Fast methods to compute the Riemann zeta function

Ghaith Hiary

University of Bristol

A general L-function

An L-function can be represented as a Dirichlet series:

$$L(s) := \prod_p L_p(p^{-s})^{-1} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \qquad \sigma > 1\,.$$

Define:

$$\Lambda(s) := \gamma(s)L(s)\,, \quad \gamma(s) := Q^{s/2} \prod_{j=1}^{d} \Gamma(s/2 + \mu_j)\,.$$

For a certain choice of Q and μ_j, $\Lambda(s)$ has:

- a meromorphic continuation with a finite number of poles (typically none),
- a functional equation: $\Lambda(s) = \omega\overline{\Lambda(1-\overline{s})}$.

Approximate functional equation

In computing $L(s)$, with $s = \sigma + it$, using an approximate functional equation, the majority of the effort is exerted on the **main sum**:

$$\sum_{n=1}^{N} \frac{a_n}{n^s} v_1(n,s) + \omega \sum_{n=1}^{N} \frac{\overline{a}_n}{n^{1-s}} v_2(n, 1-s)\,, \qquad N \approx \sqrt{Q|t|^d}\,.$$

By finding faster methods to compute the main sum, one obtains faster methods for $L(s)$.

Q. How fast can the main sum be computed?

• Alternative approaches for computing $L(s)$: shifted contour integral, explicit formula.

Approximating $L(s)$ by a single Dirichlet polynomial

Appoximating zeta under the Lindelöf hypothesis: Let $\epsilon, \delta > 0$, then for $\sigma = 1/2 + \epsilon$ and $N \gg T^{\delta}$, as $T \to \infty$:

$$L(\sigma + it) = \sum_{n \leq N} \frac{a_n(N)}{n^s} + N^{-\epsilon + o(1)}.$$

A result of Bombieri and Friedlander: Let $\epsilon, \epsilon' > 0$, suppose for $\sigma = 1/2 - \epsilon$ and $T \leq t \leq 2T$, as $T \to \infty$:

$$L(\sigma + it) = \sum_{n \leq N} \frac{a_n(N)}{n^s} + O(T^{-\epsilon'}),$$

then under certain natural conditions on L and $a_n(N)$, we have $N \gg T^{d - o(1)}$, where d is the "degree".

Fast methods for the zeta function

Theorem 1. (H.)

For any λ, $\zeta(\sigma + it)$ can be computed to within $\pm|t|^{-\lambda}$ in $t^{1/3+o_\lambda(1)}$ time.

Theorem 2. (H.)

For any λ, $\zeta(\sigma + it)$ can be computed to within $\pm|t|^{-\lambda}$ in $t^{4/13+o_\lambda(1)}$ time. (Notice $4/13 \approx 0.307$).

Also, a method for $L(s, \chi)$ with χ a character to a highly composite modulus.

The $t^{1/3+o_\lambda(1)}$ method for $\zeta(\sigma + it)$ has been implemented (jointly with J.W. Bober).

A survey and example applications

A brief survey:

- Zeta: Euler-Maclaurin formula, Riemann-Siegel formula, Odlyzko, Schönhage, Turing, Heath-Brown, Rubinstein, Paris, Berry and Keating, ...
- Dirichlet L-functions: Davies, Deuring, Hejhal, Rumely, ...
- Higher degree L-function: approximate functional equation, Rubinstein, Booker, Dokchitser, Vishe ...
- Coefficients and eigenvalues: quadratic reciprocity, Schoof's algorithm (and generalizations), Hejhal's algorithm, ...

Faster methods for $L(s)$ can be used to numerically verify the Riemann hypothesis, compute values at special points, study empirical rate of growth of $|L(1/2+it)|$, extreme behaviors of $L(s)$, ...

The Riemann-Siegel formula

Riemann derived a formula for computing zeta.

He used it to compute the first few complex zeta zeros.

Formula was later (1932) found by Siegel in old notes of Riemann.

