Centro de Investigación en Computación

Matemática Detrás de la Criptografía Basada en Lattices y una Introducción al Esquema de Cifrado NTRU.

1

Flores Rodríguez Jaziel David.

Contents

1 Definiciones Básicas. 2
2 Teoremas Iniciales. 2
3 Los Problemas del Vector Más Corto y El Más Cercano 4
4 Algunas Variantes de los Problemas 4
5 Los Teoremas de Hermite y Minkowski 5
6 La Heurística Gaussiana 6
7 El Algoritmo de Babai y El Uso de "Buenas" $\mathbb{Z}$-bases en **apprCVP** 7
8 El Algoritmo LLL 10

1 Definiciones Básicas.

Definición 1 *Sea $\beta = \{v_1, ..., v_n\} \subset \mathbb{R}^m$ un conjunto linealmente independiente de vectores. La* ***Retícula*** *Λ generada por β es el conjunto de todas las combinaciones de $v_1, ..., v_n$ con coeficientes en $\mathbb{Z}$, es decir*

$$\Lambda_\beta = \left\{ \sum_{i=1}^{n} \alpha \mathbf{v}_i | \alpha \in \mathbb{Z}, \mathbf{v}_i \in \beta \quad \forall i \in \{1, ..., n\} \right\}$$

Una $\mathbb{Z}$-base para Λ_β es cualquier conjunto de vectores que generan a Λ_β. La dimensión de Λ_β es la cantidad de vectores en una $\mathbb{Z}$-base para Λ_β.

Definición 2 *Sean Λ_β una Retícula de dimensión n y $\beta = \{v_1, ..., v_n\}$ una $\mathbb{Z}$-base para Λ_β. Se define el* ***Dominio Fundamental*** *para Λ_β correspondiente a esta $\mathbb{Z}$-base, denotado como $\mathcal{F}(v_1, ..., v_n)$ como el conjunto:*

$$\mathcal{F}(v_1, ..., v_n) = \left\{ \sum_{i=1}^{n} \alpha \mathbf{v}_i \quad | \quad 0 \leq \alpha_i < 1 \right\}$$

Al volumen n-dimensional para $\mathcal{F}(v_1, ..., v_n)$ Dominio Fundamental, es decir al determinante de la matriz cuyas filas son los vectores $v_1, ..., v_n$, se denominará un ***covolumen*** *para Λ_β, y es denotado por* ***Det(Λ_β)****.*

2 Teoremas Iniciales.

Teorema 1 *Sea $\Lambda \subset \mathbb{R}^n$ una retícula de dimensión n y sea $\mathcal{F}$ un dominio fundamental para Λ. Entonces $\forall w \in \mathbb{R}^n$ se cumple que:*

$$\exists! t \in \mathcal{F} \quad y \quad \exists! v \in \Lambda \quad tales \quad que \quad w = t + v \tag{1}$$

Equivalentemente, la unión de los dominios fundamentales trasladados:

$$\mathcal{F} + v = \{t + v \quad | \quad t \in \mathcal{F}\}$$

Así v se extiende sobre los vectores en la retícula Λ cubre exactamente $\mathbb{R}^n$

La desigualdad de Hadamard es cierta porque el volumen de un paralelepípedo nunca es mayor que el producto de las longitudes de sus lados. La desigualdad de Hadamard es una igualdad, si y sólo si, los vectores base son ortogonales (perpendiculares) entre sí. En medida de que es desigualdad mide la caracteristica de que la base no es ortogonal.

Teorema 2 *Desiguadad de Hadamard Sea Λ una retícula, sea cualquier $v_1, ..., v_n$ una $\mathbb{Z}$-base para Λ, y sea $\mathcal{F}(v_1, ..., v_n)$ un dominio fundamental para Λ. Entonces:*

$$Det(\Lambda) \leq Vol(\mathcal{F}) \leq ||\mathbf{v}_1|| \cdot ||\mathbf{v}_2|| \cdot ... \cdot ||\mathbf{v}_n||. \tag{2}$$

Un famoso teorema de Hermite dice que cada Lattice tiene una base que es razonablemente ortogonal, donde la cantidad de no ortogonalidad está limitada únicamente en términos de la dimensión.

