Random walks on Arakelov class groups

Boer, K. de

Bibliography

[AC49] N. Ankeny and S. Chowla. “The class number of the cyclotomic field.” In: *Proceedings of the National Academy of Sciences of the United States of America* 35.9 (1949), pp. 529–532 (cit. on p. 290).

[Bac90] E. Bach. “Explicit bounds for primality testing and related problems.” In: *Mathematics of Computation* 55 (1990), pp. 355–380 (cit. on p. 162).

[Ban93] W. Banaszczyk. “New bounds in some transference theorems in the geometry of numbers.” In: *Mathematische Annalen* 296.4 (1993), pp. 625–636 (cit. on pp. 77, 86).

[BCP97] W. Bosma, J. Cannon, and C. Playoust. “The Magma algebra system. I. The user language.” In: *Journal of Symbolic Computation* 24.3-4 (1997), pp. 235–265 (cit. on p. 204).

[BDF20] K. de Boer, L. Ducas, and S. Fehr. “On the quantum complexity of the continuous hidden subgroup problem.” In: *EUROCRYPT*. Springer International Publishing, 2020, pp. 341–370 (cit. on p. 38).

[BF14] J.-F. Biasse and C. Fieker. “Subexponential class group and unit group computation in large degree number fields.” In: *LMS Journal of Computation and Mathematics* 17.A (2014), pp. 385–403 (cit. on pp. 134, 204–207).

[Bha+20] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, and Y. Zhao. "Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves." In: *Journal of the American Mathematical Society* 33.4 (Oct. 2020), pp. 1087–1099 (cit. on pp. 76, 282).

[Bia+17] J.-F. Biasse, T. Espitau, P.-A. Fouque, A. Gélin, and P. Kirchner. "Computing generator in cyclotomic integer rings." In: *EUROCRYPT*. Springer. 2017, pp. 60–88 (cit. on p. 134).

[BK96] J. Buchmann and V. Kessler. "Computing a reduced lattice basis from a generating system." In: *Unpublished Manuscript* (Aug. 1996) (cit. on pp. 83, 88, 95, 96, 124, 125).

[BKK17] L. Beilina, E. Karchevskii, and M. Karchevskii. *Numerical linear algebra: theory and applications*. Springer, Sept. 2017 (cit. on p. 126).

[Boe+20] K. de Boer, L. Ducas, A. Pellet-Mary, and B. Wesolowski. "Random self-reducibility of Ideal-SVP via Arakelov random walks." In: *CRYPTO*. Springer International Publishing, 2020, pp. 243–273 (cit. on p. 39).

[Boe16] K. de Boer. "Computing the Power Residue Symbol." Available at: `http://koendeboer.com/publication/masterthesis/masterthesis_deBoer.pdf`. MA thesis. Radboud Universiteit Nijmegen, The Netherlands, 2016 (cit. on pp. 236–238, 256, 259).

[Boe17] K. de Boer. *An implementation of the power residue symbol algorithm*. Available online at: `https://github.com/kodebro/powerresiduesymbol`. 2017 (cit. on p. 237).

[Bou21] J. Bouw. "On the computation of norm residue symbols." PhD thesis. Universiteit Leiden, The Netherlands, 2021 (cit. on pp. 237, 261).

[BP17] K. de Boer and C. Pagano. "Calculating the power residue symbol and ibeta." In: *ISSAC*. Vol. 68. 2017, pp. 923–934 (cit. on pp. 134, 204, 206, 236–238, 256, 259).

[BP89] J. Buchmann and M. Pohst. "Computing a lattice basis from a system of generating vectors." In: *Proceedings of the European Conference on Computer Algebra*. EUROCAL '87. London, UK: Springer-Verlag, 1989, pp. 54–63 (cit. on pp. 95, 96, 123).

[BPR04] J. Buhler, C. Pomerance, and L. Robertson. "Heuristics for class numbers of prime-power real cyclotomic fields," in: *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*. Fields Institute Communications. Amer. Math. Soc., 2004, pp. 149–157 (cit. on p. 55).

[Bre10] R. P. Brent. "Multiple-precision zero-finding methods and the complexity of elementary function evaluation." In: *CoRR* abs /1004.3412 (2010) (cit. on p. 307).

[BS16] J.-F. Biasse and F. Song. "Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields." In: *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*. SIAM. 2016, pp. 893–902 (cit. on pp. 83, 86, 89, 166, 170).

[BS96] E. Bach and J. O. Shallit. *Algorithmic number theory: efficient algorithms*. Vol. 1. MIT press, 1996 (cit. on p. 57).

[Buc88] J. Buchmann. "A subexponential algorithm for the determination of class groups and regulators of algebraic number fields." In: *Séminaire de Théorie des Nombres, Paris* 1989 (1988), pp. 28–41 (cit. on pp. 204–207).

[Cas12] J. Cassels. *An introduction to the geometry of numbers*. Classics in Mathematics. Springer Berlin Heidelberg, 2012 (cit. on p. 282).

[CDW17] R. Cramer, L. Ducas, and B. Wesolowski. "Short stickelberger class relations and application to Ideal-SVP." In: *EUROCRYPT*. Springer. 2017, pp. 324–348 (cit. on pp. 86, 89, 168–170).

[CF10] J. Cassels and A. Fröhlich. *Algebraic number theory: proceedings of an instructional conference organized by the london mathematical society (a nato advanced study institute) with the support* *of the international mathematical union*. London Mathematical Society, 2010 (cit. on p. 240).

[CG05] H. Cohen and G. Gras. *Class field theory: from theory to practice*. Springer Monographs in Mathematics. Springer Berlin Heidelberg, 2005 (cit. on p. 240).

[Chi08] N. Childress. *Class field theory*. Universitext. Springer New York, 2008 (cit. on pp. 63, 240).

[Coh93] H. Cohen. *A course in computational algebraic number theory*. Springer, 1993 (cit. on p. 239).

[Coh99] H. Cohen. *Advanced topics in computational number theory*. Graduate Texts in Mathematics. Springer New York, 1999 (cit. on pp. 195, 231, 243, 248, 249).

[Cra+16] R. Cramer, L. Ducas, C. Peikert, and O. Regev. "Recovering short generators of principal ideals in cyclotomic rings." In: *EUROCRYPT*. Springer. 2016, pp. 559–585 (cit. on pp. 36, 86, 89, 168, 170, 188).

[CS08] H. Cohen and P. Stevenhagen. *Computational class field theory*. 2008 (cit. on pp. 204, 231, 240, 260).

[CS10] P. C. Caranay and R. Scheidler. "An efficient seventh power residue symbol algorithm." In: *International Journal of Number Theory* 6.08 (2010), pp. 1831–1853 (cit. on p. 236).

[CSV12] X. Chang, D. Stehlé, and G. Villard. "Perturbation analysis of the QR factor R in the context of LLL lattice basis reduction." In: *Math. comput.* 81.279 (2012), pp. 1487–1511 (cit. on pp. 95, 125, 126).

[CT06] T. M. Cover and J. A. Thomas. *Elements of information theory 2nd edition (wiley series in telecommunications and signal processing)*. Wiley-Interscience, July 2006 (cit. on p. 185).

[DE16] A. Deitmar and S. Echterhoff. *Principles of harmonic analysis*. 2nd. Springer Publishing Company, Incorporated, 2016 (cit. on pp. 42, 44, 46, 49, 66, 155, 158).

[DF05] I. B. Damgård and G. S. Frandsen. "Efficient algorithms for the gcd and cubic residuosity in the ring of Eisenstein integers." In: *Journal of Symbolic Computation* 39.6 (2005), pp. 643–652 (cit. on p. 236).

[Dob79] E. Dobrowolski. "On a question of Lehmer and the number of irreducible factors of a polynomial." In: *Acta Arithmetica* 34.4 (1979), pp. 391–401 (cit. on pp. 187, 188).

[DPW19] L. Ducas, M. Plançon, and B. Wesolowski. "On the shortness of vectors to be found by the Ideal-SVP quantum algorithm." In: *CRYPTO*. Springer. 2019, pp. 322–351 (cit. on pp. 86, 169).

[Dus98] P. Dusart. "Autour de la fonction qui compte le nombre de nombres premiers." PhD thesis. l'Université de Limoges: l'Université de Limoges, May 1998 (cit. on pp. 284, 291).

[Eis+14] K. Eisenträger, S. Hallgren, A. Kitaev, and F. Song. "A quantum algorithm for computing the unit group of an arbitrary degree number field." In: *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*. ACM. 2014, pp. 293–302 (cit. on pp. 34, 35, 81–83, 85–89, 91, 94, 95, 166, 170).

[Gen09] C. Gentry. "A fully homomorphic encryption scheme." `crypto.stanford.edu/craig`. PhD thesis. Stanford University, 2009 (cit. on p. 170).

[Gen10] C. Gentry. "Toward basing fully homomorphic encryption on worst-case hardness." In: *Crypto*. 2010, pp. 116–137 (cit. on pp. 170, 171).

[GKP94] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete mathematics: a foundation for computer science*. 2nd. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc., 1994 (cit. on p. 119).

[GM15] L. Grenié and G. Molteni. "Explicit versions of the prime ideal theorem for Dedekind zeta functions under GRH." In: *Mathematics of Computation* 85.298 (Oct. 2015), pp. 889–906 (cit. on pp. 57, 58).

[GM84] S. Goldwasser and S. Micali. "Probabilistic encryption." In: *Journal of Computer and System Sciences* 28.2 (1984), pp. 270–299 (cit. on p. 236).

[GP01] J. von zur Gathen and D. Panario. "Factoring polynomials over finite fields: a survey." In: *Journal of Symbolic Computation* 31.1 (2001), pp. 3–17 (cit. on p. 59).

[GPV08] C. Gentry, C. Peikert, and V. Vaikuntanathan. "Trapdoors for hard lattices and new cryptographic constructions." In: *STOC*. 2008, pp. 197–206 (cit. on pp. 176, 195, 196).

[GR02] L. Grover and T. Rudolph. "Creating superpositions that correspond to efficiently integrable probability distributions." In: *arXiv preprint quant-ph/0208112* (2002) (cit. on pp. 88, 95, 300).

[Gut09] A. Gut. *An intermediate course in probability*. Springer Texts in Statistics. Springer New York, 2009 (cit. on p. 309).

[Hal05] S. Hallgren. "Fast quantum algorithms for computing the unit group and class group of a number field." In: *Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing*. ACM. 2005, pp. 468–474 (cit. on p. 85).

[Hal07] S. Hallgren. "Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem." In: *Journal of the ACM (JACM)* 54.1 (2007), p. 4 (cit. on p. 85).

[Hei04] J. Heinonen. *Lectures on Lipschitz analysis*. 2004 (cit. on p. 80).

[HH00] L. Hales and S. Hallgren. "An improved quantum Fourier transform algorithm and applications." In: *Proceedings 41st Annual Symposium on Foundations of Computer Science*. Nov. 2000, pp. 515–525 (cit. on pp. 87, 116).

[HM89] J. L. Hafner and K. S. McCurley. "A rigorous subexponential algorithm for computation of class groups." In: *Journal of the American Mathematical Society* 2.4 (1989), pp. 837–850 (cit. on p. 207).

[HM91] J. L. Hafner and K. S. McCurley. "Asymptotically fast triangularization of matrices over rings." In: *Siam journal on computing* 20.6 (1991), pp. 1068–1083 (cit. on p. 239).

[IKS04] H. Iwaniec, E. Kowalski, and A. M. Society. *Analytic number theory*. American Mathematical Society, 2004 (cit. on pp. 56, 144, 145, 152).

[JMV09] D. Jao, S. D. Miller, and R. Venkatesan. "Expander graphs based on GRH with an application to elliptic curve cryptography." In: *Journal of number theory* (2009) (cit. on pp. 133, 170).

[JW15] D. Jetchev and B. Wesolowski. "On graphs of isogenies of principally polarizable Abelian surfaces and the discrete logarithm problem." In: *Corr* abs/1506.00522 (2015) (cit. on pp. 133, 162, 170).

[Kes91] V. Kessler. "On the minimum of the unit lattice." In: *Séminaire de théorie des nombres de bordeaux* 3.2 (1991), pp. 377–380 (cit. on pp. 187, 188).

[Kle00] P. N. Klein. "Finding the closest lattice vector when it's unusually close." In: *Soda*. 2000, pp. 937–941 (cit. on pp. 176, 195).

[Koc97] H. Koch. *Algebraic number theory*. Ed. by A. Parshin and I. Shafarevich. Algebraic Number Theory v. 62. Springer Berlin Heidelberg, 1997 (cit. on p. 240).

[Kup05] G. Kuperberg. "A subexponential-time quantum algorithm for the dihedral hidden subgroup problem." In: *SIAM Journal on Computing* 35.1 (2005), pp. 170–188 (cit. on p. 84).

[KW08] A. Kitaev and W. A. Webb. "Wavefunction preparation and resampling using a quantum computer." In: *arXiv preprint arXiv:0801.0342* (2008) (cit. on pp. 82, 88, 95, 300, 302).

[Lan12] S. Lang. *Algebraic number theory*. Graduate Texts in Mathematics. Springer New York, 2012 (cit. on pp. 55, 145, 148).

[Lee+19] C. Lee, A. Pellet-Mary, D. Stehlé, and A. Wallet. "An LLL algorithm for module lattices." In: *ASIACRYPT*. Springer. 2019, pp. 59–90 (cit. on pp. 133, 166, 168).

[Lem00] F. Lemmermeyer. *Reciprocity laws: from Euler to Eisenstein.* Springer Monographs in Mathematics. Springer Berlin Heidelberg, 2000 (cit. on pp. 236, 240).

[Len95] H. W. Lenstra Jr. “Computing Jacobi symbols in algebraic number fields.” In: *Nieuw Archief voor Wiskunde* 13 (1995), pp. 421–426 (cit. on pp. 235, 236, 242).

[LL+93] A. K. Lenstra, H. W. Lenstra Jr., et al. *The development of the number field sieve.* Vol. 1554. Springer Science & Business Media, 1993 (cit. on p. 204).

[Lou00] S. Louboutin. “Explicit bounds for residues of Dedekind zeta functions, values of L-functions at s=1, and relative class numbers.” In: *Journal of Number Theory* (2000) (cit. on p. 65).

[ME98] M. Mosca and A. Ekert. “The hidden subgroup problem and eigenvalue estimation on a quantum computer.” In: *NASA International Conference on Quantum Computing and Quantum Communications.* Springer. 1998, pp. 174–188 (cit. on p. 84).

[Mic] D. Micciancio. *Lecture notes on lattice algorithms and applications.* Available at `http://cseweb.ucsd.edu/~daniele/classes.html`, last accessed 17 Oct 2014 (cit. on p. 76).

[Mil15] J. C. Miller. “Real cyclotomic fields of prime conductor and their class numbers.” In: *Math. comp.* 84.295 (2015), pp. 2459–2469 (cit. on p. 55).

