Research Statement

James B. Wilson

My research began with finite groups, p-groups, and algorithms – areas which led to bilinear maps, $*$-algebras, and Jordan algebras. The study of p-groups often uses nonassociative algebras, which mimic the group structure, but have have more amenable linear properties [7]. These are typically Lie algebras. The methods that I have developed also use nonassociative algebras. However, the deeper results that I obtain seem to require sophisticated machinery, and my approach is quite unrelated to earlier methodologies.

Theorem 1 gives group isomorphism invariants of central product decompositions of p-groups but also shows that in general there are no group isomorphisms sending these central product decompositions to one-another. Theorem 2 helps explain how this is possible. Theorems 4 and 5 are polynomial-time algorithms to find central and direct products given only generators of a group. Finally, Theorems 6, 7, and 8 are statements about the number and structure of centrally indecomposable p-groups. Each of these I proved using Jordan and other nonassociative algebras.

One of the delights is that these theorems read like classical group theory but the proofs do not. Alse, the excursion into other areas brings with it some unexpected examples and questions for p-groups.

Central decompositions and bilinear maps.

A *central decomposition* of a group G is a set $\mathcal{H}$ of subgroups in which distinct members commute, and G is generated by $\mathcal{H}$ but no proper subset. Central decompositions make central products precise. A group is *centrally indecomposable* when it has only the trivial central decomposition. A central decomposition is *fully refined* if every member is centrally indecomposable. My first breakthrough was to translate central decompositions of p-groups into the context of bilinear maps.

Every p-group P determines bilinear maps by commutation. For instance, if P has nilpotency class 2 then define $b : V \times V \to W$, where $V = P/P'$, $W = P'$, and P' denotes the commutator subgroup of P; so that,

$$b(P'x, P'y) := [x, y] = x^{-1}y^{-1}xy, \qquad \forall x, y \in P. \tag{1}$$

If $\mathcal{H}$ is a central decomposition of P then $\mathcal{H}$ induces an orthogonal decomposition $\mathcal{X}(\mathcal{H}) = \{HP'/P' : H \in \mathcal{H}\}$ of b. Therefore the study of central decompositions relates to the study of orthogonal decompositions of bilinear maps. Indeed, bilinear maps also give rise to class 2 nilpotent groups so bilinear maps are not far removed from the original goal of studying p-groups. For 2-groups I also use an associated quadratic map resulting from the power map $x \mapsto x^2$, $x \in P$. Bilinear and quadratic maps are not new to the theory of p-groups, but outside of extraspecial p-groups (where the bilinear/quadratic maps are forms, i.e. $|P'| = p$), there has not been much use for the geometric structure of these maps for the study of p-groups.

On the uniqueness of central decompositions.

Theorem 1 *[15, Theorem 1] For p-groups P of class 2 and exponent p,*

(i) the following are invariants of fully refined central decompositions of P: the number of members, the multiset of orders of the members, and the multiset of orders of the centers of the members; and

(ii) the number of $\operatorname{Aut} P$-orbits acting on the set of fully refined central decompositions can be any positive integer.

Theorem 1.(i) can be compared with the Krull-Remak-Schmidt theorem which proves the uniqueness of direct products of groups, up to an automorphism of the group. Indeed, the proof suggests the following:

Conjecture 1 *The multiset of group isomorphism types of a fully refined central decomposition of a p-group P of class 2 and exponent p is uniquely determined by p.*

Work towards this conjecture is on going and the current results suggests any counterexamples will have order exceeding 5^{30}. Theorem 1.(ii) highlights how the proof of Theorem 1.(i) cannot use standard methods such as generalizing the proof of the Krull-Remak-Schmidt theorem.

The assumption of exponent p in these theorems makes it possible to convert all isometries of the associated bilinear map into automorphisms of the group. This leads to:

Problem 1 *Generalize Theorem 1 to p-groups of arbitrary class and exponent.*

The standard extraspecial groups show that for groups of large exponent, the multiset of group isomorphism types of fully refined central decompositions is not uniquely determined. Still, appropriately modified versions of Theorem 1 are known in larger exponent and for 2-groups, but require an equivalence of p-groups related to the *isoclinism* of P. Hall [3]. The details are carried out in [18]. More work is needed for arbitrary class p-groups.

