Recovering short generators via negative moments of Dirichlet L-functions

Iu-iong Ng and Yuichiro Toma

Graduate School of Mathematics, Nagoya University

arXiv: 2405.13420

Overview of our main result

For the basis $\mathbf{b}_j$ of the log-cyclotomic-unit lattice of a q-th cyclotomic field, Cramer, Ducas, Peikert, and Regev (EUROCRYPT'16) gave an upper bound $\|\mathbf{b}_j^\vee\|^2 \le 4\,|G|^{-1} \cdot \sum_{\chi \in \hat{G}\setminus\{1\}} f_\chi^{-1}\,|L(1,\chi)|^{-2}$ on the dual basis.

We improve this bound and its application of recovering short generators.

	This work	CDPR16
$\|\mathbf{b}_j^\vee\|^2$ when q is a prime number and under the GRH	$= \frac{4\zeta(2)}{\zeta(4)}\frac{1}{q}\left(1 + O\left(q^{-1+\varepsilon}\right)\right)$	$\le 4C_L^2\frac{(\log\log q)^2}{q}(1+o(1))$
Application: the lower bound $1-(q-3)e^{-t/2}$ on the success probability of the short generator algorithm	$t = \Theta\left(\sqrt{q}\right)$	$t = \Omega\left(\frac{\sqrt{q}}{\log\log q}\right)$

Our approach (assuming the GRH)

Instead of using the bound $\frac{1}{C_L \log\log q} \le L(1,\chi) \le C_L \log\log q$, we directly calculate the negative $2k$-th moments for any positive integer q.

Theorem (the asymptotic behaviour of the negative moment)

Let χ be a Dirichlet character modulo q and let k be a positive integer. Under the GRH, we have

$$\sum_{\substack{\chi\neq\chi_0\\ \chi(-1)=1}} \frac{1}{|L(1,\chi)|^{2k}} = \frac{C(k)}{2}\varphi(q)\prod_{p|q}\left(1+\frac{\binom{k}{1}^2}{p^2}+\cdots+\frac{\binom{k}{k}^2}{p^{2k}}\right)^{-1}\left(1+O\left(q^{-1+\varepsilon}\right)\right),$$

where $C(k) = \prod_p \left(1+\frac{\binom{k}{1}^2}{p^2}+\cdots+\frac{\binom{k}{k}^2}{p^{2k}}\right)$.

To prove the theorem, we bound the Mertens function in arithmetic progression.