THREE PIECES OF (COMPUTATIONAL) NUMBER THEORY AND A LITTLE PHILOSOPHY

Peter Borwein

Simon Fraser University Centre for Constructive and Experimental Mathematics

http://www.cecm.sfu.ca/~pborwein

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Individual Digits of Pi

• We give algorithms for the computation of the d-th digit of certain transcendental numbers in various bases.

• These algorithms can be easily implemented (multiple precision arithmetic is not needed), require virtually no memory, and feature run times that scale nearly linearly with the order of the digit desired.

• They make it feasible to compute, for example, the billionth binary digit of $\log(2)$ or π on a modest work station in a few hours run time.

These calculations rest on three observations.

• First, the d-th digit of $1/n$ is “easy” to compute.

• Secondly, this allows for the computation of certain polylogarithm and arctangent series.

• Thirdly, very special polylogarithmic ladders exist for certain numbers like π, π^2, $\log(2)$ and $\log^2(2)$.

For example the critical identity for π:

$$\pi = \sum_{i=0}^{\infty} \frac{1}{16^i}\left(\frac{4}{8i+1} - \frac{2}{8i+4} - \frac{1}{8i+5} - \frac{1}{8i+6}\right).$$

• It is widely believed that computing just the d-th digit of a number like π is really no easier than computing all of the first d digits.

• From a bit complexity point of view this may well be true, although it is probably very hard to prove.

• What we will show is that it is possible to compute just the d-th digit of many transcendentals in (essentially) linear time and logarithmic space.

• We are interested in computing in SC, polynomially logarithmic space and polynomial time.

Actually we are most interested in the space we will denote by SC* of polynomially logarithmic space and (almost) linear time (here we want the time $= O(d \log^{O(1)}(d))$).

• It is not known whether division is possible in SC, similarly it is not known whether base change is possible in SC.

• The situation is even worse in SC*, where it is not even known whether multiplication is possible. If two numbers are in SC* (in the same base) then their product computes in time $= O(d^2 \log^{O(1)}(d))$ and is in SC but not obviously in SC*.

• We will show that the class of numbers we can compute in SC* in base b includes all numbers of the form

$$\sum_{k=1}^{\infty} \frac{1}{p(k) b^{ck}}$$

where p is a polynomial with integer coefficients and c is a positive integer.

• Since addition is possible in SC*, integer linear combinations of such numbers are also feasible (provided the base is fixed).

• The algorithm for the binary digits of π, which also shows that π is in SC* in base 2, rests on the following remarkable identity:

Theorem.

$$\pi = \sum_{i=0}^{\infty} \frac{1}{16^i}\left(\frac{4}{8i+1} - \frac{2}{8i+4} - \frac{1}{8i+5} - \frac{1}{8i+6}\right).$$

Proof. This is equivalent to:

$$\pi = \int_0^{1/\sqrt{2}} \frac{4\sqrt{2} - 8x^3 - 4\sqrt{2}x^4 - 8x^5}{1-x^8}\,dx.$$

which on substituting $y := \sqrt{2}x$ becomes

$$\pi = \int_0^1 \frac{16\,y - 16}{y^4 - 2\,y^3 + 4\,y - 4}\,dy\,.$$

The equivalence follows from the identity

$$\int_0^{1/\sqrt{2}} \frac{x^{k-1}}{1-x^8}\,dx = \int_0^{1/\sqrt{2}} \sum_{i=0}^{\infty} x^{k-1+8i}\,dx$$

$$= \frac{1}{\sqrt{2}^k} \sum_{i=0}^{\infty} \frac{1}{16^i(8i+k)}$$

□

Identities. As usual, we define the m-th polylogarithm L_m by

$$L_m(z) := \sum_{i=1}^{\infty} \frac{z^i}{i^m}, \qquad |z| < 1\,.$$

The most basic identity is

$$-\log(1-2^{-n}) = L_1(1/2^n)$$

which shows that $\log(1-2^{-n})$ is in SC* base 2 for integer n.

• Less obvious are the identities

$\pi^2 =$

$$36L_2(1/2) - 36L_2(1/4) - 12L_2(1/8) + 6L_2(1/64)$$

$\log^2(2) =$

$$4L_2(1/2) - 6L_2(1/4) - 2L_2(1/8) + L_2(1/64)\,.$$

These rewrite as

$$\frac{\pi^2}{36} = \sum_{i=1}^{\infty} \frac{a_i}{2^i i^2}, \qquad [a_i] = [\overline{1,-3,-2,-3,1,0}]$$

$$\frac{\log^2(2)}{2} = \sum_{i=1}^{\infty} \frac{b_i}{2^i i^2}, \quad [b_i] = [\overline{2, -10, -7, -10, 2, -1}]\,.$$

- Thus we see that π^2 and $\log^2(2)$ are in SC* in base 2.

- These are polylogarithmic ladders in the base 1/2 in the sense of Lewin.

We found them by searching for identities of this type using an integer relation algorithm. We have not found them directly in print. However they follow from known results pretty easily.

- There are several ladder identities involving L_3:

$$35/2\zeta(3) - \pi^2 \log(2) =$$

$$36L_3(1/2) - 18L_3(1/4) - 4L_3(1/8) + L_3(1/64)\,,$$

$$2\log^3(2) - 7\zeta(3) =$$

$$-24L_3(1/2) + 18L_3(1/4) + 4L_3(1/8) - L_3(1/64)\,,$$

$$10\log^3(2) - 2\pi^2 \log(2) =$$

$$-48L_3(1/2) + 54L_3(1/4) + 12L_3(1/8) - 3L_3(1/64)\,.$$

• The favored algorithms for π of the last centuries involved some variant of Machin's 1706 formula:

$$\frac{\pi}{4} = 4 \arctan \frac{1}{5} - \arctan \frac{1}{239} \, .$$

There are many related formula but to be useful to us all the arguments of the arctans have to be a power of a common base, and we have not discovered any such formula for π .

• One can however write

$$\frac{\pi}{2} = 2 \arctan \frac{1}{\sqrt{2}} + \arctan \frac{1}{\sqrt{8}}$$

This rewrites as

$$\sqrt{2}\pi = 4 f(1/2) + f(1/8) : \quad f(x) := \sum_{i=1}^{\infty} \frac{(-1)^i x^i}{2i+1}$$

and allows for the calculation of $\sqrt{2}\pi$ in SC*.

• Another two identities involving Catalan's constant G, π and $\log(2)$ are:

$$G - \frac{\pi \log(2)}{8} = \sum_{i=1}^{\infty} \frac{c_i}{2^{\lfloor \frac{i+1}{2} \rfloor} i^2},$$

where

$$[c_i] = [\overline{1, 1, 1, 0, -1, -1, -1, 0}]$$

and

$$\frac{5}{96}\pi^2 - \frac{\log^2(2)}{8} = \sum_{i=1}^{\infty} \frac{d_i}{2^{\lfloor \frac{i+1}{2} \rfloor} i^2},$$

where

$$[d_i] = [\overline{1, 0, -1, -1, -1, 0, 1, 1}]$$

• Thus $8G - \pi \log(2)$ is also in SC* in base 2.

