

Задача CVP

Шокуров

25 февраля 2025 г.

Аппроксимация решения задачи CVP

Задача ACVP (Approximate CVP). Пусть задан вектор $\mathbf{b} \in \mathbb{R}^m$ и n -мерная решетка с базисом $\mathbf{b}_1, \dots, \mathbf{b}_n$, ($n \leq m$). Требуется найти вектор $\mathbf{b}_0 \in \mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_n)$, для которого выполнено соотношение

$$\|\mathbf{b} - \mathbf{b}_0\| \leq 2(2/\sqrt{3})^n \min_{\mathbf{x} \in \mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_n)} \|\mathbf{x} - \mathbf{b}\|.$$

ACVP-алгоритм

Вход: Базис решетки $\mathbf{B} = (\mathbf{b}_1, \dots, \mathbf{b}_n) \in \mathbb{Z}^{m \times n}$ и вектор $\mathbf{t} \in \mathbb{Q}^m$

Выход: Вектор решетки $\mathbf{x} \in \mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_n)$, для которого выполняется соотношение

$$\|\mathbf{x} - \mathbf{t}\| \leq 2(2/\sqrt{3})^n \min_{\mathbf{y} \in \mathcal{L}(\mathbf{b}_1, \dots, \mathbf{b}_n)} \|\mathbf{y} - \mathbf{t}\|.$$

Выполнить δ_n — LLL -алгоритм (найти приведенный базис $(\mathbf{b}_1, \dots, \mathbf{b}_n)$ решетки \mathbf{B}).

$\mathbf{b} := \mathbf{t}$

for $j = n, \dots, 1$

$$c_j = \lfloor (\mathbf{b}, \mathbf{b}_j^*) / (\mathbf{b}_j^*, \mathbf{b}_j^*) \rfloor$$

$\mathbf{b} := \mathbf{b} - c_j \mathbf{b}_j$

$\mathbf{x} := \mathbf{t} - \mathbf{b}$ — выход

Теорема

При $\delta_n = (1/4) + (3/4)^{n/(n-1)}$ ACVP-алгоритм решает задачу ACVP.

Доказательство теоремы

Доказательство. Без ограничения общности можно считать, что базис $(\mathbf{b}_1, \dots, \mathbf{b}_n)$ является δ LLL-приведенным, а $\mathbf{t} \in \text{span}(\mathbf{b}_1, \dots, \mathbf{b}_n)$.

Отсюда следует, что для всех $k = 1, \dots, n$ базисы $(\mathbf{b}_1, \dots, \mathbf{b}_k)$ являются также δ LLL-приведенными. Пусть $(\mathbf{b}_1^*, \dots, \mathbf{b}_n^*)$ — ортогональный базис, полученный из базиса $(\mathbf{b}_1, \dots, \mathbf{b}_n)$ в процессе ортогонализации Грамма-Шмидта.

Тогда ACVP-алгоритм имеет следующее эквивалентное описание, позволяющее провести доказательство индукцией по размерности решетки:

- Найти такое целое число c , для которого гиперплоскость $c\mathbf{b}_n^* + \text{span}(\mathbf{b}_1, \dots, \mathbf{b}_{n-1})$ является ближайшей к вектору \mathbf{t} .
- Найти проекцию \mathbf{t}' вектора $\mathbf{t} - c\mathbf{b}_n$ на $\text{span}(\mathbf{b}_1, \dots, \mathbf{b}_{n-1})$.
- Применить ACVP-алгоритм к решетке $L(\mathbf{b}_1, \dots, \mathbf{b}_{n-1})$ и вектору \mathbf{t}' . Получим вектор $\mathbf{x}' \in L(\mathbf{b}_1, \dots, \mathbf{b}_{n-1})$.
- $\mathbf{x} := \mathbf{x}' + c\mathbf{b}_n$ — решение ACVP-задачи.

