Idris Mercer's Research Statement

Broadly speaking, my interests are applying analytic and probabilistic methods to combinatorial problems. I am a pure mathematician, but I enjoy problems that are amenable to computational exploration. My interests tend to lie in the following MSC categories:

05A16	Asymptotic enumeration
05D40	Probabilistic methods
11A41	Primes
26C10	Polynomials: location of zeros
60C05	Combinatorial probability
94A55	Shift register sequences and sequences over finite alphabets

My publications so far can be grouped into three broad topics:

1. Sequences with good correlation properties
2. Polynomials with restricted coefficients
3. Distribution of prime numbers

Following are descriptions of these three topics, my contributions to them, and questions for future research.

1. SEQUENCES WITH GOOD CORRELATION PROPERTIES

A **binary sequence** is an n-tuple $A = (a_0, a_1, \ldots, a_{n-1})$ where each a_j is ± 1. We define the (acyclic) **autocorrelations** of A by

$$c_k = \sum_{j=0}^{n-k-1} a_j a_{j+k} \qquad (0 \le k \le n-1)$$

which we can regard as dot products that measure how closely the sequence A resembles shifted versions of itself. Note that $c_0 = n$, which we can call the 'trivial' autocorrelation.

For example, one of the 32 binary sequences of length 5 is $(+1, +1, +1, -1, +1)$, which we can abbreviate as $+ + + - +$. Its nontrivial acyclic autocorrelations can be visualized as follows.

+	+	+	−	+	
	+	+	+	−	+

$c_1 = +1 + 1 - 1 - 1 = 0$

+	+	+	−	+		
		+	+	+	−	+

$c_2 = +1 - 1 + 1 = +1$

+	+	+	−	+			
			+	+	+	−	+

$c_3 = -1 + 1 = 0$

+	+	+	−	+				
				+	+	+	−	+

$c_4 = +1$

A surprisingly subtle question is: Among the 2^n binary sequences of length n, can we find one whose autocorrelations are collectively close to zero? (In digital communication, this is like finding a signal that is uncorrelated with shifted versions of itself, but it can also be studied as a purely combinatorial problem.)

A binary sequence is called a **Barker sequence** if it satisfies $c_k \in \{-1, 0, +1\}$ for all $k \neq 0$. For parity reasons, this is the closest to zero that the autocorrelations of a binary sequence could possibly be. There are Barker sequences of lengths 2, 3, 4, 5, 7, 11, and 13. For example, one can verify that the sequence

$$+++++--++-+-+$$

(abbreviating in the same way as before) satisfies $c_1 = c_3 = \cdots = c_{11} = 0$ and $c_2 = c_4 = \cdots = c_{12} = +1$. However, it is known that there are no Barker sequences of length n for $13 < n \leq 4 \cdot 10^{33}$, and it has been conjectured at least since 1960 that there are no Barker sequences of length greater than 13. See, for example, Section 3.1 of [26].

If Barker sequences are rare, how close to zero can we make the autocorrelations of a length n binary sequence? If A is a length n binary sequence, then two natural measures of that closeness are

$$P(A) = \max_{1 \leq k \leq n-1} |c_k|,$$
$$E(A) = \sum_{1 \leq k \leq n-1} c_k^2,$$

which we call the **peak sidelobe level** (PSL) and **energy** of A respectively. We can then define two functions of n:

$$P_{\min}(n) = \min_A P(A),$$
$$E_{\min}(n) = \min_A E(A),$$

where the minimum is taken over all 2^n binary sequences of length n.

The asymptotic growth rates of the functions $P_{\min}$ and $E_{\min}$ are unknown. In the presumably unlikely event that there exists an infinite family of Barker sequences, their PSL would be 1 and their energy would grow like $n/2$. It has been conjectured that in fact, $P_{\min}(n)$ grows like a multiple of $\sqrt{n}$, but this has not been proved.