That G is itself in SC* in base 2 is a recent result of Broadhurst.

The Algorithm.

•We wish to evaluate the n-th base b digit of

$$\sum_{k=1}^{\infty} \frac{1}{p(k)b^{ck}}$$

by evaluating the fractional part of

$$(*)\,. \qquad \sum_{k=1}^{\infty} \frac{b^n}{p(k)b^{ck}}$$

Here p is a simple polynomial and c is a fixed integer.

• Evaluating the fractional part of the second sum will evaluate the first sum to as many base b digits after the n-th place as the precision of the calculation.

• The keys are that the fractional part of (*) is the same as the fractional part of

$$(**) \qquad \sum_{k=1}^{\infty} \frac{b^{n-ck} \mod \ p(k)}{p(k)}$$

and that $b^{n-ck} \mod \ p(k)$ can be evaluated quickly.

• Fast evaluation of $b^{n-ck} \bmod p(k)$ is well understood; it rests on the simple fact that if

$$b^m \equiv r \bmod k$$

then

$$(b^m)^2 \equiv r^2 \bmod k.$$

The allows for fast exponentiation $\bmod k$ by the so called binary method.

• (According to Knuth this trick goes back at least to 200 B.C.)

• One evaluates x^n rapidly by successive squaring and multiplication. This reduces the number of multiplications to less than $2\log_2(n)$.

• Note that this is entirely performed with positive integers that do not exceed c^2 in size. Further, it is not subject to round-off error, provided adequate numeric precision is used.

• The key observation is that the the fractional part of b^m/k can be computed quickly.

• For example, in base 10. If we solve

$$10^n \equiv \alpha \bmod k$$

then

$$\frac{10^n}{k} - \frac{\alpha}{k} \in \mathcal{Z}$$

and so $10^n/k$ and a/k have the same fractional parts.

• In particular α/k gives the digits of $1/k$ staring after the n-th place.

• This allows for the calculation of the n-th digit of $10^{-j}/k$ from the computation of

$$10^{n-j} \equiv \alpha \bmod \ k\,.$$

This explains (**) above.

• We are now in a position to evaluate the n-th "digit" (base b) of any series of the type

$$S = \sum_{k=0}^{\infty} \frac{1}{b^{ck} p(k)}$$

where p is a polynomial with integer coefficients. We seek the fractional part of $b^n S$ and so write

$$b^n S \mod 1 = \sum_{k=0}^{\infty} \frac{b^{n-ck}}{p(k)} \mod 1 =$$

$$\sum_{k=0}^{\lfloor n/c \rfloor} \frac{b^{n-ck}}{p(k)} \mod 1 + \sum_{k=\lfloor n/c \rfloor + 1}^{\infty} \frac{b^{n-ck}}{p(k)} \mod 1$$

• For each term of the first summation, the binary exponentiation scheme is used to evaluate the numerator mod $p(k)$.

• The second summation, where powers of b are negative, may be evaluated as written using floating-point arithmetic. It is only necessary to compute a few terms of this summation.

• This is then converted to the desired base b.

Computations.

• Each of our computations employed quad precision floating-point arithmetic for division and sum mod 1 operations.

• Quad precision is supported on the Sun Sparc/20, the IBM RS6000/590, and the SGI Power Challenge (R8000), which were employed in these computations. Quad precision was also used for the exponentiation algorithm on the Sun system.

• On the IBM and the SGI systems, however, we were able to avoid the usage of explicit quad precision, at least in the exponentiation scheme, by exploiting a hardware feature common to these two systems, namely the 106-bit internal registers in the multiply-add operation. This saved considerable time, because quad precision operations are significantly more expensive than 64-bit operations.

• Our results are given below. The first entry, for example, gives the 10^6-th through $10^6 + 13$-th hexadecimal digits of π after the "decimal" point. We believe that all the digits shown below are correct.

• We did the calculations twice. The second calculation, performed for verification purposes, was similar to the first but shifted back one position (this changes all the arithmetic performed).

Constant:	**Base:**	**Position:**	**Digits:**
π	16	10^6	26C65E52CB4593
		10^8	ECB840E21926EC
		10^{10}	921C73C6838FB2
$\log(2)$	16	10^6	418489A9406EC9
		10^9	B1EEF1252297EC
π^2	16	10^6	685554E1228505
		10^9	437A2BA4A13591
$\log^2(2)$	16	10^6	2EC7EDB82B2DF7
		10^9	8BA7C885CEFCE8
$\log(9/10)$	10	10^6	80174212190900
		10^9	44066397959215
		10^{10}	82528693381274

The Forty Trillionth bit of Pi is 0

Between April 19, 1998, and February 9, 1998, one hundred and twenty-six computers from eighteen different countries set a new record for calculating specific bits of Pi. This is due to Colin Percival.

The calculation took a total of about 84,500 cpu hours, and was done using 'idle' time slices (time slices which no other program wants to make use of) under Windows 95 and Windows NT.

The 'average' computer participating was a 200MHz Pentium-based system.

The answer, starting at the 39,999,999,999,997th bit of Pi:

1010 0000 1111 1001 1111 1111 0011 0111 0001 1101

For more information see the PiHex webpage at

http://www.cecm.sfu.ca/projects/pihex/

Logs in base 2. It is easy to compute, in base 2, the d-th binary digit of

$$\log(1 - 2^{-n}) = L_1(1/2^n)\,.$$

So it is easy to compute $\log m$ for any integer m that can be written as

$$m := \frac{(2^{a_1}-1)(2^{a_2}-1)\cdots(2^{a_h}-1)}{(2^{b_1}-1)(2^{b_2}-1)\cdots(2^{b_j}-1)}.$$

• In particular the n-th cyclotomic polynomial evaluated at 2 is so computable. The beginning of this list is:

$$\{2, 3, 5, 7, 11, 13, 17, 31, 43, 57\}\,.$$

• Since

$$2^{18} - 1 = 7 \cdot 9 \cdot 19 \cdot 73,$$

and since 7, $\sqrt{9}$ and 73 are all on the above list we can compute log(19) in SC* from

$$\log(19) = \log(2^{18} - 1) - \log(7) - \log(9) - \log(73).$$

• Note that $2^{11} - 1 = 23 \cdot 89$ so either both log(23) and log(89) are in SC* or neither is.

One can show that no formula of the type on the previous page exists for log(23).

Questions.

• The hardest part of our method is finding an appropriate base b expansion.

• We cannot, at present, compute decimal digits of π by our methods because we know of no identity like Theorem 1 in base 10. But it seems unlikely that this is inherently impossible.

• This raises the following obvious problem.

1] Find an algorithm for the n-th decimal digit of π in SC*.

• It is not even so clear that π is in SC in base 10. This is a result of Plouffe.

