[16] A. M. Odlyzko, Extremal and statistical properties of trigonometric polynomials with ± 1 and $0, 1$ coefficients, manuscript in preparation.

[17] A. M. Odlyzko, Minimal absolute values of random trigonometric polynomials with ± 1 coefficients, manuscript in preparation.

[18] J. Ruprecht, Maximum-likelihood estimation of multipath channels, Ph.D. thesis, ETH, 1989. (Published by Hartung Gorre Verlag, Konstanz, Germany, 1989, ISBN 3-89191-270-6.)

[19] J. Ruprecht, F. D. Neeser, and M. Hufschmid, Code time division multiple access: an indoor cellular system, *Proc. IEEE Vehicular Techn. Conf. VTC '92*, May 1992, pp. 1–4.

[20] M. R. Schroeder, *Number Theory in Science and Communication*, Springer 1984.

[21] W. D. Wallis, A. P. Street, and J. S. Wallis, *Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices*, Lecture Notes in Math. #292, Springer, 1972.

[22] J.-P. de Weck and J. Ruprecht, Real-time ML estimation of very frequency selective multipath channels, pp. 908.5.1–908.5.6 in *Proc. Globecom 1990*, (San Diego), IEEE Press, 1990.

References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, 1976.

[2] G. Björck, Functions of modulus 1 on Z_n whose Fourier transforms have constant modulus, and "cyclic n-roots," pp. 131–140 in *Recent Advances in Fourier Analysis and its Applications*, J. S. Byrnes and J. F. Byrnes, eds., Kluwer, 1990.

[3] P. J. Davis, *Circulant Matrices*, Wiley, 1979.

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

[5] M. J. E. Golay, A class of finite binary sequences with alternate autocorrelation values equal to zero, *IEEE Trans. Information Theory IT-18* (1972), 449–450.

[6] J.-P. Kahane, *Some Random Series of Functions*, Heath, 1968.

[7] B. S. Kashin, Properties of random trigonometric polynomials with coefficients ± 1, *Moscow Univ. Math. Bull. 42*, no. 5, (1987), 45–51.

[8] M. N. Kolountzakis, On nonnegative cosine polynomials with nonnegative integral coefficients, *Proc. Amer. Math. Soc.*, to appear.

[9] J. E. Littlewood, On polynomials Σz^m, $\Sigma e^{\alpha m i} z^m$, $z = e^{i\theta}$ $\Sigma e^{\alpha m i} z^m$, $z = e^{i\theta}$, *J. London Math. Soc. 41* (1966), 367–376. *Reprinted in the Collected Papers of J. E. Littlewood*, vol. 2, pp. 1423–1433, Oxford Univ. Press, 1982.

[10] J. E. Littlewood, *Some Problems in Real and Complex Analysis*, Heath, 1968.

[11] H. D. Lüke, *Korrelationssignale*, Springer, 1992.

[12] J. L. Massey, Marcel E. Golay (1902–1989), *IEEE Inform. Theory Newsletter*, June 1990.

[13] O. C. McGehee, Gaussian sums and harmonic analysis on finite fields, pp. 171–191 in Contemporary Mathematics #91, Am. Math. Soc. 1989.

[14] H. L. Montgomery, An exponential polynomial formed with the Legendre symbol, *Acta Arith. 37* (1980), 375–380.

[15] A. M. Odlyzko, Minima of cosine sums and maxima of polynomials on the unit circle, *J. London Math. Soc. (2), 26* (1982), 412–420.

$1 + g(z)$ (with $g(z)$ given by (2.2)) produce improved values for the Golay merit factor, which measures how far $|f(z)|$ is away from $(n+1)^{1/2}$ on average as z runs over $|z| = 1$. (We note that cyclic shifts of coefficients of $f(z)$ do not affect the value of $R_p(f)$.) A nonexhaustive search of cyclic shifts of the sequences constructed in Section 2 with $n = 138$, $|S| \leq 2$, found a sequence with $R_a(f) = 110.2457$, which is better than the Ruprecht et al. sequence of [19], since the length is less. Thus modifications of our construction yield good values even for $R_a(f)$, although there is no proof that they will work for large lengths. It is also possible to try other modifications, which might yield even better results.

