MT803D - Tópicos em Matemática Aplicada

Formas Quadráticas e Redução de Base

1 Introdução

O problema de encontrar o primeiro mínimo de um reticulado $\Lambda \subset \mathbb{R}^n$ com relação a um corpo convexo K é computacionalmente bastante difícil (na linguagem de complexidade computacional, ele está, sob certas hipóteses, na classe de problemas NP-difícil). Quando $K = B_2(1) \subset \mathbb{R}^n$, este problema está associado a uma fórma quadrática de maneira bastante natural. Daqui para frente omitiremos o índice K no primeiro mínimo, e consideraremos apenas $K = B_2(1) \subset \mathbb{R}^n$, denotando assim:

$$\lambda_1(\Lambda) = \max_{\boldsymbol{x} \in \Lambda \setminus \{\mathbf{0}\}} \|\boldsymbol{x}\|_2 . \tag{1}$$

Exemplo 1. *Considere o reticulado hexagonal Λ gerado pela matriz*

$$A = \begin{pmatrix} 1 & 1/2 \\ 0 & \sqrt{3}/2 \end{pmatrix}.$$

Qualquer ponto de A é da forma

$$A\boldsymbol{u} = \begin{pmatrix} u_1 + u_2/2 \\ \sqrt{3}/2 u_2 \end{pmatrix},$$

assim $\|A\boldsymbol{u}\|^2 = u_1^2 + u_1 u_2 + u_2^2$. Vemos facilmente que, para quaisquer números $u_1, u_2 \in \mathbb{Z}$, com algum deles não nulo, $\|A\boldsymbol{u}\|^2 \geq 1$ e, além disso, o valor 1 é atingível (por exemplo, por $(1, 0)$). Assim $\lambda_1(\Lambda) = 1$. Entretanto, se considerarmos a matriz geradora alternativa para Λ

$$A' = \begin{pmatrix} 2401 & \frac{57649}{2} \\ 96\sqrt{3} & \frac{2305\sqrt{3}}{2} \end{pmatrix},$$

está longe de ser trivial observar que mínimo de

$$\|A'\boldsymbol{u}\|^2 = 5792449u_1^2 + 139079089u_2u_1 + 834836569u_2^2$$

seja igual a 1 (atingido pelo vetor $(u_1, u_2) = (2305, -192)$).

Vimos no exemplo acima que para encontrar λ_1, necessitamos estudar o polinômio em duas variáveis $u_1 + u_1u_2 + u_2$. De uma maneira geral, um reticulado está associado a uma forma quadrática.

2 Formas Quadráticas

Seja $M \in \mathbb{R}^{n\times n}$ uma matriz simétrica definida positiva. A *forma quadrática* associada a M é a função

$$q_M : \mathbb{R}^n \to [0, \infty)$$

$$q_M(\boldsymbol{x}) = \boldsymbol{x}^t M \boldsymbol{x}.$$

Observe que $q_M(\boldsymbol{x})$ define, de maneira natural, um produto inteiro em $\mathbb{R}^n$, se a estendermos a uma forma bilinear do tipo $\boldsymbol{x}^t M \boldsymbol{y}$. Assim, q_M satisfaz as propriedades $q_M(\boldsymbol{x}) > 0$ para $\boldsymbol{x} \neq 0$ e $q_M(\alpha\boldsymbol{x}) = \alpha^2 q_M(\boldsymbol{x})$.

Para qualquer forma quadrática q_M, existe uma matriz diagonal D tal que a imagem de q_M é igual à imagem de M (o que pode ser visto, por exemplo, pela decomposição em auto-valores de D). Note que $f(\boldsymbol{x}) = \sqrt{q_M(\boldsymbol{x})}$ é a função de *gauge* do elipsoide

$$E = \left\{\boldsymbol{x} : \boldsymbol{x}^t M \boldsymbol{x} \leq 1\right\},$$

cujo volume é vol $E = \sqrt{\det M} V_{n,2}$, em que $V_{n,2}$ é o volume da esfera euclidiana em $\mathbb{R}^n$.

