International Journal of Algebra, Vol. 3, 2009, no. 7, 297 - 308

On the k-Conjugacy Classes of Infinite Groups

John W. Lawrence

Department of Pure Mathematics, Faculty of Mathematics
University of Waterloo, 200 University Avenue West
Waterloo, Ontario, Canada N2L 3G1

Collin D. Roberts

Department of Pure Mathematics, Faculty of Mathematics
University of Waterloo, 200 University Avenue West
Waterloo, Ontario, Canada N2L 3G1
cd2rober@math.uwaterloo.ca

Abstract

Given any group G and any positive integer k, the k-conjugacy classes of G are the equivalence classes in G^k under the equivalence relation wherein 2 k-tuples are equivalent if there exists an element $g \in G$ which conjugates one k-tuple onto the other co-ordinate wise. When $k = 1$ these are just the conjugacy classes of G.

The main result of this paper is that for an infinite group G which has finitely many 2-conjugacy classes, as k increases, there is a point after which there must be infinitely many k-conjugacy classes.

Mathematics Subject Classification: 20F38, 20F50

Keywords: conjugacy classes, locally finite groups

1 Introduction

Here we give a very brief description of the original motivating question from B. Doug Park that eventually led to the result. A slightly more detailed description is given in [5].

Let G be a discrete group. Let P be a G-principal bundle over a manifold X. By a deep theorem in differential geometry, there is a bijection between the set of flat connections on P modulo gauge equivalence and the set of group homomorphisms $\rho : \pi_1(X) \to G$ modulo the equivalence relation of conjugacy. In the special case where X is a Riemann surface of genus g, i.e. a 2-manifold with g holes (which we denote by Σ_g), then we know the shape of the fundamental group.

$$\pi_1(\Sigma_g) = \langle \alpha_1, \ldots, \alpha_g, \beta_1, \ldots, \beta_g \mid \prod_i [\alpha_i, \beta_i] = 1 \rangle$$

We can construct the desired homomorphisms $\rho : \pi_1(\Sigma_g) \to G$ which respect the necessary relation by sending α_i to 1_G and β_i wherever we like. It is desirable that even after killing half of the generators of $\pi_1(\Sigma_g)$ in this manner, that we should still have infinitely many conjugacy classes remaining. In this case the 2-conjugacy class problem (a particular case of the more general k-conjugacy class problem which we describe below) tells us something about the number of gauge equivalence classes of flat connections on a G-principal bundle P. The original motivating question was to determine the truth of the following statement.

The number of 2-conjugacy classes of G is finite implies that G is finite.

This paper takes a step toward answering the original motivating question, however we do not yet have a complete answer.

2 Definition and First Properties of k-Conjugacy Classes

Definition 2.1 *Let G be a group and k a positive integer. Define an equivalence relation on G^k, the direct product of k copies of G, by $(a_1, \ldots, a_k) \sim (b_1, \ldots, b_k)$ if and only if there exists $g \in G$ such that $g^{-1}a_ig = b_i$, $\forall i = 1, \ldots, k$. The equivalence classes are called k-conjugacy classes.*

Let $G(k)$ denote the number (possibly infinite) of k-conjugacy classes of G.

Before stating our main theorem, we record a few useful properties of the k-conjugacy classes of an arbitrary group G.

Lemma 2.2 *If G is non-trivial, and $G(k) < \infty$, then $G(k+1) \geq 2G(k)$.*

Proof: Assume that $G(k) = n$, for some positive integer n. Since G is non-trivial, we may let $1 \neq g \in G$. Fix n k-tuple representatives of the k-conjugacy classes of G.

$$\begin{gathered}(g_{11}, \ldots, g_{1k}) \\ (g_{21}, \ldots, g_{2k}) \\ \vdots \\ (g_{n1}, \ldots, g_{nk})\end{gathered}$$

Then it is clear that the following n k-tuples must lie in distinct $(k+1)$-conjugacy classes of G.

$$\begin{gathered}(1, g_{11}, \ldots, g_{1k}) \\ (1, g_{21}, \ldots, g_{2k}) \\ \vdots \\ (1, g_{n1}, \ldots, g_{nk})\end{gathered}$$

