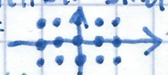
Γ = diskrete Untergruppe des euklid. Raums

Eigenes „Gesamtbild" CRYPTO1 – Gitterbasierte Verf. (I) 26.8.22

„Problem, das wir ein neues Problem brauchen." (RSA&DH durch Q.comp. gekn.)

[1] Was ist ein Gitter/„Lattice"?!
Ein n-dimensionales Gitter ist eine Teilmenge $L \subseteq \mathbb{R}^n$ mit n linear unabhängigen Vektoren $(b_1, \dots, b_n)$, sodass alle $x \in L$ als ganzzahlige Linearkombination von b_i darstellbar sind: $x = \sum_{i=1}^n z_i b_i$; $z_i \in \mathbb{Z}$.

[3] z.B. $\underbrace{b_1 = (1,0),\ b_2 = (0,1)}_{\text{(Idee: vernünftige Basis = priv. Schl.)}}$: L =  == $\underbrace{b_1 = (5,7),\ b_2 = (8,11)}_{\text{(Idee: unvernünftige Basis = öff. Schl.)}}$!

[2] 1. Gitterproblem: CVP (Closest Vector Problem)
Gegeben: $x \in \mathbb{R}^n$; Gesucht: Der (oder die) nächstgelegene Gitterpunkt?!

[3] 2. Gitterproblem: SVP (Shortest Vector Problem)
Finde einen Vektor $\neq 0$ in L mit der kürzesten Länge (d.h. alle and. mind. so lang)

[4] Bsp.: $b_1 = (5,7)$, $b_2 = (8,11)$, nächstgel. Gitterpkt. zu $(1.0, 0.9)$ ist $(1,1)$!

[5] Babai: Löse CVP zu $x \in \mathbb{R}^n$: $x = \sum_{i=1}^n x_i b_i$, $x_i \in \mathbb{R}$ (x als reeller Vektor in Vektorbasis)
$x = \sum_{i=1}^n \lceil x_i \rfloor \cdot b_i \in L$ (simpel: runde auf nächste ganze Zahl)
→ Bsp.: Gute Basis: $(1,0), (0,1)$: $\lceil 1.0 \rfloor \cdot (1,0) + \lceil 0.9 \rfloor \cdot (0,1) = (1,1)$ ☑
Schlechte Basis: $(5,7), (8,11)$: $\lceil -3.8 \rfloor \cdot (5,7) + \underbrace{\lceil 2.5 \rfloor}_{=2 \text{ (hin zur Null runden bei .5)}} \cdot (8,11) = (-4,-6) \neq (1,1)$ ↯
$\left(-3.8 \binom{5}{7} + 2.5 \binom{8}{11} = \binom{1.0}{0.9}\right)$

$x_i \in \mathbb{R}$, $y_i \in \mathbb{Z}$ [6] Für eine orthogonale Basis funktioniert dieses Herangehen von Babai: Bew.:
$\|x-y\|^2 = \|\sum_{i=1}^n x_i b_i - \sum_{i=1}^n y_i b_i\|^2 = \langle x-y, x-y \rangle = \langle \sum_{i=1}^n (x_i - y_i) b_i, \sum_{j=1}^n (x_j - y_j) b_j \rangle$
$\underset{\text{bilinear}}{=} \sum_{i,j=1}^n (x_i - y_i)(x_j - y_j) \underbrace{\langle b_i, b_j \rangle}_{=0 \text{ für } i \neq j} \underset{\text{orthogonal Basis}}{=} \sum_{i=1}^n (x_i - y_i)^2 \|b_i\|^2$ ist minimal gdw. $y_i = \lceil x_i \rfloor$ ■

[7] Babai für „fast" orthogonale Basen löst das Approximate CVP/CVP-γ.

[8] Babai für schlechte Basen funktioniert nicht. (siehe obiges Bsp.)

[9] Ein Gitter L mit Basis $(b_1, \dots, b_n)$ hat die Generatormatrix $G(L) = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ (d.h. einfach zeilenweise Basisvektoren)
Nenne Determinante dieser Matrix Det. des Gitters ⇒ betragsmäßig eindeutig ! (Basis egal)
Außerdem gilt: $\det(L) = |\det(G(L))| = \mathrm{vol}(F)$ mit Fundamentalbereich F 
$(F(b_1, \dots, b_n) := \{x = \sum x_i b_i \mid 0 \leq x_i \leq 1\})$; Sind G_1 und G_2 zwei Generatormatrizen von L,
Nenne U „unimodular". Ihre Einträge sind ganzzahlig. * dann exist. eine Matrix U mit $G_1 = U \cdot G_2$ u. $\det(U) = \pm 1$ ⇒ Äquiv.klassen ⇒ suche Vertreter!

[10] Hermitische Normalform: (ist ein solcher Vertreter UND effektiv zu berechnen)
„Unimodular": det = 1 (oder = −1) (und Einträge ganzzahlig)
Sei G eine Generatormatrix, U eine unimodulare Matrix, $U \cdot G$ in oberer Dreiecksform mit Werten > 0 in der Diagonale und ≥ 0 darüber; $U \cdot G$ heißt Hermit. Normalform.

[11] Praktisch heißt das, man darf: (eingeschränkter Gauß-Algo)
- Zeilen vertauschen
- Vielfache einer Zeile auf andere addieren
- mit ±1 durchmultiplizieren

Sage: `matrix(ZZ,[[],[]]).echelon_form()`

(*) entspricht: $\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$ •

Bsp.: $\begin{pmatrix} 5 & 7 \\ 8 & 11 \end{pmatrix} \overset{(*)}{\sim} \begin{pmatrix} 5 & 7 \\ 3 & 4 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 \\ 3 & 4 \end{pmatrix} \sim \begin{pmatrix} 2 & 3 \\ 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ = Hermit. Norm.form !
(Das Produkt unimodularer Matrizen ist wieder eine unimodulare Matrix!)
⇒ d.h. kriegt Generatormatrix leicht in Herm. NF ⇒ Probl. für alle, die was verbergen wollen

(„Bruch") [12] Hadamard-Ratio: Sei G Generatormatrix mit Zeilen $b_1, \dots, b_n$.
$\underbrace{0 \leq}_{\text{klar}} H(G) = H(b_1, \dots, b_n) = \sqrt[n]{\frac{|\det(G)|}{\|b_1\| \cdot \ldots \cdot \|b_n\|}} \leq 1$ ← Hadamard'sche Ungleichung
Es gilt: $H(G) = 1 \Leftrightarrow (b_1, \dots, b_n)$ orthogonal & je größer $H(G)$, desto besser klappt Babai-Algo

CVP ≙ [13] GGH-Kryptosystem (Goldreich-Goldwasser-Halevi): = „gescheitert" !
Öffentl. Parameter: $n \in \mathbb{N}$ Dimension, $\delta > 0$ klein („Fehler-Range"), ν („Nachr.-Range")
Privater Schlüssel: Generatormatrix G von L mit $H(G)$ nahe an 1 (geheime gute Basis)
Öffentl. Schlüssel: Generatormatrix A von L mit $H(A)$ nahe an 0 $\in L$ (schlechte Basis)
Verschlüsseln: $m \in [-\nu, \nu]^n \cap \mathbb{Z}^n$ Nachr., $e \in_R (-\delta, \delta)^n$ Fehlerv., $ENC(m) = m \cdot A + e \notin L$
CVP ≙ Entschlüsseln: $c = ENC(m)$; best. mit Babai nächstgeleg. Gitterpkt.: $m \cdot A$; $m = (m \cdot A) \cdot A^{-1}$ ■

BRUNNEN