Course Notes

Part VI

Probabilistic Combinatorics

and

Algorithms

J. A. Verstraete
Department of Mathematics
University of California San Diego
9500 Gilman Drive
La Jolla California 92037-0112

jacques@ucsd.edu
9 The Hardy-Littlewood Method

The Hardy-Littlewood circle method is an analytic technique for estimating coefficients of certain types of generating functions. Successful applications include

- The asymptotic formula for the partition function $P(n)$.
- Vinogradov’s Three Primes Theorem – every large enough odd integer is a sum of three prime numbers.
- An asymptotic formula for the number of ways of representing an integer as a sum of $s$ squares when $s$ is large.
- Proving that for certain polynomials $f \in \mathbb{Z}[X]$, any set $A \subset \mathbb{Z}$ has density zero if $V_f \cap (A - A) = \emptyset$.

Here $V_f = \{ f(x) : x \in \mathbb{Z} \}$. We have listed a few applications here, but there are many more.

9.1 Cauchy’s Formula

In a typical situation, let $\phi(z) := \sum_{n=0}^{\infty} a_n z^n$ be a generating function which is analytic on a region containing the disk $|z| \leq \delta$ in its interior, where $\delta \in (0, 1)$, and let $\gamma$ be the circle $|z| = \delta$. Cauchy’s Integral Formula states that for any $a \in \text{int}\gamma$,

$$\phi^{(n)}(a) = \frac{n!}{2\pi i} \int_{\gamma} \frac{\phi(z)}{(z-a)^{n+1}} dz.$$  

Since $a_n = n! \phi^{(n)}(0)$, we recover $a_n$ from the line integral

$$a_n = \frac{1}{2\pi i} \int_{\gamma} \frac{\phi(z)}{z^{n+1}} dz.$$  

As a simple example, let $a_n$ denote the number of ways to write an integer $n$ as an ordered sum of $r$ positive odd integers. Then the generating function is

$$\phi(z) = \left( \frac{z}{1 - z^2} \right)^r$$

and for any $\delta < 1$ we have

$$a_n = \frac{1}{2\pi i} \int_{|z| = \delta} \frac{z^{r-n-1}}{(1 - z^2)^r} dz.$$  

By the binomial theorem,

$$a_n = \frac{1}{2\pi i} \int_{|z| = \delta} \sum_{s=0}^{\infty} \binom{r + s - 1}{r - 1} z^{r+2s-n-1} dz.$$  

Replacing $z$ with $\delta e^{2\pi i \alpha}$ we obtain

$$a_n = \int_0^1 \sum_{s=0}^{\infty} \binom{r + s - 1}{r - 1} \delta^{r+2s-n} e^{2\pi i (r+2s-n)} d\alpha.$$
For $\delta < 1$, we can interchange the integration and the summation and since $e^{\alpha(r+2s-n)}$ is analytic the only term which survives is that corresponding to $2s = n - r$. In this case, if $n - r$ is even, we obtain

$$a_n = \left( \frac{n+r-2}{2} \right).$$

This completes the example: note that the value of $\delta$ did not explicitly enter the calculations.

In general, we would like to take $\delta \uparrow 1$, but $\phi(z)$ has singularities on the circle $|z| = 1$. The heart of the circle method is to deal with these singularities in the following way. We replace $\phi(z)$ with a truncated generating function $\phi_N(z) := \sum_{n=0}^{N} a_n z^n$. This has no effect on $a_n$ when $N \geq n$, and has the advantage of being a polynomial which is analytic on $|z| = 1$.

Therefore we make the change of variable $z = e^{2\pi\alpha i} = \omega^\alpha$ as in the above example, and we can rewrite the circle integral as a Riemann integral of exponential sums as follows:

**Lemma 1** Let $n, N \in \mathbb{N}$ and $N \geq n$. Then

$$a_n = \int_0^1 \phi_N(\omega^\alpha) \omega^{-n\alpha} d\alpha$$

where $\phi_N$ is the truncated generating function for $\{a_n\}_{n \in \mathbb{N}}$.