In a 2006 article [11], I used probabilistic methods to show that if $\varepsilon > 0$, then asymptotically almost all length n binary sequences A satisfy

$$P(A) \leq (\sqrt{2} + \varepsilon)\sqrt{n \log n}.$$

(Here, 'log' is natural log, and 'asymptotically almost all' means the proportion of length n binary sequences with a property approaches 1 as $n \to \infty$.) This improved upon a 1968 result of Moser and Moon [21], and was itself improved upon by Alon et al. in 2010 [1] and by Schmidt in 2014 [25]. One result of Alon et al. is that if $\varepsilon > 0$, then asymptotically almost all length n binary sequences A satisfy

$$P(A) \leq \sqrt{2n(\log n - (1.5 - \varepsilon) \log \log n)}.$$

In a 2016 article [17], I showed that for all $n > 1$, there exists a length n binary sequence A satisfying

$$P(A) \leq \sqrt{2n(\log n - \log \log n + 0.862)},$$

which does not improve upon Alon et al. in an asymptotic sense, but which does hold for all sequence lengths.

Schmidt's 2014 work mentioned above shows that if $\varepsilon > 0$, then asymptotically almost all length n binary sequences satisfy

$$(\sqrt{2} - \varepsilon)\sqrt{n \log n} \leq P(A) \leq (\sqrt{2} + \varepsilon)\sqrt{n \log n},$$

so informally, the PSL of 'most' binary sequences is close to $\sqrt{2n \log n}$. There still could exist 'rare' binary sequences whose PSL grows like $\sqrt{n \log \log n}$ or $\sqrt{n}$ or smaller. Numerical evidence suggests that a 2012 construction of Schmidt [24] gives a family of binary sequences whose PSL grows like $\sqrt{n \log \log n}$, but this has not been proved.

As a generalization of binary sequences, one can study **complex sequences** or **unimodular sequences**, which are n-tuples $A = (a_0, a_1, \ldots, a_{n-1})$ where each a_j is a complex number of modulus 1. If the a_j are mth roots of unity, then we call the sequence an **m-phase sequence** or **polyphase sequence**. The (acyclic) autocorrelations of a complex sequence are defined by

$$c_k = \sum_{j=0}^{n-k-1} \overline{a_j} a_{j+k} \qquad (0 \leq k \leq n-1)$$

where the bar denotes complex conjugation. Just as with binary sequences, the autocorrelations can be regarded as dot products, and a complex sequence with autocorrelations near zero can be regarded as a signal that is uncorrelated with shifted versions of itself. We can define the PSL and energy of a complex sequence:

$$P(A) = \max_{1 \leq k \leq n-1} |c_k|,$$

$$E(A) = \sum_{1 \leq k \leq n-1} |c_k|^2.$$

A complex sequence satisfying $|c_k| \leq 1$ for all $k \neq 0$ is known as a **generalized Barker sequence** or **unimodular Barker sequence**.

Generalized Barker sequences have been found for all lengths up to N, where the value of N has been gradually increasing. It was conjectured at one time [8] that there are no generalized Barker sequences of length significantly greater than 36, but it was subsequently shown [22] that they exist for all lengths up to 70.

Chu sequences are a previously studied family of polyphase sequences that have good autocorrelation properties. Based on observation of sequence lengths into the thousands, it was conjectured [2] that the energy of Chu sequences grows like $O(n^{3/2})$, where n is the sequence length. In a 2013 article [16], I proved this conjecture, which was the first time a family of complex sequences was shown to have energy bounded above by a multiple of $n^{3/2}$ for all lengths n. Note that if there are generalized Barker sequences of all lengths, then more would be true, because their energy would grow at most linearly in n. However, this has not been proved.

Questions for further research on sequences:

- Can one prove that there is a family of length n binary sequences (using Schmidt's 2012 construction, or otherwise) whose PSL grows more slowly than $O(\sqrt{n \log n})$, such as $O(\sqrt{n \log \log n})$ or $O(\sqrt{n})$?
- Empirically, the distribution of the energy of binary sequences of fixed length resembles the Gumbel distribution. Can one prove that this is the correct asymptotic distribution?
- Can one prove the existence of generalized Barker sequences for more lengths than are currently known, or for infinitely many lengths?
- If there is an infinite family of generalized Barker sequences, then their energy grows like $O(n)$. Can one prove the existence of an infinite family of unimodular sequences whose energy grows more slowly than the best currently known bound of $O(n^{3/2})$?

