THE BURGESS BOUND

ALEX DOBNER

Let χ denote a Dirichlet non-principal character modulo q, and let $S(M,N)$ denote the incomplete character sum

$$S(M,N) \coloneqq \sum_{n=M+1}^{M+N} \chi(n).$$

It is a classical problem to bound this sum in terms of N and q. By orthogonality of characters we may reduce to the case $N < q$. When N is small compared to q, these are called short character sums. A natural goal when bounding these is to beat the trivial bound $S(M,N) \ll N$.

If we assume χ behaves "randomly" then probabilistic heuristics suggest that there should be square-root cancellation in the sum. More precisely, one reasonable conjecture is

$$S(M,N) \ll N^{\frac{1}{2}} q^{\varepsilon}$$

for any fixed $\varepsilon > 0$. For $M = 0$ this follows from the generalized Lindelöf hypothesis $L(\frac{1}{2}+it,\chi) \ll (q(|t|+2))^{\varepsilon}$ by a standard application of Perron's formula. Note that this bound improves on the trivial bound even when N is just a tiny power of q.

Naturally we would also like to obtain unconditional bounds on these sums. In class[1] we discussed the following theorem.

Theorem 1 (Pólya-Vinogradov Inequality)**.** *Let χ be a non-principal character modulo q. Then for any integers M, N with $N > 0$,*

$$S(M,N) \ll \sqrt{q} \log q.$$

If one wants a bound that doesn't depend on N, then the Pólya-Vinogradov inequality is quite close to the best possible. Indeed, Montgomery and Vaughan have shown on GRH that

$$S(M,N) \ll \sqrt{q} \log\log q,$$

and a result of Paley shows that sums of this size are actually attained.

In the rest of this note we'll discuss a more sophisticated bound on $S(M,N)$ due to Burgess which depends on the Riemann hypothesis for curves over a finite field. The Riemann hypothesis is known to hold in this setting, so these results are unconditional.

Theorem 2 (Burgess)**.** *Let χ be a nonprincipal character modulo an odd prime p, and let r be a positive integer. We have*

$$S(M,N) \ll r N^{1-\frac{1}{r}} p^{\frac{r+1}{4r^2}} (\log p)^{\alpha_r}$$

where $\alpha_r = 1$ when $r = 1$ and $\alpha_r = \frac{1}{2r}$ otherwise.

[1]These notes were originally written as a final project for a topics course in analytic number theory.

1. Lemmas

In order to prove bounds on *incomplete* character sums (i.e. sums over some subset of residues modulo q) it is helpful to relate them in some way to *complete* sums (i.e. sums over every residue class). For example, the standard proof of the Pólya-Vinogradov theorem involves expressing the multiplicative character χ as a complete sum of additive characters.

To prove the Burgess bound, the complete sums we'll use are of the form

$$\sum_{n=1}^{p} \chi(f(n))$$

where f is a polynomial. It turns out that it is possible to prove square-root cancellation holds for these sums using the Riemann hypothesis over finite fields.

Lemma 1 (Weil)**.** *Let χ be a character modulo p of order $d > 1$. Suppose $f(x) \in \mathbb{F}_p[X]$ is a polynomial which is not of the form $c(g(X))^d$ for some $c \in \mathbb{F}_p$ and $g(X) \in \mathbb{F}_p[X]$. Let m be the number of distinct roots of $f(X)$. Then*

$$\left| \sum_{n=1}^{p} \chi(f(n)) \right| \leq (m-1)p^{\frac{1}{2}}.$$

In order to apply Weil's bound to the sums $S(M,N)$, we will need to relate $S(M,N)$ to sums of χ evaluated at the polynomial points $f(n)$. Since χ is multiplicative, such polynomials arise naturally by taking moments of short character sums. The following lemma will suffice for proving the Burgess bound.

Lemma 2. *Let χ be a non-principal character modulo p and let r be a positive integer. Then*

$$\sum_{n=1}^{p} \left| \sum_{m=1}^{h} \chi(n+m) \right|^{2r} \ll r^{2r} \left(h^r p + h^{2r} p^{\frac{1}{2}} \right).$$

The proof of Lemma 2 is a fairly straightforward application of Lemma 1 (see [1, Lemma 9.26] for details).

2. Proof of the Burgess bound

2.1. **Basic Idea.** We now give the main ideas in the proof of the Burgess bound. Note that the $r = 1$ case of the Burgess bound is identical to the Pólya-Vinogradov inequality, so we'll assume $r \geq 2$.

Recall that $S(M,N)$ is defined to be the sum of the values of χ evaluated at each of elements of $I \coloneqq \{M+1, \ldots, M+N\}$. We now make the following trivial observation: if $\mathcal{F}$ is a family of subsets of I which is a k-fold covering of I (i.e. each element of I is contained in k of the sets in $\mathcal{F}$), then

$$S(M,N) = \frac{1}{k} \sum_{E \in \mathcal{F}} \sum_{j \in E} \chi(j). \tag{1}$$

Hence, if $|S(M,N)|$ is large then it must be the case that many of the sums $\sum_{j\in E}\chi(j)$ are large as well. Conversely, if we want to bound $S(M,N)$ we can instead try to show bounds on $\sum_{j\in E}\chi(j)$ that hold "on average."

