Shortest Vector Problem (SVP)

Annangi Shashank Babu (EE21B021)

August 25, 2024

Lattice Based Cryptography

- Lattice-based cryptography: one of the main proposals for post-quantum cryptography.
- Many of the finalists of the NIST competition are from lattice-based cryptography.

Lattice

The d-dimensional lattice $\mathcal{L} \in R^m$ generated by the basis B $=$ $(\vec{b_1}, \vec{b_2}, ..., \vec{b_d})$ is the set of all integer linear combinations of its basis vectors: $\mathcal{L}(B) = \{\sum_{i=1}^{d} \lambda_i \vec{b_i}, \lambda_i \in Z\}$

SVP

Given a lattice $\mathcal{L}$, find the shortest non-zero vector $\vec{v} \in \mathcal{L}$.

example:

-322(64,218,133) $+$ 323(71,205,111) - 83(28,-48,-84) $=$ (1,3,-1).

QUBO Formulation

$$\lambda^2 = \min_{x \in Z^n \setminus 0^n} |Bx|^2$$

$$\lambda^2 = \min_{x \in Z^n \setminus 0^n} \sum_{i=1}^{n} x_i^2 B_{ii} + 2 \sum_{0<i<j<n} x_i x_j B_{ij}$$

- In order to convert the above equation into a binary optimisation problem, we need bounds $|x_i| \leq a_i$.

$$x_i = -a + \sum_{y=0}^{\lfloor \log_2 2a \rfloor - 1} (2^y \tilde{x}_{iy}) + (2a + 1 - 2^{\lfloor \log_2 2a \rfloor}) \cdot \tilde{x}_{i, \lfloor \log_2 2a \rfloor}$$

$$\min_{\tilde{x}_{1,0}, \ldots, \tilde{x}_{1,\lfloor \log_2 a_1 \rfloor}, \ldots, \tilde{x}_{n,0}, \ldots, \tilde{x}_{n,\lfloor \log_2 a_n \rfloor}} (p + \sum_{\tilde{x}_{i,j}} p_{i,j} \tilde{x}_{i,j} + \sum_{\tilde{x}_{i,j}, \tilde{x}_{k,l}} q_{i,j,k,l} \tilde{x}_{i,j} \tilde{x}_{k,l})$$

QUBO Formulation

- For imposing the condition $x \neq 0^n$, viable solution is to modify the Hamiltonian and impose a penalty for reaching the zero vector (ground state of the "naive" Hamiltonian).

$$x_i = -a+\zeta_i a+\omega_i(a+1)+\sum_{y=0}^{\lfloor \log_2(a-1)\rfloor -1}(2^y \tilde{x}_{iy})+(a-2^{\lfloor \log_2(a-1)\rfloor})\cdot \tilde{x}_{i,\lfloor \log_2(a-1)\rfloor}$$

If $x_i = 0$, then $\zeta_i = 1$.
Hamiltonian :

$$(p+\sum_{\tilde{x}_{i,j}} p_{i,j}\tilde{x}_{i,j}+\sum_{\tilde{x}_{i,j},\tilde{x}_{k,l}} q_{i,j,k,l}\tilde{x}_{i,j}\tilde{x}_{k,l})+L\cdot\left(1+\sum_{i=1}^{n} z_i\left(-(1-\zeta_i)+\sum_{k=i+1}^{n}(1-\zeta_k)\right)\right)$$

$$+$$

$$L\cdot\left(1+\sum_{i=1}^{n} z_i\left(-(1-\zeta_i)+\sum_{k=i+1}^{n}(1-\zeta_k)\right)\right)$$

GAMA Formulation

constraints :

$$\sum_{i=1}^{n} x_i^2 B_{ii} + 2 \sum_{0<i<j<n} x_{ij} B_{ij} + Z = |B[1]|^2$$

$$(p + \sum_{\tilde{x}_{i,j}} p_{i,j} \tilde{x}_{i,j} + \sum_{\tilde{x}_{i,j}, \tilde{x}_{k,l}} q_{i,j,k,l} \tilde{x}_{i,j,k,l}) + Z = |B[1]|^2$$

$$\tilde{x}_{i,j,k,l} \geq \tilde{x}_{i,j} + x_{k,l} - 1$$

$$\tilde{x}_{i,j,k,l} \leq \tilde{x}_{i,j}$$

$$\tilde{x}_{i,j,k,l} \leq \tilde{x}_{k,l}$$

$$Z = \sum_{y=0}^{\lfloor \log_2 B[1]^2 - 1 \rfloor - 1} (2^y \tilde{z}_{iy}) + (B[1]^2 - 2^{\lfloor \log_2 B[1]^2 - 1 \rfloor}) \cdot \tilde{z}_{i, \lfloor \log_2 B[1]^2 - 1 \rfloor}$$

- the above inequalities make sure that $x_{ij,kl} = x_{i,j} * x_{k,l}$
- Here we should maximise Z which will minimize the norm.

GAMA Formulation

- since the number of required quibits are higher for GAMA so the search space is higher, time taken to reach ground state of Hamiltonian is longer.

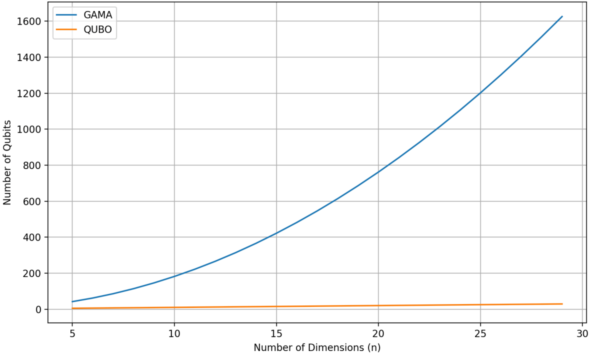

Figure: Comparing approx number of quibits required for specified QUBO and GAMA

Thank You

Thank You!