Corolario 1 *Sea $\Lambda \subset \mathbb{R}^n$ una retícula de dimensión n. Entonces cada fominio fundamental de Λ tiene el mismo volumen. Por lo tanto Det($\mathcal{F}$) es un invariante de la retícula Λ, independiente del dominio fundamental particular usado para calcularlo.*

Ejemplo 1 *Considere una retícula 3-dimensinal $\Lambda \subset \mathbb{R}^3$, generada por los vectores: $v_1 = (2, 1, 3)$, $v_2 = (1, 2, 0)$ y $v_3 = (2, -3, -5)$*
Es conveniente formar una matriz con los vectores anteriores como filas de la matriz:

$$A = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 0 \\ 2 & -3 & -5 \end{pmatrix}$$

Se crean los siguientes vectores en Λ:
$w_1 = v_1 + v_3$, $w_2 = v_1 - v_2 + 2v_3$, *y* $w_3 = v_1 + 2v_2$
Esto equivale a multiplicar la matriz A por la izquierda por:

$$U = \begin{pmatrix} 1 & 0 & 1 \\ 1 & -1 & 2 \\ 1 & 2 & -5 \end{pmatrix}$$

Y buscamos que w_1, w_2, w_3 sean las filas de la matriz:

$$B = UA = \begin{pmatrix} 4 & 5 & 4 \\ 5 & -7 & -7 \\ 4 & 5 & 3 \end{pmatrix}$$

La matriz U tiene determinante -1, así pues los vectores w_1, w_2, w_3 son también una $\mathbb{Z}$-base para Λ

3 Los Problemas del Vector Más Corto y El Más Cercano

Los problemas computacionales asociados a retículas son aquellos en los cuales encontrar el vector no nulo más corto en una retícula y encontrar un vector la retícula que es más cercano a un vector dado que no está en ella.

- **Shortest Vector Problem (SVP)**:
  Encontrar el vector no nulo más corto en la retícula Λ, es i.e. encontrar un vector no nulo $v \in \Lambda$ que minimiza la norma Euclidiana $||v||$.
- **Closest Vector Problem (CVP)**:
  Dado un vector $w \in \mathbb{R}^m$ tal que no esté en Λ. Encontrar un vector $v \in \Lambda$ más cercano a w, i.e. encontrar un vector $v \in \Lambda$ que minimiza la norma Euclidiana $||w - v||$.

Se sabe que **CVP** es $\mathcal{NP}$-hard y **SVP** es $\mathcal{NP}$-hard bajo la hipótesis de reducción aleatoria. **CVP** está considerada como más compleja que **SVP**.

4 Algunas Variantes de los Problemas

Observación Existen muchas variantes de **SVP** y **CVP** que surgen tanto en la teoría como en la práctica.

- **Shortest Basis Problem (SBP)**:
  Encontrar una $\mathbb{Z}$-base $v_1, v_2, ..., v_n$ para una retícula que es la más corta en el sentido de su norma. Se requiere que $\max_{1 \leq i \leq n} ||v_i||$ sea mínimo.
- **The Approximate Closest Vector Problem (apprCVP)**
  Dado $w \in \mathbb{R}^n$, encontrar un vector $v \in \Lambda$ tal que $||v - w||$ es pequeña. O bien $||v - w|| \leq k \min_{u \in \Lambda} ||u - w||$ Para una constante k pequeña
  .
- **The Approximate Shortest Vector Problem (apprSVP)**

5 Los Teoremas de Hermite y Minkowski

Teorema de Hermite: En cada retícula Λ de dimensión n existe in vector no nulo $v \in \Lambda$ que satisface:

$$||v|| \leq \sqrt{n} \cdot Det(\Lambda)^{\frac{1}{n}} \tag{3}$$

Observación Para dada una dimensión n, la constante de Hermite γ_n es el valor más pequeño tal que para cada retícula Λ de dimensión n contiene un vector no nulo $v \in \Lambda$ que satisface:

$$||v||^2 \leq \gamma_n \cdot Det(\Lambda)^{\frac{2}{n}} \tag{4}$$

Esto nos dice que $\gamma_n \leq n$.

