9-1992

Cubing Ordered 2-sets

Jeffery Vanderkam
Duke University

CUBING ORDERED 2-SETS

Jeffrey M. Vanderkam

MS TR 92-10

September 1992

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

FAX(812) 877-3198

Phone: (812) 877-8391

Cubing ordered 2-sets

Jeffrey M. Vanderkam*

September 16, 1992

Abstract

Given a group G, we define p_i as the probability that, given an ordered pair $X = (x, y)$, there are exactly i elements in $X^3 = \{x_1x_2x_3 | x_i \in X\}$. We show that $p_2(G) = 0$ if, and only if, $|G|$ is odd, and that $p_3(G) = 0$ if, and only if, $|G|$ is not divisible by three. The groups for which $p_4(G) = 0$ and $p_5(G) = 0$ are also determined.

1 Introduction

Suppose we take an ordered pair of elements from a group. What can we say about the group based on the number of distinct elements in the cube of the pair? Or, more generally, if no pair of elements in a group yield exactly n elements in their cube, what can this tell us about the group? We consider the cube of a pair $X = (x, y)$ to be the set $\{x^3, x^2y, xyx, yx^2, y^2x, yxy, xy^2, y^3\}$, that is, the set of all three-element products, with each element in X. Given a group G, we define a set of eight numbers $p_1(G), p_2(G), \ldots, p_8(G)$, where $p_i(G)$ represents the probability that a randomly chosen pair will have exactly i elements in its cube. In [1] those groups for which $p_8(G) = 0$ and those groups for which $p_6(G) = p_7(G) = p_8(G) = 0$ are classified. In [2] those groups for which $p_4(G) = 0$ in the analogous problem on squaring pairs are classified.

*Supported by NSF grant NSF-DMS 9100509.

Some qualifications are in order about what possibilities we are allowing for (x, y). We consider the pairs (x, y) and (y, x) to be distinct (although this has no effect on the results of this paper, as the orders of the cubes of (x, y) and (y, x) are the same), and we also allow the pair (x, x) as well, so there are exactly $|G|^2$ pairs to consider. As a result of this method of counting pairs, $p_1(G)$ cannot equal zero, since the pair (x, x) always has exactly one element, namely x^3, in its cube. In fact, this is the only way for a pair to have only one element in its cube, because if (x, y) has a cube of order one, then $x^3 = x^2y$, so $x = y$. This means that $p_1(G)$ is just the probability that the two elements are equal, which is obviously $1/|G|$. According to [3], the number of pairs yielding a cube of length i is always a multiple of the order of the group, so each of the p_i's can be expressed as $k_i/|G|$, where k_i is some nonnegative integer. It is possible for any of the p_i's other than p_1 to equal zero, and in this paper we will classify those groups G for which $p_i(G) = 0$ for $i \in \{2, 3, 4, 5\}$.

2 Conditions for $p_2(G) = 0$ and for $p_3(G) = 0$

Both of these results have fairly simple proofs, due to the strength of the conditions involved, so we will prove them both in the same section. In fact, we can completely classify in a single lemma all pairs (x, y) whose cube has two elements.

Lemma 1 *The ordered pair (x, y) yields exactly two elements in its cube if, and only if, $xy = yx$, $x^2 = y^2$, and $x \neq y$.*

PROOF: If $x = y$, then there is only one element in the cube, so we need only consider the cases when $x \neq y$. In this case, $x^3 \neq x^2y$ and $x^3 \neq xyx$. But since there are only two distinct values in the cube, this means $x^2y = xyx$, so $xy = yx$. This reduces the cube from eight elements to four: $\{x^3, x^2y, xy^2, y^3\}$. Now since $x \neq y$, we must have $x^2y \neq x^3$ and $x^2y \neq xy^2$, meaning that $x^2y = y^3$, so $x^2 = y^2$. The converse is immediate. •

Now that we have classified all pairs for which the cube has exactly two elements, it is simple to classify all groups according to whether p_2 is zero or not.

