NP-hardness of the shortest vector problem

and its relation to the closest vector problem

Jeroen van Wier

Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg

June 12, 2019

Overview

SVP/CVP definition

Definition

The *optimisation* problem SVP is defined on instances $\mathbf{B} \in \mathbb{Z}^{n \times k}$, with the objective to find a non-zero vector $\vec{u} \in \mathcal{L}(\mathbf{B})$ such that

$$\|\vec{u}\| = \lambda(\mathbf{B}).$$

SVP/CVP definition

Definition

The *optimisation* problem SVP is defined on instances $\mathbf{B} \in \mathbb{Z}^{n \times k}$, with the objective to find a non-zero vector $\vec{u} \in \mathcal{L}(\mathbf{B})$ such that

$$\|\vec{u}\| = \lambda(\mathbf{B}).$$

Definition

The *optimisation* problem CVP is defined on instances $(\mathbf{B}, \vec{v})$, where $\mathbf{B} \in \mathbb{Z}^{n \times k}$ and $\vec{v} \in \mathbb{Z}^n$, with the objective to find a vector $\vec{u} \in \mathcal{L}(\mathbf{B})$ such that

$$\|\vec{u} - \vec{v}\| = \min_{\vec{w} \in \mathcal{L}(\mathbf{B})} \|\vec{w} - \vec{v}\|.$$

SVP/CVP definition

Definition

The *optimisation* problem SVP_γ is defined on instances $\mathbf{B} \in \mathbb{Z}^{n \times k}$, with the objective to find a non-zero vector $\vec{u} \in \mathcal{L}(\mathbf{B})$ such that

$$\|\vec{u}\| \leq \gamma \cdot \lambda(\mathbf{B}).$$

Definition

The *optimisation* problem CVP_γ is defined on instances $(\mathbf{B}, \vec{v})$, where $\mathbf{B} \in \mathbb{Z}^{n \times k}$ and $\vec{v} \in \mathbb{Z}^n$, with the objective to find a vector $\vec{u} \in \mathcal{L}(\mathbf{B})$ such that

$$\|\vec{u} - \vec{v}\| \leq \gamma \cdot \min_{\vec{w} \in \mathcal{L}(\mathbf{B})} \|\vec{w} - \vec{v}\|.$$

GapSVP definition

Definition

The *optimisation* problem SVP_γ is defined on instances $\mathbf{B} \in \mathbb{Z}^{n \times k}$, with the objective to find a non-zero vector $\vec{u} \in \mathcal{L}(\mathbf{B})$ such that

$$\|\vec{u}\| \leq \gamma \cdot \lambda(\mathbf{B}).$$

GapSVP definition

Definition

The *optimisation* problem SVP_γ is defined on instances $\mathbf{B} \in \mathbb{Z}^{n \times k}$, with the objective to find a non-zero vector $\vec{u} \in \mathcal{L}(\mathbf{B})$ such that

$$\|\vec{u}\| \leq \gamma \cdot \lambda(\mathbf{B}).$$

Definition

The *promise* problem GapSVP_γ is defined on instances $(\mathbf{B}, d)$, where $\mathbf{B} \in \mathbb{Z}^{n \times k}$ and $d \in \mathbb{R}^+$, with the objective to distinguish between the cases:

$$\texttt{yes} : \lambda(\mathbf{B}) \leq d$$
$$\texttt{no} : \lambda(\mathbf{B}) > \gamma \cdot d$$

GapCVP definition

Definition

The *optimisation* problem CVP_γ is defined on instances $(\mathbf{B}, \vec{v})$, where $\mathbf{B} \in \mathbb{Z}^{n \times k}$ and $\vec{v} \in \mathbb{Z}^n$, with the objective to find a vector $\vec{u} \in \mathcal{L}(\mathbf{B})$ such that

$$\|\vec{u} - \vec{v}\| \leq \gamma \cdot \min_{\vec{w} \in \mathcal{L}(\mathbf{B})} \|\vec{w} - \vec{v}\| .$$

GapCVP definition

Definition

The *optimisation* problem CVP_γ is defined on instances $(\mathbf{B}, \vec{v})$, where $\mathbf{B} \in \mathbb{Z}^{n \times k}$ and $\vec{v} \in \mathbb{Z}^n$, with the objective to find a vector $\vec{u} \in \mathcal{L}(\mathbf{B})$ such that

$$\|\vec{u} - \vec{v}\| \leq \gamma \cdot \min_{\vec{w} \in \mathcal{L}(\mathbf{B})} \|\vec{w} - \vec{v}\| .$$

Definition

The *promise* problem GapCVP_γ is defined on instances $(\mathbf{B}, \vec{y}, d)$, where $\mathbf{B} \in \mathbb{Z}^{n \times k}$, $\vec{y} \in \mathbb{Z}^n$, and $d \in \mathbb{R}^+$, with the objective to distinguish between the cases:

$$\texttt{yes} : \exists \vec{z} \in \mathbb{Z}^k \; \|\mathbf{B}\vec{z} - \vec{y}\| \leq d$$

$$\texttt{no} : \forall \vec{z} \in \mathbb{Z}^k \; \|\mathbf{B}\vec{z} - \vec{y}\| > \gamma \cdot d$$

