Universidade Estadual de Campinas - UNICAMP

Projeções de Reticulados Gerais

Eleonesio Strey

05 de Dezembro de 2014

1 Definições e resultados preliminares

Sejam $m \leqslant n$ vetores linearmente independentes $g_1, ..., g_m \in \mathbb{R}^n$. Um *reticulado* $\Lambda \in \mathbb{R}^n$ com base $\{g_1, ..., g_m\}$ é o conjunto formado por todas as combinações lineares inteiras de g_i, $i = 1, ..., m$, isto é,

$$\Lambda = \{\alpha_1 g_1 + \cdots + \alpha_m g_m; \alpha_1, ..., \alpha_m \in \mathbb{Z}\}.$$

O conjunto $\{g_1, ..., g_m\}$ é denominado uma base de Λ. A matriz G cujas linhas são os vetores $g_1, ..., g_m$ é chamada de *matriz geradora* de Λ. A matriz $A = GG^t$ é chamada de *matriz de Gram* de Λ e o número $\det \Lambda = \det GG^t$ é dito *determinante* ou *discriminante* de Λ. Duas matrizes G e $\hat{G}$ geram o mesmo reticulado se existir uma matriz unimodular U tal que $G = U\hat{G}$. Um reticulado tem um número infinito de bases, mas o valor de $\det \Lambda$ é invariante sob mudança de base. Dizemos que um conjunto de vetores $\{v_1, ..., v_k\} \subset \Lambda$ é *primitivo* se existirem vetores $\{v_{k+1}, ..., v_m\} \subset \Lambda$ tais que $\{v_1, ..., v_k, v_{k+1}, ..., v_m\}$ é uma base de Λ. Se $v_i = a_i G, a_i \in \mathbb{Z}^m$, então uma condição necessária e suficiente para que um conjunto de vetores seja primitivo é que o mdc dos menores $k \times k$ da matriz $[a_1^t \ a_2^t \ ... \ a_k^t]$ sejam iguais a ± 1.

Sejam G_1 e G_2 matrizes geradoras dos reticulados Λ_1 e Λ_2 respectivamente. Dizemos que os reticulados são *equivalentes* se, e somente se, a seguinte relação é satisfeita $G_1 = cUG_2Q$, onde $c \in \mathbb{R}$, $c > 0$, Q é uma matriz ortogonal $m \times m$ e U é uma matriz unimodular (determinante igual a ± 1 com entradas inteiras).

Definimos o reticulado dual de $\Lambda = \Lambda(G)$ da seguinte forma

$$\Lambda^* = \{x \in span(G); \langle x, y\rangle \in \mathbb{Z}, \forall y \in \Lambda\},$$

onde $span(G) = \{xG; x \in \mathbb{R}^m\}$. Se G é uma matriz geradora de Λ, então $(GG^t)^{-1}G$ é uma matriz geradora de Λ^* e $\det \Lambda = (\det \Lambda^*)^{-1}$.

Dado $\epsilon > 0$, dizemos que Λ_1 está na ϵ-vizinhança de Λ_2 (com respeito à matriz de Gram A_1 para Λ_1) quando existe uma matriz de Gram A_2 para Λ_2 tal que $\|A_1 - A_2\| \leqslant \epsilon$. Dizemos também que uma sequência de reticulados Λ_ω ($\omega = 1, 2, ...$) converge para Λ, a menos de equivalência, se dado $\epsilon > 0$ arbtrário, existe ω_0 tal que $c_\omega \Lambda_\omega$ está na ϵ-vizinhança de Λ para algum fator de escala c_ω (possivelmente dependendo de ω) sempre que $\omega > \omega_0$. Escrevemos, simplesmente, $\Lambda_\omega \to \Lambda$ para indicar que Λ_ω converge para Λ.