To explain how group isomorphism invariants can be obtained where there are no group isomorphisms, the proof of Theorem 1 relies on coarser decompositions called *semi-refined* central decompositions (of size at least half the size of a fully refined central decomposition) admitting the following transitivity:

Theorem 2 *[15, Corollary 6.10]* $\operatorname{Aut} P$ *is transitive on the set of all semi-refined central decompositions of a p-group P of class 2 and exponent p.*

As with Theorem 1, this is fundamentally a result about bilinear maps. To study bilinear maps it was necessary to produce the following family of nonassociative algebras.

Let $b : V \times V \to W$ be a bilinear map, such as in (1). Define

$$\operatorname{Adj}(b) := \{(f, g) \in \operatorname{End} V \times (\operatorname{End} V)^{op} : b(uf, v) = b(u, vg), \forall u, v \in V\}. \tag{2}$$

If b is alternating then $(f, g) \in \operatorname{Adj}(b)$ if, and only if, $(f, g)^* := (g, f) \in \operatorname{Adj}(b)$. The operation $*$ makes $\operatorname{Adj}(b)$ an associative algebra with involution, that is, a $*$-algebra. In this case, b also has a related Jordan algebra

$$\operatorname{Sym}(b) := \{f \in \operatorname{End} V : b(uf, v) = b(u, vf), \forall u, v \in V\} \tag{3}$$

with nonassociative product $f \bullet g := \frac{1}{2}(fg + gf)$ for $f, g \in \operatorname{Sym}(b)$ (in characteristic 2 *quadratic* Jordan algebras are required). The details of these algebras are given in [15, Section 4]. Orthogonal decompositions of b are in a one-to-one correspondence with sets of idempotents of the Jordan algebra $\operatorname{Sym}(b)$. To prove Theorems 1 and 2 the action of groups of isometries and *pseudo-isometries* (conformal mappings) of the bilinear map are studied using both $\operatorname{Sym}(b)$ and $\operatorname{Adj}(b)$.

When b is a nondegenerate bilinear form these are familiar algebras: here $\operatorname{Adj}(b) \cong M_n(K)$ for some field K, with the transpose (or a variation of transpose) as the $*$ operator. Likewise, $\operatorname{Sym}(b)$ is the set of matrices fixed by the anti-isomorphism $*$ of $\operatorname{Adj}(b)$, for example, the set of symmetric matrices. However, when b is a bilinear map, $\operatorname{Adj}(b)$ and $\operatorname{Sym}(b)$ can have highly varied structure, including non-trivial radicals and multiple non-isomorphic simple quotients. Even though the bilinear map b is alternating, the simple factors of $\operatorname{Adj}(b)$ and $\operatorname{Sym}(b)$ quite often pertain to *symmetric* bilinear forms, and other non-alternating forms. The symmetric bilinear forms lead to the lack of transitivity in Theorem 1.(ii). In Jordan algebras, it is standard to obtain

transitivity by broadening the scope to groups of isotopes of the algebras [11], but for applications to p-groups only isometries and pseudo-isometries can be used. To work around this problem, linear transformations are judiciously chosen which do not preserve the bilinear map but nevertheless establish Theorem 2 which then leads to Theorem 1.(i).

The work involved in Theorems 1 and 2 leads to various results with directions left to explore. For instance, there is no theorem of Witt type for bilinear maps, maximal totally isotropic subspace can have different dimensions, and alternating bilinear maps can even have orthogonal groups as their isometries. Yet, I prove:

Theorem 3 *[15, Theorem 4.19] The isometry group of a bilinear map is unipotent-by-classical.*

Once again, this theorem is proved using techniques from nonassociative algebras. In progress is work on the following:

Problem 2 *What is the structure of the pseudo-isometry (conformal) group of a bilinear map?*

This problem has immediate application to the structure of the automorphism group of a p-group (cf. [15, Proposition 3.5] and [19]) and could help answer open problems raised by A. Mann and others [9, Section 2]. The importance of connecting these isometry/pseudo-isometry/automorphism groups to nonassociative algebras is that the algebras can be easily computed and probed using linear algebra, whereas even finding generators for the groups is a very difficult problem in practice.

Algorithms for finding central decompositions.