To give an example of this idea, suppose H is some parameter that's small relative to N and let $\mathcal{F}$ consist of translates of the set $\{1,2,\dots,H\}$. That is, we we'll consider the sets $\{n+1,\dots,n+H\}$ for each $n\in I$. Note that this is family is "approximately" an H-fold covering of I. It's not actually an H-fold covering because some of the elements of I near the endpoints are covered fewer than H times, but it is easy to see that we still get an approximate version of (1),

$$S(M,N)=\frac{1}{H}\sum_{n=M+1}^{M+N}\sum_{k=1}^{H}\chi(n+k)+O(H).$$

To bound the main term of this expression, we can apply Hölder's inequality to see

$$\left|\frac{1}{H}\sum_{n=M+1}^{M+N}\sum_{k=1}^{H}\chi(n+k)\right|\le\frac{1}{H}N^{1-\frac{1}{2r}}\left(\sum_{n=M+1}^{M+N}\left|\sum_{k=1}^{H}\chi(n+k)\right|^{2r}\right)^{\frac{1}{2r}} \tag{2}$$

$$\le\frac{1}{H}N^{1-\frac{1}{2r}}\left(\sum_{n=1}^{p}\left|\sum_{k=1}^{H}\chi(n+k)\right|^{2r}\right)^{\frac{1}{2r}} \tag{3}$$

where the second inequality is trivial because we have extended the incomplete sum to a complete sum. From this last expression it's now clear what the purpose of these manipulations was: we can apply Lemma 2 to this expression to get a bound on $S(M,N)$! Sadly it turns out that this method doesn't actually give better bounds than what we already know. That is, there is no choice of H and r where the resulting bound is better than what one gets from either the trivial bound or Pólya-Vinogradov. In order to derive the Burgess bound, one needs to be more careful.

2.2. **Improving the method.** The problem with the method above is that the inequality where we went from the incomplete sum to the complete sum is too inefficient. On the right-hand side of (2) we have the $2r$th moment over N different translates of $\{1,2,\dots,H\}$ whereas in (3) we have the $2r$th moment over all p different translates. Burgess's key insight was to choose a larger family $\mathcal{F}$. The family he considered consists of all *arithmetic progressions*

$$\{n+d,n+2d,\dots,n+Hd\}\text{ for all }d\in\{1,\dots,D\}\text{ and }n\in I.$$

Here D is another parameter which we think of as being small relative to N (we will require $D<p$).

Similarly to the previous family, this new family is an approximate DH-fold covering of I. To state this rigorously, we let

$$\mathcal{M}(y)\coloneqq\max_{\substack{M,N\\N\le y}}|S(M,N)|.$$

Then one can check that

$$S(M,N) = \frac{1}{DH} \sum_{\substack{n\in I \\ d\in\{1,\dots,D\} \\ k\in\{1,\dots,H\}}} \chi(n+kd) + 2\theta\mathcal{M}(DH) \tag{4}$$

for some $|\theta| \leq 1$. (Note that when $D = 1$, we are precisely in the special case of the method described previously.)

Since χ is multiplicative, each of the sums over the arithmetic progressions can be related to an incomplete character sum $S(m,H)$ for some m. Indeed, given some choice of n and d, we may write $n \equiv dm \pmod p$ for some unique $1 \leq m \leq p$, and we see that

$$\sum_{k=1}^{H} \chi(n+kd) = \chi(d) \sum_{k=1}^{H} \chi(m+k).$$

Letting $v(m)$ denote the number of pairs n, d with $n \in I$ and $d \in \{1,\dots,D\}$ such that $n \equiv dm \pmod p$, we see that

$$\left|\sum_{n,d,k} \chi(n+kd)\right| = \left|\sum_{m=1}^{p} \sum_{\substack{n,d \\ n\equiv dm\ (p)}} \chi(d) \sum_{k=1}^{H} \chi(m+k)\right| \tag{5}$$

$$\leq \sum_{m=1}^{p} v(m) \left|\sum_{k=1}^{H} \chi(m+k)\right|. \tag{6}$$

Now let's consider why this may give an improvement over the previous method. Suppose for a moment that for any m there is at most one pair (n,d) associated to it. This would mean that $v(m) = 1$ for ND different values of m, and $v(m) = 0$ elsewhere. Consequently, the sum in (6) is an incomplete sum just like the sums in (2) were, but the collection of residue classes we are summing over this time is less sparse (we are summing over ND residue classes rather than N of them). Hence, the step where we bound the incomplete sum by a complete sum will be more efficient in this case.

To carry out this method, there are some hurdles to overcome. For example, there may be "collisions" where different pairs (n,d) and (n',d') correspond to the same value of m. Also, we still need to worry about how to handle the error term in (4). To make sure there aren't many collisions, it's necessary to choose the parameter D such that $ND \ll p$. To handle the error term in (4), the solution is to use induction on N: if we ensure that (say) $DH \leq N/10$, then $\mathcal{M}(DH) \leq \mathcal{M}(N/10)$ which we then bound using the induction hypothesis.

