Primale/duale Segment-Reduktion von Gitterbasen

Henrik Koy

7. Mai 2004

Resultate

1. (k, δ)-primal/dual Segment-reduzierte Basen $\mathbf{b}_1, \ldots, \mathbf{b}_n$:

$$\|\mathbf{b'}_1\|^2 = \lambda_1^2(L(\mathbf{b}_1, \cdots \mathbf{b}_k)) \leq \left(\alpha\gamma_k^2\right)^{\frac{n}{k}-1} \lambda_1^2(L) \quad (1)$$
$$\|\mathbf{b'}^*_1\|^2 = \lambda_1^2(L(\mathbf{b}^*_1, \cdots \mathbf{b}^*_k)) \leq \left(\alpha\gamma_k^2\right)^{\frac{n}{k}-1} \lambda_1^2(L^*) \quad (2)$$

2. Es gibt einen Algorithmus $\mathcal{A}$ der für jede LLL-reduzierte Eingabebasis $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{Z}^n$ nach $\mathcal{O}(n^3 d \log_{\frac{1}{\delta}} 2) + n^3 \cdot k^{\mathcal{O}(k)}$ arithmetischen Schritten eine (k, δ)-primal/dual reduzierte Basis bestimmt.

Grundlagen: Gitter, Gitterbasen

- Ein *Gitter* $L \subseteq \mathbb{R}^d$ ist eine diskrete additive Untergruppe des $\mathbb{R}^d$, mit endlichen *Erzeugendensystem* $\mathbf{b}_1, \ldots, \mathbf{b}_m$:

$$L = L(\mathbf{b}_1, \ldots, \mathbf{b}_m) = \left\{ \sum_{i=1}^{m} t_i \mathbf{b}_i \;\middle|\; t_1, \ldots, t_m \in \mathbb{Z} \right\}.$$

- Jedes minimale Erzeugendensystem $\mathbf{b}_1, \ldots, \mathbf{b}_n$ für das Gitter L heißt *Basis* von L, n heißt *Rang* von L (kurz: $n = \mathrm{rg}(L)$).
- Zwei Gitterbasen $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ und $C = [\mathbf{c}_1, \ldots, \mathbf{c}_n]$ erzeugen das gleiche Gitter L (kurz: $L(B) = L(C)$), genau dann, wenn es eine *unimodulare* Matrix T gibt mit der Eigenschaft $B = CT$.
- Das zu L *duale* Gitter $L^* := \{\mathbf{b}^* \in \mathbb{R}^d \,|\, \forall \mathbf{b} \in \mathbb{R}^d \,:\, \mathbf{b}^* \cdot \mathbf{b}^\top \in \mathbb{Z}\}$. Für $d = rg(L)$ bestimmt man die zu $\mathbf{b}_1, \ldots, \mathbf{b}_n$ *duale Basis* durch das Gleichungssystem $\mathbf{b}_i^* \cdot \mathbf{b}_j^\top = \delta_{i,j}$.

Grundlagen: QR-Zerlegung

- **Definition.** Seien $\mathbb{R}^d$ und $\mathbb{R}^m$ euklidische Vektorräume versehen mit dem Standard Skalarprodukt $\langle \cdot, \cdot \rangle$. Die Gitter $L_1 \subseteq \mathbb{R}^d$ und $L_2 \subseteq \mathbb{R}^m$ heißen *isometrisch*, wenn es eine isometrische Abbildung $Q : \mathbb{R}^d \mapsto \mathbb{R}^m$ mit $Q(L_1) = L_2$ gibt.
- Zur Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ von L_1 ist $\mathbf{c}_1 := Q(\mathbf{b}_1), \ldots, \mathbf{c}_n := Q(\mathbf{b_n})$ eine Basis von L_2 mit der Eigenschaft:

$$\langle \mathbf{b}_i, \mathbf{b}_j \rangle = \langle \mathbf{c}_i, \mathbf{c}_j \rangle, \quad 1 \le i, j \le n.$$