Furthermore, the following list of n k-tuples must lie in $(k+1)$-conjugacy classes of G which are distinct from each other, and distinct from each of the first list of n $(k+1)$-conjugacy classes.

$$\begin{gathered}(g, g_{11}, \ldots, g_{1k}) \\ (g, g_{21}, \ldots, g_{2k}) \\ \vdots \\ (g, g_{n1}, \ldots, g_{nk})\end{gathered}$$

Therefore G must have at least $2n$ distinct $(k+1)$-conjugacy classes. $\Box$

Corollary 2.3 *If G is non-trivial, and if there exists a positive integer k such that $G(k) < \infty$, then $G(l) < \infty$ for all $l < k$.*

Proof: If $G(l)$ is infinite, then so is $G(k)$, by (2.2). $\Box$

Corollary 2.4 *If G is a finite group, then $G(k) \geq |G|^{k-1}$.*

Proof: Since G is finite, so is G^k. Consider the action of G by co-ordinate wise conjugation on G^k. Then the formula for counting orbits which is often referred to as Burnside's Lemma (Theorem 2.113 in [7]) gives

$$G(k) = \frac{1}{|G|} \sum_{\tau \in G} Fix(\tau)$$

where $Fix(\tau)$ is the number of elements of G^k fixed by τ. Consider the contribution to the above sum just from $\tau = 1_G$. It is clear that $Fix(1_G) = |G^k| = |G|^k$. Thus we obtain that

$$G(k) \geq \frac{1}{|G|} |G|^k = |G|^{k-1}$$

as claimed. $\Box$

Note that using the same orbit counting formula, a straightforward computation shows that $S_3(k) = 2^{k-1} + 3^{k-1} + 6^{k-1}$, where S_3 is the symmetric group on 3 letters.

We will also need the following bound on the number of k-conjugacy classes for a normal subgroup of finite index.

Lemma 2.5 *Given a group G and a normal subgroup $N \lhd G$ with $G(k) < \infty$ and $[G : N] < \infty$, we have $N(k) \leq [G : N] \cdot G(k)$.*

Proof: Let $n = [G : N]$. Fix representatives $g_1, \dots, g_n$ for the n cosets of N in G. Fix 2 k-tuples in N^k: $(a_1, \dots, a_k)$ and $(b_1, \dots, b_k)$. Suppose that $(a_1, \dots, a_k) \sim (b_1, \dots, b_k)$ in G^k, via $g \in G$. Then we can write $g = g_i n_g$, for some $1 \leq i \leq n$ and some $n_g \in N$. Then since g conjugates $(a_1, \dots, a_k)$ onto $(b_1, \dots, b_k)$, we can write

$$\begin{array}{rcll} & g^{-1} a_j g & = & b_j \quad 1 \leq j \leq k \\ \Longrightarrow & (g_i n_g)^{-1} a_j (g_i n_g) & = & b_j \quad 1 \leq j \leq k \\ \Longrightarrow & n_g^{-1} \underbrace{(g_i^{-1} a_j g_i)}_{\in N, \text{ since } N \lhd G} n_g & = & b_j \quad 1 \leq j \leq k \end{array}$$

Therefore $(g_i^{-1} a_1 g_i, \ \dots, \ g_i^{-1} a_k g_i) \sim (b_1, \dots, b_k)$ in N^k, via $n_g \in N$. Since there are n possible choices for g_i, there can be at most n k-conjugacy classes of N arising from a given k-conjugacy class of G. □

We also recall one basic result which we will use several times throughout this paper.

Lemma 2.6 *Let G be a group, and $H \leq G$ a subgroup of finite index n. Then there exists a subgroup K of H, which is normal in G, and such that $|G/K|$ is a divisor of $n!$ (in particular $|G/K|$ is finite).*

Proof: In the proof of Theorem 2.88 in [7], take $K = \ker \varphi$. Then, by the First Isomorphism Theorem, we obtain

$$G/K = G/\ker \varphi \cong im\varphi \leq S_n$$

whence the desired result follows, since $|S_n| = n!$. □

3 The Theorem

We adopt the convention that $\mathbb{P}$ denotes the set of positive integers.