2. POLYNOMIALS WITH RESTRICTED COEFFICIENTS

A **Littlewood polynomial** has coefficients that are $+1$ or -1, and a **Newman polynomial** has coefficients that are 0 or 1. More precisely, a polynomial of the form

$$\alpha(z) = a_0 + a_1 z + a_2 z^2 + \cdots + a_{n-1} z^{n-1} \qquad (a_j = \pm 1 \text{ for all } j)$$

is called a Littlewood polynomial of length n, and a polynomial of the form

$$\beta(z) = z^{b_1} + z^{b_2} + \cdots + z^{b_n} \qquad (b_1 < \cdots < b_n \text{ are nonnegative integers})$$

is called a Newman polynomial of length n. There are exactly 2^n Littlewood polynomials of length n, and infinitely many Newman polynomials of length n (since there is no upper bound on the b_j). Note also that there is an obvious bijection between Littlewood polynomials of length n and binary sequences of length n.

There is a rich literature regarding the behavior of Littlewood or Newman polynomials on the unit circle in the complex plane. Note that if $|z| = 1$ and $\alpha(z)$ and $\beta(z)$ are as above, then both $\alpha(z)$ and $\beta(z)$ are sums of n terms that each have modulus 1. So we have both $0 \le |\alpha(z)| \le n$ and $0 \le |\beta(z)| \le n$ on the unit circle.

Denote the unit circle by $\mathbb{S}$. It is easy to find Littlewood or Newman polynomials that have zeros on $\mathbb{S}$. If

$$\gamma(z) = 1 + z - z^2 + z^3 + z^4 - z^5 + z^6 + z^7 - z^8 + z^9 + z^{10} - z^{11}$$

then we could say $\gamma(z)$ has 'coefficient sequence'

$$+ + - + + - + + - + + -$$

which, informally, is a 'periodic' sequence. Note that $\gamma(z)$ can be written as

$$\gamma(z) = (1 + z - z^2)(1 + z^3 + z^6 + z^9) = (1 + z - z^2)(1 - z^{12})/(1 - z^3)$$

which will have zeros at the 12th roots of unity that are not cube roots of unity. Note also that $1+z^3+z^6+z^9$ is a Newman polynomial with zeros on $\mathbb{S}$. Informally, these polynomials have zeros on $\mathbb{S}$ for 'obvious' reasons.

The literature on Littlewood and Newman polynomials is often concerned with the opposite tendency: polynomials with relatively high minimum modulus on $\mathbb{S}$, as opposed to polynomials whose modulus dips down to 0 somewhere on $\mathbb{S}$. So speaking very informally, we want polynomials whose coefficient sequences are 'far' from periodic. Here we can see a relationship to the topic of autocorrelation.

If $\alpha(z)$ is any length n Littlewood polynomial and $|z| = 1$, then we have

$$\begin{aligned} |\alpha(z)|^2 &= \alpha(z) \cdot \overline{\alpha(z)} \\ &= \Big(a_0 + a_1 z + \cdots + a_{n-1} z^{n-1}\Big)\Big(a_0 + a_1 \frac{1}{z} + \cdots + a_{n-1} \frac{1}{z^{n-1}}\Big) \end{aligned}$$

and the autocorrelations of the binary sequence $(a_0, \ldots, a_{n-1})$ arise naturally when we expand. In particular, the average value of $|\alpha(z)|^2$ over $\mathbb{S}$ is $c_0 = n$ (which is also the sum of the squares of the coefficients of α) and so the usual L^2 norm of $\alpha(z)$ on $\mathbb{S}$ is $\sqrt{n}$.

Authors including Erdős and Littlewood have made conjectures that, loosely speaking, involve trying to find length n Littlewood polynomials $\alpha(z)$ that are 'flat' on $\mathbb{S}$, in the sense that $|\alpha(z)|$ stays 'close' to its L^2 average of $\sqrt{n}$, as opposed to dipping down near 0 or rising up near n. See, for instance, Problem 26 in [7] or Problem 19 in [10]. One currently unproved conjecture (part of a conjecture of Littlewood) is as follows.

