ACTA ARITHMETICA
146.3 (2011)

Orthogonality and the maximum of Littlewood cosine polynomials

by

Tamás Erdélyi (College Station, TX)

1. Introduction. Let $0 = \lambda_0 < \lambda_1 < \cdots < \lambda_m$. Our starting point is the following question. How large can the maximum of a trigonometric polynomial

$$S_m(t) = \sum_{j=0}^{m} A_j \cos(\lambda_j t), \qquad A_j \in \mathbb{R},$$

be on the real line? Since

$$\int_{-\pi}^{\pi} |S_m(t)|^2 \, dt = 2\pi \left(|A_0|^2 + \frac{1}{2} \sum_{j=1}^{m} |A_j|^2 \right),$$

the inequality

$$\max_{t \in [-\pi,\pi]} |S_m(t)| \ge \left(|A_0|^2 + \frac{1}{2} \sum_{j=1}^{m} |A_j|^2 \right)^{1/2}$$

obviously holds. But how large can

$$\max_{t \in [-\pi,\pi]} S_m(t) \tag{1.1}$$

be? To give a decent lower bound for (1.1) looks rather difficult.

The result below stated in [BE] is straightforward from [DeL, pp. 285–288], which offers an elegant book proof of the Littlewood Conjecture first shown in [Ko] and [McPS]. The book [Bo] deals with a number of related topics. Littlewood [L61, L64, L66, L68] was interested in many closely related problems.

2010 *Mathematics Subject Classification*: Primary 11C08, 11B75, 11P99; Secondary 05D99.

Key words and phrases: Littlewood polynomials, maximum modulus, maximum value, Chowla's Cosine Problem.

DOI: 10.4064/aa146-3-2

THEOREM 1.1. *Let $\lambda_0 < \lambda_1 < \cdots < \lambda_m$ be nonnegative integers and let*

$$S_m(t) = \sum_{j=0}^{m} A_j \cos(\lambda_j t), \qquad A_j \in \mathbb{R}.$$

Then

$$\int_{-\pi}^{\pi} |S_m(t)|\, dt \geq \frac{1}{60} \sum_{j=0}^{m} \frac{|A_{m-j}|}{j+1}.$$

The above theorem can be used to obtain a nontrivial lower bound for (1.1).

THEOREM 1.2. *Let $\lambda_1 < \lambda_2 < \cdots < \lambda_m$ be positive integers and let*

$$S_m(t) = \sum_{j=1}^{m} A_j \cos(\lambda_j t), \qquad A_j \in \mathbb{R}.$$

Then

$$\max_{t\in[-\pi,\pi]} S_m(t) \geq \frac{1}{240\pi} \sum_{j=0}^{m-1} \frac{|A_{m-j}|}{j+1}.$$

To see Theorem 1.2 observe that

$$\int_{-\pi}^{\pi} S_m(t)\, dt = 0,$$

and hence with $S_m^+(t) := \max\{S_m(t), 0\}$ and $S_m^-(t) := \min\{S_m(t), 0\}$, we have

$$\int_{-\pi}^{\pi} S_m^+(t)\, dt = \int_{-\pi}^{\pi} S_m^-(t)\, dt = \frac{1}{2} \int_{-\pi}^{\pi} |S_m(t)|\, dt,$$

which, together with Theorem 1.1, gives Theorem 1.2.

Let $\mathcal{L}_n$ be the collection of all algebraic polynomials of degree n with coefficients in $\{-1, 1\}$. Observe that if $P \in \mathcal{L}_n$ then the Parseval formula gives

$$\int_{-\pi}^{\pi} |P(e^{it})|^2\, dt = 2\pi(n+1).$$

Hence

$$\max_{t\in[-\pi,\pi]} |P(e^{it})| \geq \sqrt{n+1}$$

for every $P \in \mathcal{L}_n$. In 1957 Erdős [Er] made the following conjecture.

CONJECTURE 1.3. *There is an absolute constant $c > 0$ such that*

$$\max_{t\in[-\pi,\pi]} |P(e^{it})| \geq (1+c)\sqrt{n+1}$$

for every $P \in \mathcal{L}_n$.

This is still quite an open problem today. Even the following weaker version of the above conjecture has not been proved yet.

CONJECTURE 1.4. *There is an absolute constant $c > 0$ such that*

$$\max_{t\in[-\pi,\pi]} |P(e^{it})| \geq \sqrt{n+1} + c$$

for every $P \in \mathcal{L}_n$.

However, as a consequence of Theorem 1.2 we can observe at least the following result, the derivation of which may also be found in [B93].

THEOREM 1.5. *There is an absolute constant $c > 0$ such that*

$$\max_{t\in[-\pi,\pi]} |P(e^{it})| \geq \sqrt{n + c\log n}$$

for every $P \in \mathcal{L}_n$.

Proof. Let $P \in \mathcal{L}_n$. Observe that

$$Q(e^{it}) := |P(e^{it})|^2 = P(e^{it})P(e^{-it}) = n + 1 + S_n(t), \qquad t \in \mathbb{R},$$

with

$$S_n(t) := \sum_{j=1}^{n} A_j \cos(jt),$$

where each A_j is a sum of $n+1-j$ terms from $\{-2, 2\}$. Therefore if $n+1-j$ is odd then A_j is a nonzero (even) integer, that is, $|A_j| \geq 2$ and the theorem follows from Theorem 1.2. ∎

To improve Theorem 1.5 it would be fundamental to improve Theorem 1.2 at least in the case when the modulus of each or every second coefficient A_j is a nonzero integer, or a real number at least 1. This seems beyond reach at the moment. However, we can significantly improve Theorem 1.2 for the interesting classes of Littlewood cosine polynomials

$$T_q(t) = \sum_{j=0}^{q} a_j \cos(jt), \qquad a_j \in \{-1, 1\},$$

at least in the case when $p = 2q + 1$ is an odd prime. This is the content of our main result, Theorem 2.1. To this end we rely heavily on Ruzsa's paper [Ru], who claims the best result today to solve Chowla's Cosine Problem in [Ch] below.