One requires a good understanding of the behaviour of $\phi_N(z)$ near singularities of $\phi(z)$ to find good estimates for the integral above. This is the main machinery of the Hardy-Littlewood method: it is the case that $|\phi_N(z)|$ is large near singularities of $\phi(z)$ and small otherwise, so we partition the circle $|z| = 1$ into small intervals around the singularities of $\phi$ and the remaining intervals which are separated from the singularities of $\phi$. The first set of intervals is traditionally called the set of major arcs, while the second is the set of minor arcs. For example, when $\phi(z) = z^r(1-z^2)^{-r}$ the singularities of $\phi$ are $z = 1$ and $z = -1$. so the major arcs would consist of small intervals on the circle of $|z| = 1$ centred at $z = 1$ and $z = -1$ in the complex plane. If $z$ is not close to these values, then it is not hard to see that the integral is relatively small – this is the contribution of the minor arcs. However, it is often this part that is difficult, because the measure of minor arcs on the circle $|z| = 1$ is close to 1. It is also the case that the major arcs have to be chosen carefully: the size of the neighbourhood of the singularities of $\phi(z)$ which constitute the major arcs depends very much on the nature of the problem, and generally they depend on $n$ when we are estimating $a_n$.

We consider another example: let $P(n)$ denote the number of ways of writing a positive integer $n$ as an unordered sum of other positive integers. Clearly $P(1) = 1$, $P(2) = 2$, $P(3) = 3$ and $P(4) = 5$, but an explicit formula for $P(n)$ is highly unlikely, and even the order of magnitude of $P(n)$ is non-trivial – this was the first application of the Hardy-Littlewood method. Consider the generating function for $P(n)$, which is given explicitly by

$$\phi(z) = \prod_{i=1}^{\infty} \frac{1}{1-x^i}.$$

We truncate the sum at some large integer $N$ to get the generating function $\phi_N(z)$. According to the Hardy-Littlewood method,

$$P(n) = \frac{1}{2\pi i} \int_{|z|=1} \frac{\phi_N(z)}{z^{n+1}} dz.$$
Now $\phi(z)$ is not defined when $z = \zeta^\alpha$ and $\alpha$ is a rational number. With $n$ as an input, the really large contribution is from those rational $\alpha$ with a small denominator. The major arcs will therefore consist of small intervals around rational numbers with small denominators; the minor arcs are everything else. In order to estimate these contributions, we are left with attempting to estimate exponential sums. The main types of exponential sums we are interested in are sums of the form $\sum_{x \in I} \omega^{f(x)}$ where $f$ is a polynomial and $I$ is a set of consecutive integers. A general observation is that the sum is large when $x$ is close to a rational number with a small denominator, and the sum is small otherwise. We shall see that Weyl’s criterion for such exponential sums to be small is precisely that the numbers $f(n) - \lfloor f(n) \rfloor$ cover the unit interval $[0, 1]$ in a uniform sort of way. We shall make this precise in our study of exponential sums.

9.2 Dirichlet’s Box Principle

The following result is known as Dirichlet’s Box Principle, which gives a quantitative bound on how well a real number can be approximated by a rational number with a bounded denominator $q$.

**Theorem 2** Let $\alpha, a$ be real numbers. Then, there exists a rational number $p/q$ with $(p, q) = 1$, $1 \leq q \leq a$, and $|\alpha - p/q| \leq (qa)^{-1}$.

**Proof** The condition $(p, q) = 1$ adds no restriction on the theorem. Let $a' = \lfloor a \rfloor$. The real numbers $a_q = \alpha q - \lfloor \alpha q \rfloor$ lie in $[0, 1)$ for $q = 1, 2, .., a'$. Consider the partition of $[0, 1)$ with elements

$$I_r = \left[ \frac{r-1}{a'+1}, \frac{r}{a'+1} \right)$$

for $r = 1, 2, .., a' + 1$. If $a_q$ lies in $I_1$ or $I_{a'+1}$, then the theorem is proved, since

$$|\alpha q - q(\lfloor \alpha q \rfloor + 1)| \leq \frac{1}{a'+1} \leq \frac{1}{a}.$$

Otherwise, there exists an $I_r$ for some $2 \leq r \leq a'$ such that two of the reals $a_q$ lie in $I_r$, say $a_i$ and $a_j$, $i < j$. Setting $q' = j - i$ and

$$p = |\alpha j| - |\alpha i|$$

proves $|\alpha - p/q'| \leq (q'a)^{-1}$ as required.

