Notes on a few results from class

Ernie Croot

April 5, 2007

In this note I write up two results we have seen in class, namely the basic Large Sieve, and the method of Weyl differencing.

1 The Large Sieve

Suppose that

$$a_{M+1},\ a_{M+2},\ ...,\ a_{M+N}$$

is a sequence of complex numbers. Define the exponential sum

$$S(\alpha) \ = \ \sum_{n=M+1}^{M+N} a_n e^{2\pi i \alpha n} \ = \ e^{2\pi i \alpha N} \sum_{n=1}^{N} a_{M+n} e^{2\pi i \alpha n}.$$

The basic Large Sieve is an inequality of the form

$$\sum_{1 \le q \le Q} \sum_{\substack{1 \le a \le q \\ (a,q)=1}} |S(a/q)|^2 \ < \ (N + 3Q^2) \sum_{n=M+1}^{M+N} |a_n|^2.$$

This is not the best that is possible – in particular, the constant 3 here can be improved. In this note we will prove a somewhat weaker version of this inequality, where in place of $N + 3Q^2$ we will have $\pi N + Q^2$.

As we will see, this inequality has several arithmetic consequences. Before we prove it, and discuss these consequences, it is worth noting that this inequality is telling us that if we evaluate the poynomial

$$f(x) \ = \ \sum_{n=M+1}^{M+N} a_n x^n$$

at $x = e^{2\pi ia/q}$ – i.e. roots of unity – we cannot have that this polynomial is too big at too many of these places x at once.

Let us now prove the Large Sieve inequality. A key lemma we will need is given as follows

Lemma 1 *Suppose that $g(t)$ is a differentiable function on the interval*

$$[x-h,\ x+h].$$

Then,

$$|g(x)| \ \leq \ \frac{1}{2h}\int_{x-h}^{x+h} |g(t)|dt \ + \ \frac{1}{2}\int_{x-h}^{x+h} |g'(t)|dt.$$

Proof. To prove the lemma, first define the function

$$a(t) \ := \ \begin{cases} t-x+h, & \text{if } x-h \leq t \leq x; \\ t-x-h, & \text{if } x < t \leq x+h. \end{cases}$$

Then, consider the following integral, which we evaluate using integration-by-parts:

$$\int_{x-h}^{x+h} g'(t)a(t)dt \ = \ 2hg(x) \ - \ \int_{x-h}^{x+h} g(t)dt.$$

So, using the fact that $|a(t)| \leq h$ for $t \in [x-h, x+h]$, we find that

$$|g(x)| \ \leq \ \frac{1}{2}\int_{x-h}^{x+h} |g'(t)|dt \ + \ \frac{1}{2h}\int_{x-h}^{x+h} |g(t)|dt,$$

as claimed. ■

So, if we let

$$g(t) \ = \ S(t)^2,$$

then this lemma gives

$$\sum_{q\leq Q}\sum_{\substack{1\leq a\leq q-1\\(a,q)=1}} |S(a/q)|^2 \ \leq \ \sum_{q\leq Q}\sum_{\substack{1\leq a\leq q-1\\(a,q)=1}} \left(\frac{1}{2h}\int_{a/q-h}^{a/q+h} |S(t)|^2dt \ + \ \int_{x-h}^{x+h} |S(t)S'(t)|dt\right).$$

It is easy to see that letting

$$h \ = \ \frac{1}{2Q^2}$$

keeps these intervals

$$[a/q - h, \ a/q + h], \ 1 \leq q \leq Q, \ (a,q) = 1,$$

disjoint. And so, we will get

$$\sum_{q \leq Q} \sum_{\substack{1 \leq a \leq q-1 \\ (a,q)=1}} |S(a/q)|^2 \ \leq \ Q^2 \int_0^1 |S(t)|^2 dt \ + \ \int_0^1 |S(t)S'(t)| dt.$$

The first integral is easy to handle, as it has the following exact formula

$$\int_0^1 |S(t)|^2 dt \ = \ \sum_{n=M+1}^{M+N} |a_n|^2.$$

The second integral can be easily bounded from above using the Cauchy-Schwarz inequality, and in fact this upper bound is

$$\left(\int_0^1 |S(t)|^2 dt \right)^{1/2} \left(\int_0^1 |S'(t)|^2 dt \right)^{1/2}.$$