Theorem 3.1 *There is an increasing function $\alpha : \mathbb{P} \to \mathbb{P}$ such that if G is an infinite group with $G(2)$ finite and $k \geq \alpha(G(2))$, then $G(k)$ is infinite.*

We will prove this theorem in several steps. If the theorem is false, then there exist a positive integer N and a sequence $G_1, G_2, G_3, \dots$ of infinite groups such that

1. $G_k(2) \leq N$ for all $k = 1, 2, 3, \dots$

2. $G_k(k)$ is finite for all $k = 2, 3, \ldots$

We will assume that these conditions are satisfied and obtain a contradiction.

Theorem 3.2 *Fix any positive integers* l *and* k *with* $l < k$*. Then*

1. *If* $H \leq G_k$ *is an* l*-generated subgroup, then* $|H| \leq G_k(l+1)$ *(note that this is a uniform bound on* $|H|$*). Thus there are only finitely many isomorphism classes of* $(l+1)$*-generated subgroups of* G_k*.*
2. *Moreover, no composition series of an* $(< l)$*-generated subgroup of* G_k *has length greater than* $G_k(l)$*.*

A version of this result is proved in [5]. We present an improved proof here.

Proof: For (1), Let H be any l-generated subgroup of G_k. Fix generators $a_1, \ldots, a_l \in H$ so that we may write $H = \langle a_1, \ldots, a_l \rangle$. List all the elements of H, i.e. $H = \{h_1, h_2, \ldots\}$.

Construct all $(l+1)$-tuples of the form $(a_1, \ldots, a_l, h_i) \in H^{(l+1)}$, where h_i runs through all the elements of H. For each $(l+1)$-tuple, construct the $(l+1)$-conjugacy class to which it belongs. Each $(l+1)$-tuple is then a representative of its class. By the hypothesis that $G_k(k)$ is finite and by (2.3), $G_k(l+1)$ is finite.

Consider the set of $(l+1)$-conjugacy classes described above. They are not necessarily all distinct. We know that we have at most $G_k(l+1)$ distinct classes by hypothesis. Write a (possibly shorter) list of representatives from the distinct classes. Each representative has the form $(a_1, \ldots, a_k, h_i)$ for some $i \in \{1, 2, \ldots, G_k(l+1)\}$. We may not need all $G_k(l+1)$ of them. Since we seek a uniform bound, we treat the most pessimistic case possible.

Pick another arbitrary $(l+1)$-tuple $(a_1, \ldots, a_l, h_n)$ for any $h_n \in H$. By construction this new $(l+1)$-tuple must belong to one of the $(l+1)$-conjugacy classes constructed above, say the jth one. Then by definition there exists $g \in G_k$ such that

$$(a_1,\ \ldots,\ a_l,\ h_n) = (g^{-1}a_1g,\ \ldots,\ g^{-1}a_lg,\ g^{-1}h_jg)$$

Now observe that by the original construction of the $(l+1)$-tuples, conjugation must fix the a_is. Therefore, we have that

$$\begin{aligned} a_1 &= g^{-1}a_1g \\ a_2 &= g^{-1}a_2g \end{aligned}$$

$$\begin{array}{rcl} & \vdots & \\ a_k & = & g^{-1}a_kg \\ h_l & = & g^{-1}h_jg \\ \Longrightarrow h_l & = & h_j \end{array}$$

Here is the explanation of the last equality above. Conjugation by g must fix all the a_is. The a_is generate all of H. Therefore we can write $h_j = a_{j_1} \dots a_{j_s}$. Then:

$$\begin{array}{rcl} g^{-1}h_jg & = & g^{-1}(a_{j_1} \dots a_{j_s})g \\ & = & (g^{-1}a_{j_1}g) \dots (g^{-1}a_{j_s}g) \\ & = & (a_{j_1}) \dots (a_{j_s}) \text{ (since conjugation by g fixes the } a_i\text{s)} \\ & = & h_j \end{array}$$

Since there are at most $G_k(l+1)$ distinct $(l+1)$-tuples, there are at most $G_k(l+1)$ choices for j. Therefore there are at most $G_k(l+1)$ elements in H. This completes the proof of (1).