To make central decompositions useful it is important to be able to locate a central decomposition of a p-group or report that the group is centrally indecomposable. Abstractly the problem is finite, but brute force is unreasonable. The theorems that follow are a precise way of expressing theoretically (and practically) "reasonable" methods to find decompositions.

It is standard to input p-groups via presentations exhibiting a normal series with abelian quotients, called a *polycyclic presentation* or *pcp* [6, Chapter 8]. The input length of a pcp is roughly the length n of the presentation and so n is used for timing. *Polynomial-time* algorithms run with $O(n^c)$ steps where c is a constant. Deterministic algorithms run the same steps each time they are given the same input. There are also *Las Vegas* algorithms which allow for random variations in the process but require that any output be provably correct, and the failure to output occurs with small probability [13, Chapter 1].

Theorem 4 *[16, Theorem 1] There are polynomial-time algorithms to find generators for a fully refined central decomposition of a finite p-group of class 2. The first is deterministic with running time $O(p + \log^5 |P|)$. The second algorithm is Las Vegas with running time $O(\log^5 |P|)$.*

(The Las Vegas algorithm uses the method of Berlekamp to factor polynomials over $\mathbb{Z}_p$, cf. [1].) This I proved using effective versions of the algebras $\mathrm{Adj}(b)$ and $\mathrm{Sym}(b)$ and a modifications to the library of algorithms for associative algebras first developed by Ronyai [12].

Algorithms for finding direct products. It was brought to my attention by E. M. Luks and C.R.B. Wright that there were no known algorithms for testing if a finite group was directly indecomposable, and if not, to find a proper direct product in the group. Even for p-groups of class 2 this problem was not settled. Settling this problem is the focus of my paper [17] and the following theorem:

Theorem 5 *[17, Theorem 1] There are polynomial-time algorithms to find generators for each of the following*

(i) a fully refined direct product decomposition of a nonassociative algebra specified by structure constants,

(ii) a fully refined direct product decomposition of p-groups of class 2*, specified by a pcp.*

The first algorithm is deterministic polynomial time in the length of the input and the size of p. The second algorithm is Las Vegas polynomial time in the size of the input.

Using standard group theory the and similar methods, it is likely that an algorithm for finding direct product of general solvable groups is possible, and work continues in this direction. To solve the problem for nonassociative algebras I derived a third algebra related to the bilinear maps. This third algebra is a commutative ring whose idempotents correspond to the direct decompositions of the nonassociative algebra. Finding idempotents in a commutative ring is essentially the same problem as factoring polynomials [2, Section 1]. The prototype of this third algebra can be seen in [10].

Indecomposable p-groups

The third stage in studying central decompositions is to understand the centrally indecomposable groups. In the following result I demonstrate that a complete classification is highly unlikely.

Theorem 6 *[19] For each n there are at least $p^{2n^3/27+Cn^2}$ pairwise non-isomorphic centrally indecomposable groups of order p^n, for some constant C.*

The total number of groups of order p^n is known to be $p^{2n^3/27+O(n^{8/3})}$, with the conjectured sharper bound of $O(n^2)$ in the exponent [5, 9, 14]. Of course, the value of the constants leave open many possibilities. To strengthen this result I have also proved:

Theorem 7 *[19] A randomly presented p-group is almost always centrally indecomposable.*

Randomly presented means that the rank of the lower exponent p central factors are randomly selected and then the group is specified with random commutators and powers. This approach is similar to the meaning of *almost always* used in [4]. Unfortunately, it is possible that probability models for random p-groups of these sorts may not converge to a uniformly distributed random p-group [9]. This leads to:

Problem 3 *Construct a probability model for random presentations of p-groups which approximates the uniform distribution. Use this model to describe a typical p-group.*

A prototype of possible model is given in the proof of Sims' upper bound on the total number of p-groups of a given order.