The first integral here is what we had before, but to bound the second integral from above, we observe that

$$|S'(t)| \ = \ \left| \sum_{n=1}^{N} a_{M+n} (2\pi n) e^{2\pi i n t} \right|; \tag{1}$$

so,

$$\int_0^1 |S'(t)|^2 dt \ \leq \ (4\pi^2 N^2) \sum_{n=M+1}^{M+N} |a_n|^2.$$

It follows that

Large Sieve.

$$\sum_{q \leq Q} \sum_{\substack{1 \leq a \leq q-1 \\ (a,q)=1}} |S(a/q)|^2 \ \leq \ (Q^2 + 2\pi N) \sum_{n=M+1}^{M+N} |a_n|^2.$$

In fact, by slightly altering the index n in (1) so that it is over all $|n| \leq N/2$ or so, then we can replace the $2\pi N$ with πN.

2 Some arithmetic consequences

The arithmetic applications of the large sieve all hinge on the following easy-to-prove identity: For any integer $q \geq 1$,

$$\sum_{1 \leq a \leq q-1} |S(a/q)|^2 \;=\; q \sum_{r=0}^{q-1} \left| \sum_{n \equiv r \pmod q} a_n \;-\; \frac{\Sigma}{q} \right|^2,$$

where

$$\Sigma \;=\; \sum_{n=M+1}^{M+N} a_n.$$

So, if we restrict our attention to the primes $q \leq Q$ in the large sieve stated previously, we deduce that

$$\sum_{\substack{q \leq Q \\ q \text{ prime}}} q \sum_{r=0}^{q-1} \left| \sum_{n \equiv r \pmod q} a_n \;-\; \frac{\Sigma}{q} \right|^2 \;<\; (Q^2 + \pi N) \sum_{n=M+1}^{M+N} |a_n|^2. \qquad (2)$$

(Note that I used the slighly stronger form of the large sieve derived in the previous section – the form with the term πN in place of $2\pi N$.)

From this last inequality it is easy to derive the following basic result:

Reyni's Sieve. Let $S \subset [M+1, M+N]$ be any set of integers, and suppose that for a given prime $q \leq Q$, S avoids $\omega(q)$ residue classes modulo q (i.e. these residue classes contain no elements of S). Then,

$$|S| \;\leq\; \frac{Q^2 + \pi N}{\sum_{q \leq Q} \omega(q)/q}.$$

To prove Reyni's sieve, we define

$$a_n \;=\; \begin{cases} 1, & \text{if } n \in S; \\ 0, & \text{if } n \notin S. \end{cases}$$

Then, we have that if $r \pmod q$ is one of the $\omega(q)$ residue classes containing no elements of S, then

$$\left| \sum_{n \equiv r \pmod q} a_n \;-\; \frac{\Sigma}{q} \right|^2 \;=\; \frac{|S|^2}{q^2}.$$

So,

$$q\sum_{r=0}^{q-1}\left|\sum_{n\equiv r \pmod q} a_n \;-\; \frac{\Sigma}{q}\right|^2 \;\geq\; \frac{\omega(q)|S|^2}{q}.$$

Our consequence of the Large Sieve given in (2) then implies

$$|S|\sum_{q\leq Q}\frac{\omega(q)}{q} \;\leq\; Q^2+\pi N,$$

and Reyni's sieve follows immediately.

It is worth pointing out that there is a much more powerful version of this sieve, due to Montgomery and Vaughan, which says:

Large Sieve. Suppose that $S\subset[M+1,M+N]$ is a set of integers, such that for a given prime $p\leq Q$, S avoids $\omega(p)$ residue classes mod p. Then,

$$|S| \;\leq\; \frac{N+3Q^2}{\sum_{\substack{q\leq Q\\ q \text{ square-free}}}\prod_{\substack{p|q\\ p \text{ prime}}}\frac{\omega(p)}{p-\omega(p)}}.$$

(Note: The constant 3 can be improved, but this form is good enough for most purposes.)

2.1 An example: The squares

Let S be the set of squares in $(\sqrt{N},N]$. Note that

$$|S| \;=\; \sqrt{N}-O(N^{1/4})$$

Let us see how close an upper bound the above two sieves give.