GapCVP' definition

Definition

The *promise* problem GapCVP_γ is defined on instances $(\mathbf{B}, \vec{y}, d)$, where $\mathbf{B} \in \mathbb{Z}^{n \times k}$, $\vec{y} \in \mathbb{Z}^n$, and $d \in \mathbb{R}^+$, with the objective to distinguish between the cases:

$$\texttt{yes} : \exists \vec{z} \in \mathbb{Z}^k \, \|\mathbf{B}\vec{z} - \vec{y}\| \leq d$$

$$\texttt{no} : \forall \vec{z} \in \mathbb{Z}^k \, \|\mathbf{B}\vec{z} - \vec{y}\| > \gamma \cdot d$$

GapCVP' definition

Definition

The *promise* problem GapCVP_γ is defined on instances $(\mathbf{B}, \vec{y}, d)$, where $\mathbf{B} \in \mathbb{Z}^{n \times k}$, $\vec{y} \in \mathbb{Z}^n$, and $d \in \mathbb{R}^+$, with the objective to distinguish between the cases:

$$\texttt{yes} : \exists \vec{z} \in \mathbb{Z}^k \, \|\mathbf{B}\vec{z} - \vec{y}\| \leq d$$
$$\texttt{no} : \forall \vec{z} \in \mathbb{Z}^k \, \|\mathbf{B}\vec{z} - \vec{y}\| > \gamma \cdot d$$

Definition

The *promise* problem GapCVP'_γ is defined on instances $(\mathbf{B}, \vec{y}, d)$, where $\mathbf{B} \in \mathbb{Z}^{n \times n}$ is full-rank, $\vec{y} \in \mathbb{Z}^n$, and $d \in \mathbb{R}^+$, with the objective to distinguish between the cases:

$$\texttt{yes} : \exists \vec{z} \in \{0,1\}^n \, \|\mathbf{B}\vec{z} - \vec{y}\| \leq d$$
$$\texttt{no} : \forall \vec{z} \in \mathbb{Z}^k \forall w \in \mathbb{Z} \backslash \{0\} \, \|\mathbf{B}\vec{z} - w\vec{y}\| > \gamma \cdot d$$

Magic Geometry

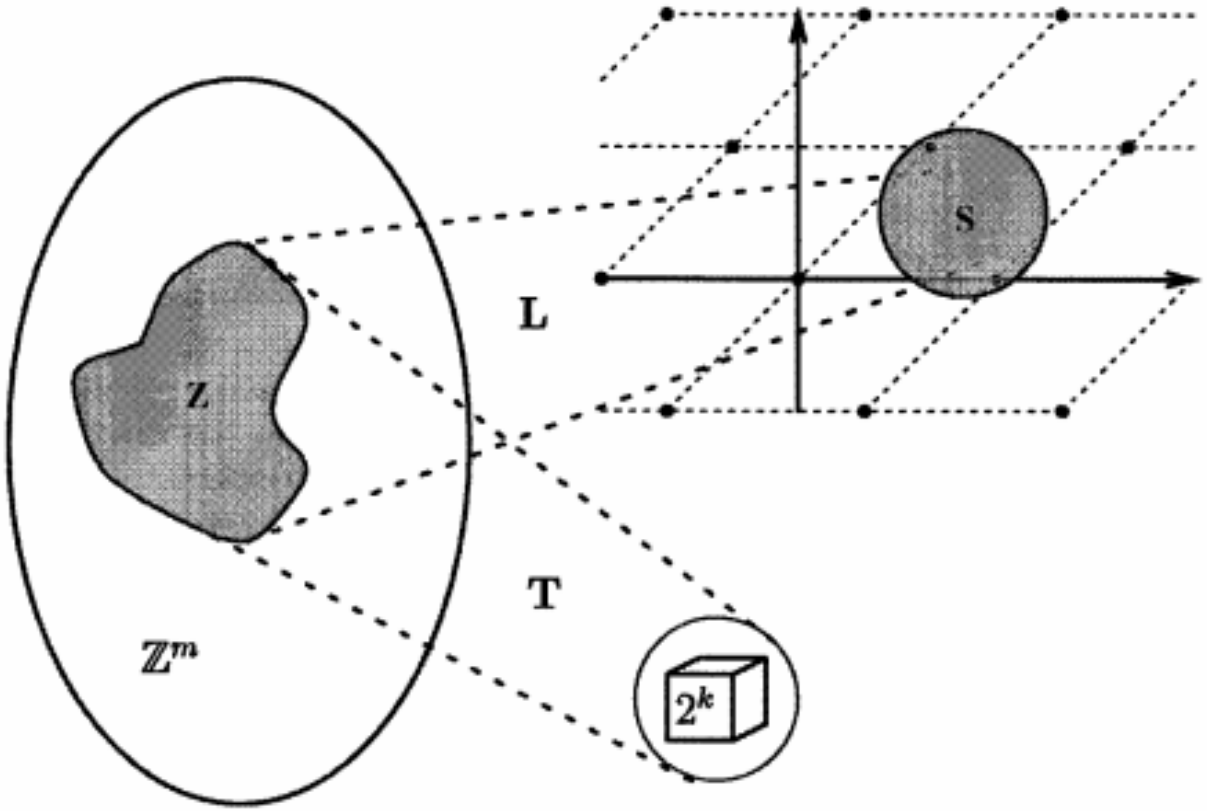
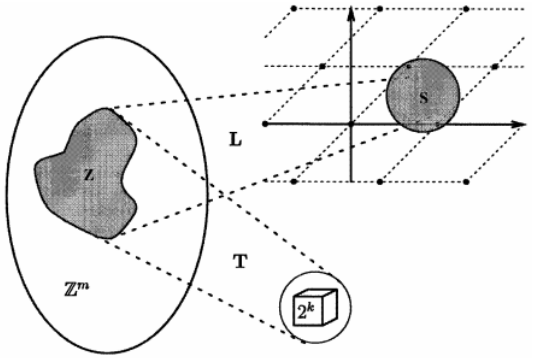


