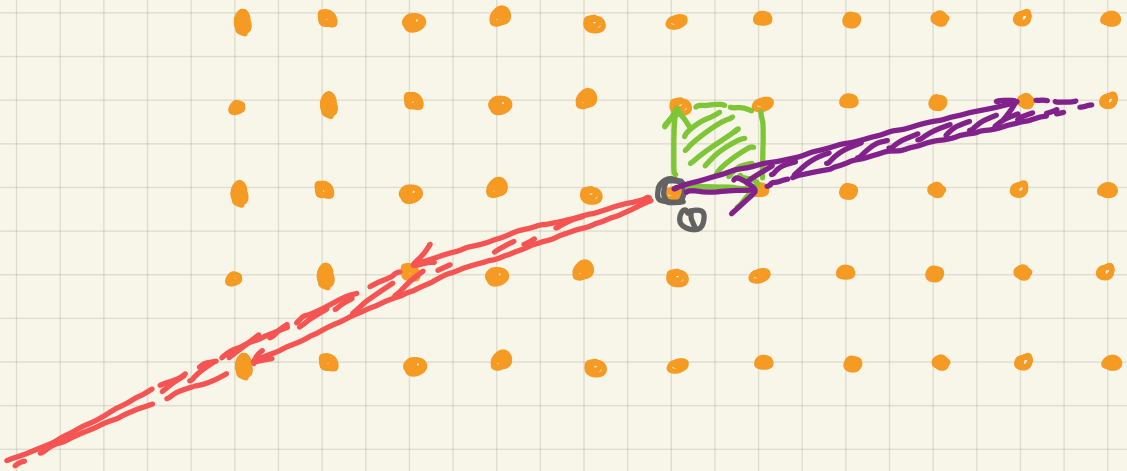
GDO-03 17.10.19

Def.: Die **Gitterdeterminante** eines n-dimensionalen Gitters $\Lambda \subseteq \mathbb{R}^n$ ist

$$\det(\Lambda) := \left|\det(B)\right| = \mathrm{vol}_n\left(B \cdot [0,1]^n\right)$$

wobei $B \subseteq \mathbb{R}^n$ eine beliebige Gitterbasis von Λ ist.
(Wohldefiniert wegen $B' = B \cdot U$, siehe letzte VL.)



Hadamard-Ungleichung: Für $B = [b^1, \dots, b^n] \in \mathbb{R}^{n \times n}$ regulär gilt:

$$|\det(B)| \leq \|b^1\|_2 \cdot \dots \cdot \|b^n\|_2$$

mit Gleichheit genau dann, wenn $b^1, \dots, b^n$ paarweise orthogonal sind, d.h. wenn $B \cdot B^T$ Diagonalmatrix ist.

Def.: Für eine Basis $B = [b^1, \dots, b^n] \in \mathbb{R}^{n \times n}$ des Gitters $\Lambda \subseteq \mathbb{R}^n$ heißt

$$OD(B) := \frac{\|b^1\|_2 \cdot \dots \cdot \|b^n\|_2}{\det(\Lambda)} \geq 1$$

der **Orthogonalitätsdefekt** von B.

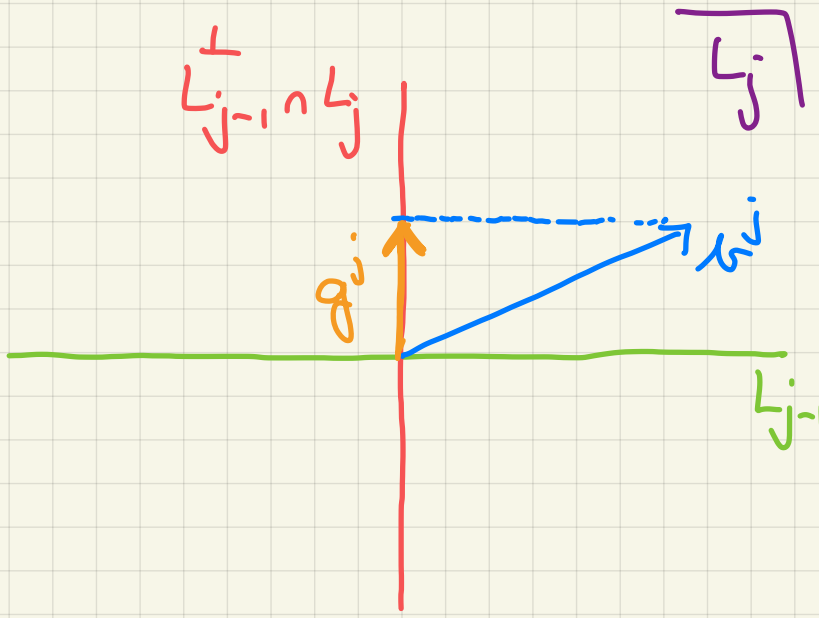
Ziel: Finde Gitterbasis mit kleinem OD und suche einen kürzesten Vektor darin als Verschlüsselung zum Knacken an.