9.3 Exponential Sums

An exponential sum is a sum of the form $S_I(f) = \sum_{x \in I} e^{2\pi if(x)}$ where $f$ is a real-valued function on $I$. If $\alpha$ is any real number, then $||\alpha||$ denotes the distance from $\alpha$ to the nearest integer. In what follows, $I$ always denotes a sub-interval of the natural numbers. If $I = \{a, a+1, \ldots, b\}$, then denote by $I^*$ the interval $\{x \in \mathbb{R} : a \leq x \leq b\}$. We begin with a general inequality which is a special case of the Kusmin-Landau inequality.
Theorem 3 Let \( f \) be a function with continuous monotonic first derivative on \( I^* \) satisfying \( \|f'(x)\| \geq \lambda > 0 \) for \( x \in I \). Then
\[
\left| \sum_{x \in I} e^{2 \pi i f(x)} \right| \ll \lambda^{-1}.
\]

Proof ▶ Replacing \( f \) with \(-f\) has no effect on the inequality. So, suppose that \( f' \) is increasing. Also, since \( \|f'(x)\| \geq \lambda \) for \( x \in I \), and \( f \) has continuous monotonic first derivative on \( I^* \), we know there exists an integer \( k \), which does not depend on \( x \), such that \( k + \lambda \leq f'(x) \leq k + 1 - \lambda \) for all \( x \in I \). However, the sum in the theorem is invariant under the replacement \( f(x) \mapsto f(x) - kx \). Therefore, we may assume that \( f'(x) \in [\lambda, 1 - \lambda] \) for \( x \in I \). Let \( g(x) = f(x + 1) - f(x) \). By straightforward application of the mean value theorem, there exists \( m_x \) such that \( x \leq m_x \leq x + 1 \) with \( g(x) = f'(m_x) \). Since \( f' \) is monotonic, \( g \) is monotonic and also satisfies \( g(x) \in [\lambda, 1 - \lambda] \). We may rewrite the summand so that it involves \( g(x) \):
\[
e^{2 \pi i f(x)} = \frac{e^{2 \pi i f(x)} - e^{2 \pi i f(x + 1)}}{1 - e^{2 \pi i g(x)}} = h(x) \left( e^{2 \pi i f(x)} - e^{2 \pi i f(x + 1)} \right)
\]
where \( h(x) = \frac{1}{2}(1 + \cot \pi x) \). Suppose that \( I = (a, b) \) for some integers \( a \) and \( b \). Substituting the above for the summand \( e^{2 \pi i f(x)} \), we obtain:
\[
\sum_{I} e^{2 \pi i f(x)} = \sum_{[a + 1, b - 1]} \left( e^{2 \pi i f(x)} - e^{2 \pi i f(x + 1)} \right) h(x) + e^{2 \pi i f(b)}
\]
\[
= \sum_{[a + 2, b - 1]} e^{2 \pi i f(x)}(h(x) - h(x - 1)) + e^{2 \pi i f(a + 1)}h(a + 1) + e^{2 \pi i f(b)}(1 - h(b - 1)).
\]
Taking moduli on both sides, we find:
\[
\left| \sum_{I} e^{2 \pi i f(x)} \right| \leq \frac{1}{2} \sum_{[a + 1, b - 1]} |h(x - 1) - h(x)| + |h(a + 1)| + |1 - h(b - 1)|
\]
\[
\leq \frac{1}{2}|h(a + 1) - h(b - 1)| + |h(a + 1)| + |1 - h(b - 1)|
\]
where we note that the sum on the first line telescopes since \( h(x - 1) - h(x) \) is of constant sign. The theorem is proved in noting that \( |\cot(\pi x)| \ll 1/x \) whenever \( 0 \leq x \leq 1/2 \).
\]

Proposition 4 Let \( I \) be an integer interval, and let \( f \) be a function with two continuous derivatives on interval \( I^* \). Suppose there exists \( \lambda > 0 \) and \( \kappa \geq 1 \) such that \( \lambda \leq |f''(n)| \leq \kappa \lambda \) on \( I \). Then
\[
\left| \sum_{x \in I} e^{2 \pi i f(x)} \right| \ll \kappa |I| \lambda^{1/2} + \lambda^{-1/2}.
\]

Proof ▶ For any positive real number \( \delta \lambda < \delta < 1/2 \), after a bit of thought using the bounds on \( |f''(n)| \), we can split \( I \) into at most \( \kappa |I| \lambda + 2 \) intervals on which \( \|f''\| \geq \delta \) and at most \( \kappa |I| \lambda + 1 \) other intervals each of length at most \( 2 \delta / \lambda \). To the former set of intervals, apply Theorem 3 and to the latter set of intervals apply the trivial estimate to obtain:
\[
\sum_{I} e^{2 \pi i f(x)} \ll (\kappa |I| \lambda + 1)(1/\delta + \delta/\lambda + 1).
\]
Now choose $\delta = \lambda^{1/2}$ to prove the required result for $\lambda \leq 1/4$. If $\lambda > 1/4$, the trivial estimate gives the result.