PROBLEM 1.6. *Let $A \subset \mathbb{N}$ be a finite set of distinct integers and set*

$$m(A) := -\min_{t\in[-\pi,\pi]} \sum_{a\in A} \cos(at).$$

What is $m(n) := \min\{m(A) : A \subset \mathbb{N},\ |A| = n\}$?

In the Introduction of [Ru] Ruzsa writes: "Let A be a finite set of positive integers, $|A| = n$, and write

$$f(x) = \sum_{a \in A} \cos(ax).$$

Since $f(0) > 0$ and $\int_0^{2\pi} f(x)\,dx = 0$, we have $\min f(x) < 0$. It is a difficult question to estimate this minimum uniformly for every set of size n. Bourgain [B84] proved

$$\min f(x) < -c_1 \exp(c_2 (\log n)^{c_3})$$

with unspecified absolute constants $c_1 > 0$, $c_2 > 0$, and $c_3 > 0$. In another paper [B86] he showed that one can take $c_3 = 1/2$ under the assumption that $A \subset [1, n2^{\sqrt{\log n}}]$. Our aim is to prove this without restriction.

THEOREM 1. *With the above notations we have*

$$\min f(x) < -c_4 \exp(c_5 (\log n)^{1/2})$$

with a positive absolute constant c_4 and $c_5 = \sqrt{(\log 2)/8}$."

Note that $\min f(x)$ in the above quotation denotes the smallest value of $f(x)$ on the (period $[0, 2\pi)$ of the) real number line. Note also that the above quotation corrects two misprints in Ruzsa's paper by removing the minus sign from the exponent at two places.

2. New result. We denote by $\mathbb{Z}_p$ the additive group of p elements $\{0, 1, \dots, p-1\}$ under addition modulo p. Let $y_j := j/p$ for $j = 0, 1, \dots, p-1$,

$$E_p := \{y_0, y_1, \dots, y_{p-1}\} \quad \text{and} \quad E_p^* := E_p \cup \left\{ \frac{3}{2p} \right\}.$$

THEOREM 2.1. *If $p = 2q + 1$ is a prime, then the maximum of a Littlewood cosine polynomial*

$$T_q(2\pi t) = \sum_{j=0}^{q} a_j \cos(2\pi j t), \qquad a_j \in \{-1, 1\},$$

on E_p^* is at least $c_1 \exp(c_2 (\log q)^{1/2})$ with an absolute constant $c_1 > 0$ and $c_2 = \sqrt{(\log 2)/8}$.

We remark that the corrected form of Cramér's conjecture about the maximal size of the gap $g(p_k)$ between a prime p_k and the next prime p_{k+1} says that

$$g(p_k) := p_{k+1} - p_k \le K (\log p_k)^2 \quad \text{with} \quad K := 2\exp(-\gamma) = 1.1229\dots,$$

where γ is the Euler constant. The probabilistic model behind the corrected form of Cramér's conjecture is explained by A. Granville in [Gr]. See also

Soundararajan's survey [So]. Modulo the truth of Cramér's conjecture, and even modulo the much weaker conjecture

$$g(p_k) = o(\exp(c(\log p_k)^{1/2})) \quad \text{with} \quad c = \sqrt{(\log 2)/8}$$

a version of Theorem 2.1 remains obviously valid for all positive integers q. That is, modulo the above mentioned conjectures, if $q > 0$ is an integer, then the maximum of a Littlewood cosine polynomial

$$T_q(2\pi t) = \sum_{j=0}^{q} a_j \cos(2\pi j t), \qquad a_j \in \{-1, 1\},$$

on the real line $\mathbb{R}$ is at least $c_1 \exp(c_2(\log q)^{1/2})$ with an absolute constant $c_1 > 0$ and $c_2 = \sqrt{(\log 2)/8}$.

3. Lemmas. Let $e(x) := \exp(2\pi i x)$. To prove the theorem we need a few lemmas. Slightly weaker versions of these are essentially due to Bourgain and Ruzsa. Let $p = 2q + 1$ be a prime and let $\mathbb{Z}'_p := \{1, \dots, q\} \subset \mathbb{Z}_p$.

LEMMA 3.1. *Let $A' \subset \mathbb{Z}'_p$ and $A := -A' \cup A' \subset \mathbb{Z}_p$. Let*

$$f(x) = \sum_{a \in A} e(ax) = 2 \sum_{a \in A'} \cos(2\pi a x).$$

Let $|A| = n$,

$$K := \min_{x \in E_p} f(x),$$

and

$$k := \left\lfloor \frac{\log n}{4 \log K + c_6} \right\rfloor \tag{3.1}$$

with a suitable absolute constant $c_6 > 0$. Then there are distinct integers

$$\beta_1, \dots, \beta_k \in \mathbb{Z}_p$$

and a set $B \subset \mathbb{Z}_p$ such that

$$B + \Big\{ \sum_{j=1}^{k} \varepsilon_j \beta_j : \varepsilon_j \in \{0, 1\} \Big\} \subset A,$$

the 2^k sums in

$$\Big\{ \sum_{j=1}^{k} \varepsilon_j \beta_j : \varepsilon_j \in \{0, 1\} \Big\} \subset \mathbb{Z}_p$$

are all distinct, and $|B| \ge \sqrt{n}$.

