Burgess bounds:
Character Sums and Dirichlet L-functions

Marios Voskou

January 27, 2021

References

1 : Burgess, D.A. (1957), The distribution of quadratic residues and non-residues. Mathematatika, 4: 106-112.

2 : Burgess, D.A. (1962), On Character Sums and Primitive Roots†. Proceedings of the London Mathematical Society, s3-12: 179-192.

3 : Burgess, D.A. (1962), On Character Sums and L-Series†. Proceedings of the London Mathematical Society, s3-12: 193-206.

4 : **Burgess, D.A. (1963), On Character Sums and L-Series. II. Proceedings of the London Mathematical Society, s3-13: 524-536.**

Introduction

For a fixed non-principal character $\chi \mod q$ we define:

- $$S_H(N) := \sum_{n=N+1}^{n=N+H} \chi(n),$$

  where N and H positive integers.

- $$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

  where $s = \sigma + it$ will be a fixed complex number with $0 < \sigma < 1$.

We are interested in:

- Bounds for $S_H(N)$ in terms of H and/or q.
- Using them to derive (sub-convexity) bounds for the L-series $|L(s,\chi)|$ with respect to q (via partial summation).

From Characters Sums to L-series

- By partial summation:

$$L(s,\chi) = \sum (S(n))(1/n^s - 1/(n+1)^s) \ll \sum |S(n)| n^{-1-\sigma}$$

where $S(n) = S_n(0)$.

- Character bounds available:
  - In n, the trivial bound:
  $$|S(n)| \leq n$$
  - In q, Pólya-Vinogradov:
  $$S(n) \ll q^{1/2} \log q$$
- Using those optimally:

$$L(s,\chi) \ll \sum |S(n)| n^{-1-\sigma} \ll (q^{1/2} \log q)^{1-\sigma}$$

From Characters Sums to L-series

- Note:
  - n-bound is better for small n's.
  - q-bound is better for large n's.
- Potential for better results using mixed bounds for middle-sized n's.
- In that end, we write:

$$\begin{aligned} L(s,\chi) &\ll \sum |S(n)| n^{-1-\sigma} \\ &= \sum_{n \leq N} + \sum_{N<n<M} + \sum_{n \geq M} \end{aligned}$$

- First term is bounded trivially by $N^{1-\sigma}$. Last term is, using Pólya-Vinogradov, $O(M^{-\sigma} q^{1/2} \log q)$.

Goals: Chatacter Sums

We will follow the work of Burgess on such mixed bounds.
In particular, for $q = p$ prime:

Theorem 1 (Burgess, 1962)

For N, H, r positive integers:

$$|S_H(N)| \ll H^{1-1/r} p^{(r+1)/4r^2} \log p$$

with the implied constant being absolute.

This can be generalized to:

Theorem 2 (Burgess, 1962)

For N, H, r positive integers (r fixed), and given that q is cube-free or $r = 2$:

$$|S_H(N)| \ll H^{1-1/r} q^{(r+1)/4r^2+\epsilon}$$

with the implied constant depending on r (and ϵ).

Goals: L-series

Taking $r = 2$ and applying partial summation in the sense discussed above:

Theorem 3 (Burgess, 1962)

Let $s = \sigma + it$ be a fixes complex number with $0 < \sigma < 1$. Then, for any fixed $\epsilon > 0$:

$$|L(s,\chi)| \ll \begin{cases} q^{\frac{4-5\sigma+\epsilon}{8}} & 0 < \sigma \leq \frac{1}{2} \\ q^{\frac{3-3\sigma+\epsilon}{8}} & \frac{1}{2} \leq \sigma < 1 \end{cases}$$

In particular, for $\sigma = \frac{1}{2}$:

$$\left| L\left(\frac{1}{2} + it, \chi\right) \right| \ll q^{\frac{3}{16}+\epsilon}$$

Sketch of Proof

- **Idea**:

  - Relate $S_H(N)$ to a sum of shorter sums $S_h(x)$, then use Holder Inequality to get a sum of the form
  $$\sum_x |S_h(x)|^{2r}$$
  over a controlled number of x's.
  - **How:** $\{N+1, \cdots, N+H\}$ contains copys of $\{1, \cdots, h\}$ (as APs)

- **Motivation:**

  - For small h, can think of $|S_h(x)|^{2r}$, after expansion, as a sum of terms of the form $\chi(f(n))$, where f runs overs a family of polynomials that reduce fully over $\mathbb{Z}$.
  - For such polynomials, sums $\sum_{n=1}^{p} \chi(f(n))$ can be bounded naturally using work of H.Hasse and A.Weil on L-functions belonging to algebraic function fields.