[Min67] H. Minkowski. *Gesammelte abhandlungen.* Chelsea, New York, 1967 (cit. on p. 53).

[MR07] D. Micciancio and O. Regev. “Worst-case to average-case reductions based on Gaussian measures.” In: *Siam j. comput.* 37.1 (Apr. 2007), pp. 267–302 (cit. on pp. 77, 78, 86, 178, 188, 200, 309).

[MS18] S. D. Miller and N. Stephens-Davidowitz. “Generalizations of Banaszczyk’s transference theorems and tail bound.” In: *arXiv preprint arXiv:1802.05708* (2018) (cit. on p. 77).

[MV73] H. L. Montgomery and R. C. Vaughan. “The large sieve.” In: *Mathematika* 20.2 (1973), pp. 119–134 (cit. on p. 289).

[Nar04] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer Berlin Heidelberg, 2004 (cit. on p. 285).

[Nat17] National Institute of Standards and Technology. *Post-quantum cryptography standardization*. 2017 (cit. on p. 84).

[NC11] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information: 10th anniversary edition*. 10th. New York, NY, USA: Cambridge University Press, 2011 (cit. on pp. 44, 301, 304, 305).

[Neu85] J. Neukirch. *Class field theory*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 1985 (cit. on pp. 56, 237, 240, 260, 262).

[NS13] J. Neukirch and N. Schappacher. *Algebraic number theory*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2013 (cit. on pp. 1, 4, 53, 56, 65, 149, 152, 240).

[NS16] A. Neumaier and D. Stehlé. “Faster LLL-type reduction of lattice bases.” In: *Proceedings of the acm on international symposium on symbolic and algebraic computation*. 2016, pp. 373–380 (cit. on pp. 95, 231).

[Ove14] M. Overholt. *A course in analytic number theory*. Graduate Studies in Mathematics. American Mathematical Society, 2014 (cit. on p. 209).

[PAR19] *PARI/GP version* `2.11.2`. Available at `http://pari.math.u-bordeaux.fr/`. The PARI Group. Univ. Bordeaux, 2019 (cit. on p. 204).

[Pei16] C. Peikert. “A decade of lattice cryptography.” In: *Foundations and Trends in Theoretical Computer Science* 10.4 (2016), pp. 283–424 (cit. on p. 1).

[PHS19] A. Pellet-Mary, G. Hanrot, and D. Stehlé. "Approx-SVP in ideal lattices with pre-processing." In: *EUROCRYPT*. Springer. 2019, pp. 685–716 (cit. on pp. 86, 133, 166, 168, 169).

[RA08] M. Reiter and S. Arthur. *Fourier transform & Solobev spaces (lecture notes)*. Available at: https://www.mat.univie.ac.at/~stein/teaching/SoSem08/sobolev_fourier.pdf. 2008 (cit. on p. 80).

[Rab89] S. Rabinowitz. "The volume of an n-simplex with many equal edges." In: *Missouri Journal of Mathematical Sciences* 1 (Jan. 1989) (cit. on p. 279).

[Reg04a] O. Regev. *Lecture notes in 'lattices in computer science'*. Available at https://cims.nyu.edu/~regev/teaching/lattices_fall_2004/. Nov. 2004 (cit. on p. 122).

[Reg04b] O. Regev. "Quantum computation and lattice problems." In: *SIAM Journal on Computing* 33.3 (2004), pp. 738–760 (cit. on p. 84).

[Reg09] O. Regev. "On lattices, learning with errors, random linear codes, and cryptography." In: *J. ACM* 56.6 (2009). Preliminary version in STOC 2005, pp. 1–40 (cit. on p. 170).

[Sch08] R. Schoof. "Computing Arakelov class groups." In: *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*. Cambridge University Press. 2008, pp. 447–495 (cit. on pp. 1, 74, 132, 166, 207).

[Sch98] R. Scheidler. "A public-key cryptosystem using purely cubic fields." In: *Journal of Cryptology* 11.2 (1998), pp. 109–124 (cit. on p. 236).

[Ser77] J.-P. Serre. *Linear representations of finite groups*. Vol. 42. Graduate texts in mathematics. Springer, 1977, pp. I–X, 1–170 (cit. on p. 155).

[Sey87] M. Seysen. "A probabilistic factorization algorithm with quadratic forms of negative discriminant." In: *Mathematics of Computation* 48.178 (1987), pp. 757–780 (cit. on p. 207).

[Sho94] P. W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring." In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE. 1994, pp. 124–134 (cit. on pp. 84, 236).

[Sho95] V. Shoup. "A new polynomial factorization algorithm and its implementation." In: *Journal of symbolic computation* 20.4 (1995), pp. 363–397 (cit. on p. 59).

[SL96] A. Storjohann and G. Labahn. "Asymptotically fast computation of Hermite normal forms of integer matrices." In: *Proceedings of the 1996 international symposium on symbolic and algebraic computation*. ISSAC '96. Zurich, Switzerland: Association for Computing Machinery, 1996, pp. 259–266 (cit. on pp. 231, 239).

[Son13] F. Song. "Quantum computing: a cryptographic perspective." Available at: `https://etda.libraries.psu.edu/files/final_submissions/8820`. PhD thesis. The Pennsylvania State University, 2013 (cit. on p. 89).

[Squ97] D. Squirrel. *An algorithm for the power residue symbol*. 1997 (cit. on pp. 235, 236, 242, 246, 249).

[SV05] A. Schmidt and U. Vollmer. "Polynomial time quantum algorithm for the computation of the unit group of a number field." In: *Proceedings of the Thirty-seventh Annual ACM Sumposium on Theory of Computing*. ACM. 2005, pp. 475–480 (cit. on p. 85).

[SW95] R. Scheidler and H. C. Williams. "A public-key cryptosystem utilizing cyclotomic fields." In: *Designs, Codes and Cryptography* 6.2 (1995), pp. 117–131 (cit. on p. 236).

[Vil85] A. Villani. "Another note on the inclusion $L^p(\mu) \subset L^q(\mu)$." In: *The American Mathematical Monthly* 92.7 (1985), pp. 485–487 (cit. on p. 80).

[Was12] L. C. Washington. *Introduction to cyclotomic fields*. Vol. 83. Springer Science & Business Media, 2012 (cit. on pp. 187, 188).

[Wei02] A. Weilert. “Fast computation of the biquadratic residue symbol.” In: *Journal of Number Theory* 96.1 (2002), pp. 133–151 (cit. on p. 236).

[Wer07] D. Werner. *Funktionalanalysis*. Springer-Lehrbuch. Springer Berlin Heidelberg, 2007 (cit. on p. 80).

[Wes18] B. P. Wesolowski. “Arithmetic and geometric structures in cryptography.” PhD thesis. École Polytechnique Fédérale de Lausanne, Nov. 2018 (cit. on p. 144).

[Wil85] H. C. Williams. “An M^3 public-key encryption scheme.” In: *Conference on the Theory and Application of Cryptographic Techniques*. Springer. 1985, pp. 358–368 (cit. on p. 236).

[Yud76] V. A. Yudin. “The multidimensional Jackson theorem.” In: *Mathematical notes of the Academy of Sciences of the USSR* 20.3 (Sept. 1976), pp. 801–804 (cit. on pp. 52, 294, 295).

Appendix

Appendix A.

Appendix

A.1. Number-theoretic Computations

Lemma A.1. *The volume of the simplex* $S_\alpha = \{x \in \operatorname{Log} K_\mathbb{R} \mid x_\sigma \leq \alpha\,, \sum_\sigma x_\sigma = 0\}$ *for some* $\alpha > 0$ *is given by*

$$\operatorname{Vol}(S_\alpha) = \frac{(n\alpha)^{\mathbb{r}} \cdot \sqrt{n}}{\sqrt{2}^{n_\mathbb{C}} \cdot \mathbb{r}!},$$

where $\mathbb{r} = n_\mathbb{R} + n_\mathbb{C} - 1$.

Proof. Define $S'_\alpha = \{x \in \mathbb{R}^{\mathbb{r}+1} \mid \sum_\nu x_\nu = 0, x_\nu \leq \alpha$ for real places ν, $x_\nu \leq 2\alpha$ for complex $\nu\}$. The map

$$A : \mathbb{R}^{\mathbb{r}+1} \to \operatorname{Log} K_\mathbb{R},\, e_\nu \mapsto \begin{cases} e_{\sigma_\nu} & \text{when } \nu \text{ is real} \\ \frac{1}{2}(e_{\sigma_\nu} + e_{\overline{\sigma_\nu}}) & \text{when } \nu \text{ is complex} \end{cases}$$

sends S'_α to S_α bijectively. By applying on $S'_\alpha \subseteq \mathbb{R}^{\mathbb{r}+1}$ the translation $y_\sigma = \alpha - x_\sigma$ or $y_\sigma = 2\alpha - x_\sigma$ depending on whether σ is real or complex, one can see that it is a regular $\mathbb{r}$-simplex with edge length $\sqrt{2} \cdot n\alpha$. Therefore, the volume of S'_α equals $\frac{(n\alpha)^{\mathbb{r}}\sqrt{\mathbb{r}+1}}{\mathbb{r}!}$ [Rab89]. In order to compute the volume of S_α, we need to estimate how the linear map A scales the subspace $\{x \in \mathbb{R}^{\mathbb{r}+1} \mid \sum_\nu x_\nu = 0\}$. Therefore, we choose the basis $B = (e_1 - e_{\mathbb{r}+1}, \ldots, e_{\mathbb{r}} - e_{\mathbb{r}+1})$, and compute the scaling factor by means of taking the square root of the determinant of $(AB)^T AB$ and dividing it by the square root of the determinant of $B^T B$, i.e.,

$$\mathrm{Vol}(S_\alpha) = \frac{\sqrt{\det(B^T A^T AB)}}{\sqrt{\det(B^T B)}} \mathrm{Vol}(S'_\alpha).$$

By the Weinstein–Aronszajn identity, we obtain that $\det(B^T B) = \det(I + \mathbf{1} \cdot \mathbf{1}^T) = n_\mathbb{R} + n_\mathbb{C} = \mathbb{r} + 1$, where $\mathbf{1}$ is the all-one column vector of dimension $\mathbb{r} = n_\mathbb{R} + n_\mathbb{C} - 1$. Note that $A^T A = \mathrm{diag}(1, \ldots, 1, 1/2, \ldots, 1/2)$, where the 1 is repeated $n_\mathbb{R}$ times and the 1/2 is repeated $n_\mathbb{C}$ times. Therefore, $B^T A^T AB = J + \frac{1}{2}\mathbf{1} \cdot \mathbf{1}^T$, where $J = \mathrm{diag}(\underbrace{1, \ldots, 1}_{n_\mathbb{R}}, \underbrace{1/2, \ldots, 1/2}_{n_\mathbb{C}-1})$. Again using the Weinstein-Aronszajn identity, we obtain

$$\begin{aligned}\det(B^T A^T AB) &= \det(J + 1/2 \cdot \mathbf{1} \cdot \mathbf{1}^T) = \det(J)(1 + 1/2 \cdot \mathbf{1}^T J^{-1}\mathbf{1}) \\ &= 2^{-n_\mathbb{C}+1}(1 + 1/2(n_\mathbb{R} + 2n_\mathbb{C} - 2)) = 2^{-n_\mathbb{C}} \cdot n\end{aligned}$$

So, we conclude the argument by spelling out all formula's:

$$\mathrm{Vol}(S_\alpha) = \frac{2^{-n_\mathbb{C}}\sqrt{n}}{\sqrt{\mathbb{r}+1}} \mathrm{Vol}(S'_\alpha) = \frac{2^{-n_\mathbb{C}}\sqrt{n}}{\sqrt{\mathbb{r}+1}} \cdot \frac{(n\alpha)^\mathbb{r}\sqrt{\mathbb{r}+1}}{\mathbb{r}!} = \frac{(n\alpha)^\mathbb{r} \cdot \sqrt{n}}{\sqrt{2}^{n_\mathbb{C}} \cdot \mathbb{r}!}$$

□

Lemma A.2. *Let* $\mathrm{Log}\,\mathcal{O}_K^\times \subseteq H \subseteq \log K_\mathbb{R}$ *be the logarithmic unit lattice. Then the covolume of this lattice in* H *equals* $\sqrt{n} \cdot 2^{-n_\mathbb{C}/2} \cdot R$.

Proof. In the literature, often one uses the embedding $\mathrm{Log}'\,\mathcal{O}_K^\times \subseteq H' \subseteq \mathbb{R}^{n_\mathbb{R}+n_\mathbb{C}}$, where $(\mathrm{Log}'(\eta))_\sigma$ equals $\log|\sigma(\eta)|$ or $2\log|\sigma(\eta)|$, depending on whether σ is real or complex. The space $H' = \{x \in \mathbb{R}^{n_\mathbb{R}+n_\mathbb{C}} \mid \sum_j x_j = 0\}$ is the equivalent hyperplane. It is evident that the linear map

$$A : \mathbb{R}^{\mathbb{r}+1} \to \mathrm{Log}\,K_\mathbb{R},\, e_\nu \mapsto \begin{cases} e_{\sigma_\nu} & \text{when } \nu \text{ is real} \\ \frac{1}{2}(e_{\sigma_\nu} + e_{\overline{\sigma_\nu}}) & \text{when } \nu \text{ is complex} \end{cases}$$

maps $\mathrm{Log}'\,\mathcal{O}_K^\times \subseteq H'$ to $\mathrm{Log}\,\mathcal{O}_K^\times \subseteq H$.

Let $\underline{U}$ be a basis of $\operatorname{Log}' \mathcal{O}_K^\times$, and denote U by the same basis, but the last row removed; the determinant of U is called the regulator R of the number field K. Define $B : \mathbb{R}^{\mathfrak{r}} \to \mathbb{R}^{\mathfrak{r}+1}$, $e_j \mapsto e_j - e_{n_\mathbb{R}+n_\mathbb{C}}$. By the fact that for any element in $\operatorname{Log}' \mathcal{O}_K^\times$ holds that the sum of the entries equals zero, we have $BU = \underline{U}$. As A maps $\operatorname{Log}' \mathcal{O}_K^\times$ to $\operatorname{Log} \mathcal{O}_K^\times$, we obtain that ABU is a basis of $\operatorname{Log} \mathcal{O}_K^\times$. The covolume of this basis equals $\sqrt{\det(B^T A^T AB)} \det(U) = \sqrt{\det(B^T A^T AB)} R = \sqrt{n} 2^{-n_\mathbb{C}/2} R$.