LEMMA 3.2. *Let $A' \subset \mathbb{Z}_p'$ and $A := -A' \cup A' \subset \mathbb{Z}_p$. Suppose $\varepsilon \in (0,1)$ and $|A| < (1-\varepsilon)p$. Let*

$$f(x) = \sum_{a \in A} e(ax) = 2 \sum_{a \in A'} \cos(2\pi a x).$$

Suppose that there are sets $S, T \subset \mathbb{Z}_p$, an integer $0 \neq d \in \mathbb{Z}_p$, and a positive integer $L \geq 2/\varepsilon$ such that $|S|, |T| \geq L$ and $S + T + \{0, d\} \subset A$. Then

$$\min_{x \in E_p} f(x) \leq -\frac{1}{2} (\varepsilon L)^{1/2}.$$

LEMMA 3.3. *Let $A' \subset \mathbb{Z}_p'$ and $A := -A' \cup A' \subset \mathbb{Z}_p$. Suppose $|A| < \frac{7}{8}p$. Let*

$$f(x) = \sum_{a \in A} e(ax) = 2 \sum_{a \in A'} \cos(2\pi a x).$$

Then with $|A| = n$ we have

$$\min_{x \in E_p} f(x) \leq -c_4 \exp(c_5 (\log n)^{1/2})$$

with an absolute constant $c_4 > 0$ and $c_5 = \sqrt{(\log 2)/8}$.

To prove the above lemmas we modify the proofs of Lemmas 2.1 and 3.1 in [Ru] by integrating over the discrete measure

$$\mu_p := \frac{1}{p} \sum_{j=0}^{p-1} \delta_{x_j},$$

rather than over the usual Lebesgue measure, where δ_x is the measure with support $\{x\}$ and mass 1 at x. We will exploit the discrete orthogonality relations

$$\langle e(jx), e(kx) \rangle_p := \int e(jx) \overline{e(kx)} \, d\mu_p = \int e((j-k)x) \, d\mu_p = \delta_{j,k},$$

where

$$\delta_{j,k} := \begin{cases} 0, & j \neq k, \\ 1, & j = k, \end{cases} \qquad \text{for } j, k \in \{0, 1, \dots, p-1\}.$$

Proof of Lemma 3.1. Throughout the proof we use the notation

$$\|f\|_\alpha := \int |f(x)|^\alpha \, d\mu_p, \qquad \|f\|_\infty := \max_{x \in E_p} |f(x)|,$$

for numbers $\alpha > 0$ and functions f defined on E_p. Also, we define

$$(f * g)(x) := \int f(t) g(x-t) \, d\mu_p$$

for functions f and g defined on E_p. We find inductively

$$\beta_1, \dots, \beta_k \in \mathbb{Z}_p \quad \text{and} \quad B_0, B_1, \dots, B_k \subset \mathbb{Z}_p$$

with the following properties for every $j = 0, 1, \dots, k$. First, the 2^j numbers

$$\sum_{\nu=1}^{j} \varepsilon_\nu \beta_\nu, \qquad \varepsilon_\nu \in \{0, 1\},$$

are all distinct in $\mathbb{Z}_p$. Next, we always have

$$\sum_{\nu=1}^{j} \varepsilon_\nu \beta_\nu + B_j \subset A \tag{3.2}$$

and

$$|B_j| \geq M_j = (4K^2)^{-j} n. \tag{3.3}$$

The last property asserts that the function

$$g_j(x) = \sum_{b \in B_j} e(bx)$$

has a decomposition

$$g_j = h_1^{(j)} + h_2^{(j)} + h_3^{(j)} \tag{3.4}$$

such that

$$|h_1^{(j)}(x)| \leq f(x) + K, \qquad x \in E_p, \tag{3.5}$$

$$|h_2^{(j)}(x)| \leq L_j := 4^j K^{j+1}, \qquad x \in E_p, \tag{3.6}$$

$$\|h_3^{(j)}\|_1 \leq \eta_j := (8K^2)^j n^{-1/2}. \tag{3.7}$$

An important consequence of (3.5) is

$$\|h_1^{(j)}\|_1 \leq \|f + K\|_1 = K. \tag{3.8}$$

We start with $B_0 := A$. The above decomposition of $g_0 = f$ will be

$$h_1^{(0)}(x) := f(x)^+ := \max(0, f(x)), \quad h_2^{(0)}(x) := -f(x)^- := -\min(0, f(x)),$$
$$L_0 := K, \quad h_3^{(0)} := 0.$$

Assume now that the set $B_j \subset \mathbb{Z}_p$, the integers $\beta_1, \dots, \beta_j \in \mathbb{Z}_p$ and the functions $h_\nu^{(j)}$, $\nu = 1, 2, 3$, are given. We are going to find $B_{j+1} \subset \mathbb{Z}_p$ and the functions $h_\nu^{(j+1)}$. To simplify notation we shall write B, M, g, h_ν, L, η for B_j, M_j, g_j, $h_\nu^{(j)}$, L_j, η_j, and B', M', g', h'_ν, L', η' for B_{j+1}, M_{j+1}, g_{j+1}, $h_\nu^{(j+1)}$, L_{j+1}, η_{j+1}. Write $|B| = m$ $(\geq M)$.

