Jeffrey Paul Wheeler
Research Statement

201 Regency Place
Mars, PA
16046
Cell: (412) 926-2159

607 Thackeray Hall
jpw41@pitt.edu
http://jeffreypaulwheeler.com/
Office Phone: (412) 624-8315

1 Areas of Research

The primary area of my research has thus far been in Additive Number Theory. My main accomplishments involve extending some combinatorial results which have their history in classical Number Theory to finite groups and , hence my results belong in the areas of Combinatorics, Number Theory, and Algebra.

2 A Brief History of My Main Results

Additive Number Theory can be best described as the study of sumsets of integers. By sumset, we mean for sets A and B, $A + B := \{a + b | a \in A, b \in B\}$. A very familiar result in Number Theory, namely Lagrange's theorem that every nonnegative integer can be written as the sum of four squares, can be expressed in terms of sumsets. In particular, if we let $\mathbb{N}_0$ be the set of nonnegative integers and if we let S be the set of all integers that are perfect squares, then Lagrange's Theorem has the form

$$\mathbb{N}_0 = S + S + S + S.$$

As well, if we let $\mathbb{E}$ be the set of all even integers greater than 2 and if we put P equal to the set of all primes, then the binary from of Goldbach's Conjecture can be restated as

$$\mathbb{E} \subseteq P + P.$$

We consider two classic direct problems in Additive Number Theory. The first is the classical Cauchy-Davenport Theorem and the second a conjecture of Paul Erdős and Hans Heilbronn [15] which stood as an open problem for over 30 years until partially proven in 1994. This conjecture has its roots in the theorem of Cauchy and Davenport; proven by Cauchy [7] in 1813 and independently by Davenport [10] in 1935 (Davenport discovered in 1947 [11] that Cauchy had previously proved the theorem). In particular,

Theorem 2.1. *(Cauchy-Davenport)*
Let k, l be positive integers. If nonempty $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$, p prime, with $|A| = k$ and $|B| = l$, then $|A + B| \geq min\{p, k + l - 1\}$ where $A + B := \{a + b \mid a \in A \text{ and } b \in B\}$.

It is with noting that in 1935 Inder Chowla [9] extended this result to composite m with the conditions that $0 \in B$ and the other elements of B are relatively prime to m.

In the early 1960's, Paul Erdős and Hans Heilbronn conjectured that if the addition in the Cauchy-Davenport Theorem is restricted to distinct elements the lower bound changes slightly. Erdős stated this conjecture in 1963 during a number theory conference at the University of Colorado [15]. Interestingly, Erdős and Heilbronn did not mention the conjecture in their 1964 paper on sums of sets of congruence classes [18] though Erdős mentioned it often in his lectures (see [25], page 106). Eventually the conjecture was formally stated in Erdős' contribution to a 1971 text [16] as well as in a book by Erdős and Graham in 1980 [17]. In particular,

Theorem 2.2 (Erdős-Heilbronn Problem).
Let p be a prime and A, $B \subseteq \mathbb{Z}/p\mathbb{Z}$ with $A \neq \emptyset$ and $B \neq \emptyset$. Then $|A \dot{+} B| \geq \min\{p, |A| + |B| - 3\}$, where $A \dot{+} B := \{a + b \text{ mod } p \mid a \in A,\ b \in B \text{ and } a \neq b\}$.

The conjecture was first proved for the case $A = B$ by J.A. Dias da Silva and Y.O. Hamidounne in 1994 [12] with the more general case ($A \neq B$) established by Noga Alon, Melvin B. Nathanson, and Imre Z. Ruzsa using the polynomial method in 1995 [1].

Relevant to our work we also state that Gyula Károlyi extended each result (basically) to abelian groups and extended the Cauchy-Davenport Theorem to finite groups in various papers from 2003 − 2005.

3 The Main Result

My coauthor and I did extend the Cauchy-Davenport Theorem to finite groups but discovered - the day before I presented my result to the Memphis Combinatorics Seminar - that Gyula Károlyi had already established the result. Hence we will concentrate on extending the Erdős-Heilbronn Problem to finite groups.