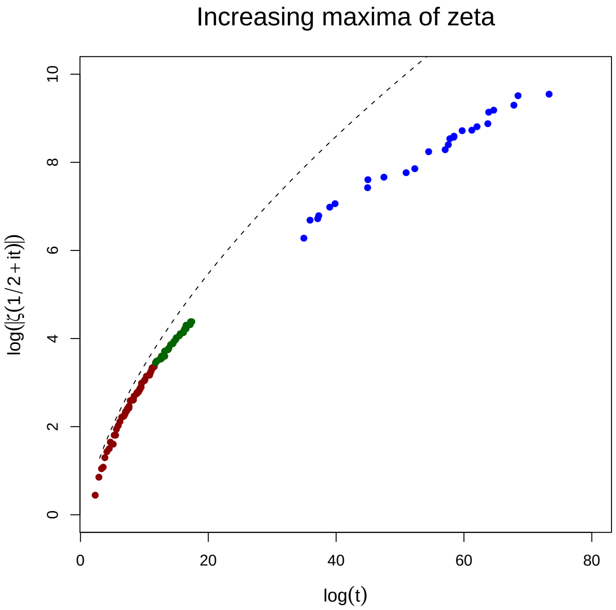
On the critical line ($\sigma = 1/2$):

$$\vartheta(t) := \arg \pi^{-it/2}\,\Gamma(1/4 + it/2)\,,$$
$$Z(t) := e^{i\vartheta(t)}\zeta(1/2 + it)\,.$$

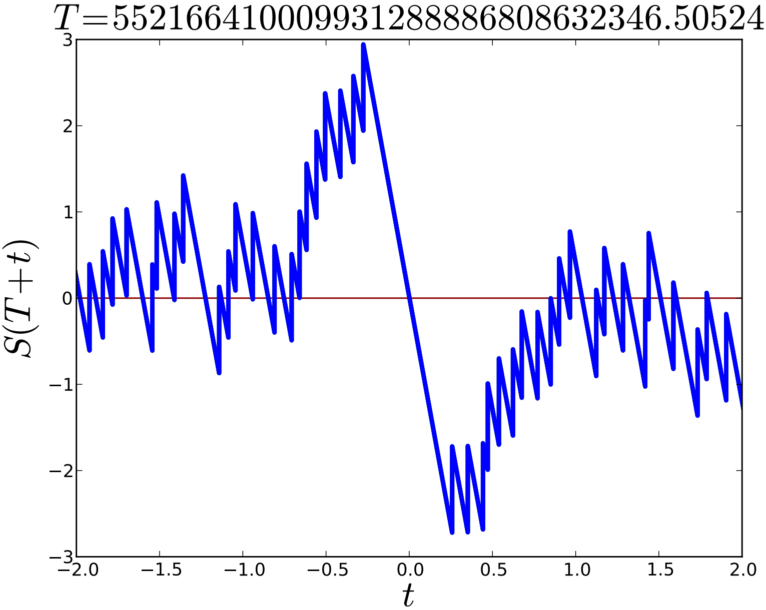
Then $Z(t)$ is real, $|Z(t)| = |\zeta(1/2 + it)|$, and

$$Z(t) = 2 \sum_{1 \le n \le \sqrt{t/2\pi}} \frac{\cos(t \log n - \vartheta(t))}{\sqrt{n}} + \textit{ remainder terms}\,.$$

Example 1: growth of $|\zeta(1/2+it)|$



Example 2: $S(t)$ near a large value of zeta



Some generalities

The basic idea:

1. Reduce to computing a large number of quadratic, or cubic, exponential sums.

2. **Intervene** to suitably normalizes the arguments of the quadratic, or cubic, sum.

3. Apply van der Corput iteration to obtain a **shorter** sum of a **similar type**, and compute the resulting **remainder**.

4. Repeat steps 2 and 3.

The following computational model suffices:

- *Compute*: numerically eval. to within $\pm|t|^{-\lambda}$ for any $\lambda > 0$.
- *Complexity (time)*: # of required operations: $+$, $-$, $\times$, $/$.
- *Arithmetic*: $\log(2 + \lambda + |t|)$ bits $\Rightarrow$ bit bound.

Main sum for $\zeta(\sigma + it)$: reducing to exponential sums

The main sum for $\zeta(\sigma + it)$ is $\displaystyle\sum_{1 \le n \ll t^{1/2}} n^{-\sigma - it}$.