• Numbers that are not given by special values of polylogarithms aren't susceptible to our methods. Is this necessarily the case?

2] Are e and $\sqrt{2}$ in SC (SC*) in any base?

• Similarly the treatment of log is incomplete.

3] Is log(2) in SC^* in base 10?

4] Is log(23) in SC^* in base 2?

References

1. M. Abramowitz & I.A. Stegun, *Handbook of Mathematical Functions*, Dover, New York, NY, 1965.

2. A.V. Aho, J.E. Hopcroft, & J.D. Ullman, *The Design and Analysis of Computer Algorithms*, Addison-Wesley, Reading, MA, 1974.

3. D.H. Bailey, J. Borwein and R. Girgensohn, *Experimental evaluation of Euler sums*, Experimental Mathematics **3** (1994), 17–30.

4. J. Borwein, & P Borwein, *Pi and the AGM – A Study in Analytic Number Theory and Computational Complexity*, Wiley, New York, NY, 1987.

5. J. Borwein & P. Borwein, *On the complexity of familiar functions and numbers*, SIAM Review **30** (1988), 589–601.

6. J. Borwein, P. Borwein & D.H. Bailey, *Ramanujan, modular equations and approximations to pi*, M.A.A. Monthly **96** (1989), 201–219.

7. R. Brent, *The parallel evaluation of general arithmetic expressions*, J. Assoc. Comput. Mach. **21** (1974), 201–206.

8. S. Cook, *A taxonomy of problems with fast parallel algorithms*, Information and Control **64** (1985), 2–22.

9. R. Crandall, K. Dilcher, and C. Pomerance, *A search for Wieferich and Wilson primes (preprint).*

10. R. Crandall and J. Buhler, *On the evaluation of Euler sums*, Experimental Mathematics **3,** (1995), 275–285.

11. D.E. Knuth, *The Art of Computer Programming. Vol. 2: Seminumerical Algorithms*, Addison-Wesley, Reading, MA, 1981.

12. L. Lewin, *Polylogarithms and Associated Functions*, North Holland, New York, 1981.

13. L. Lewin, *Structural Properties of Polylogarithms*, Amer. Math. Soc., RI., 1991.

14. N. Nielsen, *Der Eulersche Dilogarithmus*, Halle, Leipzig, 1909.

15. A. Schönhage, *Asymptotically fast algorithms for the numerical multiplication and division of polynomials with complex coefficients*, in: EUROCAM (1982) Marseille, Springer Lecture Notes in Computer Science, vol. 144, 1982, pp. 3–15.

16. J. Todd, *A problem on arc tangent relations*, MAA Monthly **56** (1940), 517–528.

17. H.S. Wilf, *Algorithms and Complexity*, Prentice Hall, Englewood Cliffs, NJ, 1986.

Cyclotomic polynomials with coefficients ± 1

We characterize all cyclotomic polynomials of even degree with coefficients restricted to the set $\{+1, -1\}$. In this context a cyclotomic polynomial is any monic polynomial with integer coefficients and all roots of modulus 1. Inter alia we characterize all cyclotomic polynomials with odd coefficients.

The characterization is as follows. A polynomial $P(x)$ with coefficients ± 1 of even degree $N-1$ is cyclotomic if and only if

$$P(x) = \pm \Phi_{p_1}(\pm x)\Phi_{p_2}(\pm x^{p_1}) \cdots \Phi_{p_r}(\pm x^{p_1 p_2 \cdots p_{r-1}}),$$

where $N = p_1 p_2 \cdots p_r$ and the p_i are primes, not necessarily distinct. Here $\Phi_p(x) := \frac{x^p - 1}{x-1}$ is the pth cyclotomic polynomial.

We conjecture that this characterization also holds for polynomials of odd degree with ± 1 coefficients. This conjecture is based on substantial computation plus a number of special cases.

Mahler raised the question of maximizing the Mahler measure of Littlewood polynomials. The Mahler measure is just the L_0 norm on the circle and one would expect this to be closely related to the minimization problem for the L_4 norm (which has been much studied).

Of course the minimum possible Mahler measure for a Littlewood polynomial is 1 and this is achieved by any cyclotomic polynomial.

For us a cyclotomic polynomial is any monic polynomial with integer coefficients and all roots of modulus 1. While $\Phi_n(x)$ denotes **the** nth irreducible cyclotomic polynomial (the minimum polynomial of a primitive nth root of unity).

As above we show that a polynomial $P(x)$ with coefficients ± 1 of even degree $N-1$ is cyclotomic if and only if

$$P(x) = \pm\Phi_{p_1}(\pm x)\Phi_{p_2}(\pm x^{p_1})\cdots\Phi_{p_r}(\pm x^{p_1 p_2 \cdots p_{r-1}}),$$

where $N = p_1 p_2 \cdots p_r$ and the p_i are primes (not necessarily distinct). The "if" part is obvious since $\Phi_{p_i}(x)$ has coefficients ± 1.

We also give an explicit formula for the number of such polynomials.

This analysis is based on a careful treatment of Graeffe's root squaring algorithm. It transpires that all cyclotomic Littlewood polynomials of a fixed degree have the same fixed point on iterating Graeffe's root squaring algorithm. This allows us to also characterize all cyclotomic polynomials with odd coefficients.

Substantial computations, as well as a number of special cases, lead us to conjecture that the above characterization of cyclotomic Littlewood polynomials of even degree also holds for odd degree. One of the cases we can handle is when N is a power of 2.

It is worth commenting on the experimental aspects of this paper. (As is perhaps usual, much of this is carefully erased in the final exposition). It is really the observation that the cyclotomic Littlewood polynomials can be explicitly constructed essentially by inverting Graeffe's root squaring algorithm that is critical. This allows for computation over all cyclotomic Littlewoods up to degree several hundred (with exhaustive search failing far earlier). A construction which is of interest in itself. Indeed it was these calculations that allowed for the conjectures of the paper and suggested the route to some of the results.

Cyclotomic Polynomials with Odd Coefficients.

We discuss the factorization of cyclotomic polynomials with odd coefficients as a product of irreducible cyclotomic polynomials. To do this, we first consider the factorization over $\mathcal{Z}_p[x]$ where p is a prime number. The most useful case is $p = 2$ because every Littlewood polynomial reduces to the Dirichlet kernel $1 + x + \cdots + x^{N-1}$ in $\mathcal{Z}_2[x]$. In $\mathcal{Z}_p[x]$, $\Phi_n(x)$ is no longer irreducible in general but $\Phi_n(x)$ and $\Phi_m(x)$ are still relatively prime to each other. Here, as before, $\Phi_n(x)$ is **the** nth irreducible cyclotomic polynomial.

Lemma. *Suppose n and m are distinct positive integers relatively prime to p. Then $\Phi_n(x)$ and $\Phi_m(x)$ are relatively prime in $\mathcal{Z}_p[x]$.*

The following lemma tells which $\Phi_m(x)$ can possibly be factors of polynomials with odd coefficients.

