

Algorithmen für das CVP

Wir haben in der letzten Vorlesung Gebrauch von einem Algorithmus gemacht, welcher ein CVP mit einem in der Dimension exponentiellen Approximationsfaktor berechnet. Es sollen nun drei solche Approximationsalgorithmen vorgestellt werden.

1. Babai's Round Off Algorithmus
2. Babai's Nearest Plane Algorithmus
3. Das Einbettungsverfahren

Wir kennen schon einen Algorithmus, mit dem wir das CVP exakt ausrechnen können: Den Auszählalgorithmus vom Anfang der Vorlesung. Dieser erlaubt es, alle Gittervektoren in einem gewissen Radius um einen gegebenen Vektor zu bestimmen. Der Aufwand hierfür ist aber im allgemeinen exponentiell in der Dimension (nicht allein nur, weil schon exponentiell viele Vektoren zu berechnen sein könnten).

Sei $\Lambda \subseteq \mathbb{R}^n$ ein Gitter und $a \in \mathbb{R}^n$. Ohne Einschränkung können wir im folgenden annehmen, daß Λ vollständig ist. Das CVP bezüglich Λ und a ist nämlich äquivalent zum CVP bezüglich Λ und der orthogonalen Projektion von a auf $\mathbb{R}\Lambda$, welche sich leicht berechnen läßt.

Mit b_1, \dots, b_n wird eine LLL-reduzierte Basis von Λ bezeichnet. Mit b_1^*, \dots, b_n^* wird die zugehörige Gram-Schmidt orthogonalisierte Basis von $\mathbb{R}\Lambda$ bezeichnet.

Babai's Round Off Algorithmus

Dieser Algorithmus ist sehr leicht zu beschreiben.

1. Schreibe $a = \sum_{i=1}^n \lambda_i b_i$ mit $\lambda_i \in \mathbb{R}$. Dies kann mit linearer Algebra über \mathbb{R} erreicht werden.
2. Setze $v = \sum_{i=1}^n \lceil \lambda_i \rceil b_i$, wobei $\lceil \lambda_i \rceil$ die nächste ganze Zahl aus \mathbb{Z} bezeichnet.

3. Ausgabe von v .

Die Analyse der Qualität von v erfordert eine etwas längere Untersuchung von Eigenschaften LLL-reduzierter Basen, die wir hier auslassen. Das Ergebnis ist das folgende.

1 Satz. *Der durch den Rounding Off Algorithmus und für eine LLL reduzierte Basis b_1, \dots, b_n mit $\delta = 3/4$ erzeugte Vektor $v \in \Lambda$ erfüllt*

$$\|v - a\| \leq (1 + 2n(9/2)^{n/2})\|w - a\|$$

für alle $w \in \Lambda$.

Babai's Nearest Plane Algorithmus

Dieser Algorithmus funktioniert wie folgt.

1. Sei $U = \sum_{i=1}^{n-1} \mathbb{R}b_i$ die Hyperebene und $\Lambda' = \Lambda \cap U$ das zugehörige Gitter.
2. Berechne $u \in \Lambda$, so daß der Abstand zwischen a und $u + U$ minimal wird. Sei $a' \in U$ die orthogonale Projektion von $a - u$ auf U .
3. Finde rekursiv $v' \in \Lambda'$ nahe an a' . Ausgabe von $v = v' + u$.

Im zweiten Schritt wird die an a nächstgelegene Hyperebene bestimmt. Konkret geht man zur Berechnung von u wie folgt vor. Man schreibt $a = \sum_{i=1}^n \lambda_i b_i^*$ mit $\lambda_i \in \mathbb{R}$. Dann können wir wählen $u = \lceil \lambda_n \rceil b_n$ und es gilt $a' = \sum_{i=1}^{n-1} \lambda_i b_i^*$. Man kann sich die Situation gut mit einem Bild klarmachen. Da wir am kürzesten Abstand zu U interessiert, zählt nur, wie wir den Abstand von a zu U durch Addition von $u \in \Lambda$ verringern können. Daher ist klar, daß $u \in \mathbb{Z}b_n$ gewählt werden kann. Der Abstand verändert sich dann aber genau um ganzzahlige Vielfache von $\|b_n^*\|$. Daher wählt man $u = \lceil \lambda_n \rceil b_n$, weil dann der b_n^* -Gram-Schmidt Koeffizient von $a - u$ betragsmäßig kleiner gleich $1/2$ ist.

Die in den nachfolgenden Rechnungen auftretenden Vektoren haben alle b_n^* -Gram-Schmidt Koeffizient Null. Daher gilt zum Schluß für die Gram-Schmidt Koeffizienten $|\langle v, b_i^* \rangle| / \|b_i^*\|^2 \leq 1/2$. Es handelt sich bei diesem Verfahren also um eine Längenreduktion von a bezüglich der b_i . Dies liefert folgende alternative Beschreibung.

1. Längenreduziere a modulo der b_1, \dots, b_n . Dies liefert $a' \in \mathbb{R}\Lambda$ mit $v = a - a' \in \Lambda$.

2. Ausgabe von v .

Hier ist noch eine weitere Formulierung. Fordern wir, daß bei der Längenreduktion die Gram-Schmidt Koeffizienten $> -1/2$ und $\leq 1/2$ sind, so ist a' eindeutig bestimmt und liegt in $P = \{\sum_{i=1}^n \lambda_i b_i^* \mid -1/2 < \lambda_i \leq 1/2\}$. Also gilt $a' = a - v \in P$. Damit erhalten wir die folgende Beschreibung.