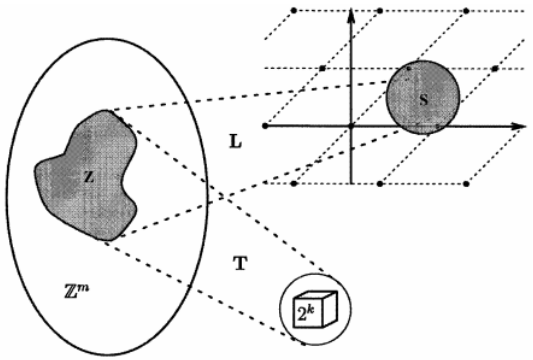
Figure: Source: [Mic01]

Magic Geometry



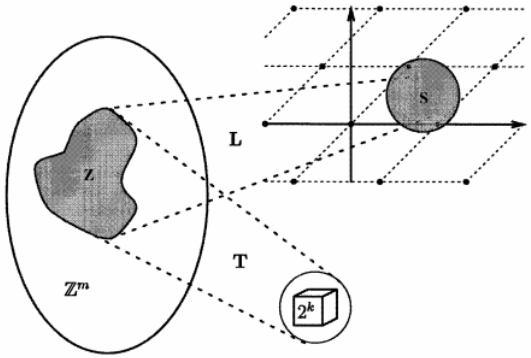
Parameter: $\tilde{\gamma} \in [1, \sqrt{2})$

Magic Geometry



Parameter: $\tilde{\gamma} \in [1, \sqrt{2})$
Input: $k \in \mathbb{Z}^+$

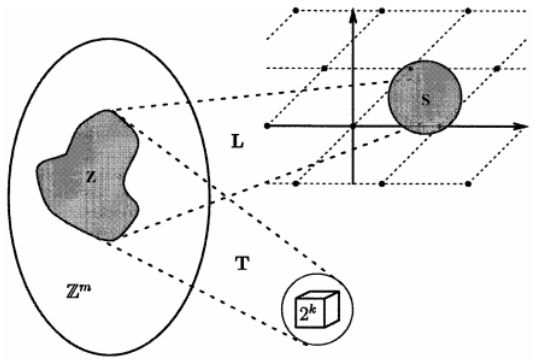
Magic Geometry



Parameter: $\tilde{\gamma} \in [1, \sqrt{2})$
Input: $k \in \mathbb{Z}^+$
Output: $m, r \in \mathbb{Z}^+, \mathbf{L} \in \mathbb{Z}^{(m+1)\times m}, \vec{s} \in Z^{m+1}, \mathbf{T} \in \mathbb{Z}^{k\times m}$

- $\lambda(\mathbf{L}) > \tilde{\gamma} \cdot r$

Magic Geometry



Parameter: $\tilde{\gamma} \in [1, \sqrt{2})$
Input: $k \in \mathbb{Z}^+$
Output: $m, r \in \mathbb{Z}^+, \mathbf{L} \in \mathbb{Z}^{(m+1)\times m}, \vec{s} \in Z^{m+1}, \mathbf{T} \in \mathbb{Z}^{k\times m}$

- $\lambda(\mathbf{L}) > \tilde{\gamma} \cdot r$

- $\forall \vec{x} \in \{0,1\}^k \exists \vec{z} \in \mathbb{Z}^m (\mathbf{T}\vec{z} = \vec{x} \wedge \|\mathbf{L}\vec{z} - \vec{s}\| \leq r)$

Reducing $\mathrm{GapCVP}'_{\gamma'}$ to GapSVP_{γ} [Mic01]

Fix: $\gamma \in [1, \sqrt{2})$

Reducing $\mathrm{GapCVP}'_{\gamma'}$ to GapSVP_{γ} [Mic01]

Fix: $\gamma \in [1, \sqrt{2})$
Pick: $\tilde{\gamma} \in (\gamma, \sqrt{2}]$ and γ'