Conjecture: There is a positive constant K (perhaps $K = 1/2$) such that for all n, there exists a length n Littlewood polynomial $\alpha(z)$ such that

$$|\alpha(z)| \ge K\sqrt{n} \qquad \text{for all } z \in \mathbb{S}.$$

Computations in [23] reveal that for each n in the set

$$\{11, 12, 13, \ldots, 25\} \cup \{27, 29, 31, \ldots, 65\},$$

there exists a length n Littlewood polynomial $\alpha(z)$ that satisfies $|\alpha(z)| \geq 0.56\sqrt{n}$ for all $z \in \mathbb{S}$.

Define $\lambda(n)$ to be the highest minimum modulus on $\mathbb{S}$ among all 2^n Littlewood polynomials of length n. Then the conjecture on page 4 is that $\lambda(n) \geq K\sqrt{n}$ for some positive K. It was shown by Carroll et al. [6] that $\lambda(n) > n^{0.4308}$.

Relevant to these questions is the specific length 13 Littlewood polynomial

$$\delta(z) = 1 + z + z^2 + z^3 + z^4 - z^5 - z^6 + z^7 + z^8 - z^9 + z^{10} - z^{11} + z^{12}$$

whose coefficient sequence is the length 13 Barker sequence. As z ranges over $\mathbb{S}$, it turns out that $|\delta(z)|$ never dips below 83% of its L^2 average of $\sqrt{13}$. So this polynomial has unusually high minimum modulus on $\mathbb{S}$.

The total number of length n Littlewood polynomials is 2^n, which grows quickly enough to make it difficult to do brute-force exhaustive searches. We thus sometimes focus on special types of Littlewood polynomials that have certain symmetries and hence, informally speaking, fewer 'degrees of freedom'.

Let $\alpha(z) = a_0 + \cdots + a_{n-1}z^{n-1}$ be any Littlewood polynomial. If we have $a_j = a_{n-1-j}$ for all j, we say $\alpha(z)$ is **palindromic**. If n is odd, say $n = 2m + 1$, then if we have $a_{m+j} = (-1)^j a_{m-j}$ for all j, we say $\alpha(z)$ is **skew-symmetric**. The polynomial $\delta(z)$ shown above is skew-symmetric, as are many of the polynomials with high minimum modulus in [6] and [23].

In a 2006 article [12], I proved that a skew-symmetric Littlewood polynomial cannot have any zeros on the unit circle, as well as providing a new proof of the known result that a palindromic Littlewood polynomial must have a zero on the unit circle.

Switching our attention from Littlewood polynomials to Newman polynomials, define the function

$$M(b_1, \ldots, b_n) = \min_{z \in \mathbb{S}} \left| z^{b_1} + \cdots + z^{b_n} \right|$$

and then define

$$\mu(n) = \sup M(b_1, \ldots, b_n)$$

where the supremum is taken over all sets of n nonnegative integers. In other words, $\mu(n)$ is the highest minimum modulus on $\mathbb{S}$ of a length n Newman polynomial. Note that in these definitions, as well as assuming $b_1 < \cdots < b_n$, we can assume $b_1 = 0$, because if $z \in \mathbb{S}$, we have

$$\begin{aligned} \left| z^{b_1} + z^{b_2} + \cdots + z^{b_n} \right| &= \left| z^{b_1}(1 + z^{b_2 - b_1} + \cdots + z^{b_n - b_1}) \right| \\ &= \left| 1 + z^{b_2 - b_1} + \cdots + z^{b_n - b_1} \right|. \end{aligned}$$

Notice that $\mu(n)$ is mathematically well-defined, but it is not obvious how to compute $\mu(n)$ for a given n in a finite number of steps, since there is no upper bound on the b_j. Playing with specific examples can lead to some conjectures:

$$\begin{aligned} &\mu(3) \text{ appears to be } M(0, 1, 3) \approx 0.607346, \\ &\mu(4) \text{ appears to be } M(0, 1, 2, 4) \approx 0.752394, \\ &\mu(5) \text{ appears to be } M(0, 1, 2, 6, 9) = 1. \end{aligned}$$

Not much is known about the function $\mu(n)$. In the 1980s, Boyd conjectured [4] that $\mu(n) > 1$ for all $n \geq 6$, and further conjectured that $\mu(n)$ approaches infinity with n, perhaps growing like n^c where c is a positive constant.

