ELEMENTARY AND ANALYTIC THEORY OF NUMBERS
BANACH CENTER PUBLICATIONS, VOLUME 17
PWN POLISH SCIENTIFIC PUBLISHERS
WARSAW 1985

DIRICHLET POLYNOMIALS

M. N. HUXLEY

Department of Pure Mathematics, University College
Cardiff, Great Britain

1. Elementary theory.

Montgomery's philosophy, for which he won the Salem Prize, is to view n^{it} as an analogue of $e(nx)$. I. M. Vinogradov invented the Method of Trigonometric Sums, and Montgomery's analogues are the Dirichlet Polynomials, which I shall take as

$$F(s, \chi) = \sum_{N+1}^{2N} \frac{a(n)\chi(n)}{n^s}, \qquad s = \sigma + it,\ \sigma \geqslant 0.$$

There are two big differences between Dirichlet and trigonometric polynomials. The first is that if you multiply two trigonometric polynomials of length N, you get a trigonometric polynomial of length $2N$, with large coefficients. If you multiply two Dirichlet polynomials of length N, you get a Dirichlet polynomial of length at least N^2. The second difference is that a trigonometric polynomial with all coefficients one is known exactly, and is usually small. A Dirichlet polynomial with all coefficients one is a partial sum of the zeta function or the Dirichlet L-function, and so is rather mysterious. In fact we have three related topics

$$\begin{tikzcd} & \text{Bounds for } \zeta(s) \text{ and } L(s,\chi) \\ \text{Dirichlet polynomials} \arrow[ur] \arrow[dr] & \\ & \text{Zeros of } \zeta(s) \text{ and } L(s,\chi) \arrow[uu] \end{tikzcd}$$

In Vinogradov's method one proves that a trigonometric sum is small on the minor arcs, and the major arcs correspond to rationals a/q with small denominator. For Dirichlet polynomials we have no explicit major arcs, so that the theorems take the form

$$|F(s, \chi)| \leqslant V \text{ except on a set of cardinality } \leqslant R.$$

From another point of view we do have major arcs — the values of t for which $\zeta(\sigma+it)=0$, or $L(\sigma+it,\chi)=0$ with σ close to one.

To discuss the main ideas we need some more notation. There are two useful norms you can put on the coefficients

$$G(F)=\sum_{N+1}^{2N}|a(n)|^2, \qquad A(F)=\max|a(n)|,$$

so that

$$G \leqslant A^2 N.$$

Note how these behave under products:

$$A(F_1F_2) \leqslant A(F_1)A(F_2) \max_{N^2<n\leqslant 4N^2} d(n),$$

$$G(F_1F_2) \leqslant G(F_1)G(F_2) \max_{N^2<n\leqslant 4N^2} d(n).$$

It is very convenient to use an extended Vinogradov notation

$$f(x_1,\ldots,x_n) \lll g(x_1,\ldots,x_n)$$

to mean

$$f(x_1,\ldots,x_n)=O\big(g(x_1,\ldots,x_n)(x_1\ldots x_n)^{\varepsilon}\big)$$

so that the notation swallows up divisor functions and powers of logarithms, and we may write

$$A(F_1F_2) \lll A(F_1)A(F_2),$$

$$G(F_1F_2) \lll G(F_1)G(F_2).$$

Next we need a name for the exceptional set. Let U be a set of pairs (s,χ) where $s=\sigma+it$, $0\leqslant\sigma\leqslant 1/4$. The *difference set of* U is the set of pairs $(\bar{s}+s', \bar{\chi}\chi')$, counted according to multiplicity; we write it U^2. It arises naturally if we take the modulus squared of a sum over U. The main lemmas will require that U be well spaced in a region of size D, given by $|t|\leqslant T$, the modulus q of χ satisfies $q_0|q$ and $q\leqslant Q$. Here

$$D=Q^2T/q_0.$$

Well-spaced means

$$|t-t'|\geqslant 1 \quad \text{if} \quad \bar{\chi}\chi' \text{ is a principal character.}$$