Proposition 1 *The value of $p_2(G)$ is zero if, and only if, the order of the group is odd.*

PROOF: Assume $p_2(G) = 0$. We will show that no element in G has order two. Suppose instead that there is an element x such that $x^2 = e$. Then the cube of the pair (x, e) has exactly two elements, contradicting the assumption. All groups of even order contain an element with order two, so the order of the group must be odd. Now assume that $p_2(G) \neq 0$. Then there is a pair (x, y) such that $xy = yx$ and $x^2 = y^2$ but $x \neq y$. But then $z = x^{-1}y$ has order two, so $|G|$ must be even. •

Classifying all groups with p_3 nonzero requires analysis of only a few more cases, and the result is very similar to that for p_2.

Proposition 2 *The value of $p_3(G)$ is nonzero if, and only if, the order of the group is divisible by three.*

PROOF: If the order of the group is divisible by three, then the group has an element x of order three, so the cube of the pair (x, e) has exactly three elements. Now we prove the converse. We assume that there exists a pair (x, y) such that its cube has exactly three elements. Because of Lemma 1, we know that not both of $xy = yx$ and $x^2 = y^2$ can occur. Thus we have three cases to consider.

1. $xy = yx$ and $x^2 \neq y^2$. The set $\{x^3, x^2y, xy^2, y^3\}$ must then consist of exactly three elements. But since the squares are distinct, this means that $x^3 = y^3$, so the element $z = x^{-1}y$ has order three.

2. $x^2 = y^2$ and $xy \neq yx$. The set $\{x^3, xyx, yxy, y^3\}$ must contain exactly three distinct elements. But we cannot have $x^3 = y^3$ or $x^3 = xyx$, so $x^3 = yxy$, $y^3 = xyx$, or $xyx = yxy$. But if

$x^3 = yxy$, then $xy^2 = yxy$, so $xy = yx$, which is impossible. The same reasoning (with y and x interchanged) also eliminates $y^3 = xyx$. If $xyx = yxy$, then (since $xy^{-1} = x^{-1}y$, and $yx^{-1} = y^{-1}x$) we know that $(xy^{-1})^3 = xy^{-1}xy^{-1}xy^{-1} = xyx^{-1}yx^{-1}y^{-1} = xyxy^{-1}x^{-1}y^{-1} = xyx(yxy)^{-1} = e$, so xy^{-1} has order three.

3. $xy \neq yx$ and $x^2 \neq y^2$. Then the four elements x^3, x^2y, xyx, xy^2 are all distinct, so the cube of (x, y) must have at least four elements. •

3 Conditions for $p_4(G) = 0$

Based on the results of the previous section, one might think that conditions on all p_i's are only related to the divisibility conditions of the order of G. Unfortunately, this ceases to be the case for the higher values, and the conditions become more and more case-dependent.

Theorem 1 $p_4(G) = 0$ *if, and only if,* G *belongs to one of the following three cases:*

1. *Exponent(G) = 2.*
2. $G = Z_2 \propto (Z_3)^n$, *with* $|x| = 2$ *if* $x \notin Z_3^n$.
3. *Exponent(G) = 3.*

In the course of the proof of the theorem, we will make repeated use of the following Lemma.

Lemma 2 *If* $p_4(G) = 0$, *then all elements of* G *have order less than four.*

PROOF: Assume there exists some element x with order four or more. Then the cube of the pair (e, x) has exactly four distinct elements: $\{e, x, x^2, x^3\}$. •

PROOF(OF THEOREM): Thus we see that any group G with p_4 zero must have order that is divisible only by two or three. If $|G| = 2^n$, then each element has order two, meaning that $G = (Z_2)^n$. Any such G satisfies $p_4(G) = 0$, as all pairs of elements in G commute and have equal squares, so this completes case (1). Next we consider the case in which the order of G is divisible by both two and three.

Lemma 3 *No group of order 12 has* $p_4 = 0$.

PROOF: There are five groups of order twelve. Both abelian groups and $Z_2 \times S_3$ contain an element of order 6. The other two groups may be checked quickly.•

We will use Lemma 3 to eliminate a large class of options for G by combining it with the following lemma.