Lemma. *Suppose $P(x)$ is a polynomial with odd coefficients of degree $N-1$. If $\Phi_m(x)$ divides $P(x)$, then m divides $2N$.*

In view of the Lemmas every cyclotomic polynomial, $P(x)$, with odd coefficients of degree $N-1$ can be written as

$$P(x) = \prod_{d|2N} \Phi_d^{e(d)}(x)$$

where $e(d)$ are non-negative integers.

For each prime p let T_p be the operator defined over all monic polynomials in $\mathcal{Z}[x]$ by

$$T_p[P(x)] := \prod_{i=1}^{N} (x - \alpha_i^p)$$

for every $P(x) = \prod_{i=1}^{N}(x - \alpha_i)$ in $\mathcal{Z}[x]$.

We extend T_p to be defined over the quotient of two monic polynomials in $\mathcal{Z}[x]$ by

$$T_p[(P/Q)(x)] := T_p[P(x)]/T_P[Q(x)].$$

This operator obviously takes a polynomial to the polynomial whose roots are the pth powers of the roots of P. Also we let M_p be the natural projection from $\mathcal{Z}[x]$ onto $\mathcal{Z}_p[x]$. So,

$$M_p[P(x)] = P(x) \pmod{p}.$$

Lemma. *Let n be a positive integer relatively prime to p and $i \geq 2$. Then we have*

$T_p[\Phi_n(x)] = \Phi_n(x),$

$T_p[\Phi_{pn}(x)] = \Phi_n(x)^{p-1},$

$T_p[\Phi_{p^i n}(x)] = \Phi_{p^{i-1}n}(x)^p.$

When $P(x)$ is cyclotomic, the iterates $T_p^n[P(x)]$ converge in a finite number of steps to a fixed point of T_p and we define this to be the fixed point of $P(x)$ with respect to T_p.

Lemma. *If $P(x)$ is a monic cyclotomic polynomial in $\mathcal{Z}[x]$, then*

$$M_p[T_p[P(x)]] = M_p[P(x)],$$

in $\mathcal{Z}_p[x]$, where M_p is the above natural projection.

The Lemma shows that if $T_p[P(x)] = T_p[Q(x)]$ then $M_p[P(x)] = M_p[Q(x)]$. The next result shows that the converse is also true.

Theorem. *$P(x)$ and $Q(x)$ are monic cyclotomic polynomials in $\mathcal{Z}[x]$ and $M_p[P(x)] = M_p[Q(x)]$ in $\mathcal{Z}_p[x]$ if and only if both $P(x)$ and $Q(x)$ have the same fixed point with respect to iteration of T_p.*

From the Theorem we can characterize the monic cyclotomic polynomials by their images in $\mathcal{Z}_p[x]$ under the projection M_p. They all have the same fixed point under T_p. In particular, when $p = 2$ we have

Corollary. *All monic cyclotomic polynomials with odd coefficients of the degree $N-1$ have the same fixed point under iteration of T_2. Specifically, if $N = 2^t M$ where $t \geq 0$ and $(2, M) = 1$ then the fixed point occurs at the $t+1$-th step of the iteration and equals*

$$(x^M - 1)^{2^t} (x-1)^{-1}.$$

The Corollary when N is odd ($t = 0$) shows that $T_2[P(x)]$ equals to $1 + x + \cdots + x^{N-1}$ for all cyclotomic polynomials with odd coefficients and we have the following characterization of cyclotomic polynomials with odd coefficients.

Corollary. *Let $N = 2^t M$ with $t \geq 0$ and $(2, M) = 1$. A polynomial, $P(x)$, with odd coefficients of degree $N-1$ is cyclotomic if and only if*

$$P(x) = \prod_{d|M} \Phi_d^{e(d)}(x)\Phi_{2d}^{e(2d)}(x) \cdots \Phi_{2^{t+1}d}^{e(2^{t+1}d)}(x),$$

and the $e(d)$ satisfy the conditions:

$$e(d) + \sum_{i=1}^{t+1} 2^{i-1} e(2^i d) = 2^t \ for\ t > 1$$

and is $2^t - 1$ for $t = 1$.

Furthermore, if N is odd, then any polynomial, $P(x)$, with odd coefficients of even degree $N-1$ is cyclotomic if and only if

$$P(x) = \prod_{d|N, d>1} \Phi_d^{e(d)}(\pm x)$$

where the $e(d)$ are non-negative integers.

This Corollary allows us to compute the number of cyclotomic polynomials with odd coefficients. Let $B(n)$ be the number of partitions of n into a sum of terms of the sequence $\{1, 1, 2, 4, 8, 16, \cdots\}$. Then $B(n)$ has generating function

$$F(x) = (1-x)^{-1} \prod_{k=0}^{\infty} (1 - x^{2^k})^{-1}.$$

It follows that

Corollary. *Let* $N = 2^t M$ *with* $t \geq 0$ *and* $(2, M) = 1$. *The number of cyclotomic polynomials with odd coefficients of degree* $N-1$ *is*

$$C(N) = B(2^t)^{d(M)-1} \cdot B(2^t - 1)$$

where $d(M)$ *denotes the number of divisors of* M. *Furthermore,*

$$\log C(N) \sim (\frac{t^2}{2} \log 2)(d(M) - 1) + \frac{(\log(2^t - 1))^2}{\log 4}.$$

Cyclotomic Littlewood Polynomials.

We now specialize the discussion to the case where the coefficients are all plus one or minus one.

One natural way to build up Littlewood polynomial of higher degree is as follows: if $P_1(x)$ and $P_2(x)$ are Littlewood polynomials and $P_1(x)$ is of degree $N-1$ then $P_1(x)P_2(x^N)$ is a Littlewood polynomials of higher degree. In this section, we are going to show that this is also the only way to produce cyclotomic Littlewood polynomials, at least, for even degree.

To prove this, it is equivalent to show that the coefficients of $P(x)$ are "periodic". This is the key to the next result.

Theorem. *Suppose N is odd. A Littlewood polynomial, $P(x)$, of degree $N-1$ is cyclotomic if and only if*

$$P(x) = \pm\Phi_{p_1}(\pm x)\Phi_{p_2}(\pm x^{p_1})\cdots\Phi_{p_r}(\pm x^{p_1 p_2 \cdots p_{r-1}}),$$

where $N = p_1 p_2 \cdots p_r$ and the p_i are primes, not necessarily distinct.

Corollary. *Suppose N is odd. Then $P(x)$ is cyclotomic in L of degree $N-1$ if and only if*

$$P(x) = \pm\prod_{i=1}^{t} \frac{x^{N_i} + (-1)^{\epsilon+i}}{x^{N_{i-1}} + (-1)^{\epsilon+i}}$$

where $\epsilon = 0$ or 1, $N_0 = 1, N_t = N$ and N_{i-1} is a proper divisor of N_i for $i = 1, 2, \cdots, t$.

Using this Corollary we can count the number of cyclotomic Littlewood polynomials of given even degree.