Let R be the number of pairs in U. If U is well spaced, $R \ll D$. We want relations between R and V, where

$$V=V(F,U)=\min_U |F(s,\chi)|.$$

We often use the means

$$E_k(F, U) = \sum_U |F(s, \chi)|^k$$

usually with $k = 1$ or 2. If we can find a constant $B = B_k(M, U)$ with $E_k(F, U) \leqslant G^{k/2} B$ for $2N \leqslant M$ then

$$R \leqslant (G/V^2)^{k/2} B.$$

Similarly, if we can find a constant $B^* = B_k^*(M, U)$ with $E_k(F, U) \leqslant A^k N^{k/2} B^*$ for $2N \leqslant M$ then

$$R \leqslant (A^2 N/V^2)^{k/2} B^*.$$

So the general programme is to find the constants B and B^* as functions of M and U. There are some fairly trivial bounds

$$R \leqslant B_k(M, U) \leqslant R(\tfrac{1}{2}M)^{k/2},$$

$$(\tfrac{1}{2}M - 1)^{k/2} \leqslant B_k^*(M, U) \leqslant B_k(M, U),$$

and

$$B_k^*(M, U) \geqslant R \quad \text{for} \quad k \geqslant 2.$$

The large sieve theorem of Montgomery gives a nice bound.

THEOREM. *If U is pure (that means either $q_0 = Q$ or each χ is primitive) and well spaced, then*

$$B_2(M, U) \ll D + M.$$

The proof is basically just working out the mean square of an integral. In his book Montgomery makes two nice conjectures.

MEAN VALUES CONJECTURE:

$$B_k(M, U) \lll D + M^{k/2},$$

LARGE VALUES CONJECTURE:

$$B_2^*(M, U) \lll R + M.$$

He actually states the Large Values Conjecture with B^2 in place of B_2^*, but Heath-Brown has pointed out that this bound cannot be true for B_2 if $Q > 1$. The large sieve theorem is best possible if $M \gg D$ or if $R \gg D$.

Some easy comments.

Dissection. If U is the union of sets U_i,

$$B_k(M, U) \leqslant \sum B_k(M, U_i),$$

and in particular

$$B_k(M, U^2) \leqslant RB_k(M, U).$$

This was an essential trick in the first proof of the exponent 7/12 for gaps between prime numbers.

Changing k. If $j \geqslant 1$, $k > 1$

$$B_j(M, U) \leqslant R^{1-1/k}\{B_{jk}(M, U)\}^{1/k},$$
$$B_{jk}(M, U) \lll \max_{U' \subseteq U} R^{1-k}\{B_j(M, U')\}^k,$$

and if k is an integer

$$B_{jk}(M, U) \lll B_j(M^k, U).$$

These elementary relations also hold for B^*.

A big nuisance is that there is no useful peak function like the Fejér kernel in Fourier theory. The best that one can do is the following result.

Peak Function Lemma. *Given a particular* $F(s, \chi)$ *with* $V = V(F, U)$

$$B_k(M, U) \lll (G/V^2)^{ck/2} B_k(MN^c, U)$$

for any positive integer $c \geqslant 1$.

For the proof we suppose that $F_1(s, \chi)$ attains the maximum in the definition of $B_k(M, U)$, and then use

$$E_k(F_1 F^c, U) \geqslant V^{ck} E_k(F, U).$$

A related lemma was proved by Heath-Brown, who happened to need it at the time.

Localisation Lemma. *Given* M *and* U, *there is an* $F(s, \chi)$ *with* $N \geqslant M$ *for which*

$$E_2(F, U) \ggg GB_2(M, U).$$

Again we suppose that $F_1(s, \chi)$ attains the maximum. If it is too short, we multiply by a sum $\sum c(p)/p^s$ over primes in an interval, and average the coefficients $c(p)$ round the unit circle.

The concept that brings the zeta function to the centre of things is that of a Halász majorant.

$$H(s, \chi) = \sum_1^\infty \frac{h(n)\chi(n)}{n^s}$$

is a *Halász majorant* for $N_1 \leqslant n \leqslant N_2$, $H(N_1, N_2)$ if $h(n) \geqslant 0$ for all n, $h(n) \geqslant 1$ for $N_1 \leqslant n \leqslant N_2$, and $\sum_1^\infty h(n)$ converges.

Halász Lemma. *Let* $H(s, \chi)$ *be an* $H(N, 2N)$ *majorant. Then*

$$\{E_1(F, U)\}^2 \leqslant GE_1(H, U^2).$$

COROLLARY. $B_1^2(M, U) \leqslant M^{1/2} B_1^*(M, U^2)$.

