Variational Quantum Solutions to the Shortest Vector Problem

Martin R. Albrecht, Miloš Prokop*, Yixin Shen, Petros Wallden

*m.prokop@sms.ed.ac.uk

Abstract

We explore how (efficiently) Noisy Intermediate Scale Quantum (NISQ) devices may be used to solve SVP by mapping the problem to that of finding the ground state of a suitable Hamiltonian. In particular, (i) we propose an approach to the reduce number of required qubits to $\approx 10^3$ to tackle instances on the edge of classical capabilities; (ii) we exclude the zero vector from the optimization space by proposing (a) a different classical optimisation loop or alternatively (b) a different mapping to the Hamiltonian. Full paper [1].

Shortest Vector Problem

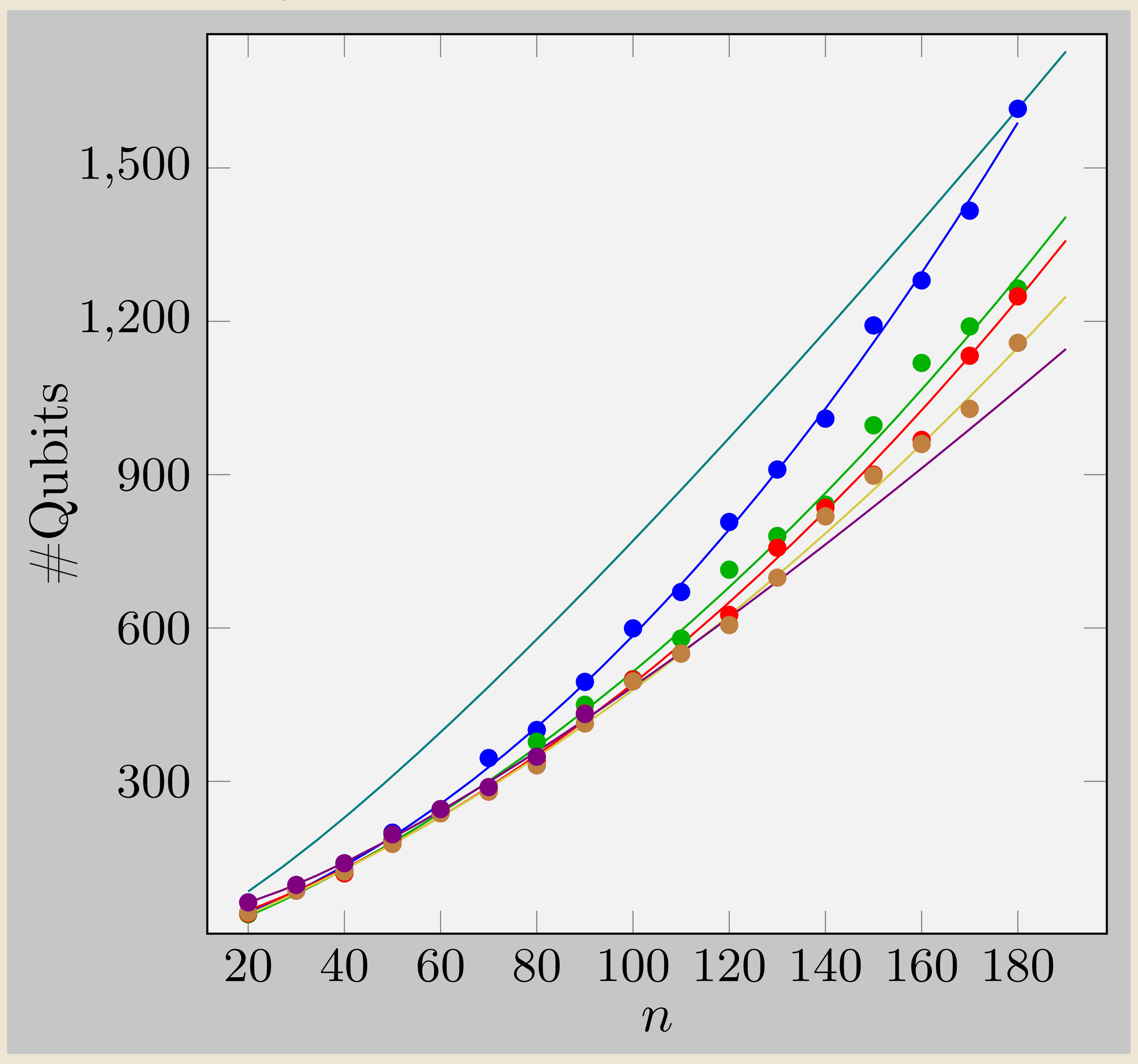
Given an integer lattice basis B, the SVP finds the shortest non-zero vector of lattice $\mathcal{L}(B) = \{Bx : x \in \mathbb{Z}^n\}$ denoted by $\lambda(\mathcal{L}) = \min\{||y||_p : y \in \mathcal{L}, y \neq \mathbf{0}\}$. NP-Hardness of SVP has been shown for $p = \infty$ [3] and for $p = 2$ under randomized reductions [4]. Although not proven, hardness of SVP is also conjectured in quantum settings. It is particularly appealing to cryptography as **many quantum-safe classical cryptographic protocol proposals are based on the hardness of SVP**.