Los valores exctos de γ_n son conocidos para $1 \leq n \leq 8$ y para $n = 24$:

${\gamma_2}^2$	${\gamma_3}^3$	${\gamma_4}^4$	${\gamma_5}^5$	${\gamma_6}^6$	${\gamma_7}^7$	${\gamma_8}^8$	${\gamma_{24}}^{24}$
$\frac{4}{3}$	2	4	8	$\frac{64}{3}$	64	256	4

Para propósitos dentro de la criptografía estamos principalmente ineresados en el valor de γ_n cuando n es grande. Para valores grandes de n es conocido que la constante de Hermite satisface:

$$\frac{n}{2\pi e} \leq \gamma_n \leq \frac{n}{\pi e} \tag{5}$$

Observación Se puede probar que una retícula Λ n-dimensional siempre tiene una base $v_1, ..., v_n$ satisface:

$$||v_1|| \cdot \cdots \cdot \leq n^{\frac{n}{2}} \cdot Det(\Lambda) \tag{6}$$

Definición 3 *Una región $\mathcal{R} \subset \boldsymbol{V}$ se dice de Minkowski cumple las siguientes condiciones:*

Compacto: Es decir que sea cerrado y acotado
Convexo: Es decir, si $\mathbf{u}, \mathbf{w} \in \mathcal{R}$ entonces $\mathbf{seg}[\mathbf{u}, \mathbf{v}] \subset \mathcal{R}$
Simétrico: $\forall \mathbf{v} \in \mathcal{R}$ implica $-\mathbf{v} \in \mathcal{R}$

Teorema 3 *Sea $\Lambda \subset \mathbb{R}^n$ una retícula de dimensión n y sea $\mathcal{R} \subset \mathbb{R}^n$ una región de Minkowski cuyo volumen satisface:*

$$2^n \cdot Det(\Lambda) \leq Vol(\mathcal{R})$$

Entonces $\mathcal{R}$ contiene un vector no nulo en la retícula.

6 La Heurística Gaussiana

Definición 4 *La función gamma $\Gamma(s)$ está definida para $s > 0$ por la integral:*

$$\Gamma(s) = \int_0^\infty t^{s-1} e^{-t} dt$$

La bola cerrada $\mathbb{B}_R(0)$ con centro en el origen y radio R, es compacto, convexo, y simétrico, cumple el Teorema de Minkowski dice que si se escoge R tal que:

$$2^n \cdot Det(\Lambda) \leq Vol(\mathbb{B}_R(0))$$

Entonces la bola $\mathbb{B}_R(0)$ contiene un vector no nulo de la retícula. Asumiendo que n es grande, podemos aproximar el volumen de $\mathbb{B}_R(0)$ y eligiendo R que satisface:

$$\sqrt{\frac{2\pi e}{n}} R \gtrapprox 2 \cdot Det(\Lambda)^{1/n}$$

Por lo tanto para una n grande existe un vector no nulo $v \in \Lambda$ satisface:

$$\sqrt{\frac{2n}{\pi e}} \cdot Det(\Lambda)^{1/n} \gtrapprox ||v||$$

Aunque los límites exactos para el tamaño de un tamaño del vector más corto son desconocidos cuando la dimensión n es grande, podemos estimar su tamaño mediante un argumento probabilístico que se basa en el siguiente principio. Principio Sea $\mathbb{B}_R(0)$ una bola centrada en el origen muy grande. El número de puntos de la retícula Λ en $\mathbb{B}_R(0)$ es aproximadamente igual al volumen de $\mathbb{B}_R(0)$ dividido por el volumen del Dominio Fundamental $\mathcal{F}$.

Asuminendo que n es grande, se hace una estimación y así se tiene:

$$\left(\frac{2\pi e}{n}\right)^{n/2} \approx Vol[\mathbb{B}_R(0)]$$

Y así se cumple que $R \approx \sqrt{n/2\pi e} \cdot (Det(\Lambda))^{1/n}$

Definición 5 *Sea Λ una retícula de dimensión n.* ***La Longitud Gaussiana esperada más corta****, denotada por $\sigma(\Lambda)$, es:*

$$\sigma(\Lambda) = \sqrt{\frac{n}{2\pi e}} \cdot (Det(\Lambda))^{1/n}$$

Lo que la Heurística Gaussiana nos dice es que un vector más corto no nulo en una retícula elegida al azar, satisfará que:

$$|||v_{shortest}|| \approx \sigma(\Lambda)$$

7 El Algoritmo de Babai y El Uso de "Buenas" $\mathbb{Z}$-bases en apprCVP

Si una retícula $\Lambda \subset \mathbb{R}^n$ con una $\mathbb{Z}$-base $\mathbf{v_1}, ..., \mathbf{v_n}$ que consiste de vectores que son mutuente ortogonales, i.e tales que:

$$\mathbf{v_i} \cdot \mathbf{v_j} = 0 \quad \forall i \neq j$$

Entonces es más fácil resolver tanto **SVP** Y **CVP**. Ahora, para resolver **SVP** entonces observamos que la longitud de cualquier vector en Λ está dada por la fórmula:

$$||\alpha_1 \mathbf{v_1} + \alpha_1 \mathbf{v_1} + ... + \alpha_n \mathbf{v_n}||^2 = \alpha_1^2 ||\mathbf{v_1}||^2 + \alpha_2^2 ||\mathbf{v_2}||^2 + ... + \alpha_n^2 ||\mathbf{v_n}||^2$$

Entonces $a_1, ..., a_n \in \mathbb{Z}$, entonces vemos que el vector (o los vectores) más corto(s) no nulo(s) en Λ son simplemente los vectores más pequeños en el conjunto $\{\pm\mathbf{v_1}, ..., \pm\mathbf{v_n}\}$

Similarmente, suponga que se quiere encontrar el vector en Λ que es más cercano a dado un vector $\mathbf{w} \in \mathbb{R}^n$. Entonces primero escribimos en términos:

$$\mathbf{w} = t_1 \mathbf{v_1} + t_2 \mathbf{v_2} + ... + t_n \mathbf{v_n} \quad con \quad t_1, ..., t_n \in \mathbb{R}^n$$

Entonces para $\mathbf{v} = \alpha_1\mathbf{v_1} + ... + \alpha_n\mathbf{v_n} \in \Lambda$, tenemos:

$$||\mathbf{v} - \mathbf{w}||^2 = (\alpha_1 - t_1)^2||\mathbf{v_1}||^2 + ... + (\alpha_1 - t_1)^2||\mathbf{v_1}||^2$$

Los escalares α_i requieren ser enteros, entonces la ecuación anterior debería ser minimizada si tomamos cada α_i como el entero más cercano al correstopndeinte t_i. Es tentador probar un procedimiento similar con una base arbitraria de L. Si los vectores en la base son razonablemente ortogonales entre sí, entonces es probable que tengamos éxito en la resolución de CVP; pero sino, entonces el procedimiento no funciona bien.

El **Teorema 1** dice que las traslaciones de $\mathcal{F}$ por los elementos de Λ llenan todo el espacio $\mathbb{R}^n$, por lo que cualquier $\mathbf{w} \in \mathbb{R}^n$ está en una traslación única $\mathcal{F} + \mathbf{v}$ de $\mathcal{F}$ por un elemento $\mathbf{v} \in \Lambda$. Tomamos el vértice de la paralelepípedo $\mathcal{F} + \mathbf{v}$ que está más cerca de $\mathbf{w}$ como nuestra solución hipotética para **CVP**. Este procedimiento se ilustra. Es fácil encontrar el vértice más cercano, ya que:

$$\mathbf{w} = \mathbf{v} + \epsilon_1\mathbf{v_1} + \epsilon_2\mathbf{v_2} + ... + \epsilon_n\mathbf{v_n} \quad para \quad 0 \leq \epsilon_1, \epsilon_2, ..., \epsilon_n < 1$$

Así que simplemente reemplazamos ϵ_i por 0 si es menor que $\frac{1}{2}$ y lo reemplazamos por 1 si es mayor o igual a $\frac{1}{2}$.

Teorema 4 *Sea $\Lambda \subset \mathbb{R}^n$ una retícula de dimensión n con la $\mathbb{Z}$- base formada por los vectores $\mathbf{v_1}, ..., \mathbf{v_n}$, y sea $\mathbf{w} \in \mathbb{R}^n$ un vector arbirario. Si los vectores base son suficientemente ortogonales mutuamente, entonces el siguiente algoritmo resuelve **CVP**. En general, si los vectores en la base son*

Sea: $\mathbf{w} = t_1\mathbf{v_1} + t_2\mathbf{v_2} + ... + t_n\mathbf{v_n}$ con $t_1, ..., t_n \in \mathbb{R}$
Tome: $\alpha_i = \lfloor t_i \rfloor \ \forall i \in \{1, 2, ..., n\}$
Regrese el vector: $\mathbf{v} = \alpha_1\mathbf{v_1} + \alpha_2\mathbf{v_2} + ... + \alpha_n\mathbf{v_n}$.