For (2), Let $H = \langle a_1, \dots, a_{l-1} \rangle \leq G_k$ be any $(l-1)$-generated subgroup. By the result in (1), we then have $|H| \leq G_k(l)$. Since H contains at most $G_k(l)$ distinct elements, any composition series of H could contain at most $G_k(l)$ factors. Any choice of fewer than $(l-1)$ generators for H will yield the same result. This completes the proof of (2). □

Corollary 3.3 *If $k > 1$, then G_k has finite exponent.*

Proof: Let $k > 1$. Let $H = \langle g \rangle$ be any 1-generated (i.e. cyclic) subgroup of G_k. Since $1 < k$, we have by (3.2) that $|H| \leq G_k(2)$. Recall that by hypothesis $G_k(2) \leq N < \infty$. Therefore $|H| \leq N$, independently of the choice of k. Since we have a uniform bound on the order of cyclic subgroups of G_k, we have a uniform bound on the order of elements of G_k. Thus G_k has finite exponent as claimed. □

Define S to be the set of simple homomorphic images (up to isomorphism) of finite subgroups of each G_k, for $k = 1, 2, 3, \dots$.

Lemma 3.4 *S is a finite set.*

Proof: By (3.3), there is a uniform bound on the exponent of all the groups in S.

The members of S are homomorphic images of finite groups, so they are themselves finite groups. By Proposition 2.2 in [3], every finite simple group can be generated by 2 elements. Therefore every member of S is 2-generated, since they are all finite simple groups.

We have uniform bounds on the exponent and the number of generators for all the groups which are members of S.

Denote by B_n the restricted 2-generated Burnside group of exponent n. Recall that by the Hall-Higman reduction and Zelmanov's solution of the Restricted Burnside Problem for prime power exponent (see [8]), we have that B_n is finite for all all n. Thus each B_n has (up to isomorphism) only finitely many distinct homomorphic images.

Any finite 2-generated group of exponent n is a homomorphic image of B_n. Since we have uniform bounds on the number of generators and the exponent of each member of S, we obtain only finitely many B_n of which the members of S can be homomorphic images. Each B_n can have only finitely many distinct homomorphic images. Therefore there can be only finitely many distinct isomorphism classes lying in S.

Therefore S is finite (and is determined by N). □

Definition 3.5 *Recall that if G is a finite group, then a normal series of G is a chain of subgroups, each of which are normal in G, of the form*

$$\{1\} = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_a = G$$

The series is proper if $N_i \subsetneq N_{i+1}$ for all i.

A subnormal series of G is a chain of subgroups of the form

$$\{1\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_a = G$$

Note that for a subnormal series each group N_i is not required to be normal in G, only in its immediate successor.

A composition series of G is a subnormal series of G, all of whose factors are simple.

Consider now a proper normal series of G which cannot be further refined to a proper normal series. The length of such a chain as well as the set of factors $\{N_{i+1}/N_i\}$ are invariants of the group G. The factors N_{i+1}/N_i are called the chief factors of G. See [6], pp 17-18 for details.

Lemma 3.6 *If H is a homomorphic image of an l-generated subgroup of any G_k (where $k \geq 2$ and $1 \leq l < k$), then the factors of a composition series of H all lie in S (up to isomorphism).*

Proof: The proof is by induction on $|H|$.

If H is simple, then $H \in S$ and we are done. So assume for the rest of the proof that H is not simple.

Since H is not simple, we can find a non-trivial proper normal subgroup $N \triangleleft H$. Then N and H/N are both homomorphic images of finite subgroups of G_k and strictly smaller that H, and the desired result follows by the induction hypothesis. □

Lemma 3.7 *If A is a finite homomorphic image of any G_k, then the order of A is uniformly bounded as a function of N.*

Proof: By (2.3), G_k has no more than N conjugacy classes. Therefore G_k has no more than N normal subgroups. Thus there is a uniform bound on the length of any proper normal series of A. This bound is a function of N.

Since S is finite, we may let s denote the order of the largest simple group in S. Then A has a proper normal subgroup $A_1 \triangleleft A$ of index at most s. If A_1 is non-trivial, then A_1 contains a proper subgroup B_1, of index at most s in A_1.