Cyclotomic Littlewood Polynomials of Odd Degree. We conjecture explicitly tha the main Theorem also holds for polynomials of odd degree.

Conjecture. *A Littlewood polynomial, $P(x)$, of degree $N-1$ is cyclotomic if and only if*

$$P(x) = \pm\Phi_{p_1}(\pm x)\Phi_{p_2}(\pm x^{p_1})\cdots\Phi_{p_r}(\pm x^{p_1p_2\cdots p_{r-1}}),$$

where $N = p_1p_2\cdots p_r$ and the p_i are primes, not necessarily distinct.

We computed up to degree 210 (except for the case $N-1 = 191$). The computation was based on computing all cyclotomic polynomials with odd coefficients of a given degree and then checking which were actually Littlewood and seeing that this set matched the set generated by the conjecture. For example, for $N-1 = 143$ there are 6773464 cyclotomic polynomials with odd coefficients of which 416 are Littlewood. For $N-1 = 191$ there are 697392380 cyclotomic polynomials with odd coefficients (which was too big for our program).

We can generate all the cyclotomics with odd coefficients from Corollary 2.7 quite easily so the bulk of the work is involved in checking which ones have height 1. The set in the conjecture computes very easily recursively.

Some special cases also support the conjecture. Most notably the case where N is a power of 2.

Littlewood Type Problems

We are primarily concerned with polynomials with coefficients in the set $\{+1,-1\}$. Since many of these problems were raised by Littlewood we denote the set of such polynomials by $\mathcal{L}_n$ and refer to them as Littlewood polynomials. Specifically

$$\mathcal{L}_n := \left\{ p : p(x) = \sum_{j=0}^{n} a_j x^j \,, \quad a_j \in \{-1, 1\} \right\}.$$

The following conjecture is due to Littlewood probably from some time in the fifties. It has been much studied and has associated with it a considerable literature

Conjecture. *It is possible to find $p_n \in \mathcal{L}_n$ so that*

$$C_1\sqrt{n+1} \le |p_n(z)| \le C_2\sqrt{n+1}$$

for all complex z of modulus 1. Here the constants C_1 and C_2 are independent of n.

Such polynomials are often called "locally flat". Because the L_2 norm of a polynomial from $\mathcal{L}_n$ is exactly $\sqrt{n+1}$ the constants must satisfy $C_1 \le 1$ and $C_2 \ge 1$.

It is still the case that no sequence is known that satisfies the lower bound.

A sequence of Littlewood polynomials that satisfies just the upper bound is given by the Rudin-Shapiro polynomials:

$$p_0(z) := 1, \qquad q_0(z) := 1$$

and

$$p_{n+1}(z) := p_n(z) + z^{2^n} q_n(z),$$

$$q_{n+1}(z) := p_n(z) - z^{2^n} q_n(z)$$

These have all coefficients ± 1 and are of degree $2^n - 1$. From

$$|p_{n+1}|^2 + |q_{n+1}|^2 = 2(|p_n|^2 + |q_n|^2)$$

we have for all z of modulus 1

$$|p_n(z)| \leq 2\sqrt{2}^n = \sqrt{2}\sqrt{\deg(p_n)}$$

and

$$|q_n(z)| \leq 2\sqrt{2}^n = \sqrt{2}\sqrt{\deg(q_n)}$$

This conjecture is complemented by a conjecture of Erdős.

Conjecture. *The constant C_2 in Littlewood's conjecture is bounded away from 1 (independently of n).*

This is also still open. Though a remarkable result of Kahane's shows that if the polynomials are allowed to have complex coefficients of modulus 1 then "locally flat" polynomials exist and indeed that it is possible to make C_1 and C_2 asymptotically arbitrarily close to 1.

Another striking result due to Beck proves that "locally flat" polynomials exist from the class of polynomials of degree n whose coefficients are 400th roots of unity.

Because of the monotonicity of the L_p norms it is relevant to rephrase Erdős' conjecture in other norms. Newman and Byrnes speculate that

$$||p||_4^4 \geq (6-\delta)n^2/5$$

for $p \in \mathcal{L}_n$ and n sufficiently large. This, of course, would imply Erdős' conjecture above. Here

$$||q||_p = \left(\int_0^{2\pi} |q(\theta)|^p \, d\theta/(2\pi)\right)^{1/p}$$

is the normalized p norm on the boundary of the unit disc.

It is possible to find a sequence of $p_n \in \mathcal{L}_n$ so that

$$||p_n||_4^4 \asymp (7/6)n^2.$$

This sequence is constructed out of the Fekete polynomials

$$f_p(z) := \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) z^k$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. One now takes the Fekete polynomials and cyclically permutes the coefficients by about $p/4$ to get the above example due to Turyn.

Problem. *Show for some absolute constant $\delta > 0$ and for all $p_n \in \mathcal{L}_n$*

$$||p||_4 \geq (1 + \delta)\sqrt{n}$$

or even the much weaker

$$||p||_4 \geq \sqrt{n} + \delta.$$

A very interesting question is how to compute the minimal L_4 Littlewood polynomials (say up to degree 200).

A Barker polynomial

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

with each $a_k \in \{-1, +1\}$ so that

$$p(z)\overline{p(z)} := \sum_{k=-n}^{n} c_k z^k$$

satisfies $c_0 = n + 1$ and

$$|c_j| \leq 1, \qquad j = 1, 2, 3 \ldots .$$

Here

$$c_j = \sum_{k=0}^{n-j} a_k a_{n-k} \qquad and \qquad c_{-j} = c_j.$$

If $p(z)$ is a Barker polynomial of degree n then

$$||p||_4 \leq ((n+1)^2 + 2n))^{1/4}$$

The nonexistence of Barker polynomials of degree n is now shown by showing

$$||p_n||_4 \geq (n+1)^{1/2} + (n+1)^{-1/2}/2.$$

This is even weaker than the weak form of the preceding problem.

It is conjectured that no Barker polynomials exist for $n > 12$.

We can compute the expected L_p norm of Littlewood polynomials (B and Lockhart).

For random $q_n \in \mathcal{L}_n$

$$\frac{\mathrm{E}(||q_n||_p)}{n^{1/2}} \to (\Gamma(1+p/2))^{1/p}$$

and for derivatives

$$\frac{\mathrm{E}(||q_n^{(r)}||_p)}{n^{(2r+1)/2}} \to (2r+1)^{-1/2}(\Gamma(1+p/2))^{1/p}.$$

Explicit Merit Calculations

Our main purpose is to give explicit formulas for the L_4 norms (on the boundary of the unit disc) and hence, also the merit factors of various polynomials that are closely related to the Fekete polynomials.