Proof. Let $\eta(s, \chi)$ be a complex number of unit modulus and the same argument as $F(s, \chi)$. Write

$$E_1(F, U) = \sum_U |F(s, \chi)| = \sum_U \bar{\eta}(s, \chi) F(s, \chi) = \sum_n a(n) \sum_U \bar{\eta}(s, \chi) \frac{\chi(n)}{n^s}.$$

Applying Cauchy's inequality, we see that the left-hand side of the lemma is

$$\leqslant G \sum_{N+1}^{2N} \left| \sum_U \bar{\eta}(s, \chi) \frac{\chi(n)}{n^s} \right|^2 \leqslant G \sum_1^{\infty} h(n) \left| \sum_U \bar{\eta}(s, \chi) \frac{\chi(n)}{n^s} \right|^2$$

$$= G \sum_{(s, \chi) \in U} \eta(s, \chi) \sum_{(s', \chi') \in U} \bar{\eta}(s', \chi') \sum_{n=1}^{\infty} \frac{h(n) \overline{\chi(n)} \chi'(n)}{n^{\bar{s}+s'}},$$

which gives the result.

This lemma explains why difference sets are important. The best choices one has for Halász majorants are partial sums of the zeta function and Dirichlet L functions. Since we want bounds in terms of R and D which measure the size of U, there will be some sets U which are worse than others. In the bounds we have, the worst sets U on which to estimate B would be the pairs (it, χ) for which $L(s, \chi)$ has a zero $\beta + it$ with β close to 1. This would not matter if we could construct useful Halász majorants without using the zeta function. At one time I thought that the Rankin Dirichlet series associated with modular forms and Maass forms could be used, but Shimura and Zagier have proved that every zero of $\zeta(s)$ is a zero of these functions also.

Jutila has proved a lemma related to Halász's.

JUTILA'S DIFFERENCE SET LEMMA. *Let $H(s, \chi)$ be an $H(N^k, 2^k N^k)$ majorant. Then*

$$E_{2k}(F, U^2) \lll A^{2k} E_2(H, U^2).$$

This lemma says more than just

$$B_{2k}^*(M, U^2) \lll B_2(M^k, U^2)$$

since on the right there stands an arbitrary Halász majorant, and we have more control.

2. Involving the zeta and L-functions

First we introduce a concept: the flat set $U^{(1)}$ is the projection of U onto $\sigma = 0$, consisting of pairs (it, χ) corresponding to the pairs (s, χ) of U.

A contour integral gives

$$B_k(M, U) \ll B_k(M, U^{(1)}),$$

and if $0 \leqslant \sigma \leqslant 1/\log MR$ for each (s, χ) in U, the converse is true,

$$B_k(M, U^{(1)}) \ll B_k(M, U).$$

We write $U^{(2)}$ for the flat set corresponding to the difference set U^2. Montgomery was very fond of this majorant:

$$\begin{aligned} H(s, \chi) &= \sum_1^{\infty} \frac{\chi(n)\, e^{2-n/N}}{n^s} \\ &= \frac{e^2}{2\pi i} \int\limits_{\mathrm{Re}(s+w)=1/2} L(s+w, \chi)\, \Gamma(w)\, N^w\, dw + \varepsilon(\chi)\, e^2\, \Gamma(1-s)\, N^{1-s}, \end{aligned}$$

where $\varepsilon(\chi)$ is $\varphi(q)/q$ if χ is a principal character to some modulus q; otherwise $\varepsilon(\chi)$ is zero. This gives

$$E_k(H, U) \ll N^k + N^{k/2} \int_{-\infty}^{\infty} \sum_{U^{(1)}} |L(s+\tfrac{1}{2}+i\tau, \chi)|^k\, |\Gamma(\tfrac{1}{2}+i\tau)|^k\, d\tau,$$

$$E_k(H, U^2) \ll RN^k + N^{k/2} \int_{-\infty}^{\infty} \sum_{U^{(2)}} |L(s+\tfrac{1}{2}+i\tau, \chi)|^k\, |\Gamma(\tfrac{1}{2}+i\tau)|^k\, d\tau.$$

There are many treatments possible, taking the integral to any convenient region where we know a good bound for $L(s, \chi)$. My opinion now is that this is a time-waster. However, if you want to play this game you will find Littlewood's lemma useful.

Lemma (usually called 'Riemann hypothesis implies Lindelöf').

$$L(s, \chi) \ll (q(|t|+e))^{\varepsilon}$$

unless there is a zero $\beta + i\gamma$ *of* $L(s, \chi)$ *with*

$$\beta > \sigma - \frac{c}{\log l}, \quad |\gamma - t| \leqslant l^2 \quad (l = \log q(|t|+e)).$$

This lemma provides the connection between zeros and bounds mentioned in the first section.