Lemma 4 *If* $|G|$ *is divisible by 12, and all elements of* G *have order less than four, then* G *has a subgroup of order 12.*

PROOF: Since four divides the order of G, G must have a subgroup of order four, and since this subgroup cannot be cyclic, we know that there exists $\{x, y\} \subseteq G$ such that $x^2 = y^2 = e$, and $xy = yx \neq e$. Next we consider an element $z \in G$ of order three. If z commutes with x (or y), then the element xz (resp. yz) has order six, which we cannot have, so z commutes with neither. Now consider the order of the element xz. If it is three, then $< x, z >$ has order 12, as it consists of only the elements $e, x, z, xz, z^2, xz^2, zx, xzx, z^2x, xz^2x, z^2xz, zxz^2$, which the reader may easily check to be distinct. Thus both xz and yz must be involutions. But then $xz = z^2x$ and $yz = z^2y$, so the group $< x, y, z >$ has exactly twelve elements, namely $e, x, y, xy, z, zx, zy, zxy, z^2, z^2x, z^2y, z^2xy$, which again are easily seen to be distinct. •

As a result, the only possible non-p-groups remaining are those in which $|G| = 2(3)^n$, where n is a positive integer. We now show that $p_4(G) = 0$ and $|G| = 2(3)^n$ completely determine G.

Lemma 5 *If* $|G| = 2(3)^n$, *and* $p_4(G) = 0$, *then the (unique) Sylow 3-group of* G *is Abelian.*

Remark. This in fact implies that the Sylow 3-group is isomorphic to Z_3^n, since all of its elements have order three.

PROOF: We note first that the Sylow 3-group is unique, because it is normal (as its index is 2). We show that any pair of elements x, y from the Sylow 3-group must commute. Let $z \in G$ be an element of order 2. No element outside the Sylow 3-group (such as zx or zy) can have order three, meaning that all such elements have order two. In particular, the elements xzy, zy, and zx are not in the Sylow group, so $zy = y^2z$, $zx = x^2z$, and $(xzy)^2 = xzyxzy = e$. We may rewrite this as $e = x(zy)xzy = xy^2(zx)zy = xy^2x^2z^2y = xy^2x^2y = xy^{-1}x^{-1}y \Rightarrow xy = yx$, as desired. •

We note that in the proof of Lemma 5, we in fact showed that G must be as given in case (2) of Theorem 1. All that remains to be shown for this case is that if $G = Z_2 \propto (Z_3)^n$, as in case (2), then $p_4(G) = 0$.

Lemma 6 *If $G = Z_2 \propto (Z_3)^n$, as in Theorem 1, then $p_4(G) = 0$.*

PROOF: Suppose instead that there is some pair (x, y) with exactly four elements in its cube. If x and y cannot both have order three, then they would commute and have only three elements in their cube: $\{e, x^2y, xy^2\}$. If $x^2 = y^2 = 1$, then only x^3, xyx, yxy, y^3 could possibly be distinct. Letting $x = az$ and $y = aw$, where $|a| = 2$ and $|w| = |z| = 3$, we see that $xyx = azawaz = a^2z^2wz^2a = wza$, while $yxy = awazaw = a^2w^2zw^2a = wza$, so in fact there are only three distinct elements in the cube. Finally, if x has order two and y has order three, then $xy \neq yx$ (since otherwise $|xy| = 6$) and $x^2 \neq y^2$, so $\{y^3, y^2x, yxy, yx^2\}$ are all distinct. Now $xy^2 \neq y^3$ and $xy^2 \neq yxy$, and $xy^2 \neq y^2x$ because $|x| = 2$ while $|y^2| = 3$, so they cannot commute. The only possibility left is then $xy^2 = yx^2$, but this is impossible because $yx^2 = y$, and $xy \neq 1$. Thus there is no pair in G whose cube has exactly four elements. •

This leaves only one possibility, $|G| = 3^n$. We will now show that Exponent(G)=3 is a sufficient condition for this case.

Lemma 7 *If Exponent(G)=3, then* $p_4(G) = 0$.