Доказательство теоремы

Пусть $\mathbf{y} \in L(\mathbf{b}_1, \dots, \mathbf{b}_n)$ — ближайший вектор решетки для \mathbf{t} . Требуется доказать, что

$$\|\mathbf{t} - \mathbf{x}\| \leq 2(2/\sqrt{3})^n \|\mathbf{t} - \mathbf{y}\|.$$

Возможны два случая.

Случай 1. $\|\mathbf{t} - \mathbf{y}\| < \|\mathbf{b}_n^*\|/2$. В этом случае \mathbf{y} лежит в гиперплоскости $\text{span}(\mathbf{b}_1, \dots, \mathbf{b}_{n-1}) + c\mathbf{b}_n$. Поэтому $\mathbf{y}' = \mathbf{y} - c\mathbf{b}_n$ ближайшая к \mathbf{t}' точка решетки $L(\mathbf{b}_1, \dots, \mathbf{b}_{n-1})$. Тогда по предположению индукции алгоритм ACVP находит точку $\mathbf{x}' \in \text{span}(\mathbf{b}_1, \dots, \mathbf{b}_{n-1})$, являющуюся решением задачи ACVP для проекции \mathbf{t}' вектора $\mathbf{t} - c\mathbf{b}_n$ на $\text{span}(\mathbf{b}_1, \dots, \mathbf{b}_{n-1})$, т.е. выполняется неравенство

$$\|\mathbf{t}' - \mathbf{x}'\| \leq 2(2/\sqrt{3})^{n-1} \|\mathbf{t}' - \mathbf{y}'\|.$$

Доказательство теоремы

Следовательно, учитывая неравенство $1 \leq 4(2/\sqrt{3})^{2(n-1)}$ и ортогональность вектора $\mathbf{t} - \mathbf{t}'$ гиперплоскости $\text{span}(\mathbf{b}_1, \dots, \mathbf{b}_{n-1})$,

$$\begin{aligned}\|\mathbf{t} - \mathbf{x}\|^2 &= \|(\mathbf{t} - c\mathbf{b}_n) - \mathbf{t}'\|^2 + \|\mathbf{t}' - \mathbf{x}'\|^2 \\ &\leq \|(\mathbf{t} - c\mathbf{b}_n) - \mathbf{t}'\|^2 + 4(2/\sqrt{3})^{2(n-1)}\|\mathbf{t}' - \mathbf{y}'\|^2 \\ &\leq 4(2/\sqrt{3})^{2(n-1)}\|(\mathbf{t} - c\mathbf{b}_n) - \mathbf{t}'\|^2 + 4(2/\sqrt{3})^{2(n-1)}\|\mathbf{t}' - \mathbf{y}'\|^2 \\ &= 4(2/\sqrt{3})^{2(n-1)}(\|(\mathbf{t} - c\mathbf{b}_n) - \mathbf{t}'\|^2 + \|\mathbf{t}' - \mathbf{y}'\|^2) \\ &= 4(2/\sqrt{3})^{2(n-1)}\|\mathbf{t} - \mathbf{y}\|^2,\end{aligned}$$

т.е.

$$\|\mathbf{t} - \mathbf{x}\| \leq 2(2/\sqrt{3})^{n-1}\|\mathbf{t} - \mathbf{y}\| < 2(2/\sqrt{3})^n\|\mathbf{t} - \mathbf{y}\|.$$

Случай 2. $\|\mathbf{t} - \mathbf{y}\| \geq \|\mathbf{b}_n^*\|/2$. Из свойств коэффициентов c следует, что выполняется равенство $\mathbf{t} - \mathbf{x} = \sum_{i=1}^n \mu_i \mathbf{b}_i^*$, где $|\mu_i| \leq 1/2$. Условие δ -LLL-приведенности базиса $\mathbf{b}_1, \dots, \mathbf{b}_n$ означает, что для всех $i \leq n$ выполняются неравенства $\|\mathbf{b}_i^*\| \leq \alpha^{n-i} \|\mathbf{b}_n^*\|$, где $\alpha = 2/\sqrt{4\delta - 1}$. Поэтому,

