Karp reduction from $(0,1)$-CVP$_2$ to Weighted Max-2-SAT

1 Overview

In the report, we will show a Karp reduction from the $(0,1)$-Closest Vector Problem in l_2 norm ($(0,1)$-CVP$_2$) to the Weighted Max-2-SAT problem. If the Weighted Max-2-SAT problem has a solution, then the $(0,1)$-CVP$_2$ problem also has a solution.

First, we use *split-and-list* approach to reduce $(0,1)$-CVP to minimum-weight k-Clique using the following steps:

1. Arbitrarily partition n-basis vectors $\mathbf{B}$ into k sets $\mathbf{B}^1, \mathbf{B}^2 \cdots \mathbf{B}^k$ of size n/k each.
2. Let $N = 2^{n/k}$. Enumerate all possible N vectors in each set $\mathbf{B}^i$ attainable by taking the sum of all possible combinations of basis vectors in $\mathbf{B}^i$. We now have k lists of N vectors each - $\mathbf{C}^1, \mathbf{C}^2 \cdots \mathbf{C}^k$.
3. Any sum of k vectors from $\mathbf{C}^1 \times \mathbf{C}^2 \times \cdots \times \mathbf{C}^k$ is a valid candidate for being the closest vector. The closest vector $v = \sum_{i=1}^{n} z[i]\mathbf{b}_i$ can be represented as the sum of k vectors $v = \sum_{i=1}^{k} \mathbf{c}_i$ where $\mathbf{c}_i \in \mathbf{C}^i$.
4. Task is now to find the optimal way of selecting k vectors from $\mathbf{C}^1 \times \mathbf{C}^2 \times \cdots \times \mathbf{C}^k$.
5. The main idea to convert $(0,1)$-CVP to minimum-weight k-Clique can now be summarized as follows:
   - Represent each vector in $\mathbf{c}_i$ as a vertex in a graph G.
   - k-Clique represents sum of k vectors.
   - Total weight of the k-Clique corresponds ot the distance to the target vector $\mathbf{t}$.
   - Minimum-weight k-Clique corresponds to the closest vector to $\mathbf{t}$.

Main Problem:

1. Total weight of k-Clique can only be influenced by *pairwise contributions* of its k vertices.
2. In CVP interpretation, we need a way to represent the distance of the vector $z = c_1 + \cdots + c_k$ from the target vector $\mathbf{t}$ as a sum of pairwise contributions.

Solution: Under the *Euclidean norm* the expression $\|c_1 + \cdots + c_k - t\|^2$ can be broken into a sum that depends only on pairs c_i, c_j and can therefore be implemented as the weight of a k-clique under a careful choice of weights.

How does this relate to MAX-2-SAT? Set $k = n$. On a high level, we are partitioning the basis vectors into singletons and thinking of either including or excluding each vector in the sum. These singletons corresponds to a Boolean variable that determines if the corresponding vector is included in the sum or not.

2 Preliminaries

We will use $\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Z}_{>0}$, and $\mathbb{Q}$ to represent the sets of real numbers, integers, positive integers, and rational numbers, respectively. We will use boldface lower-case letters to denote column vectors, e.g., $\mathbf{v} \in \mathbb{R}^m$, and we will use $\mathbf{v}[i]$ to denote the i-th coordinate of $\mathbf{v}$. We use boldface upper-case letters to denote a matrix, e.g., $\mathbf{M} \in \mathbb{R}^{m \times n}$ and $\mathbf{m}_i$ to denote the i-th column vector of $\mathbf{M}$.

For vector $\mathbf{v} \in \mathbb{R}^m$, the ℓ_2 norm a.k.a the Euclidean norm of vector $\mathbf{v}$ is defined as:

$$\|\mathbf{v}\|_2 := \sqrt{\left(\sum_{i=1}^{m} |\mathbf{v}[i]|^2\right)},$$

For the sake of simplicity, we will use $\|\mathbf{v}\|$ to denote $\|\mathbf{v}\|_2$.