*razonablemente ortogonales entre sí, entonces el algoritmo resuelve alguna versión de **apprCVP**, pero si los vectores base son altamente no ortogonales, entonces el vector devuelto por el algoritmo generalmente está lejos del vector dentro de la reticula que está más cercano a $\boldsymbol{w}$.*

Ejemplo 2 *Considere una retícula 2-dimensinal $\Lambda \subset \mathbb{R}^3$, generada por los vectores:*
$v_1 = (137, 312)$, *y* $v_2 = (215, -187)$

Vamos a usar el algoritmo de Babai para encontrar el vector más corto al vector $w = (53172, 81743)$. *El primer paso es exprear a* w *como combinación linal de los vectores base. Para eso usaremos álgebra lineal.*

$$w = t_1\mathbf{v_1} + t_2\mathbf{v_2}$$

Esto nos da dos ecuaciones lineales

$$53172 = 137t_1 + 215t_2, 81743 = 312t_1 - 187t_2$$

Es decir:

$$(53172, 81743) = (t_1, t_2)\begin{pmatrix} 137 & 312 \\ 215 & -187 \end{pmatrix}$$

Resolviendo se tiene que $t_1 = 296.85$ *y* $t_2 = 58.15$. *Entonces tenemos que aproximar a su parte entera. Así:*
$\mathbf{v} = \lfloor t_1 \rfloor \mathbf{v_1} + \lfloor t_2 \rfloor \mathbf{v_2} = 297(137, 312) + 58(215, 187)$
$= (53159, 81818)$. *Luego:* $||\mathbf{v} - \mathbf{w}|| = 76.12$.
Mientras que si usamos $u_1 = (1975, 438)$ *y* $u_2 = (7548, 1627)$ *como* $\mathbb{Z}$*-base obtenemos* $||\mathbf{v} - \mathbf{w}|| = 3308.12$.

Definición 6 ***Reducción de una Retícula:*** *El nombre dado al problema práctico de resolver SVP y CVP, o más generalmente de encontrar vectores razonablemente cortos y bases buenas o más convenientes.*

Suponga que tiene un conjunto linealmente independiente de vectores $\{\mathbf{v_1}, ..., \mathbf{v_n}\}$ y después del proceso de ortogonalizaión de Gram-Schmidth se obtiene un conjunto $\{\mathbf{v*_1}, ..., \mathbf{v*_n}\}$. Si algún coeficiente en el proceso de satisface:

$$\frac{|\mathbf{v_i} \cdot \mathbf{v*_j}|}{||\mathbf{v*_j}||^2} > \frac{1}{2}$$

Luego reemplazando v_i por $v_i - av_j$ con un a apropiado en $\mathbb{Z}$ hace que el coeficiente sea más pequeño. Decimos que una base satisface la **Condición de Tamaño** si:

$$\frac{|\mathbf{v_i} \cdot \mathbf{v*_j}|}{||\mathbf{v*_j}||^2} \leq \frac{1}{2} \quad \forall i < j$$

8 El Algoritmo LLL

Para equilibrar esto, queremos que los vectores base sean lo más ortogonales entre sí, por lo que imponemos la **Condición de Pseudo-Ortogonalidad**:

$$||\mathbf{v*_{i+1}}|| \geq \frac{\sqrt{3}}{2}||\mathbf{v*_i}||$$

Desafortunadamente, los algoritmos más conocidos para encontrar esa base son exponenciales en la dimensión. Entonces cambiamos la Condición de pseudo-ortogonalidad a una menos escritcta, la **Condición de Lovász**:

$$||\mathbf{v*_{i+1}}|| \geq \sqrt{\frac{3}{4} - \frac{|\mathbf{v_{i+1}} \cdot \mathbf{v*_i}|}{||\mathbf{v_i}||^2}}||\mathbf{v*_i}||$$

Teorema 5 ***Hermite***
En cada retícula existe una base que satisface tanto la Condición de tamaño como la Condición de pseudo-ortogonalidad. ***Demostración.****[5]*

Bibliography

[1] D. Simon, Selected applications of LLL in number theory, Bosma, Wieb. "4. LLL" (PDF). Lecture notes, 2010

[2] An Introduction to Mathematical Criptography, Springer; 2 edition, 2018, Jeffrey Hoffstein, Jill Pipher, Jose Silverman