4. Final remarks

How large are the $R_p(f)$ produced by the above construction for moderate lengths n? For $n = 82$, the largest $R_p(f)$ that is known is 72.02 [16]. The construction of this section produces a sequence with $R_p(f) = 69.90$. Surprisingly, this result is achieved with $|S| = 1$. As was noted at the beginning of this section, if $|S| = 0$, then $R_p(f) \sim q/2$ as $q \to \infty$ (for $n = q-1$, q a prime). However, if we choose $|S| = 1$, $a = -b = 1$, then we obtain $R_p(f) \sim 9q/10$ as $q \to \infty$. Choices of S with $|S| \geq 2$ give better $R_p(f)$ only for $q \gtrsim 130$, and the improvement is slight initially. (We note also that while $R_p(f)$ is the same for all choices of S with $|S| = 1$, $a = -b$, the precise selection of S does make a slight difference for $|S| \geq 2$.) The resulting sequences for $p < 180$ are not as good (say, when judged by the value of the ratio $R_p(f)/(n+1)$) as the sequence obtained from the 13-term Barker sequence (see the discussion preceding Eq. (1.8)), but they are better than some other sequences that have been proposed. For example, Ruprecht, Neeser, and Hufschmid [19] list a sequence with $n = 143$ and $R_p(f) = 120.69862$. Our construction with $n = q - 1 = 138$ and $|S| = 2$ yields a value of $R_p(f) = 121.32578$, so that $R_p(f)$ is higher even though n is lower. (It should be mentioned, though, that the Ruprecht et al. sequence was chosen to have a high $R_a(f)$, not a high $R_p(f)$.)

The construction of Theorem 1 produces a sequence with high $R_p(f)$ because the polynomials associated to the Legendre sequences already have the desired behavior at the points $z = \exp(2\pi ik/q)$ for $1 \leq k \leq q-1$, and it is only at $z = 1$ that they need to be modified. Unfortunately the behavior of these polynomials at other points on the unit circle is not as well controlled. Montgomery [14] showed that

$$\max_{|z|=1} |f(z)| > 2\pi^{-1} q^{1/2} \log\log q \tag{4.1}$$

for all sufficiently large q, and he conjectured that this bound is of the right order of magnitude. If Montgomery's conjecture is right, these polynomials will be smaller than random ones, which reach $q^{1/2}(\log q)^{1/2}$ in size (cf. [16]). However, these polynomials do have small minimal absolute values. B. Conrey and A. Granville have observed (unpublished) that the polynomial $g(z)$ of Eq. (2.2) has $> p/2$ zeros with $|z| = 1$. Therefore it is not straightforward to modify those polynomials to obtain large $R_a(f)$. The highest value of $R_a(f)$ that our construction obtains for $n = 138$, $|S| \leq 2$ is 28.764, while the Ruprecht et al. sequence of [19] has $R_a(f) = 110.57658$. However, there are ways of modifying our construction to obtain higher values of $R_a(f)$. For example, it is known (see [16] for references) that cyclic shifts of the coefficients of *where the a_k are real constants, $|a_k| \le 1$ for all k, and the τ_k are independent random variables with*

$$Pr(\tau_k = -\gamma_k) = 1 - \gamma_k, \qquad Pr(\tau_k = 1 - \gamma_k) = \gamma_k \ , \tag{3.8}$$

for some constants γ_k, $0 \le \gamma_k \le 1$, then

$$Pr\left(|W| > C \left(\sum_{k=1}^{n} \gamma_k \right)^{1/2} (\log n)^{1/2} \right) < n^{-10} \ . \tag{3.9}$$

Proof. We have, for any $\lambda > 0$,

$$Pr(W > x) e^{\lambda x} \le \mathcal{E}(e^{\lambda W}) \ . \tag{3.10}$$

Now the τ_k are independent, so

$$\mathcal{E}(e^{\lambda W}) = \prod_{k=1}^{n} \mathcal{E}(e^{\lambda \tau_k a_k}) \ . \tag{3.11}$$

We next note that

$$\mathcal{E}(e^{\lambda \tau_k a_k}) = e^{-\lambda \gamma_k a_k}(1 - \gamma_k) + e^{\lambda(1-\gamma_k) a_k} \gamma_k \le e^{C' \lambda^2 \gamma_k} \tag{3.12}$$

if C' is sufficiently large. Therefore

$$Pr(W > x) \le \exp\left(C' \lambda^2 \sum_{k=1}^{n} \gamma_k - \lambda x \right) \ . \tag{3.13}$$