Reducing $\mathrm{GapCVP}'_{\gamma'}$ to GapSVP_{γ} [Mic01]

Fix: $\gamma \in [1, \sqrt{2})$
Pick: $\tilde{\gamma} \in (\gamma, \sqrt{2}]$ and γ'
Input: $\mathrm{GapCVP}'_{\gamma'}$ instance $(\mathbf{B}, \vec{y}, d)$

Reducing $\mathrm{GapCVP}'_{\gamma'}$ to GapSVP_{γ} [Mic01]

Fix: $\gamma \in [1, \sqrt{2})$
Pick: $\tilde{\gamma} \in (\gamma, \sqrt{2}]$ and γ'
Input: $\mathrm{GapCVP}'_{\gamma'}$ instance $(\mathbf{B}, \vec{y}, d)$
Magic$_{\tilde{\gamma}}(\mathit{rank}(\mathbf{B}))$: $m, r \in \mathbb{Z}^+, \mathbf{L} \in \mathbb{Z}^{(m+1)\times m}, \vec{s} \in Z^{m+1}, \mathbf{T} \in \mathbb{Z}^{k\times m}$

Reducing $\mathrm{GapCVP}'_{\gamma'}$ to GapSVP_{γ} [Mic01]

Fix: $\gamma \in [1, \sqrt{2})$
Pick: $\tilde{\gamma} \in (\gamma, \sqrt{2}]$ and γ'
Input: $\mathrm{GapCVP}'_{\gamma'}$ instance $(\mathbf{B}, \vec{y}, d)$
Magic$_{\tilde{\gamma}}(\mathit{rank}(\mathbf{B}))$: $m, r \in \mathbb{Z}^+, \mathbf{L} \in \mathbb{Z}^{(m+1)\times m}, \vec{s} \in Z^{m+1}, \mathbf{T} \in \mathbb{Z}^{k\times m}$

$$\mathbf{V} = \left[\begin{array}{c|c} a \cdot \mathbf{BT} & a \cdot \vec{y} \\ b \cdot \mathbf{L} & b \cdot \vec{s} \end{array}\right]$$

Reducing $\mathrm{GapCVP}'_{\gamma'}$ to GapSVP_{γ} [Mic01]

Fix: $\gamma \in [1, \sqrt{2})$
Pick: $\tilde{\gamma} \in (\gamma, \sqrt{2}]$ and γ'
Input: $\mathrm{GapCVP}'_{\gamma'}$ instance $(\mathbf{B}, \vec{y}, d)$
Magic$_{\tilde{\gamma}}(rank(\mathbf{B}))$: $m, r \in \mathbb{Z}^+, \mathbf{L} \in \mathbb{Z}^{(m+1)\times m}, \vec{s} \in Z^{m+1}, \mathbf{T} \in \mathbb{Z}^{k\times m}$

$$\mathbf{V} = \left[\begin{array}{c|c} a \cdot \mathbf{BT} & a \cdot \vec{y} \\ b \cdot \mathbf{L} & b \cdot \vec{s} \end{array}\right]$$

no case: $\left\| \mathbf{V} \begin{bmatrix} \vec{z} \\ w \end{bmatrix} \right\|^2 = (a \cdot \|\mathbf{BT}\vec{z} + w\vec{y}\|)^2 + (b \cdot \|\mathbf{L}\vec{z} + w\vec{s}\|)^2$

Reducing $\mathrm{GapCVP}'_{\gamma'}$ to GapSVP_{γ} [Mic01]

Fix: $\gamma \in [1, \sqrt{2})$
Pick: $\tilde{\gamma} \in (\gamma, \sqrt{2}]$ and γ'
Input: $\mathrm{GapCVP}'_{\gamma'}$ instance $(\mathbf{B}, \vec{y}, d)$
Magic$_{\tilde{\gamma}}(rank(\mathbf{B}))$: $m, r \in \mathbb{Z}^+, \mathbf{L} \in \mathbb{Z}^{(m+1)\times m}, \vec{s} \in Z^{m+1}, \mathbf{T} \in \mathbb{Z}^{k\times m}$

$$\mathbf{V} = \left[\begin{array}{c|c} a \cdot \mathbf{BT} & a \cdot \vec{y} \\ b \cdot \mathbf{L} & b \cdot \vec{s} \end{array}\right]$$

no case: $\left\| \mathbf{V} \begin{bmatrix} \vec{z} \\ w \end{bmatrix} \right\|^2 = (a \cdot \|\mathbf{BT}\vec{z} + w\vec{y}\|)^2 + (b \cdot \|\mathbf{L}\vec{z} + w\vec{s}\|)^2$

yes case: $\exists \vec{x} \in \{0,1\}^k, \vec{z} \in \mathbb{Z}^m$ such that $\|\mathbf{B}\vec{x} - \vec{y}\| \leq d$ and $\mathbf{T}\vec{z} = \vec{x}$

$$\left\| \mathbf{V} \begin{bmatrix} \vec{z} \\ -1 \end{bmatrix} \right\|^2 = (a \cdot \|\mathbf{B}\vec{x} - \vec{y}\|)^2 + (b \cdot \|\mathbf{L}\vec{z} - \vec{s}\|)^2$$