The theorem and proposition above may be generalized to arbitrary derivatives, in the form of the following theorem, which we do not prove:

**Theorem 5** Let $r$ be a positive integer and $I$ an integer interval. Suppose that $f$ is a real-valued function with $r + 2$ continuous derivatives on interval $I^*$. In addition suppose that, for some $\lambda > 0$ and $\kappa \geq 1$, $\lambda \leq |f^{(r)}(x)| \leq \kappa \lambda$ on $I$. Then, with $R = 2^r$,

$$\sum_{x \in I} e^{2\pi if(x)} \ll |I|((\kappa^2 \lambda)^{1/(4R-2)} + |I|^{1-1/2R} \kappa^{1/2R} + |I|^{1-1/2R+1/R^2} \lambda^{-1/2R})$$

We will be particularly interested in what follows in the case of exponential sums $S_I(f)$ when $f$ is a polynomial – these are called Weyl sums – and in these cases we obtain finer estimates than the general ones presented above.

### 9.4 Linear Exponential Sums

The most basic form of exponential sum is when $f$ is linear – $f(x) = \alpha x + \beta$. In this case, $\|\alpha\|$ enters explicitly into the bounds. This result will be the basis for estimating exponential sums $S_I(f)$ when $f$ is a polynomial of degree more than two – such sums are often called Gauss sums when $f$ is quadratic and Weyl sums when $f$ is a general polynomial.

**Lemma 6** Let $\alpha, \beta$ be real numbers. Then

$$\sum_{x \in I} e^{2\pi i(\alpha x + \beta)} \leq \min\left\{\frac{1}{2\|\alpha\|}, |I|\right\}.$$ 

**Proof** The constant $\beta$ does not affect the inequality. If $\alpha = 0$, then the sum is $|I|$. Suppose $\alpha \neq 0$ and $I = [a, b]$. Then the sum is precisely:

$$s = \frac{e^{2\pi i\alpha a} (1 - e^{2\pi i\alpha(b-a+1)})}{1 - e^{2\pi i\alpha}}.$$ 

Since $\sin(z) = \frac{1}{2i} (e^z - e^{-z})$,

$$|s| = \left|\frac{e^{2\pi i\alpha b} - e^{2\pi i\alpha a}}{e^{2\pi i\alpha} - 1}\right| \leq |\sin \pi \alpha|^{-1}.$$ 

Since $|\sin \pi \alpha| \geq 2\|\alpha\|$, the result follows.

In the next section, we will develop the inductive machinery for passing from linear exponential sums to polynomial exponential sums.
9.5 Finite differences

For any function \( f \), and real numbers \( x_1, \ldots, x_k, k \geq 1 \), we define a finite difference of the \( k \)th order, \( \Delta_{x_1, \ldots, x_k} \) as follows: let \( \Delta_{x_1} f(x) = f(x+x_1) - f(x) \), and \( \Delta_{x_1, \ldots, x_k} = \Delta_{x_k} (\Delta_{x_1, \ldots, x_{k-1}} f(x)) \).

The following basic lemma is left as an exercise:

**Lemma 7** If \( f(x) = \alpha_1 x^r + \cdots \alpha_1 x + \alpha_0 \) and \( r \geq 2 \), then

\[
\Delta_{x_1, \ldots, x_{r-1}} f(x) = r! \alpha_r x^r \cdots x_{r-1} x + \beta
\]

where \( \beta \) is dependent only on \( \alpha_0, \ldots, \alpha_r \) and \( x_1, \ldots, x_{r-1} \).

The main inductive step in estimating Weyl sums \( S_I(f) \) when \( f \) has degree at least two is the following lemma:

**Lemma 8** For \( k \geq 1 \),

\[
\left| \sum_{x=1}^{n} e^{2\pi i f(x)} \right|^{2^k} \leq 2^{2^k-1} n^{2^k-k-1} \sum_{x_1=0}^{n-k-1} \cdots \sum_{x_k=0}^{n-k-1} \sum_{x=1}^{n} e^{2\pi i \Delta_{x_1, \ldots, x_k} f(x)}
\]

where \( n_1 = n, n_{i+1} = n_i - x_i \) for \( i = 1, 2, \ldots, k \).