$\sum \chi(f)$: Goal

- The first step will be to establish the necessary bounds for

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

.

- We will start with the case $q = p$ prime.

Lemma 1.1

Let $d = ord(\chi)$.
Take $f(n) = (n - a_1)^{r_1} \cdots (n - a_t)^{r_t}$, where all the a_i's are distinct $\mod p$, $0 < r_i < d$, and $degf = \nu d$ where ν is an integer.
We will show that:

$$\left| \sum_{n=1}^{p} \chi(f(n)) \right| \leq (t-2)p^{1/2} + 1$$

Proof (of Lemma 1.1)

- Let $K = \mathbb{F}_p(x)$ be the field of rational functions on $\mathbb{F}_p$.
- Recall:
  - Divisors of K: formal products of places/"prime divisors".
  - All places of K are induced from $v_{q(x)}$ (for q irreducible) and v_∞.
- To an element g of K, we attach the divisor

$$(g)' = \prod_{\mathfrak{p} \text{ prime}} \mathfrak{p}^{v_{\mathfrak{p}}(g)} \pmod{d}$$

- For **divisors** $\mathfrak{a}$ of K,define:

$$\chi(\mathfrak{a}) := \begin{cases} \chi(N_{\mathfrak{a}}(f)) & \mathfrak{a} \quad \text{"coprime" to} \quad (f)' \\ 0 & \text{otherwise} \end{cases}$$

where $N_{\mathfrak{a}}(-)$ is the norm in the residue-class ring modulo $\mathfrak{a}$.

$\sum \chi(f)$

- The corresponding L-function is:

$$L(s,\chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{R(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \left(1 - \frac{\chi(\mathfrak{p})}{R(\mathfrak{p})^s}\right)^{-1}$$

, where $\mathfrak{a}$ runs overs all the divisors of K and $\mathfrak{p}$ runs overs the prime divisors only. Here $R(\mathfrak{a})$ is the size of the corresponding residue-class ring.

- Let σ be the coefficient of p^{-s} in $L(s,\chi)$, so that

$$\sigma = \sum_{\mathfrak{p}}{}' \chi(\mathfrak{p})$$

where $\sum'$ indicates summation over prime divisors of degree 1 in K (as those give a residue-class ring isomorphic to $\mathbb{F}_p$)

$\sum \chi(f)$: H. Hasse

- In our case, degree 1 prime divisors $\mathfrak{p}$ (except $\mathfrak{p}_\infty$) correspond to polynomials $x - n$ where $n \in \mathbb{F}_p$.
- In particular,

$$\chi(\mathfrak{p}) = \chi\left(N_{\mathfrak{p}}(f)\right) = \chi(f(n))$$

- So:

$$\left|\sum_{n=1}^{p} \chi(f(n))\right| = \left|\sum_{\mathfrak{p} \neq \mathfrak{p}_\infty}^{\prime} \chi(\mathfrak{p})\right| \leq 1 + |\sigma|$$

- **Hasse (1935)**: $p^{(t-2)s} L(s, \chi)$ is a polynomial of degree $t - 2$ in terms of p^s.
- Hence: if $w_1, \ldots, w_{t-2}$ its roots we get

$$\sigma = -\sum_{i=1}^{t-2} w_i$$

$\sum \chi(f)$: A. Weil

- Let $Z = K(y)$ the algebraic extension of K defined by $y^d = f(x)$.
- $L(s,\chi)$ divides the zeta function $\zeta_Z(s)$.
- **Weil (1945): RH for $\zeta_Z(s)$.**
- Therefore: $|w_i| = p^{1/2}$ for every i.
- Hence:

$$\left|\sum_{n=1}^{p} \chi(f(n))\right| \leq 1 + |\sigma| = 1 + \left|\sum_{i=1}^{t-2} w_i\right| \leq 1 + (t-2)p^{1/2}$$

$\sum \chi(f)$: q composite

We will now derive the following generalization:

Lemma 1.2

Assume that either q is cube-free or $r = 2$. Assume further that χ is a proper character modulo q.
Let

$$f(n) = (n - a_1) \cdots (n - a_r)(n - a_{r+1})^{\phi(q)-1} \cdots (n - a_{2r})^{\phi(q)-1}$$

, where $r \geq 2$ and at least $r + 1$ out of the a_i's are distinct. Let

$$A_i := \prod_{j \neq i} (a_i - a_j)$$

For some non-trivial A_i,

$$\left| \sum_{n=1}^{q} \chi(f(n)) \right| \leq (4r)^{\omega(q)} (q, A_i) q^{1/2}$$

Set-up of Proof:

- Write

$$\sigma(m) := \sum_{n=1}^{m} \chi(f(n))$$

- $\sigma(m)$ multiplicative, so for $\sigma(q)$ enough to consider $\sigma(p^a)$ for p^a dividing q.