  Die Basen $\mathbf{b}_1, \ldots, \mathbf{b}_n$ und $\mathbf{c}_1, \ldots, \mathbf{c}_n$ heißen *isometrisch*.
- Die *QR-Zerlegung* der Basismatrix $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ bestimmt eine isometrische Basismatrix $R = [\mathbf{r}_1, \ldots, \mathbf{r}_n]$ mit der besonderen Eigenschaft, daß R obere Dreiecksmatrix ist.
  - QR-Zerlegung durch n *Householder-Transformationen*
  - QR-Zerlegung durch $dn - n(n+1)/n$ *Givens-Rotationen*

QR-Zerlegung, orthogonale Projektion $\pi_j(\cdot)$

$$R = \begin{bmatrix} r_{1,1} & r_{1,2} & r_{1,3} & r_{1,4} & r_{1,5} & r_{1,6} & r_{1,7} & r_{1,8} & r_{1,9} & r_{1,10} & r_{1,11} & r_{1,12} \\ & r_{2,2} & r_{2,3} & r_{2,4} & r_{2,5} & r_{2,6} & r_{2,7} & r_{2,8} & r_{2,9} & r_{2,10} & r_{2,11} & r_{2,12} \\ & & r_{3,3} & r_{3,4} & r_{3,5} & r_{3,6} & r_{3,7} & r_{3,8} & r_{3,9} & r_{3,10} & r_{3,11} & r_{3,12} \\ & & & r_{4,4} & r_{4,5} & r_{4,6} & r_{4,7} & r_{4,8} & r_{4,9} & r_{4,10} & r_{4,11} & r_{4,12} \\ & & & & r_{5,5} & r_{5,6} & r_{5,7} & r_{5,8} & r_{5,9} & r_{5,10} & r_{5,11} & r_{5,12} \\ & & & & & r_{6,6} & r_{6,7} & r_{6,8} & r_{6,9} & r_{6,10} & r_{6,11} & r_{6,12} \\ & & & & & & r_{7,7} & r_{7,8} & r_{7,9} & r_{7,10} & r_{7,11} & r_{7,12} \\ & & & & & & & r_{8,8} & r_{8,9} & r_{8,10} & r_{8,11} & r_{8,12} \\ & & & & & & & & r_{9,9} & r_{9,10} & r_{9,11} & r_{9,12} \\ & & & & & & & & & r_{10,10} & r_{10,11} & r_{10,12} \\ & 0 & & & & & & & & & r_{11,11} & r_{11,12} \\ & & & & & & & & & & & r_{12,12} \end{bmatrix}$$

Gitterreduktion: Konstanten und Schranken

- Sukzessive Minima $\lambda_1, \ldots, \lambda_n$ bzgl. der euklidischen Norm $\|\cdot\|$:

  $$\lambda_i = \lambda_i(L) := \min\left\{ \max_{1\le j\le i} \|\mathbf{c}_j\| \,\middle|\, \mathbf{c}_1, \ldots, \mathbf{c}_i \in L \text{ linear unabhängig} \right\}.$$

- Hermite Konstanten γ_n:

  $$\gamma_n := \sup\left\{ \frac{\lambda_1(L)^2}{(\det L)^{\frac{2}{n}}} \;\middle|\; \text{für Gitter mit Rang } n \right\}.$$

  Für die Hermite Konstanten gelten die Abschätzungen

  $$\frac{n}{2e\pi} + o(n) \le \gamma_n \le \frac{n}{e\pi} + o(n).$$

- Betrachte das Gitter L und sein duales Gitter L^* es gilt $\gamma_n \ge \lambda_1(L)/(\det L)^{-2/n}$ und $\gamma_n \ge \lambda_1(L^*)(\det L)^{2/n}$ also:

  $$\gamma_n \ge \lambda_1(L)\lambda_1(L^*).$$

Gitterreduktion: Bekannte Problemstellungen

Wir betrachten nur Gitterprobleme bezüglich der euklidischen Norm:

- Das **Shortest Vector Problem** (**SVP**) Bestimme einen Gittervektor $\mathbf{b} \in L$ mit $\|\mathbf{b}\| = \lambda_1(L)$.
- Das **Closest Vector Problem** (**CVP**) Bestimme zu einen gegebenen Punkt $\mathbf{p} \in \mathbb{R}^d$ einen Gittervektor $\mathbf{b}$, der den Abstand $\|\mathbf{b} - \mathbf{p}\|$ minimiert.
- Das **Shortest Basis Problem** (**SBP**) Bestimme eine Gitterbasis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ für L, die das Produkt $\prod_i \|\mathbf{b}_i\|$ minimiert.

