Second Moment Estimation

Erik Agrell

For a given $n \times m$ *generator matrix* $\boldsymbol{B}$ with linearly independent rows, a *lattice* $\mathcal{L}$ consists of the points $\boldsymbol{uB}$ for all $\boldsymbol{u} \in \mathbb{Z}^n$. By definition, the all-zero vector $\mathbf{0}$ belongs to any lattice. The inner products of all basis vectors with each other are collected in the symmetric, positive definite *Gram matrix* $\boldsymbol{A} = \boldsymbol{B}\boldsymbol{B}^{\mathrm{T}}$. The set of vectors in this subspace that are closer to $\mathbf{0}$ than to any other point in $\mathcal{L}$ is the *Voronoi region* Ω of the lattice. The normalized second moment (NSM) [1], [2, pp. 34, 56–62] is

$$G = \frac{1}{nV^{1+2/n}} \int_{\Omega} \|\boldsymbol{x}\|^2 \,\mathrm{d}\boldsymbol{x}, \tag{1}$$

where $V = (\det \boldsymbol{A})^{1/2}$ is the n-volume of Ω.

An elegant method to generate random vectors uniformly in the Voronoi region Ω of a given lattice was proposed in [3] for the purpose of NSM estimation. Let $\boldsymbol{z}$ be a random vector drawn uniformly from the unit n-cube $[0,1)^n$ and let, for a given generator matrix $\boldsymbol{B}$,

$$\hat{\boldsymbol{u}} = \arg\min_{\boldsymbol{u} \in \mathbb{Z}^n} \|(\boldsymbol{z} - \boldsymbol{u})\boldsymbol{B}\|^2. \tag{2}$$

Now $\hat{\boldsymbol{u}}\boldsymbol{B}$ is the lattice point closest to $\boldsymbol{zB}$ (which is normally not a lattice point). Therefore, $\boldsymbol{e} = (\boldsymbol{z} - \hat{\boldsymbol{u}})\boldsymbol{B}$ is uniformly distributed in Ω. To calculate (2) requires solving the *closest point problem* for a given lattice. Algorithms for this purpose are available for classical, well-structured lattices [3], [4] as well as arbitrary lattices [5], [6].

Using these definitions of $\boldsymbol{z}$, $\hat{\boldsymbol{u}}$, and $\boldsymbol{e}$, the NSM in (1) can be written as

$$G = \mathbb{E}_{\boldsymbol{z}}[g(\boldsymbol{B}, \boldsymbol{z})], \tag{3}$$

where

$$g(\boldsymbol{B}, \boldsymbol{z}) = \frac{1}{n} V^{-2/n} \|\boldsymbol{e}\|^2. \tag{4}$$

Here V is a function of $\boldsymbol{B}$ and $\boldsymbol{e}$ is a function of both $\boldsymbol{B}$ and $\boldsymbol{z}$.

If $\boldsymbol{z}_1, \ldots, \boldsymbol{z}_T$ denote T independent realizations of $\boldsymbol{z}$, then an unbiased estimate of G follows immediately from (3) as

$$\hat{G} = \frac{1}{T} \sum_{t=1}^{T} g(\boldsymbol{B}, \boldsymbol{z}_t). \tag{5}$$

To quantify the estimation accuracy, the variance of $\hat{G}$ can be estimated as [7, Sec. IV]

$$\hat{\sigma}^2 = \frac{1}{T-1} \left(\frac{1}{T} \sum_{t=1}^{T} g^2(\boldsymbol{B}, \boldsymbol{z}_t) - \hat{G}^2 \right), \tag{6}$$

which is much more accurate than the "jackknife" estimator recommended in earlier literature.

This text was extracted from https://arxiv.org/abs/2401.01799 in Jan. 2024.

It is easily verified that (5) remains unchanged if the lattice, represented by $\boldsymbol{B}$, is rescaled. However, previous descriptions of the same NSM estimation method are valid only for lattices with $V = 1$. This is because of an unfortunate error in the original publication [3], where the right-hand sides of [3, Eqs. (2), (4)] are missing a factor corresponding to the volume of the Voronoi region (here denoted by V). This error appears to have propagated to [8, Eqs. (73)–(74)] and [7, Eqs. (12)–(15)].

References

[1] A. Gersho, "Asymptotically optimal block quantization," *IEEE Trans. Inf. Theory*, vol. IT-25, no. 4, pp. 373–380, July 1979. [Online]. Available: https://doi.org/10.1109/TIT.1979.1056067

[2] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York, NY: Springer, 1999. [Online]. Available: https://doi.org/10.1007/978-1-4757-6568-7

[3] ——, "On the Voronoi regions of certain lattices," *SIAM J. Alg. Disc. Meth.*, vol. 5, no. 3, pp. 294–305, Sept. 1984. [Online]. Available: https://doi.org/10.1137/0605031

[4] ——, "Fast quantizing and decoding algorithms for lattice quantizers and codes," *IEEE Trans. Inf. Theory*, vol. IT-28, no. 2, pp. 227–232, Mar. 1982. [Online]. Available: https://doi.org/10.1109/TIT.1982.1056484

[5] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, "Closest point search in lattices," *IEEE Trans. Inf. Theory*, vol. 48, no. 8, pp. 2201–2214, Aug. 2002. [Online]. Available: https://doi.org/10.1109/TIT.2002.800499

[6] A. Ghasemmehdi and E. Agrell, "Faster recursions in sphere decoding," *IEEE Trans. Inf. Theory*, vol. 57, no. 6, pp. 3530–3536, June 2011. [Online]. Available: https://doi.org/10.1109/TIT.2011.2143830

[7] D. Pook-Kolb, E. Agrell, and B. Allen, "The Voronoi region of the Barnes–Wall lattice Λ_{16}," *J. Sel. Areas Inf. Theory*, vol. 4, pp. 16–23, 2023. [Online]. Available: https://doi.org/10.1109/JSAIT.2023.3276897

[8] S. Lyu, Z. Wang, C. Ling, and H. Chen, "Better lattice quantizers constructed from complex integers," *IEEE Trans. Commun.*, vol. 70, no. 12, pp. 7932–7940, Dec. 2022. [Online]. Available: https://doi.org/10.1109/TCOMM.2022.3215685