This bound holds for all $\lambda > 0$, so for $x > 0$ we select $\lambda = x(2C' \sum \gamma_k)^{-1}$ and obtain

$$Pr(W > x) \le \exp\left(-x^2 \left(4C' \sum_{k=1}^{n} \gamma_k \right)^{-1} \right) \ . \tag{3.14}$$

Since the same bound for $Pr(W < -x)$ follows by applying (3.14) to the problem with a_k replaced by $-a_k$, we easily obtain the claim of the lemma. ∎

To conclude the proof of Theorem 2, we apply Lemma 1 to the real and imaginary parts of

$$h(\zeta^j) - \mathcal{E}(h(\zeta^j)) \ , \qquad 0 \le j \le q - 1 \ .$$

We find that with probability $\ge 1 - n^{-8}$,

$$\left| h(\zeta^j) - \mathcal{E}(h(\zeta^j)) \right| < 10 C q^{1/4} (\log q)^{1/2} \tag{3.15}$$

holds for all j, $0 \le j \le q - 1$. Therefore

$$|f(\zeta^j)| = q^{1/2} + O(q^{1/4} (\log q)^{1/2}) \tag{3.16}$$

for all j, which yields Theorem 2.

There is a method of Kolountzakis [8] that often manages to remove factors such as the $(\log q)^{1/2}$ in the estimate (3.16). However, it does not seem to apply in this case.

3. Proof of Theorem 2

Theorem 2 follows from a modification of the proof of Theorem 1, using methods similar to those of [15]. As in the preceding section, we define $f(z)$ by (2.6) and (2.7) with $a = 1$. However, this time we will take S to be of size about $q^{1/2}$, and it will contain only nonresidues. The set S will be chosen at random, with each k, $1 \le k \le q-1$, $\left(\frac{k}{q}\right) = -1$, selected independently to be in S with probability

$$Pr(k \in S) = q^{-1/2}/2 \ . \tag{3.1}$$

Thus we have

$$h(z) = 1 - 2\sum_{k=1}^{q-1} \eta_k \left(\frac{k}{q}\right) z^k \ , \tag{3.2}$$

where $\eta_k = 0$ or 1 is a random variable with η_k identically 0 if $\left(\frac{k}{q}\right) = 1$, and $\mathcal{E}(\eta_k) = q^{-1/2}/2$ if $\left(\frac{k}{q}\right) = -1$.

We need to determine the behavior of $h(\zeta^j)$ for $0 \le j \le q-1$, where ζ is defined by (2.1). We first consider the expected value $\mathcal{E}(h(\zeta^j))$ for a fixed j. For $j = 0$ we have

$$\mathcal{E}(h(1) = 1 + 2 \sum_{\substack{h=1 \\ \left(\frac{k}{q}\right)=-1}}^{q-1} \mathcal{E}(\eta_k) = 1 + (q-1)q^{-1/2} = q^{1/2} + 1 - q^{-1/2} \ . \tag{3.3}$$

For $1 \le j \le q-1$, on the other hand,

$$\mathcal{E}(h(\zeta^j)) = 1 + q^{-1/2} \sum_{\substack{k=1 \\ \left(\frac{k}{q}\right)=-1}}^{q-1} \zeta^{kj} \ . \tag{3.4}$$

Since $\sum_{k=0}^{q-1} \zeta^{kj} = 0$ for $1 \le j \le q-1$, the sum in (3.4) is $-\left(\left(\frac{j}{q}\right) g(\zeta) + 1\right)/2$. Hence

$$\mathcal{E}(h(\zeta^j)) = 1 - q^{-1/2}/2 - \left(\frac{j}{q}\right) q^{-1/2} g(\zeta)/2 \ , \tag{3.5}$$

and so

$$\mathcal{E}(h(\zeta^j)) = O(1) \ . \tag{3.6}$$

We conclude that $\mathcal{E}(h(\zeta^j))$ has the desired behavior uniformly for all j, $0 \le j \le q-1$.

It remains to prove that for some choice of coefficients, $h(\zeta^j)$ will be close to $\mathcal{E}(h(\zeta^j))$ for all j. This will follow from the following result, which is similar to those in [6, 15].