Gitterreduktion: Algorithmen

Betrachte die ganzzahlige Eingabebasis $B = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ mit $M = \max\{\|\mathbf{b}_1\|^2, \ldots, \|\mathbf{b}_n\|^2\}$

- Längenreduktion:
  I.a. keine Reduktion der Größen, Werkzeug für bessere Reduktionsalgorithmen. $\mathcal{O}(n^2 d)$ arithmetische Schritte.
- der LLL-Algorithmus von Lenstra, Lenstra und Lovasz:
  Kürzeste Gittervektor wird bis auf den Faktor $(4/3 + \epsilon)^{n/2}$ approximiert. Laufzeit: $\mathcal{O}(n^4 d \log M)$ arithmetische Schritte.
- geschnittene Aufzählung von Gittervektoren:
  Kürzeste Gittervektor wird bestimmt, bzgl. des Gitterranges n exponentielle Laufzeit.
- (Semi-)Block Korkin-Zolotarev reduzierte Basen nach Schnorr:
  $(1 + \epsilon)^n$ Approximation des kürzesten Gittervektors; für die Semi-Block Korkin-Zolotarev Reduktion polynomielle Laufzeit.

Gitterreduktion: Längenreduktion

$$R = \begin{bmatrix} r_{1,1} & r_{1,2} & r_{1,3} & r_{1,4} & r_{1,5} & r_{1,6} & r_{1,7} & r_{1,8} & & r_{1,7} & r_{1,9} & r_{1,10} & r_{1,11} & r_{1,12} \\ & r_{2,2} & r_{2,3} & r_{2,4} & r_{2,5} & r_{2,6} & r_{2,7} & r_{2,8} & & r_{2,7} & r_{2,9} & r_{2,10} & r_{2,11} & r_{2,12} \\ & & r_{3,3} & r_{3,4} & r_{3,5} & r_{3,6} & r_{3,7} & r_{3,8} & & r_{3,7} & r_{3,9} & r_{3,10} & r_{3,11} & r_{3,12} \\ & & & r_{4,4} & r_{4,5} & r_{4,6} & r_{4,7} & r_{4,8} & - \left\lceil \frac{r_{7,8}}{r_{7,7}} \right\rfloor & r_{4,7} & r_{4,9} & r_{4,10} & r_{4,11} & r_{4,12} \\ & & & & r_{5,5} & r_{5,6} & r_{5,7} & r_{5,8} & & r_{5,7} & r_{5,9} & r_{5,10} & r_{5,11} & r_{5,12} \\ & & & & & r_{6,6} & r_{6,7} & r_{6,8} & & r_{6,7} & r_{6,9} & r_{6,10} & r_{6,11} & r_{6,12} \\ & & & & & & r_{7,7} & r_{7,8} & & r_{7,7} & r_{7,9} & r_{7,10} & r_{7,11} & r_{7,12} \\ & & & & & & 0 & r_{8,8} & & 0 & r_{8,9} & r_{8,10} & r_{8,11} & r_{8,12} \\ & & & & & & & & & & r_{9,9} & r_{9,10} & r_{9,11} & r_{9,12} \\ & & & & & & & & & & & r_{10,10} & r_{10,11} & r_{10,12} \\ & & & & & & & & & & & & r_{11,11} & r_{11,12} \\ & & & & & & & & & & & & & r_{12,12} \end{bmatrix}$$