Extending the Erdős-Heilbronn Problem to finite groups involves the following structure of finite solvable groups[1]:

Theorem 3.1 (The Associated Field Structure Theorem).
Let G be a finite solvable group and $\theta \in \operatorname{Aut}(G)$. Then there exists a $K \trianglelefteq G$, $K \neq G$, such that

1. *$\theta(K) = K$,*
2. *$G/K \cong (\mathbb{F}_{p^n}, +)$ for some prime p and $n \geq 1$, and*
3. *$\overline{\theta}(x) = \gamma x$ where $\gamma \in \mathbb{F}_{p^n}^{\times}$, $x \in G/K$, and $\overline{\theta}$ is the map induced by θ on G/K which we identify with $\mathbb{F}_{p^n}$ by (2).*

By the theorem, for each $h \in (\mathbb{F}_{p^n}, +) \cong G/K$ we fix a representative $\hat{h} \in G$ of h and we use $\hat{0} = 1$. Define $\psi : K \times (\mathbb{F}_{p^n}, +) \to G$ by $\psi(k, h) = k\hat{h}$. We have that ψ is a bijection by

$$\begin{aligned}
\psi(k_1, h_1) \cdot \psi(k_2, h_2) &= k_1\hat{h}_1 \cdot k_2\hat{h}_2 \\
&= k_1\phi_{h_1}(k_2)\hat{h}_1\hat{h}_2 \\
&= (k_1\phi_{h_1}(k_2)g_{h_1,h_2})(\widehat{h_1 + h_2}) \\
&= \psi(k_1\phi_{h_1}(k_2)g_{h_1,h_2}, h_1 + h_2) \qquad (1)
\end{aligned}$$

where $\phi_h(k) = \hat{h}k\hat{h}^{-1}$ (so, in particular $\phi_h \in \operatorname{Aut}(K)$) and $g_{h_i,h_j} = \hat{h}_i \cdot \hat{h}_j \cdot (\widehat{h_i + h_j})^{-1} \in K$ with $\hat{h}$ the coset representative of h in G. Hence ψ can be considered an isomorphism if we put the following non-standard multiplication on $K \times (\mathbb{F}_{p^n}, +)$:

$$(k_1, h_1) \cdot (k_2, h_2) = (k_1\phi_{h_1}(k_2)g_{h_1,h_2}, h_1 + h_2).$$

In summary, for $A \subseteq G$, we can consider $A \subseteq K \times (\mathbb{F}_{p^n}, +)$, in particular, $A = \{(k_1, h_1), (k_2, h_2), \ldots, (k_t, h_t)\}$ for some $k_1, k_2, \ldots, k_t \in K$ and $h_1, h_2, \ldots h_t \in (\mathbb{F}_{p^n}, +)$.

As stated, our goal is to extend the result to finite groups. As such we need the following definitions:

[1] it is worth mentioning that there is significantly less algebraic structure required to extend the Cauchy-Davenport Theorem. The interested reader is encouraged to read my dissertation.

Definition 3.2 (Minimal Torsion Element).
Let G be a group. We define $p(G)$ to be the smallest positive integer p for which there exists a nonzero element g of G with $pg = 0$ (or, if multiplicative notation is used, $g^p = 1$). If no such p exists, we write $p(G) = \infty$.

and

Definition 3.3.
For a group G let $\mathrm{Aut}(G)$ be the group of automorphisms of G. Suppose $\theta \in \mathrm{Aut}(G)$ and $A, B \subseteq G$. Write

$$A \overset{\theta}{\cdot} B := \{a \cdot \theta(b) \mid a \in A, b \in B, \text{ and } a \neq b\}.$$

With these definitions we may now state that the above lay the groundwork for establishing

Theorem 3.4 (Erdős-Heilbronn Problem for Finite Groups).
Let G be a finte group and let $A, B \subseteq G$ with $|A| = a$ and $|B| = b$. Then $|A \overset{\theta}{\cdot} B| \geq \min\{p(G) - \delta, a + b - 3\}$ where $|A \overset{\theta}{\cdot} B| = \{ab | a \in A, b \in B, \theta \in \mathrm{Aut}(G), a \neq b\}$ and where $\delta = 1$ if θ is of even order in $\mathrm{Aut}(G)$ and $\delta = 0$ otherwise.

Actually, we showed something more general:

Theorem 3.5 (Generalized Erdős-Heilbronn for Finite Groups).
Let G be a finite group, $\theta \in \mathrm{Aut}(G)$, and let $A, B \subseteq G$ with $|A| = a$ and $|B| = b$. Then $|A \overset{\theta}{\cdot} B| \geq \min\{p(G) - \delta, a + b - 3\}$ where $\delta = 1$ if θ is of even order in $\mathrm{Aut}(G)$ and $\delta = 0$ otherwise.

This result is a very nice result on its own, but there is another aspect that makes it quite beautiful. The proof involves using the techniques of Károlyi together with the Polynomial Method of Alon, Nathanson, and Ruzsa. Hence the result is quite comprehensive in bringing together elements of the different proof techniques for previous results.