The last equality is proven by the computation of $\det(B^T A^T AB)$ below. Note that $A^T A = \operatorname{diag}(1, \ldots, 1, 1/2, \ldots, 1/2)$, where the 1 is repeated $n_\mathbb{R}$ times and the $1/2$ is repeated $n_\mathbb{C}$ times. Therefore, $B^T A^T AB = J + \frac{1}{2}\mathbf{1} \cdot \mathbf{1}^T$, where

$$J = \operatorname{diag}(\underbrace{1, \ldots, 1}_{n_\mathbb{R}}, \underbrace{1/2, \ldots, 1/2}_{n_\mathbb{C}-1}).$$

and $\mathbf{1}$ is the all-one vector of dimension $\mathfrak{r}$. Using the Weinstein-Aronszajn identity, we obtain

$$\det(B^T A^T AB) = \det(J + 1/2 \cdot \mathbf{1} \cdot \mathbf{1}^T) = \det(J)(1 + 1/2 \cdot \mathbf{1}^T J^{-1} \mathbf{1})$$

$$= 2^{-n_\mathbb{C}+1}(1 + \frac{1}{2}(n_\mathbb{R} + 2n_C - 2)) = 2^{-n_\mathbb{C}} \cdot n$$

$\square$

Lemma A.3. *Let $H \subseteq \operatorname{Log}(K_\mathbb{R})$ be the hyperplane orthogonal to the all-one vector, and let $\rho_s^{(n)}$ be the Gaussian function. Then*

$$\int_{x \in H} s^{-\mathfrak{r}} \rho_s^{(n)}(x) dx = 1$$

Proof. Use the matrices A and B from the previous lemma to apply integration by substitution, observing that $H = AB\mathbb{R}^{\mathfrak{r}}$.

$$\int_{x \in AB\mathbb{R}^{\mathfrak{r}}} s^{-\mathfrak{r}} \rho_s^{(n)}(x) dx = \sqrt{\det(B^T A^T AB)} \int_{x \in \mathbb{R}^{\mathfrak{r}}} s^{-\mathfrak{r}} \rho_s^{(n)}(ABx) dx$$

$$= \sqrt{\det(D^T D)} \int_{x \in \mathbb{R}^{\mathfrak{r}}} s^{-\mathfrak{r}} e^{-\pi x^T D^T D x/s^2} dx = \int_{x \in \mathbb{R}^{\mathfrak{r}}} s^{-\mathfrak{r}} e^{-\pi x^T x/s^2} dx = 1$$

Where $D^T D = B^T A^T A B^T$ is the $\mathbb{r}$-dimensional Cholesky decomposition, and the last equality follows then again by integration by substitution. □

Theorem A.4 (Bhargava,Shankar,Taniguchi,Thorne,Tsimerman,Zhao)**.** *Let K be any number field of degree n and let $\mathcal{O}_K$ be its ring of integers. Let $\mathcal{O}_K \subseteq K_{\mathbb{R}}$ have the structure of a lattice via the Minkowski embedding (see Section 2.3), and denote $\lambda_j^\infty(\mathcal{O}_K)$ for the j-th successive minimum with respect to the infinity norm in $K_{\mathbb{R}}$. Then*

$$\lambda_n^\infty(\mathcal{O}_K) \leq |\Delta_K|^{1/n}.$$

The following proof is a copy of [Bha+20, Thm. 3.1], with the difference that it is applied to the infinity norm and has explicit constants everywhere.

Proof. Let $\alpha_j \in \mathcal{O}_K$ attain the successive minima for the infinity norm $\lambda_j^\infty(\mathcal{O}_K)$ for $j \in \{1, \ldots, n\}$, with $\alpha_1 = 1$. For any element $\beta \in \mathcal{O}_K$, we write $\beta = \sum_{j=1}^n [\beta]_j \alpha_j$, i.e., $[\beta]_j$ are the coordinates of β with respect to $(\alpha_1, \ldots, \alpha_n)$.

For $2 \leq k, \ell \leq n-1$ consider the $(n-2) \times (n-2)$-matrix $C = ([\alpha_k \alpha_\ell]_n)$, i.e., the matrix consisting of the coordinates of $\alpha_k \alpha_\ell$ with respect to α_n. We will show at the end of this proof that this is a non-degenerate matrix, implying that there are no zero rows or columns. In other words, there exists a permutation $\pi : \{2, \ldots, n-1\} \to \{2, \ldots, n-1\}$ such that $[\alpha_k \alpha_{\pi(k)}]_n \neq 0$ for all $k \in \{2, \ldots, n-1\}$.

So, the product $\alpha_k \alpha_{\pi(k)} \in \mathcal{O}_K$ extends $\{\alpha_1, \ldots, \alpha_{n-1}\}$ to a n-dimensional lattice; therefore we have $\|\alpha_k\|_\infty \|\alpha_{\pi(k)}\|_\infty \geq \|\alpha_k \alpha_{\pi(k)}\|_\infty \geq \lambda_n^\infty(\mathcal{O}_K)$. Taking products over all $k \in \{2, \ldots, n-1\}$ we obtain

$$\prod_{k=2}^{n-1} \|\alpha_k\|_\infty^2 = \prod_{k=2}^{n-1} \|\alpha_k\|_\infty \|\alpha_{\pi(k)}\|_\infty \geq \left(\lambda_n^\infty(\mathcal{O}_K)\right)^{n-2}.$$

Multiplying above equation by $\|\alpha_1\|_\infty^2 = 1$ and $\|\alpha_n\|_\infty^2 = \lambda_n^\infty(\mathcal{O}_K)^2$, and using Minkowski's second inequality [Cas12, Ch. VIII] $\prod_{k=1}^n \lambda_k^\infty(\Lambda) \leq \det(\Lambda)$, we obtain

$$|\Delta_K| \geq \prod_{k=1}^{n} \|\alpha_k\|_\infty^2 \geq (\lambda_n^\infty(\mathcal{O}_K))^n.$$

It remains to prove that $C = ([\alpha_k \alpha_\ell]_n)$ is non-degenerate. Suppose it is not, and there exists d_ℓ for $\ell \in \{2, \ldots, n-1\}$ (not all zero) such that

$$\Big[\sum_{\ell=2}^{n-1} d_\ell \alpha_k \alpha_\ell\Big]_n = \sum_{\ell=2}^{n-1} d_\ell [\alpha_k \alpha_\ell]_n = 0 \text{ for all } k \in \{2, \ldots, n-1\}$$

Writing $\beta = \sum_{\ell=2}^{n-1} d_\ell \alpha_\ell$, this means that $\alpha_k \beta$ lies in the span of the elements $(\alpha_1, \ldots, \alpha_{n-1})$. In other words, $L = \mathbb{Q}\alpha_1 + \ldots + \mathbb{Q}\alpha_{n-1}$ is $\mathbb{Q}(\beta)$-invariant, i.e., a $\mathbb{Q}(\beta)$-vector (strict) subspace of K. That is, $\dim_{\mathbb{Q}(\beta)}(L) \leq \dim_{\mathbb{Q}(\beta)}(K) - 1$. But then

$$\begin{aligned} n - 1 = \dim_{\mathbb{Q}}(L) &= \dim_{\mathbb{Q}(\beta)}(L) \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] \\ &\leq (\dim_{\mathbb{Q}(\beta)}(K) - 1) \cdot [\mathbb{Q}(\beta) : \mathbb{Q}] = n - [\mathbb{Q}(\beta) : \mathbb{Q}], \end{aligned}$$

yielding $[\mathbb{Q}(\beta) : \mathbb{Q}] = 1$, i.e., $\beta \in \mathbb{Q}$, which is impossible by the fact that $\beta = \sum_{\ell=2}^{n-1} d_\ell \alpha_\ell$ is assumed to be non-zero and has no $\alpha_1 = 1$ part.

We conclude that C is non-degenerate, which finishes the proof. $\square$

A.2. Bound on the Residue of the Zeta Function for Cyclotomic Fields

In the proof of Lemma 7.20, we used that for the cyclotomic field $K = \mathbb{Q}(\zeta_m)$, the residue ρ_K of the zeta function for cyclotomic fields is in $O(m^4)$. This section is dedicated to the proof of this fact.

Theorem A.5 (ERH). *Let $K = \mathbb{Q}(\zeta_m)$ with $m \geq 3$. Then, assuming the Riemann Hypothesis for L-functions $L(\chi, s)$ for all Dirichlet characters modulo m, we have*

$$\rho_K \leq e^{15} \cdot m^4 = O(m^4).$$

Proof. The proof extends to the rest of this section, through the following steps.

(Appendix A.2.1) Writing $\log(\rho_K) = R_K + M_K$

We first split the computation of ρ_K into two parts, a *ramified part* R_K and a *main part* M_K. This ramified part occurs because the characters $\chi \in \hat{G}\backslash 1$ for $G = \mathrm{Gal}(K/Q)$ are defined modulo their conductor $f_\chi \mid m$. For computations it is simpler to consider characters modulo m instead, denoted, $\chi|_m$. The ramified term pops up as a correction factor, just being the sum of $L(\chi, 1) - L(\chi|_m, 1)$ for the non-trivial characters χ.

(Appendix A.2.2) Bounding the ramified term $R_K \leq 2\log(m)$

By elementary methods one can show that $R_K \leq 2\log(m)$ (see Proposition A.9).

(Appendix A.2.3) Splitting $M_K = M_K^{(w)} + \lim_{x\to\infty}(M_K^{(x)} - M_K^{(w)})$**.**

The main part $M_K = \sum_q \frac{a_q}{q}$ can be seen as a sum where q ranges over all prime powers. By defining the partial sum $M_K^{(w)} = \sum_{q<w} \frac{a_q}{q}$ one obtains an 'initial' part $M_K^{(w)}$ and a 'tail part' $\lim_{x\to\infty}(M_K^{(x)} - M_K^{(w)})$ of M_K.

(Appendix A.2.4) The initial part $M_K^{(w)} \leq 2\log(m) + 11$ **for** $w = \max(e^{5/4\cdot m}, 10^{10})$**.**

By applying partial summation to the Brun-Titchmarsh bound (see Lemma A.13) one obtains the bound $M_K^{(w)} \leq 2\log\log w + 7$. It easy to show that for $w = \max(e^{5/4\cdot m}, 10^{10})$ holds $2\log\log w + 7 \leq 2\log(m) + 11$.

(Appendix A.2.5) The tail part $\lim_{x\to\infty}(M_K^{(x)} - M_K^{(w)}) \leq 4$ **for** $w = \max(e^{5/4\cdot m}, 10^{10})$**.**

This bound, proven in Proposition A.17, assumes the Riemann Hypothesis for L-functions for Dirichlet characters modulo m, and follows from an explicit result of Dusart [Dus98].

Combining the bounds yields $\log(\rho_K) \leq 4\log(m) + 15$**.**

We have the following bound, of which taking the exponent yields the final claim.

$$\log \rho_K \leq R_K + M_K^{(w)} + \lim_{x\to\infty}(M_K^{(x)} - M_K^{(w)}) \leq 2\log(m) + (2\log(m) + 11) + 4.$$

∎

A.2.1. Splitting $\log(\rho_K) = R_K + M_K$ into a Ramified Term and a Main Term

Notation A.6. *In the following, every Dirichlet character χ is assumed to be primitive, i.e., defined modulo its conductor f_χ. If we, instead, want to consider a Dirichlet character modulo a larger modulus m (with $f_\chi \mid m$), we write $\chi|_m$ (and we have $\chi|_m(a) = 0$ whenever $\gcd(a,m) > 1$). We denote by $\mathbf{1}$ the trivial character that has value one everywhere.*

Lemma A.7. *Let $K = \mathbb{Q}(\zeta_m)$ be a cyclotomic field extension with Galois group $G \simeq (\mathbb{Z}/m\mathbb{Z})^*$ and consider all characters $\hat{G}$ as Dirichlet characters. Then we have $\log(\rho_K) = R_K + M_K$, where*

$$R_K = -\sum_{\chi \in \hat{G}\backslash \mathbf{1}} \sum_{\substack{p \mid m \\ p \nmid f_\chi}} \log(1 - \chi(p)/p) \text{ and } M_K = \sum_{\chi \in \hat{G}\backslash \mathbf{1}} \log L(\chi|_m, 1)$$

Proof. We have the following formula for the logarithm of the residue ρ_K, by considering the quotient of the Dedekind zeta function and the Riemann zeta function [Nar04, Thm. 8.6].

$$\log(\rho_K) = \sum_{\chi \in \hat{G}\backslash \mathbf{1}} \log L(\chi, 1)$$

Concentrating on a fixed $\chi \in \hat{G}\backslash\mathbf{1}$, and applying the Euler product formula, we obtain

$$\begin{aligned}
\log L(\chi, 1) &= -\sum_{p \nmid f_\chi} \log(1 - \chi(p)/p) \\
&= -\sum_{p \nmid m} \log(1 - \chi(p)/p) - \sum_{\substack{p \mid m \\ p \nmid f_\chi}} \log(1 - \chi(p)/p) \\
&= \log L(1, \chi|_m) - \sum_{\substack{p \mid m \\ p \nmid f_\chi}} \log(1 - \chi(p)/p).
\end{aligned}$$

Summing over all non-trivial $\chi \in \hat{G}$ yields

$$\log(\rho_K) = -\sum_{\chi \in \hat{G} \setminus \mathbf{1}} \sum_{\substack{p \mid m \\ p \nmid f_\chi}} \log(1 - \chi(p)/p) + \sum_{\chi \in \hat{G} \setminus \mathbf{1}} \log L(1, \chi|_m) = R_K + M_K.$$

□

We call the terms R_K and M_K the *ramified term* and the *main term* respectively.