Also, recall that an inner product for any two vectors $\mathbf{v_1}, \mathbf{v_2} \in \mathbb{R}^m$ is defined as:

$$\langle \mathbf{v_1}, \mathbf{v_2} \rangle = \sum_{i=1}^{m} \mathbf{v_1}[i]\mathbf{v_2}[i].$$

2.1 Lattice Problems

For any set of linearly independent vectors $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \in \mathbb{R}^{m \times n}$, the lattice generated by $\mathbf{B}$ is defined as:

$$\mathcal{L} = \mathcal{L}(\mathbf{B}) := \left\{ \sum_{i=1}^{n} z[i]\mathbf{b}_i \mid z[i] \in \mathbb{Z} \right\}.$$

Here, n is called the rank of the lattice and m is the dimension. A lattice can have infinitely many bases. $\mathbf{B}$ is called a basis of $\mathcal{L}$ if $\mathcal{L} = \mathcal{L}(\mathbf{B})$.

For any vector $\mathbf{t} \in \mathbb{R}^m$, we define the distance of $\mathbf{t}$ from the lattice $\mathcal{L}$ as:

$$\text{dist}(\mathcal{L}, \mathbf{t}) := \min_{\mathbf{v} \in \mathcal{L}} \|\mathbf{v} - \mathbf{t}\|.$$

Definition 1. *(0, 1)-Lattices: For any set of linearly independent vectors $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \in \mathbb{R}^{m \times n}$, the (0, 1)-lattice generated by $\mathbf{B}$ is defined as:*

$$\mathcal{L}_{(0,1)} := \left\{ \sum_{i=1}^{n} z[i]\mathbf{b}_i \mid z[i] \in \{0, 1\} \right\}.$$

Definition 2. *Search $(0, 1)$-Closest Vector Problem in l_2 norm (Search-CVP$_2$): Given a basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \in \mathbb{R}^{m \times n}$ of a lattice $\mathcal{L}_{(0,1)}$ and a target vector $\mathbf{t} \in \mathbb{R}^m$, the goal is to find a vector $\mathbf{z} \in \{0, 1\}^n$ such that $\|\mathbf{Bz} - \mathbf{t}\|$ is minimized.*

This variant of the CVP$_2$ problem is called Search CVP.

Definition 3. *Decisional $(0, 1)$-Closest Vector Problem in l_2 norm (Decisional-CVP$_2$): Given a basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \in \mathbb{Z}^{m \times n}$ of a lattice $\mathcal{L}_{(0,1)}$, a target vector $\mathbf{t} \in \mathbb{Z}^m$, and a distance parameter $d \in \mathbb{Z}_{>0}$, the goal is to determine if there exists a vector $\mathbf{z} \in \{0, 1\}^n$ such that $\|\mathbf{Bz} - \mathbf{t}\| \leq d$.*

Another variant of the CVP$_2$ problem is the Gap CVP$_2$ problem, defined as follows:

Definition 4. *Gap $(0, 1)$-Closest Vector Problem in l_2 norm (Gap-CVP$_2$): For any $\gamma \geq 1$. Given a basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \in \mathbb{Z}^{m \times n}$ of a lattice $\mathcal{L}_{(0,1)}$, a target vector $\mathbf{t} \in \mathbb{Z}^m$, and a distance parameter $d \in \mathbb{Z}_{>0}$, the goal is to distinguish between the following two cases:*

- *YES instance if $\exists \mathbf{z} \in \{0, 1\}^n$ such that $\|\mathbf{Bz} - \mathbf{t}\| \leq d$.*
- *NO instance if $\forall \mathbf{z} \in \{0, 1\}^n$, $\|\mathbf{Bz} - \mathbf{t}\| > \gamma d$.*

In this paper we will use the Gap-CVP$_2$ problem on $(0, 1)$ lattices to show a Karp reduction to the Weighted Max-2-SAT problem.

2.2 Weighted Max-2-SAT

A k-SAT formula $\Psi = \bigwedge_{i=1}^{m} C_i$ on Boolean variables $x_1, \ldots, x_n$ is a conjunction of m clauses $C_1, \ldots, C_m$ where each clause C_i is a disjunction of at most k literals. A literal is either a variable x_j or its negation $\neg x_j$.