**Proof** Let \( k = 1 \). Then

\[
\left| \sum_{x=1}^{n_1} e^{2\pi i f(x)} \right|^2 = \sum_{x,y=1}^{n_1} e^{2\pi i (f(y)-f(x))} = n_1 + \sum_{x \neq y} e^{2\pi i (f(y)-f(x))}
\]

\[
= n_1 + \sum_{x < y} e^{2\pi i (f(y)-f(x))} + \sum_{x > y} e^{2\pi i (f(y)-f(x))}
\]

\[
\leq n_1 + 2 \sum_{x=1}^{n_1} \sum_{y=1}^{n_1-x} e^{2\pi i (f(x+y)-f(x))}
\]

\[
\leq 2 \sum_{y=0}^{n_1-1} \sum_{x=1}^{n_1-y} e^{2\pi i (f(x+y)-f(x))}
\]

\[
\leq 2 \sum_{x_1=0}^{n_1-1} \sum_{x=1}^{n_1-x_1} e^{2\pi i \Delta_{x_1} f(x)}
\]

where we have interchanged the order of summation and used the triangle inequality. Using the fundamental inequality \( (\sum_{x=1}^{n} r_x)^k \leq n^{k-1} \sum_{x=1}^{n} r_x^k \), valid for non-negative reals \( r_x \), we have:

\[
\left| \sum_{x=1}^{n_1} e^{2\pi i f(x)} \right|^{2^k} \leq 2^{2^k-1} n_1^{2^k-k-1} \sum_{x_1=1}^{n_1-1} \sum_{x=1}^{n_1-x_1} e^{2\pi i \Delta_{x_1} f(x)}
\]

Successively applying this inequality to the internal sum on the right hand side, we find:
\[
\sum_{x=1}^{n_k} e^{2\pi if(x)} \leq \left( \prod_{i=1}^{k} \frac{n_i^{2k-i} - 1}{n_i^{2k-i}} \right) \sum_{x_1=0}^{n_1-1} \cdots \sum_{x_k=0}^{n_k-1} \sum_{x=1}^{n_{k+1}} e^{2\pi i \Delta x_{x_1, x_2, \ldots, x_k} f(x)} \right)^{2^{k-1}}
\]

using the definition of \( \Delta x_{x_1, x_2, \ldots, x_k} \) and \( n_1, n_2, \ldots, n_{k+1} \). Since the product is at most \( 2^{2k-1} n^{2k-k-1} \), the proof is complete.

### 9.6 Weyl sums

In this section we estimate exponential sums \( S(f) \) when \( f \) is a polynomial of degree at least two. The method for estimating such Weyl sums is to reduce the degree and then use induction, starting with the case of linear exponential sums and using the lemma on finite differences. For exponential sums of very large degree, Vinogradov’s Mean Value Theorem is more effective, but we do not discuss this here.

Let \( f : \mathbb{N} \to \mathbb{R} \) be a function and write \( \{ f(x) \} := f(x) - \lfloor f(x) \rfloor \) for the fractional part of \( f(x) \). We say that \( f \) is uniformly distributed (or equidistributed mod 1) if for \( \alpha \in (0, 1] \),

\[
\lim_{n \to \infty} | \{ m \leq n : \{ f(m) \} < \alpha \} | = \alpha
\]

Weyl established that if \( f(x) \) is a polynomial that has at least one non-constant term with an irrational coefficient, then \( f \) is uniformly distributed. This theorem is proved using a fundamental inequality, known as Weyl’s Inequality, involving exponential sums. We shall prove this theorem with \( f(x) = \alpha x^k \): that is, the function \( f(x) = \alpha x^k \) is uniformly distributed. For instance, as a consequence, if \( \alpha \) is a real number then for any \( \varepsilon > 0 \) there exists \( N \) such that \( N^2 \alpha \) is at distance at most \( \varepsilon \) from an integer. Before proving these statements, we need some basic technical lemmas. The statements here are written for simplicity, rather than for finding optimal bounds.