We will search for B' in the form $B' = B \cap (B - \alpha)$, and then put $\beta_{j+1} := \alpha$. This guarantees (3.2).

To estimate the size of such an intersection, first observe that

$$\sum_{\alpha \in \mathbb{Z}_p} |B \cap (B - \alpha)| = m^2 \tag{3.9}$$

and

$$\sum_{\alpha\in\mathbb{Z}_p} |B\cap(B-\alpha)|^2 = \|g\|_4^4. \tag{3.10}$$

To estimate this quantity we start with

$$\|g-h_2\|_2 \ge \|g\|_2 - \|h_2\|_2 \ge \|g\|_2 - \|h_2\|_\infty \ge \sqrt{m} - L$$

and

$$\|g-h_2\|_1 = \|h_1+h_3\|_1 \le \|h_1\|_1 + \|h_3\|_1 \le K+\eta$$

by (3.8) and (3.7). By Hölder's inequality we have

$$\|g-h_2\|_4 \ge \frac{\|g-h_2\|_2^{3/2}}{\|g-h_2\|_1^{1/2}} \ge \frac{(\sqrt{m}-L)^{3/2}}{(K+\eta)^{1/2}} \ge \frac{8}{9}\, m^{3/4}K^{-1/2},$$

if we suppose

$$\eta < cK, \quad L < c\sqrt{M} \le c\sqrt{m} \tag{3.11}$$

with a suitably small absolute constant $c>0$. This implies

$$\|g\|_4 \ge \|g-h_2\|_4 - \|h_2\|_4 \ge \frac{8}{9}\, m^{3/4}K^{-1/2} - L \ge \frac{7}{8}\, m^{3/4}K^{-1/2}$$

if $L\sqrt{K} < cm^{3/4}$ with a suitably small absolute constant $c>0$. This assumption follows from the second inequality of (3.11), since $L\ge K$ by (3.6). Hence by (3.10) we obtain

$$\sum_{\alpha\in\mathbb{Z}_p} |B\cap(B-\alpha)| \ge \frac{1}{2}\,\frac{m^3}{K^2}. \tag{3.12}$$

The contribution of terms satisfying $|B\cap(B-\alpha)| \le \frac{1}{4}m/K^2$ to the sum in (3.12) is at most $\frac{1}{4}m^3/K^2$ by (3.9), so at least $\frac{1}{4}m^3/K^2$ comes from α such that $|B\cap(B-\alpha)| > \frac{1}{4}m/K^2$. As each summand is at most m^2, we infer that there are at least $\frac{1}{4}m/K^2$ values of α such that $|B\cap(B-\alpha)| > \frac{1}{4}m/K^2$.

We shall select our $\beta_j = \alpha$ from these values. This guarantees the inductive step for (3.3). To arrange that the sums $\sum_{\nu=1}^{j+1}\varepsilon_\nu\beta_\nu$ are distinct we need to avoid the at most 3^j numbers of the form

$$\sum_{\nu=1}^{j}\delta_\nu\beta_\nu, \qquad \delta_\nu\in\{-1,0,1\}.$$

If we suppose that

$$3^j \le \frac{m}{8K^2}, \tag{3.13}$$

then we still have at least $m/(8K^2)$ values of β to choose from. We have to find the decomposition of g' and show properties (3.5)–(3.7). Write $e_\alpha(x) =$

$e(\alpha x)$. With this notation we can write g' as a convolution

$$g' := g * (ge_\alpha).$$

If we substitute the decomposition of g into this formula we get an expression for g' as a sum of nine convolutions, which will be dealt with in different ways.

First observe that

$$|h_1 * (h_1 e_\alpha)| \le |h_1| * |h_1| \le (f + K) * (f + K) = f + K^2$$

for every input $x \in E_p$. In the last step we use the fact that $f * f = f$, which is equivalent to the property that each coefficient of f is 0 or 1.

Clearly, we can decompose $h_1 * (h_1 e_\alpha)$ as

$$h_1 * (h_1 e_\alpha) = h_1' + h_{2,1}',$$

where $|h_1'| \le f + K$ and $|h_{2,1}'| \le K^2 - K$ for every input $x \in E_p$. The function $h_{2,1}'$ will contribute to h_2'. Other contributions to h_2' come from the convolutions involving h_2 and h_1 or h_3. We have

$$\|(h_1 + h_3) * (h_2 e_\alpha)\|_\infty \le \|h_1 + h_3\|_1 \|h_2\|_\infty \le (K + \eta)L,$$

and the same estimate holds for $\|((h_1 + h_3)e_\alpha) * h_2\|_\infty$. So finally

$$h_2' := h_{2,1}' + (h_1 + h_3) * (h_2 e_\alpha) + ((h_1 + h_3)e_\alpha) * h_2$$

satisfies

$$\|h_2'\|_\infty \le (K^2 - K) + 2(K + \eta)L \le 4KL$$

(recall also (3.11)). This is exactly (3.6) for $j + 1$. The other terms make up h_3'. We have

$$\|h_1 * (h_3 e_\alpha)\|_1 \le \|h_1\|_1 \|h_3\|_1 \le \eta K,$$

and the same estimate holds for $\|h_3 * (h_1 e_\alpha)\|_1$. Similarly

$$\|h_3 * (h_3 e_\alpha)\|_1 \le \|h_3\|_1^2 \le \eta^2 < \eta K.$$

To estimate $\|h_2 * (h_2 e_\alpha)\|_1$ we shall use averaging in α. An application of Parseval's formula yields

$$\sum_{\alpha \in \mathbb{Z}_p} \|h_2 * (h_2 e_\alpha)\|_2^2 = \|h_2\|_2^4 \le \|h_2\|_\infty^4 \le L^4.$$