Let $Q=\sqrt{N}$, and note that for each $q\leq Q$, S avoids about $q/2$ residue classes mod q; so, we expect $\omega(q)$ is about $q/2$. More precisely, we will have

$$\omega(q) \;=\; \begin{cases} 0, & \text{if } q=2;\\ (q-1)/2, & \text{if } 3\leq q\leq\sqrt{N}.\end{cases}$$

Reyni's sieve then gives us that

$$|S| \ \leq \ \frac{(\pi+1)N}{\sum_{3\leq q\leq\sqrt{N}}\left(1-\frac{2}{q}\right)} \ \ll \ \sqrt{N}\log N.$$

That's pretty good – we are only off by a factor about $c\log N$ from the true upper bound.

It takes a little work, but it is relatively painless to show that the Montgomery-Vaughan large sieve gives the upper bound

$$|S| \ \ll \ \sqrt{N}.$$

So, it is within a constant factor of the true upper bound!

3 Weyl differencing

We have seen on several occasions that getting good upper bounds on exponential sums such as

$$S(t) \ := \ \sum_{n\leq N} e^{2\pi i t f(n)},$$

where f is some integer-valued function, has good consequences as far as studying additive problems. In particular, we have seen this in the case where $f(x)\in\mathbb{Z}[x]$ is monic (i.e. leading coefficient is 1) and where $t=a/q$ is a rational number.

Weyl differencing gives one a general procedure for establishing upper bounds on certain special exponential sums where f is a "linearizable function" (you will figure out what this means by looking at the examples below), and a "power savings" can often be achieved. By power savings, I mean that the quality of the upper bounds will be of the type

$$|S(a/q)| \ < \ |S|^{1-\varepsilon}.$$

Here, the trivial upper bound would be $|S|$; so, we save the power $|S|^{\varepsilon}$ over this trivial upper bound.

There are many techniques which are superior to Weyl differencing for when f is a polynomial, in that they give much better bounds for exponential

sums. Two such methods are Vinogradov's method and van der Corput's method; actually, van der Corput's method is little more than a refinement of Weyl's method. In the case where $t = a/q$, there are even more techniques, some of which come from algebraic arithmetic geometry, and some just use sophisticated combinatorics (like the sum-product inequalities of Bourgain, Katz, and Tao).

Although the most impressive consequences of Weyl's method come from when f is not a polynomial and t is not a rational number, we will instead work with the case $f(x) \in \mathbb{Z}[x]$ and $t = a/q$.

First, suppose that

$$f(x) \;=\; x^2 + bx + c.$$

Then, consider

$$W(a) \;=\; \sum_{0 \leq n \leq N} e^{2\pi i a f(n)/q},$$

where we assume that

$$(a, q) \;=\; 1, \text{ and } N \;\leq\; q - 1.$$

Note that if $f(x)$ were not monic, and its leading coefficient is coprime to q, then we could quickly reduce to the monic case by absorbing that lead coefficient into the factor a in $af(n)/q$.

The first step in Weyl's method is to rewrite $|W(a)|^2$ in a funny way:

$$\begin{aligned}
|W(a)|^2 &= \sum_{0 \leq n_1, n_2 \leq N} e^{2\pi i a (f(n_1) - f(n_2))/q} \\
&= \sum_{|h| \leq N} \sum_{\substack{n_1 \leq N \\ (n_2 = n_1 + h)}} e^{2\pi i a (n_1^2 + b n_1 + c - (n_1+h)^2 - b(n_1+h) - c)} \\
&\leq \sum_{|h| \leq N} \left| \sum_{0 \leq n_1 \leq N} e^{2\pi i a (-2 n_1 h)} \right|.
\end{aligned}$$

This final inner sum is a geometric series, so we have that it equals

$$\left| \frac{e^{-2\pi i (N+1) 2ha/q} - 1}{e^{2\pi i 2ha/q} - 1} \right| \;\leq\; \frac{2}{|e^{-\pi i 2ha/q} - e^{\pi i 2ha/q}|} \;=\; \frac{1}{|\sin(\pi 2ha/q)|}.$$

Well, this isn't quite right, because the denominator could vanish; so, the upper bound is actually

$$\min\left(|\sin(\pi 2ha/q)|^{-1},\ N+1\right).$$

We can simplify a little bit, using the inequality that for $0 \le t \le \pi/2$,

$$\sin(t) \ \ge \ 2t/\pi,$$

which can be seen by noting that $\sin(x)$ lies above the line with endpoints $(0,0)$ and $(\pi/2,1)$ – this line is $y = 2x/\pi$.