Lemma 1. *There exists a constant $C > 0$ such that if*

$$W = \sum_{k=1}^{n} \tau_k a_k \ , \tag{3.7}$$

where $b = \pm 1$. The precise selection of a and S will be discussed later. We now observe that all coefficients of $f(z)$ are ± 1. Further, we have

$$f(1) = g(1) = a - 2b|S| \ . \tag{2.9}$$

For $1 \le j \le q-1$,

$$|f(\zeta^j)|^2 = |g(\zeta^j) + h(\zeta^j)|^2 = q + |h(\zeta^j)|^2 + 2 \ \mathrm{Re} \ \left(\overline{g(\zeta^j)} h(\zeta^j)\right) \ . \tag{2.10}$$

Since $|S| < q^{1/2}/100$, we find that for large q,

$$|h(\zeta^j)| < q^{1/2}/10 = |g(\zeta^j)|/10 \ . \tag{2.11}$$

Therefore we can write, for $1 \le j \le q-1$,

$$|f(\zeta^j)|^{-2} = q^{-1} \left(1 - 2q^{-1} \ \mathrm{Re} \ \left(\overline{g(\zeta^j)} h(\zeta^j)\right) + O(q^{-1}|h(\zeta^j)|^2)\right) \ . \tag{2.12}$$

This implies, by (2.3), that

$$|f(\zeta^j)|^{-2} = q^{-1} \left(1 - 2q^{-1} \left(\frac{j}{q}\right) \ \mathrm{Re} \ \left(\overline{g(\zeta)} h(\zeta^j)\right) + O(q^{-1}|h(\zeta^j)|^2)\right) \ , \tag{2.13}$$

and therefore

$$\sum_{j=1}^{q-1} |f(\zeta^j)|^{-2} = \frac{q-1}{q} - 2q^{-2} \ \mathrm{Re} \ \overline{g(\zeta)} \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) h(\zeta^j) + O\left(q^{-2} \sum_{j=1}^{q-1} |h(\zeta^j)|^2\right) \ . \tag{2.14}$$

Now

$$\sum_{j=1}^{q-1} |h(\zeta^j)|^2 \le \sum_{j=0}^{q-1} |h(\zeta^j)|^2 = 4q|S| \ . \tag{2.15}$$

On the other hand, by (2.8),

$$\begin{aligned} \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) h(\zeta^j) &= a \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) - 2b \sum_{k \in S} \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \zeta^{kj} \\ &= -2b \sum_{k \in S} \left(\frac{k}{q}\right) g(\zeta) = -2g(\zeta)|S| \ . \end{aligned} \tag{2.16}$$

If we now combine (2.9), (2.14), (2.15), and (2.16), we find that

$$\sum_{j=0}^{q-1} |f(\zeta^j)|^{-2} = (2b|S| - a)^{-2} + \frac{q-1}{q} + O(q^{-1}|S|) \ . \tag{2.17}$$

If we select $|S| \sim q^{1/3}$ as $q \to \infty$, say, then we obtain

$$\sum_{j=0}^{q-1} |f(\zeta^j)|^{-2} = 1 + O(q^{-2/3}) \ , \tag{2.18}$$

which yields the claim of Theorem 1.

$$g(z) = \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) z^k , \tag{2.2}$$

where $\left(\frac{k}{q}\right)$ is the Legendre symbol. (Thus $\left(\frac{k}{q}\right)$ is 0 for $k = 0$, 1 if k is a nonzero quadratic residue modulo q, and -1 if k is a nonresidue modulo q.) The $g(\zeta^j)$ are Gauss suns, and have an extensive literature. It is known (and easy to derive [1]) that

$$g(1) = 0, \quad g(\zeta^j) = \left(\frac{j}{q}\right) g(\zeta) \quad \text{for} \quad 1 \le j \le q-1 . \tag{2.3}$$

It is also easy to see (cf. [1]) that

$$g(\zeta)^2 = (-1)^{(q-1)/2} q . \tag{2.4}$$

It is further known that

$$g(\zeta) = \begin{cases} q^{1/2} , & q \equiv 1 \pmod 4 , \\ iq^{1/2} , & q \equiv 3 \pmod 4 , \end{cases} \tag{2.5}$$

but this is much harder to prove, and we will not use it. It is also known that $g(z)$ is large for some z with $|z| = 1$ [14].