$$\begin{aligned}
 \|\mathbf{t} - \mathbf{x}\|^2 &= \sum_{i=1}^n \mu_i^2 \|\mathbf{b}_i^*\|^2 \\
 &\leq \frac{1}{4} \sum_{i=1}^n \alpha^{2(n-i)} \|\mathbf{b}_n^*\|^2 \\
 &= \frac{\alpha^{2n}-1}{\alpha^2-1} \|\mathbf{b}_n^*\|^2 \\
 &= \frac{\alpha^{2(n-1)}}{4} \left(1 + \frac{1-\alpha^{2(1-n)}}{\alpha^2-1}\right) \|\mathbf{b}_n^*\|^2.
 \end{aligned} \tag{1}$$

Поскольку $\alpha = 2/\sqrt{4\delta - 1}$ и $\delta = (1/4) + (3/4)^{n/(n-1)}$, выполняются равенства $\alpha^{2(n-1)} = (4/3)^n$ и $\alpha^2 = (4/3)^{1+1/(n-1)}$. Поэтому из соотношения (1) следует

$$\|\mathbf{t} - \mathbf{x}\|^2 \leq \frac{1}{4} \left(\frac{4}{3}\right)^n \left(1 + \frac{1 - \left(\frac{3}{4}\right)^n}{\left(\frac{4}{3}\right)^{1+\frac{1}{n-1}} - 1}\right) \|\mathbf{b}_n^*\|^2 \leq \left(\frac{4}{3}\right)^n \|\mathbf{b}_n^*\|^2.$$

Задачи SVP нахождения кратчайшего вектора (Shortest Vector Problem).

1. Точное решение задачи SVP.

- **Дано:** Базис B целочисленной решетки $\Lambda = L(B)$.
- **Найти:** ненулевой вектор $\mathbf{v} \in \Lambda$, для которого $\|\mathbf{v}\| = \lambda_1$.

2. Поиск короткого вектора в решетке. Оценка качества решения

- **Дано:** Базис B целочисленной решетки $\Lambda = L(B)$.
- **Найти:** ненулевой вектор $\mathbf{v} \in \Lambda$ и указать $\gamma \geq 1$, для которого $\|\mathbf{v}\| \leq \gamma \lambda_1$.

3. Поиск γ -приближения.

- **Дано:** Базис B целочисленной решетки $\Lambda = L(B)$ и число $\gamma \geq 1$.
- **Найти:** $\mathbf{v} \in \Lambda$, для которого $\|\mathbf{v}\| \leq \gamma \lambda_1$.

Задачи CVP нахождения ближайшего вектора (Closest Vector Problem).

1 Точное решение задачи CVP.

- ▶ **Дано:** Базис B целочисленной решетки $\Lambda = L(B)$ и вектор $\mathbf{t} \in \mathbb{Q}^n$.
- ▶ **Найти:** $\mathbf{x} \in \Lambda$, для которого $\|\mathbf{t} - \mathbf{x}\|$ минимальна.

2 Поиск ближайшего вектора в решетке. Оценка качества решения

- ▶ **Дано:** Базис B целочисленной решетки $\Lambda = L(B)$ и вектор $\mathbf{t} \in \mathbb{Q}^n$.
- ▶ **Найти:** $\mathbf{v} \in \Lambda$ и указать $\gamma \geq 1$, для которого $\|\mathbf{v} - \mathbf{t}\| \leq \gamma \|\mathbf{By} - \mathbf{t}\|$ при всех $\mathbf{y} \in \Lambda$.

3 Поиск γ -приближения.

- ▶ **Дано:** Базис B целочисленной решетки $\Lambda = L(B)$, вектор \mathbf{t} и число γ .
- ▶ **Найти:** $\mathbf{v} \in \Lambda$, для которого $\|\mathbf{v} - \mathbf{t}\| \leq \gamma \|\mathbf{By} - \mathbf{t}\|$ при всех $\mathbf{y} \in \Lambda$.