PROOF: We assume there is a pair (x, y) whose cube contains exactly four elements, and show that this creates a contradiction. Now since $x^3 = y^3$, we must have $xy \neq yx$ (since otherwise we only have three elements in their cube). Also, we cannot have $x^2 = y^2$, since $x \neq y$. Thus the four elements x^3, x^2y, xyx, xy^2 are all distinct, as are the four elements y^3, y^2x, yxy, yx^2, so these two sets must contain four equal pairs when combined. We know that $x^3 = y^3$, and the only remaining possibility for xyx is for it to equal yxy, since $xyx = y^2x$ implies $x = y$ and $xyx = yx^2$ implies $xy = yx$. We now consider the two possibilities for x^2y.

1. $x^2y = yx^2$ and $xy^2 = y^2x$. Then both y^2 and y^3 commute with x, so all powers of y, including y itself, commute with x. But since $xy \neq yx$, this is impossible.

2. $x^2y = y^2x$ and $xy^2 = yx^2$. Then $e = xyx(yxy)^{-1} = xy(xy^2)x^2y^2 = xy^2x^4y^2 = xy^2xy^2 = (xy^2)^2$. But no element can have order 2, so $xy^2 = e = y^3$, implying $x = y$, again a contradiction. •

We have shown that the three cases imply and are implied by $p_4(G) = 0$, so the proof of Theorem 1 is complete.

4 Conditions for $p_5(G) = 0$

The conditions on a group for it to have a zero value for p_5 are based on the subgroups of the group, rather than being based on global properties of the group. We will show that any group with a nonzero p_5 value has a subgroup of the following type.

Definition 1 *H_n is the group generated by two elements $\{a, b\}$ subject to three relations:*

1. $a^{4n} = 1$

2. $b^5 = 1$

3. $ba = ab^2$.

We note that H_n is a metacyclic group, as $a^{-1}ba = b^2$ and $2^{4n} \equiv 1 \pmod 5$, so the order of H_n is given by $(4n)(5) = 20n$. Also, there exists one and only one H_n for each value of n. This definition enables us to state the following, the main result of this section.

Theorem 2 *Every H_n has a nonzero value for p_5, and two elements yield exactly five elements in their cube only if they generate one of the H_n's.*

The theorem immediately implies the following result, analogous to the results of the previous sections.

Corollary 1 *The value of $p_5(G)$ is nonzero if, and only if, G has a subgroup of the form H_n.*

PROOF(OF THEOREM): The first half of Theorem 2 is simple—the pair (ab, b) in the group $H_n = \langle a, b\rangle$ has exactly five elements in its cube regardless of the value for n. Thus, we restrict our attention to the second half. Suppose we have a group G and a pair of elements $\{x, y\}$ in G whose cube contains exactly five elements. It follows that that $xy \neq yx$, and that $x^2 \neq y^2$, since either of those conditions would be sufficient to limit the cube to having no more than four distinct elements. This means that the elements in the set $S_1 = \{x^3, x^2y, xyx, xy^2\}$ must all be distinct, as must those in $S_2 = \{x^3, xyx, yx^2, y^2x\}$ as well as those in $S_3 = \{yx^2, yxy, y^2x, y^3\}$ and $S_4 = \{x^2y, xy^2, yxy, y^3\}$, since all four sets were created by multiplying the set $\{x^2, xy, yx, y^2\}$ by either x or y on either the left or the right. We examine S_1, and consider the possibilities for the four remaining elements (all of which are in S_3). If x and y are to yield exactly five elements in their cube, then one these four must not be contained in S_1, and the other three must each be equal to distinct elements of S_1. Many of the ways for this to happen can be eliminated due to the restrictions from S_2 and S_4 (for example, we cannot have $y^2x = xyx$ or $x^2y = y^3$). As a result, for each element in S_3, there are only two elements in S_1 that it can equal (y^3 and yxy both can only equal x^3 or xyx, while y^2x and yx^2 can only equal x^2y and xy^2). Upon counting the remaining options, we find that there are exactly sixteen cases to consider and, as we will now show, only two are actually possible.