The initial sum $\displaystyle\sum_{1 \le n \ll t^{\alpha}} n^{-\sigma - it}$ is evaluated directy.

The remaining sum is divided into "blocks":

$$\sum_{t^{\alpha} \ll n \ll t^{1/2}} n^{-\sigma - it} = \sum_{v \in \mathcal{V}_t} \sum_{n=v}^{v+K_v} n^{-\sigma - it}, \qquad K_v / v \approx t^{-\alpha}.$$

So $|\mathcal{V}_t| \ll t^{\alpha} \log t$.

Main sum for $\zeta(\sigma + it)$: reducing to exponential sums

$$\sum_{n=v}^{v+K} n^{-\sigma-it} = e^{-(\sigma+it)\log v} \sum_{k=0}^{K} e^{-(\sigma+it)\log(1+k/v)}$$
$$= \sum_{j=0}^{J} \frac{w_j}{K^j} \sum_{k=0}^{K} k^j e^{2\pi i f(k)} + \epsilon_J \,.$$

- total # of blocks $\ll t^{\alpha} \log t$.
- $K/v \ll t^{-\alpha}$.
- the degree of $f(x)$ is $\lceil 1/\alpha \rceil - 1$.

$1/3 \le \alpha < 1/2$	$f(x)$ is quadratic	$t^{1/3} \ll \#$ blocks $\ll t^{1/2}$
$1/4 \le \alpha < 1/3$	$f(x)$ is cubic	$t^{1/3} \ll \#$ blocks $\ll t^{1/4}$
$\vdots$		

Want fast methods to compute such exponential sums.

The quadratic case ($\alpha = 1/3$): zeta in $t^{1/3+o_\lambda(1)}$

We can write the main sum as a linear combintation of $\ll t^{1/3}\log^2 t$ quadratic (theta) sums:

$$F(K, j; a, b) := \frac{1}{K^j}\sum_{k=0}^{K} k^j e^{2\pi i a k + 2\pi i b k^2},$$

The θ-algorithm: $F(K, j; a, b)$ can be computed to within $\pm\epsilon$ in $\ll (j+1)^2 \log^2(K/\epsilon)$ time.

This yields zeta in $t^{1/3+o_\lambda(1)}$.

Classical: incomplete Gauss sums, partial theta sums

Define $F(K;a,b) := \sum_{k=0}^{K} e^{2\pi iak+2\pi ibk^2}$.

Partial theta sums studied extensively via Poisson summation.

Special cases:

- $F(K;a,0)$ is easy $\rightarrow$ Geometric Sum.
- If $bK \ll 1 \rightarrow$ use Euler-Maclaurin summation.
- If $F\left(K;m/K,n/K\right) \rightarrow$ complete Gauss sum.

Remark: Quadratic reciprocity implies that $F(K;a,b)$ is computable in poly-log time for $(a,b) = (m/K, n/K)$. The θ-algorithm implies $F(K;a,b)$ is still computable in poly-log time for any $a, b \in [0,1)$.

The basic iteration: the case $j = 0$

$$F(K; a, b) = \frac{c_1}{\sqrt{b}} F\left(\lfloor a + 2bK \rfloor; \frac{a}{2b}, -\frac{1}{4b}\right) + \mathcal{R}\,.$$

- Intervention:

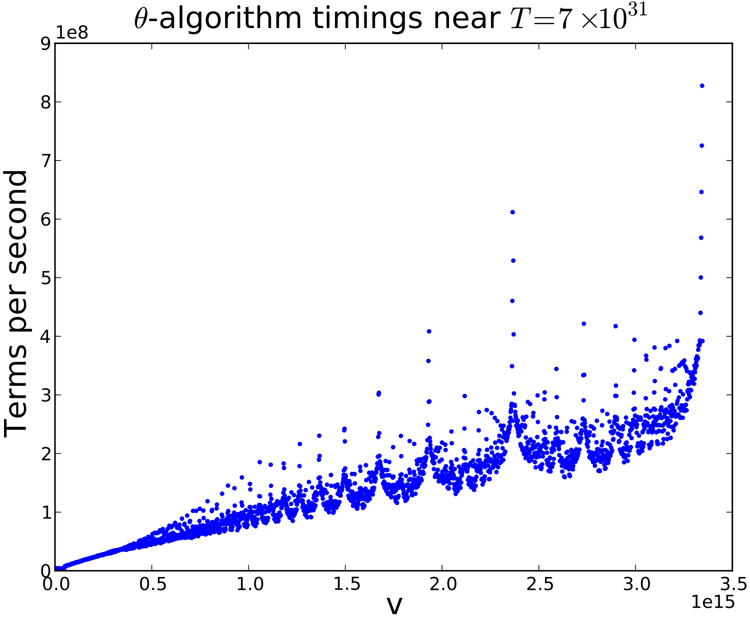
$$\begin{aligned} F(K; a, b) &= F(K; a \pm 1; b) = F(K; a, b \pm 1) \\ &= F(K; a \pm 1/2, b \pm 1/2)\,. \end{aligned}$$

$\Rightarrow$ can ensure $b \in [0, 1/4] \Rightarrow 2bK \leq K/2$.

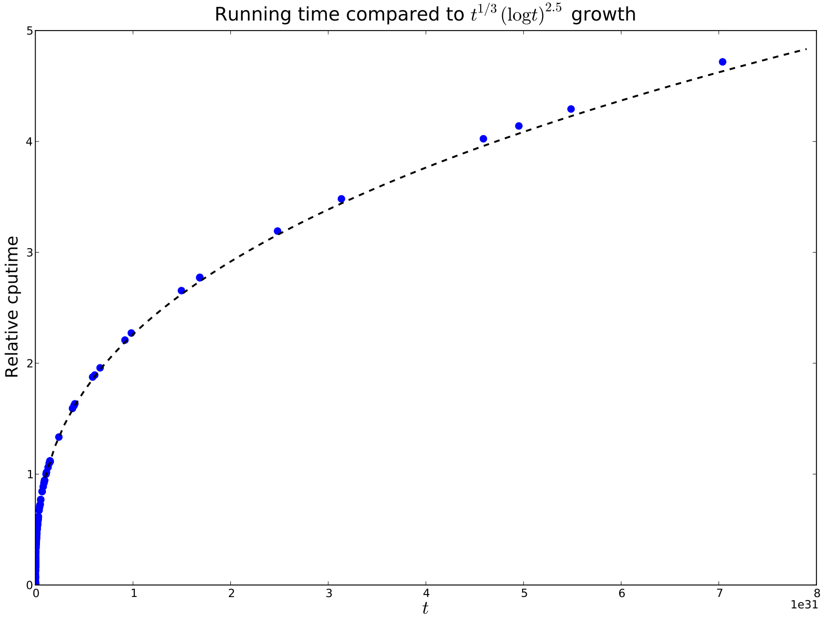
So with each iteration the length decreases by at least 1/2.

- Computing the remainder: no saddle-points, Cauchy's theorem, stationary phase, exponential decline, truncate after distance $\ll \log(K/\epsilon)$, reduce to a simple type of incomplete Gamma function. This is the time consuming part.

Numerical behavior of the θ-algorithm



Zeta algorithm timings



Faster methods: the cubic sums algorithm

$$H(K,j;a,b,c) := \frac{1}{K^j}\sum_{k=0}^{K} k^j e^{2\pi iak+2\pi ibk^2+2\pi ick^3}$$

Still have periodicity, but not self-similarity..

Special cases:

- If $bK \ll 1$ and $cK^2 \ll 1 \to$ Euler-Maclaurin summation.
- If $cK^3 \ll 1 \to \theta$-algorithm.

Cubic sums algorithm. Given $\mu \le 1$, then for any $0 \le c \le K^{\mu-3}$:

- the cubic sum $H(K,j;a,b,c)$ can be computed to within $\pm\,\epsilon$ in $\ll (j+1)^5 \log^5(K/\epsilon)$ time,
- provided a one-time precomputation costing $\ll (j+1)^5 \log^5(K/\epsilon) K^{4\mu}$ time is performed via the FFT.