In a 2012 article [15], I proved that $\mu(n) > 0$ for each $n > 2$, and found examples showing that $\mu(n) > 1$ for $6 \leq n \leq 20$. There is a construction showing that $\mu(n) > n^{0.14}$ when n is a power of 9, but very little seems to be known about lower bounds for $\mu(n)$ that hold for all n.

In 1983, Campbell et al. [5] proved that $\mu(3) = M(0,1,3)$, and in 1992, Goddard [9] proved that $\mu(4) = M(0,1,2,4)$. The conjecture that $\mu(5) = 1$ has still not been proved. In an unpublished work [20], I show that $\mu(5) \leq 1+\pi/6$ and that for every positive ε, the task of showing $\mu(5) \leq 1+\varepsilon$ can be reduced to checking a finite number of cases.

In addition to studying the function $\mu(n)$, we can ask about the proportion of length n Newman polynomials that have zeros on the unit circle (or that have other properties). Although the set of all length n Newman polynomials is infinite, we can define

$$\mathrm{Newm}_n(K) = \left\{1 + z^{b_2} + \cdots + z^{b_n} \mid 0 < b_2 < \ldots < b_n \leq K\right\}$$

which is a set of size $\binom{K}{n-1}$. (We assume $b_1 = 0$ for reasons discussed previously.) Then, if S is the set of all length n Newman polynomials that have some property P, it is reasonable to define

$$\lim_{K\to\infty} \frac{|S \cap \mathrm{Newm}_n(K)|}{|\mathrm{Newm}_n(K)|}$$

to be the proportion of length n Newman polynomials that have property P.

In a 2012 article [14], I proved that using this definition, we have:

1/4 of length 3 Newman polynomials are reducible over the rationals,

1/4 of length 3 Newman polynomials have zeros on the unit circle,

3/7 of length 4 Newman polynomials are reducible over the rationals,

3/7 of length 4 Newman polynomials have zeros on the unit circle,

and I proved that certain plausible conjectures imply that the proportion of length 5 Newman polynomials with zeros on the unit circle is precisely 909/9464.

In a 2008 article [3], my coauthors and I found explicit formulae for the average fourth power of the L^4 norm of a Newman polynomial on $\mathbb{S}$ (for natural meanings of 'average'), and showed that this gave a new proof of a known result about what are called **Sidon sets** in additive number theory.

Questions for further research on polynomials:

- Can one prove that $\lambda(n) > \sqrt{n}/2$ for more values of n than currently known, or for infinitely many n? If not, can we improve upon the result of Carroll et al. that $\lambda(n) > n^{0.4308}$?
- What proportion of Littlewood polynomials of length n have zeros on the unit circle?
- Can one prove that $\mu(n) > 1$ for all $n \geq 6$? Probabilistic methods may be useful here, since Newman polynomials with minimum modulus greater than 1 do not appear to be rare.
- Can one prove that for infinitely many n, we have $\mu(n) > f(n)$ for some function $f(n)$ that grows faster than $n^{0.14}$?
- Can one prove that $\mu(n)$ can be calculated for a given n in finitely many steps (even an impractically large finite number)?
- Can one prove anything about the proportion of Newman polynomials of length 6 (or 7, or higher) that have roots on the unit circle?

3. DISTRIBUTION OF PRIME NUMBERS

I have had two articles published in the American Mathematical Monthly giving alternative proofs that there are infinitely many prime numbers. One [13] was a variant of Furstenberg's topological proof, rephrased without the language of topology. The other [18] is a short explicit argument based on an idea of Chaitin.

More broadly, I am interested in new elementary proofs of classic results from number theory, such as those regarding the distribution of primes. For instance, in an unpublished work [19], I provide a combinatorial argument (using values of Jacobsthal's function) that every arithmetic progression with common difference at most 76 contains at least one prime, and I also show that certain plausible bounds on the growth of Jacobsthal's function would lead to an elementary proof of Dirichlet's theorem.