A.2.2. Estimating the Ramified Term

Lemma A.8. *For any prime-power cyclotomic number field $K = \mathbb{Q}(\zeta_{p^k})$, the ramified term R_K equals zero.*

Proof. For a prime-power cyclotomic field $\mathbb{Q}(\zeta_{p^k})$, the conductor of every non-trivial character $\chi \in \hat{G}$ is divisible by p, since $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^k})/\mathbb{Q}) \simeq (\mathbb{Z}/p^k\mathbb{Z})^*$. Therefore, $R_K = -\sum_{\chi \in \hat{G} \setminus \mathbf{1}} \sum_{\substack{p \mid m \\ p \nmid f_\chi}} \log(1 - \chi(p)/p) = 0$. □

Proposition A.9. *For any cyclotomic number field $K = \mathbb{Q}(\zeta_m)$ with $m \geq 3$, we have*

$$R_K \leq 2 \log(m)$$

Proof. Denoting $G \simeq (\mathbb{Z}/m\mathbb{Z})^*$ for the Galois group of K, swapping sums and using the Taylor expansion of the logarithm, we obtain

$$\begin{aligned} R_K &= \sum_{p \mid m} \sum_{\substack{\chi \in \hat{G} \setminus \mathbf{1} \\ p \nmid f_\chi}} \sum_{j > 0} \frac{\chi(p^j)}{j p^j} = \sum_{p \mid m} \sum_{j > 0} \frac{1}{j p^j} \sum_{\substack{\chi \in \hat{G} \setminus \mathbf{1} \\ p \nmid f_\chi}} \chi(p^j) \\ &= \sum_{p \mid m} \sum_{j > 0} \frac{1}{j p^j} \left(-1 + \sum_{\chi \in \hat{G}_p} \chi(p^j) \right). \end{aligned}$$

where $\hat{G}_p = \{\chi \in \hat{G} \mid p \nmid f_\chi\}$. Note that $\hat{G}_p \simeq (\mathbb{Z}/m_p\mathbb{Z})^*$ is isomorphic to the Galois group of $\mathbb{Q}(\zeta_{m_p})$, where m_p is the p-free part of m. By character orthogonality relations , we know that

$$\sum_{\chi \in \hat{G}_p} \chi|_{m_p}(a) = \begin{cases} |\hat{G}_p| = \phi(m_p) & \text{if } a \equiv 1 \bmod m_p \\ 0 & \text{otherwise} \end{cases}$$

Since p is coprime with m_p, we know that for any character χ of $\hat{G}_p$ and exponent $j > 0$, it holds that $\chi(p^j) = \chi|_{m_p}(p^j)$. Denoting j_p for the order of p in $(\mathbb{Z}/m_p\mathbb{Z})^*$, we deduce that j_p is the smallest non-zero exponent such satisfying $\sum_{\chi \in \hat{G}_p} \chi(p^{j_p}) = \phi(m_p)$. Moreover, we have $p^{j_p} = 1 + km_p > m_p$. Using these properties, we obtain the following rather crude bound.

$$\begin{aligned} \sum_{p|m} \sum_{j>0} \frac{1}{jp^j} \left(-1 + \sum_{\chi \in \hat{G}_p} \chi(p^j) \right) &\leq \sum_{p|m} \sum_{k>0} \frac{\phi(m_p) - 1}{(kj_p)p^{kj_p}} \\ &\leq -\sum_{p|m} (\phi(m_p) - 1) \log(1 - p^{-j_p}) \\ &\leq \sum_{p|m} \frac{2\log(2) \cdot (\phi(m_p) - 1)}{p^{j_p}} \\ &\leq 2\log(2) \cdot \omega(m) \leq 2\log(m) \end{aligned}$$

The first inequality omits the $p^j \not\equiv 1$ modulo m_p, as they add negative value anyway; the second inequality uses the equation $\sum_{k>0} (p^{-j_p})^k/k = -\log(1 - p^{-j_p})$ after disposing j_p in the denominator. The third inequality uses the fact that $-\log(1-x) \leq 2\log(2) \cdot x$ for $x < 1/2$, the fourth inequality uses the fact that $p^{j_p} > m_p$. By Lemma A.8, we may assume, without loss of generality, that m has at least 2 distinct prime divisors, i.e., $\omega(m) > 1$. Then the fifth inequality is just a trivial upper bound on the prime omega function $\omega(m)$, the number of *distinct* prime divisors of m. □

A.2.3. Splitting the Main Term in an Initial Part and a Tail Part

Notation A.10. *For $a \in \mathbb{N}$ with* $\gcd(a, m) = 1$, *we put*

$$S_{a,x} = \sum_{\substack{p \ prime, j>0, \\ p^j \equiv a \bmod m \\ p^j \leq x}} \frac{1}{jp^j}$$

Proposition A.11 (Estimating the main term)**.** *Let $K = \mathbb{Q}(\zeta_m)$ be a cyclotomic field. Then*

$$M_K = \lim_{x \to \infty} \left(\phi(m) \cdot S_{1,x} - \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^*} S_{a,x} \right)$$

Proof. We have

$$M_K = \sum_{\chi \in \hat{G} \setminus 1} \log L(\chi|_m, 1) = \sum_{p \nmid m} \sum_j \frac{1}{jp^j} \sum_{\chi \in \hat{G} \setminus 1} \chi|_m(p^j)$$

For numbers a coprime with m we know that $\sum_{\chi \in \hat{G}} \chi|_m(a)$ equals $\phi(m)$ if $a \equiv 1 \bmod m$ and 0 otherwise.This yields:

$$M_K = (\phi(m) - 1) \sum_{\substack{p \ \text{prime}, j>0 \\ p^j \equiv 1 \bmod m}} \frac{1}{jp^j} - \sum_{\substack{p \ \text{prime}, j>0 \\ p \nmid m, p^j \not\equiv 1 \bmod m}} \frac{1}{jp^j}.$$

Writing out the new notation and flipping summands corresponding to $p^j \equiv 1 \bmod m$ from the left-hand to the right-hand side yields the result. □

It will be proven useful to cut the main term into two parts:

$$M_K = M_K^{(w)} + \lim_{x \to \infty} \left(M_K^{(x)} - M_K^{(w)} \right).$$

That is, a finite initial part $M_K^{(w)}$ and a tail part $\lim_{x \to \infty} \left(M_K^{(x)} - M_K^{(w)} \right)$. More precisely, for $w > 1$,

Notation A.12.

$$M_K^{(w)} = \phi(m) S_{1,w} - \sum_{b \in (\mathbb{Z}/m\mathbb{Z})^*} S_{b,w}$$

A.2.4. Estimating the Initial Part of the Main Term

Lemma A.13. *For $w \geq m^4$ we have*

$$M_K^{(w)} \leq 2 \log \log w + 7.$$

Proof. By omitting the negative terms in Notation A.12, we obtain

$$M_K^{(w)} \leq \phi(m) S_{1,w} = \phi(m) \sum_{\substack{p \text{ prime}, j>0 \\ p^j \equiv 1 \bmod m \\ p^j \leq w}} \frac{1}{jp^j} \leq 5 + \phi(m) \sum_{\substack{p \text{ prime} \\ p \equiv 1 \bmod m \\ p \leq w}} \frac{1}{p}.$$

where the last inequality follows from Lemma A.14

$$\sum_{\substack{p \text{ prime}, j>1 \\ p^j \equiv 1 \bmod m}} \frac{1}{jp^j} \leq 5/m,$$

For a fixed m, we denote by $\pi_1(t)$ the number of primes p with $p \leq t$ that satisfy $p \equiv 1 \bmod m$. For $t > m$, we have the Brun-Titchmarsh bound $\pi_1(t) \leq \frac{2t}{\phi(m) \log(t/m)}$ [MV73]. Combining this bound with Abel partial summation, we obtain

$$\begin{aligned}
\sum_{\substack{p \text{ prime} \\ p \equiv 1 \bmod m \\ p \leq w}} \frac{1}{p} &\leq \frac{1}{m} + \frac{1}{2m} + \sum_{\substack{p \text{ prime} \\ p \equiv 1 \bmod m \\ em \leq p \leq w}} \frac{1}{p} \\
&= \frac{1}{m} + \frac{1}{2m} + \frac{\pi_1(w)}{w} - \frac{\pi_1(em)}{em} + \int_{em}^{w} \frac{2dx}{\phi(m) x \log(x/m)} \\
&\leq \frac{3}{2m} + \frac{1}{\phi(m) \log(w/m)} + 2/\phi(m) \cdot \log \log(w/m)
\end{aligned}$$

The first inequality just writes out the first two terms of the sum, the subsequent equality is the Abel summation formula, using the facts that t^{-1} has derivative $-t^{-2}$ and π_1 has the Brun-Titchmarsh bound. The last inequality follows from evaluating the integral, combining the terms and using again the Brun-Titchmarsh bound for $\pi_1(w)$. Concluding, one can deduce that $M_K^{(w)}$ is bounded by $5 + 3/2 + 1/\log(w/m) + 2 \log \log w \leq 7 + 2 \log \log w$. $\square$

Lemma A.14. *For all $m \geq 2$ holds*

$$\sum_{\substack{p \text{ prime}, j>1 \\ p^j \equiv 1 \bmod m}} \frac{1}{jp^j} \leq \frac{5}{m},$$

Proof. Using the technique from Ankeny and Chowla [AC49, p. 532] we split the sum into a part where $p > m$ and a part where $p < m$.

For $p > m$ we have

$$\sum_{\substack{p \text{ prime}, j>1 \\ p^j \equiv 1 \bmod m \\ p>m}} \frac{1}{jp^j} \leq \sum_{k>m} \frac{1}{k^2} \leq \int_m^\infty 1/x^2 \cdot dx = \frac{1}{m} \tag{A.115}$$

The first inequality follows from the fact that for every fixed prime $p > m$ we have

$$\sum_{j>1} \frac{1}{jp^j} \leq \frac{1}{2p^2} \left(\sum_{j=0}^{\infty} p^{-j} \right) \leq \frac{1}{2p^2} \cdot \frac{p}{p-1} \leq \frac{1}{p^2}.$$

For $p < m$ we use the fact that $X^k \equiv 1$ modulo m can have at most k incongruent solutions [AC49, p. 532]. This implies, by considering all numbers $am + 1$ with $a \in \mathbb{Z}$,

$$\sum_{\substack{p \text{ prime}, j>1 \\ p^j \equiv 1 \bmod m \\ p<m}} \frac{1}{jp^j} \leq \sum_{j=2}^{\infty} \frac{1}{j} \left[\sum_{a=A(j)}^{B(j)} \frac{1}{am+1} \right] \leq \sum_{j=2}^{\infty} \frac{1}{(\frac{j^2-j}{2}+1)m+1},$$

where $A(j) = \frac{j^2-j}{2} + 1$ and $B(j) = \frac{j^2+j}{2}$. Dividing out $\frac{1}{m}$, using $j^2 - j \geq (j-1)^2$ for $j \geq 2$, and applying the Basel problem equality, we obtain

$$\sum_{\substack{p \text{ prime}, j>1 \\ p^j \equiv 1 \bmod m \\ p<m}} \frac{1}{jp^j} \leq \sum_{j=2}^{\infty} \frac{1}{(\frac{j^2-j}{2}+1)m+1} \leq \frac{2}{m} \cdot \sum_{j=2}^{\infty} \frac{1}{(j-1)^2} \leq \frac{\pi^2}{3m}. \tag{A.116}$$

Combining Equation (A.115) and Equation (A.116), and simplifying $\pi^2/3 + 1 \leq 5$ we obtain the claim. $\square$

A.2.5. Estimating the Tail Part of the Main Term

Defining $\mathcal{M}_a(k) = \mathcal{M}(k)$ if $k \equiv a \bmod m$ and zero otherwise, and putting $\psi_a(x) = \sum_{k<x} \mathcal{M}_a(k)$, we have the following explicit result, due to Dusart [Dus98, Thm. 3.7, p. 114].

Theorem A.15 (ERH)**.** *For every $x > \max(e^{5/4\cdot m}, 10^{10})$, we have, assuming the Riemann Hypothesis for $L(\chi, s)$ for all Dirichlet characters χ modulo m,*

$$|\psi_a(x) - x/\phi(m)| \leq \frac{1}{4\pi}\sqrt{x}\log^2(x)$$

Lemma A.16 (ERH)**.** *Let m be a fixed modulus and let a be coprime with m and let $x \geq w \geq e^{5/4\cdot m}$. Then there is a value $K_{x,w}$ that does not depend on a, and a value η_a with $|\eta_a| \leq 1$, such that*

$$\left|(S_{a,x} - S_{a,w}) - K_{x,w} - \frac{2\eta_a}{m}\right| = O(1/\log x).$$

Proof. We have

$$S_{a,x} - S_{a,w} = \sum_{\substack{p \text{ prime}, j>0, \\ p^j \equiv a \bmod m \\ w<p^j\leq x}} \frac{1}{jp^j}.$$

Applying Abel summation, using that the derivative of $\frac{1}{t\log t}$ equals $\frac{-(\log(t)+1)}{\log(t)^2t^2}$, we obtain

$$S_{a,x} - S_{a,w} = \sum_{w<k\leq x} \frac{\mathcal{M}_a(k)}{k\log k} = \frac{\psi_a(x)}{x\log x} - \frac{\psi_a(w)}{w\log w} + \int_w^x \frac{\psi_a(t)(\log(t)+1)}{\log(t)^2t^2}dt.$$

Writing $\psi_a(t) = \frac{t}{\phi(m)} + 1/(4\pi)\cdot\eta(t)\sqrt{t}\log^2(t)$ with $|\eta(t)| \leq 1$, we obtain that, for some η' with $|\eta'| \leq 1$,

$$\int_w^x \frac{\psi_a(t)(\log(t)+1)}{\log(t)^2t^2}dt$$

$$= O(1/\log(x)) + \log\log x + \log\log w - 1/\log w + \eta' \underbrace{\frac{2\log(w)+3}{4\pi\sqrt{w}}}_{\leq 1/m}.$$

Since $w \geq e^{5/4 \cdot m}$, we have $\frac{2\log(w)+3}{4\pi\sqrt{w}} \leq \frac{1}{m}$. Also, for some η'' with $|\eta''| \leq 1$, we have

$$\frac{\psi_a(w)}{w \log w} = \frac{1}{\log(w)\phi(m)} + \frac{\eta(t)\log^2(w)}{4\pi w^{1/2}} = \frac{1}{\log(w)\phi(m)} + \eta''/m$$

Combining all equations and putting $K_{x,w} = \log\log x + \log\log w - 1/\log w + \frac{1}{\log(w)\phi(m)}$, we obtain

$$\left| \sum_{w<k\leq x} \frac{\mathcal{M}_a(k)}{k \log k} - K_{x,w} - (\eta' + \eta'')/m \right| = O(1/\log(x)).$$

$\square$

Proposition A.17 (ERH)**.** *Let $x \geq w \geq e^{5/4 \cdot m}$. Then*

$$M_K^{(x)} - M_K^{(w)} \leq O(m/\log(x)) + 4,$$

where the implied constant is absolute (and does not depend on m).

Proof. We have, using Lemma A.16,

$$M_K^{(x)} - M_K^{(w)} = \phi(m)(S_{1,x} - S_{1,w}) - \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^*} (S_{a,x} - S_{a,w})$$

$$= (\phi(m) - \phi(m))(O(1/\log x) + K_{x,w}) + \phi(m) \cdot 2\eta_1/m + \sum_{a \in (\mathbb{Z}/m\mathbb{Z})^*} 2\eta_a/m.$$

By using the fact that $|\eta_a| \leq 1$ for all $a \in (\mathbb{Z}/m\mathbb{Z})^*$, we obtain the result. $\square$

A.3. Exact Sequences

Lemma A.18 (Kernel-cokernel exact sequence)**.** *Let A, B, C be abelian groups and let $f : A \to B$ and $g : B \to C$ be group homomorphisms, fitting in the following commutative diagram.*

$$
\begin{tikzcd}
 & B \arrow[dr, "g"] & \\
A \arrow[ur, "f"] \arrow[rr, "gf"] & & C
\end{tikzcd}
$$

*Then, denoting '*ker*' for the kernel of a map and '*coker*' for the cokernel of a map, we have the following exact sequence.*

$$
0 \to \ker f \to \ker gf \to \ker g \to \operatorname{coker} f \to \operatorname{coker} gf \to \operatorname{coker} g \to 0.
$$

This sequence can be obtained mnemonically by observing the outer, blue arrows in Figure A.1.