  (Note: this is where $(4r)^{\omega(q)}$ comes from)

$\sum \chi(f)$: q composite

(Sketch of) Proof of Lemma 1.2

- Work with $\sigma(p^a)$ where $p^a | q$.
- Main idea: reduce modulo p^γ ($\gamma = \lfloor \frac{1}{2} a \rfloor$) and group the equivalent terms.
- Noting that

$$f(x) = f(x_0 + p^\gamma y) \equiv f(x_0) + f'(x_0) p^\gamma y + \frac{f''(x_0)}{2!} (p^\gamma y)^2 \, (mod \; p^a),$$

  we can reduce each group of terms to a sum of the form

$$\sum_n e\left(\frac{An + Bn^2}{p}\right) = \begin{cases} p^{\frac{1}{2}} & \text{if } p \nmid B \\ 0 & \text{if } \; p | B, \; p \nmid A \\ p & \text{if } \; p | B, \;\; p | A \end{cases}$$

- Cases determined by whether some prime powers divide certain polynomials.
- Bound number of occurrences of each case (this is where we use our assumptions for q).
- Combine. Done.

$\sum \chi(f)$

- From now on: assume $q = p$ prime.
- General case essentially the same from this point on.
- In the way discussed we can get:

Lemma 2

For any positive integers r and h,

$$\sum_{n=1}^{p} |S_h(n)|^{2r} < (4r)^{r+1} p h^r + 2rp^{\frac{1}{2}} h^{2r}$$

Proof of Lemma 2

- We have:

$$\sum_{n=1}^{p} |S_h(n)|^{2r}$$

$$= \sum_{n=1}^{p} \sum_{m_1,..,m_{2r}=1}^{h} \chi\left((n+m_1)\cdots(n+m_r)\right)\bar{\chi}\left((n+m_{r+1})\cdots(n+m_{2r})\right)$$

$$= \sum_{m_1,..,m_{2r}=1}^{h} \sum_{n=1}^{p} \chi\left((n+m_1)\cdots(n+m_r)(n+m_{r+1})^{p-2}\cdots(n+m_{2r})^{p-2}\right)$$

- Reduce modulo p and exponents modulo d (ignoring for now the effect of term where the polynomial vanishes).
- Most of the polynomials are now in the form discussed, except for perfect d powers (recall $d = ord(\chi)$).

Proof of Lemma 2 (cont.)

- Fortunately: at most $(4r)^{r+1}h^r$ such exceptions.
- They give total contribution of $p(4r)^{r+1}h^r$.
- For a polynomial that indeed satisfies our conditions, and having t distinct roots after the reduction, its sum contributes at most

$$2r - t + (t-2)p^{1/2} + 1 \leq 2rp^{1/2}$$

  (where $2r - t$ is there to correct the terms lost in the reduction).
- The number of such polynomials can be bounded trivially by h^{2r}.
- This gives a total contribution of at most $2rp^{\frac{1}{2}}h^{2r}$
- The result follows by combining the two contributions.

Applying Holder's Inequality

- For a set $A \in \{1, 2, \cdots, p\}$, we have:

$$\sum_{n=1}^{p} |S_h(n)|^{2r} \geq \sum_{n \in A} |S_h(n)|^{2r} \geq \left(\sum_{n \in A} |S_h(n)| \right)^{2r} \left(\sum_{n \in A} 1 \right)^{1-2r}$$

- Note: Second factor larger for smaller $\#A$.

  (so full A not necessarily optimal)

- **Our goal for now on**: Relate $S_H(N)$ to a sum

$$\sum_{n \in A} |S_h(n)|$$

in an efficient way.

