, at which point we can no longer use Lemma 1 to cancel the c and the c^{-1}. At this point the element which we wish to show equals the identity can be written as

$$cx_{i_1} \cdots c(x_{i_{n-v}}x_{i_{n-v+1}} \cdots x_{i_n}x_{i_{n+1}}^{-1} \cdots x_{i_{n+v}}^{-1}x_{i_{n+v+1}}^{-1})c^{-1} \cdots x_{i_{2n}}^{-1}c^{-1}.$$

But we may replace the product between the innermost c and c^{-1} with a shorter product, since

$$x_{i_1} \cdots x_{i_n} x_{i_{n+1}}^{-1} \cdots x_{i_{2n}}^{-1} = e$$

implies that

$$x_{i_{n-v}} \cdots x_{i_n} x_{i_{n+1}}^{-1} \cdots x_{i_{n+v+1}}^{-1} = x_{i_{n-v-1}}^{-1} \cdots x_{i_1}^{-1} x_{i_{2n}} \cdots x_{i_{n+v+2}}.$$

As a result, we may write the element of S as

$$cx_{i_1} \cdots cx_{i_{n-v-1}} c(x_{i_{n-v-1}}^{-1} \cdots x_{i_1}^{-1} x_{i_{2n}} \cdots x_{i_{n+v+2}}) c^{-1} x_{i_{n+v+2}}^{-1} c^{-1} \cdots x_{i_{2n}}^{-1} c^{-1}.$$

But now we again have either a product of $2v$ elements or $(2v-2)$ elements (depending on the parity of n) in the middle of the expression. Since this product is of the form of the product in Lemma 2, c commutes with it, so we may cancel the innermost c and c^{-1}. But then we are also able to cancel both $x_{i_{n-v-1}}$ and $x_{i_{n+v+2}}$ with their inverses, meaning that we now have a $(2v-2)$-tuple or a $(2v-4)$-tuple between the innermost c and c^{-1}. Repeating the process, we see that we may continue eliminating c's and cancelling until we reduce all the way to the identity, which was what we wanted.

This argument also implies that if the ordered k-set cX yields the identity for a specific element in S, then so does the ordered k-set X, since we can just consider the ordered k-set $c^{-1}cX$. Thus we have proven that the number of ordered k-sets that work for the given q's and r's is in fact a multiple of $|\overline{C}|$.

To finish the proof, we note that the number of ordered k-sets that work for a given set of q's and r's is equal to the number that work for the same $q_{1,1}$ but with all the other q's and r's conjugated by any element in the centralizer of $q_{1,1}$, since we may just conjugate each x_i by the same element. The number of different sets of q's and r's we may get in this fashion is just equal to the number of elements in the centralizer of $q_{1,1}$ divided by $|\overline{C}|$ (since the number of elements in $C(q_{1,1})$ that fix all of the q's and r's upon conjugation is equal to $|\overline{C}|$). But the number of ordered

k-sets that work for any given collection of q's and r's is just a multiple of $|\overline{C}|$, and we may take advantage of as follows. We count the number of ordered k-sets X which

- yield the fixed sequence of identity elements in S, and
- either yield the original q's and r's or yield instead $aq_{s,t}a^{-1}$ and $ar_{s,t}a^{-1}$, where a is an element in $C(q_{1,1})$.

This total is just (number of X for original q's and r's)(number of distinct conjugates over $C(q_{1,1})$ of the original $q_{s,t}$'s and $r_{s,t}$'s), which we may write as $(k_q|\overline{C}|)(|C(q_{1,1})|/|\overline{C}|) = k_q|C(q_{1,1})|$, where k_q is an integer. The total number of ordered k-sets which fix the sequence of identities in S and the value of $q_{1,1}$ can be counted by totalling over conjugacy classes of possible q's and r's, and as we have just shown, the count for any one of these conjugacy classes is a multiple of $|C(q_{1,1})|$. The total number of ordered k-sets that have a given sequence of identity elements in S and a given value for $q_{1,1}$ is thus equal to a multiple of $|C(q_{1,1})|$ as well, and the proof is complete. •

4 Acknowledgements

The author would like to thank Dr. Gary Sherman of Rose-Hulman for his suggestions and support, as well as for organizing the NSF-REU program at which this research was done. Some recognition for the role played by the computer algebra system CAYLEY is also in order, since the calculations which inspired this paper would have been impossible without it.

References

[1] Brailovsky, L. and M. Herzog. *Lemma on squares of 2-element sets.* Unpublished note.

Jeffrey M. Vanderkam

Duke University