Errata of the PhD thesis
'Random Walks on Arakelov Class Groups'

Koen de Boer

December 8, 2023

1 Introduction

2 Preliminaries

- Page 55, equation (2.11) should be

$$\rho_K = \lim_{s \to 1}(s-1)\zeta_K(s) = \frac{2^{n_{\mathbb{R}}} \cdot (2\pi)^{n_{\mathbb{C}}} \cdot R_K \cdot h_K}{|\mu_K| \cdot \sqrt{|\Delta_K|}},$$

  that is, with an additional equation sign '='.

3 The Continuous Hidden Subgroup Problem

- Page 124, Theorem 3.26, the inequality involving γ on the second line of the theorem should read,

$$\|\Delta_G\|_\infty < \gamma < \frac{\lambda_1^* \cdot \det(\Lambda^*)}{2^{O(km)} \cdot \|\tilde{G}\|_\infty^m}$$

  that is, $\tilde{G}$ instead of $\tilde{G}^*$.

- The same theorem, page 124, Theorem 3.26, the inequality at the end of the theorem statement should read

$$\frac{2^{O(km)}\|\tilde{G}\|_\infty^{m+1}}{\lambda_1^* \cdot \det(\Lambda^*)} \cdot \gamma,$$

  that is, $\tilde{G}$ instead of $\tilde{G}^*$.

4 Random Walks on Arakelov Ray Class Groups

5 A Worst-case to Average-case Reduction for Ideal Lattices

6 Ideal Sampling

7 The Power Residue Symbol is in ZPP

- Page 262, Algorithm 9, the 'Ensure:' line should read:
  Ensure: $\left(\frac{\mathfrak{b}}{L/K}\right) \in \mathrm{Gal}(L/K)$, or failure.

8 Appendices

- Page 308, Lemma A.33 is wrong, as the inequality $|1-x| \leq |\ln(x)|$ is false. This impacts the following bounds, which will be reproven in the next section (with slightly weaker bounds).
  - Page 109, Lemma 3.15, the bound on
    $$\sum_{z\in\mathbb{Z}^m} |\rho_{\sqrt{2}/s}(x+z) - \rho_{\sqrt{2}/s}(y+z)|$$
  - Page 310, Lemma A.37, the bound on
    $$\|\mathcal{G}_{\Lambda,s,c} - \mathcal{G}_{\Lambda,s,\tilde{c}}\|_1$$
  - Page 310, Lemma A.38, the bound in (A.8) on
    $$\|\mathcal{G}_{\Lambda,s/\mathbf{t},c} - \mathcal{G}_{\Lambda,s,c}\|_1$$
  - Page 311, Lemma A.39, the bound on
    $$\|\mathcal{G}_{\Lambda,s/\mathbf{t}_0,c/\mathbf{t}_0} - \mathcal{G}_{\Lambda,s/\mathbf{t}_1,c/\mathbf{t}_1}\|_1,$$
    which is proven using Lemma A.38. Note that the original statement of Lemma A.39 is about
    $$\|\mathcal{G}_{\Lambda_0,s,c} - \mathcal{G}_{\Lambda_0,s/\mathbf{t},c/\mathbf{t}}\|_1,$$
    which is equivalent, using $\Lambda_0 = \mathbf{t}_0\Lambda$ and $\mathbf{t} = \mathbf{t}_1\mathbf{t}_0^{-1}$, but nonetheless a typographic error, since in the statement of Lemma A.39 no mention is made of the variables Λ_0 and $\mathbf{t}$.

Fixes of Lemma 3.15, Lemma A.37, Lemma A.38 and Lemma A.39

- Page 109, Lemma 3.15. The proof of this lemma is fixed by resorting to the reasoning in the original article [1, Step 2, p. 362], where the Lipschitz constant $\mathrm{Lip}(h|^{\mathbb{T}^m})$ is computed by means of derivatives. This then yields [1, Step 2, p. 362]
  $$\mathrm{Lip}(h|^{\mathbb{T}^m}) \leq s^{m/2}(2V\mathrm{Lip}(\mathbf{f}) + 2\pi s^2),$$
  where the extra V comes from the fact that in the original paper [1, §5.3] we will in the end instantiate all results with $f_V := f(V\cdot)$, whereas in the thesis, this instantiation already happened on Page 109.

