Idris Mercer's Research Interests (October 2013)

I am interested in combinatorics, number theory, and classical analysis. More specifically, I tend to be attracted to problems in the following MSC categories:

05A16	Asymptotic enumeration
05D40	Probabilistic methods
11C08	Polynomials
26C10	Polynomials: location of zeros

My publications have mostly been concerned with two topics: sequences with good autocorrelation properties, and polynomials with restricted coefficients.

Sequences with Good Autocorrelation Properties

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

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

and can be regarded as measuring how closely the sequence A resembles shifted versions of itself. Note that $c_0 = n$, which we 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 autocorrelations can be visualized as follows.

+	+	+	−	+	
	+	+	+	−	+

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

+	+	+	−	+		
		+	+	+	−	+

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

+	+	+	−	+			
			+	+	+	−	+

$$c_3 = -1 + 1 = 0$$

+	+	+	−	+				
				+	+	+	−	+

$$c_4 = +1 = 1$$

A notorious problem, arising originally in signal processing, asks to find binary sequences of length n whose autocorrelations are as close to zero as possible. For parity reasons, the closest to zero imaginable is if $c_k \in \{-1, 0, +1\}$ for $k \neq 0$.

A binary sequence satisfying $|c_k| \leq 1$ for all $k \neq 0$ is called a **Barker sequence**. There exist Barker sequences of lengths $2, 3, 4, 5, 7, 11$, and 13. For example, a Barker sequence of length 13 is given by (abbreviating as on page 1)

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

whose nontrivial autocorrelations are all 0 or 1.

It is known that there are no Barker sequences of any length from 14 to $2 \cdot 10^{30}$ (see [9]). It has been conjectured, but not proved, that there are only finitely many Barker sequences.

Since Barker sequences are rare, we can ask: How close to zero can we make the autocorrelations of a binary sequence? Two measures of that closeness are

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

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

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

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

Little is known about the true growth rates of the functions $E_{\min}$ and $P_{\min}$. It is conjectured that $P_{\min}(n) = O(\sqrt{n})$ and $E_{\min}(n) = O(n^2)$. (If there is an infinite family of Barker sequences, their PSL is 1 and their energy grows like $n/2$.) To find upper bounds for $E_{\min}(n)$ or $P_{\min}(n)$, we must show the existence of families of binary sequences whose autocorrelations achieve a certain "closeness" to zero. This can be done either directly or indirectly.

I used probabilistic methods to prove [11] that for all $\varepsilon > 0$, there exists $N \in \mathbb{Z}^+$ such that

$$P_{\min}(n) \leq (\sqrt{2} + \varepsilon)\sqrt{n \log n} \qquad \text{for all } n \geq N.$$

This improved upon the best upper bound for $P_{\min}$ appearing in the previous literature. Later, K. Schmidt proved [17] via an explicit construction that

$$P_{\min}(n) \leq \sqrt{2n \log 2n}.$$

There are also recent results [1, 18] saying, roughly paraphrased, that "most" binary sequences have PSL "near" $\sqrt{2n \log n}$ (this can be made more precise).

This of course does not rule out the possible existence of "rare" binary sequences whose PSL is closer to, say, $\sqrt{n \log\log n}$ or $\sqrt{n}$, or even lower.

As a generalization of binary sequences, one can study **complex 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 1, we call the sequence an **m-phase sequence** or **polyphase sequence**.) The autocorrelations are then defined by

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

where the bar denotes complex conjugation. We can study PSL or energy of complex sequences (the energy is defined by $\sum_{k \neq 0} |c_k|^2$). A complex sequence satisfying $|c_k| \le 1$ for all $k \neq 0$ is called a **generalized Barker sequence**.

Generalized Barker sequences exist for all lengths up to N, where the value of N has been gradually increasing. It was conjectured at one time [7] that there are no generalized Barker sequences of length significantly greater than 36, but it was subsequently shown [16] that they exist for all lengths up to 70.

How close to zero can we make the autocorrelations of a complex sequence? Chu sequences are a previously studied class of polyphase sequences that have good autocorrelation properties. Based on empirical observation of sequence lengths into the thousands [2], it was conjectured that the energy of Chu sequences grows like $O(n^{3/2})$. I proved this conjecture [15], 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 n.

Questions for further research on sequences:

- Can one simplify the proofs of nonexistence of Barker sequences for certain lengths?
- Can one show the existence of binary sequences with PSL smaller 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 probability distribution. Can one prove that this is the correct asymptotic distribution?
- Can one show the existence of generalized Barker sequences for more lengths than currently known, or for infinitely many lengths?
- If there are infinitely many generalized Barker sequences, their energy grows at most linearly in n. Can one show the existence of a family of complex sequences whose energy grows more slowly than the best known bound of $O(n^{3/2})$?