Dado um reticulado Λ com matriz geradora A, e tome $M = A^t A$. A forma quadrática associada à base A de Λ (ou, simplificadamente, a $\Lambda(A)$) é dada por $q_M(\boldsymbol{x}) = \boldsymbol{x}^t A^t A \boldsymbol{x} = \|A\boldsymbol{x}\|^2$. Note que a forma quadrática *não é* um invariante do reticulado. Entretanto, existe uma noção de equivalência entre essas formas. Duas formas quadráticas q_{M_1} e Q_{M_2} são ditas *aritmeticamente equivalentes* se $M_1 = U^t M_2 U$, em que $U \in \mathrm{Gl}_n(\mathbb{Z})$. Isso implica que a imagem de q_{M_1} é igual à imagem de q_{M_2}. Temos assim:

Proposição 2.1. *Formas quadráticas associadas a diferentes matrizes geradoras de um reticulado Λ são aritmeticamente equivalentes.*

Por outro lado, dado duas matrizes A e B tais que $B = QA$, em que $Q \in \mathbb{R}^{n\times n}$ é uma matriz ortogonal (isto é, $Q^t Q = I$), temos $q_{A^t A}(\boldsymbol{x}) = q_{B^t B}(\boldsymbol{x})$, assim as formas quadráticas são iguais. Deste modo, transformações ortogonais não afetam o estudo de formas quadráticas. Diremos portanto que dois reticulados $\Lambda(A)$ e $\Lambda(B)$ são *congruentes* se existe $U \in \mathrm{Gl}_n(\mathbb{Z})$, $Q \in \mathbb{R}^{n\times n}$ ortogonal, tais que $A = QBU$. Um pouco de Álgebra Linear nos mostra que

Proposição 2.2. *As formas quadráticas associadas a $\Lambda(A)$ e $\Lambda(B)$ são aritmeticamente equivalentes se, e somente se, os reticulados são congruentes.*

Assim, a congruência de reticulados é uma relação de equivalência entre formas quadráticas.

2.1 (Formas Quadráticas Universais)

Aqui vale um parênteses para um tema que foge ao escopo deste curso (e cujo entendimento das demonstrações está fora do escopo da Geometria dos Números). Demonstramos na aula passada que todo inteiro pode ser representado como a soma de quatro quadrados. Desde modo, a forma imagem de $\mathbb{Z}^4$ pela forma quadrática $q_{I_4}(\boldsymbol{x})$, em que I_4 é a matriz identidade 4×4, resulta no conjunto $\mathbb{N}$. Foi Gauss em seu *Disquisitiones Arithmeticae* quem primeiro estudou outras formas quadráticas cuja imagem é o conjunto de inteiros $\mathbb{N}$.

De maneira geral, seja $q_M(\boldsymbol{x})$ uma forma quadrática. Dizemos que $q_M(\boldsymbol{x})$ é *universal* se $q_M(\mathbb{Z}^n) = \mathbb{N}$ ou, em outras palavras, se todo inteiro pode ser representado por q_M. Se $M \in \mathbb{Z}^{n\times n}$ dizemos que a forma é *clássica* (ou inteira). Se $q_M(\boldsymbol{x})$, vista como um polinômio, possui todos os coeficientes inteiros, dizemos que $q_M(\boldsymbol{x})$ é *integral*. Note que as duas definições não são equivalentes. Por exemplo, a forma

$$q_M(\boldsymbol{x}) = x_1^2 + x_1x_2 + x_2^2 = (x_1\ x_2) \begin{pmatrix} 1 & 1/2 \\ 1/2 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

é integral, mas não é inteira. Em [P. 12], Clark et. al apresentam resultados sobre formas quadráticas derivados utilizando métodos de Geometria dos Números. Os dois teoremas essecialmente resolvem a questão de determinais quais formas quadráticas são universais.

Teorema 1 (Teorema 15 [Bha00])**.** *Uma forma quadrática clássica que representa todos os números inteiros de* 1 *a* 15 *é universal.*

Teorema 2 (Teorema 290 [Bha11])**.** *Uma forma quadrática integral que representa todos os números inteiros de* 1 *a* 290 *é universal.*

Os Teoremas de Minkowski para Corpos Convexos não são suficientes para lidar com formas quadráticas universais, de uma maneira geral.