Proof. Apply the snake lemma twice to obtain the result.

$$
\begin{tikzcd}
 & 0 \arrow[r] \arrow[d] & \ker f \arrow[r] \arrow[d] & \ker gf \arrow[d] \arrow[dddll, rounded corners, "\partial"] & \\
 & 0 \arrow[r] \arrow[d] & A \arrow[r, "id"] \arrow[d, "f"] & A \arrow[r] \arrow[d, "gf"] & 0 \\
0 \arrow[r] & \ker g \arrow[r] \arrow[d] & B \arrow[r, "g"] \arrow[d] & C \arrow[d] & \\
 & \ker g \arrow[r] & \operatorname{coker} f \arrow[r] & \operatorname{coker} gf &
\end{tikzcd}
$$

$$
\begin{tikzcd}
 & \ker gf \arrow[r] \arrow[d] & \ker g \arrow[r] \arrow[d] & \operatorname{coker} f \arrow[d] \arrow[dddll, rounded corners, "\partial"] & \\
 & A \arrow[r, "f"] \arrow[d, "gf"] & B \arrow[r] \arrow[d, "g"] & \operatorname{coker} f \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & C \arrow[r, "id"] \arrow[d] & C \arrow[r] \arrow[d] & 0 \arrow[d] & \\
 & \operatorname{coker} gf \arrow[r] & \operatorname{coker} g \arrow[r] & 0 &
\end{tikzcd}
$$

□

$$\begin{tikzcd}
 & & \ker g \arrow[dr] \arrow[rr, bend left] & & \operatorname{coker} f \arrow[ddrr] & & \\
 & & & B \arrow[ur] \arrow[dr, "g"] & & & \\
 \ker gf \arrow[rr] \arrow[uurr] & & A \arrow[ur, "f"] \arrow[rr, "gf"] & & C \arrow[rr] \arrow[dr] & & \operatorname{coker} gf \arrow[dl, bend left] \\
 & \ker f \arrow[ur] \arrow[ul, bend left] & & 0 \arrow[ll] & & \operatorname{coker} g \arrow[ll] &
\end{tikzcd}$$

Figure A.1.: The kernel-cokernel exact sequence in the outer, blue arrows.

A.4. The Yudin-Jackson Theorem

In the chapter about the Continuous Hidden Subgroup Problem (Chapter 3), the main issue is the impact of discretization on the success probability of the quantum algorithm. This impact turns out to be largely influenced by how well a complex vector-valued function on the torus $\mathbb{T}^m = \mathbb{R}^m/\mathbb{Z}^m$ can be approximated by trigonometric functions with bounded frequencies.

This problem of finding the best trigonometric approximation has already been solved in the specific case of scalar complex functions on the torus by Yudin [Yud76], using Fourier analysis. We show here that Yudin's reasoning applies straightforwardly to vector-valued functions as well. To be clear, the following text contains the same proof as in Yudin's work [Yud76] and it is restated here for the sake of self-containedness.

Generalized result of Yudin

Recall that the L_p-norm for $p \in [1, \infty]$ for a vector-valued function $\mathbf{f} : \mathbb{T}^m \to \mathbb{C}^N$ is defined as follows[1].

$$\|\mathbf{f}\|_{p,\mathbb{T}^m} := \left(\int_{x \in \mathbb{T}^m} \|\mathbf{f}(x)\|_{\mathbb{C}^N}^p \, dx \right)^{1/p},$$

where $\|\cdot\|_{\mathbb{C}^N}$ is the Euclidean norm on $\mathbb{C}^N$. Any function for which the value $\|\mathbf{f}\|_{p,\mathbb{T}^m}$ is well-defined is called an L_p-function. For a function $\mathbf{f} : \mathbb{T}^m \to \mathbb{C}^N$ we define its Lipschitz constant to be

$$\mathrm{Lip}(\mathbf{f}) = \inf\{L \mid \|\mathbf{f}(x) - \mathbf{f}(y)\|_{\mathbb{C}^N} \leq L\|x - y\|_{\mathbb{T}^m} \text{ for all } x, y \in \mathbb{T}^m\}.$$

For $\mathbf{f}$ we also define a related constant, the modulus of smoothness [Yud76]:

$$\omega_2(\mathbf{f}, \delta)_p := \sup_{|y| \leq \delta} \|\mathbf{f}(\cdot - y) - 2\mathbf{f}(\cdot) + \mathbf{f}(\cdot + y)\|_{p,\mathbb{T}^m}.$$

It is evident that $\omega_2(\mathbf{f}, \delta)_p \leq \omega_2(\mathbf{f}, \delta)_\infty \leq 2 \,\mathrm{Lip}(\mathbf{f})\delta$ for functions $\mathbf{f}$ for which both quantities are defined.

Theorem A.19 (Yudin-Jackson)**.** *Let $\mathbf{f} : \mathbb{T}^m \to \mathbb{C}^N$ be an L_p-function. Then there exists a function $\mathbf{t} : \mathbb{T}^m \to \mathbb{C}^N$ with $\mathcal{F}_{\mathbb{T}^m}\{\mathbf{t}\}$ having support in $[-r/2, r/2]^m$ such that*

$$\|\mathbf{f} - \mathbf{t}\|_{p,\mathbb{T}^m} \leq 2\omega_2(\mathbf{f}, \sqrt{m}/r)_p \leq 2\sqrt{m}\,\mathrm{Lip}(\mathbf{f})/r.$$

In essence, above theorem just states that the best trigonometric approximation of a function mainly depends on the smoothness of that function (in terms of the Lipschitz constant, for example) and how high the frequencies of the trigonometric functions are allowed to be, which is measured by r.

[1] For $p = \infty$, we let $\|\mathbf{f}\|_{\infty,\mathbb{T}^m}$ to be the essential supremum of the function $x \mapsto \|\mathbf{f}\|_{\mathbb{C}^N}$.

Proof

First we prove a basic result about the modulus of smoothness; it satisfies the following 'scaling' property.

Lemma A.20 (Scaling property of the modulus of smoothness)**.** *For any L_p function $\mathbf{f} : \mathbb{T}^m \to \mathbb{C}^N$ and for any $\rho, \delta > 0$, we have $\omega_2(\mathbf{f}, \rho\delta)_p \leq 2(1+\rho^2)\omega_2(\mathbf{f}, \delta)_p$.*

Proof. Note that we have the following 'telescopic' finite sum

$$\begin{aligned}&\mathbf{f}(x-nt) - 2\mathbf{f}(x) + \mathbf{f}(x+nt)\\ =&\sum_{j=-n+1}^{n-1}(n-|j|)\big[\mathbf{f}(x+(j-1)t) - 2\mathbf{f}(x+jt) + \mathbf{f}(x+(j+1)t)\big].\end{aligned}$$

So, for $|t| \leq \delta$, we have, by the triangle inequality,

$$\begin{aligned}\|\mathbf{f}(\cdot - nt) - 2\mathbf{f}(\cdot) + \mathbf{f}(\cdot + nt)\|_{p,\mathbb{T}^m} &\leq \sum_{j=-n+1}^{n-1}(n-|j|)\omega_2(\mathbf{f},\delta)_p\\ &= n^2\omega_2(\mathbf{f},\delta)_p.\end{aligned}$$

Therefore, for any $\rho > 0$, $\omega(\mathbf{f}, \rho\delta)_p \leq \omega(\mathbf{f}, \lceil\rho\rceil\delta)_p \leq \lceil\rho\rceil^2\omega(\mathbf{f},\delta)_p \leq (1+\rho)^2\omega(\mathbf{f},\delta)_p$. Using the fact that $(1+\rho)^2 \leq 2(1+\rho^2)$, we obtain the result. $\square$

Next, we try to approximate the function $\mathbf{f}$ by the function $\mathbf{f} \star K$, a convolution of f with a suitable kernel K. The closeness of this approximation largely depends on the smoothness of $\mathbf{f}$ and the value of of a certain integral involving the kernel K.

Lemma A.21. *Let $K : \mathbb{T}^m \to [0,\infty)$ be a L_1-function satisfying $\int_{t\in\mathbb{T}^m} K(t)dt = 1$ and $K(-t) = t$ for all $t \in \mathbb{T}^m$. Denote $\mathbf{t} = \mathbf{f} \star K = \int_{t\in\mathbb{T}^m}\mathbf{f}(\,\cdot - t)K(t)dt$. Then, for all $r > 0$,*

$$\|\mathbf{f} - \mathbf{t}\|_{p,\mathbb{T}^m} \leq \omega_2(\mathbf{f}, \sqrt{m}/r)_p\left(1 + \frac{r^2}{m}\int_{t\in[-1/2,1/2]^m}|t|^2\cdot K(t)dt\right), \quad \text{(A.117)}$$

Proof. By the fact that K is even,

$$\mathbf{t}(x) = \mathbf{f} \star K(x) = \int_{t\in\mathbb{T}^m} \mathbf{f}(x-t)K(t)dt = \int_{t\in\mathbb{T}^m} \mathbf{f}(x+t)K(t)dt$$
$$= \frac{1}{2}\int_{t\in\mathbb{T}^m} \mathbf{f}(x-t) + \mathbf{f}(x+t)K(t)dt.$$

We can write $f(x) = \int_{t\in\mathbb{T}^m} f(x)K(t)dt$, since $\int_{t\in\mathbb{T}^m} K(t)dt = 1$. Therefore,

$$\mathbf{t}(x) - \mathbf{f}(x) = \frac{1}{2}\int_{t\in\mathbb{T}^m} (\mathbf{f}(x-t) - 2\mathbf{f}(x) + \mathbf{f}(x+t))K(t)dt.$$

Taking L_p-norms, using the integral-triangle inequality, integrating over the set $[-1/2, 1/2]^m$, using the fact that $K(t)$ is a positive scalar and applying Lemma A.20 with $\delta = \sqrt{m}/r$ and $\rho = r|t|/\sqrt{m}$, we obtain

$$\|\mathbf{f} - \mathbf{t}\|_{p,\mathbb{T}^m} \leq \frac{1}{2}\int_{t\in[-1/2,1/2]^m} \omega_2(\mathbf{f}, |t|)_p K(t)dt$$
$$\leq \int_{t\in[-1/2,1/2]^m} \left(1 + \frac{|t|^2 r^2}{m}\right) \omega_2(\mathbf{f}, \sqrt{m}/r)_p K(t)dt.$$

Rewriting the integral, using $\int_{t\in\mathbb{T}^m} K(t)dt = 1$, we arrive at Equation (A.117). □

In the next step, we will instantiate the kernel $K = K_r$ in such a way that its Fourier coefficients have support in $[-r/2, r/2]^m$. This means, by the convolution formula, that $\mathbf{t} = \mathbf{f} \star K_r$ also has Fourier coefficients with support only in $[-r/2, r/2]^m$. Furthermore, K_r is chosen in such a way that

$$\frac{r^2}{m} \cdot \int_{t\in[-1/2,1/2]^m} |t|^2 K_r(t)dt \leq 1.$$

Lemma A.22. *Let $\lambda = \phi \star \phi = \int_{t\in\mathbb{R}^m} \phi(\cdot - t)\phi(t)dt$, where*

$$\phi(x_1, \ldots, x_m) = \begin{cases} 2^m \prod_{j=1}^m \cos(2\pi x_j) & \textit{if } (x_1, \ldots, x_m) \in [-1/4, 1/4]^m \\ 0 & \textit{otherwise} \end{cases}$$

Furthermore, define $K_r : \mathbb{T}^m \to \mathbb{C}$ by the rule $K_r(t) := \mathcal{F}^{-1}_{\mathbb{T}^m}\{\lambda(\cdot/r)|_{\mathbb{Z}^m}\}(t) = \sum_{z\in\mathbb{Z}^m} \lambda(z/r)e^{2\pi i\langle t,z\rangle}$. Then *(i)* $K_r(t) \geq 0$ *and* $K_r(t) = K_r(-t)$ *for all* $t \in \mathbb{T}^m$*,*

(ii) $\int_{t\in\mathbb{T}^m} K_r(t)dt = 1$*,*

(iii) $\mathcal{F}_{\mathbb{T}^m}\{K_r\}$ *has support only in* $[-r/2, r/2]^m$*,*

(iv) $\int_{t\in\mathbb{T}^m} |t|^2 K_r(t)dt \leq m/r^2$*.*

Proof. For (i), note that K_r is even because λ is. For positivity, we apply the Poisson summation formula.

$$K_r = \mathcal{F}^{-1}_{\mathbb{T}^m}\{\lambda(\cdot/r)|_{\mathbb{Z}^m}\} = \mathcal{F}^{-1}_{\mathbb{R}^m}\{\lambda(\cdot/r)\}\Big|^{\mathbb{Z}^m} = r^m\hat{\lambda}(r\cdot)\Big|^{\mathbb{Z}^m} \geq 0.$$

The last inequality follows from the convolution formula: $\hat{\lambda} = \widehat{\phi \star \phi} = \hat{\phi}\cdot\hat{\phi} \geq 0$. For (ii), note that $\int_{t\in\mathbb{T}^m} K_r(t)dt = \mathcal{F}_{\mathbb{T}^m}\{K_r\}[0] = \lambda(0) = \int_{t\in\mathbb{R}^m}\phi(t)^2 dt = 1$. Part (iii) is can be shown by combining the following facts: $\mathcal{F}_{\mathbb{T}^m}\{K_r\} = \lambda(\cdot/r)|_{\mathbb{Z}^m}$ and $\lambda(x) = 0$ if $|x|_\infty > 1/2$. Part (iv) is the most technical; since $K_r = r^m\hat{\lambda}(r\cdot)\Big|^{\mathbb{Z}^m}$ and $|t|^2 \leq |t+v|^2$ for any $v \in \mathbb{Z}^m$ and $t \in [-1/2, 1/2]^m$, we have

$$\begin{aligned}\int_{t\in[-\frac{1}{2},\frac{1}{2}]^m} |t|^2 K(t)dt &= \int_{t\in[-\frac{1}{2},\frac{1}{2}]^m} |t|^2 r^m \sum_{z\in\mathbb{Z}^m}\hat{\lambda}(r(t+z))dt \\ &\leq \int_{\mathbb{R}^m}|t|^2\hat{\lambda}(rt)r^m dt = r^{-2}\int_{\mathbb{R}^m}|y|^2\hat{\lambda}(y)dy, \qquad \text{(A.118)}\end{aligned}$$

where the last equality holds by the substitution rule. By the definition of λ, Plancherel's theorem and the fact that $2\pi iy\hat{\phi} = \mathcal{F}_{\mathbb{R}^m}\{\nabla\phi\}$, we obtain that the right side of Equation (A.118) equals

$$r^{-2}\int_{y\in\mathbb{R}^m}|y|^2\hat{\phi}(y)\hat{\phi}(y)dy = r^{-2}\|y\hat{\phi}(y)\|^2_{2,\mathbb{R}^m} = r^{-2}\|(2\pi)^{-1}\nabla\phi\|^2_{2,\mathbb{R}^m} = m/r^2.$$

where the last equation follows from integrating the following function over $\mathbb{R}^m$, which proves (iv).

$$|(2\pi)^{-1}\nabla\phi(x)|^2 = \begin{cases} 2^{2m}\sum_{j=1}^m \sin^2(2\pi x_j)\prod_{k\neq j}\cos^2(2\pi x_k) & \text{if } \mathbf{x} \in [-\frac{1}{4},\frac{1}{4}]^m \\ 0 & \text{otherwise}\end{cases}$$

$\square$

Combining Lemma A.22 and Lemma A.21 we arrive at a proof for Theorem A.19.