We solve the remaining three issues by using [2, Lemma 2.3] (whose proof is in [3, §A.3]), which states

Lemma 1 ([2, Lemma 2.3])**.** *Let $L \subset \mathbb{R}^n$ be a full rank lattice, $\mathbf{S}_1, \mathbf{S}_2 \in \mathrm{GL}_n(\mathbb{R})$ be two invertible matrices and $\mathbf{c}_1, \mathbf{c}_2 \in \mathbb{R}^n$ be two vectors. If $\eta_{1/2}(\mathbf{S}_1^{-1}L), \eta_{1/2}(\mathbf{S}_2^{-1}L) \leq 1/2$, then it holds that*
$$\|\mathcal{G}_{L,\mathbf{S}_1,\mathbf{c}_1} - \mathcal{G}_{L,\mathbf{S}_2,\mathbf{c}_2}\|_1 \leq 4\sqrt{n}\left(\sqrt{\|\mathbf{S}_2^{-1}\mathbf{S}_1 - I_n\|} + \sqrt{\|\mathbf{S}_2^{-1}(\mathbf{c}_1 - \mathbf{c}_2)\|}\right).$$

- Page 310, Lemma A.37, by applying Lemma 1 the assumption changes into $s \geq 2\cdot\eta_\varepsilon(\Lambda)$ and the bound changes into
  $$\|\mathcal{G}_{\Lambda,s,c} - \mathcal{G}_{\Lambda,s,\tilde{c}}\|_1 \leq 4\sqrt{n/s}\cdot\sqrt{\|c-\tilde{c}\|},$$
  since $\eta_{1/2}(\Lambda/s) \leq \eta_\varepsilon(\Lambda/s) \leq 1/2$ by assumption.

- Page 310, Lemma A.38, by applying Lemma 1 the assumption changes into $s \geq 2 \cdot \eta_\varepsilon(\Lambda)$ and the bound changes into

$$\|\mathcal{G}_{\Lambda,s/\mathbf{t},c} - \mathcal{G}_{\Lambda,s,c}\|_1 \leq 4\sqrt{n}\sqrt{\|\mathbf{t}-1\|} \leq 4\sqrt{n}\sqrt{\delta}$$

- Page 311, Lemma A.39, by applying Lemma 1 the assumption changes into $s \geq 2 \cdot \max(\eta_\varepsilon(\mathbf{t}_0\Lambda), \eta_\varepsilon(\mathbf{t}_1\Lambda))$ and the bound changes into

$$\begin{aligned}
\|\mathcal{G}_{\Lambda,s/\mathbf{t}_0,c/\mathbf{t}_0} - \mathcal{G}_{\Lambda,s/\mathbf{t}_1,c/\mathbf{t}_1}\|_1 &\leq 4\sqrt{n}\left(\sqrt{\|\mathbf{t}_1\mathbf{t}_0^{-1} - I_n\|} + \sqrt{\frac{1}{s}\cdot\|\mathbf{t}_1(c/\mathbf{t}_0 - c/\mathbf{t}_1)\|}\right) \\
&\leq 4\sqrt{n}\left(\sqrt{\|\mathbf{t}_1\mathbf{t}_0^{-1} - 1\|} + \sqrt{\frac{1}{s}\|(\mathbf{t}_1\mathbf{t}_0^{-1} - I_n)c\|}\right) \\
&\leq 4\sqrt{n}\sqrt{\delta}(1 + \sqrt{\|c\|/s})
\end{aligned}$$

Implications of the change in the bounds

Summary

The implications of the change in the bounds are minor and only impact Lemma 5.19 and Lemma 5.20 in §5.5.4, the section about the closeness proofs (pp. 198-202). In Lemma 5.19 the bound on D should be quadratically increased. In Lemma 5.20 the discretization of the circle (k in definition 5.13) needs to be quadratically increased. Those two merely quadratic increases in discretization parameters have no impact on the polynomial runtime of the discretized algorithms in Chapter 5.