3 Redução de Base

Voltemos ao problema de encontrar $\lambda_1(\Lambda)$, ou $\sqrt{\min_{\boldsymbol{x}\neq 0} q_{A^tA}(\boldsymbol{x})}$.

3.1 Caso 2-dimensional

Seja $\{\boldsymbol{a}_1, \boldsymbol{a}_2\}$ uma base para um reticulado Λ. Dizemos que esta base é *Minkowski-reduzida* se as seguintes condições são válidas

$$\begin{aligned} \langle \boldsymbol{a}_1, \boldsymbol{a}_1 \rangle \leq \langle \boldsymbol{a}_2, \boldsymbol{a}_2 \rangle \text{ e} \\ |\langle \boldsymbol{a}_1, \boldsymbol{a}_2 \rangle| \leq \frac{\langle \boldsymbol{a}_1, \boldsymbol{a}_1 \rangle}{2} \quad . \end{aligned} \tag{2}$$

As condições acima são também chamadas de *condições de Minkowski*. Geometricamente, o coeficiente da projeção de $\boldsymbol{a}_2$ ao longo de $\boldsymbol{a}_1$ não ultrapassa $1/2$ ($\boldsymbol{a}_2$ não é "muito maior"que $\boldsymbol{a}_1$). A justificativa da definição é dada pelo Teorema 3 abaixo. Antes, enunciaremos um lema de invarância da condição de Minkowski por transformações ortogonais e mudanças de escala.

Lema 1. *Seja uma base $\{\boldsymbol{a}_1, \boldsymbol{a}_2\}$ associada à matriz geradora A para o reticulado Λ, Q uma matriz ortogonal e $\alpha > 0$. A base $\{\boldsymbol{a}_1, \boldsymbol{a}_2\}$ satisfaz as condições de Minkowski se, e somente se, $\{\alpha Q\boldsymbol{a}_1, \alpha Q\boldsymbol{a}_2\}$ satisfaz a as condições de Minkowski.*

Demonstração. Imediata. □

Além disso, como formas quadráticas associadas a transformações ortognais de uma base de um reticulado são idênticas, $\lambda_1(\Lambda(A)) = \lambda_1(\lambda(QA))$ e, é claro $\lambda_1(\alpha\Lambda) = \alpha\lambda_1(\Lambda)$.

Teorema 3. *Se $\{\boldsymbol{a}_1, \boldsymbol{a}_2\}$ é uma base Minkowski-reduzida, então $\|\boldsymbol{a}_1\|_2 = \lambda_1$.*

Demonstração. Das observações e do lema acima, podemos supor, sem perda de generalidade que a matriz geradora do reticulado associada à base $\{\boldsymbol{a}_1, \boldsymbol{a}_2\}$ tem a forma

$$\begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix}, \tag{3}$$

caso contrário realizamos uma transformação ortogonal que leva o vetor $\boldsymbol{a}_1$ em $(\|\boldsymbol{a}_1\|, 0)$ e uma mudança de escala, de modo a transformar $\boldsymbol{a}_1$ em $(1, 0)$. Suponha agora que (3) satisfaça as condições de Minkowski, ou seja

$$1 \leq x^2 + y^2 \text{ e } |x| \leq \frac{1}{2}.$$

A norma de um ponto de Λ satisfaz

$$\begin{aligned} \|A\boldsymbol{u}\|^2 &= u_1^2 + u_2^2(x^2 + y^2) + 2xu_1u_2 \geq u_1^2 + u_2^2 + 2xu_1u_2 \\ &\geq u_1^2 + u_2^2 - |u_1u_2| \geq 1 \end{aligned}$$

Como 1 é atingido pelo menor vetor, $(1, 0)$ é um vetor de norma mínima (e portanto, em um reticulado geral, $\boldsymbol{a}_1$ seria o vetor de norma mínima).

□

Uma base de Minkowski contém, portanto, o menor vetor de um reticulado. A pergunta natural é como encontrar (caso exista) uma base de Minkowski. A resposta é algoritmica. Seguiremos o algoritmo dado por [Coh00], que pode ser visto como uma generalização do algoritmo euclidiano para encontrar o máximo divisor comum entre dois números.