Definition 5. *Max-2-SAT: Given a 2-SAT formula Ψ on n variables and a number $\delta \in [0,1]$, the goal is to distinguish between YES instances where there exists an assignment that satisfies at least a δ fraction of the clauses of Ψ and NO instances where all assignments satisfy less than a δ fraction of the clauses.*

Definition 6. *Weighted Max-2-SAT: Given a 2-SAT formula Ψ on n variables, a number $\delta \in [0,1]$, and a weight $w_i \in \mathbb{Z}_{>0}$ for each clause C_i, the goal is to distinguish between YES instances where there exists an assignment for which the sum of weights of satisfied clauses is at leastδ and NO instances where for all assignments the sum of weight of satisfied clauses is less than δ.*

3 Reduction

We want a poly-time reduction from $(0,1)$-CVP (ℓ_2 norm) on the lattice of rank n to Weighted Max-2-SAT with n variables. Given a basis $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$ of a $(0,1)$-lattice, we will construct a 2-SAT formula Ψ with n variables, using the following steps:

1. Let $\chi = \{x_1, x_2, \cdots, x_n\}$ be the set of n Boolean variables. Let's also set $x_{n+1} = 1$.
2. For S of the form (x_{i_1}, x_{i_2}) where $i_1, i_2 \in \{1, 2, \cdots, n+1\}$, let $\sigma(S) \in \{0,1,2\}$ denote the number of occurrences of the variable x_{n+1} in S.
3. Now consider the following weighted clauses for the 2-SAT formula Ψ:
   (a) $C^0_{i_1,i_2} = x_{i_1} \vee x_{i_2}$
   (b) $C^1_{i_1,i_2} = \overline{x_{i_1}} \vee x_{i_2}$
   (c) $C^2_{i_1,i_2} = x_{i_1} \vee \overline{x_{i_2}}$
   (d) $C^3_{i_1,i_2} = \overline{x_{i_1}} \vee \overline{x_{i_2}}$

   with weights[1]:

$$w(C^j_{i_1,i_2}) = \begin{cases} D - \frac{1}{3}(-1)^{\sigma(\{x_{i_1}, x_{i_2}\})}\langle b_{i_1}, b_{i_2}\rangle & 0 \le j \le 2 \\ D + \frac{2}{3}(-1)^{\sigma(\{x_{i_1}, x_{i_2}\})}\langle b_{i_1}, b_{i_2}\rangle & j = 3 \end{cases}$$

Intituively, the weights are chosen such that the sum of weights of satisfied clauses is minimized when the sum of pairwise contributions of the vectors in the sum is minimized. This is done by putting +2/3 weight on when both variables are not included in the sum and -1/3 weight when one of the variables is included in the sum.

4 Proof of Correctness

For any $(x_{i_1}, x_{i_2}) \in \{\chi \cup x_{n+1}\}^2$, any assignment of these variables will satisfy exactly three of the clauses from $\{C^0_{i_1,i_2}, C^1_{i_1,i_2}, C^2_{i_1,i_2}, C^3_{i_1,i_2}\}$.

i_1	i_2	$C^0_{i_1,i_2}$	$C^1_{i_1,i_2}$	$C^2_{i_1,i_2}$	$C^3_{i_1,i_2}$
0	0	0	1	1	1
0	1	1	0	1	1
1	0	1	1	0	1
1	1	1	1	1	0

Total weight of the satisfied clauses is given by:

$$T_w = \begin{cases} 3D - (-1)^{\sigma(\{x_{i_1}, x_{i_2}\})}\langle b_{i_1}, b_{i_2}\rangle & x_{i_1} = x_{i_2} = 1 \\ 3D & \text{otherwise} \end{cases}$$

If the given $(0,1)$-CVP instance is a YES instance, i.e., $\min_{z \in \{0,1\}^n} \|\mathbf{Bz} - \mathbf{t}\| \le d$, then there exists an assignment to the variables χ that satisfies clauses ϕ of weight at least $(n+1)^2 \cdot 3D - d^2$.

Assumptions:

1. Let $\mathbf{z} \in \{0,1\}^n$ be the vector satisfying $\|\mathbf{Bz} - \mathbf{t}\| \le d$.

[1] D is some large enough constant.