References

[1] N. Alon, S. Litsyn & A. Shpunt, *Typical peak sidelobe level of binary sequences*, IEEE Trans. Inform. Theory **56** (2010), 545–554.

[2] M. Antweiler & L. Bömer, *Merit factor of Chu and Frank sequences*, Electron. Lett. **26** (1990), 2068–2070.

[3] P. Borwein, K.-K. S. Choi & I. Mercer, *Expected norms of zero-one polynomials*, Canad. Math. Bull. **51** (2008), 497–507.

[4] D. W. Boyd, *Large Newman polynomials*, in *Diophantine analysis (Kensington, 1985)*, 159–170, London Math. Soc. Lecture Note Ser., 109, Cambridge Univ. Press, Cambridge (1986).

[5] D. M. Campbell, H. R. P. Ferguson & R. W. Forcade, *Newman polynomials on* $|z| = 1$, Indiana Univ. Math. J. **32** (1983), 517–525.

[6] F. W. Carroll, D. Eustice & T. Figiel, *The minimum modulus of polynomials with coefficients of modulus one*, J. London Math. Soc. **16** (1977), 76–82.

[7] P. Erdős, *Some unsolved problems*, Michigan Math. J. **4** (1957), 291–300.

[8] M. Friese, *Polyphase Barker sequences up to length 36*, IEEE Trans. Inform. Theory **42** (1996), 1248–1250.

[9] B. Goddard, *Finite exponential series and Newman polynomials*, Proc. Amer. Math. Soc. **116** (1992), 313–320.

[10] J. E. Littlewood, *Some Problems in Real and Complex Analysis*, D. C. Heath and Co., Lexington, MA (1968).

[11] I. Mercer, *Autocorrelations of random binary sequences*, Combin. Probab. Comput. **15** (2006), 663–671.

[12] I. Mercer, *Unimodular roots of special Littlewood polynomials*, Canad. Math. Bull. **49** (2006), 438–447.

[13] I. Mercer, *On Furstenberg's proof of the infinitude of primes*, Amer. Math. Monthly **116** (2009), 355–356.

[14] I. Mercer, *Newman polynomials, reducibility, and roots on the unit circle*, Integers **12** (2012), paper no. A6, 16 pp.

[15] I. Mercer, *Newman polynomials not vanishing on the unit circle*, Integers **12** (2012), paper no. A67, 7 pp.

[16] I. Mercer, *Merit factor of Chu sequences and best merit factor of polyphase sequences*, IEEE Trans. Inform. Theory **59** (2013), 6083–6086.

[17] I. Mercer, *Bounding the peak sidelobe level of binary sequences of all lengths*, IEEE Trans. Inform. Theory **62** (2016), 4775–4777.

[18] I. Mercer, *Another proof that there are infinitely many primes*, Amer. Math. Monthly **124** (2017), 169.

[19] I. Mercer, *Dirichlet's theorem and Jacobsthal's function*, `arXiv:1708.05415` (2017).

[20] I. Mercer, *Finite searches, Chowla's cosine problem, and large Newman polynomials*, `arXiv:1709.06612` (2017).

[21] J. W. Moon & L. Moser, *On the correlation function of random binary sequences*, SIAM J. Appl. Math. **16** (1968), 340–343.

[22] C. J. Nunn & G. E. Coxson, *Polyphase pulse compression codes with optimal peak and integrated sidelobes*, IEEE Trans. Aerosp. Electron. Syst. **45** (2009), 775–781.

[23] L. Robinson, *Polynomials with plus or minus one coefficients: Growth properties on the unit circle*, M.Sc. thesis, Simon Fraser University (1997).

[24] K.-U. Schmidt, *Binary sequences with small peak sidelobe level*, IEEE Trans. Inform. Theory **58** (2012), 2512–2515.

[25] K.-U. Schmidt, *The peak sidelobe level of random binary sequences*, Bull. Lond. Math. Soc. **46** (2014), 643–652.

[26] K.-U. Schmidt, *Sequences with small correlation*, Des. Codes Cryptogr. **78** (2016), 237–267.