Since we have at least $m/(8K^2)$ values of α to choose from, there is one such that

$$\|h_2 * (h_2 e_\alpha)\|_1 \le \|h_2 * (h_2 e_\alpha)\|_2 < 3KL^2 m^{-1/2}.$$

So

$$h_3' := h_1 * (h_3 e_\alpha) + h_3 * (h_1 e_\alpha) + h_3 * (h_3 e_\alpha) + h_2 * (h_2 e_\alpha)$$

satisfies

$$\|h_3'\|_1 < 3\eta K + 3KLm^{-1/2}.$$

By substituting the definition of η and L from (3.4), (3.6) and (3.7) and using the estimate (3.3) for m ($\geq M$), a simple calculation shows (3.7) for $j+1$. This α will be our β_{j+1}, and this ends the induction.

This process goes on as long as conditions (3.11) and (3.13) are satisfied. Both inequalities of (3.11) lead to a bound for k as given by (3.1) in the lemma, while (3.13) gives about twice that. The lower bound for $|B|$ is the case $j=k$ of (3.3). ∎

Proof of Lemma 3.2. By removing some elements from S if necessary, without loss of generality we may assume that $|S|=L$. First we establish the existence of sets of integers $U, V \subset \mathbb{Z}_p$ such that $|U|, |V| \geq \varepsilon L$, $U-V \subset A$, $U \subset A$, $V \cap A = \emptyset$ and $0 \notin V$.

Assume $0 \in T$ (this can be achieved by shifting S and T if necessary), and write

$$r_j = |(S+jd) \cap A|.$$

We have $r_0 \geq L$ and there is a $j \in \mathbb{Z}_p$ such that

$$r_j \geq (1-\varepsilon)L > r_{j+1},$$

otherwise $p(1-\varepsilon)L \leq |A|L$, contradicting our assumption $|A| < p(1-\varepsilon)$. Write $A_0 = A \cup \{0\}$. Now if

$$|(jd-T) \cap A| < (1-\varepsilon)L, \tag{3.14}$$

then put

$$U = (S+jd) \cap A, \quad V = (jd-T) \setminus A_0.$$

We have

$$|U| = r_j \geq (1-\varepsilon)L,$$

$$|V| = |T| - |(jd-T) \cap A_0| > L - (1-\varepsilon)L - 1 \geq \varepsilon L - 1 \geq \frac{1}{2}\varepsilon L,$$

and

$$U - V \subset (S+jd) - (jd-T) = S+T \subset A.$$

If (3.14) does not hold, then we put

$$U = (jd-T) \cap A, \quad V = (S+(j+1)d) \setminus A_0.$$

We have $|U| \geq (1-\varepsilon)L$ by the negation of (3.14),

$$|V| = |S| - |(S+(j+1)d) \cap A_0| \geq |S| - r_{j+1} - 1 > L - (1-\varepsilon)L - 1$$
$$= \varepsilon L - 1 \geq \frac{1}{2}\varepsilon L,$$

and

$$U - V \subset (jd-T) - (S+(j+1)d) = (S+T+d) \subset -A = A.$$

We define K by

$$-K := \min_{x \in E_p} f(x),$$

and another function h by

$$h(x) = \frac{1}{|U|} \sum_{u \in U} e(ux) - \frac{1}{|V|} \sum_{v \in V} e(vx).$$

Recall that $0 \notin V$ and also $0 \notin U$ by $U \subset A$, hence $\int h(x)\, d\mu_p = 0$. We have

$$\int h(x) f(x)\, d\mu_p = 1$$

by $U \subset A$, $V \cap A = \emptyset$, thus

$$\int h(x)(f(x) + K)\, d\mu_p = 1. \tag{3.15}$$

Furthermore

$$|h(x)|^2 = |U|^{-2} \sum_{u,u' \in U} e((u-u')x) + |V|^{-2} \sum_{v,v' \in V} e((v-v')x) - (|U|\,|V|)^{-1} \sum_{u \in U, v \in V} (e((u-v)x) + e((v-u)x)).$$

Since $u - v, v - u \in A$ for all $u \in U$ and $v \in V$, we see that

$$\int |h(x)|^2 f(x)\, d\mu_p \le 1 + 1 - 2 = 0.$$

Also, clearly

$$\int |h(x)|^2\, d\mu_p \le |U|^{-1} + |V|^{-1} \le \frac{4}{\varepsilon L},$$

which implies

$$\int |h(x)|^2 (f(x) + K)\, d\mu_p \le \frac{4K}{\varepsilon L}.$$

By Cauchy's inequality and (3.15) we have

$$\begin{aligned} 1 &= \int h(x)(f(x) + K)\, d\mu_p \\ &\le \Big(\int |h(x)|^2 (f(x) + K)\, d\mu_p \Big)^{1/2} \Big(\int (f(x) + K)\, d\mu_p \Big)^{1/2} \\ &\le \left(\frac{4K}{\varepsilon L} \right)^{1/2} K^{1/2}, \end{aligned}$$