Polynomials with Restricted Coefficients

Determining information about a polynomial and its roots from its coefficients is a very old topic in mathematics. Even if those coefficients are chosen from a small finite set, some natural questions turn out to be surprisingly subtle. If

$$\alpha(z) = a_0 + a_1 z + \cdots + a_{n-1} z^{n-1}$$

then we call $\alpha(z)$ a **Littlewood polynomial** if each $a_j \in \{-1, +1\}$, and we call $\alpha(z)$ a **Newman polynomial** if each $a_j \in \{0, 1\}$. The **length** of either of those two types of polynomial is the number of coefficients that are nonzero.

Note that there is a natural bijection between sequences $A = (a_0, \ldots, a_{n-1})$ and polynomials $\alpha(z) = a_0 + \cdots + a_{n-1} z^{n-1}$. There is a general tendency for the autocorrelations of the sequence A to be related to the behavior of the polynomial $\alpha(z)$ on the unit circle. (If z is on the unit circle and α has real coefficients, then $|\alpha(z)|^2 = \alpha(z) \cdot \overline{\alpha(z)} = \alpha(z) \cdot \alpha(1/z)$, and the autocorrelations arise naturally when we expand.)

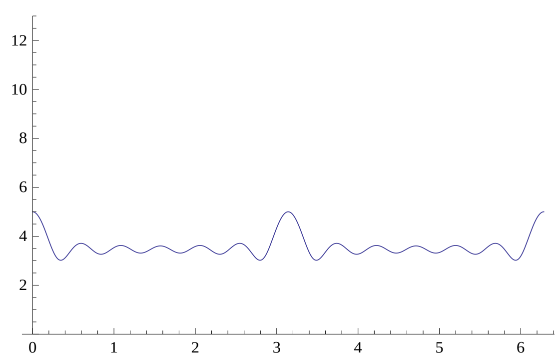
Denote the unit circle by $\mathbb{S}$. Some interesting questions involve: Among a specified class of polynomials, which ones have zeros on $\mathbb{S}$, and which ones have high minimum modulus on $\mathbb{S}$?

As an illustrative example, consider the polynomial

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

whose coefficient sequence is the length 13 Barker sequence from page 2. This is one of the $2^{13} = 8192$ Littlewood polynomials of length 13, and it happens to have higher minimum modulus on $\mathbb{S}$ than any other length 13 Littlewood polynomial.

Note that for $z \in \mathbb{S}$, any length 13 Littlewood polynomial $\alpha(z)$ is a sum of 13 terms of modulus 1, and therefore trivially $0 \le |\alpha(z)| \le 13$. Also, the L^2 norm on the unit circle of any such α is $\sqrt{13}$. The fact that the above polynomial β has unusually high minimum modulus can be rephrased by saying that for $z \in \mathbb{S}$, $|\beta(z)|$ never dips very far below its L^2 average of $\sqrt{13}$. More specifically, if $z = e^{i\theta}$, then the minimum value of $|\beta(z)|$ for $0 \le \theta \le 2\pi$ is $\approx 3.01974 \approx 0.8375\sqrt{13}$.



In order to state some questions about polynomials more precisely, we now give some definitions.

$$L(a_0, \ldots, a_{n-1}) = \min_{z \in \mathbb{S}} \left| a_0 + a_1 z + \cdots + a_{n-1} z^{n-1} \right| \quad (a_j = \pm 1)$$
$$M(b_1, \ldots, b_n) = \min_{\theta} (\cos b_1 \theta + \cdots + \cos b_n \theta) \quad (b_j \in \mathbb{Z},\ 1 \leq b_1 < \cdots < b_n)$$
$$N(b_1, \ldots, b_n) = \min_{z \in \mathbb{S}} \left| z^{b_1} + \cdots + z^{b_n} \right| \quad (b_j \in \mathbb{Z},\ 0 \leq b_1 < \cdots < b_n)$$

So for instance, L and N represent the minimum modulus on $\mathbb{S}$ of a specific Littlewood or Newman polynomial of length n.

We then further define

$$\lambda(n) = \max_{\{a_j\}} L(a_0, \ldots, a_{n-1})$$
$$\mu(n) = -\max_{\{b_j\}} M(b_1, \ldots b_n)$$
$$\nu(n) = \max_{\{b_j\}} N(b_1, \ldots, b_n)$$

where the maxima range over all sets of a_j or b_j as specified previously. Note that for a given n, there are finitely many possibilities for the a_j, but infinitely many possibilities for the b_j. Note also that $M(b_1, \ldots, b_n)$ is negative.

So roughly speaking, the functions λ, μ, ν are measures of the "best" Littlewood polynomial or cosine polynomial or Newman polynomial of length n, where "best" means "highest minimum".

There is a huge gap between what has been conjectured and what has been proved about the functions λ, μ, ν. Note that statements of the form $\lambda(n) > 0$ or $\nu(n) > 0$ are equivalent to saying that there exists a Littlewood polynomial or Newman polynomial of length n without zeros on $\mathbb{S}$. One topic of research is to try to characterize the Littlewood polynomials or Newman polynomials that have zeros on $\mathbb{S}$. Another is to find bounds on the functions λ, μ, ν.

I proved in [12] that a Littlewood polynomial with a so-called "skew-symmetric" coefficient sequence cannot have any zeros on $\mathbb{S}$, as well as giving a new proof of the known result that a Littlewood polynomial with a palindromic coefficient sequence must have zeros on $\mathbb{S}$.