Proof of Theorem A.19. Put $\mathbf{t} = \mathbf{f} \star K_r = \int_{t \in \mathbb{T}^m} \mathbf{f}(t) K_r(\cdot - t) dt$ with K_r as in Lemma A.22. As K_r satisfies the requirements of Lemma A.21 and

$$\frac{r^2}{m} \int_{t \in [-1/2,1/2]^m} |t|^2 K_r(t) dt \leq 1,$$

by Lemma A.22(iv), we have $\|\mathbf{f} - \mathbf{t}\|_{p,\mathbb{T}^m} \leq 2\omega_2(\mathbf{f}, \sqrt{m}/r) \leq 2\sqrt{m}\,\mathrm{Lip}(f)/r$. By Lemma A.22(iii) and the convolution formula, we have $\mathcal{F}_{\mathbb{T}^m}\{\mathbf{t}\} = \mathcal{F}_{\mathbb{T}^m}\{\mathbf{f}\} \cdot \mathcal{F}_{\mathbb{T}^m}\{K_r\} = \mathcal{F}_{\mathbb{T}^m}\{\mathbf{f}\} \cdot \lambda(\cdot/r)\big|_{\mathbb{Z}^m}$. Since $\lambda(\cdot/r)$ only has support in $[-r/2, r/2]^m$, the Fourier transform of $\mathbf{t}$ has also only support there. $\square$

A.5. The Gaussian State

A.5.1. Reducing to the One-dimensional Case

In this section, we estimate the exact quantum complexity of obtaining an approximation, in the trace distance, of the state

$$\frac{1}{\sqrt{\rho_{1/s}(\mathbb{D}^m_{\mathrm{rep}})}} \sum_{\mathbf{x} \in \mathbb{D}^m_{\mathrm{rep}}} \sqrt{\rho_{1/s}(\mathbf{x})} |\mathbf{x}\rangle, \tag{A.119}$$

where $\mathbb{D}^m_{\mathrm{rep}} = \frac{1}{q}\mathbb{Z}^m \cap [-1/2, 1/2)^m$, and where $\rho_{1/s}(\cdot) = e^{-\pi s^2 \|\cdot\|^2}$ is the Gaussian function (see Section 2.5.3).

An element $|\mathbf{x}\rangle$ with $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{D}^m_{\mathrm{rep}}$ is represented as a tensor product $|x_1\rangle \otimes \ldots \otimes |x_m\rangle$. As the function $\sqrt{\rho_{1/s}(x)} = \rho_{\sqrt{2}/s}(\mathbf{x})$ can be written as a product of functions with separated variables as well, we obtain that Equation (A.119) equals

$$\bigotimes_{j=1}^{m} \frac{1}{\sqrt{\rho_{1/s}(\frac{1}{q}[q]_c)}} \sum_{x \in \frac{1}{q}[q]_c} \sqrt{\rho_{1/s}(x)} |x\rangle,$$

where $\frac{1}{q}[q]_c = \frac{1}{q}\mathbb{Z} \cap [-1/2, 1/2)$. Therefore, the problem of approximating the state as in Equation (A.119) reduces to the one-dimensional case. By rescaling the variable $x \in \frac{1}{q}[q]_c$, the computation of this one-dimensional state boils down to calculating the following quantum state, with $\varsigma = q/s$.

$$|\rho_{\varsigma,q}\rangle := \frac{1}{\sqrt{\rho_\varsigma([q]_c)}} \sum_{x\in[q]_c} \sqrt{\rho_\varsigma(x)} \cdot |x\rangle.$$

Here, $[q]_c = \{-\frac{q}{2}+1, \dots, 0, \dots, \frac{q}{2}\}$, and $q = 2^Q$ is a 2-power, for simplicity.

A.5.2. The Periodic and Non-periodic Discrete Gaussian

To obtain a Gaussian superposition in one dimension, we follow a method of Kitaev and Webb [KW08]. Their algorithm is an improvement of that of Grover and Rudolph [GR02].

Kitaev and Webb's algorithm actually does not compute a discrete Gaussian quantum state, but something very close; a *periodized* discrete Gaussian quantum state. This periodized state has the advantage of having a more natural normalization and, more importantly, having a specific *sum decomposition.* These advantages lead to a slightly more efficient algorithm [KW08] computing the discrete Gaussian superposition, compared to the algorithm of Grover and Rudolph.

Definition A.23 (Discrete Periodized Gaussian function)**.** *For $\varsigma \in \mathbb{R}_{>0}$ and $q = 2^Q$ a power of two, we denote by $\xi_{\varsigma,q} : \mathbb{Z}/q\mathbb{Z} \to \mathbb{R}_{>0}$ the function defined by the following rule*

$$\xi_{\varsigma,q}(x) = \sqrt{\sum_{z\in\mathbb{Z}} \rho_\varsigma(x+qz)}.$$

The associated quantum state is defined as follows

$$|\xi_{\varsigma,q}\rangle = \frac{1}{\sqrt{\rho_\varsigma(\mathbb{Z})}} \sum_{x\in[q]_c} \xi_{\varsigma,q}(x)|x\rangle$$

Lemma A.24. *Let $\varsigma \in \mathbb{R}_{>0}$ and $q = 2^Q \in \mathbb{N}$, with $q \geq \varsigma$. Then*

$$D\left(|\xi_{\varsigma,q}\rangle, |\rho_{\varsigma,q}\rangle\right) \leq \exp\left(-\frac{q^2}{2\varsigma^2}\right)$$

where D is the trace distance [NC11, §9.2.1].

Proof. Since $\xi_{\varsigma,q}(x) \geq \sqrt{\rho_\varsigma(x)}$, we have, writing out the definitions,

$$\begin{aligned}\langle \xi_{\varsigma,q} | \rho_{\varsigma,q} \rangle &= \frac{\sum_{x\in[q]_c} \xi_{\varsigma,q}(x)\sqrt{\rho_\varsigma(x)}}{\sqrt{\rho_\varsigma(\mathbb{Z})\rho_\varsigma([q]_c)}} \\ &\geq \frac{\sum_{x\in[q]_c} \rho_\varsigma(x)}{\sqrt{\rho_\varsigma(\mathbb{Z})\rho_\varsigma([q]_c)}} = \sqrt{\rho_\varsigma([q]_c)/\rho_\varsigma(\mathbb{Z})}\,.\end{aligned}$$

Since the trace distance between the pure states $|\xi_{\varsigma,q}\rangle$ and $|\rho_{\varsigma,q}\rangle$ is equal to $\sqrt{1-|\langle \xi_{\varsigma,q}|\rho_{\varsigma,q}\rangle|^2}$ [NC11, §9.2], we obtain

$$\begin{aligned}D\left(|\xi_{\varsigma,q}\rangle, |\rho_{\varsigma,q}\rangle\right) &\leq \sqrt{1-\rho_\varsigma([q]_c)/\rho_\varsigma(\mathbb{Z})} = \sqrt{\rho_\varsigma(\mathbb{Z}\setminus[q]_c)} \\ &\leq \sqrt{\beta^{(1)}_{q/\varsigma}} \leq \exp\left(-\frac{q^2}{2\varsigma^2}\right)\,,\end{aligned}$$

where we applied Banaszczyk's tail bound (see Lemma 2.25). □

Above lemma essentially states that whenever q is relatively large, and ς is not too large, then the periodic discrete Gaussian and the (non-periodic) discrete Gaussian are very close in trace distance. That has as a consequence that the associated measurement probability distributions are close in total variation distance [NC11, Thm. 9.1].

A.5.3. Computing the Periodic Gaussian State

According to the previous subsection, we can resort to computing the state $|\xi_{\varsigma,q}\rangle$ instead of $|\rho_{\varsigma,q}\rangle$, as they are close to each other for a suitable choice of parameters. As already mentioned, the quantum state $|\xi_{\varsigma,q}\rangle$ can be decomposed into a superposition that can be exploited algorithmically. In order to phrase this decomposition we first introduce the following notation of a quantum state 'translated' by $t \in \mathbb{R}$.

$$|\xi_{\varsigma,q}(\cdot + t)\rangle = \frac{1}{\sqrt{\rho_\varsigma(\mathbb{Z}+t)}} \sum_{x\in[q]_c} \xi_{\varsigma,q}(x+t)|x\rangle$$

Likewise, we denote

$$|\rho_{\varsigma,q}(\cdot + t)\rangle := \frac{1}{\sqrt{\rho_\varsigma([q]_c + t)}} \sum_{x \in [q]_c} \sqrt{\rho_\varsigma(x+t)} \cdot |x\rangle$$

Now we are ready to state the decomposition lemma.

Lemma A.25 ([KW08, Eq. (11)]). *Let $\varsigma \in \mathbb{R}_{>0}$, $t \in \mathbb{R}$ and let $q \in \mathbb{N}$ be even. Then*

$$|\xi_{\varsigma,q}(\cdot + 2t)\rangle = |\xi_{\frac{\varsigma}{2},\frac{q}{2}}(\cdot + t)\rangle \otimes \cos\alpha|0\rangle + |\xi_{\frac{\varsigma}{2},\frac{q}{2}}(\cdot + t + \tfrac{1}{2})\rangle \otimes \sin\alpha|1\rangle,$$

with $\alpha = \arccos\left(\sqrt{\rho_{\frac{\varsigma}{2}}(\mathbb{Z}+t)/\rho_\varsigma(\mathbb{Z}+2t)}\right)$.

Proof. Splitting the sum into a part with even numbers and a part with odd numbers, we obtain

$$\begin{aligned}
&\sqrt{\rho_\varsigma(\mathbb{Z}+2t)} \cdot |\xi_{\varsigma,q}(\cdot + 2t)\rangle \\
&= \sum_{x \in [q]_c} \xi_{\varsigma,q}(x+2t)|j\rangle \\
&= \sum_{x \in [\frac{q}{2}]_c} \xi_{\varsigma,q}(2x+2t)|x\rangle|0\rangle + \sum_{x \in [\frac{q}{2}]_c} \xi_{\varsigma,q}(2x+1+2t)|x\rangle|1\rangle. \qquad \text{(A.120)}
\end{aligned}$$

We now focus the computation on the sum over the odd numbers, as the computation for the even numbers is similar. By writing out the definition of $\xi_{\varsigma,q}(x)$ and putting the scalar 2 into the standard deviation ς, we obtain

$$\begin{aligned}
\xi_{\varsigma,q}(2x+1+2t)^2 &= \rho_\varsigma(2x+1+2t+q\mathbb{Z}) \\
&= \rho_{\frac{\varsigma}{2}}(x+t+\tfrac{1}{2}+\tfrac{q}{2}\cdot\mathbb{Z}) = \xi_{\frac{\varsigma}{2},\frac{q}{2}}(x+\tfrac{1}{2}+t)^2.
\end{aligned}$$

Using a similar computation for the even case and writing out the definitions, we obtain

$$\begin{aligned}
&\sqrt{\rho_\varsigma(\mathbb{Z}+2t)} \cdot |\xi_{\varsigma,q}(\cdot + 2t)\rangle \\
=&\sqrt{\rho_{\frac{\varsigma}{2}}(\mathbb{Z}+t)} \cdot |\xi_{\frac{\varsigma}{2},\frac{q}{2}}(\cdot + t)\rangle \otimes |0\rangle + \sqrt{\rho_{\frac{\varsigma}{2}}(\mathbb{Z}+t+\tfrac{1}{2})} \cdot |\xi_{\frac{\varsigma}{2},\frac{q}{2}}(\cdot + t + \tfrac{1}{2})\rangle \otimes |1\rangle.
\end{aligned}$$

Dividing above expression by $\sqrt{\rho_\varsigma(\mathbb{Z}+2t)}$ we obtain Equation (A.120), where we use the fact that $\rho_{\varsigma/2}(\mathbb{Z}+t) + \rho_{\varsigma/2}(\mathbb{Z}+t+\frac{1}{2}) = \rho_\varsigma(\mathbb{Z}+2t)$. □

This lemma directly leads to an algorithm for computing (an approximation of) the state $|\xi_{\varsigma,q}\rangle$, which is spelled out in Algorithm 10.

Algorithm 10: Recursive algorithm preparing the periodic Gaussian state

Require: The parameters $\varsigma \in \mathbb{R}_{>0}, t \in \mathbb{R}$, $k \in \mathbb{N}$ and $q = 2^Q \in \mathbb{N}$.

Ensure: An approximation of the state $|\xi_{\varsigma,q}(\cdot + t)\rangle$

1: **Initial state**: $|t, \varsigma, q\rangle|0^Q\rangle$;

2: **Compute the α-rotation by on the last qubit**: Compute α with bit-precision k and store it in a k-qubit ancilla register. Apply the α-rotation on the last qubit and uncompute α again, which yields the state $|t, \varsigma, q\rangle|0^{Q-1}\rangle\,(\cos\alpha|0\rangle + \sin\alpha|1\rangle)$;

3: **Apply a parameter change, controlled by the last qubit** yielding $\cos\alpha|\frac{t}{2}, \frac{\varsigma}{2}, \frac{q}{2}\rangle|0^{Q-1}\rangle|0\rangle + \sin\alpha|\frac{t+1}{2}, \frac{\varsigma}{2}, \frac{q}{2}\rangle|0^{Q-1}\rangle|1\rangle$;

4: **Apply quantum recursion (step 2 and 3) on all qubits except the last, whenever** $q > 1$, yielding $\cos\alpha|\frac{t}{2}, \frac{\varsigma}{2}, \frac{q}{2}\rangle|\xi_{\frac{\varsigma}{2},\frac{q}{2}}(\cdot + \frac{t}{2})\rangle|0\rangle + \sin\alpha|\frac{t+1}{2}, \frac{\varsigma}{2}, \frac{q}{2}\rangle|\xi_{\frac{\varsigma}{2},\frac{q}{2}}(\cdot + \frac{t+1}{2})\rangle|0\rangle$;

5: **Un-apply the controlled parameter change,** yielding $|t, \varsigma, q\rangle\left(\cos\alpha|\xi_{\frac{\varsigma}{2},\frac{q}{2}}(\cdot + \frac{t}{2})\rangle|0\rangle + \sin\alpha|\xi_{\frac{\varsigma}{2},\frac{q}{2}}(\cdot + \frac{t+1}{2})\rangle|1\rangle\right) =$ $|t, \varsigma, q\rangle|\xi_{\varsigma,q}(\cdot + t)\rangle$;

A.5.4. Estimating the Complexity and Fidelity of Algorithm 10

We will discuss now how well Algorithm 10 approximates the state $|\xi_{\varsigma,q}\rangle$. For ease of analysis, we will assume (without loss of generality) that the operations on the parameters ς (in step 3 of Algorithm 10) are exact. Then it turns out that the approximation error is primarily caused by the fact that the angle α in the algorithm is computed up to bit precision k (meaning, with error at most 2^{-k}). This is made precise in the following lemma.