Variational Q. Algorithms

Variational Quantum Algorithms are promising candidates for NISQ era due to low qubit requirements and partial resilience against noise without quantum error correction. Given a problem encoded as ground state of Hamiltonian $\mathcal{H}$, they utilize classical optimization to find θ minimizing a cost $C(\theta) = \min_\theta \langle\psi(\theta)|\mathcal{H}|\psi(\theta)\rangle$ evaluated on a quantum device. There exists a natural mapping of **Quadratic Unconstrained Binary Optimization (QUBO)** problem formulation to Ising Hamiltonians.

Estimated Qubit Scaling

Average qubit requirements to encode SVP in a problem Hamiltonian. $n = 180$ is an upper bound on cabability of classical SVP solvers.



Basis preprocessing: LLL, BKZ-20, BKZ-50, BKZ-70, pseudo-HKZ[1]. q.enum HKZ[1]

Mapping SVP to a Hamiltonian Operator

Given an n-dimensional full-rank row-major lattice basis matrix B, let $G = BB^T$. The shortest non-zero lattice vector can be found by solving the following **integer constrained optimization problem**:

$$[\lambda(\mathcal{L})]^2 = \min_{y\in\mathcal{L}(B)\setminus\{0\}} |y|^2 = \min_{x\in\mathbb{Z}^n\setminus\{0\}} \sum_{i=1}^{n} x_i G_{ii} + 2 \sum_{1\leq i<j\leq n} x_i x_j G_{ij}.$$

To construct a **QUBO** formulation we propose the following:

1. Conversion to a binary optimization problem

To express x_i as a finite sum of binary variables, bounds $|x_i| \leq a_i$ that are **sufficient** (encode the SVP solution) and **efficient** (realistic qubit overhead) need to be determined. Letting $\widehat{B} := (BB^T)^{-1}B$ be a specific basis of a dual lattice $\mathcal{L}^* = \{y \in \mathbb{R}^n : \forall x \in \mathcal{L} | < x, y > \in \mathbb{Z}\}$, the following results improve the estimates on qubit requirements for solving the SVP with VQAs. Assuming a bound A on the SVP solution is known apriori (e.g. Gaussian Heuristic) we can bound each individual element of x:

Lemma [1]. *Let $x_1, \ldots, x_n$ be such that $||x_1 \cdot \vec{b}_1 + \cdots + x_n \cdot \vec{b}_n|| \leq A$, then for all $i = 1, \ldots, n$ we have $|x_i| \leq A||\hat{\vec{b}}_i||$ where $\hat{\vec{b}}_1, \ldots, \hat{\vec{b}}_n$ are the rows of $\widehat{B}$ and B is the matrix whose rows are $\vec{b}_1, \ldots, \vec{b}_n$.*