Gitterreduktion: LLL-Austauschschritt

$$R' = \begin{bmatrix} r_{1,1} & r_{1,2} & r_{1,3} & r_{1,4} & r_{1,5} & r_{1,7} & r_{1,6} & r_{1,8} & r_{1,9} & r_{1,10} & r_{1,11} & r_{1,12} \\ & r_{2,2} & r_{2,3} & r_{2,4} & r_{2,5} & r_{2,7} & r_{2,6} & r_{2,8} & r_{2,9} & r_{2,10} & r_{2,11} & r_{2,12} \\ & & r_{3,3} & r_{3,4} & r_{3,5} & r_{3,7} & r_{3,6} & r_{3,8} & r_{3,9} & r_{3,10} & r_{3,11} & r_{3,12} \\ & & & r_{4,4} & r_{4,5} & r_{4,7} & r_{4,6} & r_{4,8} & r_{4,9} & r_{4,10} & r_{4,11} & r_{4,12} \\ & & & & r_{5,5} & r_{5,7} & r_{5,6} & r_{5,8} & r_{5,9} & r_{5,10} & r_{5,11} & r_{5,12} \\ & & & & 0 & r_{6,7} & r_{6,6} & r_{6,8} & r_{6,9} & r_{6,10} & r_{6,11} & r_{6,12} \\ & & & & & r_{7,7} & 0 & r_{7,8} & r_{7,9} & r_{7,10} & r_{7,11} & r_{7,12} \\ & & & & & & & r_{8,8} & r_{8,9} & r_{8,10} & r_{8,11} & r_{8,12} \\ & & & & & & & & r_{9,9} & r_{9,10} & r_{9,11} & r_{9,12} \\ & & & & & & & & & r_{10,10} & r_{10,11} & r_{10,12} \\ & & & & & & & & & & r_{11,11} & r_{11,12} \\ & & & & & & & & & & & r_{12,12} \end{bmatrix}$$

(l-1, l)

Einteilung der Gitterbasis in Segmenten

Segmente, Segmentreduktion

- Basis in lokalen Koordinaten R_l
- Übertragung von lokalen Basistransformationen $R_l = R_l T$ auf globale Koordinaten
- kürzester Gittervektor in lokalen Koordinaten
- lokale Determinante $\det L(R_l) = \prod_{i=kl-k+1}^{kl} |r_{i,i}|$
- Potentialfunktion

$$D := \prod_{i=1}^{m-1} \prod_{l=1}^{i} D_l, \quad D_l := \det L(R_l)^2 = \prod_{j=kl-k+1}^{kl} r_{j,j}^2.$$

Satz 1. *Sei $R = [\mathbf{r}_1, \ldots, \mathbf{r}_n]$, $n = km$ eine mit δ LLL-reduzierte Eingabebasis. Wenn außerhalb der Segmente nur zwischen $\mathbf{r}_{kl}$ und $\mathbf{r}_{kl+1}$ LLL-Austauschschritte ausgeführt werden, dann ist die Gesamtzahl dieser LLL-Schritte durch $mn^2 \log_{1/\delta} \alpha$ beschränkt.*

Duale Basismatrix $S = (R^{-1})^\top$ von R, Segmente

Segmente in der Dualen Basis

- Die Lokalen Basen S_l und R_l sind dual.
- $\det L(S_l) \cdot \det L(R_l) = 1$
- Für jede Basistransformation $T \in GL_k(\mathbb{Z})$ gilt $S_l T$ und $R_l (T^{-1})^\top$ sind duale Basen.
- Wenn im Segment S_l der Vektor $\mathbf{s}_{kl}$ lokal kürzester Gittervektor ist, dann ist $|r_{kl,kl}|$ maximal.