Observação 1.1. *Se $\Lambda_\omega \to \Lambda$, então $\Lambda_\omega^* \to \Lambda^*$. Com efeito, seja A_ω uma sequência de matrizes de Gram para Λ_ω tal que $c_\omega A_\omega \to A$. Como A_ω é não singular, temos que a sua inversa existe, e vale que $(1/c_\omega)A_\omega^{-1} \to A^{-1}$, ou seja, $\Lambda_\omega^* \to \Lambda^*$.*

2 Projeções de Reticulados Gerais

Seja V uma matriz de ordem $k \times n$, $k < n$, de posto completo. Denotamos por $span(V)^\perp$ o complemento ortogonal do espaço vetorial gerado pelas linhas de V , isto é,

$$span(V)^\perp = \{x \in \mathbb{R}^n; \langle x, y\rangle = 0 \ \ \forall y \in span(V)\}$$

Todo vetor $x \in \mathbb{R}^n$ pode ser escrito de forma única como $x = v + v^\perp$, onde $v \in span(V)$ e $v^\perp \in span(V)^\perp$. Dado $x \in \mathbb{R}^n$, definimos a projeção ortogonal de x em $span(V)^\perp$ pondo $P_{v^\perp}(x) = v^\perp$. Daí, segue que $P_{v^\perp}(x) = xP$, onde $P = I_n - V^t(VV^t)^{-1}V$. De fato, para cada $x \in \mathbb{R}^n$, existem vetores $u \in \mathbb{R}^k$ e $v^\perp \in span(V)^\perp$ tais que $x = uV + v^\perp$ e logo

$$xP = (uV + v^\perp)P = uV(I_n - V^t(VV^t)^{-1}V) + v^\perp(I_n - V^t(VV^t)^{-1}V) = 0 + v^\perp = P_{v^\perp}(x).$$

Lema 2.1. *Seja V uma matriz de ordem $k \times n$ cujas linhas formam um conjunto primitivo de vetores de um reticulado $\Lambda \subset \mathbb{R}^n$. Valem as seguintes propriedades*

(i) O conjunto $P_{v^\perp}(\Lambda)$ é um reticulado.

(ii) O discriminante de $P_{v^\perp}(\Lambda)$ é dado por $\det P_{V^\perp}(\Lambda) = \dfrac{\det \Lambda}{\det(VV^t)}$.

Demonstração. (i) Como as linhas de V são um conjunto primitivo, existe uma matriz $\tilde{V}$ de ordem $(n-k) \times n$ e posto completo tal que

$$\hat{V} = \begin{bmatrix} V \\ \tilde{V} \end{bmatrix}$$

é uma matriz geradora de Λ e qualquer elemento $x \in \Lambda$ pode ser escrito como $x = u\hat{V}$, $u \in \mathbb{Z}^n$. Projetando $x \in \Lambda$ em $span(V)^\perp$, temos

$$xP = u\hat{V}P = u \begin{bmatrix} 0 \\ \tilde{V}P \end{bmatrix}.$$

Logo as linhas de $\tilde{V}P$ formam um conjunto cujas combinações inteiras geram $P_{v^\perp}(\Lambda)$. Para concluir a demonstração, resta mostrar que $\tilde{V}P$ tem posto completo. Com efeito, observe que as linhas de $\tilde{V}P$ são LI, uma vez que

$$x\tilde{V}P = 0 \implies x\tilde{V} \in span(V) \implies x\tilde{V} = yV \text{ para algum } y \in \mathbb{Z}^k \implies x = y = 0 \text{ pois as linhas de } \hat{V} \text{ são LI.}$$

(ii) Da demonstração de (i), temos que $\hat{V}$ é uma matriz geradora para Λ. Daí segue que

$$\begin{aligned} \det \Lambda &= \det \hat{V}\hat{V}^t = \det \begin{bmatrix} VV^t & V\tilde{V}^t \\ \tilde{V}V^t & \tilde{V}^t\tilde{V}^t \end{bmatrix} = \det \begin{bmatrix} VV^t & V\tilde{V}^t \\ 0 & \tilde{V}^t\tilde{V}^t - \tilde{V}V^t(VV^t)^{-1}V\tilde{V}^t \end{bmatrix} \\ &= \det(VV^t)\det(\tilde{V}^t\tilde{V}^t - \tilde{V}V^t(VV^t)^{-1}V\tilde{V}^t) = \det(VV^t)\det(\tilde{V}P\tilde{V}^t) = \det(VV^t)\det P_{V^\perp}(\Lambda). \end{aligned}$$

□

Observação 2.2. $P_{v^\perp}(\Lambda)$ *nem sempre é um reticulado* (*ver página 57 de* [2]).