**Lemma 9** Let \( m, r, Q \in \mathbb{N} \) with \( Q \geq 2 \) and \( m \leq r \). Let \( \theta_1, \theta_2, \ldots, \theta_m \) be real numbers with \( \| \theta_i - \theta_j \| \geq r^{-1} \) whenever \( i \neq j \). Then

\[
\sum_{i=1}^{m} \min\left\{ \frac{1}{\| \theta_i \|}, Q \right\} \leq 6 \log Q(Q + r).
\]

**Proof** By translating the \( \theta_i \) by integers and replacing \( \theta_i \) with \( 1 - \theta_i \) where necessary, we can assume \( \theta_i \in [-1/2, 1/2] \) for all \( i \). We may also assume the contribution \( S^+ \) to the sum from the non-negative \( \theta_i \) is at least one half of the total. Suppose the positive \( \theta_i \) are ordered:
0 ≤ θ_1 < θ_2 < ⋅⋅⋅ < θ_{k+1}. Then

\[ S^+ := \sum_{i=1}^{k+1} \min \left\{ \frac{1}{\| \theta_i \|}, Q \right\} = \sum_{i=1}^{k} \min \left\{ \frac{1}{\theta_i}, Q \right\} \]

\[ \leq \min \left\{ \frac{1}{\theta_1}, Q \right\} + \sum_{i=2}^{k+1} \min \left\{ \frac{r}{i-1}, Q \right\} \]

\[ \leq Q + \sum_{i=2}^{k+1} \min \left\{ \frac{r}{i-1}, Q \right\} \]

\[ = Q + \sum_{i=0}^{\lfloor r/Q \rfloor} Q + \sum_{i=[r/Q]+1}^{k+1} \frac{r}{i}. \]

Estimating the last term with logarithms,

\[ S^+ \leq (1 + r/Q)Q + 2r(\log k + \log Q - \log r) < Q + r + 2r \log Q \leq 3 \log Q(Q + r). \]

Here we used the fact that \( \log k < \log r \), which comes from \( k \frac{r}{\theta_k} \leq \frac{1}{2} \). Therefore the entire sum is at most \( 2S^+ \leq 6 \log Q(Q + r) \).

Lemma 10 Let \( Q, R \in \mathbb{N}, Q \geq 2, \) and \( \alpha \in \mathbb{R} \). Suppose that for some \( a, q \in \mathbb{N} \) with \((a, q) = 1\), we have \( |\alpha - a/q| \leq q^{-2} \). Then

\[ \sum_{x=0}^{R} \min \left\{ \frac{1}{\| \alpha x + \beta \|}, Q \right\} \leq 24 \log Q(Q + q + R + QR/q). \]

Proof We consider the cases \( R \leq q/2 \) and \( R > q/2 \) separately. If \( R \leq q/2 \), then we claim that the real numbers \( \theta_i = \beta + i\alpha \) for \( i = 1, 2, \ldots, R \) satisfy \( \| \theta_i - \theta_j \| \geq 1/2q \). To see this, note that

\[ \| (i - j)\alpha \| \geq \| (i - j) \frac{a}{q} \| + \frac{|i - j|}{q^2} \geq \frac{1}{q} - \frac{R}{q^2} \geq \frac{1}{2q} \]

as required. Note that we used the fact that \((i - j)a \equiv (i - j) \neq 0 \mod q \). Now we can apply Lemma 9 with \( r = 2q \) to obtain

\[ \sum_{x=0}^{R} \min \left\{ \frac{1}{\| \theta_i \|}, Q \right\} \leq 6 \log Q(Q + 2q). \]

For the case \( R > q/2 \), partition the range of summation into intervals of length at most \( q/2 \) – certainly there are at most \( 2R/q \) intervals in total. By Lemma 9, each contributes at most \( 6 \log Q(Q + 2q) \) to the whole sum. Therefore the sum is at most \( 12 \log Q(QR/q + 2R) \). In both cases, we obtain the upper bound \( 24 \log Q(Q + q + R + QR/q) \) with room to spare, as required.