Вычислительные задачи SVP и CVP для точного решения

- **Задача поиска.** Найти (ненулевой) вектор решетки $\mathbf{x} \in \Lambda$ минимизирующий величину $\|\mathbf{x} - \mathbf{t}\|$ (соответственно, $\|\mathbf{x}\|$).
- **Задача оптимизации.** Найти минимум $\|\mathbf{x} - \mathbf{t}\|$ (соответственно, $\|\mathbf{x}\|$) по всем $\mathbf{x} \in \Lambda$ (соответственно, $\mathbf{x} \in \Lambda \setminus \{0\}$).
- **Задача распознавания.** По заданному рациональному числу $r > 0$ определить, существует ли (ненулевой) вектор решетки \mathbf{x} , для которого $\|\mathbf{x} - \mathbf{t}\| \leq r$ (соответственно, $\|\mathbf{x}\| \leq r$).

Вычислительные задачи SVP и CVP для γ -приближения

Задача поиска приближенного решения. Найти (ненулевой) вектор $\mathbf{v} \in \Lambda$, такой что $\|\mathbf{v} - \mathbf{t}\| \leq \gamma \cdot \|\mathbf{y} - \mathbf{t}\|$ для всех $\mathbf{y} \in \Lambda$ ($\|\mathbf{v}\| \leq \gamma \cdot \|\mathbf{y}\|$ для всех $\mathbf{y} \in \Lambda \setminus \{0\}$).

Приближенная задача оптимизации. Найти (ненулевое) число d , такое что $\|\mathbf{z} - \mathbf{t}\| \leq d \leq \gamma \cdot \|\mathbf{y} - \mathbf{t}\|$ для всех $\mathbf{y} \in \Lambda$ при некотором $\mathbf{z} \in \Lambda$ ($\lambda_1 \leq d < \gamma \cdot \lambda_1$).

Эффективно решаемые задачи на решетках

- 1 **Задача принадлежности.** Даны базис B решетки и вектор \mathbf{x} . Проверить, является ли \mathbf{x} элементом решетки $L(B)$?
- 2 **Нахождение ядра.** Дана целочисленная матрица $A \in \mathbb{Z}^{m \times n}$. Найти базис решетки $\{\mathbf{x} \in \mathbb{Z}^n \mid A\mathbf{x} = 0\}$. Аналогичная задача для сравнений по модулю. Даны натуральное число M и матрица $A \in \mathbb{Z}_M^{m \times n}$. Найти базис решетки $\{\mathbf{x} \in \mathbb{Z}^n \mid A\mathbf{x} = 0 \pmod{M}\}$.
- 3 **Построение базиса.** Задан набор целочисленных векторов. Найти базис решетки, которую они порождают.
- 4 **Объединение решеток.** Даны две решетки $L(B_1)$ и $L(B_2)$ в \mathbb{Z}^n . Найти минимальную содержащую их решетку.
- 5 **Построение двойственной решетки.** Дана решетка $L(B)$. Построить двойственную решетки, иными словами множество всех векторов \mathbf{y} в $\text{Span}(L(B))$, для которых скалярные произведения $\langle \mathbf{x}, \mathbf{y} \rangle$ целочисленны при всех $\mathbf{x} \in L(B)$.

Эффективно решаемые задачи на решетках

- ❶ **Пересечение решеток.** Даны две решетки $L(B_1)$ и $L(B_2)$ в \mathbb{Z}^n . Найти базис пересечения $L(B_1) \cap L(B_2)$.
- ❷ **Задача эквивалентности решеток.** Даны две решетки $L(B_1)$ и $L(B_2)$ в \mathbb{Z}^n . Проверить равенство $L(B_1) = L(B_2)$.
- ❸ **Проверка цикличности решетки.** Дана решетка $L(C)$. Проверить, что решетка циклична, т.е. при циклической перестановке ее элементов снова получаются элементы этой же решетки.

О сложности задач CVP и SVP

Теорема

Пусть A — оракул решающий распознавательный вариант задачи CVP. Тогда существует полиномиальный алгоритм с оракулом A для решения задачи поиска для CVP.

Следствие

Три варианта задачи CVP: задача поиска, задача оптимизации и задача распознавания, - полиномиально эквивалентны.