We cannot use the sequence of coefficients of $g(z)$, because (i) $a_0 = 0$ and (ii) $g(1) = 0$. The main idea behind the construction below is to modify $g(z)$ slightly. We note that if we take $f(z) = 1 + g(z)$, then the coefficient sequence does consist of ± 1's, and $f(1) = 1$, $|f(\zeta^k)| \ge q^{1/2} - 1$ for $1 \le k \le q-1$. Therefore $R(f) \sim q/2$ as $q \to \infty$, and this already gives a merit factor far superior to that of almost all ± 1 sequences.

We set

$$f(z) = g(z) + h(z) , \tag{2.6}$$

where

$$h(z) = a - 2 \sum_{k \in S} \left(\frac{k}{q}\right) z^k , \tag{2.7}$$

$a = \pm 1$, and $S \subseteq \{1, \ldots, q-1\}$, $|S| < q^{1/2}/100$. It is easy to see, using the results on maximal values of random trigonometric polynomials, that random choices of S give $R(f) \sim n$ as $n \to \infty$. What we show, however, is that a nonrandom choice produces much better answers due to the special number theoretic properties of the Legendre sequence. We will select S to consist entirely of residues or else entirely of nonresidues, so that

$$\left(\frac{k}{q}\right) = b \quad \text{for all} \quad k \in S , \tag{2.8}$$

The construction of Theorem 1 produces sequences for which $n^{-1/2}|f(\exp(2\pi ik/(n+1))| = 1 + o(1)$ as $n \to \infty$ uniformly in k satisfying $1 \le k \le n$. For $k = 0$, though, $|f(1)|$ is of order $n^{1/3}$. However, we prove the following result.

Theorem 2. *If $n = q - 1$ for q a prime, then there exists a sequence $a_0, \ldots, a_n$ with $a_j = \pm 1$ for all j such that*

$$n^{-1/2}|f(\exp(2\pi ik/(n+1))| = 1 + O(n^{-1/4}(\log n)^{1/2}) \quad as \quad n \to \infty \tag{1.11}$$

uniformly in k, $0 \le k \le n$.

If we use only the bound (1.11) for the sequences of Theorem 2, we find that these sequences have $R_p(f) \ge n - c'n^{3/4}(\log n)^{1/2}$ for some constant $c' > 0$. With more care, one can show that these sequences have larger $R_p(f)$, but the bound for $n - R_p(f)$ that one can prove for these sequences appears to be considerably weaker than that given by Theorem 1 for its sequences.

We note that if

$$n^{-1/2}|f(e^{2\pi ik/(n+1)})| = 1, \quad 0 \le k \le n \ , \tag{1.12}$$

which is equivalent to $R_p(f) = n + 1$, then $a_0, \ldots, a_n$ is a Barker sequence and also the first row of a circulant Hadamard matrix, and so is thought not to exist for $n > 3$ [3, 21]. However, there is still no proof of this conjecture.

We leave several problems open. For example, can Theorems 1 and 2 be generalized so that n does not have to be of the form $n = q - 1$ for q a prime? Also, can one prove analogs of Theorems 1 and 2 for the aperiodic merit factor $R_a(f)$? Numerical evidence (cf. [16]) suggests that there do exist ± 1 sequences $a_0, \ldots, a_n$ for $n \ge 10$ such that the associated polynomials $f(z)$ have

$$\min_{|z|=1} n^{-1/2}|f(z)| \ge 1/2 \ . \tag{1.13}$$

A sequence satisfying (1.13) is guaranteed to have $R_a(f) \ge n/4$. However, since $R_a(f)$ is an average result, we might expect that some of these sequences might have $R_a(f) \sim n$ as $n \to \infty$. That is what seems to happen for the sequences listed in [16].

Acknowledgement. The author thanks Jürg Ruprecht for helpful correspondence.

2. Proof of Theorem 1

Let q be an odd prime, and define

$$\zeta \quad = \quad \exp(2\pi i/q) \ , \tag{2.1}$$

associated to a ±1 sequence of 169 terms, and

$$R_a(f(z^{13})f(z)) = 153.1014\ldots\ , \qquad R_p(f(z^{13})f(z)) = 154.6331\ \ldots \tag{1.8}$$

However, even this construction does not produce good asymptotic results.

The main result of this note is to show that high periodic Ruprecht merit factors can be achieved for a dense sequence of values of n.

