Transference

Debadatta Kar, PhD Scholar,
Electrical Engineering and Computer Science,
Indian Institute of Science Education and Research, Bhopal

September, 2025

$\boxed{X}$

---

1 Introduction

2 Transference

Definition 2.1. *For a basis* $B = \{\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}\}$ *define the projection function* π_i *to be projection on span*$(\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_{i-1}})^{\perp}$

$$\pi_i(x) := \sum_{j=i}^{n} \frac{\left\langle \mathbf{x}, \mathbf{b_j^*} \right\rangle}{\left\langle \mathbf{b_j^*}, \mathbf{b_j^*} \right\rangle} \mathbf{b_j^*}$$

Theorem 2.2. *Let* $B = \{\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}\}$ *and* $D = \{\mathbf{d_1}, \mathbf{d_2}, \cdots, \mathbf{d_n}\}$ *be dual bases then* $B' = \{\pi_{\mathbf{i}}(\mathbf{b_i}), \cdots, \pi_{\mathbf{i}}(\mathbf{b_n})\}$ *and* $D' = \{\mathbf{d_{i+1}}, \cdots, \mathbf{d_n}\}$ *are also dual bases.*

Proof. $\mathbf{span(B')} = \mathbf{span(D')}$
We have $span(B') = span(\pi_{\mathbf{i}}(\mathbf{b_i}), \cdots, \pi_{\mathbf{i}}(\mathbf{b_n})) = span(\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_{i-1}})^{\perp}$
We now have dual basis which satisfy $\langle d_i, b_j \rangle = 0 \quad \forall j < i$.
Hence, $d_j \in span(\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_{i-1}})^{\perp}$.
Finally, $D \subseteq span(\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_{i-1}})^{\perp}$
We already have D' as a set of linearly independent vectors. So, $span(D') = span(B)$
$\mathbf{B'D'^T = I}$ □

Definition 2.3. *content...*

Definition 2.4. **HKZ Reduced Basis**
A basis $B = \{\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}\}$ *of a full rank lattice* $\mathcal{L} \subset \mathbb{R}^n$ *is Hermite-Koekine-Zolotareff-reduced(HKZ) if*

- ✓ *B is size reduced.*
- ✓ $\|\mathbf{b_i^*}\| = \lambda_1(\pi_i(\mathcal{L}))$ *for* $i = 1, 2, \cdots, n$

Theorem 2.5. *For a full rank lattice* $\mathcal{L} \subset \mathbb{R}^n$ *we have* $\frac{1}{2} \leq \mu(\mathcal{L}) \cdot \lambda_1(\mathcal{L}^*) \leq \frac{1}{2} n^{3/2}$

Theorem 2.6. *For a full rank lattice* $\mathcal{L} \subset \mathbb{R}^n$ *we have* $1 \leq \lambda_i(\mathcal{L}) \cdot \lambda_{n-i+1}(\mathcal{L}^*) \leq n^2$

Result 2.7. $GapSVP_n \in$ **coNP**

References

[Con07] Keith Conrad. *Dual Modules*. 2007. URL: https://kconrad.math.uconn.edu/blurbs/linmultialg/dualmod.pdf.

[Kre10] Erwin Kreyszig. *Advanced Engineering Mathematics 10E*. Chichester, England: John Wiley & Sons, Dec. 2010.

[Mic14] Daniel Micciancio. *Lecture Notes on Lattices Algorithms and Applications*. 2014. URL: https://cseweb.ucsd.edu/classes/sp14/cse206A-a/.

[Mus01] C Musili. *Introduction to Rings and Modules*. en. 2nd ed. New Delhi, India: Narosa Publishing House, Jan. 2001.

[Pei13] Chris Peikert. "Lecture Notes on Lattices in Cryptography". Georgia Tech, Fall 2013. 2013. URL: https://github.com/cpeikert/LatticesInCryptography.

[Reg09] Regev. *Lecture Notes on Lattices in Computer Science*. Tel Aviv University, 2009.

[Sha11] Rami Shakarchi. *Fourier Analysis*. Princeton, NJ: Princeton University Press, Feb. 2011.