ÉCOLE NORMALE SUPÉRIEURE DE LYON

May 22nd, 2017

Weiqiang Wen
LIP, ENS Lyon

Mission: **progress report (09.2015–05.2017) and future plan (from 05.2017)**

PhD advisor. Damien Stehlé (ENS de Lyon professor, LIP)
PhD project. Algorithm for hard lattice problems.
PhD duration. From September, 2015 to August, 2018 (planned).

Research during 09.2015–05.2017.

A (full-rank) Euclidean lattice $\mathcal{L}$ is the set of all integer linear relations of some linearly independent vectors in a Euclidean space. These vectors form a basis of this lattice. There are two central computational problems on lattice: the shortest vector problem (SVP), which gives as input a basis of a lattice, asks to find a shortest non-zero vector in the lattice; and the closest vector problem (CVP), which gives as inputs a basis of a lattice and a (target) vector in the real span of the lattice, asks to find a lattice vector closest to the target vector.

The first minimum $\lambda_1(\mathcal{L})$ is the smallest length between two distinct lattice vectors in lattice $\mathcal{L}$. A commonly used variant of CVP is the Bounded Distance Decoding problem with parameter $\alpha > 0$ (BDD_α): Given as inputs a basis of a lattice $\mathcal{L}$ and a (target) vector $\mathbf{t} \in \mathbb{Q}^n$ within distance $\alpha \cdot \lambda_1(\mathcal{L})$ of $\mathcal{L}$, the goal is to find a vector $\mathbf{b} \in \mathcal{L}$ closest to $\mathbf{t}$. The second minimum $\lambda_2(\mathcal{L})$ is defined as the minimal radius of a zero-centered ball that contains two or more linearly independent vectors from $\mathcal{L}$. Respectively, we also consider a variant of SVP, called the unique Shortest Vector Problem with parameter $\gamma \geq 1$ (uSVP_γ). uSVP_γ consists in finding a shortest non-zero vector in a given lattice $\mathcal{L}$, under the promise that $\lambda_2(\mathcal{L}) \geq \gamma \cdot \lambda_1(\mathcal{L})$.

My main result last year defines the hardness relationship between BDD and uSVP. The reduction from BDD to uSVP is initially given by Lyubashevsky and Micciancio in [1], who showed that $\mathrm{BDD}_{1/(2\gamma)}$ reduces to uSVP_γ for any $\gamma \geq 1$. Later, Liu *et al.* [2] refined the analysis of Lyubashevsky and Micciancio and proved that $\mathrm{BDD}_{1/\gamma_1}$ reduces to uSVP_γ with $\gamma_1 = \sqrt{3/(4-\gamma^2)}\gamma + 1$, for any $\gamma \in (1, 1.9318)$. It is folklore [3, 4] that the analysis can be tightened even more, resulting in a proof that $\mathrm{BDD}_{1/\gamma_1}$ reduces to uSVP_γ with $\gamma_1 = (2\gamma^2 + 2\lfloor\gamma\rfloor\lfloor\gamma+1\rfloor)/(2\lfloor\gamma\rfloor+1)$, for any $\gamma \geq 1$.

We give a probabilistic polynomial-time reduction from $\mathrm{BDD}_{1/(\sqrt{2}\gamma)}$ to uSVP_γ for any $\gamma \geq 1$ that is polynomially bounded as a function of dimension. This new reduction supersedes all prior results mentioned above. This work has been accepted to ICALP'16, and I presented it in Italy, in July, 2016. Later on, I also gave an extended talk on this in Seminar Crypto, Université de Caen, in December, 2016.

My second work is to study the quantum hardness of lattice problems in terms of Learning with Error (LWE) problem, which is introduced by Regev in [5]. In 2002, Regev [6] showed that uSVP, and therefore also BDD and LWE, are no harder to solve than the quantumly-defined Dihedral Coset Problem (DCP). An instance of $\mathrm{DCP}_{N,\ell}$, for integer parameters N and ℓ, consists of ℓ quantum registers in superposition $|0, x_k\rangle + |1, x_k + s\rangle$, with a common $s \in \mathbb{Z}_N$ and random and independent $x_k \in \mathbb{Z}_N$ for $k \in [\ell]$. The goal is to find s.