Algorithm 1 Redução de Minkowski Bi-Dimensional

procedure MINKOWSKI($\boldsymbol{a}_1, \boldsymbol{a}_2$)
  Se $\|\boldsymbol{a}_1\|_2 > \|\boldsymbol{a}_2\|_2$, troque $\boldsymbol{a}_1$ e $\boldsymbol{a}_2$
  $\boldsymbol{r} \to 0$
  while $\|\boldsymbol{r}\|_2 < \|\boldsymbol{a}_1\|_2$ **do**
    $\boldsymbol{a}_2 \leftarrow \boldsymbol{a}_1$
    $\boldsymbol{a}_1 \leftarrow \boldsymbol{r}$
    $w \leftarrow \left\lfloor \dfrac{\langle \boldsymbol{a}_1, \boldsymbol{a}_2 \rangle}{\langle \boldsymbol{a}_1, \boldsymbol{a}_1 \rangle} \right\rceil$
    $\boldsymbol{r} \leftarrow \boldsymbol{a}_2 - w\boldsymbol{a}_1$
  end while
  retorne $\{\boldsymbol{a}_1, \boldsymbol{a}_2\}$
end procedure

Teorema 4. *O algoritmo está correto e, ao fim, retorna uma base reduzida de Minkowski para* $\Lambda(\boldsymbol{a}_1, \boldsymbol{a}_2)$

Demonstração. Primeiramente, é claro que todas as operações efetuadas no algoritmo são elementares e, a cada passo, $\|\boldsymbol{a}_1\|$ é reduzida. Assim, certamente o algoritmo para em uma quantidade finita de passos. Para a corretude, mostraremos que $\|\boldsymbol{a}_1\|_2 = \lambda_1$. A demonstração das outras condições de Minkowski fica a cargo do leitor.

Em cada passo do *loop*, w é o coeficiente inteiro que minimiza a norma de $\boldsymbol{a}_2 - t\boldsymbol{a}_1$. Com efeito,

$$\|\boldsymbol{a}_2 - t\boldsymbol{a}_1\|_2^2 = \|\boldsymbol{a}_2\|^2 - 2t \langle \boldsymbol{a}_1, \boldsymbol{a}_2 \rangle + t^2 \|\boldsymbol{a}_2\|^2$$

é uma parábola em t. O mínimo da parábola, para t real, é atingido quando $t^* = \langle \boldsymbol{a}_1, \boldsymbol{a}_2 \rangle / \langle \boldsymbol{a}_1, \boldsymbol{a}_1 \rangle$ e, como a parábola é simétrica em relação ao ponto mínimo, o inteiro t que minimiza a norma é $\lfloor t^* \rceil = w$. Portanto, ao final do algoritmo temos $\|\boldsymbol{a}_2 - t\boldsymbol{a}_1\| \geq \|\boldsymbol{a}_1\|$ para qualquer $t \in \mathbb{Z}$. Tomando um

elemento $\boldsymbol{x} = u_1\boldsymbol{a}_1 + u_2\boldsymbol{a}_2$, seja $u_1 = ku_2 + r$, onde $0 \leq r < |u_2$. Utilizando o fato de que $\|\boldsymbol{a}_2 - t\boldsymbol{a}_1\| \geq \|\boldsymbol{a}_1\|$, vemos que $\|\boldsymbol{x}\| \geq (|u_1| - |r|)\,\|\boldsymbol{a}_1\|$,e portanto $\boldsymbol{a}_1$ é um vetor de norma mínima. □

3.2 Aplicação: A constante de Hermite γ_2

Vimos nas aulas passadas que, dado um reticulado Λ, o primeiro mínimo satisfaz

$$\frac{\lambda_1}{(\det \Lambda)^{1/n}} \leq c\sqrt{n},$$

em que $0 < c \leq 1$. A razão $\frac{\lambda_1}{(\det \Lambda)^{1/n}}$ é uma medida de quão "eficiente" é um reticulado em termos de norma mínima e determinante (explicações geométricas mais precisas serão dadas no estudo de empacotamentos). Seja

$$\gamma(\Lambda) = \frac{\lambda_1^2}{(\det \Lambda)^{2/n}}.$$

A *constante de Hermite*[1] γ_n é definida domo

$$\gamma_n = \sup\left\{\gamma(\Lambda) : \Lambda \text{ possui posto } n\right\}. \tag{4}$$