Note that B_1 may not be normal in A. However B_1 is a proper subgroup of A_1, of index at most s^2 in A. Then by (2.6), B_1 contains a subgroup A_2, which is properly contained in A_1 and is normal in A, and of index at most $(s^2)!$ in A.

If A_2 is not trivial, then we may iterate this construction once more, to obtain a proper subgroup A_3 of A_2, which is normal in A, and of index at most $((s^2)!s)!$ in A.

Because there is a uniform bound on the length of any proper normal series of A, this construction must terminate after finitely many steps. Since s is determined by N, we therefore have a uniform bound on the order of A as a function of N, as required. □

Definition 3.8 *Recall that a variety of groups is a class of groups (in some universe) closed under direct products, subgroups, and homomorphic images. Equivalently, a variety of groups is a class of groups defined by a set of identities.*

If $\mathbb{V}$ is a variety of groups and G is a group then the *verbal subgroup* *of G (denoted by G^*) is the subgroup of G generated by*

$$\{w(a_1, \ldots a_n) : w = 1 \text{ is an identity of } \mathbb{V}, a_i \in G\}$$

Equivalently, it is the intersection of all the normal subgroups $N \lhd G$ such that $G/N \in \mathbb{V}$.

The verbal subgroup is a fully invariant subgroup of G. See Theorem 12.33 in [4] for details.

Let $\mathbb{V}$ be the variety of groups generated by the set S as defined above. Note that since S is a finite set of finite groups, we may regard $\mathbb{V}$ as being the variety generated by a single finite group (since a variety is closed under homomorphic images).

Lemma 3.9 *If H is an l-generated subgroup of any G_k (where $k \geq 2$ and $1 \leq l < k$), then every chief factor of H lies in $\mathbb{V}$.*

Proof: Consider the normal series

$$H \supseteq H^* \supseteq \cdots \supseteq H^{*(n)} \supseteq \cdots$$

where $H^{*(n)}$ denotes the verbal subgroup operation iterated n times.

If H has a composition series (i.e. a subnormal series) of length t, then by (3.6), $H^{*(t)} = \{1\}$. Clearly all the factors $H^{*(i)}/H^{*(i+1)}$ lie in $\mathbb{V}$. If this series is refined to a maximal proper normal series, then all the factors of the new series will lie in $\mathbb{V}$ also by (3.6). □

Lemma 3.10 *Without loss of generality, G_k is simple for all $k \geq 2$.*

Proof: Let $k \geq 2$. By (2.3), G_k has no more than N conjugacy classes. Therefore G_k has no more than N normal subgroups.

Let $N_k \lhd G_k$ be minimal with respect to the property 'G_k/N_k is finite'. Then since $G_k(k)$ is finite and since N_k is a normal subgroup of finite index, by (2.5) $N_k(k)$ is finite.

Any proper subgroup of N_k has infinite index, for by (2.6), a subgroup of finite index always contains a normal subgroup of finite index, contradicting the minimality of N_k. Let $M_k \lhd N_k$ be a maximal proper normal subgroup of N_k.

Then N_k/M_k is simple and infinite. By (2.5), we have that

$$N_k(k) \leq [G_k : N_k] \cdot G_k(k)$$

G_k/N_k is a finite homomorphic image of G_k. Therefore, by (3.7), we have that $[G_k : N_k] = |G_k/N_k|$ is uniformly bounded as a function of N, independently of the choice of k. So we may re-define our G_k to be this N_k/M_k, and it has all the required properties to continue with the proof. $\square$

Observe that $\mathbb{V}$ is generated by a finite group and is therefore finitely based by the Oates-Powell Theorem (Corollary 52.12 in [4]). We may assume that there is a positive integer n such that the variables $x_1, \ldots, x_n$ are the only ones required by the finite base for $\mathbb{V}$.

Lemma 3.11 *If* $k > nN + 1$, *then* $G_k \in \mathbb{V}$.

Proof: Let $k > nN + 1$. Since $\mathbb{V}$ is finitely based, we only have to check finitely many identities to decide whether G_k lies in $\mathbb{V}$.