In a joint publication [3], my coauthors and I computed average L^4 norms for certain natural classes of Newman polynomials, and showed that this gave a new proof of a known result about existence of Sidon sets.

I proved the following in [13], which can be made precise in a natural way:

- Exactly 1/4 of length 3 Newman polynomials have zeros on $\mathbb{S}$
- Exactly 3/7 of length 4 Newman polynomials have zeros on $\mathbb{S}$
- At least 909/9464 of length 5 Newman polynomials have zeros on $\mathbb{S}$

Empirically speaking, Newman polynomials without zeros on $\mathbb{S}$ do not appear to be rare. Nevertheless, it is nontrivial to prove that they exist for all lengths, which I accomplished in [14]. Notice that this result can be rephrased in the form: $\nu(n) > 0$ for all n.

Much more is conjectured about the function ν. It has been conjectured [4] that $\nu(n) > 1$ for all $n \geq 6$, and that $\nu(n)$ approaches infinity with n.

A conjecture due to Littlewood [10] says, in part, that for all n, there is a Littlewood polynomial α of length n such that $|\alpha(z)| \geq C\sqrt{n}$ for all $z \in \mathbb{S}$, where $C > 0$ is constant. In other words, it is conjectured that $\lambda(n) \geq C\sqrt{n}$. Explicit computations have shown that $\lambda(n) \geq 0.56\sqrt{n}$ for all n in $\{11, 12, 13, \ldots, 25\} \cup \{27, 29, 31, \ldots, 65\}$. However, the known infinite family of Littlewood polynomials that comes closest to showing $\lambda(n) \geq C\sqrt{n}$ is a family whose minimum modulus grows like $n^{0.4308}$. That family is built out of the polynomial β on page 4, and the lengths n are powers of 13.

A conjecture due to Chowla [6] is that the function $\mu(n)$ on page 5 grows like a constant times $\sqrt{n}$. (In other words, the highest minimum of a length n cosine polynomial is roughly $-C\sqrt{n}$.) This is still unproved, but people have found both upper and lower bounds for $\mu(n)$, with some space between them.

Notice that computing $\mu(n)$ or $\nu(n)$ for specific values of n is nontrivial, because there are infinitely many possibilities for the b_j. It was shown in 1983 [5] that

$$\nu(3) = \sqrt{\frac{47 - 14\sqrt{7}}{27}} \approx 0.607346$$

and it was shown in 1992 [8] that

$$\nu(4) = \min_{-1 \leq x \leq 1} \sqrt{16x^4 + 8x^3 - 8x^2 - 2x + 2} \approx 0.752394.$$

I am unaware of anyone computing specific values of $\mu(n)$. In an unpublished note, I show that $\mu(2) = 9/8 = 1.125$ and that $\mu(3) = (17+7\sqrt{7})/27 \approx 1.315565$. It would perhaps be of more interest to have a proof that $\mu(n)$ can be calculated for a given n in a finite number of steps.

Questions for further research on polynomials:

- Can one prove that $\nu(n) > 1$ for all $n \geq 6$? It may be helpful to study random Newman polynomials whose degree is not much bigger than their length.
- Can one prove that $\lambda(n) \geq C\sqrt{n}$ for all n, where $C > 0$ is constant (maybe $C = 1/2$)? If not, can one prove that the highest minimum modulus of Littlewood polynomials on $\mathbb{S}$ grows faster than $n^{0.4308}$ (for example, maybe $\sqrt{n/\log n}$)? It may be helpful to study random skew-symmetric Littlewood polynomials.
- Can one show that the computation of $\mu(n)$ or $\nu(n)$ for a given n can be reduced to a finite problem (even an impractically large finite problem)?

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. Choi & I. Mercer, *Expected norms of zero-one polynomials*, Canad. Math. Bull. **51** (2008), 497–507.

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

[6] S. Chowla, *Some applications of a method of A. Selberg,* J. Reine Angew. Math. **217** (1965), 128–132.

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

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

[9] K. Leung & B. Schmidt, *New restrictions on possible orders of circulant Hadamard matrices*, Des. Codes Cryptogr. **64** (2012), 143–151.

[10] J. Littlewood, *On polynomials* $\sum^n \pm z^m$, $\sum^n e^{\alpha_m i} z^m$, $z = e^{\theta_i}$, J. London Math. Soc. **41** (1966), 367–376.

[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, *Newman polynomials, reducibility, and roots on the unit circle*, Integers **12** (2012), A6, 16 pp.

[14] I. Mercer, *Newman polynomials not vanishing on the unit circle*, Integers **12** (2012), A67, 7 pp.

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

[16] C. Nunn & G. Coxson, *Polyphase pulse compression codes with optimal peak and integrated sidelobes*, IEEE Trans. Aerospace and Electronic Systems **45** (2009), 775–781.

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

[18] K. Schmidt, *The peak sidelobe level of random binary sequences.* Preprint at `http://www-e.uni-magdeburg.de/kai-usch/research.html`