Mais para frente, veremos que de fato o sup acima pode ser substituído por "max" (ou seja, o supremo é efetivamente atingido por algum reticulado). Segue do Teorema de Minkowski para o primeiro mínimo que $\gamma_n = O(n)$. Mostraremos na próxima aula que $\gamma_n = \Theta(n)$ (ou seja, existem constantes c_1 e c_2 tais que $c_1 n \leq \gamma_n \leq c_2 n$ para n suficiemente grande). Este resultado, conhecido como Teorema de Minkowski-Hlawka, é uma das principais realizações da Geometria dos Números.

Utilizando o conceito de base Minkowski-reduzida podemos encontrar a constante de Hermite γ_2:

Teorema 5. $\gamma_2 = \dfrac{2}{\sqrt{3}}$.

Demonstração.

$$\gamma_2 = \sup\left\{\gamma(\Lambda) : \Lambda \text{ possui posto } 2\right\}.$$

Podemos, é claro, restringirnos a reticulados em $\mathbb{R}^2$, isto é:

$$\gamma_2 = \sup\left\{\gamma(\Lambda(A)) : A \in \mathbb{R}^{2\times 2}, \det A \neq 0\right\},$$

[1]Por razões históricas, a constante é definida a partir do quadrado da razão $\lambda_1/(\det \Lambda)^{1/n}$

ou, ainda mais, como qualquer reticulado possui base reduzida

$$\gamma_2 = \sup\left\{\gamma(\Lambda(A)) : A \in \mathbb{R}^{2\times 2}, \det A \neq 0, \{\boldsymbol{a}_1, \boldsymbol{a}_2\} \text{ é Minkowski-reduzida}\right\}$$

Mais que isso, seja A uma matriz geradora para Λ. Temos, para qualquer matriz ortogonal Q e número real $\alpha > 0$

$$\gamma_n(\Lambda(A)) = \gamma_n(\Lambda(\alpha Q A)).$$

Assim, podemos supor no supremo acima que a matriz A cuja base associada é Minkowski-reduzida tem forma

$$\begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix}. \tag{5}$$

(Veja a Equação (3) e os argumentos ao redor dela). Por estes argumentos

$$\gamma_2 = \sup\left\{\gamma(\Lambda(A)) : A = \begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix}, x^2 + y^2 \geq 1, |x| \leq 1\right\}.$$

Sob estas condições, temos que $\lambda_1(\Lambda(A)) = 1$ e $\det \Lambda(A) = y$ (supondo, também sem perda de generalidade, que $y > 0$). Deste modo:

$$\gamma_2 = \sup\left\{1/y : x^2 + y^2 \geq 1, |x| \leq 1, y > 0.\right\}.$$

Neste ponto, está claro que "sup = max" na equação acima. Como minimizar $1/y$ é equivalente a maximizar y, temos o seguinte problema de otimização com restrições:

$$\begin{aligned} &\max y \\ \text{t.q. } &x^2 + y^2 \geq 1, \\ &|x| \leq 1, \\ &y > 0. \end{aligned}$$

É fácil ver que o único máximo do problema ocorre quando $y = \sqrt{3}/2$ e $x = \pm 1/2$. □

De fato, os argumentos acima mostram não apenas que $\gamma_2 = 2/\sqrt{3}$ mas que, a menos de uma mudança de escala e uma transformação ortogonal, existe um *único* reticulado que atinge γ_2. Esse reticulado é conhecido como Hexagonal (re-veja Exemplo 1).

4 Redução de Base em Dimensões Maiores

4.1 Base Reduzida de Minkowski

Seja $\Lambda = \Lambda(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n) \subset \mathbb{R}^n$ um reticulado. Um conjunto de vetores $\{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k\} \subset \Lambda$, $k < n$, é dito *primitivo* se existem $\boldsymbol{x}_{k+1}, \ldots, \boldsymbol{x}_n$ tais que $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ formam uma base para Λ. Em outra palavras, um conjunto primitivo de vetores pode ser estendido de modo a formar uma base para Λ.