We now come to our first theorem which gives an estimate for a Weyl sum involving quadratic exponents.
Theorem 11 (Weyl’s Inequality) Let $q, Q \in \mathbb{N}$, $Q \geq 2$, let $(a, q) = 1$ and let $\alpha \in \mathbb{R}$ with $|\alpha - a/q| \leq q^{-2}$. Let $\phi(x) = x^2 + cx + d$. Then
\[
\left| \sum_{x=0}^{Q} e^{2\pi i \alpha \phi(x)} \right| \leq 10(\log Q)^{1/2}(Q^{1/2} + q^{1/2} + Q/q^{1/2}).
\]

Proof ▷ Let $\psi_u(y) = \frac{1}{2\pi i} [\phi(y + u) - \phi(y)] = y + u/2 + c/2$. Then
\[
\left| \sum_{x=0}^{Q} e^{2\pi i \alpha \phi(x)} \right|^2 = \sum_{y=0}^{Q} \sum_{x=0}^{Q} e^{2\pi i \alpha \phi(x) - \alpha \phi(y)} = \sum_{y=0}^{Q} \sum_{u=-y}^{Q-y} e^{2\pi i \alpha \phi(y + u) - \alpha \phi(y)} + \sum_{u=0}^{Q} \sum_{y=0}^{Q} e^{2\pi i \alpha \phi(y + u) - \alpha \phi(y)} = \sum_{u=-Q}^{Q} \sum_{y \in I_u} e^{2\pi i 2\alpha y \psi_u(y)} \leq \sum_{u=-Q}^{Q} \sum_{y \in I_u} e^{2\pi i 2\alpha y + \beta u}.
\]

By Lemma 6, with $R = 2Q$ and room to spare,
\[
\sum_{u=-Q}^{Q} \min\{\|2u\alpha\|^{-1}, Q\} \leq \sum_{u=-2Q}^{2Q} \min\{\|u\alpha\|^{-1}, Q\} < 100 \log (Q + q + Q^2/q).
\]
where $I_u$ denotes the appropriate range of $y$-summation. This gives the desired bound. □

In particular, if $Q = q$ we obtain the bound of order $Q^{1/2}(\log Q)^{1/2}$. This is close to the best possible bound of $Q^{1/2}$, and such a bound was obtained early on by Gauss when $Q = q$ is prime, and more generally for character sums by Katz. Weyl’s Inequality can be extended to the case of Weyl sums of larger degree. The proof is very similar, but involves an induction on the degree using the lemma on finite differences.

Theorem 12 Let $q, Q \in \mathbb{N}$, $Q \geq 2$, let $(a, q) = 1$ and let $\alpha \in \mathbb{R}$ with $|\alpha - a/q| \leq q^{-2}$. Let $\phi(x)$ be a polynomial of degree $k$ whose leading coefficient is $\alpha$. Then
\[
\left| \sum_{x=0}^{Q} e^{2\pi i \alpha \phi(x)} \right| \ll^* Q(Q^{k-1} + q + Q^k/q)^{-2^{1-k}}.
\]

The star here means up to logarithmic factors of $Q$. So we observe that the bound has order of magnitude $Q^{1-(k-1)2^{1-k}}$ up to logarithmic factors when $Q = q$, and this agrees with the case $k = 2$. 9
9.7 Weyl’s Theorem

Weyl’s Theorem is a consequence of 11 which states that the function \( f(x) = \alpha x^k \) is uniformly distributed when \( \alpha \) is irrational. Before proving 11, we need some technical lemmas.

**Lemma 13** For \( n \in \mathbb{N} \), the number of factors of \( n \) is at most \( n^{4/(\log \log n)} \).

**Proof** Let \( 2 \leq t \leq n \) and write \( \tau(n) \) for the number of divisors of \( n \). If the prime factorization of \( n \) is \( p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k} \), then observe that the number of distinct factors of \( n \) is

\[
\prod_{i=1}^{k} (e_i + 1) \leq \prod_{p_i \leq t} (e_i + 1) \cdot \prod_{p_i > t} 2^{e_j + 1}
\]

for any \( t \in [k] \). This is at most

\[
\left(1 + \frac{\log n}{\log 2}\right)^t \cdot n^{\frac{1}{2\log t}} \leq \exp\left(t(2 + \log \log n) + \log 2 \cdot \log n / \log t\right).
\]

On choosing \( t = \log n / (\log \log n)^3 \), we obtain the result. \( \square \)

For the next lemma, we recall that if \( I(r) \) denotes the characteristic function of set \( I \), then the convolution \( (I * I)(r) \) is the same as the number of representations of \( r \) as a difference of two elements of \( I \), and if \( \hat{I} \) is the Fourier transform of \( I(r) \), then the Fourier transform of \( I * I \) is \( |\hat{I}|^2 \) — see the basic properties of Fourier transforms. We also recall \( \omega = e^{2\pi i/N} \) and let \( |r|_N \) denote \( \min\{r \mod N, -r \mod N\} \).