This allows for asymptotic estimation of qubit scaling with $\delta(\widehat{B}) = 2^{\mathcal{O}(n^2)}$ being orthogonality defect[1]:

Corollary [1]. *The number of qubits required for the enumeration on the basis B, assuming the Gaussian heuristic with multiplicative factor C, is bounded by $2n + \log_2\left(\left(\frac{C^2 n}{2\pi e}\right)^{n/2} \delta(\widehat{B})\right)$.*

2. Avoiding the constraint by optimizing towards the 1st excited state

We have analyzed two possibilities that differ by suitable quantum computational models:

- **Modify the cost function** $C'(\theta) := \frac{1}{1-|\langle\psi(\theta)|\psi_0\rangle|^2}\langle\psi(\theta)|H|\psi(\theta)\rangle$ to penalize states proportionally to their overlap with the ground state. The method does not increase qubit requirements, but due to classical cost post-processing, is suitable only for *Variational Quantum Eigensolver (VQE)* algorithm.
- **Construct a new Ising Hamiltonian by encoding a penalty term**. This approach is suitable if SVP is to be tackled by *Quantum Approximate Optimization Algorithm*, *Adiabatic Quantum Computation* or *Quantum Annealing*. n additional binary variables $\{\zeta_i\}_{i=1,\ldots,n}$ are to be introduced with bijective correspondence to $\{x_i\}_{i=1,\ldots,n}$.

  If the bound $|x_i| \leq a$ is determined then x_i can be encoded as

$$x_i = -a + \zeta_i a + \omega_i(a+1) + \sum_{j=0}^{\lfloor\log(a-1)\rfloor-1} 2^j \tilde{x}_{ij} + (a - 2^{\lfloor\log(a-1)\rfloor})\tilde{x}_{i,\lfloor\log(a-1)\rfloor} \quad (1)$$

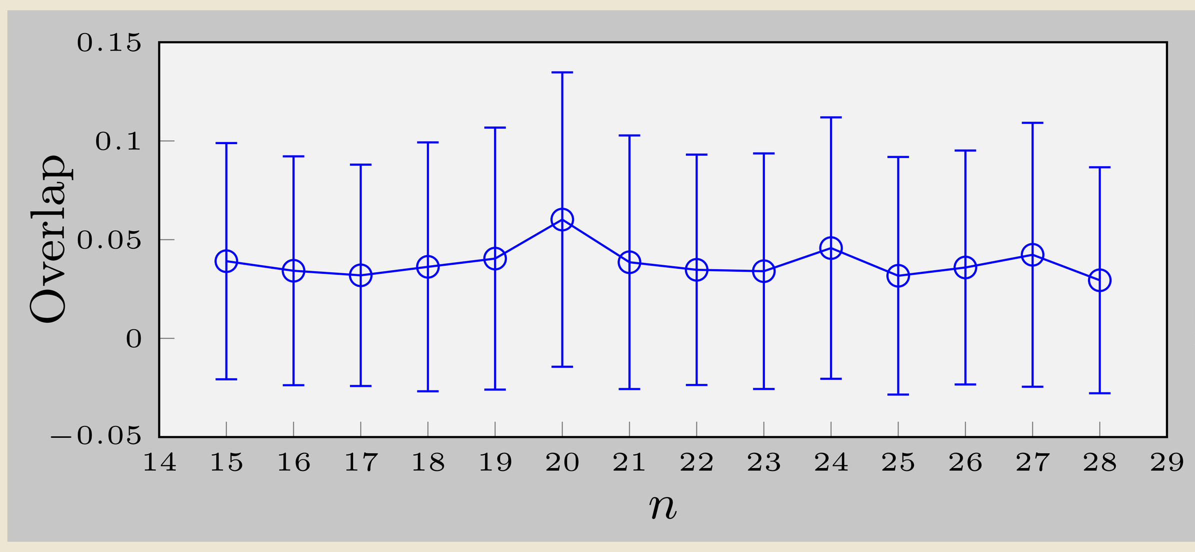
  It follows that $x_i = 0 \implies \zeta_i = 1$ and the penalization term $L\prod\zeta_i$ (expressed as a QUBO term below) introduces penalty $L >> 0$ iff $\forall\zeta_i = 1$.