На вход алгоритма подаются решетка $B \in \mathbb{Z}^{n \times m}$ и вектор $\mathbf{t} \in \mathbb{Z}^n$.

Требуется найти вектор $\mathbf{x} = (x_1, \dots, x_m)$, такой что

$\|B\mathbf{x} - \mathbf{t}\| = \min_{\mathbf{y} \in \mathbb{L}(B)} \|\mathbf{t} - \mathbf{y}\| = \mathbf{dist}(\mathbf{t}, L(B))$. Рассмотрим решетку

$B' = [2\mathbf{b}_1, \mathbf{b}_2, \dots, \mathbf{b}_m]$. Выполняется неравенство

$\mathbf{dist}(\mathbf{t}, L(B)) \leq \mathbf{dist}(\mathbf{t}, L(B'))$, поскольку $L(B') \subset L(B)$. Чтобы проверить выполняется ли строгое неравенство, воспользуемся оракулом \mathcal{A} . Без ограничения общности, можно считать, что $\mathbf{t} \in \mathbf{Span}(B)$ (В противном случае рассмотрим вектор $\mathbf{t}' = \mathbf{t} - \pi_B \mathbf{t}$, где $\pi_B \mathbf{t}$ — проекция вектора \mathbf{t} на $\mathbf{Span}(B)$). В этом случае квадрат расстояния от вектора \mathbf{t} до решетки не превосходит величины $R = \|\mathbf{b}_1 - \mathbf{t}\|^2$. Воспользовавшись бинарным поиском и оракулом \mathcal{A} найдем за полиномиальное время такое целое r , для которого выполняются неравенства

$r < \mathbf{dist}(\mathbf{t}, L(B))^2 \leq r + 1$. Обратимся теперь к оракулу \mathcal{A} на входе $(B', \mathbf{t}, \mathbf{ratapp}(\sqrt{r+1}))$, где $\mathbf{ratapp}(\sqrt{r})$ — рациональное число из полуинтервала $(\sqrt{r}, \sqrt{r+1}]$. В случае ответа **NO**, выполняются неравенства

$$\mathbf{dist}(\mathbf{t}, L(B')) > \sqrt{r+1} \geq \mathbf{dist}(\mathbf{t}, L(B)).$$

В случае же ответа **YES** выполняются неравенства

$$\sqrt{r} < \mathbf{dist}(\mathbf{t}, L(B)) \leq \mathbf{dist}(\mathbf{t}, L(B')) \leq \sqrt{r+1}$$

и, следовательно $\mathbf{dist}(\mathbf{t}, L(B)) = \mathbf{dist}(\mathbf{t}, L(B'))$, поскольку $\mathbf{dist}(\mathbf{t}, L(B))^2$ и $\mathbf{dist}(\mathbf{t}, L(B'))^2$ — целые. Заметим теперь, что если для некоторого ближайшего к \mathbf{t} вектора \mathbf{x} координата x_1 четная, то $\mathbf{dist}(\mathbf{t}, L(B)) = \mathbf{dist}(\mathbf{t}, L(B'))$, если же координата x_1 нечетна для всех ближайших векторов \mathbf{x} , то $\mathbf{dist}(\mathbf{t}, L(B)) < \mathbf{dist}(\mathbf{t}, L(B'))$. Поэтому результат сравнения величин $\mathbf{dist}(\mathbf{t}, L(B))$ и $\mathbf{dist}(\mathbf{t}, L(B'))$ позволяет определить четность координаты x_1 для некоторого ближайшего вектора $B\mathbf{x}$. Теперь зная младший бит координаты x_1 для некоторого ближайшего вектора, найдем следующие по значению биты этой координаты с помощью следующей процедуры. Положим $\mathbf{t}' = \mathbf{t} - \varepsilon \mathbf{b}_1$, где $\varepsilon = 0$ для выбора четного бита и $\varepsilon = 1$ в случае выбора нечетного бита. Применяем теперь описанную процедуру для решетки B' и вектора \mathbf{t}' . Отметим, что число требуемых шагов (количество битов координаты x_1 , т.е. оценка модуля коэффициента x_1) оценивается при помощи правила Крамера и полиномиально относительно размера входа (B, \mathbf{t}) . Следовательно, после полиномиального числа итераций координата x_1 будет найдена.