4 Co-Sidon Sets

Motivated by a question of András Sárközy, colleagues and I investigated sufficient conditions for existence of sets of natural numbers A and B such that the number of solutions of the equation $a + b = n$ where $a \in A$ and $b \in B$ is monotone increasing for $n > n_0$. We also examine pairs A, B with the property that, for every $n \geq 0$, the equation above has at most one solution, i.e. their pairwise sums are distinct.

The roots of this paper are in the notion of Sidon sets, which were a personal favorite of Erdős. In particular, Erdős and his coauthors considered the functions

$$r(A, n) = |\{(a_1, a_2) \in A \times A : a_1 + a_2 = n\}| \tag{2}$$

$$r_1(A, n) = |\{(a_1, a_2) \in A \times A : a_1 + a_2 = n \text{ and } a_1 \leq a_2\}| \tag{3}$$

$$r_2(A, n) = |\{(a_1, a_2) \in A \times A : a_1 + a_2 = n \text{ and } a_1 < a_2\}| \tag{4}$$

where $A \subseteq \mathbb{N}_0 =$ the set of nonnegative integers.

A set $A \subset \mathbb{N}$ is called *Sidon* if $r_1(A, n) \leq 1$ for all $n \in \mathbb{N}$, i.e. the sums of non-ordered pairs of elements of A are all distinct. Note that it is possible to extend the notion of a Sidon set to a pair of sets in different ways. In our paper, we considered the following generalization:

Definition 4.1 (Co-Sidon Sets).
Two sets $A, B \subset \mathbb{N}_0$ are called *co-Sidon* if $r(A, B, n) \leq 1$ for all $n \in \mathbb{N}_0$, i.e. the sums of ordered pairs from $A \times B$ are all distinct.

We showed numerous properties of Co-Sidon sets, with our main result being:

Theorem 4.2 (Main Theorem).
For all $\alpha, \beta \in [0,1]$, there exist sets $A, B \subset \mathbb{N}_0$ such that A has lower (or upper) asymptotic density α, B has lower (or upper) asymptotic density β, and $r(A, B, n)$ is monotone increasing in n.

5 Additional Work

My Master's Thesis has been well read (#4 document when Googling the *abc Conjecture*). It is listed on the abc Conjecture Home Page (`http://www.math.unicaen.fr/ nitaj/abc.html`) maintained by Abderrahmane Nitaj and cited in the online encyclopedia *everything2*'s entry for the abc Conjecture. More noteworthy, though, is that every summer I get at least one email from someone directing an REU that they used my thesis essentially as a text to introduce their students to the problem.

Additionally Jonathan Hulgan I and I answered the following question:

Let $\{a_1, a_2, a_3, \dots\}$ be any sequence of real (or complex) numbers. Define

$$\rho_n := \frac{a_1 + \cdots + a_n}{a_{n+1} + \cdots + a_{2n}}.$$

Observe that if we consider the sequence of odd integers $\{1, 3, 5, \dots\}$ then $\rho_1 = \rho_2 = \rho_3 = \cdots = \frac{1}{3}$. Define ρ to be the constant ratio, i.e. if $\rho_1 = \rho_2 = \rho_3 = \cdots =$ constant, then $\rho_1 = \rho_2 = \cdots = \rho$.

Hence we ask for each nonzero ρ, does there exist a sequence with the property

$$\rho_1 = \rho_2 = \rho_3 = \cdots = \rho? \tag{5}$$

A simpler question:
Show that if the sequence is an arithemtic progression such that $\rho_1 = \rho_2 = \rho_3 = \cdots = \rho$, then $\rho = \frac{1}{3}$. Describe which arithmetic progressions meet condition (5).

Our solution has appeared in the Pi Mu Epsilon Journal (Spring 2008).

6 Future Work

Paul Balister and I have made significant progress on the inverse problem related to our result extending the Erdős-Heilbronn Problem to finite groups (i.e. given that we have equality, what does this tell us about the structure of the. sets A and B?). It seems that it is also possible to extend other Combinatorial Number Theory results on sumsets to groups. As well, I am exploring some convergence questions with h-fold sumsets. In particular, such questions as: if A is a subset of some group G and if $hA = A + A + \cdots + A = G$, what does this tell us about G? If we consider the restricted sum, then this leads to at least two different types of convergence questions. As well, the notion of co-Sidon sets is new and - as such - there are many questions to be considered.

References

[1] Alon, Noga and Nathanson, Melvyn B. and Ruzsa, Imre *The polynomial method and restricted sums of congruence classes*, Journal of Number Theory, **56** (1996) 404–417.

[2] Alon, N. and Tarsi, M., *Colorings and orientations of graphs*, Combinatorica. An International Journal on Combinatorics and the Theory of Computing, **12** No.2 (1992) 125–134.