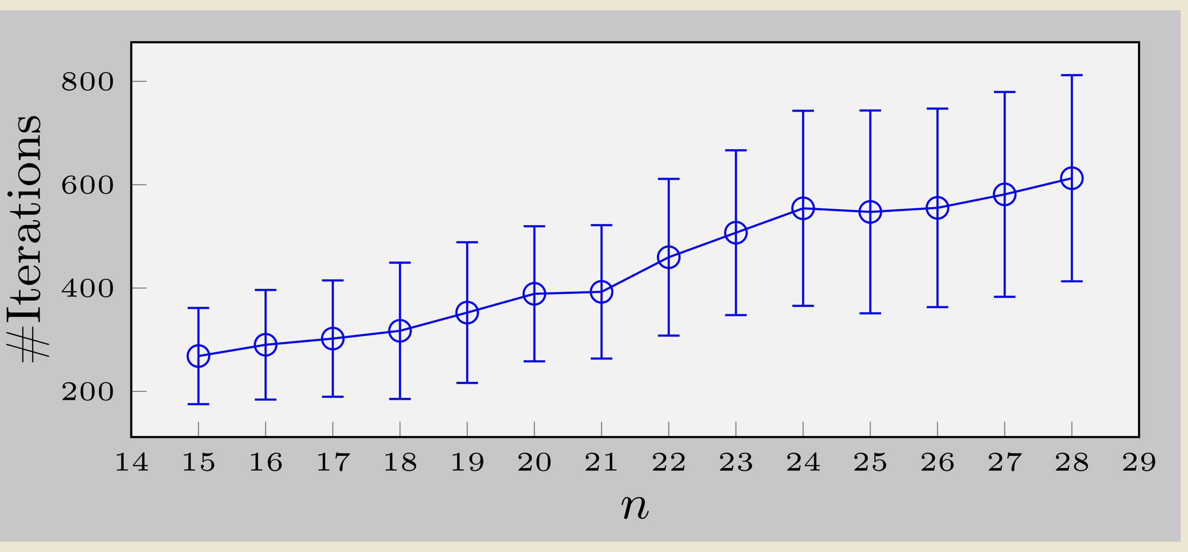
$$L\prod\zeta_i = L(1 + \sum_{i=1}^{n} z_i(-(1-\zeta_i) + \sum_{k=i+1}^{n}(1-\zeta_k))) \quad (2)$$

[1] True for LLL or BKZ reduced basis. $\delta(\widehat{B}) = 2^{\mathcal{O}(n\log(n))}$ if basis is quasi-HKZ [1] reduced.

Classical Emulation of the Quantum SVP Approach

SVP approached by **VQE** was emulated using *FastVQA*[2] library omitting effects of noise up to 28 dimensions of qary lattice instances, setting a new record in the existing literature [1]. Constant overlap $\langle\psi(\theta_{\text{returned by VQE}})|ground\_state(\mathcal{H})\rangle \approx 4\%$ and linear time scaling have been observed.





References

[1] M. R. Albrecht, M. Prokop, Y. Shen, and P. Wallden, Variational quantum solutions to the Shortest Vector Problem. arXiv, 2022. doi: 10.48550/ARXIV.2202.06757.

[2] FastVQA: Simulation framework of variational quantum algorithms focused on performance, portability and distributivity on parallel architectures. `https://github.com/Milos9304/FastVQA`

[3] R. Kumar and D. Sivakumar, "A note on the shortest lattice vector problem," Proceedings. Fourteenth Annual IEEE Conference on Computational Complexity (Cat.No.99CB36317), 1999, pp. 200-204, doi: 10.1109/CCC.1999.766277.

[4] M. Ajtai, The shortest vector problem in L2 is NP-hard for randomized reduction, in "Proc. 30th ACM Symposium on Theory of Computing (STOC), 1998."