that is, $K \ge \frac{1}{2}(\varepsilon L)^{1/2}$ as claimed. ∎

Proof of Lemma 3.3. Let

$$-K := \min_{x \in E_p} f(x).$$

By Lemma 3.1, with k defined in the lemma, there are integers $\beta_1, \dots, \beta_k \in \mathbb{Z}_p$ and a set $B \subset \mathbb{Z}_p$ such that

$$B + \Big\{ \sum_{j=1}^{k} \varepsilon_j \beta_j : \varepsilon_j \in \{0,1\} \Big\} \subset A,$$

the 2^k sums in

$$\Big\{ \sum_{j=1}^{k} \varepsilon_j \beta_j : \varepsilon_j \in \{0,1\} \Big\} \subset \mathbb{Z}_p$$

are all distinct, and $|B| \ge \sqrt{n}$. Choose $S := B$,

$$T := \Big\{ \sum_{j=1}^{k-1} \varepsilon_j \beta_j \Big\},$$

and $d := \beta_k$. We have $S + T + \{0, d\} \subset A$ and $|S| > |T| = 2^{k-1}$, so an application of Lemma 3.2 yields

$$K \ge 2^{(k-6)/2} \ge \exp\left(\frac{\log 2}{2} \, \frac{\log n}{4 \log K + c_6} - 4 \right).$$

After taking the logarithm and rearranging this yields a quadratic inequality for $\log K$, and by a simple calculation we find the bound of the lemma. ∎

4. Proof of Theorem 2.1. Every Littlewood cosine polynomial

$$T_q(2\pi t) = \sum_{j=0}^{q} a_j \cos(2\pi j t), \qquad a_j \in \{-1, 1\},$$

can be written as

$$T_q(2\pi t) = \frac{1}{2} + D_q(2\pi t) - U_q(2\pi t),$$

where

$$D_q(2\pi t) := \frac{1}{2} + \sum_{j=1}^{q} \cos(2\pi j t)$$

is the qth Dirichlet kernel, and $U_q(2\pi t)$ is of the form

$$U_q(2\pi t) = 2 \sum_{a \in A'} \cos(2\pi a t) = \sum_{a \in A} e(at),$$

where $A' \subset \mathbb{Z}'_p$ and $A := -A' \cap A' \subset \mathbb{Z}_p$. A key observation is that $D_q(2\pi t)$ vanishes on $E_p \setminus \{0\}$. So if $\frac{1}{8}p \le |A| \le \frac{7}{8}p$, then Lemma 3.3 gives the result of the theorem (note that $U_q(0) = |A| > 0$). If $|A| < \frac{1}{8}p$, then

$$T_q(0) = \frac{1}{2} + D_q(0) - U_q(0) = q + 1 - 2|A| > q + 1 - \frac{p}{4} > \frac{p}{4}.$$

If $|A| > \frac{7}{8}p$, then $T_q(2\pi t)$ can be written as

$$T_q(2\pi t) = -\frac{1}{2} - D_q(2\pi t) + V_q(2\pi t),$$

where $D_q(2\pi t)$ is the Dirichlet kernel as before, and

$$V_q(2\pi t) = 2\sum_{a\in B'} \cos(2\pi a t) = \sum_{a\in B} e(at),$$

with

$$B' := \mathbb{Z}_q \setminus A' \subset \mathbb{Z}_q, \qquad B := -B' \cup B' \subset \mathbb{Z}_p,$$

and $|B| < \frac{1}{8}p$. Observe that at $t := \frac{3}{2p} \in E_p^*$ we have

$$-D_q(2\pi t) \geq \frac{p}{6} \quad \text{and} \quad |V_q(2\pi t)| \leq \frac{p}{8},$$

hence

$$\begin{aligned} T_q(2\pi t) &= -1/2 - D_q(2\pi t) + V_q(2\pi t) \\ &\geq -\frac{1}{2} + \frac{p}{6} - \frac{p}{8} \geq \frac{p}{24} - \frac{1}{2}. \end{aligned}$$

So, in fact, if $|A| < \frac{1}{8}p$ or $|A| > \frac{7}{8}p$, then we have a much better lower bound for the maximum of T_q on E_p^* than the one stated in the theorem.

5. Maximum modulus of Barker polynomials. Let, as before, $\mathcal{L}_n$ be the collection of all polynomials of degree n with each coefficient in $\{-1, 1\}$. Let D and ∂D denote the closed unit disk and the unit circle of the complex plane, respectively. For a polynomial

$$p(z) := \sum_{k=0}^{n} a_k z^k$$

the kth *acyclic autocorrelation coefficient* is defined by

$$c_k = \sum_{j=0}^{n-k} a_j a_{j+k} \quad \text{and} \quad c_{-k} = c_k.$$

A *Barker polynomial* $p \in \mathcal{L}_n$ has autocorrelation coefficients c_k satisfying $|c_k| \leq 1$, $k = 1, \ldots, n$, which by parity gives $c_k = 0$ if $n - k$ is odd, and $|c_k| = 1$ if $n - k$ is even. Since

$$p(z)p(1/z) = n + 1 + \sum_{\substack{k=-n \\ k\neq 0}}^{n} c_k z^k,$$

if $p \in \mathcal{L}_n$ is a Barker polynomial of even degree n, then

$$\|p\|_{L_4(\partial D)} = ((n+1)^2 + n)^{1/4},$$

while if $p \in \mathcal{L}_n$ is a Barker polynomial of odd degree n, then

$$\|p\|_{L_4(\partial D)} = ((n+1)^2 + n + 1)^{1/4}.$$

It is widely believed that no Barker polynomials exist of degree greater than 12 but this seems a very difficult problem.