Heuristics

- Want to say:

$$\begin{aligned} S_H(N) &\approx \frac{1}{h}\sum_{m=1}^{H} S_h\left(\frac{N+m}{d}\right) \quad \left(\begin{array}{c} \textit{identifying copies of } [1..h] \\ \textit{in } \{N+1,\dots,N+H\} \textit{ as APs.}\end{array}\right) \\ &\ll \frac{1}{H}\sum_{d=1}^{H/h}\sum_{m=1}^{h}\left|S_h\left(\frac{N+m}{d}\right)\right| \\ &\ll \frac{1}{H}\left(\frac{H^2}{h}\right)^{1-\frac{1}{2r}}\left((4r)^{r+1}ph^r + 2rp^{\frac{1}{2}}h^{2r}\right)^{1/2r} \\ &\ll H^{1-1/r}p^{(r+1)/4r^2} \quad (\text{taking } h \approx p^{1/2r}) \end{aligned}$$

- Note: here $\#A \approx \frac{H^2}{h}$
- **Unfortunately:** errors cost too much.
- We'll try to make this more efficient.

Introducing Intervals

- First Step from above:

$$S_H(N) \approx \frac{1}{h}\sum_{m=1}^{H} S_h\left(\frac{N+m}{d}\right)$$

Idea:

- Associate $S_H(N)$ to sums over disjoint intervals.
  (appearing as affine transformations of APs in $\{N+1,\cdots,N+H\}$).
- Apply First Step of the heuristic argument in each interval (for $d=1$).
- Choose the intervals so that we have control over the errors.
- Take A to be the union of the intervals
  (disjointedness guarantees that this makes sense).

Making Sense of the Heuristics

Consider an interval $I = \{n_1 + 1, \cdots, n_2\}$. (some integers n_1,n_2)
We apply heuristic argument on the interval, for $d = 1$:

- Define
$$\phi_i(m) := \sum_{y=1}^{m} \chi(n_i + y), \quad i = 1, 2$$
- We have that, for any given positive integer m,
$$\sum_{n \in I} \chi(n) = \sum_{n \in I} \chi(n + m) + \phi_1(m) - \phi_2(m)$$
- For any given positive integer h:
$$\sum_{n \in I} \chi(n) = \frac{1}{h} \sum_{m=1}^{h} \sum_{n \in I} \chi(n)$$

Making Sense of the Heuristics

- Consider a set $\mathcal{I}$ of disjoint intervals.
- Let $A' = \cup\, \mathcal{I}$.
- Combine last slide's results:

$$\begin{aligned} h \times \sum_{I \in \mathcal{I}'} \left| \sum_{n \in I} \chi(n) \right| &= \sum_{\mathcal{I}'} \left| \sum_{m=1}^{h} \sum_{n \in I} \chi(n) \right| \\ &\leq \sum_{n \in A'} |S_h(n)| + \sum_{i=1,2} \sum_{\mathcal{I}'} \left| \sum_{m=1}^{h} \phi_i(m) \right| \end{aligned}$$

Making Sense of the Heuristics

- $$h \times \sum_{I \in \mathcal{I}'} \left| \sum_{n \in I} \chi(n) \right| \leq \sum_{n \in A'} |S_h(n)| + \sum_{i=1,2} \sum_{\mathcal{I}'} \left| \sum_{m=1}^{h} \phi_i(m) \right|$$
- First term: "main term" - denote S_0.
- Other two: "error terms"- denote $S_{1,2}$.

Error Control

Suppose that S_0 is not the largest out of the three.
We can show the following:

Lemma 3

Suppose that no element of $\mathcal{I}$ has less than h elements.
Suppose further that

$$max\left\{S_1, S_2\right\} \geq 2eh \times \#\mathcal{I}$$

Then: For some M of the form $M = h_0 \times \#\mathcal{I} \leq h \times \#\mathcal{I}$ there exist a set A'' of M distinct integers for which:

$$\sum_{n \in A''} |S_h(n)| = \sum_{n \in A''} \left| \sum_{m=1}^{h} \chi(n+m) \right| \geq \frac{h_0}{ehlog_2(h)} \times max\left\{S_1, S_2\right\}$$

APs as Affine Transformations of Intervals

- **Left to Do:** Find appropriate family of intervals $\mathcal{I}$.
- Write $\eta := |S_H(N)|$.
- Can assume that $\eta > 1$ and $0 \leq N < N + H < p$ (otherwise trivial).
- Intervals in range as affine transformations:

We can see that for any positive integer $w < p$,

$$\eta = \left| \sum_{n=N+1}^{N+H} \chi(n) \right| \leq \sum_{t=0}^{w-1} \left| \sum_{\substack{n = N+1 \\ n \equiv -tp \pmod{w}}}^{N+H} \chi(n) \right|$$

APs as Affine Transformations of Intervals

- Write $I(w,t) := \left\{ z \in \mathbb{Z} \mid \frac{N+1+tp}{w} \leq z \leq \frac{N+H+tp}{w} \right\}$,
- Note that for $n = -tp + wz$ we have $\chi(n) = \chi(-tp + wz) = \chi(w)\chi(z)$
- Rewrite above as:

$$\eta \leq \sum_{t=0}^{w-1} \left| \sum_{z \in I(w,t)} \chi(z) \right|$$

- We can then take average for various w, and have a sum over various intervals $I(w,t)$.