The focus of this work is a generalization of the DCP problem, i.e. rather than considering registers containing $|0, x_k\rangle + |1, x_k + s\rangle$, we allow (1) x_i's and s be n-dimensional vectors, and (2) other than non-uniform distribution for amplitudes. We name this problem Extrapolated DCP (EDCP). To be more precise, $\mathrm{EDCP}^{\ell}_{n,N,f}$, with parameters three integers n, N, ℓ and a function $f : \mathbb{Z} \mapsto \mathbb{C}$

with $\sum_{j\in\mathbb{Z}} j\cdot|f(j)|^2 < +\infty$, consists in recovering $\mathbf{s}\in\mathbb{Z}_N^n$ from the following ℓ states over $\mathbb{Z}\times\mathbb{Z}_N^n$: $\left\{\frac{1}{\sqrt{\sum_{j\in\mathbb{Z}}|f(j)|^2}}\cdot\sum_{j\in\mathbb{Z}} f(j)\,|j,\mathbf{x}_k+j\cdot\mathbf{s}\rangle\right\}_{k\leq\ell}$, where the $\mathbf{x}_k$'s are arbitrary in $\mathbb{Z}_N^n$. Note that DCP is the special case of EDCP for $n=1$ and f being the indicator function of $\{0,1\}$. In [7], Childs and van Dam consider the particular case of EDCP where f is the indicator function of $\{0,\ldots,M-1\}$ for some integer M, which we will refer to as uniform EDCP (or, U-EDCP$^{\ell}_{n,N,M}$).

My main result this year is that there exists a quantum polynomial-time reduction from LWE$_{n,q,\alpha}$ to U-EDCP$^{\ell}_{n,N,M}$, with $N=q$, $\ell=\mathrm{poly}(n\log q)$ and $M=\frac{\mathrm{poly}(n\log q)}{\alpha}$. Conversely, there exists a polynomial-time reduction from U-EDCP to LWE with the same parameter relationships, up to $\mathrm{poly}(n\log q)$ factors. This work is going to be submitted to SODA 2018.

Research plan for 05.2017-08.2018.

I am working/plan to work on the following directions.

Improving the reductions between BDD and uSVP. We have a conjecture on this relation between BDD and uSVP that computational equality holds between BDD$_{1/(\sqrt{2}\gamma)}$ and uSVP$_\gamma$. Currently, we already know that BDD$_{1/(\sqrt{2}\gamma)}$ is reduced to uSVP$_\gamma$. For the opposite direction, there is a reduction from uSVP$_\gamma$ to BDD$_{1/\gamma}$ given by Lyubashevsky and Micciancio [1]. To obtain the conjectured equality, we need to improve this result to reduce uSVP$_\gamma$ to BDD$_{1/(\sqrt{2}\gamma)}$. I am also considering the practical relevance of the improved uSVP to BDD.

Hardness of EDCP **with more input states.** We show in this work that LWE and U-EDCP are computationally equivalent up to small parameter losses, when the number of U-EDCP states ℓ is polynomial. In these reductions, the U-EDCP bound M is within a polynomial factor of the LWE noise rate $1/\alpha$. When more states are available, U-EDCP is likely to become easier. For instance, with $M=2$, the best known algorithms when ℓ is polynomially bounded are exponential. Oppositely, Kuperberg's algorithm [8] runs in time $2^{\widetilde{O}(\sqrt{\log N})}$ when $\ell=2^{\widetilde{O}(\sqrt{\log N})}$. This suggests that there may be a U-EDCP self-reduction allowing to trade ℓ for M: Is it possible to reduce EDCP$^{\ell}_{N,M}$ to EDCP$^{\ell'}_{N,M'}$ with $\ell'\leq\ell$, while allowing for $M'\geq M$?

References

[1] V. Lyubashevsky and D. Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem. In *Proc. of CRYPTO*, pages 577–594, 2009.

[2] M. Liu, X. Wang, G. Xu, and X. Zheng. A note on BDD problems with λ_2-gap. *Inf. Process. Lett.*, 114(1-2):9–12, January 2014.

[3] D. Micciancio. Private communication, 2015.

[4] S. Galbraith. Private communication, 2015.

[5] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proc. of STOC*, pages 84–93. ACM, 2005.

[6] O. Regev. Quantum computation and lattice problems. In *Proceedings of the 43rd Symposium on Foundations of Computer Science*, FOCS '02, pages 520–529. IEEE Computer Society, 2002.

[7] A. M. Childs and W. van Dam. Quantum algorithm for a generalized hidden shift problem. In *Proc. of SODA*, pages 1225–1232. SIAM, 2007.

[8] G. Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM J. Comput*, 35(1):170–188, 2005.