Todo reticulado de posto completo é equivalente a um reticulado gerado por uma matriz triangular superior. Com efeito, seja Λ um reticulado gerado por uma matriz $G \in \mathbb{R}^{n\times n}$ de posto completo. Escrevendo

$$G = \begin{bmatrix} g_1 \\ \vdots \\ g_n \end{bmatrix}$$

e aplicando o processo de Gram-Schmidt no conjunto $\{g_n, g_{n-1}, ..., g_1\}$ (que é linearmente independente, pois G tem posto completo), obtemos um conjunto de vetores $\{q_n, q_{n-1}, ..., q_1\}$ dois a dois ortonormais tais que

$$\begin{gathered} g_n \in span\{q_n\} \\ g_{n-1} \in span\{q_n, q_{n-1}\} \\ \vdots \\ g_1 \in span\{q_n, q_{n-1}, ..., q_1\}. \end{gathered}$$

Daí segue que existem números reais r_{ij}, $1 \leqslant i \leqslant j \leqslant n$, tais que

$$G = \begin{bmatrix} g_1 \\ \vdots \\ g_n \end{bmatrix} = \begin{bmatrix} r_{11} & \cdots & r_{1n} \\ & \ddots & \vdots \\ & & r_{nn} \end{bmatrix} \begin{bmatrix} q_1 \\ \vdots \\ q_n \end{bmatrix}.$$

Logo $G = RQ$, onde $R \in \mathbb{R}^{n\times n}$ é uma matriz triangular superior e $Q \in \mathbb{R}^{n\times n}$ é uma matriz ortogonal. Isto mostra que os reticulados gerados por G e R são equivalentes. Portanto podemos assumir, sem perda de generalidade, que Λ possui matriz geradora G triangular superior e, por conveniência, escreveremos a matriz G da seguinte forma:

$$G = \begin{bmatrix} G_1 & G_2 \\ 0 & G_3 \end{bmatrix}, \tag{1}$$

onde G_1 e G_3 são matrizes quadradas triangulares superiores de ordem $k\times k$ e $(n-k)\times(n-k)$, respectivamente.

Agora, considerando $A = [I \ \ \hat{A}] \in \mathbb{Z}^{k\times n}$, $V = AG = [G_1 \ \ \hat{V}]$ (logo $\hat{V} = G_2 + \hat{A}G_3$) e $M = [-G_3^{-t}\hat{V}^tG_1^{-t} \ \ G_3^{-t}]$ temos o seguinte lema:

Lema 2.3. *Considere as matrizes* G, V *e* M *descritas acima. Se* $\Lambda = \Lambda(G)$ *e* $P_{V^\perp}(\Lambda)$ *é a projeção de* Λ *sobre* $span(V)^\perp$*, então*

$$\Lambda(M) = \Lambda^* \cap span(V)^\perp = P_{V^\perp}(\Lambda)^*.$$

Demonstração. Primeiramente vamos provar a inclusão $\Lambda(M) \subseteq \Lambda^* \cap span(V)^\perp$. Seja $x \in \Lambda(M)$, isto é, $x = uM$ para algum $u \in \mathbb{Z}^{n-k}$. Observe que

$$xV^t = uMV^t = u\begin{bmatrix} -G_3^{-t}\hat{V}^t G_1^{-t} & G_3^{-t} \end{bmatrix}\begin{bmatrix} G_1^t \\ \hat{V}^t \end{bmatrix} = u\begin{bmatrix} -G_3^{-t}\hat{V}^t G_1^{-t} G_1 + G_3^{-t}\hat{V}^t \end{bmatrix} = u[0] = 0.$$

Logo $x \in span(V)^\perp$. Observe também que para qualquer $y \in \Lambda$, isto é, $y=\omega G$ com $\omega \in \mathbb{Z}^n$, temos

$$\langle x, y\rangle = yx^t = \omega G M^t u^t = \omega \begin{bmatrix} G_1 & G_2 \\ 0 & G_3 \end{bmatrix}\begin{bmatrix} -G_1^{-1}\hat{V}G_3^{-1} \\ G_3^{-1} \end{bmatrix} u^t = \omega \begin{bmatrix} -\hat{V}G_3^{-1} + G_2 G_3^{-1} \\ I_{n-k} \end{bmatrix} u^t = \omega \begin{bmatrix} -\hat{A} \\ I_{n-k} \end{bmatrix} u^t$$

Como todas as entradas das matrizes ω, $\begin{bmatrix} -\hat{A}^t & I_{n-k} \end{bmatrix}^t$ e u^t são inteiras, segue que $\langle x, y\rangle \in \mathbb{Z}$. Logo $x \in \Lambda^*$. Isto finaliza a prova da inclusão.