Dizemos que $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ é uma base *Minkowski-reduzida* para $\Lambda(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n)$ se $\boldsymbol{a}_i$ é o vetor de menor norma tal que o conjunto formado pelos vetores $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{i-1}, \boldsymbol{a}_i$ é primitivo em Λ.

Como Λ é discreto, uma base reduzida de Minkowski sempre existe (Ver Exercício 1). Entretanto, calcular a base reduzida de Minkowski é computacionalmente muito difícil (implica, por exemplo, encontrar o menor vetor de Λ). O primeiro algoritmo que resolve o problema (com complexidade exponencial, aproximadamente $O((5/4)^{4n^3 - o(1)})$ pode ser visto em [Hel85]. Atualmente, novos algoritmos (mais eficientes) podem ser encontrados na literatura. Um algoritmo que calcule a redução de Minkowski em reticulados gerais de maneira "prática" é um problema em aberto.

4.2 Base Reduzida LLL

Podemos estender as condições de Minkowski 2 para pares de vetores em uma base de um reticulado n-dimensional. O celebrado algoritmo LLL segue o princípio 2-dimensional para encontrar uma base "reduzida por blocos".

Seja $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n\}$ uma base para Λ. Aplicando o processo de ortogonalização de Gram-Schmidt nesta base, obtemos:

$$\tilde{\boldsymbol{a}}_i = \boldsymbol{a}_i - \sum_{j=1}^{i-1} \frac{\langle \boldsymbol{a}_i, \tilde{\boldsymbol{a}}_j \rangle}{\langle \tilde{\boldsymbol{a}}_j, \tilde{\boldsymbol{a}}_j \rangle} \tilde{\boldsymbol{a}}_j := \boldsymbol{a}_i - \sum_{j=1}^{i-1} \mu_{ij} \tilde{\boldsymbol{a}}_j.$$

Dizemos que a base $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n\}$ é δ-LLL reduzida se as seguintes condições são satisfeitas

(i) $|\mu_{ij}| \leq \frac{1}{2}$.

(ii) $\delta \left\|\tilde{\boldsymbol{a}}_i\right\|^2 \leq \mu_{i+1,i}^2 \left\|\tilde{\boldsymbol{a}}_i\right\|^2 + \left\|\tilde{\boldsymbol{a}}_{i+1}\right\|^2$

A primeira condição diz que o coeficiente da projeção de um vetor $\boldsymbol{b}_i$ em $\tilde{\boldsymbol{b}_j}$ não é "muito grande" e a segunda diz que vetores consecutivos não tem uma grande diferença de norma entre eles. A demonstração do seguinte teorema pode ser encontrada em [MG02]:

Teorema 6. *Se* $\{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n\}$ *é uma base reduzida* δ*-LLL, então*

$$\|\boldsymbol{a}_1\|_1 \leq \left(\frac{2}{\sqrt{4\delta - 1}}\right)^n \lambda_1(\Lambda).$$

De fato, também é [MG02] é exibido um algoritmo em tempo polinomial nas entradas de $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n$ e na dimensão n para calcular a base reduzida LLL de um reticulado qualquer (isso é assunto para um dos trabalhos de fim de curso...)

Referências

[Bha00] M. Bhargava. On the Conway-Schneeberger fifteen theorem, Quadratic forms and their applications. *ontemp. Math.Amer. Math. Soc., Providence,*, 272:2737, 2000.

[Bha11] M. Bhargava. Universal Quadratic Forms and the 290 Theorem. *Inventiones Mathematicae (to appear)*, 272, 2011.

[Coh00] H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer, 2000.

[Hel85] B. Helfrich. Algorithms to construct minkowski reduced and hermite reduced lattice bases. *Theoretical Computer Science*, 41(0):125 – 139, 1985.

[MG02] D. Micciancio and S. Goldwasser. *Complexity of Lattice Problems: a cryptographic perspective.* Kluwer Academic Publishers, Boston, Massachusetts, March 2002.

[P. 12] P. L. Clark, J. Hicks, K. Thompson and N. Walters. GoN II: Universal quaternary quadratic forms. *Integers*, 12:A50, 2012.