So,

$$|\sin(\pi 2ha/q)|^{-1} \ = \ (\sin \pi ||2ha/q||)^{-1} \ \le \ (2||2ha/q||)^{-1}.$$

Here, $||x||$ denotes the distance from x to the nearest integer.

Putting together the above estimates, we deduce that

$$|W(a)|^2 \ \le \ (N+1)|\{0 \le |h| \le N \ : \ q|2ha\}| \ + \ \sum_{\substack{|h|\le N \\ q\nmid 2ha}} \frac{1}{2||2ha/q||}$$

If we assume that $q \ge 3$ is prime, then the only value of h for which $q|2ah$ is $h = 0$, and therefore we will have

$$|W(a)|^2 \ \le \ (N+1) \ + \ \sum_{|h|\le N} \frac{1}{||2ha/q||}.$$

The largest each term $||2ha/q||$ can be is q, and there are at most two values of h that can make this happen; the second-largest value each term $||2ha/q||$ can be is $q/2$, and again there are at most two values of h that can make this happen. And so, extending this principle to its ultimate conclusion, we can deduce that

$$|W(a)|^2 \ \le \ (N+1) \ + \ 2q\sum_{j=1}^{N} \frac{1}{j} \ \ll \ q\log q.$$

it follows that:

Weyl's Estimate for Quadratics. Suppose that $N \leq q-1$ and $(a,q)=1$. Then,

$$|W(a)| \ \ll \ \sqrt{q \log q}.$$

Let us now consider the case of cubics; that is, we assume

$$g(n) \ = \ n^3 + bn^2 + cn + d.$$

Then, let

$$X(a) \ = \ \sum_{0 \leq n \leq N} e^{2\pi i a g(n)/q}.$$

As before, we compute $|X(a)|^2$, and so we will need to consider

$$n^3+bn^2+cn+d-(n+h)^3-b(n+h)^2-c(n+h)+d \ = \ -3hn^2-3h^2n-2bhn+r(h),$$

where $r(h)$ is a polynomial in h (which we can ignore when we go to bound $|X(a)|^2$ from above). Notice that this polynomial is of degree 2 in the variable n.

Using the same approach as was used to bound $|W(a)|^2$ from above, we will have for $(a,q)=1$, q prime, and $1 \leq N \leq q-1$,

$$|X(a)|^2 \ \leq \ \sum_{|h| \leq N} \left| \sum_{0 \leq n \leq N} e^{2\pi i a(-3hn^2-3h^2n-2bhn)/q} \right|.$$

Each of these inner sums is an exponential sum involving polynomials of degree 2, with the exception of the term $h=0$; and so, using the case we already worked out for quadratics, we deduce that

$$|X(a)|^2 \ \ll \ (N+1) \ + \ N\sqrt{q \log q} \ \ll \ q^{3/2}(\log q)^{1/2}.$$

It follows that

$$|X(a)| \ \ll \ q^{3/4}(\log q)^{1/4} \ = \ q^{3/4+o(1)}.$$

So, we have established

Weyl's estimate for cubics. For $1 \leq N \leq q-1$, q prime, $1 \leq a \leq q-1$, we have

$$|X(a)| \ \leq \ q^{3/4+o(1)}.$$

Continuing in this vein we find that:

Weyl's estimate, general case. If $h(n)$ is a monic, degree $d \geq 2$ polynomial with integer coefficients, we will have that as q runs through the primes, for every $1 \leq a \leq q-1$,

$$\left| \sum_{0 \leq n \leq N} e^{2\pi i a h(n)/q} \right| \ \leq \ q^{1-1/2^{d-1}+o(1)}.$$

One can use this to prove the following:

Theorem. For every $d \geq 2$ there exists $\varepsilon = \varepsilon(d)$ and $k = k(d)$, such that for *any* collection of k polynomials

$$f_1(x), \ f_2(x), \ ..., \ f_n(x) \ \in \ \mathbb{Z}[x],$$

each of degree at least 2 and at most d, we have that for every $c \in \mathbb{F}_q$, the number of solutions

$$(x_1, ..., x_k) \in (\mathbb{F}_q)^k \ : \ f_1(x_1) + \cdots + f_k(x_k) \ = c$$

is asymptotically

$$q^{k-1}.$$