As usual the L_α norm on the boundary of the unit disc is defined by

$$\|p\|_\alpha = \left(\frac{1}{2\pi} \int_0^{2\pi} |p(e^{i\theta})|^\alpha \, d\theta \right)^{1/\alpha}.$$

The L_4 norm of a polynomial is particularly easy to work with because it can be computed as the square root of the L_2 norm of $p(z)\overline{p(z)}$ and hence, computes exactly as the fourth root of the sum of the squares of the coefficients of $p(z)\overline{p(z)}$. In contrast, the supremum norm or other L_p norms, where p is not an even integer, are computationally difficult.

Let q be a prime number and let $\left(\frac{\cdot}{q}\right)$ be the Legendre symbol.

The Fekete polynomials are defined by

$$f_q(z) := \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) z^k$$

and the closely related polynomials

$$F_q(z) := 1 + f_q(z) = 1 + \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) z^k.$$

The half–Fekete polynomials are defined by

$$G_q(z) := \sum_{k=1}^{(q-1)/2} \left(\frac{k}{q}\right) z^k.$$

If we cyclically permute the coefficients of f_q by about $q/4$ places we get an example of Turyn's which we denote by

$$R_q(z) := \sum_{k=0}^{q-1} \left(\frac{k + [q/4]}{q} \right) z^k$$

where $[\cdot]$ denotes the nearest integer, and we denote the general shifted Fekete polynomials by

$$f_q^t(z) := \sum_{k=0}^{q-1} \left(\frac{k + t}{q} \right) z^k.$$

Note that R has one coefficient that is zero (from the permutation of the constant term in f). For example

$$f_{11} := -x^{10} + x^9 - x^8 - x^7 - x^6 + x^5 + x^4 + x^3 - x^2 + x$$

and

$$R_{11} := -x^{10} + x^9 - x^7 + x^6 - x^5 - x^4 - x^3 + x^2 + x + 1.$$

The explicit formulas involve the class number of the imaginary quadratic field of $\mathbb{Q}(\sqrt{-d})$ which is denoted by $h(-d)$. For any odd prime d it can be computed as

$$h(-d) = \lambda_d \sum_{k=1}^{(d-1)/2} \left(\frac{k}{d}\right)(-1)^k = \lambda_d G_d(-1)$$

where

$$\lambda_d := \begin{cases} 1 & \text{if} \quad d \equiv 1, 7 \pmod 8, \\ -1/3 & \text{if} \quad d \equiv 3 \pmod 8, \\ -1 & \text{if} \quad d \equiv 5 \pmod 8. \end{cases}$$

For primes $d \equiv 3 \pmod 4$ it can also be computed as

$$h(-d) = -\frac{f_d'(1)}{d} = -\frac{1}{d} \sum_{k=1}^{d-1} \left(\frac{k}{d}\right) k$$

(this sum is 0 for $d \equiv 1 \pmod 4$).

There are two natural measures of smallness for the L_4 norm of a polynomial p. One is the ratio of the L_4 norm to the L_2 norm, $\|p\|_4/\|p\|_2$. The other (equivalent) measure is the merit factor, defined by

$$\mathrm{MF}(p) = \frac{\|p\|_2^4}{\|p\|_4^4 - \|p\|_2^4}.$$

Littlewood polynomials are the set

$$\mathcal{L}_n := \left\{ p : p(x) = \sum_{j=0}^{n} a_j x^j \,, \;\; a_j \in \{-1, 1\} \right\}.$$

The L_2 norm of any element of $\mathcal{L}_{n-1}$ is $\sqrt{n}$ and this is, of course, a lower bound for the L_4 norm.

The expected L_4 norm of an element of $\mathcal{L}_n$ is is $2^{1/4}\sqrt{n}$. The expected merit factor is thus 1.

The $\{R_q\}$ above are a sequence with asymptotic merit factor 6. Golay gives a heuristic argument for this observation of Turyn's and this is proved rigorously by T. Høholdt and H. Jensen

The Fekete polynomials themselves have asymptotic merit factor 3/2 and different amounts of cyclic permutations can give rise to any asymptotic merit factor between 3/2 and 6.

Golay speculates that 6 may be the largest possible asymptotic merit factor. He writes "the eventuality must be considered that no systematic synthesis will ever be found which will yield higher merit factors."

Newman and Byrnes, apparently independently, make a similar conjecture. As do Høholdt and Jensen.

Computations by a number of people on polynomials up to degree 200 are equivocal. See the web page of A. Reinholz at http://borneo.gmd.de/∼andy/ACR.html.

The Fekete polynomial f_q has modulus $\sqrt{q}$ at each qth root of unity (as does f_q^t) and one might hope that they also satisfy the upper bound in Littlewood's conjecture but Montgomery shows that this is not the case.

Littlewood's conjecture is that it is possible to find $p_n \in \mathcal{L}_{n-1}$ so that

$$C_1\sqrt{n} \leq |p_n(z)| \leq C_2\sqrt{n}$$

for all z of modulus 1 and for two constants C_1, C_2 independent of n.

2. Results

Theorem 1. *For q an odd prime, the Fekete polynomial,*

$$f_q(z) := \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) z^k$$

satisfies

$$\|f_q\|_4^4 = \frac{5q^2}{3} - 3q + \frac{4}{3} - \gamma_q$$

where

$$\gamma_q := \begin{cases} 0 & \textit{if} \quad q \equiv 1 \pmod 4, \\ 12(h(-q))^2 & \textit{if} \quad q \equiv 3 \pmod 4. \end{cases}$$

Theorem 2. *For q an odd prime, the modified Fekete polynomial,*

$$F_q(z) := 1 + \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) z^k$$

satisfies

$$\|F_q\|_4^4 = \frac{5q^2}{3} + q - \frac{5}{3} - \gamma_q$$

where

$$\gamma_q := \begin{cases} 0 & \textit{if} \quad q \equiv 1 \pmod 4, \\ 12h(-q)(h(-q)+1) & \textit{if} \quad q \equiv 3 \pmod 4. \end{cases}$$

Theorem 3. *For q an odd prime the half–Fekete polynomials*

$$G_q(z) := \sum_{k=1}^{(q-1)/2} \left(\frac{k}{q}\right) z^k.$$

satisfy

$$\|G_q\|_4^4 = \frac{q^2}{3} - \frac{q}{2} + \frac{1}{6} - \gamma_q (h(-q))^2$$

where

$$\gamma_q := \begin{cases} 0 & \textit{if} \quad q \equiv 1 \pmod 4, \\ 2 & \textit{if} \quad q \equiv 7 \pmod 8, \\ 6 & \textit{if} \quad q \equiv 3 \pmod 8. \end{cases}$$

The exact same formulae above hold for the polynomials $(f_q(z) + f_q(-z))/2$ and $(f_q(z) - f_q(-z))/2$.