- $y^3 = x^3$ and $yxy = xyx$.

  1. $yx^2 = xy^2$, $y^2x \notin S_1$. Then $x^3y = y^4 = yx^3 = xy^2x$. But if $x^3y = xy^2x$, then $x^2y = y^2x$, which is impossible.

  2. $yx^2 = x^2y$, $y^2x \notin S_1$. Then x^2 and x^3 both commute with y, meaning that x must commute with y, a contradiction.

  3. $y^2x = xy^2$, $yx^2 \notin S_1$. This is the same as case (2), except that now y^3 and y^2 commute with x, still implying $xy = yx$.

  4. $y^2x = x^2y$, $yx^2 \notin S_1$. Then $xy^3 = y^4 = y^3x = yx^2y$, so, cancelling the y's, we find that $xy^2 = yx^2$.

- $y^2x = x^2y$ and $yx^2 = xy^2$.

  1. $y^3 = x^3$, $yxy \notin S_1$. Then $yxyx^2 = yx^2y^2 = y^3xy = x^4y = xy^4 = xyx^3$. But cancelling x^2 from the right side of the first and last terms tells us that $yxy = xyx$, a contradiction.

  2. $y^3 = xyx$, $yxy \notin S_1$. Then $x^2y^2 = xyx^2 = y^3x = yx^2y = xy^3$, and the first and last term imply that $x = y$, which is impossible.

  3. $yxy = x^3$, $y^3 \notin S_1$. Then, as in case (2), $y^2x^2 = yxy^2 = x^3y = xy^2x = yx^3$, so again $x = y$.

4. $yxy = xyx$, $y^3 \notin S_1$. Then $x^4y = x^2y^2x = xyx^3 = yxyx^2 = yx^2y^2 = y^3xy$. But cancelling xy from the first and last terms gives $x^3 = y^3$, again a contradiction.

- $y^2x = xy^2$ and $x^2y = yx^2$.

  1. $y^3 = x^3$, $yxy \notin S_1$. Then x commutes with both y^2 and y^3, so x must commute with y, a contradiction.

  2. $y^3 = xyx$, $yxy \notin S_1$. Then $yxy^4 = y^5x = y^2xyx^2 = y^2x^3y = x^3y^3$, implying that $yxy = x^3$, a contradiction.

  3. $yxy = x^3$, $y^3 \notin S_1$. Then we proceed exactly as in case (3), except with x and y interchanged, to find that $xyx = y^3$, still a contradiction.

  4. $yxy = xyx$, $y^3 \notin S_1$. Then $yx^3 = x^2yx = xyxy = yxy^2 = y^3x$, implying that $x^2 = y^2$, which is impossible.

- $y^3 = xyx$ and $yxy = x^3$.

  1. $y^2x = xy^2$, $yx^2 \notin S_1$. Then $yx^2y^2 = yxy^2x = x^3yx = x^2y^3$, so that $yx^2 = x^2y$, a contradiction.

  2. $yx^2 = x^2y$, $y^2x \notin S_1$. This is the same as case (1), with x and y interchanged, implying that $xy^2 = y^2x$, still impossible.

  3. $y^2x = x^2y$, $yx^2 \notin S_1$. We consider this case in the next paragraph.

  4. $yx^2 = xy^2$, $yx^2 \notin S_1$. We consider this case in the next paragraph.

This leaves us with two cases, both when $y^3 = xyx$ and $yxy = x^3$: $y^2x = x^2y$, $yx^2 \notin S_1$ and $yx^2 = xy^2$, $y^2x \notin S_1$. Clearly the two cases give the same result due to their symmetry, so we will only consider the first. We show that this case can in fact happen, and that when it does, $< x, y >= H_n$ for some n. The roles of a and b in the definition of H_n will be played by y and