**Lemma 14** Let \( A \subset \mathbb{Z}_N \), \( |A| = M \), and suppose that \( A \cap (-2L, 2L] = \emptyset \). Then there exists \( r \in \mathbb{N} \) such that \( |r|_N < (N/L)^2 \) and \( |\hat{A}(r)| \geq LM/N \).

**Proof** Let \( I = (-L, L] \). We first observe that for any \( s \in \mathbb{Z}_N \), \( (I * I)(s) \cdot A(s) = 0 \). This follows from the fact that \( I - I \subseteq (-2L, 2L] \) which is disjoint from \( A \) by assumption. Consequently, using the fact that the sum of roots of unity is zero,

\[
\sum_{r \in \mathbb{Z}_N} \sum_{s \in \mathbb{Z}_N} (I * I)(s) A(t) \omega^{r(s-t)} = 0
\]

and this implies

\[
\sum_{s \in \mathbb{Z}_N} |\hat{I}(r)|^2 \hat{A}(r) = 0.
\]

The \( r = 0 \) term is exactly \( |I|^2|A| = 4L^2M \). From this and Parseval’s Identity we already know there exists \( r \neq 0 \) such that \( |\hat{A}(r)| \geq 2LM/N \), but we want to say more, namely that a similar bound holds for some \( r \) with \( |r|_N < (N/L)^2 \). Let \( J = \{r : 0 < |r|_N < (N/L)^2\} \). By Lemma 6,

\[
|\hat{I}(r)| = \left| \sum_{s \in I} \omega^{rs} \right| \leq \min\{\|r\|_N^{-1}, 2L\} \leq \frac{N}{r}
\]
since we may consider a sum over \( r \in \mathbb{Z}_N \) as a sum over \( r : -N/2 \leq r < N/2 \). Finally

\[
4L^2M \leq \sum_{r \neq 0} |\hat{I}(r)|^2 |\hat{A}(r)| \leq \max_{r \in J} |\hat{A}(r)| \sum_{r \neq 0} |\hat{I}(r)|^2 + M \sum_{r \notin J} \left( \frac{N}{r} \right)^2 \leq \max_{r \in J} |\hat{A}(r)| \cdot 2LN + ML^2.
\]

In the second line we used Parseval’s Identity on the first sum. Therefore there exists \( r \in J \) for which \( |\hat{A}(r)| \geq LM/N \).

Finally we state and prove Weyl’s Theorem for squares. In fact the theorem extends to \( k \)th powers in a similar way (see 12) so we stick to squares for simplicity.

**Theorem 15** (Weyl’s Theorem) There exists \( \varepsilon > 0 \) such that for all \( M \) sufficiently large and \( \alpha \in \mathbb{R} \), there exists \( q \leq M \) such that \( \|q^2\alpha\| \leq 2M^{-1/64} \).

**Proof** Use Dirichlet’s Box Principle to write \( \alpha = a/q + \theta \) where \( q \leq M \) and \( |\theta| \leq 1/qN \). If the claim of the theorem is false, then \( A = \{a, 4a, 9a, \ldots, M^2a\} \) and \((−2L, 2L]\) are disjoint when \( L = \lfloor qM^{-1/64} \rfloor \). Applying the last lemma, we find \( r \) such that \( |r|_q \leq (q/L)^2 \leq M^{1/16} \), and such that

\[
|\hat{A}(r)| \geq \frac{1}{2}M^{1-1/64}.
\]

Now

\[
|\hat{A}(r)| = \left| \sum_{s=1}^{M} e^{2\pi iars^2} \right|.
\]

If \( q \geq M^{1/4} \), applying Weyl’s inequality gives

\[
\sum_{s=1}^{M} e^{2\pi iars^2} < M^{1+1/64} \cdot M^{-1/16} \leq M^{1-3/64}.
\]

This is a contradiction if \( M \) is large enough. If \( q < M^{1/4} \), then \( \|q\alpha r\| \leq M^{-1} \). But then

\[
\|\alpha(qr)^2\| \leq 4M^{-1/2}M^{1/16} < 2M^{-1/64}
\]

for \( M \) sufficiently large, as required. \( \blacksquare \)