Пусть найдены координаты x_1, \dots, x_k . Заменяем теперь решетку B подрешеткой $[\mathbf{b}_{k+1}, \dots, \mathbf{b}_m]$, а вектор \mathbf{t} вектором $\mathbf{t}' = \mathbf{t} - \sum_{i=1}^k x_i \mathbf{b}_i$ и выполним процедуру для нахождения x_{k+1} . Заметим, что по окончании каждой итерации построена такая последовательность координат x_1, \dots, x_k , для которой существует решение исходной задачи CVP вида $\sum_{i=1}^k x_i \mathbf{b}_i + \mathbf{t}'$ для некоторого $\mathbf{t}' \in L(\mathbf{b}_{k+1}, \dots, \mathbf{b}_m)$. В частности, после m итераций получим решение задачи CVP для входа (B, \mathbf{t}) .

Задача о рюкзаке

Определение

Задача о рюкзаке (The Knapsack problem), задача КР. Заданы $n + 1$ целых чисел $\{a_1, \dots, a_n, s\}$. Найти подмножество $J \subset \{1, \dots, n\}$, для которого $\sum_{i \in J} a_i = s$. Задача распознавания КР заключается в проверке существования такого подмножества J .

Теорема

Задача распознавания КР является NP-полной.

NP-полнота задачи CVP

Теорема

Для всех $p \geq 1$ задача распознавания CVP является NP-полной для любой нормы l_p .

Задача CVP, очевидно, принадлежит классу NP. Достаточно продемонстрировать полиномиальную сводимость распознавательного варианта задачи KP к распознавательному варианту задачи CVP.

Итак, пусть требуется решить задачу KP на входе $\{a_1, \dots, a_n, s\}$. Определим векторы \mathbf{b}_i и \mathbf{t} формулами

$$\mathbf{b}_i = (a_i, \overbrace{0, \dots, 0}^{i-1}, 2, \overbrace{0, \dots, 0}^{n-i})^T$$

и

$$\mathbf{t} = (s, \underbrace{1, \dots, 1}_n)^T.$$

В матричных обозначениях базис B можно выразить в виде

$$B = \begin{pmatrix} \mathbf{a} \\ 2I_n \end{pmatrix},$$

где \mathbf{a} — вектор-строка (a_1, \dots, a_n) .

Сводим теперь задачу КР на входе $\{a_1, \dots, a_n, s\}$ к задаче распознавания для CVP на входе $(B, \mathbf{t}, \sqrt[p]{n})$. Здесь под $\sqrt[p]{n}$ будем понимать любое рациональное число, принадлежащее интервалу $[\sqrt[p]{n}, \sqrt[p]{n+1})$. При $p = +\infty$ подставляем 1 вместо $\sqrt[p]{n}$, поскольку $\lim_{p \rightarrow +\infty} n^{1/p} = 1$.

Докажем правильность такой редукции, т.е. если в задаче распознавания КР на входе (a, s) получаем результат YES, то и на входе $(B, \mathbf{t}, \sqrt[p]{n})$ для задачи CVP получаем результат YES, а если в задаче распознавания КР на входе (a, s) получаем результат NO, то и на входе $(B, \mathbf{t}, \sqrt[p]{n})$ для задачи CVP получаем результат NO. Сначала предположим, что существует решение задачи КР, т.е. при некоторых $x_i \in \{0, 1\}$ выполняется равенство $\sum_{i=1}^n x_i a_i = s$.