Def.: Sei $B = [b^1, \dots, b^n] \in \mathbb{R}^{n \times n}$ eine (geordnete) Basis. Die Gram-Schmidt Orthogonal-Basis von B ist $G = [g^1, \dots, g^n] \in \mathbb{R}^{n \times n}$ mit

$$g^1 := b^1$$

$$\forall j > 1: \quad g^j := b^j - \sum_{k=1}^{j-1} \mu_{kj} g^k$$

$$\text{mit } \mu_{kj} := \frac{\langle b^j, g^k \rangle}{\|g^k\|_2^2}$$



Bemerkungen:

- $L_j := \text{lin}\{b^1, \dots, b^j\}$ für $j \in [n]$
- Ist B rational, so sind auch G und alle μ_{kj} rational.
- g^j ist die orthogonale Projektion von b^j auf das orthogonale

Komplement von L_{j-1} in L_j.

- G ist eine orthogonale Basis von $\mathbb{R}^n$.
- Mit $R := (\mu_{kj}) \in \mathbb{R}^{n \times n}$ und

$$\mu_{jj} := 1 \quad \forall j \in [n] \quad , \quad \mu_{kj} := 0 \quad \forall j < k \leq n$$

(obere Dreiecksmatrix mit Einsen auf der Hauptdiagonalen)

gilt $B = GR$.

- $\det(R) = 1 \Rightarrow \det(B) = \det(G)$
- G orthogonal, also:

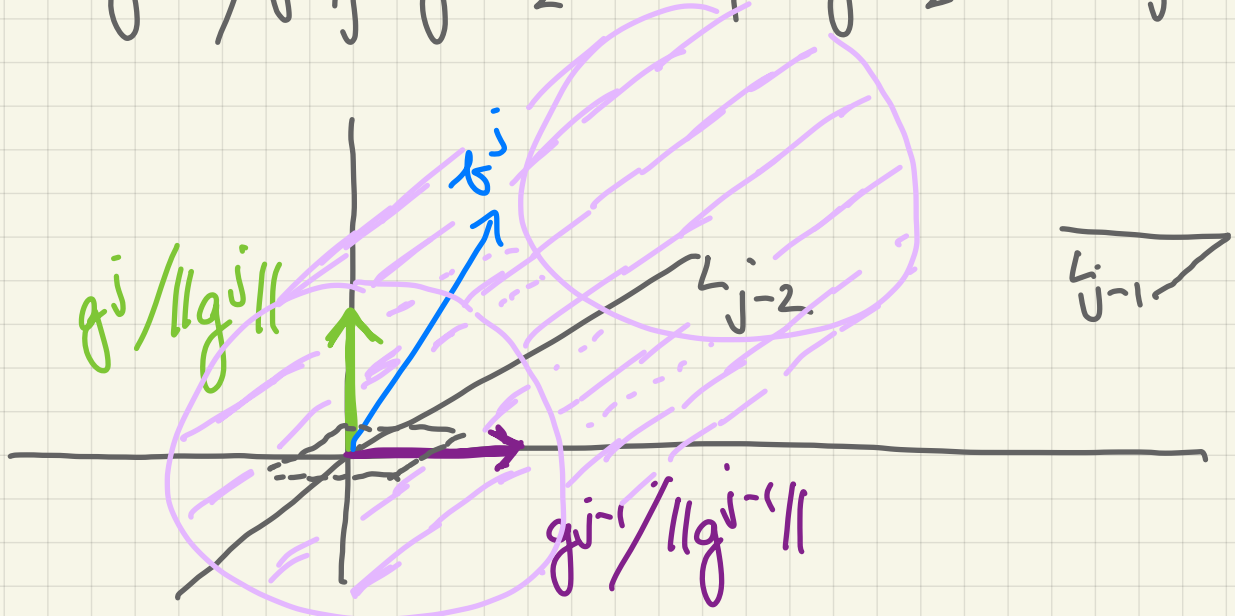
$$\|g^1\|_2 \cdot \ldots \cdot \|g^n\|_2 = \sqrt{\det(G^T G)} = |\det(G)| = \det(\Delta(B))$$

(wegen $\|b^j\|_2 \geq \|g^j\|_2$ benutze das die Hadamard-Ungleichung).

Def.: Eine (geordnete) Basis $\mathcal{B} = [b^1, \dots, b^n] \in \mathbb{R}^{n \times n}$ heißt **(Lovász-) reduziert**, wenn für ihre Gram-Schmidt-Orthogonalisierung $G = [g^1, \dots, g^n] \in \mathbb{R}^{n \times n}$ und die zugehörigen μ_{kj} gilt:

(i) $|\mu_{kj}| \leq \frac{1}{2} \quad \forall 1 \leq k < j, \; j = 2, \dots, n$

(ii) $\|g^j + \mu_{j-1,j} \cdot g^{j-1}\|_2^2 \geq \frac{3}{4} \|g^{j-1}\|_2^2 \quad \forall j = 2, \dots, n$



Projektion von b^j in Richtung von L_{j-1} und b^j auf Richtung von

Satz 1.1: Für eine reduzierte Basis $B = [b^1, \dots, b^n] \in \mathbb{R}^{n \times n}$ mit Gram-Schmidt Orthogonalisierung $G = [g^1, \dots, g^n] \in \mathbb{R}^{n \times n}$ gelten:

(i) $\|b^j\|_2^2 \leq 2^{j-1} \|g^j\|_2^2 \quad \forall j \in [n]$

(ii) $\det(B) \leq 2^{\frac{n(n-1)}{4}}$