Theorem 4. *For q an odd prime, the Turyn type polynomials*

$$R_q(z) := \sum_{k=0}^{q-1} \left(\frac{k + [q/4]}{q} \right) z^k$$

where $[\cdot]$ denotes the nearest integer, satisfy

$$\|R_q\|_4^4 = \frac{7q^2}{6} - q - \frac{1}{6} - \gamma_q$$

and

$$\gamma_q := \begin{cases} h(-q)(h(-q) - 4) & \textit{if} \quad q \equiv 1, 5 \pmod 8, \\ 12(h(-q))^2 & \textit{if} \quad q \equiv 3 \pmod 8, \\ 0 & \textit{if} \quad q \equiv 7 \pmod 8. \end{cases}$$

Theorem 5. *For q an odd prime, the shifted Fekete polynomials*

$$f_q^t(z) := \sum_{k=0}^{q-1} \left(\frac{k+t}{q}\right) z^k$$

satisfy

$$\|f_q^t\|_4^4 =$$

$$\frac{1}{3}(5q^2+3q+4)+8t^2-4qt-8t-\frac{8}{q^2}\left(1-\frac{1}{2}\left(\frac{-1}{q}\right)\right)\left|\sum_{n=1}^{q-1} n\left(\frac{n+t}{q}\right)\right|^2,$$

and

$$\|f_q^{q-t+1}\|_4^4 = \|f_q^t\|_4^4$$

if $1 \le t \le (q-1)/2$.

Montgomery shows that the maximum modulus of $f_q(z)$ at the $2q$th root of unity is at least $\frac{2}{\pi}\sqrt{q}\log\log q$.

Corollary 6. *For q an odd prime, we have*

$$\sum_{j=0}^{q-1} |f_q(-e^{\frac{2\pi i k}{q}})|^4 = \frac{q}{3}(7q-8)(q-1) - 2q\gamma_q$$

where γ_q is the same as in Theorem 1.

Theorem 7. *For q an odd prime, the shifted Fekete polynomials*

$$f_q^t(z) := \sum_{k=0}^{q-1} \left(\frac{k+t}{q}\right) z^k$$

satisfy

$$\|f_q^t\|_4^4 = \|f_q^{q-t+1}\|_4^4 = \frac{5q^2}{3} + 8t^2 - 4qt + O(q(\log q)^2)$$

if $1 \le t \le (q-1)/2$.

Theorem 7 follows from Theorem 5 on observing that

$$\frac{1}{q}\sum_{n=1}^{q-1} n\left(\frac{n+k}{q}\right) = \sum_{n=1}^{k-1}\left(\frac{n}{q}\right) + \frac{1}{q}\sum_{n=1}^{q-1} n\left(\frac{n}{q}\right).$$

This is coupled with the known estimate

$$\left|\sum_{n=1}^{k-1}\left(\frac{n}{q}\right)\right| < q^{\frac{1}{2}} \log q$$

and the observation that

$$-\frac{1}{q}\sum_{n=1}^{q-1} n\left(\frac{n}{q}\right)$$

equals the class number, $h(-q)$, for primes $q \equiv 3 \pmod 4$ and is zero for primes $q \equiv 1 \pmod 4$. The asymptotics of Turyn et al mentioned previously are the above theorem in the case where t is a constant multiple of q.

Theorem 8. *Let*

$$L_n(z) := \sum_{k=0}^{n-1} e^{\frac{k(k+1)\pi i}{n}} z^k$$

$$\|L_n\|_4^4 = n^2 + \frac{2n^{3/2}}{\pi} + \delta_n \frac{n^{1/2}}{3} + O(n^{-1/2})$$

where

$$\delta_n := \begin{cases} -2 & \text{if} \quad n \equiv 0, 1 \pmod 4, \\ 1 & \text{if} \quad n \equiv 2, 3 \pmod 4). \end{cases}$$

The above example of Littlewoods depends on the asymptotic series for

$$\sum_{j=1}^{n-1} \frac{sin^2(j^2\pi/n)}{sin^2(j\pi/n)}$$

because, in the above notation,

$$\|L_n\|_4^4 = n^2 + 2\sum_{j=1}^{n-1} \frac{sin^2(j^2\pi/n)}{sin^2(j\pi/n)}.$$

Let q be a prime and χ be a non-principal character mod q. Let

$$f_\chi^t(z) := \sum_{n=0}^{q-1} \chi(n+t) z^n$$

for $1 \le t \le q$ be the character polynomial associated to χ (cyclically permuted t places).

Theorem 9. *For any non-principal and non-real character χ modulo q and $1 \le t \le q$, we have*

$$\|f_\chi^t(z)\|_4^4 = \frac{4}{3} q^2 + O(q^{3/2} \log^2 q)$$

where the implicit constant is independent of t and q. Here $\| \cdot \|_4$ denotes the L_4 norm on the unit circle.

It follows from this that all cyclically permuted character polynomials associated with non-principal and non-real characters have merit factors that approach 3.

We also compute the averages of the L_4 norms:

Theorem 10. *Let q be a prime number. We have*

$$\sum_{\chi \pmod q} \|f_\chi^t\|_4^4 = (2q-3)(q-1)^2$$

where the summation is over all characters modulo q.

Proof of Theorem 5

Let q be a prime number and, as before, let

$$f_q(z) := \sum_{n=1}^{q-1} \left(\frac{n}{q}\right) z^n$$

be the Fekete polynomial. Define

$$\epsilon_q := \begin{cases} 1 & \text{if} \quad q \equiv 1 \pmod 4, \\ i & \text{if} \quad q \equiv 3 \pmod 4. \end{cases}$$

Then we have the following well-known result

$$f_q(\omega^k) = \epsilon_q \sqrt{q} \left(\frac{k}{q}\right).$$

for $k = 0, 1, \cdots, q-1$, where $\omega := e^{2\pi i/q}$.

Lemma 1. *For any $1 \le t \le q$, we have*

$$\sum_{b=1}^{q-1} \left(\frac{b}{q}\right) \frac{\omega^{bt}}{\omega^b - 1} = \frac{\epsilon_q}{\sqrt{q}} \sum_{n=1}^{q-1} n \left(\frac{n+t}{q}\right).$$

Lemma 2. *If* $1 \leq k \leq q$, *then*

$$\sum_{\substack{n,m=1 \\ k+n+m\equiv 0 \pmod q}}^{q-1} nm = \frac{q}{6}(q^2 - 6q - 1 + 6k + 3qk - 3k^2).$$

Lemma 3. *If* $1 \leq k \leq q$, *then*

$$\sum_{\substack{a,b=1 \\ a\neq b}}^{q-1} \frac{\omega^{(a-b)k}}{(\omega^{a-b}-1)^2} = -\frac{1}{12}(q-2)(q^2+6q+5-12k-6qk+6k^2).$$

As before let $f_q^t(z)$ be the shifted Fekete polynomial obtained by shifting the coefficients to the left by t where $1 \leq t \leq q$. So $f_q^q(z) = f_q(z)$. Then we have

$$f_q^t(\omega^k) = \omega^{-tk} f_q(\omega^k)$$

for any $0 \leq k \leq q-1$. We are going to evaluate the following summation

$$\sum_{k=0}^{q-1} |f_q^t(-\omega^k)|^4.$$

We use the basic approach of T. Høholdt and H. Jensen which is by interpolation at the $2q$th roots of unity. Using the Lagrange interpolation formula at the qth roots of unity, we have

$$f_q^t(z) = \frac{1}{q} \sum_{j=0}^{q-1} \frac{z^q - 1}{z - \omega^j} \omega^j f_q^t(\omega^j).$$