SetCover definition

Definition

The *promise* problem $\mathrm{SetCover}_c$ is defined on instances $(\mathcal{U}, S_1, \ldots, S_m, K)$, where $\mathcal{U}$ is a set, $S_1, \ldots, S_n \subseteq \mathcal{U}$, and $K \in \mathbb{Z}^+$, with the objective to distinguish between the cases:

`yes` :There is a collection of K pairwise disjoint S_i's whose union is $\mathcal{U}$

`no` :There is no collection of less cK S_i's whose union is $\mathcal{U}$

SetCover definition

Definition

The *promise* problem $\mathrm{SetCover}_c$ is defined on instances $(\mathcal{U}, S_1, \ldots, S_m, K)$, where $\mathcal{U}$ is a set, $S_1, \ldots, S_n \subseteq \mathcal{U}$, and $K \in \mathbb{Z}^+$, with the objective to distinguish between the cases:

`yes` :There is a collection of K pairwise disjoint S_i's whose union is $\mathcal{U}$

`no` :There is no collection of less cK S_i's whose union is $\mathcal{U}$

Theorem ([Bel+93])

For any constant $c \geq 1$, $\mathrm{SetCover}_c$ is NP-hard.

Reducing $\mathrm{SetCover}_c$ to $\mathrm{GapCVP}'_{\gamma'}$ [Aro+97]

Fix: $c = \gamma'^2$

Reducing $\mathrm{SetCover}_c$ to $\mathrm{GapCVP}'_{\gamma'}$ [Aro+97]

Fix: $c = \gamma'^2$

Input: $\mathrm{SetCover}_c$ instance $(\mathcal{U}, S_1, \ldots, S_m, K)$

Reducing $\mathrm{SetCover}_c$ to $\mathrm{GapCVP}'_{\gamma'}$ [Aro+97]

Fix: $c = \gamma'^2$

Input: $\mathrm{SetCover}_c$ instance $(\mathcal{U}, S_1, \ldots, S_m, K)$

Define: $L = cK$, $\vec{b_0} \in \mathbb{Z}^{|\mathcal{U}|+m}$ is L in the first $|\mathcal{U}|$ coordinates and 0 in the rest

Reducing $\mathrm{SetCover}_c$ to $\mathrm{GapCVP}'_{\gamma'}$ [Aro+97]

Fix: $c = \gamma'^2$

Input: $\mathrm{SetCover}_c$ instance $(\mathcal{U}, S_1, \ldots, S_m, K)$

Define: $L = cK$, $\vec{b_0} \in \mathbb{Z}^{|\mathcal{U}|+m}$ is L in the first $|\mathcal{U}|$ coordinates and 0 in the rest

$$\mathbf{B} = \left[\begin{array}{ccc} L\chi_{S_1} & \ldots & L\chi_{S_m} \\ \hline & \mathbb{I}_m & \end{array}\right]$$

Reducing $\mathrm{SetCover}_c$ to $\mathrm{GapCVP}'_{\gamma'}$ [Aro+97]

Fix: $c = \gamma'^2$

Input: $\mathrm{SetCover}_c$ instance $(\mathcal{U}, S_1, \ldots, S_m, K)$

Define: $L = cK$, $\vec{b_0} \in \mathbb{Z}^{|\mathcal{U}|+m}$ is L in the first $|\mathcal{U}|$ coordinates and 0 in the rest

$$\mathbf{B} = \left[\begin{array}{ccc} L\chi_{S_1} & \ldots & L\chi_{S_m} \\ \hline & \mathbb{I}_m & \end{array}\right]$$

Define: $O_w = \min_{\vec{a} \in \mathbb{Z}^m} \left\| \mathbf{B}\vec{a} - w\vec{b_0} \right\|$

Reducing $\mathrm{SetCover}_c$ to $\mathrm{GapCVP}'_{\gamma'}$ [Aro+97]

Fix: $c = \gamma'^2$

Input: $\mathrm{SetCover}_c$ instance $(\mathcal{U}, S_1, \ldots, S_m, K)$

Define: $L = cK$, $\vec{b_0} \in \mathbb{Z}^{|\mathcal{U}|+m}$ is L in the first $|\mathcal{U}|$ coordinates and 0 in the rest

$$\mathbf{B} = \left[\begin{array}{ccc} L\chi_{S_1} & \ldots & L\chi_{S_m} \\ \hline & \mathbb{I}_m & \end{array}\right]$$

Define: $O_w = \min_{\vec{a} \in \mathbb{Z}^m} \left\| \mathbf{B}\vec{a} - w\vec{b_0} \right\|$

yes case: $\exists I \subseteq [m] \bigcup_{i \in I} S_i = \mathcal{U}$ and thus $\vec{a} = \chi_I \in \{0,1\}^m$ shows $O_1 \leq \sqrt{K}$