[3] Balister, Paul N. and Wheeler, Jeffrey Paul *The Cauchy-Davenport theorem for finite Groups*, Preprint, *http://jeffreypaulwheeler.com/*, 2006

[4] Balister, Paul N. and Wheeler, Jeffrey Paul *The Erdős-Heilbronn problem for finite groups*, *http://jeffreypaulwheeler.com/*, -to appear in *Acta Aritmetica.*

[5] Balasubramanian, R., A note on a result of Erdős, Sárközy and Sós, *Acta Arith.* **49** (1987), 45–53

[6] Benevides, F., Hulgan, J., Lemons, N., Palmer, C., Riet, A.E., and Wheeler, J.P., Additive properties of a pair of sequences, *Acta Arithmetica* 139 (2009), 185-197

[7] Cauchy, A.L., *Recherches sur les nombres*, J. École polytech., **9**, (1813) 99–116.

[8] Chen, Y. and Tang, M., On the monotonicity properties of additive representation functions, II, *preprint*

[9] Chowla, Inder, *A theorem on the addition of residue classes: application to the number* $\Gamma(k)$ *in Waring's problem.*, Proceedings of the Indian Academy of Sciences, Section A, **1**, (1935) 242–243.

[10] Davenport, H., *On the addition of residue classes*, Journal of the London Mathematical Society, **10**, (1935) 30–32.

[11] Davenport, H., *A historical note*, Journal of the London Mathematical Society, **22**, (1947) 100–101.

[12] Dias da Silva, J. A. and Hamidoune, Y. O., *Cyclic spaces for Grassmann derivatives and additive theory*, The Bulletin of the London Mathematical Society, **26** No.2, (1994) 140–146.

[13] Erdős, P., Sárközy, A. and Sós, T., Problems and results on additive properties of general sequences, III, *Studia Sci. Math. Hungar.* **22** (1987), 53–63; IV, in *Number Theory*, Proceedings, Ootacamund, India, 1984, ed. K. Alladi, Lecture Notes in Mathematics 1122, Spring-Verlag, Berlin-Heidelberg-New York, 1985, 85–104; and V, *Monatshefte Math.* **102** (1986), 183–197.

[14] Erdős, P., Turán, P. On a problem of Sidon in additive number theory, and on some related problems, *J. London Math. Soc.* **16** (1941), 212–215

[15] Erdős, P., *On the addition of residue classes (mod p)*, Proceedings of the 1963 Number Theory Conference at the University of Colorado, Univeristy of Colorado Press, (1963) 16–17.

[16] Erdős, P., Some problems in number theory, in *Computers in number theory*, edited by A.O.L. Atkin and B.J. Birch, Academic Press, (1971) 405–414.

[17] Erdős, P. and Graham, R. L., *Old and new problems and results in combinatorial number theory*, Monographies de L'Enseignement Mathématique [Monographs of L'Enseignement Mathématique], volume 28, Université de Genève L'Enseignement Mathématique, 1980.

[18] Erdős, P. and Heilbronn, H., *On the addition of residue classes (mod p)*, Acta Arithmetica, **9** (1964) 149–159.

[19] Károlyi, Gyula *On restricted set addition in abelian groups*, Annales Universitatis Scientiarum Budapestinensis de Rolando Eötvös Nominatae. Sectio Mathematica, **46** (2003) 47–53.

[20] Károlyi, Gyula *The Erdős-Heilbronn problem in abelian groups*, Israel Journal of Mathematics, **139** (2004) 349–359.

[21] Károlyi, Gyula *The Cauchy-Davenport theorem in group extensions*, L' Enseignement Mathematique, **51** (2005) 239–254.

[22] Károlyi, Gyula *An inverse theorem for the restricted set addition in abelain groups*, Journal of Algebra, **290** (2005) 557–593.

[23] Halberstam, H. and Roth, K.F., Sequences (Vol 1), *Oxford University Press*, 1966, 89–90.

[24] Krückeberg, F., B_2-Folgen und verwandte Zahlenfolgen (in German), *J. Reine Angew. Math.* **206** (1961), 53–60

[25] Nathanson, Melvyn B., *Additive number theory, inverse problems and the geometry of subsets*, Springer-Verlag, 1996.

[26] Sárközy, A., Unsolved problems in number theory, *Period. Math. Hungar.* **42** (2001), 17–35

[27] Stöhr, A., Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe II (in German), *J. Reine Angew. Math.* **194** (1955), 111–40.

[28] Tijdeman, R., Wang, L., Sums of products of powers of given prime numbers, *Paci c J. Math.* **132** (1988), 177-193. *Corr.* **135** (1988), 396-398.

[29] Wheeler, Jeffrey Paul *The abc conjecture*, Master's Thesis, *http://jeffreypaulwheeler.com/*, 2002