Theorem 1. *There is a constant $c > 0$ such that if $n = q - 1$ for q a prime, then there exists a sequence $a_0, \ldots, a_n$ with $a_j = \pm1$ for all j such that*

$$n - cn^{1/3} \le R_p(f) \le n + 1\ . \tag{1.9}$$

The proof of Theorem 1, given in Section 2, shows how to construct these sequences. The sequences of Theorem 1 do have higher $R_a(f)$ than random sequences, but not very high ones. There is a discussion of this disappointing behavior in Section 4.

The search for ±1 sequences with large Ruprecht merit factors is just one part of the huge subject of extremal and statistical properties of ±1 sequences. For results, surveys, and applications, see [11, 16, 20]. In particular, there are connections to the search for sequences with large Golay merit factor [5, 12, 16].

For $R_p(f)$ to be large, $|f(\exp(2\pi ik/(n+1)))|$ has to be large for most k. Erdös [4] and Littlewood [9, 10] have raised the question of whether there exist ±1 sequences $a_0, \ldots, a_n$ such that the associated polynomials $f(z)$ satisfy

$$\min_{|z|=1}\ n^{-1/2}|f(z)| = 1 + o(1) \quad \text{as} \quad n \to \infty\ . \tag{1.10}$$

If such sequences existed, then we would have $R_a(f) \sim n$ and $R_p(f) \sim n$ as $n \to \infty$ for their polynomials. The current evidence is that such sequences don't exist (cf. [16]). However, to obtain large $R_p(f)$ we do not require (1.10) to hold. We even do not require $n^{-1/2}|f(\exp(2\pi ik/(n+1))| = 1 + o(1)$ as $n \to \infty$ to hold uniformly for all k, $0 \le k \le n$. Instead, we prove Theorem 1 by modifying the Legendre sequence $a_j = \left(\frac{j}{q}\right)$. It is easy to see that modifications of that sequence achieve $R_p(f) \sim n$ as $n = q - 1 \to \infty$, but the difference $R_p(f) - n$ usually turns out to be much larger than $n^{1/3}$ when one uses some of the obvious methods. By a careful analysis of what happens to $R_p(f)$ as the Legendre sequence is changed, we can obtain the bound of Theorem 1.

defined as

$$R_a(f) = \left(\int_0^1 |f(e^{2\pi i t})|^{-2} dt \right)^{-1} . \tag{1.5}$$

(For $R_a(f)$ to exist, we require that $f(z)$ be an invertible sequence.) Sequences with large $R_a(f)$ are more desirable than those with large $R_p(f)$, since they can be used for transmission [19], not just for multipath estimation. Unfortunately while we will provide constructions of sequences with large $R_p(f)$, the problem of obtaining large $R_a(f)$ remains open.

Since

$$\sum_{k=0}^{n} \left| f(e^{2\pi i k/(n+1)}) \right|^2 = (n+1)^2 \tag{1.6}$$

and

$$\int_0^1 |f(e^{2\pi i t})|^2 dt = n+1 \tag{1.7}$$

by a familiar calculation, the Cauchy-Schwarz inequality shows that $R_p(f) \leq n+1$, $R_a(f) \leq n+1$ for any sequence $a_0, \ldots, a_n$. How close can $R_a(f)$ and $R_p(f)$ come to $n+1$? Ruprecht [18] lists in Table B.6 the sequences $a_0, \ldots, a_n$ with the highest values of $R_p(f)$ for $n \leq 29$, as well as some sequences with high values of $R_p(f)$ for $30 \leq n \leq 32$. The maximal value of $R_p(f)$ for $n = 29$ is 26.6583, for example. Ruprecht also gives, in Table B.8, the best sequences drawn from a restricted class, that of the *skew-symmetric* a_j (i.e., those with even n and $a_{n/2-r} = (-1)^r a_{n/2+r}$) for $n \leq 44$. (The value for $n = 44$ is incorrect, though. See [16].) The maximal value of $R_p(f)$ for $n = 42$ is 37.4244. In Tables B.9 and B.10 of [18] Ruprecht lists sequences with large $R_a(f)$, for $n \leq 23$ in the general case and $n \leq 44$ for the skew-symmetric case. For example, for $n = 44$ he gives a skew-symmetric sequence with $R_a(f) = 39.7753$. Most of the values, especially for large n, are not known to be maximal. Skew-symmetric sequences with large $R_a(f)$ and $R_p(f)$ for $n \leq 90$ (obtained from a search for other types of extremal ± 1 sequences) are given in [16]. The nonexhaustive search for high $R_a(f)$ and $R_p(f)$ that is documented in that paper has produced a value of $R_p(f) = 77.5820$ for $n = 90$, for example.