Reducing $\mathrm{SetCover}_c$ to $\mathrm{GapCVP}'_{\gamma'}$ [Aro+97]

Fix: $c = \gamma'^2$

Input: $\mathrm{SetCover}_c$ instance $(\mathcal{U}, S_1, \ldots, S_m, K)$

Define: $L = cK$, $\vec{b_0} \in \mathbb{Z}^{|\mathcal{U}|+m}$ is L in the first $|\mathcal{U}|$ coordinates and 0 in the rest

$$\mathbf{B} = \left[\begin{array}{ccc} L\chi_{S_1} & \cdots & L\chi_{S_m} \\ \hline & \mathbb{I}_m & \end{array}\right]$$

Define: $O_w = \min_{\vec{a} \in \mathbb{Z}^m} \left\| \mathbf{B}\vec{a} - w\vec{b_0} \right\|$

`yes` case: $\exists I \subseteq [m] \bigcup_{i \in I} S_i = \mathcal{U}$ and thus $\vec{a} = \chi_I \in \{0,1\}^m$ shows $O_1 \leq \sqrt{K}$

`no` case: Let $\vec{a}$ witness O_w, then either

Reducing $\mathrm{SetCover}_c$ to $\mathrm{GapCVP}'_{\gamma'}$ [Aro+97]

Fix: $c = \gamma'^2$

Input: $\mathrm{SetCover}_c$ instance $(\mathcal{U}, S_1, \ldots, S_m, K)$

Define: $L = cK$, $\vec{b_0} \in \mathbb{Z}^{|\mathcal{U}|+m}$ is L in the first $|\mathcal{U}|$ coordinates and 0 in the rest

$$\mathbf{B} = \left[\begin{array}{ccc} L\chi_{S_1} & \cdots & L\chi_{S_m} \\ \hline & \mathbb{I}_m & \end{array}\right]$$

Define: $O_w = \min_{\vec{a} \in \mathbb{Z}^m} \left\| \mathbf{B}\vec{a} - w\vec{b_0} \right\|$

`yes` case: $\exists I \subseteq [m] \bigcup_{i \in I} S_i = \mathcal{U}$ and thus $\vec{a} = \chi_I \in \{0,1\}^m$ shows $O_1 \leq \sqrt{K}$

`no` case: Let $\vec{a}$ witness O_w, then either

- $\bigcup \{S_i \mid a_i \neq 0\} = \mathcal{U}$, then $O_w \geq \|\vec{a}\| \geq \sqrt{cK} = \gamma'\sqrt{K}$

Reducing $\mathrm{SetCover}_c$ to $\mathrm{GapCVP}'_{\gamma'}$ [Aro+97]

Fix: $c = \gamma'^2$

Input: $\mathrm{SetCover}_c$ instance $(\mathcal{U}, S_1, \ldots, S_m, K)$

Define: $L = cK$, $\vec{b_0} \in \mathbb{Z}^{|\mathcal{U}|+m}$ is L in the first $|\mathcal{U}|$ coordinates and 0 in the rest

$$\mathbf{B} = \left[\begin{array}{ccc} L\chi_{S_1} & \cdots & L\chi_{S_m} \\ \hline & \mathbb{I}_m & \end{array}\right]$$

Define: $O_w = \min_{\vec{a} \in \mathbb{Z}^m} \left\| \mathbf{B}\vec{a} - w\vec{b_0} \right\|$

yes case: $\exists I \subseteq [m] \bigcup_{i \in I} S_i = \mathcal{U}$ and thus $\vec{a} = \chi_I \in \{0,1\}^m$ shows $O_1 \leq \sqrt{K}$

no case: Let $\vec{a}$ witness O_w, then either

- $\bigcup \{S_i \mid a_i \neq 0\} = \mathcal{U}$, then $O_w \geq \|\vec{a}\| \geq \sqrt{cK} = \gamma'\sqrt{K}$
- One of the first $|\mathcal{U}|$ coordinates is not 0 and thus $O_w \geq \sqrt{L} = \gamma'\sqrt{K}$

Reducing $\mathrm{SetCover}_c$ to $\mathrm{GapCVP}'_{\gamma'}$ [Aro+97]

Fix: $c = \gamma'^2$

Input: $\mathrm{SetCover}_c$ instance $(\mathcal{U}, S_1, \ldots, S_m, K)$

Define: $L = cK$, $\vec{b_0} \in \mathbb{Z}^{|\mathcal{U}|+m}$ is L in the first $|\mathcal{U}|$ coordinates and 0 in the rest

$$\mathbf{B} = \left[\begin{array}{ccc} L\chi_{S_1} & \ldots & L\chi_{S_m} \\ \hline & \mathbb{I}_m & \end{array}\right]$$

Define: $O_w = \min_{\vec{a} \in \mathbb{Z}^m} \left\| \mathbf{B}\vec{a} - w\vec{b_0} \right\|$

`yes` case: $\exists I \subseteq [m] \bigcup_{i \in I} S_i = \mathcal{U}$ and thus $\vec{a} = \chi_I \in \{0,1\}^m$ shows $O_1 \leq \sqrt{K}$