Bemerkung 2.

$$\begin{aligned} \gamma_k &\geq \lambda_1(L(S_l))^2 \det L(S_l)^{-\frac{2}{k}} = \lambda_1(L(S_l))^2 \det L(R_l)^{\frac{2}{k}} \\ &\geq \lambda_1(L(S_l))^2 \left(\prod_{i=kl-k+1}^{kl} r_{i,i}^2 \right)^{\frac{1}{k}} \end{aligned} \tag{3}$$

(k, δ)-primal/duale Segmentreduktion

Definition. Die Gitterbasis $B = [\mathbf{b}_1, \ldots, \mathbf{b_n}]$, $n = km$ (beachte die R-Matrix der QR-Zerlegung) ist (k, δ)-primal/dual Segment-reduziert mit $\delta \in]\frac{1}{4}, 1]$, wenn für jedes feste $l: \; l = 1, \ldots, m-1$ gilt:

Die längenreduzierten Segmente B_l, B_{l+1} mit den Eigenschaften

1. der Basisvektor $\mathbf{b}_{kl+1}$ ist im Segment B_{l+1} lokal kürzester Gittervektor ($r^2_{kl+1,kl+1}$ ist in R_{l+1} minimal) und
2. der Basisvektor $\mathbf{b}^*_{kl}$ ist im Segment $B^*_l := [\mathbf{b}^*_{kl-k+1}, \ldots, \mathbf{b}^*_{kl}]$ der zu B *dualen* Basis B^* lokal kürzester Basisvektor ($r^2_{kl,kl}$ ist in R_l maximal und $\mathbf{s}_{kl}$ ist in S_l minimal),

erfüllen die LLL-Bedingung: $\delta r^2_{kl,kl} \leq r^2_{kl,kl+1} + r^2_{kl+1,kl+1}$.

(δ, k)-primal/duale Segmentreduktion

Lemma 3. *Für (k, δ)-primal/duale Segment-reduzierte Basen gilt:*

$$\alpha\gamma_k^2 \geq \left(\frac{D_l}{D_{l+1}}\right)^{\frac{1}{k}}.$$

Satz 4. *Sei $\mathbf{b}_1, \ldots, \mathbf{b}_n$, $n = km$ eine (k, δ)-primal/dual segment reduzierte Basis für das Gitter L. Dann Gilt:*

$$\|\mathbf{b'}_1\|^2 = \lambda_1^2(L(\mathbf{b}_1, \cdots \mathbf{b}_k)) \quad \leq \quad \left(\alpha\gamma_k^2\right)^{\frac{n}{k}-1} \lambda_1^2(L) \qquad (4)$$

$$\|\mathbf{b'}^*_1\|^2 = \lambda_1^2(L(\mathbf{b}^*_1, \cdots \mathbf{b}^*_k)) \quad \leq \quad \left(\alpha\gamma_k^2\right)^{\frac{n}{k}-1} \lambda_1^2(L^*) \qquad (5)$$

(k, δ)-primal/duale Segmentreduktion

INPUT: LLL-Reduzierte Basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$, $n = km$, δ, k
OUTPUT: (k, δ)-primal/duale Segment-reduzierte Basis.

1. $l := 1$

2. berechne S_l aus R_l, bestimme in S_l kürzesten Gittervektor $\mathbf{s}$, füge $\mathbf{s}$ in S_l an letzter Stelle ein und eliminiere linear abh. Gittervektor. Speichere Basistransformationen in der Matrix $T \in GL_k(\mathbb{Z})$. $B_l := B_l(T^{-1})^\top$.

3. bestimme in R_{l+1} kürzesten Gittervektor $\mathbf{r}$ und füge $\mathbf{r}$ an erster Position in R_{l+1} ein, eliminiere l. abh. Gittervektor. Übertrage diese Transformationen T': $B_{l+1} := B_{l+1}T'$.

4. **if** $\delta r_{kl,kl}^2 > r_{kl,kl+1}^2 + r_{kl+1,kl+1}^2$ **then**
LLL-Reduziere B_l, B_{l+1}, $l := \max\{1, l-1\}$ **go to 2.**

5. **if** $l < m - 1$ **then** $l := l + 1$ **go to 2.**

Analyse

Wir nehmen an, daß k konstant bleibt.

- Schritt **2.** und **3.** $\mathcal{O}(ndk) + k^{\mathcal{O}(k)}$
- Schritt **4.** $\mathcal{O}(ndk)$
- Nach Satz 1. wird l höchstens $n^2 m \log_{1/\delta} \alpha$ erniedrigt.