Lemma A.26. *Let $|\tilde{\xi}_{\varsigma,q}(\cdot+t)\rangle$ be the output of Algorithm 10 with input parameters $\varsigma \in \mathbb{R}_{>0}$, $k \in \mathbb{N}$, $q = 2^Q \in \mathbb{N}$ and $t \in (-1,1)$, then we have*

$$T\left(|\tilde{\xi}_{\varsigma,q}(\cdot+t)\rangle, |\xi_{\varsigma,q}(\cdot+t)\rangle\right) \leq 2^{-k}Q$$

where T denotes the trace distance.

Proof. The proof proceeds by induction on Q, where $q = 2^Q$. We use the the identity $D(|\psi\rangle, |\phi\rangle)^2 + |\langle\psi|\phi\rangle|^2 = 1$ multiple times throughout the proof (see [NC11, §9.2]). Let $\tilde{\alpha}$ be a k-bit approximation of α, i.e., $|\alpha - \tilde{\alpha}| < 2^{-k}$, and denote $|\tilde{\xi}_{\varsigma,q}(\cdot+t)\rangle = \cos\tilde{\alpha}|\tilde{\xi}_{\frac{\varsigma}{2},\frac{q}{2}}(\cdot+\frac{t}{2})\rangle|0\rangle + \sin\tilde{\alpha}|\tilde{\xi}_{\frac{\varsigma}{2},\frac{q}{2}}(\cdot+\frac{t+1}{2})\rangle|1\rangle$ for the output of Algorithm 10 with input parameters $\varsigma, k, q = 2^Q$ and $t \in (-1,1)$. Without loss of generality, we assume that $t = 0$ for sake of clarity; for arbitrary $t \in (-1,1)$ the calculation is similar.

$$\langle\tilde{\xi}_{\varsigma,q}|\xi_{\varsigma,q}\rangle = \cos(\alpha)\cos(\tilde{\alpha})\langle\tilde{\xi}_{\frac{\varsigma}{2},\frac{q}{2}}|\xi_{\frac{\varsigma}{2},\frac{q}{2}}\rangle + \sin(\alpha)\sin(\tilde{\alpha})\langle\tilde{\xi}_{\frac{\varsigma}{2},\frac{q}{2}}(\cdot+\tfrac{1}{2})|\xi_{\frac{\varsigma}{2},\frac{q}{2}}(\cdot+\tfrac{1}{2})\rangle.$$

By the induction hypothesis, we have

$$|\langle\tilde{\xi}_{\frac{\varsigma}{2},\frac{q}{2}}(\cdot+t)|\xi_{\frac{\varsigma}{2},\frac{q}{2}}(\cdot+t)\rangle| \geq \sqrt{1-(Q-1)^2 2^{-2k}}$$

for $t \in (-1,1)$. Using the trigonometric identity $\cos(\alpha)\cos(\tilde{\alpha}) + \sin(\alpha)\sin(\tilde{\alpha}) = \cos(\alpha - \tilde{\alpha})$ and the fact that the periodic Gaussian state only has positive amplitudes, we obtain

$$|\langle\tilde{\xi}_{\varsigma,q}|\xi_{\varsigma,q}\rangle| \geq \cos(\alpha-\tilde{\alpha})\sqrt{1-(Q-1)^2 2^{-2k}}$$

Therefore $D(|\xi_{\varsigma,q}\rangle, |\tilde{\xi}_{\varsigma,q}\rangle) = \sqrt{1-|\langle\xi_{\varsigma,q}|\tilde{\xi}_{\varsigma,q}\rangle|^2} \leq \sin(\alpha-\tilde{\alpha}) + (Q-1)2^{-k} \leq Q2^{-k}$. Note that we omitted the base case, which can be done by a very similar computation using the same trigonometric identity. □

Lemma A.27. *Computing α with k-bits of precision in step 2 of Algorithm 10 can be done within $O(k^{3/2} \cdot \mathrm{polylog}(k))$ operations.*

Proof. Can be found in Appendix A.5.5. □

Proposition A.28. *Algorithm 10 with input $\varsigma \in \mathbb{R}_{>0}$, $k \in \mathbb{N}$, $q = 2^Q \in \mathbb{N}$ and $t \in (-1, 1)$ uses $O(Q + k)$ qubits and $O(Q \cdot k^{3/2} \cdot \operatorname{polylog}(k))$ quantum gates.*

Proof. The number of qubits used in Algorithm 10 equals $O(Q+k)$, because α is stored in k ancilla qubits during step 2 with bit precision k. The variable $\varsigma \in \mathbb{R}$ can be stored with similar precision.

For the number of gates, we go through the relevant steps of Algorithm 10. Step 2 computes (and uncomputes) α with precision 2^{-k}. By Lemma A.27, this costs at most $O(k^{3/2} \operatorname{polylog}(k))$ quantum gates. The α-rotation in this step costs k quantum gates, as a sequence of controlled $R_{\pi/2^j}$-gates.

Step 3 (and step 5) is a parameter change, which costs a mere constant number of gates. Step 6 applies recursion, which, by induction, costs $O((Q-1) \cdot k^{3/2} \cdot \operatorname{polylog}(k))$ gates. Adding all together gives a number of $O(Q \cdot k^{3/2} \cdot \operatorname{polylog}(k))$ gates. $\square$

Theorem A.29. *For $q = 2^Q \in \mathbb{N}$, $k \in \mathbb{N}$ and $\varsigma > 1$, there exists an quantum algorithm that prepares the one-dimensional Gaussian state*

$$|\rho_{\varsigma,q}\rangle = \frac{1}{\sqrt{\rho_\varsigma([q]_c)}} \cdot \sum_{x \in [q]_c} \sqrt{\rho_\varsigma(x)} |x\rangle \tag{A.121}$$

within trace distance $\exp(-\frac{q^2}{2\varsigma^2}) + \log(q) 2^{-k}$, using $O(\log(q) + k)$ qubits and $O(\log(q) \cdot k^{3/2} \cdot \operatorname{polylog}(k))$ quantum gates. Here, $[q]_c$ denotes $\{-\frac{q}{2}, \ldots, \frac{q-1}{2}\}$.

Proof. The state in Equation (A.121) can be approximated by running Algorithm 10 with parameters $\varsigma, q = 2^Q$, $t = 0$ and k. Combining Lemma A.24 and Lemma A.26 and using the fact that we can add trace distances [NC11, Ch. 9], this approximation is within trace distance $\exp(-\frac{q^2}{2\varsigma^2}) + Q 2^{-k}$.

For the running time, use Proposition A.28 to conclude that Algorithm 10 with the mentioned parameters uses $O(Q+k)$ qubits and $O(Q \cdot k^{3/2})$ quantum gates, which proves the claim. $\square$

Theorem 3.12. *For $q = 2^Q \in \mathbb{N}$, error parameter $\eta \in (0,1)$ and $s > 2\sqrt{\log(m/\eta)}$, there exists an quantum algorithm that prepares the higher-dimensional Gaussian state*

$$\frac{1}{\sqrt{\rho_{1/s}(\mathbb{D}^m_{\text{rep}})}} \sum_{\mathbf{x} \in \mathbb{D}^m_{\text{rep}}} \sqrt{\rho_{1/s}(\mathbf{x})} |\mathbf{x}\rangle = \bigotimes_{j=1}^{m} \frac{1}{\sqrt{\rho_{1/s}(\frac{1}{q}[q]_c)}} \sum_{x \in \frac{1}{q}[q]_c} \sqrt{\rho_{1/s}(x)} |x\rangle,$$

within trace distance η, using $O(mQ + \log(\eta^{-1}))$ qubits and using $O(mQ \cdot \log(mQ\eta^{-1})^2)$ quantum gates.

Proof. Instantiating Theorem A.29 with $\varsigma = q/s$ and $k = \lceil \log(2mQ\eta^{-1}) \rceil$ and rescaling the states x by q, gives the desired quantum state.

Note that the trace distance needs to be multiplied by m, due to the m-fold tensor product. This yields a trace distance of $m \exp(-s^2/2) + mQ2^{-k} \leq \frac{1}{2}\eta + \frac{1}{2}\eta \leq \eta$. Regarding qubits, we need $O(mQ)$ qubits for storing the m-dimensional Gaussian state and $O(k) = O(\log(\eta^{-1}) + \log(mQ))$ ancilla qubits, for computing and uncomputing the rotation angle α. Together this is at most $O(mQ + \log(\eta^{-1}))$ qubits.

For the number of quantum gates we just multiply the number of gates used in Theorem A.29 by m, instantiating $k = \lfloor \log(2mQ\eta^{-1}) \rceil$ and simplifying the expressions using the big-O notation:

$$O(m \cdot \log(q) \cdot k^{3/2} \cdot \text{polylog}(k)) \leq O(mQ \cdot k^2) = O(mQ \cdot \log(mQ\eta^{-1})^2).$$

□

A.5.5. Proof of Lemma A.27

Lemma A.30. *The value $\rho_{\frac{\mu}{2}, \frac{\varsigma}{2\sqrt{2}}}(\mathbb{Z})$ can be computed with relative precision 2^{-k} within time $O(k^{3/2}\,\text{polylog}(k))$.*

Proof. We distinguish two cases.

- $\varsigma < \sqrt{2}$. Then, by Lemma 2.25,

$$\left|\rho_{\mu,\frac{\varsigma}{\sqrt{2}}}(\mathbb{Z}) - \rho_{\lfloor\mu\rceil,\frac{\varsigma}{\sqrt{2}}}(\{-h,\dots,0,\dots h\})\right| \leq \beta^{(1)}_{\sqrt{2}h/\varsigma} \cdot \rho_{\mu,\frac{\varsigma}{\sqrt{2}}}(\mathbb{Z}).$$

- $\varsigma > \sqrt{2}$. Applying the Poisson summation formula, we obtain

$$\rho_{\mu,\frac{\varsigma}{\sqrt{2}}}(\mathbb{Z}) = \frac{\varsigma}{\sqrt{2}} \sum_{t\in\mathbb{Z}} \rho_{0,\frac{\sqrt{2}}{\varsigma}}(t)e^{-2\pi i t\mu}.$$

  Therefore

$$\left|\rho_{\mu,\frac{\varsigma}{\sqrt{2}}}(\mathbb{Z}) - \frac{\varsigma}{\sqrt{2}} \sum_{t\in\{-h,\dots,0,\dots h\}} \rho_{\frac{\sqrt{2}}{\varsigma}}(t)e^{-2\pi i t\mu}\right| \leq \frac{\varsigma}{\sqrt{2}}\beta^{(1)}_{\varsigma h/\sqrt{2}} \cdot \rho_{0,\sqrt{2}/\varsigma}(\mathbb{Z})$$

  which is bounded by $\beta^{(1)}_{\varsigma h/\sqrt{2}} \cdot \rho_{0,\varsigma/\sqrt{2}}(\mathbb{Z}) \leq 2\beta^{(1)}_{\varsigma h/\sqrt{2}} \cdot \rho_{\mu,\frac{\varsigma}{\sqrt{2}}}(\mathbb{Z})$, by the Poisson summation formula and by smoothing arguments (see Lemma 2.31), as $\rho_{\mu,\varsigma/\sqrt{2}}(\mathbb{Z}) \geq (1-2\beta^{(1)}_{s/\sqrt{2}})\rho_{0,\varsigma/\sqrt{2}} \geq \frac{1}{2}\rho_{0,\varsigma/\sqrt{2}}$.

So the relative error is at most $2\beta^{(1)}_h \leq e^{-(h-1)^2}$ for $h > 2$. Therefore, choosing $h = k^{1/2}+1$ is enough to compute $\rho_{\frac{\mu}{2},\frac{\varsigma}{2\sqrt{2}}}(\mathbb{Z})$ with relative error 2^{-k}. Because evaluating an exponential function takes $O(k\cdot\mathrm{polylog}(k))$ time [Bre10], we arrive at the claim. □

Lemma A.31. *The fraction $\rho_{\frac{\mu}{2},\frac{\varsigma}{2\sqrt{2}}}(\mathbb{Z})/\rho_{\mu,\frac{\varsigma}{\sqrt{2}}}(\mathbb{Z})$ can be computed with precision 2^{-k} within time $O(k^{3/2}\cdot\mathrm{polylog}(k))$.*

Proof. Denote $a = \rho_{\frac{\mu}{2},\frac{\varsigma}{2\sqrt{2}}}(\mathbb{Z})$ and $b = \rho_{\mu,\frac{\varsigma}{\sqrt{2}}}(\mathbb{Z})$. Suppose we have relative errors $|\tilde{a}-a| \leq 2^{-k}a/2 \leq 2^{-k}b/2$, $|\tilde{b}-b| \leq 2^{-k}b/2$ and $\tilde{a}/\tilde{b} < 1$, then $\left|\frac{\tilde{a}}{\tilde{b}} - \frac{a}{b}\right| \leq \frac{|\tilde{b}(a-\tilde{a})-\tilde{a}(b-\tilde{b})|}{b\tilde{b}} \leq \frac{|a-\tilde{a}|}{b} + \frac{|b-\tilde{b}|}{b} \leq 2^{-k}$. By Lemma A.30, we see that both a and b can be computed within relative precision $2^{-k}/2$ within time $O(k^{3/2}\,\mathrm{polylog}(k))$. Therefore, the fraction a/b can be computed with absolute precision 2^{-k} within time $O(k^{3/2}\,\mathrm{polylog}(k))$. □

Lemma A.32. *For $x \in [0, 1-\varepsilon]$ and $\varepsilon < \frac{3}{4}$, we have*

$$|\arccos(\sqrt{x+\varepsilon}) - \arccos(\sqrt{x})| \leq 8\sqrt{\varepsilon}$$

Proof. The derivative of $\arccos(\sqrt{t})$ equals $w(t) = -\frac{2}{\sqrt{(1-t)t}}$. Therefore

$$\begin{aligned}|\arccos(\sqrt{x+\varepsilon}) - \arccos(\sqrt{x})| &\leq \left|\int_x^{x+\varepsilon} w(t)dt\right| \\ &\leq \int_x^{x+\varepsilon} |w(t)|dt \leq \int_0^{\varepsilon} |w(t)|dt.\end{aligned}$$

The last inequality follows from the fact that $w(t)$ is both strictly decreasing on $[0, 1/2]$ and symmetric around $t = 1/2$. The claim then follows from the bound $\int_0^\varepsilon |w(t)|dt = \int_0^\varepsilon \frac{2}{\sqrt{(1-x)x}} \leq 4\int_0^\varepsilon \frac{dt}{\sqrt{t}} = 8\sqrt{\varepsilon}$. ◻

By combining Lemma A.31 and Lemma A.32, we obtain that the expression $\arccos\sqrt{\rho_{\frac{\mu}{2},\frac{\varsigma}{2\sqrt{2}}}(\mathbb{Z})/\rho_{\mu,\frac{\varsigma}{\sqrt{2}}}(\mathbb{Z})}$ can be approximated with k bits of precision within $O(k^{3/2} \cdot \mathrm{polylog}(k))$ time, which proves Lemma A.27.