When U is well spaced one treatment (Montgomery again) is to take the integrals back to $\mathrm{Re}(s+w) = 0$, which gives

$$B_2(M, U) \ll M + RD^{1/2}.$$

In my paper *Large values of Dirichlet polynomials I* I had an iteration starting from a non-trivial bound, and I used this bound. Ramachandra pointed out that it was always better to start the iteration from the large sieve bound

$$B_2(M, U) \ll M+D.$$

The moral is that the most difficult result may not be the strongest.

The next lemma began as a proof of an approximate functional equation, suggested by Montgomery and worked out in my thesis. It was simplified in *Large values of Dirichlet polynomials I* and was stated explicitly by Ramachandra.

FOURTH POWER MOMENT. *If U is well-spaced and flat, $|\tau| \leqslant T$ and $k \geqslant 1$*

$$\sum_{(s,\chi)\in U} |L(s+\tfrac{1}{2}+i\tau, \chi)|^k \lll B_k^*(D^{1/2}, U),$$

and similarly for U^2.

The proof sketched here follows Jutila's simple version. We use a fearsome Halász majorant – strictly it is $eH(s, \chi)$ which is an $H(1, M)$ majorant – given by

$$\begin{aligned} H(u, \chi) &= \sum_1^\infty \frac{\chi(n)}{n^u} \exp\left(-\frac{n^g}{M^g}\right) \\ &= L(u, \chi)+\varepsilon(\chi)\Gamma\left(1+\frac{1-u}{g}\right)\frac{M^{1-u}}{1-u}+ \\ &\qquad + \frac{1}{2\pi i}\int_{\mathrm{Re}\, w=-g/2} L(u+w, \chi)\Gamma\left(1+\frac{w}{g}\right)\frac{M^w}{w}\,dw. \end{aligned}$$

For the fourth power moment we take

$$g = l^2, \quad \text{where } l = \log D; \quad M = \tfrac{1}{2}D^{1/2}; \quad \mathrm{Re}\, u = \tfrac{1}{2}.$$

We use this to estimate $|L(u, \chi)|^k$. The terms in $H(u, \chi)$ with $n > 3M/2$ are negligible, so the sum over $|H|^k$ is bounded by B_k^* as claimed, and so is the $\varepsilon(\chi)$ term.

In the integral we put $v = 1-w$, and use the functional equation

$$L(1+u-v, \chi) = (f/\pi)^{v-u-1/2}G(v-u)J(v-u)L(v-u, \bar{\chi})$$

where f is the conductor of the character χ, G is the gamma-function factor, and J is the finite product over the primes that divide q but not f which is needed to compensate for χ not being a primitive character. Now

$$\mathrm{Re}\,(v-u) = \tfrac{1}{2}(g+1),$$

safely within the convergence region. Let M' be the greatest even integer with $M' \leqslant D^{1/2}$, and write

$$L(u-z, \bar{\chi}) = \sum_1^{M'} \frac{\bar{\chi}(n)}{n^{u-z}} + \sum_{M'+1}^{\infty} \frac{\bar{\chi}(n)}{n^{u-z}}.$$

The sum from $M'+1$ to infinity turns out to be quite negligible. We move the integral over the first N terms back to $\operatorname{Re} v = 1+1/\log D$ (the extra $1/\log D$ avoids a pole at $w=0$), and the sum can again be estimated by $B_k^*(D^{1/2}, U)$. Since

$$B_4^*(D^{1/2}, U) \lll B_2^*(D, U) \leqslant B_2(D, U) \ll D$$

by the Large Sieve, the case $k=4$ gives the fourth power moment of $L(s, \chi)$ in a discrete notation.

A slight modification of the proof of the fourth power moment gives a result that looks very different. Instead of $M = \frac{1}{2} D^{1/2}$, write down $H(u, \chi)$ with $M = 2N$ and $M = N$ and subtract. The term in $L(u, \chi)$ on the right cancels out. The series on the left gives an $H(N, 2N)$ majorant when we multiply it by a constant. The integral is treated in the same way, with $M' = D/N$. The $\varepsilon(\chi)$ term is negligible unless χ is principal and t is small.