`no` case: Let $\vec{a}$ witness O_w, then either

- $\bigcup \{S_i \mid a_i \neq 0\} = \mathcal{U}$, then $O_w \geq \|\vec{a}\| \geq \sqrt{cK} = \gamma'\sqrt{K}$
- One of the first $|\mathcal{U}|$ coordinates is not 0 and thus $O_w \geq \sqrt{L} = \gamma'\sqrt{K}$

Thus $(\mathbf{B}, \vec{b_0}, \sqrt{K})$ is an equivalent $\mathrm{GapCVP}'_{\gamma'}$ instance

Reducing GapSVP_γ to GapCVP_γ

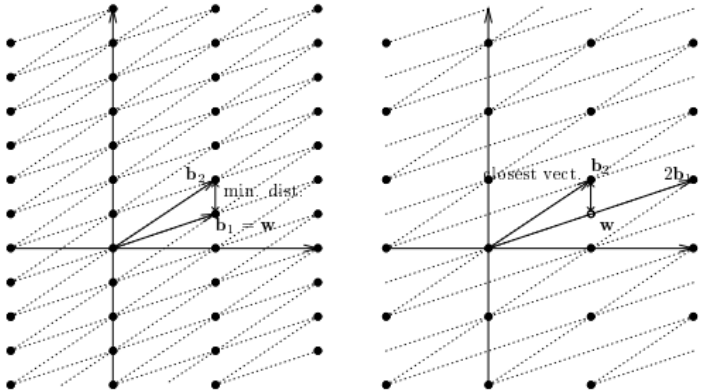


Figure: Source: [GoI+99]

Input: GapSVP_γ instance $(\mathbf{B}, d)$, where $\mathbf{B} = [\vec{b}_1, \ldots, \vec{b}_n]$

Reducing GapSVP_γ to GapCVP_γ

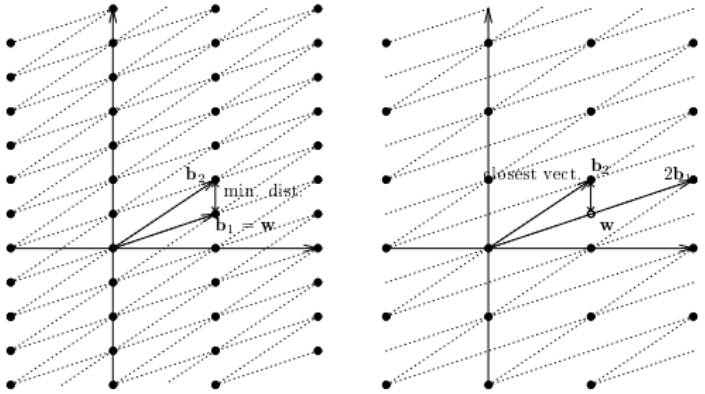


Figure: Source: [Gol+99]

Input: GapSVP_γ instance $(\mathbf{B}, d)$, where $\mathbf{B} = [\vec{b}_1, \ldots, \vec{b}_n]$

Define for all j: $\mathbf{B}^{(j)} = [\vec{b}_1, \ldots, \vec{b}_{j-1}, 2\vec{b}_j, \vec{b}_{j+1}, \ldots, \vec{b}_n]$

Reducing GapSVP_γ to GapCVP_γ

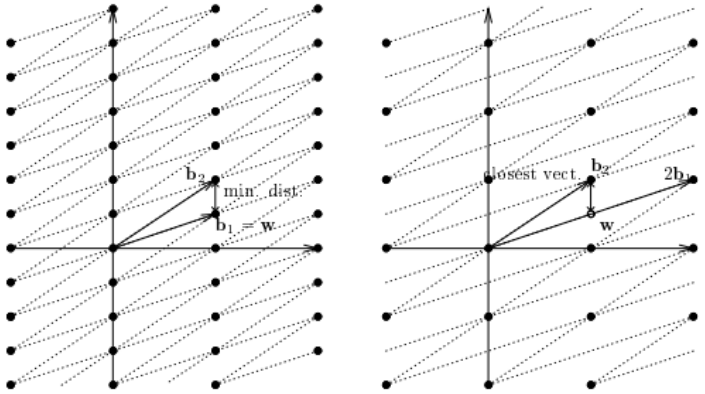


Figure: Source: [GoI+99]

Input: GapSVP_γ instance $(\mathbf{B}, d)$, where $\mathbf{B} = [\vec{b}_1, \ldots, \vec{b}_n]$
Define for all j: $\mathbf{B}^{(j)} = [\vec{b}_1, \ldots, \vec{b}_{j-1}, 2\vec{b}_j, \vec{b}_{j+1}, \ldots, \vec{b}_n]$
yes case: Let $\mathbf{B}\vec{x} = \vec{v}$ be such that $\|\vec{v}\| \leq d$, then at least one x_j is odd and $\vec{v} + \vec{b}_j \in \mathcal{L}(\mathbf{B}^{(j)})$