What can one do for larger lengths n? Random choices of the a_j almost always give small values of $R(f)$ (cf. [16]). This is because random trigonometric polynomials have small minimal absolute values [7, 17], as was conjectured by Littlewood [9, 10]. Thus the situation is completely different than it is in coding theory, where random codes are good.

Sometimes one can construct a sequence with a large Ruprecht merit factor from shorter sequences. For example, if $n = 12$ and $(a_0, \ldots, a_n) = (1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, 1)$ is the 13-term Barker sequence, with associated polynomial $f(z)$, then $f(z^{13})f(z)$ is a polynomial

Construction of invertible sequences for multipath estimation

A. M. Odlyzko

AT&T Bell Laboratories
Murray Hill, New Jersey 07974
amo@research.att.com

1. Introduction

In the Ph.D. thesis [18], written under the supervision of Jim Massey, Jürg Ruprecht has proposed coding schemes designed for effective multipath estimation. Such schemes might be useful in indoor wireless systems [19, 21] or other communication settings. These schemes use *invertible sequences*, which are sequences $a_0, \ldots, a_n$, with $a_j = \pm 1$ for each j, such that the associated polynomial

$$f(z) = \sum_{j=0}^{n} a_j z^j \tag{1.1}$$

satisfies

$$f(e^{2\pi i t}) \neq 0 \quad \text{for all real} \quad t\ . \tag{1.2}$$

In some situations these schemes use *invertible periodic sequences*, for which the polynomial $f(z)$ only has to satisfy

$$f(e^{2\pi i k/(n+1)}) \neq 0, \qquad 0 \leq k \leq n\ . \tag{1.3}$$

(These invertible periodic sequences possess inverses under periodic convolution, which is required for Ruprecht's maximum likelihood estimation methods [18].) For best performance in estimating multipath interference, it is desirable to find invertible periodic sequences that maximize

$$R_p(f) = \frac{n+1}{\sum_{k=0}^{n} \left| f(e^{2\pi i k/(n+1)}) \right|^{-2}}\ . \tag{1.4}$$

In [18], this figure of merit is referred to as even processing gain $G_e^{(vs)}$ of a sequence s and its periodic inverse v, and is defined in a much more complicated form. However, a short calculation based on the formulas on p. 27 and in Appendix A of [18] shows that it equals our $R_p(f)$. We will call $R_p(f)$ the periodic Ruprecht merit factor, to distinguish it from other merit factors, such as that of Golay [5, 12, 16], as well as the aperiodic Ruprecht merit factor,

Construction of invertible sequences for multipath estimation

A. M. Odlyzko

AT&T Bell Laboratories
Murray Hill, New Jersey 07974
amo@research.att.com

Dedicated to Jim Massey on the occasion of his 60th birthday

ABSTRACT

J. Ruprecht has proposed coding schemes that allow for multipath estimation. They use sequences $a_0, \ldots, a_n$ with $a_j = \pm 1$ for each j such that the associated polynomial $f(z) = \sum a_j z^j$ has a large

$$R_p(f) = \frac{n+1}{\sum_{k=0}^{n} \left| f(e^{2\pi i k/(n+1)}) \right|^{-2}} .$$

Most sequences have a small $R_p(f)$, and those with maximal $R_p(f)$ are hard to find. This note shows for n of the form $n = q - 1$, q a prime, one can construct sequences with $R_p(f) \geq n - O(n^{1/3})$. Since $R_p(f) \leq n + 1$ for any sequence, this construction is asymptotically close to optimal. It also produces large values of $R_p(f)$ for small n.

It is also shown that for $n = q - 1$, q a prime, there exist sequences $a_0, \ldots, a_n$ such that the associated polynomial $f(z)$ satisfies

$$|f(e^{2\pi i k/(n+1)})| = (1 + o(1)) n^{1/2} \quad \text{as} \quad n \to \infty$$

uniformly for $0 \leq k \leq n$.