Rewritings of Lemma 5.19, Lemma 5.20

As Lemma A.38 only has an influence on Lemma A.39 (which is already fixed by Lemma 1), we consider only the implications of the change of bounds in Lemma A.37 and Lemma A.39. These lemmas only impact §5.5.4, the section about the closeness proofs (pp. 198-202).

More specifically, Lemma A.37 impacts the proof of Lemma 5.19 on page 200 and the proof of Lemma 5.20 on page 202. Lemma A.39 only impacts the proof of Lemma 5.19 on page 200.

For Lemma 5.20, the discretization on the circle (Definition 5.13) should be $k = \sqrt{n} \cdot M \cdot \lceil 1/(\varepsilon/n)^2 \rceil$. For this instantiation, we have that $\ddot{\mathcal{C}}_M$ is ϵ^2/n-close to the circle $\mathcal{C}_M$. Hence, the bound in (5.12) on page 202 can be replaced by

$$\leq 4\sqrt{n/\varsigma}\sqrt{\|c - \tilde{c}\|} \leq 4\varepsilon.$$

For Lemma 5.19, the bound on D should be $D \geq \lceil \max(2n^2M/\varepsilon^2, s^{-1}n^{3/2}/\varepsilon^2) \rceil$. Then equation (5.9) on page 200 should read

$$\|\mathcal{G}_{\mathfrak{p},\varsigma/e^y,c} - \mathcal{G}_{\mathfrak{p},\varsigma/\lfloor e^{\ddot{y}} \rceil,c}\| \leq 4\sqrt{n}\sqrt{\delta}(1 + \sqrt{\|c\|/\varsigma}),$$

with $\delta = \frac{2\sqrt{n}}{D} \geq \|y - \tilde{y}\|$ and $\|c\| = \sqrt{n}M$, hence, using $\varsigma \geq 1$ and $\sqrt{n}M \geq 1$,

$$\leq 4\sqrt{n}\sqrt{\frac{2\sqrt{n}}{D}}\left(1 + \sqrt{\sqrt{n}M/\varsigma}\right) \leq 4\sqrt{n}\sqrt{\frac{2nM}{D}} \leq 4\sqrt{n} \cdot \varepsilon/\sqrt{n} \leq 4\varepsilon.$$

And, then equation (5.10) on page 200 should read

$$4\varepsilon + \max_{y \in F_H} \|\mathcal{G}_{\frac{1}{D}\mathbb{Z}_H,s,y} - \mathcal{G}_{\frac{1}{D}\mathbb{Z}_H,s,0}\| \leq 4\varepsilon + 4\sqrt{n/s} \cdot \sqrt{\|y\|} \leq 4\varepsilon + 4\sqrt{n/s}\sqrt{\frac{\sqrt{n}}{D}}$$
$$\leq 4\varepsilon + 4\sqrt{n/s}\sqrt{\varepsilon^2 s/n} \leq 8\varepsilon$$

Hence, Lemma 5.19 reads the same result, with the sole difference the lower bound on $D \geq \lceil \max(2n^2 M/\varepsilon^2, s^{-1}n^{3/2}/\varepsilon^2) \rceil$. Also, Lemma 5.20 reads the same result, but instead the discretization of the circle should use $k = \sqrt{n} \cdot M \cdot \lceil 1/(\varepsilon/n)^2 \rceil$.

Since these are only quadratic increases, the overall polynomial run time of these discretizations is not impacted.

References

[1] K. de Boer, L. Ducas, and S. Fehr. On the quantum complexity of the continuous hidden subgroup problem. In A. Canteaut and Y. Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020*, pages 341–370, Cham, 2020. Springer International Publishing.

[2] A. Pellet-Mary and D. Stehlé. On the hardness of the ntru problem. In M. Tibouchi and H. Wang, editors, *Advances in Cryptology – ASIACRYPT 2021*, pages 3–35, Cham, 2021. Springer International Publishing.

[3] A. Pellet-Mary and D. Stehlé. On the hardness of the ntru problem. Cryptology ePrint Archive, Paper 2021/821, 2021. `https://eprint.iacr.org/2021/821`.