INVERSION LEMMA. *Let $N \leqslant D$, and let U be well spaced. There is an $H(N, 2N)$ series with*

$$H(s, \chi) \lll N^{1/2} \int_{-l^4}^{l^4} \Big|\sum_{1}^{D/N} \bar{\chi}(n) n^{-1/2+it-i\tau}\Big| d\tau + 1$$

for all (s, χ) in U^2 except those with χ principal and $|t| \leqslant l^4$.

I used to call this the Reflection Lemma, but there is an analogy with van der Corput's method of estimating exponential sums, with Lemma A corresponding to our Inversion Lemma, Lemma B corresponding to Halász's Lemma to give

$$(B_1(M, U))^2 \ll MR + R^2 + M^{1/2} B_1^*(D/M, U^2).$$

We use this to obtain my bound for the exceptional set.

THEOREM. *If U is pure and well spaced, and $V = V(F, U)$, then*

$$R \lll \frac{GN}{V^2} + \frac{G^3}{V^6} DN.$$

Proof. The case $N \geqslant D$ follows from the Large Sieve. Suppose for simplicity that U is flat. By Halász's Lemma and inversion

$$R^2 V^2 \leqslant \{E_1(F, U)\}^2 \leqslant GE_1(H, U^2) \lll GRN + GR^2 + GN^{1/2} B_1^*(D/N, U^2).$$

If either of the first two terms is the largest, the result follows. If the third term is the largest,

$$\frac{R^2 V^2}{GN^{1/2}} \lll B_1^*(D/N, U^2) \lll RB_1^*(D/N, U) \qquad \text{(dissection)}$$

$$\lll R^{3/2} \{B_2^*(D/N, U)\}^{1/2} \qquad \text{(Hölder)},$$

so that

$$\frac{RV^4}{G^2 N} \lll B_2^*(D/N, U) \lll B_2(D/N, U)$$

$$\lll \frac{G}{V^2} B_2(D, U) \qquad \text{(peak functions)}$$

$$\lll \frac{GD}{V^2} \qquad \text{(large sieve).}$$

Heath-Brown has used the Inversion Lemma to show that for $M \gg D^{2/3+\varepsilon}$ (constant depending on ε)

$$B_2^*(M, U^2) \lll MR + R^2,$$

a best possible result. This implies the Large Values Conjecture for the special case when U is an arithmetic progression.

At the other extreme, if U forms what Professor Erdős has called an S^k-sequence, we may combine Halász's lemma and the large sieve. An S^k-sequence is one in which each non zero difference occurs at most k times. With little loss of generality the pairs of U are of the form (it, χ) where t is an integer. If U is well spaced, so is the set U' formed from the distinct members of U^2. In Halász's lemma we have

$$\{E_1(F, U)\}^2 \leqslant GE_1(H, U^2) \ll GRN + kGE_1(H, U').$$

By Hölder and the large sieve, for $N \leqslant D$

$$\{E_1(H, U')\}^2 \leqslant \min(R^2, D) E_2(H, U') \ll ND \min(R^2, D)$$

and

$$R \ll \frac{GN}{V^2} + \left(\frac{GN}{V^2}\right)^{1/2} k^{1/2} D.$$

What we now need is a combinatorial method to fill the gap between an arithmetic progression and a negative Sidon sequence.

References

The subject is first set out in:

H. L. Montgomery, *Topics in multiplicative number theory*, Springer Lecture Notes 227, Berlin 1971.

Most of the ideas of earlier papers are summarised in:

M. N. Huxley and M. Jutila, *Large values of Dirichlet polynomials IV*, Acta Arith. 32 (1977), 297–312.

Other important papers:

M. Forti and C. Viola, *Density estimates for the zeros of L-functions*, Acta Arith. 23 (1973), 379–391.

K. Ramachandra, *A simple proof of the mean fourth power estimate for the Riemann zeta function*, Ann. Scuola Norm. Sup. Pisa 1 (1974), 81–97.

D. R. Heath-Brown, *A large values estimate for Dirichlet polynomials*, J. London Math. Soc. 20 (1979), 8–18.

H. Iwaniec, *On mean values for Dirichlet polynomials and the Riemann zeta function*, ibid. 22 (1980), 39–45.

A. Ivić, *Topics in recent zeta function theory*, to appear.

There are many papers by the authors above applying these ideas to zeros of the zeta function and L-functions. Heath-Brown and Ivić have many new bounds for the zeta function which can be used to estimate Halász majorants.

Presented to the Semester
Elementary and Analytic Theory of Numbers
September 1–November 13, 1982