The following conjecture implies that the acyclic autocorrelation coefficient cannot even remain bounded for large n.

Merit Factor Problem of Golay. Find the polynomial in $\mathcal{L}_n$ that has the smallest possible $L_4(\partial D)$ norm on the unit circle. Show that there exists a constant $c > 0$ so that for all n and $p \in \mathcal{L}_n$ we have

$$\|p\|_{L_4(\partial D)} \geq (1+c)\sqrt{n+1}.$$

Even the following much weaker problem is open.

The Barker Polynomial Problem. Show that

$$\|p\|_{L_4(\partial D)} > ((n+1)^2 + n + 1)^{1/4}$$

for all $p \in \mathcal{L}_n$ with $n > 12$.

Note that this would imply the nonexistence of Barker polynomials for $n > 12$. Also

$$\|p\|_{L_4(\partial D)} > \sqrt{n+1} + 1$$

implies

$$\|p\|_{L_4(\partial D)} > ((n+1)^2 + n + 1)^{1/4}.$$

In [Bo] P. Borwein writes "It is conjectured that no Barker polynomials exist for $n > 12$. See [FSS] and [S90] for more about Barker polynomials and the proof of the nonexistence of self-reciprocal Barker polynomials. In [TS] and [T63] Turyn and Storer showed that no even degree Barker polynomials exist for $n > 12$ (and indeed, as Schmidt [Sc] shows, none exist for any degree between 12 and 10^{20}). It can also be shown (see Turyn [T65]) that any odd degree Barker polynomial of degree greater than 12 must have degree of the form $4s^2 - 1$, where s is an odd composite number."

In [BM] the authors amend an argument of Saffari showing that Barker polynomials are flat. More precisely, if p_n is a Barker polynomial of degree n, then

$$\alpha_1 + O(1/n) = \frac{|p_n(z)|}{\sqrt{n}} \leq \alpha_2 + O(1/n)$$

for each $z \in \partial D$, where $\alpha_1 = \sqrt{1-\theta} = 0.52477485\ldots$ and $\alpha_2 = \sqrt{1+\theta} = 1.31324459\ldots$, and

$$\theta := \sup_{t>0} \frac{\sin 2t}{t} = 0.7246113537\ldots.$$

In a recent work, M. Mossinghoff [Mo] showed that if a Barker sequence of length $n > 13$ exists, then either $n = 189260468001034441522766781604$ or $n > 2 \cdot 10^{30}$.

In this section we record the following observation about the maximum modulus $\|p\|_D$ of a Barker polynomial $p \in \mathcal{L}_n$ on the closed unit disk D.

THEOREM 5.1. *Let $p \in \mathcal{L}_n$ be a Barker polynomial. Then*

$$\max_{z\in\partial D} |p(z)| \geq \sqrt{n} + \sqrt{1/3} \quad \textit{and} \quad \min_{z\in\partial D} |p(z)| \leq \sqrt{n+2} - \sqrt{1/3}.$$

We doubt that the constant $\sqrt{1/3}$ can be pushed above 1 easily.

To prove Theorem 5.1 we need the following result of Turyn and Storer ([TS], [T63]).

LEMMA 5.2. *Suppose*

$$p(z) := \sum_{k=0}^{n} a_k z^k$$

is a Barker polynomial of degree n. Let

$$p(z)p(1/z) = n + 1 + \sum_{\substack{k=-n \\ k\neq 0}}^{n} c_k z^k.$$

Then

$$c_k + c_{n+1-k} \equiv n + 1 \pmod 4$$

and

$$a_k a_{n-k} = (-1)^{n-k}.$$

If $n+1$ is even and $n > 3$, then $n+1 = 4m^2$ for some positive integer m, and $c_{n+1-k} = -c_k$ for $0 < k < n+1$. If $n+1$ is odd, then $c_k + c_{n+1-k} = (-1)^{n/2}$ for each $0 < k < n+1$.

We also need Szegő's inequality (which is sometimes called the inequality of van der Corput and Schaake) below. For a proof see [DeL, p. 97].

LEMMA 5.3. *We have*

$$Q'(t)^2 + n^2 Q(t)^2 \leq n^2 \max_{\tau\in[-\pi,\pi]} |Q(\tau)|^2$$

for every trigonometric polynomial of degree at most n. As a consequence,

$$n^{-2}\|Q'\|^2_{L_2[-\pi,\pi]} + \|Q\|^2_{L_2[-\pi,\pi]} \leq \max_{\tau\in[-\pi,\pi]} |Q(\tau)|^2.$$

Proof of Theorem 5.1. Let $p \in \mathcal{L}_n$ be a Barker polynomial and write $n + 1 = 4m$. Using the fact that the off-peak autocorrelations satisfy $c_{n+1-k} = -c_k$, and that $c_{2j} = 0$ for $j \geq 1$, we deduce by Lemma 5.2 that

$$\begin{aligned} Q(t) := |p(e^{it})|^2 - (n+1) &= 2\sum_{k=1}^{n} c_k \cos(kt) \\ &= 2\sum_{k=1}^{2m-1} c_k(\cos(kt) - \cos((n-k)t)) \end{aligned}$$

$$= 4\sin(2mt)\sum_{k=1}^{2m-1} c_k \sin((2m-k)t)$$
$$= 4\sin(2mt)\sum_{k=1}^{m} c_{2m-2k+1}\sin((2k-1)t).$$