A.6. Discrete Gaussians

Recall, for $n \in \mathbb{N}_{>0}$ and any parameter $s > 0$, we consider the n-dimensional *Gaussian function*

$$\rho_s^{(n)} : \mathbb{R}^n \to \mathbb{C}\,,\ x \mapsto e^{-\frac{\pi\|x\|^2}{s^2}}\,,$$

where we drop the (n) whenever it is clear from the context.

Lemma A.33. *We have*

$$|\rho_s(x) - \rho_s(y)| \leq \tfrac{\pi}{s^2} \cdot \|x-y\|\|x+y\| \cdot \rho_{2s}(x-y)\rho_{2s}(x+y).$$

Proof. We have, using the inequality $|1-x| \leq |\ln(x)|$ (for all $x > 0$) and the reverse triangle inequality,

$$\begin{aligned}|\rho_s(x) - \rho_s(y)| \leq \rho_s(x)|1 - \rho_s(x)/\rho_s(y)| &\leq \tfrac{\pi}{s^2} \cdot \rho_s(x)\big|\|x\|^2 - \|y\|^2\big| \\ &\leq \tfrac{\pi}{s^2} \cdot \rho_s(x) \cdot \|x-y\|\|x+y\|.\end{aligned}$$

Since the bound above is symmetric in x and y, we might as well replace $\rho_s(x)$ by $\rho_s(y)$ in the rightmost expression, or even by their *harmonic* *mean* $\sqrt{\rho_s(x)\rho_s(y)}$. Rewriting this harmonic mean $\sqrt{\rho_s(x)\rho_s(y)} = \rho_{2s}(x+y)\rho_{2s}(x-y)$ using multiplicative properties of the Gaussian function (see Lemma 2.23), we obtain the result. $\square$

Lemma A.34 (Bounds on the first and second moment of the discrete Gaussian)**.** *Let* $\Lambda \subseteq \mathbb{R}^n$ *be a full-rank lattice and let* $c \in \mathbb{R}^n$ *and let* $s > 4\sqrt{n} \cdot \lambda_n(\Lambda)$. *Then, we have*

$$\frac{1}{\rho_s(\Lambda - c)} \sum_{\ell \in \Lambda} \rho_s(\ell - c)\|\ell - c\|^2 \leq 2ns^2$$
$$\frac{1}{\rho_s(\Lambda - c)} \sum_{\ell \in \Lambda} \rho_s(\ell - c)\|\ell - c\| \leq 1 + 2ns^2.$$

Proof. Using a result from Micciancio and Regev [MR07, Lm. 4.3] and the fact that $s > 4\sqrt{n}\lambda_n(\Lambda) > 2\eta_{1/2}(\Lambda)$, we directly obtain

$$\frac{1}{\rho_s(\Lambda - c)} \sum_{\ell \in \Lambda} \rho_s(\ell - c)\|\ell - c\|^2 \leq \left(\frac{1}{2\pi} + 1\right) ns^2 \leq 2ns^2.$$

For the second bound, split up the sum in a part where $\|\ell - c\| \leq 1$ and $\|\ell - c\| > 1$. It is clear that the former must be bounded by 1, whereas the latter is bounded by $2ns^2$, by the fact that $\|\ell - c\| \leq \|\ell - c\|^2$ in that case. $\square$

Definition A.35. *Let* $\mathbf{t} \in SL_m(\mathbb{R})$ *be a diagonal matrix and let* $\Lambda \subseteq \mathbb{R}^m$ *be a full rank lattice. Then we define the distribution* $\mathcal{G}_{\Lambda,s/\mathbf{t},c}$ *by the rule*

$$\mathcal{G}_{\Lambda,s/\mathbf{t},c}(\ell) = \frac{\rho_s(\mathbf{t}(\ell - c))}{\rho_s(\mathbf{t}(\Lambda - c))}$$

Remark A.36. *Note that this definition coincides reasonably with the definition of the Gaussian distribution with a 'variance matrix' [Gut09, Ch. 5].*

Lemma A.37. *Let $\Lambda \subseteq \mathbb{R}^m$ be a full-rank lattice, $\varepsilon \in (0, \frac{1}{2})$, $c, \tilde{c} \in \mathbb{R}^m$, and $s \geq \eta_\varepsilon(\Lambda)$. Then*

$$\|\mathcal{G}_{\Lambda,s,c} - \mathcal{G}_{\Lambda,s,\tilde{c}}\| \leq 4\varepsilon + (\tfrac{2\pi}{s^2} + 4\pi n)\|c - \tilde{c}\|$$

Proof. By smoothing properties, we have $\rho_s(\Lambda - c), \rho_s(\Lambda - \tilde{c}) \in (1 - \varepsilon, 1 + \varepsilon)\rho_s(\Lambda)$. Allowing an extra error of 4ε, we can therefore replace the denominator in the definitions of $\mathcal{G}_{\Lambda,s,c}$ and $\mathcal{G}_{\Lambda,s,\tilde{c}}$ by $\rho_s(\Lambda)$.

$$\|\mathcal{G}_{\Lambda,s,c} - \mathcal{G}_{\Lambda,s,\tilde{c}}\| \leq 4\varepsilon + \frac{1}{\rho_s(\Lambda)} \sum_{\ell \in \Lambda} |\rho_s(\ell - c) - \rho_s(\ell - \tilde{c})|.$$

By Lemma A.33 (using the fact that $\rho_{s/2}(c - \tilde{c}) \leq 1$) and subsequently Lemma A.34, we have

$$\begin{aligned}\sum_{\ell \in \Lambda} |\rho_s(\ell - c) - \rho_s(\ell - \tilde{c})| &\leq \tfrac{\pi}{s^2}\|c - \tilde{c}\| \sum_{\ell \in \Lambda} \rho_{2s}(2\ell - (c + \tilde{c}))\|2\ell - (c + \tilde{c})\| \\ &\leq \tfrac{\pi}{s^2}(1 + 2ns^2)\|c - \tilde{c}\|\rho_s(\Lambda - \tfrac{c+\tilde{c}}{2}) \\ &\leq \tfrac{2\pi}{s^2}(1 + 2ns^2)\|c - \tilde{c}\|\rho_s(\Lambda).\end{aligned}$$

Combining the two bounds yields the result. □

Lemma A.38. *Let $\Lambda \subseteq \mathbb{R}^m$ be a full-rank lattice, $c \in \mathbb{R}^m$, $\varepsilon, \delta \in (0, \frac{1}{2})$, $\mathbf{t} \in SL_m(\mathbb{R})$ be a diagonal matrix with*[2] *$|\mathbf{t} - 1| \leq \delta$. Additionally, assume that $s \geq \max(\eta_\varepsilon(\Lambda), \eta_\varepsilon(\mathbf{t}\Lambda))$. Then*

$$\|\mathcal{G}_{\Lambda,s/\mathbf{t},c} - \mathcal{G}_{\Lambda,s,c}\| \leq 4\varepsilon + 2\pi n\delta$$

Proof. Since $\det(\mathbf{t}\Lambda) = \det(\Lambda)\prod_i \mathbf{t}_{ii} = \det(\Lambda)$, we have $\rho_s(\Lambda - c), \rho_s(\mathbf{t}(\Lambda - c)) \in (1 - \varepsilon, 1 + \varepsilon)\rho_s(\Lambda)$, by smoothing properties of the Gaussian function. Allowing an extra error of 4ε, we can therefore replace the denominator in the definitions of $\mathcal{G}_{\Lambda,s,c}$ and $\mathcal{G}_{\Lambda,s/\mathbf{t},c}$ by $\rho_s(\Lambda)$.

$$\|\mathcal{G}_{\Lambda,s/\mathbf{t},c} - \mathcal{G}_{\Lambda,s,c}\| \leq 4\varepsilon + \frac{1}{\rho_s(\Lambda)} \sum_{v \in \Lambda - c} |\rho_s(\mathbf{t}v) - \rho_s(v)|. \tag{A.122}$$

[2] Here, we mean that the vector $\mathbf{v}$ consisting of the diagonal elements of $\mathbf{t}$ satisfies $|\mathbf{v} - 1| \leq \delta$ in the Euclidean norm.

By Lemma A.33, using the fact that $\rho_{2s}((\mathbf{t}-1)v) \leq 1$ and $\|(\mathbf{t}-1)v\| \leq \delta\|v\|$, we have

$$\begin{aligned} |\rho_s(\mathbf{t}v) - \rho_s(v)| &\leq \tfrac{\delta\pi}{s^2} \cdot \rho_{2s}((1+\mathbf{t})v) \cdot \|v\| \cdot \|(1+\mathbf{t})v\| \\ &\leq \tfrac{\delta\pi}{s^2} \cdot \rho_s((1+\mathbf{t})v) \cdot \|(1+\mathbf{t})v\|^2. \end{aligned} \tag{A.123}$$

Where the last inequality follows from $\|v\| \leq \|(1+\mathbf{t})v\|$, which can be deduced by applying the triangle inequality on $\|v\|$ in the following way.

$$\begin{aligned} \|v\| &\leq \tfrac{1}{2}\|(1+\mathbf{t})v\| + \tfrac{1}{2}\|(1-\mathbf{t})v\| \leq \tfrac{1}{2}\|(1+\mathbf{t})v\| + \tfrac{\delta}{2}\|v\| \\ &\leq \tfrac{1}{2}\|(1+\mathbf{t})v\| + \tfrac{1}{2}\|v\|. \end{aligned}$$

Plugging Equation (A.123) into Equation (A.122), and applying Lemma A.34, we obtain

$$\|\mathcal{G}_{\Lambda,s/\mathbf{t},c} - \mathcal{G}_{\Lambda,s,c}\| \leq 4\varepsilon + \frac{\delta\pi}{s^2}(2ns^2) = 4\varepsilon + 2\pi n\delta.$$

□

Lemma A.39. *Let $\mathbf{t}_0, \mathbf{t}_1 \in SL_m(\mathbb{R})$ be diagonal matrices satisfying*[3] $|\mathbf{t}_0/\mathbf{t}_1 - 1| \leq \delta < 1/2$*, let $\varepsilon \in (0, 1/2)$, let $c \in \mathbb{R}^m$ and let $\Lambda \subseteq \mathbb{R}^m$ be a full rank lattice. Let furthermore $s > \max(\eta_\varepsilon(\mathbf{t}_0\Lambda), \eta_\varepsilon(\mathbf{t}_1\Lambda))$.*

Then,

$$\|\mathcal{G}_{\Lambda_0,s,c} - \mathcal{G}_{\Lambda_0,s/\mathbf{t},c/\mathbf{t}}\| \leq 8\varepsilon + (2\pi n + (\tfrac{2\pi}{s^2} + 4\pi n)\|c\|) \cdot \delta.$$

Proof. We have, writing $\Lambda_0 = \mathbf{t}_0\Lambda$ and $\mathbf{t} = \mathbf{t}_1\mathbf{t}_0^{-1}$,

$$\sum_{\ell\in\Lambda}\left|\frac{\rho_s(\mathbf{t}_0\ell - c)}{\rho_s(\mathbf{t}_0\Lambda - c)} - \frac{\rho_s(\mathbf{t}_1\ell - c)}{\rho_s(\mathbf{t}_1\Lambda - c)}\right| \leq \sum_{\ell_0\in\Lambda_0}\left|\frac{\rho_s(\ell_0 - c)}{\rho_s(\Lambda_0 - c)} - \frac{\rho_s(\mathbf{t}\ell_0 - c)}{\rho_s(\mathbf{t}\Lambda_0 - c)}\right|$$

$$= \|\mathcal{G}_{\Lambda_0,s,c} - \mathcal{G}_{\Lambda_0,s/\mathbf{t},c/\mathbf{t}}\| \leq \|\mathcal{G}_{\Lambda_0,s,c} - \mathcal{G}_{\Lambda_0,s,c/\mathbf{t}}\| + \|\mathcal{G}_{\Lambda_0,s,c/\mathbf{t}} - \mathcal{G}_{\Lambda_0,s/\mathbf{t},c/\mathbf{t}}\|. \tag{A.124}$$

[3] By this we mean that the vector $\mathbf{v} = \mathbf{t}_0/\mathbf{t}_1$ consisting of the diagonal elements of the matrix $\mathbf{t}_0/\mathbf{t}_1$ satisfies $|\mathbf{v} - 1| \leq \delta$ in the Euclidean norm.

Since $s \geq \eta_\varepsilon(\Lambda_0)$, by assumption, we have, by Lemma A.37,

$$\|\mathcal{G}_{\Lambda_0,s,c} - \mathcal{G}_{\Lambda_0,s,c/\mathbf{t}}\| \leq 4\varepsilon + (\tfrac{2\pi}{s^2} + 4\pi n)\|c - c/\mathbf{t}\| \leq 4\varepsilon + (\tfrac{2\pi}{s^2} + 4\pi n)\|c\| \cdot \delta,$$

since $\|1 - 1/\mathbf{t}\| \leq \|1 - \mathbf{t}_0/\mathbf{t}_1\| \leq \delta$ by assumption. Also, since $s \geq \eta_\varepsilon(\mathbf{t}\Lambda_0)$ (note that $\mathbf{t}\Lambda_0 = \mathbf{t}_1\Lambda$), we have, by Lemma A.38,

$$\|\mathcal{G}_{\Lambda_0,s,c/\mathbf{t}} - \mathcal{G}_{\Lambda_0,s/\mathbf{t},c/\mathbf{t}}\| \leq 4\varepsilon + 2\pi n\delta.$$

Combining the bounds into Equation (A.124), we obtain the final claim. □