Satz 5. Der Bei LLL-Reduzierten Eingabebasen, bestimmt man eine (δ, k)-primal/duale Segmentreduzierte Basis nach $\mathcal{O}(n^3 \cdot d \log_{\frac{1}{\delta}} 2) + n^3 \cdot k^{\mathcal{O}(k)}$ arithmetischen Schritten.

Gitterreduktion: geschnittene Aufzählung

Gegeben die Gitterbasis $\mathbf{r}_1, \ldots, \mathbf{r}_n$, bestimme den kürzesten Gittervektor $r_{\min} \neq 0$.

Sei $r = \sum_{i=1}^{n} t_i \mathbf{r_i}$. Beachte:

$$\mathbf{r} = \sum_{i=1}^{n} t_i \mathbf{r}_i = \sum_{j=1}^{n} \left(\sum_{i=j}^{n} t_i r_{j,i} \right) \mathbf{e}_i \tag{6}$$

$$\|\mathbf{r}\|^2 = \sum_{j=1}^{n} \left(\sum_{i=j}^{n} t_i r_{j,i} \right)^2 \tag{7}$$

$$\|\pi_t(\mathbf{r})\|^{\mathbf{2}} = \sum_{j=t}^{n} \left(\sum_{i=j}^{n} t_i r_{j,i} \right)^2 \tag{8}$$

Gitterreduktion: geschnittene Aufzählung

INPUT: $\mathbf{r}_1, \ldots, \mathbf{r}_n$,
OUTPUT: kürzester Gittervektor $\mathbf{r}_{\hat{\mathbf{u}}}$ (Linearkombination $\hat{\mathbf{u}}$).

1. $\mathbf{u} = \hat{\mathbf{u}} := (1, 0, \ldots, 0)$, $t = \hat{t} := 1$, $\|r_{\hat{\mathbf{u}}}\|^2 := \|\mathbf{r}_1\|^2$
2. $\|\pi_t(r_{\mathbf{u}})\|^2 = \sum_{j=t}^{n} \left(\sum_{i=j}^{n} u_i r_{j,i} \right)^2 = \|\pi_{t+1}(r_{\mathbf{u}})\|^2 + (\sum_{i=t}^{n} u_i r_{j,i})^2$
3. **if** $\|\pi_t(r_{\mathbf{u}})\|^2 \geq \|r_{\hat{\mathbf{u}}}\|^2$ **then**
   $t = t + 1$, wähle für u_t die "nächst-mögliche" Kombination
   else
   $t = t - 1$, starte die Aufzählungsreihenfolge für u_t.
4. **if** $t = 0$ **then** $\hat{\mathbf{u}} = \mathbf{u}$, $\|r_{\hat{\mathbf{u}}}\|^2 = \|r_{\mathbf{u}}\|^2$, $t = 1$.
5. **if** $t \leq n$ **then go to 2.**

Gitterreduktion: geschnittene Aufzählung Laufzeitanalyse

Sei Ω die Liste aller Kandidaten $\mathbf{u} = (u_1, \ldots, u_n)$ für den kürzesten Gittervektor $\mathbf{r} = \sum_{i=1}^{n} \hat{u}_i \mathbf{r}_i$.

$$
\begin{aligned}
|\Omega| &\leq \prod_{i=1}^{n} (1 + 2\|\mathbf{r_1}\|/\pi_i(\mathbf{r}_i)) && (9)\\
&\leq 3^n \prod_{i=1}^{n} (\|\mathbf{r_1}\|/|r_{i,i}|) && (10)\\
&= 3^n \frac{\|\mathbf{r}_1\|^n}{\det(L)} = 3^n \left(\frac{\|\mathbf{r}_1\|^2}{\det(L)^{2/n}} \right)^{\frac{n}{2}} . && (11)
\end{aligned}
$$

$T_{\mathrm{ENUM}}(L) = \mathcal{O}(|\Omega| P(n))$ arithmetische Schritte.