1. Finde den eindeutig bestimmten Vektor v in $(a + P) \cap \Lambda$.

2. Ausgabe von v .

2 Satz. *Der durch den Nearest Plane Algorithmus und für eine LLL reduzierte Basis b_1, \dots, b_n mit $\delta = 3/4$ erzeugte Vektor $v \in \Lambda$ erfüllt*

$$\|v - a\| \leq 2^{n/2} \|w - a\|$$

für alle $w \in \Lambda$.

Beweis. Sei $w = \sum_{i=1}^n \rho_i b_i \in \Lambda$ eine optimale Lösung für das CVP bezüglich Λ und a , also $\|w - a\|$ ist minimal. Sei $v = \sum_{i=1}^n \lambda_i b_i \in \Lambda$ die Lösung des Nearest Plane Algorithmus. Mit ρ_i^* und λ_i^* bezeichnen wir die Koeffizienten aus \mathbb{R} von $w - a$ und $v - a$ bezüglich der b_1^*, \dots, b_n^* . Ferner bezeichnen $\rho, \rho^*, \lambda, \lambda^*$ die Spaltenvektoren mit den entsprechenden Koeffizienten $\rho_i, \rho_i^*, \lambda_i, \lambda_i^*$. Für $v = w$ stimmt die Aussage. Wir nehmen daher $v \neq w$ an. Sei s der größte Index, für welchen $\rho_i \neq \lambda_i$ ist.

Als erste Beobachtung halten wir fest: Für alle $i > s$ gilt $\rho_i^* = \lambda_i^*$ und $\rho_s^* - \lambda_s^* \in \mathbb{Z}$. Sei M die Gram-Schmidt Transformationsmatrix mit $(b_1^*, \dots, b_n^*)M = (b_1, \dots, b_n)$. Es folgt aus

$$\begin{aligned} (b_1^*, \dots, b_n^*)M\rho - a &= (b_1^*, \dots, b_n^*)\rho^*, \\ (b_1^*, \dots, b_n^*)M\lambda - a &= (b_1^*, \dots, b_n^*)\lambda^* \end{aligned}$$

durch Subtrahieren und wegen der linearen Unabhängigkeit der b_i^* , daß

$$M(\rho - \lambda) = \rho^* - \lambda^*$$

gilt. Die Beobachtung folgt dann aus der Tatsache, daß M eine obere Dreiecksmatrix mit 1 auf der Diagonalen ist.

Als zweite Beobachtung halten wir fest: $|\rho_s^*| \geq 1/2$. Andernfalls würde gelten $|\rho_s^* - \lambda_s^*| \leq |\rho_s^*| + |\lambda_s^*| < 1/2 + 1/2 = 1$, welches ein Widerspruch zu $\lambda_s^* - \rho_s^* \in \mathbb{Z}$ ist.

Schließlich kommen wir zur Aproximationsfehlertermabschätzung.

$$\begin{aligned}
\|v - a\|^2 &\leq \|(b_1^*, \dots, b_n^*)\lambda^*\|^2 = \sum_{i=1}^n (\lambda_i^*)^2 \|b_i^*\|^2 \\
&= \sum_{i=1}^s (\lambda_i^*)^2 \|b_i^*\|^2 + \sum_{i=s+1}^n (\lambda_i^*)^2 \|b_i^*\|^2 \\
&\leq \sum_{i=1}^s (1/4) 2^{s-i} \|b_s^*\|^2 + \sum_{i=s+1}^n (\lambda_i^*)^2 \|b_i^*\|^2 \\
&= (2^s - 1) \|b_s^*\|^2 / 4 + \sum_{i=s+1}^n (\rho_i^*)^2 \|b_i^*\|^2 \\
&< 2^s \left((\rho_s^*)^2 \|b_s^*\|^2 + \sum_{i=s+1}^n (\rho_i^*)^2 \|b_i^*\|^2 \right) \\
&\leq 2^s \sum_{i=1}^n (\rho_i^*)^2 \|b_i^*\|^2 = 2^s \|(b_1^*, \dots, b_n^*)\rho^*\|^2 \\
&\leq 2^n \|w - a\|^2.
\end{aligned}$$

Die dritte Zeile gilt nach Konstruktion von v und aufgrund der Abschätzungen für LLL Basen. Die vierte Zeile gilt nach der geometrischen Summe und der ersten Beobachtung. Die fünfte Zeile gilt nach der zweiten Beobachtung. Der Rest ist klar. \square

Das Einbettungsverfahren

Das dritte Verfahren ist heuristisch und besitzt im allgemeinen keine Abschätzung des Approximationsterms. Es funktioniert jedoch häufig recht gut, und in geeigneten Fällen kann man sogar Abschätzungen angeben.

Die Methode beruht auf einer einfachen Reduktion vom CVP auf das SVP. Man betrachtet das $n + 1$ dimensionale Gitter $\Lambda' \subseteq \mathbb{R}^{n+1}$, für welches eine Basis wie folgt gegeben ist. An die b_i wird eine Null angehängt, und an a eine 1 oder eine der Situation angepaßte, andere Konstante. Die Erwartung ist, daß ein kurzer Vektor in Λ' von der Form $(v - a, 1)$ ist, wobei $v \in \Lambda$ ein zu a naher Vektor ist, und daß ein kürzester Vektor in Λ' einen zu a nächsten Vektor in Λ ergibt, wenn $\lambda_1(\Lambda)$ größer als $\min_{w \in \Lambda} \|w - a\|$ ist.

Man wendet dann also einfach LLL auf die Basis von Λ' an. Es gibt Beispiele, in denen das Verfahren bewiesenermaßen funktioniert, und es gibt Beispiele, in denen das Verfahren bewiesenermaßen nicht funktioniert.