The key observation is the precomputation costs $\approx K^{4\mu}$ time.

A heuristic device: the case $j = 0$, $a = 0$

van der Corput iteration

$f'(x)$ strictly increasing in $0 \leq x \leq K$, and x_m is defined by $f'(x_m) = m$ for $f'(0) < m < f'(k)$:

$$\sum_{0<k<K} e^{2\pi i f(k)} = c_1 \sum_{f'(0)<m<f'(k)} \frac{e^{2\pi i (f(x_m) - m x_m)}}{\sqrt{|f''(x_m)|}} + \mathcal{R}\,.$$

- Consider $\sum_{k=0}^{K} e^{2\pi i b k^2 + 2\pi i c k^3}$.
- For $m \in (0, 2bK + 3cK^2)$, we have:

$$f(x_m) - m x_m = \frac{2b^3 + 9bcm - 2\left(b^2 + 3cm\right)^{3/2}}{27c^3}\,.$$

This is not a cubic... but what if c is small?

“Approximate self-similarity”

Assuming $cK^2 \ll 1$, and $bK \geq 1$, then

$$f(x_m) - mx_m = -\frac{1}{4b}m^2 + \frac{c}{8b^3}m^3 + O\left(\frac{c^2K^4}{b}\right).$$

If $c^2K^4/b \ll 1 \Rightarrow$ can make new sum cubic.

Thus, the van der Corput iteration suggests:

- K terms $\to 2bK + 3cK^2 = 2bK + O(1)$ terms.
- $bk^2 + ck^3 \to -\frac{1}{4b}m^2 + \frac{c}{8b^3}m^3 + O\left(\frac{c^2K^4}{b}\right)$.

Can ensure $b \in [0, 1/4]$, so length decreases by a factor of $\leq 1/2$.

But also, since $c \to c/(8b^3) \geq 8c$, the cubic coeff. c grows.

Character sums

Let χ be a Dirichlet character mod q. Define:

$$S(K,\chi) := \sum_{k=1}^{K} \chi(k)$$

Q. How fast can $S(K,\chi)$ be computed?

A.G. Postnikov, 1955

χ primitive mod p^a (p odd) $\Rightarrow \chi(1+kp^b) \equiv e^{2\pi i f(k)}$, $f(x) \in \mathbb{Q}[x]$.

Lemma 1.

χ mod p^a (p odd), $b := \lceil a/3 \rceil$, then

$$\chi(1+p^b k) \equiv \exp\left(\frac{4\pi i L k}{p^{a-b}} + \frac{2\pi i L k^2}{p^{a-2b}}\right),$$

and L can be determined in $O(\log p)$ time.

Twisted quadratic sums and $L(s, \chi)$

Using lemma 1, we can write:

$$S(K, \chi) = \sum_{\substack{0 < r < p^{\lceil a/3 \rceil} \\ \gcd(r,p)=1}} \chi(r) F(K/p^{\lceil a/3 \rceil}; a_r, b_r)\,.$$

Via the θ-algorithm, $S(K, \chi)$ can be computed in $\approx p^{\lceil a/3 \rceil}$ steps.

Example. $q = p^3$, χ mod $q \Rightarrow S(K, \chi)$ in $pq^{\epsilon} = q^{1/3+\epsilon}$ steps.

Example. $q = p^a$, χ mod $q \Rightarrow$ improves on $q^{1/2}$ unless $a = 1, 2, 4$.

Let $q = p_1^{a_1} p_2^{a_2} \ldots p_h^{a_h}$ (p's odd), and χ be a character mod $q \Rightarrow$ $S(K, \chi)$ is computable in $p_1^{\lceil a_1/3 \rceil} p_2^{\lceil a_2/3 \rceil} \ldots p_h^{\lceil a_h/3 \rceil} q^{\epsilon}$ steps.

The approach generalizes to $\sum_{k=1}^{K} (k/K)^j \chi(k) e^{2\pi i a k + 2\pi i b k^2}$. Gives $L(s, \chi)$ in better than $q^{1/2} t^{1/2}$, best case $q^{1/3} t^{1/3}$.