Тогда

$$B\mathbf{x} - \mathbf{t} = \begin{pmatrix} \sum_i a_i x_i - s \\ 2x_1 - 1 \\ \vdots \\ 2x_n - 1 \end{pmatrix}$$

и p -я степень l_p -нормы этого вектора равна

$$\|B\mathbf{x} - \mathbf{t}\|^p = \left| \sum_{i=1}^n a_i x_i - s \right|^p + \sum_{i=1}^n |2x_i - 1|^p = n,$$

поскольку $\sum_{i=1}^n x_i a_i - s = 0$ и $2x_i - 1 = \pm 1$ для всех i . Поэтому

расстояние от вектора \mathbf{t} до решетки $L(B)$ не превосходит $\sqrt[p]{n}$ и следовательно результатом задачи распознавания CVP на входе $(B, \mathbf{t}, \sqrt[p]{n})$ будет YES.

Предположим теперь, что результатом задачи распознавания CVP на входе $(B, \mathbf{t}, \sqrt[p]{n})$ будет YES. Следовательно, существует такой целочисленный вектор \mathbf{x} , такой что $\|B\mathbf{x} - \mathbf{t}\| \leq \sqrt[p]{n}$. Тогда

$$\|B\mathbf{x} - \mathbf{t}\|^p = \left| \sum_{i=1}^n a_i x_i - s \right|^p + \sum_{i=1}^n |2x_i - 1|^p,$$

причем для второго слагаемого в правой части равенства

выполняется соотношение $\sum_{i=1}^n |2x_i - 1|^p \geq n$, поскольку все величины

$2x_i - 1$ нечетные. Поэтому соотношение $\|B\mathbf{x} - \mathbf{t}\| \leq \sqrt[p]{n}$ возможно лишь при выполнении соотношения $\sum_{i=1}^n a_i x_i = s$ и $|2x_i - 1|^p = 1$ для

всех i . Таким образом доказано, что $\sum_{i=1}^n a_i x_i = s$ и $x_i \in \{0, 1\}$ для всех i , т.е. \mathbf{x} — решение задачи о рюкзаке.

О сложности задач SVP и CVP

Теперь рассмотрим соотношение между сложностями задач SVP и CVP. Начнем с простой леммы.

Лемма (1.)

Пусть $\mathbf{v} = \sum_{i=1}^n c_i \mathbf{b}_i$ — кратчайший вектор в решетке $\Lambda = L(B)$. Тогда при некотором i коэффициент c_i нечетный.

Доказательство. Пусть $\mathbf{v} = \sum_{i=1}^n c_i \mathbf{b}_i$ — кратчайший вектор в решетке и все коэффициенты c_i четные. Тогда вектор $\frac{1}{2}\mathbf{v} = \sum_{i=1}^n \frac{1}{2}c_i \mathbf{b}_i$ также вектор решетки и его длина вдвое меньше длины вектора \mathbf{v} .

Сведение задачи SVP к задаче CVP

Сведение. По заданному базису $B = (\mathbf{b}_1, \dots, \mathbf{b}_m)$ построим m задач CVP следующим образом. Задача с номером j задается базисом

$$B^{(j)} \stackrel{\text{def}}{=} (\mathbf{b}_1, \dots, \mathbf{b}_{j-1}, 2\mathbf{b}_j, \mathbf{b}_{j+1}, \dots, \mathbf{b}_m)$$

и вектором \mathbf{b}_j . В задаче поиска используем m обращений к оракулу для CVP и из полученных m ответов $\mathbf{v}_i, i = 1, \dots, m$ выбираем такой \mathbf{v}_j , на котором достигается минимум погрешностей $\|\mathbf{v}_i - \mathbf{b}_i\|$. Для задачи распознавания в качестве входа добавляется параметр r и выдается ответ YES, тогда и только тогда, когда хотя бы в одной из задач получен ответ YES.

Леммы

Лемма (2.)

Пусть $\mathbf{v} = \sum_{i=1}^n c_i \mathbf{b}_i$ — вектор в решетке $\Lambda = L(B)$, причем для некоторого j число c_j нечетно. Тогда $\mathbf{u} = \frac{c_j+1}{2}(2\mathbf{b}_j) + \sum_{i \neq j}^n c_i \mathbf{b}_i$ принадлежит решетке $L(B^{(j)})$ и расстояние между \mathbf{u} и \mathbf{b}_j равно длине вектора \mathbf{v} .