xy^{-1}. First we show that xy^{-1} has order five. Now since $y^2x = x^2y$, we have $xy^{-1} = y^{-2}x^2$. But since $x^4 = x(yxy) = (xyx)y = y^4$, we also have $y^{-2}x^2 = y^2x^{-2}$. In a similar fashion, $yx^{-1} = x^{-2}y^2$. Using all of this, we see that $(xy^{-1})^5 = xy^{-1}xy^{-1}xy^{-1}xy^{-1}xy^{-1} = xy^{-1}y^2x^{-2}xy^{-1}xy^{-1}y^2x^{-2} = xyx^{-1}y^{-1}xyx^{-2} = xx^{-2}y^2y^{-1}xyx^{-2} = x^{-1}yxyx^{-2}$. But since $yxy = x^3$, this last term is equal to the identity, so $(xy^{-1})^5 = e$. Since xy^{-1} cannot be the identity, this means that it has order five. Now we show that the order of y is divisible by four. We prove that the other three possibilities for the order of y (mod 4) are impossible. Note first that the order of y cannot be 1 or 2, since y is not the identity (it does not commute with x) nor is it an involution (since otherwise $x = y^2x = x^2y$, so $xy = 1$, so $x = y$). Now we consider the other possibilities for $|y|$ (mod 4), making frequent use of the fact (shown earlier) that $x^4 = y^4$:

- $|y| \equiv 1 \pmod 4$. Then there exists an n such that $e = y^{4n+5} = y^{4n+2}xyx = y^2x^{4n+1}yx = (y^2x)y^{4n+1}x = x^2y^{4n+2}x$. Then x commutes with x^2y^{4n+2}, since they are inverses, so $x^3y^{4n+2} = y^{4n+5} \Rightarrow x^3 = y^3$, which we cannot have.

- $|y| \equiv 2 \pmod 4$. Then there exists an n such that $e = y^{4n+6} = y^{4n+3}xyx = y^{4n}xyx^2yx = x^{4n+1}y(x^2y)x = x^{4n+1}y^3x^2 = xy^{4n+3}x^2$, so x and $y^{4n+3}x^2$ commute, so $y^{4n+6} = y^{4n+3}x^3 \Rightarrow y^3 = x^3$, an impossibility.

- $|y| \equiv 3 \pmod 4$. Then there exists an n such that $e = y^{4n+3} = y^{4n}xyx = x^{4n+1}yx$. But then x commutes with $x^{4n+1}y$, so $x^{4n+2}y = 1 = y^{4n+3} \Rightarrow x^{4n+2} = y^{4n+2} \Rightarrow x^2 = y^2$, an impossibility.

Thus we must have $|y| = 4n$, for n a positive integer. All that is left now to prove is that $ba = ab^2$, that is, $(xy^{-1})y = y(xy^{-1})^2$, which we may simplify as $x = yxy^{-1}xy^{-1}$. But as before, $xy^{-1} = y^2x^{-2}$, so $yxy^{-1}xy^{-1} = yxy^{-1}y^2x^{-2} = yxyx^{-2} = x^3x^{-2} = x$, as desired. Thus we have shown that $< y, xy^{-1} >= H_n$, which immediately implies that $< x, y >= H_n$, and the proof of the theorem is complete.

One result of this is that the smallest group which could have all eight of its p_i's nonzero is the group $Z_3 \otimes H_1$, which has order sixty, and in fact, all eight are nonzero for this group.

5 Acknowledgements

The author would like to express his appreciation to Dr. Gary Sherman of Rose-Hulman, who suggested investigating the topic and provided invaluable suggestions along the way. Some recognition of the role played by the computer algebra system CAYLEY is also in order, as the computations that inspired the results in this paper would have been impossible without it.

References

[1] Berkovich, Y., G. Freiman, and C. Praeger. *Small Squaring and Cubing Properties for Finite Groups.* Bull. Austral. Math. Soc., **44** (1991), 429-450.

[2] Freiman, G. *On two- and three-elements subsets of groups.* Aequationes Mathematicae, **22** (1981), 140-152.

[3] Vanderkam, J. *Divisibility by $|G|$ for powers of ordered k-sets.* Rose-Hulman Inst. of Tech. Math. Sci. Tech. Report 9209.

Jeffrey M. Vanderkam

Duke University