Agora, vamos mostrar que $\Lambda^* \cap span(V)^\perp \subseteq P_{V^\perp}(\Lambda)^*$. Seja $x \in \Lambda^* \cap span(V)^\perp$ e seja P a projeção sobre $span(V)^\perp$. Cada elemento em $P_{V^\perp}(\Lambda)$ é da forma uP com $u \in \Lambda$. Daí, temos

$$\langle x, uP\rangle = uPx^t = uP^t x^t = u(xP)^t = ux^t \in \mathbb{Z},$$

uma vez que $span(V)^\perp$, $u \in \Lambda$ e $x \in \Lambda^*$. Até agora, temos $\Lambda(M) \subseteq \Lambda^* \cap span(V)^\perp \subseteq P_{V^\perp}(\Lambda)^*$.

Para mostrar que essas inclusões são de fato igualdades, basta mostrar que $\Lambda(M)$ e $P_{V^\perp}(\Lambda)^*$ possuem o mesmo determinante. Com efeito,

$$\begin{aligned}
\det \Lambda(M) &= \det MM^t = \det[-G_3^{-t}\hat{V}^t G_1^{-t} \quad G_3^{-t}]\begin{bmatrix} -G_1^{-1}\hat{V}G_3^{-1} \\ G_3^{-1} \end{bmatrix} \\
&= \det(G_3^{-t}\hat{V}^t G_1^{-t} G_1^{-1}\hat{V}G_3^{-1} + G_3^{-t}G_3^{-1}) \\
&= \det(G_3^{-t}G_3^{-1})\det(\hat{V}^t G_1^{-t}G_1^{-1}\hat{V} + I) \\
&= \det(G_3^{-t}G_3^{-1})\det(G_1^{-1}\hat{V}\hat{V}^t G_1^{-t} + I) \\
&= \det(G_3^{-t}G_3^{-1})\det(G_1^{-t}G_1^{-1})\det(\hat{V}\hat{V}^t + G_1 G_1^t) \\
&= \frac{\det(\hat{V}\hat{V}^t + G_1 G_1^t)}{\det(G_3 G_3^t)\det(G_1 G_1^t)} = \frac{\det(VV^t)}{\det(\Lambda)}.
\end{aligned}$$

□

Teorema 2.4. . *Sejam* Λ_1 *e* Λ_2 *reticulados de posto* n *e* $n-k$*, respectivamente. Existe uma sequência de matrizes* V_ω *cujas linhas formam um conjunto primitivo de vetores de* Λ_1 *tal que* $P_{V_\omega^\perp}(\Lambda_1) \to \Lambda_2$*, quando* $\omega \to \infty$

Demonstração. Basta construir sequências de duais de projeções de Λ_1 que convergem, a menos de equivalência, para o dual de Λ_2 (ver observação 1.1). Com efeito, considere uma representação de Λ_2, cujo dual possui uma matriz geradora L^* triangular inferior de ordem $(n-k)\times(n-k)$. Seja Λ_1 o reticulado com matriz geradora na forma (1). Considere a matriz

$$\overline{L}^* = [L^* \quad 0],$$

onde 0 é de ordem $(n-k)\times k$. Consideramos também uma outra decomposição de $\overline{L}^*$, da forma

$$\overline{L}^* = [\overline{L}_1^* \quad \overline{L}_2^*],$$

onde $\overline{L}_1^*$ e $\overline{L}_2^*$ possuem ordem $(n-k)\times k$ e $(n-k)\times(n-k)$, respectivamente. Observe que $\overline{L}^*$ e $\overline{L}_1^*$ possuem o mesmo número de linhas, $n-k$, correspondente ao posto do reticulado Λ_2. Para cada $\omega \in \mathbb{N}\setminus\{0\}$, definimos as seguintes matrizes

$$H_\omega = \left\lfloor \omega \overline{L}_2^* G_3^t \right\rfloor + I_{n-k},$$

$$(L_\omega^*)_1 = \left(\left\lfloor \omega \overline{L}_1^* G_1^t + H_\omega G_3^{-t} G_2^t \right\rfloor - H_\omega G_3^{-t} G_2^t \right) G_1^{-t},$$

$$(L_\omega^*)_2 = H_\omega G_3^{-t} \text{ e}$$

$L^*_\omega = \left[(L^*_\omega)_1 \;\; (L^*_\omega)_2\right]$.