2. Let ρ be the assignment to the variables χ such that $\rho(x_i) = z[i], \forall i \in [n]$.
3. $\rho(x_{n+1}) = 1$

Computational Proof: The total weight of the satisfied clauses by the assignment ρ is given by:

$$\begin{aligned}
\sum_{i_1,i_2\in[n+1]^2}\sum_{j=0}^{3}\rho(C^j_{i_1,i_2})w(C^j_{i_1,i_2}) &= \sum_{\substack{i_1,i_2\in[n+1]^2\\ \rho(x_{i_1})=\rho(x_{i_2})=1}} 3D-(-1)^{\sigma(\{x_{i_1},x_{i_2}\})}\langle b_{i_1},b_{i_2}\rangle \\
&\quad+\sum_{\substack{i_1,i_2\in[n+1]^2\\ \rho(x_{i_1})\neq\rho(x_{i_2})}} 3D+\sum_{\substack{i_1,i_2\in[n+1]^2\\ \rho(x_{i_1})=\rho(x_{i_2})=0}} 3D \\
&= (n+1)^2\cdot 3D-\sum_{\substack{i_1,i_2\in[n+1]^2\\ \rho(x_{i_1})=\rho(x_{i_2})=1}}(-1)^{\sigma(\{x_{i_1},x_{i_2}\})}\langle b_{i_1},b_{i_2}\rangle \\
&= (n+1)^2\cdot 3D-\|\mathbf{Bz}-\mathbf{b_{n+1}}\|^2 \\
&= (n+1)^2\cdot 3D-\|\mathbf{Bz}-\mathbf{t}\|^2 \\
&= (n+1)^2\cdot 3D-d^2
\end{aligned}$$

The red part is due to `Lemma 2.5` in the paper.

For the `NO` instance, the total weight of the satisfied clauses by any assignment is less than $(n+1)^2\cdot 3D-d^2$. For the sake of contradiction, let's assume that there exists an assignment ρ that satisfies the clauses of weight greater than $(n+1)^2\cdot 3D-d^2$.

$$\begin{aligned}
\sum_{i_1,i_2\in[n+1]^2}\sum_{j=0}^{3}\rho(C^j_{i_1,i_2})w(C^j_{i_1,i_2}) &= \sum_{\substack{i_1,i_2\in[n+1]^2\&\\ \rho(x_{i_1})=\rho(x_{i_2})=1}} 3D-(-1)^{\sigma(\{x_{i_1},x_{i_2}\})}\langle b_{i_1},b_{i_2}\rangle \\
&\quad+\sum_{\substack{i_1,i_2\in[n+1]^2\&\\ \rho(x_{i_1})\neq\rho(x_{i_2})}} 3D+\sum_{\substack{i_1,i_2\in[n+1]^2\&\\ \rho(x_{i_1})=\rho(x_{i_2})=0}} 3D \\
&= (n+1)^2\cdot 3D-\sum_{\substack{i_1,i_2\in[n+1]^2\&\\ \rho(x_{i_1})=\rho(x_{i_2})=1}}(-1)^{\sigma(\{x_{i_1},x_{i_2}\})}\langle b_{i_1},b_{i_2}\rangle \\
&= (n+1)^2\cdot 3D-\left\|\sum_{i=1}^{n}\rho(x_i)\mathbf{b}_i-\rho(x_{n+1})\mathbf{b}_{n+1}\right\|^2 \\
&= (n+1)^2\cdot 3D-\left\|\sum_{i=1}^{n}\rho(x_i)\mathbf{b}_i-t\right\|^2 \\
&\geq (n+1)^2\cdot 3D-\left(\min_{z\in\{0,1\}^n}\|Bz-t\|\right)^2 \\
&> (n+1)^2\cdot 3D-d^2
\end{aligned}$$

This is a contradiction as the total weight of the satisfied clauses by the assignment ρ is less than $(n+1)^2\cdot 3D-d^2$.

The red part and the inequality is follows from `Corollory 3.1` in the paper.

5 Other Results

Here is the summary of the main results from the paper:

1. Reduction from $(0,1)$-CVP (ℓ_2 norm) to the minimum-weight k-Clique problem (`Section 3`). Generalizes the same for all even norms (`Section 5`).
2. Reduction from weighted MAX-p-SAT to $(0,1)$-CVP$_p$ is already known (`Theorem 4.1`). Shows the reverse direction (`Section 4`) and hence equivalence.
3. Any $(0,1)$-CVP in even norms can be reduced to odd norms (but not the other way around).