Доказательство. Первое утверждение леммы следует из нечетности c_j при некотором j . Второе утверждение следует из равенства

$$\mathbf{u} - \mathbf{b}_j = \frac{c_j + 1}{2} 2\mathbf{b}_j + \sum_{i \neq j}^n c_i \mathbf{b}_i - \mathbf{b}_j = c_j \mathbf{b}_j + \sum_{i \neq j}^n c_i \mathbf{b}_i = \mathbf{v}.$$

Леммы

Лемма (3.)

Пусть $\mathbf{u} = c'_j(2\mathbf{b}_j) + \sum_{i \neq j}^n c_i \mathbf{b}_i$ — вектор в решетке

$\Lambda = L(B^{(j)})$. Тогда $\mathbf{v} = (2c'_j - 1)\mathbf{b}_j + \sum_{i \neq j}^n c_i \mathbf{b}_i$ —

ненулевой вектор решетки $L(B)$ и длина \mathbf{v} равна расстоянию между \mathbf{u} и \mathbf{b}_j .

Доказательство. Первое утверждение леммы следует из нечетности коэффициента $2c'_j - 1$. Второе — из равенства

$$\mathbf{v} = (2c'_j - 1)\mathbf{b}_j + \sum_{i \neq j}^n c_i \mathbf{b}_i = 2c'_j(2\mathbf{b}_j) + \sum_{i \neq j}^n c_i \mathbf{b}_i - \mathbf{b}_j = \mathbf{u} - \mathbf{b}_j.$$

Сводимость

Теорема

Описанная выше процедура **Сводимость** сводит задачу *SVP* к задаче *CVP*.

Докажем теорему в случае задачи распознавания:

$(B, r) \in SVP \Leftrightarrow \exists j : (B^{(j)}, \mathbf{b}_j, r) \in CVP$. Другие случаи разбираются аналогично.

Пусть (B, r) — вход задачи SVP. Ему соответствуют m задач CVP для входов $(B^{(j)}, \mathbf{b}_j, r)$. Докажем, что если на входе (B, r) задачи SVP получен ответ YES, то хотя бы один ответ YES получен в последовательности результатов решения задачи CVP для входов $(B^{(j)}, \mathbf{b}_j, r)$, а если на входе (B, r) задачи SVP получен ответ NO, то ответ NO получен для всех входов $(B^{(j)}, \mathbf{b}_j, r)$ для задачи CVP.

Пусть на входе (B, r) задачи SVP получаем YES и $\mathbf{v} = \sum_{i=1}^n c_i \mathbf{b}_i$ — кратчайший вектор в решетке $L(B)$. Тогда $\|\mathbf{v}\| \leq r$ и согласно лемме 1 при некотором j коэффициент c_j нечетный. Тогда согласно лемме 2 вектор $\mathbf{u} = \frac{c_j+1}{2}(2\mathbf{b}_j) + \sum_{i \neq j} c_i \mathbf{b}_i$ принадлежит решетке $L(B^{(j)})$ и расстояние между $\|\mathbf{u} - \mathbf{b}_j\| = \|\mathbf{v}\| \leq r$, что означает исход YES для запроса оракула на входе $(B^{(j)}, \mathbf{b}_j, r)$.

Предположим теперь, что на входе $(B^{(j)}, \mathbf{b}_j, r)$ задачи CVP получаем YES, т.е. при некотором $\mathbf{u} \in L(B^{(j)})$ выполняется соотношение

$\|\mathbf{u} - \mathbf{b}_j\| \leq r$. Тогда согласно лемме 3 для ненулевого вектора

$\mathbf{v} = (2c'_j - 1)\mathbf{b}_j + \sum_{i \neq j}^n c_i \mathbf{b}_i$ решетки $L(B)$ выполняются соотношения

$\|\mathbf{v}\| = \|\mathbf{u} - \mathbf{b}_j\| \leq r$, что означает исход YES для запроса на входе (B, r) задачи SVP.