It follows that

$$\begin{aligned}
\sum_{k=0}^{q-1} |f_q^t(-\omega^k)|^4 &= \frac{16}{q^4} \sum_{k=0}^{q-1} \left| \sum_{j=0}^{q-1} \frac{\omega^j}{\omega^k + \omega^j} f_q^t(\omega^j) \right|^4 \\
&= \frac{16}{q^4} \sum_{a,b,c,d=0}^{q-1} f_q^t(\omega^a) \bar{f}_q^t(\omega^b) f_q^t(\omega^c) \bar{f}_q^t(\omega^d) \omega^{a+c} \\
&\qquad \times \sum_{k=0}^{q-1} \frac{1}{\omega^k + \omega^a} \frac{\omega^k}{\omega^k + \omega^b} \frac{1}{\omega^k + \omega^c} \frac{\omega^k}{\omega^k + \omega^d}.
\end{aligned}$$

We then group the terms in the above summation over a, b, c and d by the following cases:

(1) $a = c$ and $a \neq b \neq d$,
(2) $a = b = c \neq d$,
(3) $a = b \neq c = d$,
(4) $a = b = c = d$,
(5) $a \neq b \neq c \neq d$,

and we obtain the following formula

$$\sum_{k=0}^{q-1} |f_q^t(-\omega^k)|^4 = \frac{16}{q^4}(A+B+C+D)$$

where

$$A = \frac{1}{48} q^2(q^2+2) \sum_{a=0}^{q-1} |f_q^t(\omega^a)|^4$$

$$B =$$

$$\frac{q^2}{4} \sum_{\substack{a,b=0 \\ a\neq b}}^{q-1} |f_q^t(\omega^a)|^2 (\bar{f}_q^t(\omega^a) f_q^t(\omega^b)\omega^b + f_q^t(\omega^a)\bar{f}_q^t(\omega^b)\omega^a) \left(\frac{\omega^a+\omega^b}{(\omega^a-\omega^b)^2} \right)$$

$$C = -\frac{q^2}{4} \sum_{\substack{a,b,c=0 \\ a\neq b\neq c}}^{q-1} 2|f_q^t(\omega^a)|^2 \left(\frac{f_q^t(\omega^b)\bar{f}_q^t(\omega^c)\omega^{a+b} + f_q^t(\omega^c)\bar{f}_q^t(\omega^b)\omega^{a+c}}{(\omega^b-\omega^a)(\omega^c-\omega^a)} \right)$$

$$- \frac{q^2}{4} \sum_{\substack{a,b,c=0 \\ a\neq b\neq c}}^{q-1} \frac{f_q^t(\omega^a)^2 \bar{f}_q^t(\omega^b)\bar{f}_q^t(\omega^c)\omega^{2a} + \bar{f}_q^t(\omega^a)^2 f_q^t(\omega^b) f_q^t(\omega^c)\omega^{b+c}}{(\omega^b-\omega^a)(\omega^c-\omega^a)}$$

$$D = -\frac{q^2}{4}$$

$$\sum_{\substack{a,b=0 \\ a\neq b}}^{q-1} \frac{4|f_q^t(\omega^a)|^2|f_q^t(\omega^b)|^2\omega^{a+b} + f_q^t(\omega^b)^2\bar{f}_q^t(\omega^a)^2\omega^{2b} + f_q^t(\omega^a)^2\bar{f}_q^t(\omega^b)^2\omega^{2a}}{(\omega^a-\omega^b)^2}.$$

Here A, B, C and D are the sum of terms according to the above cases (1), (2), (3) and (4) respectively and the sum of terms corresponding to the case (5) is zero.

We now evaluate A, B, C and D separately. The details are formidable.

To prove Theorem 4 we need .

Lemma 4. *Let q be a prime and $q > 3$. Then we have*

$$\sum_{n=1}^{[\frac{q}{4}]-1} \left(\frac{n}{q}\right) = \begin{cases} \frac{1}{2}h(-q) - 1 & \text{if} \quad q \equiv 1 \pmod 4, \\ 0 & \text{if} \quad q \equiv 3 \pmod 8, \\ h(-q) & \text{if} \quad q \equiv 7 \pmod 8. \end{cases}$$

References

[Be-91] J. Beck, *Flat polynomials on the unit circle – note on a problem of Littlewood*, Bull. London Math. Soc. **23** (1991), 269–277.

[Bo-A] P. Borwein, *Some Old Problems on Polynomials with Integer Coefficients*, Proceedings of the Ninth Conference on Approximation Theory, 1998.

[BL-A] P. Borwein and R. Lockhart, *The expected L_p norm of random polynomials*, (under submission).

[BM-A] P. Borwein and M. Mossinghoff, *Rudin-Shapiro like Polynomials in L_4*, (under submission).

[CGP-98] B. Conrey, A. Granville and B. Poonen, *Zeros of Fekete polynomials*, (in press).

[Go-77] M. J. Golay, *Sieves for low autocorrelation binary sequences*, IEEE Trans. Inform. Theory **23** (1977), 43–51.

[Go-83] M. J. Golay, *The merit factor of Legendre sequences*, IEEE Trans. Inform. Theory **29** (1983), 934–936.

[Hø-88] T. Høholdt and H. Jensen, *Determination of the merit factor of Legendre sequences*, IEEE Trans. Inform. Theory **34** (1988), 161–164.

[Hu-82] L. K. Hua, *Introduction to Number Theory*, Springer–Verlag, Berlin, 1982.

[Je-91] J. Jensen, H. Jensen and T. Høholdt, *The merit factor of binary sequences related to difference sets*, IEEE Trans. Inform. Theory **37** (1991), 617–626.

[Ka-80] J-P. Kahane, *Sur les polynômes á coefficients unimodulaires*, Bull. London Math. Soc. **12** (1980), 321–342.

[Li-68] J. E. Littlewood, *Some Problems in Real and Complex Analysis*, Heath Mathematical Monographs, Lexington, Massachusetts, 1968.

[Me-96] S. Mertens, *Exhaustive search for low-autocorrelation binary sequences*, J. Phys. A **29** (1996), L473–L481.

[Mo-80] H. L. Montgomery, *An exponential sum formed with the Legendre symbol*, Acta Arith. **37** (1980), 375–380.

[Ne-90] D. J. Newman and J. S. Byrnes, *The L^4 norm of a polynomial with coefficients* ± 1, Amer. Math. Monthly **97** (1990), 42–45.

[Re-93] A. Reinholz, *Ein paralleler genetische Algorithmus zur Optimierung der binären Autokorrelations-Funktion*, Diplomarbeit, Rheinische Friedrich-Wilhelms-Universität Bonn, 1993.

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