Chosing the Right Intervals

- Want intervals disjoint.
- **Observation**:
  For fixed coprime w, w' (wlog $w > w'$), by comparing endpoints:

If $2Hw < p$, there is at most one pair (t, t') with $I(w, t)$ and $I(w', t')$ not disjoint.

- Under this assumption, for a fixed set W of w's taking a set $T(w)$ for each w all values of t that do not appear in a pair, we get:

Lemma 4

Suppose $w_1 < w < w_2$ for every $w \in W$.

Suppose $2Hw_2 < p$.

Then, for every w in W, we can associate a set $T(w)$ of integers t with $0 \leq t < w$ with $\#T(w) \geq w - Q$, so that **all the resulting** $I(w, t)'s$ **are disjoint**.

Choosing the Right Intervals

Remark

Regarding our selection above, we can also note the following:
If $N(w,t)$ is the number of (other) intervals $I(w',t')$ that intersect $I(w,t)$ then, for every $w \in W$:

$$\sum_{t \notin T(w)} N(w,t) \leq Q$$

- We take W to be a set of Q primes.
- Take also $w_2 = 2w_1 < \frac{1}{2}pH^{-1}$.
- Length of $I(w,t)$ is $\frac{H}{w}$ so control over range of w means control over range of lengths.

Choosing the Right Intervals

We have:

$$Q\eta \leq \sum_{w\in W}\sum_{t=0}^{w-1}\left|\sum_{z\in I(w,t)}\chi(z)\right|$$

$$\leq \sum_{w\in W}\sum_{t\in T(w)}\left|\sum_{z\in I(w,t)}\chi(z)\right| + \sum_{w\in W}\sum_{t\notin T(w)}\left|\sum_{z\in I(w,t)}\chi(z)\right|$$

We have 2 cases.
Either:

$$\sum_{w\in W}\sum_{t\in T(w)}\left|\sum_{z\in I(w,t)}\chi(z)\right| \geq \frac{1}{2}\eta Q$$

or:

$$\sum_{w\in W}\sum_{t\notin T(w)}\left|\sum_{z\in I(w,t)}\chi(z)\right| \geq \frac{1}{2}\eta Q$$

Case I: Main Term Wins

In the first case:

- Total number of $I(w,t)$'s is, by the definition of $T(w)$'s,

$$\# \leq Qw_2$$

- Therefore: for any M, there is a collection $\mathcal{I}$ of I's, of size M s.t:

$$\sum_{I(w,t)\in\mathcal{I}} \left| \sum_{z\in I(w,t)} \chi(z) \right| \geq \frac{\eta Q}{2} \times \frac{M}{Qw_2} = \frac{\eta M}{2w_2}$$

Case II: Error Term Wins

In the second case:

$$\sum_{w\in W}\sum_{t\notin T(w)}\left|\sum_{z\in I(w,t)}\chi(z)\right| \geq \frac{1}{2}\eta Q,$$

Recall the remark from the last lemma:

For every $w \in W$:

$$\sum_{t\notin T(w)} N(w,t) \leq Q$$

Using that, we can show:

There is a $\mathcal{I} \subset \{I(w,t) \mid t \notin T(w)\}$ and a constant $C \geq 1$ with

$$\#\mathcal{I} \leq 10Q^2C^{-2} \quad \text{and} \quad \sum_{I(w,t)\in\mathcal{I}}\left|\sum_{z\in I(w,t)}\chi(z)\right| \geq \frac{\frac{1}{2}\eta Q}{50C\log Q}$$

Conclusion

Combining our estimates, and optimizing the parameters Q, M, h, w_1 we get the required result:

Theorem 1 (Burgess, 1962)

For N, H, r positive integers:

$$|S_H(N)| \ll H^{1-1/r} p^{(r+1)/4r^2} \log p$$

with the implied constant being absolute.