For a contradiction, suppose that $w(x_1, \ldots, x_n) = 1$ is an identity of $\mathbb{V}$ such that for some $a_1, \ldots, a_n \in G_k$, we have

$$w(a_1, \ldots, a_n) = b \neq 1$$

By (3.10), G_k is simple. Therefore G_k is the normal closure of the subgroup generated by any non-trivial set of elements of G_k. In particular, G_k is the normal closure of $\langle b \rangle$. By (2.3), G_k has at most N conjugacy classes. Therefore each a_i is a product of at most N conjugates of b. Thus there exist $g_1, \ldots, g_N \in G_k$ such that $a_1, \ldots, a_n$ lie in the subgroup of G_k generated by $\{g_i^{-1} b g_i\}_{i=1}^{N}$.

Let $H = \langle b, g_1, \ldots, g_N \rangle \leq G_k$. Then H is an $(N+1)$-generated subgroup of G_k, where $(N + 1) < k$. Let K be the normal closure of $\langle b \rangle$ in H. Then $K^* \subseteq K$ always holds (recall K^* is the verbal subgroup of K). As $a_1, \ldots, a_n \in K$ and K^* is a normal subgroup of H containing b, we must also have $K \subseteq K^*$ since K, being the normal closure of $\langle b \rangle$ in H, is contained in any normal subgroup containing b. Therefore we must have $K = K^*$.

Let $M < K$ be a proper subgroup which is maximal with respect to

1. $M \trianglelefteq H$
2. $b \notin M$

Then any larger subgroup of K which is normal in H will contain b and will therefore be equal to K. Therefore K/M is a chief factor of H, and so by (3.9), $K/M \in \mathbb{V}$ and

$$K^* \subseteq M \subsetneq K$$

which contradicts $K = K^*$ above. □

See Theorem 5.27 on p154 in [6] for a similar proof.

Corollary 3.12 *If $k > nN + 1$, then G_k is finite.*

Proof: Let $k > nN + 1$. By (3.11), $G_k \in \mathbb{V}$. Recall that by earlier remarks, $\mathbb{V}$ is a variety generated by a finite group. Ross Willard has pointed out some very general results in universal algebra. Theorem 14.5 (p185) of [1] implies that an infinite simple group cannot be in the variety generated by a finite group. By 3.10, G_k is simple. If G_k is also infinite, then we get a contradiction with Theorem 14.5 (p185) of [1]. Thus the only possibility that remains is that G_k is finite, as claimed. □

But now (3.12) contradicts the original assumption that G_k was infinite for all $k \geq 1$ and this contradiction completes the proof of Theorem 3.1.

Here we make a few additional closing remarks.

As we noted in (3.3), if G is a group for which $G(2)$ is finite, then G must be a torsion group with a uniform bound on the orders of the elements.

A similar argument to that presented here can also be used to show the following result.

Corollary 3.13 *If G is a locally finite group G with $G(2)$ finite, then G must be finite.*

References

[1] D. Hobby, and R. McKenzie, *The Structure of Finite Algebras (Contemporary Mathematics, v.76),* American Mathematical Society, Providence, Rhode Island, 1988

[2] O. H. Kegel and B. A. F. Wehrfritz, *Locally Finite Groups,* North Holland, Amsterdam, 1973

[3] M. Liebeck and A. Shalev, The Probability of Generating a Finite Simple Group, *Geometriae Dedicata,* **56** (1995), 103-113

[4] H. Neumann, *Varieties of Groups,* Springer-Verlag, New York, 1967

[5] C. D. Roberts, *A k-Conjugacy Class Problem, Masters Thesis,* University of Waterloo, Waterloo, Ontario, 2007

[6] D. J. S. Robinson, *Finiteness Conditions and Generalized Soluble Groups (Volume 1),* Springer-Verlag, Berlin, 1972

[7] J. J. Rotman, *Advanced Modern Algebra,* Prentice-Hall, Upper Saddle River, New Jersey, 2002

[8] M. Vaughn-Lee, *The Restricted Burnside Problem,* Second Edition, Oxford University Press, Oxford, England, 1993

Received: October 30, 2008