Applying (6) and Hölder's inequality to bound (4) we see that

$$|S(M,N)| \leq \frac{1}{DH} ||v||_{\frac{2r}{2r-1}} \left(\sum_{n=1}^{p} \left|\sum_{k=1}^{H} \chi(n+k)\right|^{2r}\right)^{\frac{1}{2r}} + 2\mathcal{M}(DH)$$

where we have used the notation $||v||_s$ to mean $(\sum_{m=1}^{p} v(m)^s)^{\frac{1}{s}}$. Applying Lemma 2 then gives

$$|S(M,N)| \leq \frac{1}{D}||v||_{\frac{2r}{2r-1}} Cr\left(H^{-\frac{1}{2}}p^{\frac{1}{2r}} + p^{\frac{1}{4r}}\right) + 2\mathcal{M}(DH) \tag{7}$$

for some absolute constant $C > 0$.

If there were no "collisions" at all, then we'd have that $||v||_{\frac{2r}{2r-1}} = (ND)^{1-\frac{1}{2r}}$. Inserting this this into (7) one can check that the optimal choice (subject to our constraints) of D and H is

$$H = \left\lfloor p^{\frac{1}{2r}} \right\rfloor, \qquad D = \left\lfloor \frac{1}{10} N p^{-\frac{1}{2r}} \right\rfloor. \tag{8}$$

Inserting these into (7) and doing the induction on N that we mentioned above would then give the Burgess bound without out any logarithmic loss.

In reality of course there will be some collisions. Consequently the size of $||v||_{\frac{2r}{2r-1}}$ will be a bit larger than the idealized scenario. To get a bound, we'll interpolate between bounds on $||v||_1$ and $||v||_2$. From the definition of $v(m)$ we know that

$$||v||_1 = \sum_{m=1}^{p} v(m) = DN,$$

so our goal is to get a bound on $||v||_2^2$ that isn't much worse than this. The following lemma shows that we can get a bound that only loses a $\log p$.

Lemma 3. *Suppose $DN < p/2$ and $1 \leq D \leq N$. Then $||v||_2^2 \ll DN \log p$.*

Proof. Note that by the definition of $v(m)$, the sum $\sum_{m=1}^{p} v(m)^2$ counts the number of choices of n, n', d, d', m such that $n, n' \in \{1, \dots, N\}$, and $d, d' \in \{1, \dots, D\}$, and $M + n \equiv dm \pmod p$, $M + n' \equiv d'm \pmod p$. Eliminating m, these congruences are equivalent to the condition

$$(d - d')M \equiv d'n - dn' \pmod p.$$

Given any pair d, d' we will derive an upper bound on the number of choices of n, n' that can satisfy the condition above. Let k be the unique integer such that $|k| < p/2$ and $(d - d')M \equiv k \pmod p$. Note that by the assumption $DN < p/2$, any solution to the congruence $d'n - dn' \equiv k \pmod p$ must in fact be an equality $d'n - dn' = k$. If n_0, n_0' are a fixed pair of solutions, elementary number theory tells us that solutions to this equation are given by $n = n_0 + \frac{d}{(d,d')}h, n = n_0 + \frac{d'}{(d,d')}h$. By the restriction on the range of n, n' the solutions we care about must satisfy $|h| \leq \frac{N(d,d')}{\max\{d,d'\}}$. This means the total number of choices of n, n' is at most $1 + \frac{2N(d,d')}{\max\{d,d'\}}$.

Summing now over all choices of d, d' we get

$$\begin{aligned}\sum_{m=1}^{p} v(m)^2 &\ll \sum_{1\leq d\leq d'\leq D}\left(1+\frac{2N(d,d')}{d'}\right)\\ &\ll D^2+N\sum_{l\leq D}\sum_{1\leq e\leq e'\leq D/l}\frac{1}{e'}\\ &\ll D^2+DN\log 2D.\end{aligned}$$

which gives the result. □

To see that our choice of D in (8) satisfies the constraints of the lemma, note that $DN \leq \frac{1}{10}N^2p^{-\frac{1}{2r}}$. One can verify that this quantity is less than $p/2$ for any values of N and p that we are interested in (i.e. values which are not already covered by the Pólya-Vinogradov inequality).

Hence, from Hólder's inequality deduce that

$$||v||_{\frac{2r}{2r-1}} \leq ||v||_1^{1-\frac{1}{r}}||v||_2^{\frac{1}{r}} \ll (DN)^{1-\frac{1}{2r}}(\log p)^{\frac{1}{2r}}.$$

Inserting this into (7) with our choice of parameters (8) we get

$$|S(M,N)| \leq C'rN^{1-\frac{1}{r}}p^{\frac{r+1}{4r^2}}(\log p)^{\frac{1}{2r}} + 2\mathcal{M}(N/10).$$

Performing the induction on N (and using the trivial bound as soon as $N < p^{1/4+1/(4r)}$) gives the Burgess bound.

References

[1] Hugh L. Montgomery and Robert C. Vaughan. *Multiplicative number theory. I. Classical theory*, volume 97 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2007.

Email address: adobner@umich.edu