Seja a sequência $\Lambda^*_\omega = \Lambda(L^*_\omega)$. No que segue, provaremos:

(i) Λ^*_ω é equivalente a $P_{V^\perp_\omega}(\Lambda_1)^*$ para alguma matriz V_ω cujas linhas são um conjunto primitivo de Λ_1.

(ii) Λ^*_ω converge, a menos de equivalência, para Λ^*_2.

Para provar a primeira afirmação, observamos que, como L^* e G_3^t são matrizes triangulares inferiores e as entradas da diagonal de L^*_2 são nulas, H_ω é uma matriz triangular inferior com todos os elementos da diagonal iguais a 1. Logo H_ω é unimodular, assim como H_ω^{-1}. Portanto, para cada $\omega \in \mathbb{N} \setminus \{0\}$, Λ^*_ω é também gerado pela matriz $H_\omega^{-1}L^*_\omega$. Desenvolvendo o produto matricial, temos

$$\begin{aligned} H_\omega^{-1}L^*_\omega &= \left[H_\omega^{-1}(L^*_\omega)_1 \quad G_3^{-t}\right] \\ &= \left[(H_\omega^{-1}\left\lfloor \omega\overline{L}_1^* G_1^t + H_\omega G_3^{-t} G_2^t \right\rfloor - G_3^{-t}G_2^t)G_1^{-t} \quad G_3^{-t}\right] \\ &= \left[-\hat{A}^t G_1^{-t} - G_3^{-t}G_2^t G_1^{-t} \quad G_3^{-t}\right] \\ &= \left[-G_3^{-t}\hat{V}^t G_1^{-t} \;\; G_3^{-t}\right], \end{aligned}$$

onde $\hat{A}^t = -H_\omega^{-1}\left\lfloor \omega\overline{L}_1^* G_1^t + H_\omega G_3^{-t}G_2^t \right\rfloor$ é uma matriz inteira de ordem $(n-k)\times k$ e $\hat{V}^t = G_2^t + G_3^t\hat{A}^t$. Comparando estes resultados com o lema 2.3 concluímos (i) com V_ω dado por

$$V_\omega = \left[G_1 \quad G_2 - \left(H_\omega^{-1}\left\lfloor \omega\overline{L}_1^* G_1^t + H_\omega G_3^{-t}G_2^t \right\rfloor\right)^t G_3\right].$$

Para demonstrar (ii), começamos com as seguintes desigualdades simples sobre a operação chão

$$\frac{1}{\omega}\left(\left\lfloor \omega\overline{L}_1^* G_1^t + H_\omega G_3^{-t}G_2^t \right\rfloor - H_\omega G_3^{-t}G_2^t\right)_{ij} \geqslant (L_1^* G_1^t)_{ij} - \frac{1}{\omega}$$

$$\frac{1}{\omega}\left(\left\lfloor \omega\overline{L}_1^* G_1^t + H_\omega G_3^{-t}G_2^t \right\rfloor - H_\omega G_3^{-t}G_2^t\right)_{ij} \leqslant (L_1^* G_1^t)_{ij}$$

Daí, obtemos

$$\frac{1}{\omega}\left(\left\lfloor \omega\overline{L}_1^* G_1^t + H_\omega G_3^{-t}G_2^t \right\rfloor\right)_{ij} \longrightarrow (L_1^* G_1^t)_{ij} \text{ quando } \omega \longrightarrow \infty,$$

e portanto $(L^*_\omega)_1/\omega \to \overline{L}_1^*$. Analogamente, é possível provar que $(L^*_\omega)_2/\omega \to \overline{L}_2^*$. Dessa maneira,

$$\frac{L^*_\omega}{\omega} \longrightarrow [L^* \;\; 0] \quad \Longrightarrow \quad \frac{L^*_\omega L^{*\,t}_\omega}{w^2} \longrightarrow L^* L^{*t} \text{ quando } \omega \longrightarrow \infty.$$

Concluindo a demonstração.

Referências

[1] A. Campello, J. Strapasson, S.I.R. Costa, *On projections of arbitrary lattices*. 2013.

[2] A. Campello, *Reticulados, Projeções e Aplicações à Teoria da Informação*. 2014.

□