Reducing GapSVP_γ to GapCVP_γ

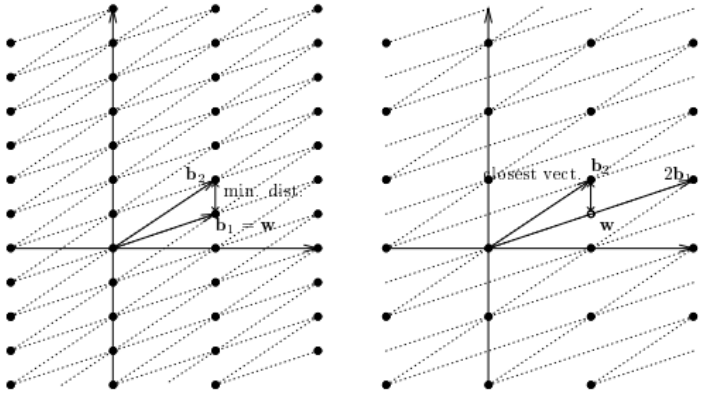


Figure: Source: [GoI+99]

Input: GapSVP_γ instance $(\mathbf{B}, d)$, where $\mathbf{B} = [\vec{b}_1, \ldots, \vec{b}_n]$

Define for all j: $\mathbf{B}^{(j)} = [\vec{b}_1, \ldots, \vec{b}_{j-1}, 2\vec{b}_j, \vec{b}_{j+1}, \ldots, \vec{b}_n]$

yes case: Let $\mathbf{B}\vec{x} = \vec{v}$ be such that $\|\vec{v}\| \leq d$, then at least one x_j is odd and $\vec{v} + \vec{b}_j \in \mathcal{L}(\mathbf{B}^{(j)})$

no case: For any $\vec{b}_j$ and any $\vec{u} \in \mathcal{L}(\mathbf{B}^{(j)})$, $\vec{v} = \vec{u} - \vec{b}_j \in \mathcal{L}(\mathbf{B})$ thus $\left\|\vec{u} - \vec{b}_j\right\| \geq \gamma d$

Reducing GapSVP_γ to GapCVP_γ

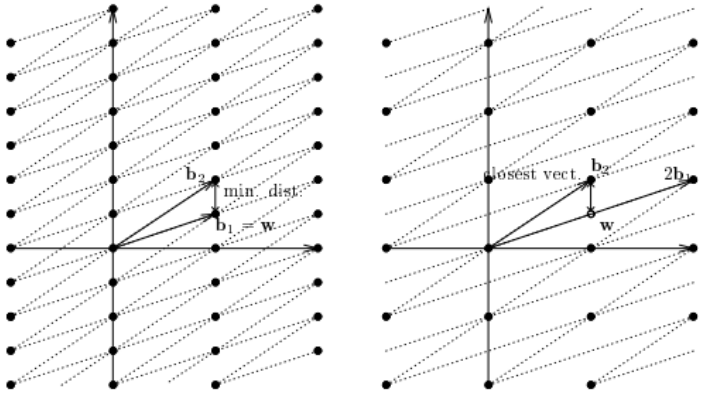


Figure: Source: [Gol+99]

Input: GapSVP_γ instance $(\mathbf{B}, d)$, where $\mathbf{B} = [\vec{b}_1, \ldots, \vec{b}_n]$

Define for all j: $\mathbf{B}^{(j)} = [\vec{b}_1, \ldots, \vec{b}_{j-1}, 2\vec{b}_j, \vec{b}_{j+1}, \ldots, \vec{b}_n]$

yes case: Let $\mathbf{B}\vec{x} = \vec{v}$ be such that $\|\vec{v}\| \leq d$, then at least one x_j is odd and $\vec{v} + \vec{b}_j \in \mathcal{L}(\mathbf{B}^{(j)})$

no case: For any $\vec{b}_j$ and any $\vec{u} \in \mathcal{L}(\mathbf{B}^{(j)})$, $\vec{v} = \vec{u} - \vec{b}_j \in \mathcal{L}(\mathbf{B})$ thus $\left\|\vec{u} - \vec{b}_j\right\| \geq \gamma d$

Thus the OR of $\mathrm{GapCVP}_\gamma(\mathbf{B}^{(j)}, \vec{b}_j, d)$ is equivalent to $\mathrm{GapSVP}_\gamma(\mathbf{B}, d)$

Thanks!

References

Sanjeev Arora et al. "The hardness of approximate optima in lattices, codes, and systems of linear equations". In: *Journal of Computer and System Sciences* 54.2 (1997), pp. 317–331.

M Bellare et al. "Efficient multi-prover interactive proofs with applications to approximation problems". In: *Proc. 25th ACM Symp. on Theory of Computing*. Vol. 113. 1993, p. 131.

Oded Goldreich et al. "Approximating shortest lattice vectors is not harder than approximating closest lattice vectors". In: *Information Processing Letters* 71.2 (1999), pp. 55–61.

Daniele Micciancio. "The shortest vector in a lattice is hard to approximate to within some constant". In: *SIAM journal on Computing* 30.6 (2001), pp. 2008–2035.