The key observation is that while Lemma 5.3 implies that

$$n^{-2}\|Q'\|^2_{L_2[-\pi,\pi]} + \|Q\|^2_{L_2[-\pi,\pi]} = \pi n^{-2}\Big(\sum_{1\le 2j+1\le n} 4(2j+1)^2\Big) + \pi\Big(\sum_{1\le 2j+1\le n} 4\Big) \ge \frac{8\pi}{3}n \tag{5.1}$$

we also have

$$Q(t) = -Q(t+\pi), \quad t\in\mathbb{R}. \tag{5.2}$$

Now (5.1) and (5.2) ensure that there is a $\tau\in[-\pi,\pi]$ for which $Q(\tau)\ge(4n/3)^{1/2}$ and $Q(\tau+\pi)\le -(4n/3)^{1/2}$, and the theorem follows. ∎

We remark that the simple property (5.2) of Q allows us to conclude a much better result than the one implied by an application of our main result, Theorem 2.1. In addition, Theorem 2.1 could be used only under some restrictions, for example, in the cases when n or $n+2$ is a prime.

Acknowledgements. I profited much from e-mail discussions with Imre Ruzsa related to the paper. I also thank Bahman Saffari for pointing out the corrected form of Cramér's conjecture related to the main result, Theorem 2.1 of this paper, and suggesting to use Szegő's inequality rather than the Parseval formula to improve the constant in Theorem 5.1.

References

[Bo] P. Borwein, *Computational Excursions in Analysis and Number Theory*, Springer, New York, 2002.

[BE] P. Borwein and T. Erdélyi, *Lower bounds for the number of zeros of cosine polynomials in the period: a problem of Littlewood*, Acta Arith. 128 (2007), 377–384.

[BM] P. Borwein and M. J. Mossinghoff, *Barker sequences and flat polynomials*, in: Number Theory and Polynomials, J. McKee and C. Smyth (eds.), London Math. Soc. Lecture Note Ser. 352, Cambridge Univ. Press, Cambridge, 2008, 71–88.

[B84] J. Bourgain, *Sur le minimum de certaines sommes de cosinus*, in: Harmonic Analysis: Study Group on Translation-Invariant Banach Spaces, Publ. Math. Orsay 84-1, exp. 2, Univ. Paris XI, Orsay, 1984, 7 pp.

[B86] —, *Sur le minimum d'une somme de cosinus*, Acta Arith. 45 (1986), 381–389.

[B93] —, *On the spectral type of Ornstein's class one transformations*, Israel J. Math. 84 (1993), 53–63.

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

[DeL] R. A. DeVore and G. G. Lorentz, *Constructive Approximation*, Springer, Berlin, 1993.

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

[FSS] M. L. Fredman, B. Saffari et B. Smith, *Polynômes réciproques: conjecture d'Erdős en norme L^4, taille des autocorrélations et inexistence des codes de Barker*, C. R. Acad. Sci. Paris Sér. I Math. 308 (1989), 461–464.

[Gr] A. Granville, *Harald Cramér and the distribution of prime numbers*, Harald Cramér Symposium (Stockholm, 1993), Scand. Actuarial J. 1995, 12–28.

[Ko] S. V. Konyagin, *On a problem of Littlewood*, Math. USSR-Izv. 18 (1981), 205–225.

[L61] J. E. Littlewood, *On the mean values of certain trigonometrical polynomials*, J. London Math. Soc. 36 (1961), 307–334.

[L64] —, *On the real roots of real trigonometrical polynomials (II)*, ibid. 39 (1964), 511–552.

[L66] —, *On polynomials $\sum_0^n \pm z^m$ and $\sum_0^n e^{\alpha_m i} z^m$, $z = e^{\theta i}$*, ibid. 41 (1966), 367–376.

[L68] —, *Some Problems in Real and Complex Analysis*, Heath Math. Monogr., Heath, Lexington, MA, 1968.

[McPS] O. C. McGehee, L. Pigno and B. Smith, *Hardy's inequality and the L_1 norm of exponential sums*, Ann. of Math. 113 (1981), 613–618.

[Mo] M. J. Mossinghoff, *Wieferich pairs and Barker sequences*, Des. Codes Cryptogr. 53 (2009), 149–163.

[Ru] I. Z. Ruzsa, *Negative values of cosine sums*, Acta Arith. 111 (2004), 179–186.

[S90] B. Saffari, *Barker sequences and Littlewood's "two-sided conjectures" on polynomials with ± 1 coefficients*, in: Séminaire d'Analyse Harmonique, Année 1989/90, Univ. Paris XI, Orsay, 1990, 139–151.

[Sc] B. Schmidt, *Cyclotomic integers and finite geometry*, J. Amer. Math. Soc. 12 (1999), 929–952.

[So] K. Soundararajan, *The distribution of prime numbers*, in: Equidistribution in Number Theory, An Introduction, A. Granville and Z. Rudnick (eds.), NATO Sci. Ser. II Math. Phys. Chem. 237, Springer, Dordrecht, 2007, 59–83.

[T63] R. Turyn, *On Barker codes of even length*, Proc. IEEE 51 (1963), no. 9, 1256.

[T65] —, *Character sums and difference sets*, Pacific J. Math. 15 (1965), 319–346.

[TS] R. Turyn and J. Storer, *On binary sequences*, Proc. Amer. Math. Soc. 12 (1961), 394–399.

Tamás Erdélyi
Department of Mathematics
Texas A&M University
College Station, TX 77843, U.S.A.
E-mail: terdelyi@math.tamu.edu

Received on 12.2.2009
and in revised form on 13.4.2010 (5939)