The most ambitious future direction comes from the following observation: if a group P is centrally indecomposable then so is any group Q where $Q/N \cong P$ and $N \leq Q'$ (such a group Q is called a *descendant* of P). Thus there is a natural meaning of a *minimal centrally indecomposable group* but even these groups are numerous and complex. However, the bilinear commutation maps can often be simplified if the ground field is extended. For p-groups P of small class (and possibly in general) this extension can be applied to P directly to produce a p-group $k \otimes P$ of the same class as P but with the property that the associated bilinear map of commutation is now over the field k. With this process it is possible to prove theorems such as:

Theorem 8 *[19] Let P be a centrally indecomposable p-group of class* 2*, exponent p, and rank $2n$. If $P' \cong \mathbb{Z}_p^2$ and k is the algebraic closure of $\mathbb{Z}_p$, then $k \otimes P$ is either centrally decomposable or isomorphic to the p-group with bilinear commutation map $b : (U \oplus U) \times (U \oplus U) \to W$ where $U := k[x]/(x^n)$, $W := U/\langle 1, \ldots, x^{n-3}\rangle$ as a k-vector space, and b is defined by*

$$b\big(p(x) \oplus q(x), r(x) \oplus s(x)\big) \equiv p(x)r(x) - q(x)s(x) \pmod{\langle 1, \ldots, x^{n-3}\rangle}. \tag{4}$$

Call a p-group P *absolutely centrally indecomposable* when $k \otimes P$ is centrally indecomposable for every field extension k, in particular, over the algebraic closure of $\mathbb{Z}_p$. In this terminology, Theorem 8 is one of several results I have uncovered while addressing the following broader goal:

Problem 4 *Study minimal absolutely centrally indecomposable p-groups.*

The resulting groups $k \otimes P$, for k the algebraic closure of $\mathbb{Z}_p$, are locally finite and of infinite rank, but the class is the same as the class of P. In this sense the process is dual to the study of descendants and their related pro p-groups where the rank is fixed but the class is infinite [8]. I am in the process of synthesizing both points of view.

References

[1] E. R. Berlekamp, Factoring polynomials over finite fields, Bell System Tech. J. 46 (1967) 1853–1859.

[2] P. Gianni, V. Miller, B. Trager, Decomposition of algebras, in: Symbolic and algebraic computation (Rome, 1988), vol. 358 of Lecture Notes in Comput. Sci., Springer, Berlin, 1989, pp. 300–308.

[3] P. Hall, The classification of prime-power groups, J. Reine Angew. Math. 182 (1940) 130–141.

[4] G. T. Helleloid, U. Martin, The automorphism group of a finite p-group is almost always a p-group, J. Algebra 312 (1) (2007) 294–329.

[5] G. Higman, Enumerating p-groups. I. Inequalities, Proc. London Math. Soc. (3) 10 (1960) 24–30.

[6] D. F. Holt, B. Eick, E. A. O'Brien, Handbook of computational group theory, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2005.

[7] E. I. Khukhro, p-automorphisms of finite p-groups, vol. 246 of London Mathematical Society Lecture Note Series, Cambridge University Press, Cambridge, 1998.

[8] C. R. Leedham-Green, S. McKay, The structure of groups of prime power order, vol. 27 of London Mathematical Society Monographs. New Series, Oxford University Press, Oxford, 2002, , Oxford Science Publications.

[9] A. Mann, Some questions about p-groups, J. Austral. Math. Soc. Ser. A 67 (3) (1999) 356–379.

[10] A. G. Myasnikov, The theory of models of bilinear mappings, Sibirsk. Mat. Zh. 31 (3) (1990) 94–108.

[11] H. P. Petersson, Conjugacy of idempotents in Jordan pairs, Comm. Algebra 6 (7) (1978) 673–715.

[12] L. Rónyai, Computations in associative algebras, in: Groups and computation (New Brunswick, NJ, 1991), vol. 11 of DIMACS Ser. Discrete Math. Theoret. Comput. Sci., Amer. Math. Soc., Providence, RI, 1993, pp. 221–243.

[13] Á. Seress, Permutation group algorithms, vol. 152 of Cambridge Tracts in Mathematics, Cambridge University Press, Cambridge, 2003.

[14] C. C. Sims, Enumerating p-groups, Proc. London Math. Soc. (3) 15 (1965) 151–166.

[15] J. B. Wilson, Decomposing p-groups via Jordan algebras, submitted for publication, http://www.arxiv.org/abs/0711.0201

[16] J. B. Wilson, Finding central decompositions of p-groups, to be submitted December 2007.

[17] J. B. Wilson, Finding direct product decompositions in groups and nonassociative algebras, to be submitted December 2007.

[18] J. B. Wilson, Lie equivalent p-groups (in preparation).

[19] J. B. Wilson, p-groups, bilinear maps, and their algebras (in preparation).