Komplexitätstheoretische Betrachtungen von gitterbasierten Kryptografiesystemen

Patrick Vogt

Hochschule RheinMain

4. September 2013

Übersicht

Einführung

Asymmetrische Kryptografie

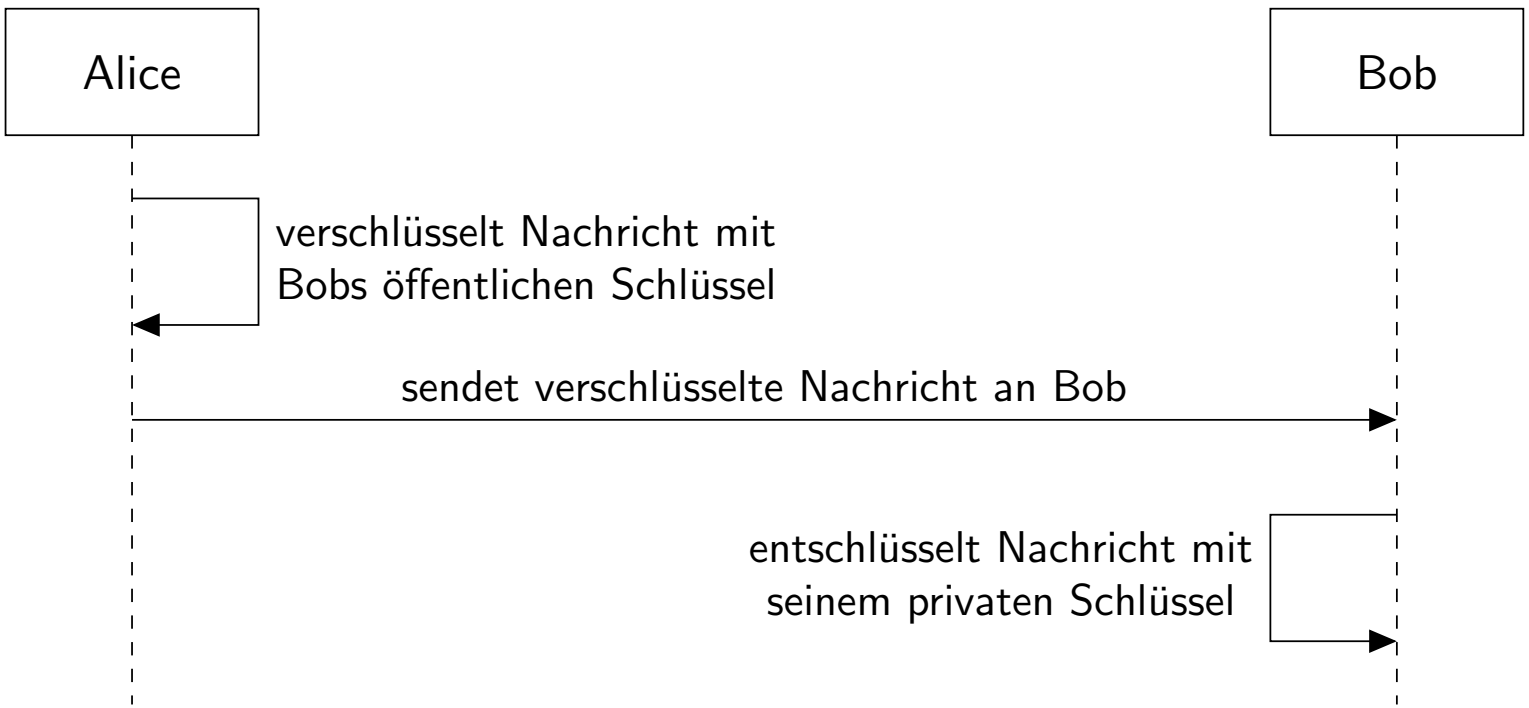


Abbildung : Die Ver- und Entschlüsselung mithilfe eines asymmetrischen Kryptografieverfahrens.

Einwegfunktionen mit Falltür

Zentraler Baustein eines asymmetrischen Krpytografieverfahrens ist eine Einwegfunktion mit *Falltür*.

D.h.:

- $x \to f(x)$ - „relativ“ leicht.
- $f(x) \to x$ - „relativ“ schwierig (ohne Falltürinformation).

Beispiele (u. a.):

- Telefonbuch
- Primfaktorzerlegung

Post-Quantum Kryptografie

RSA basiert auf der Primfaktorzerlegung
$\rightarrow$ mithilfe eines Quantumcomputers in P lösbar.

(Noch nicht effiziente) Alternativen:

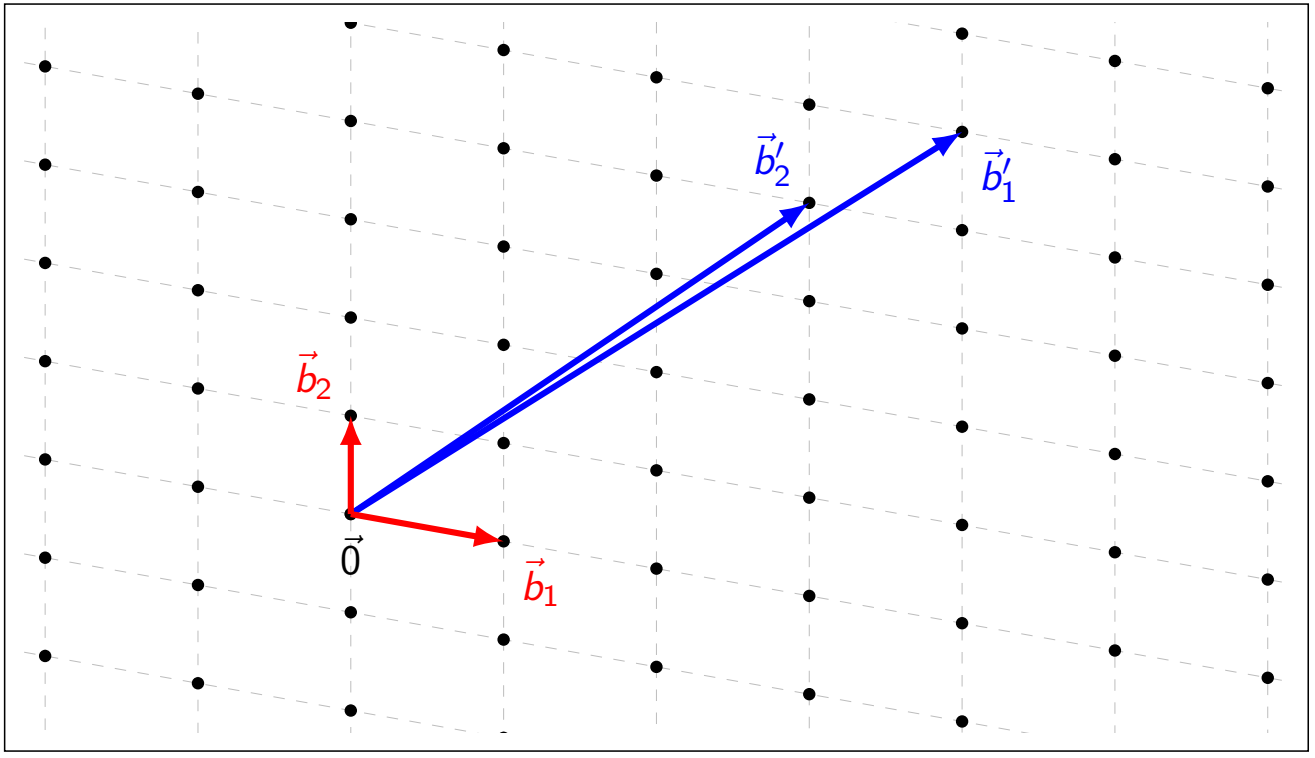
- Hash-basierte Kryptografie
- Codebasierte Kryptografie
- Gitterbasierte Kryptografie

Warum schon heute nach Nachfolger(n) suchen?

Grundlagen

Gittertheorie: Einführung

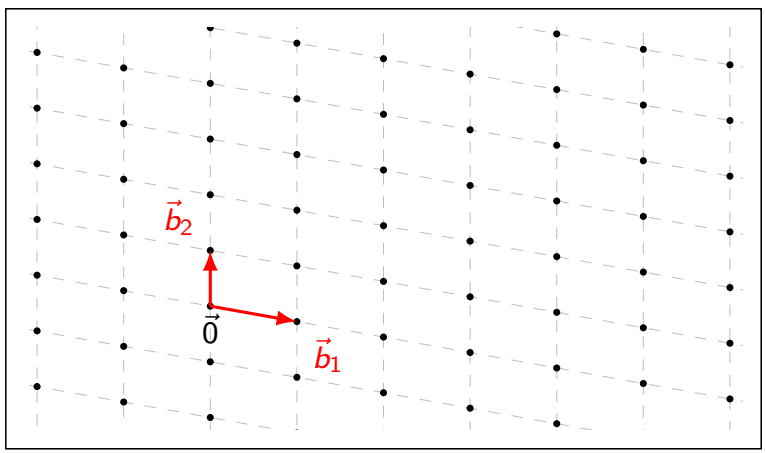
$$\mathcal{L}(\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n) =_{\text{def}} \{x_1\vec{b}_1 + x_2\vec{b}_2 + \cdots + x_n\vec{b}_n\},\ x_1, x_2, \ldots, x_n \in \mathbb{Z}$$



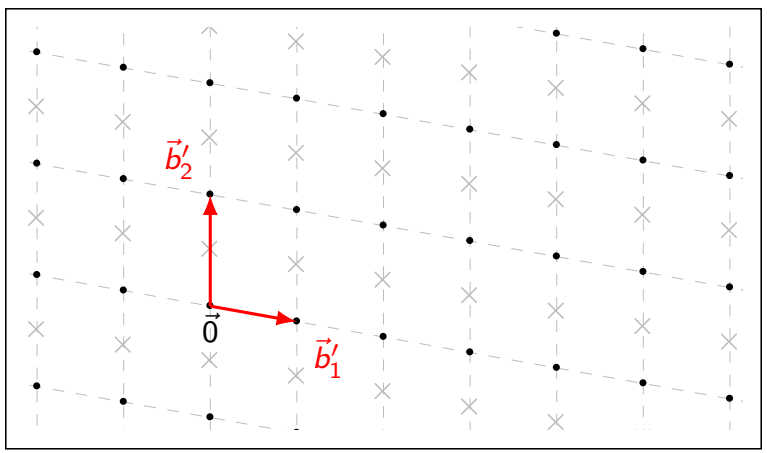
Lineare Hülle: $\text{span}(\mathcal{L}(B)) = \text{span}(B) =_{\text{def}} \{B\vec{q} : \vec{q} \in \mathbb{R}^n\}$.

Gittertheorie: Äquivalenz

Gitter können in Relation stehen:



$\mathcal{L}(B)$

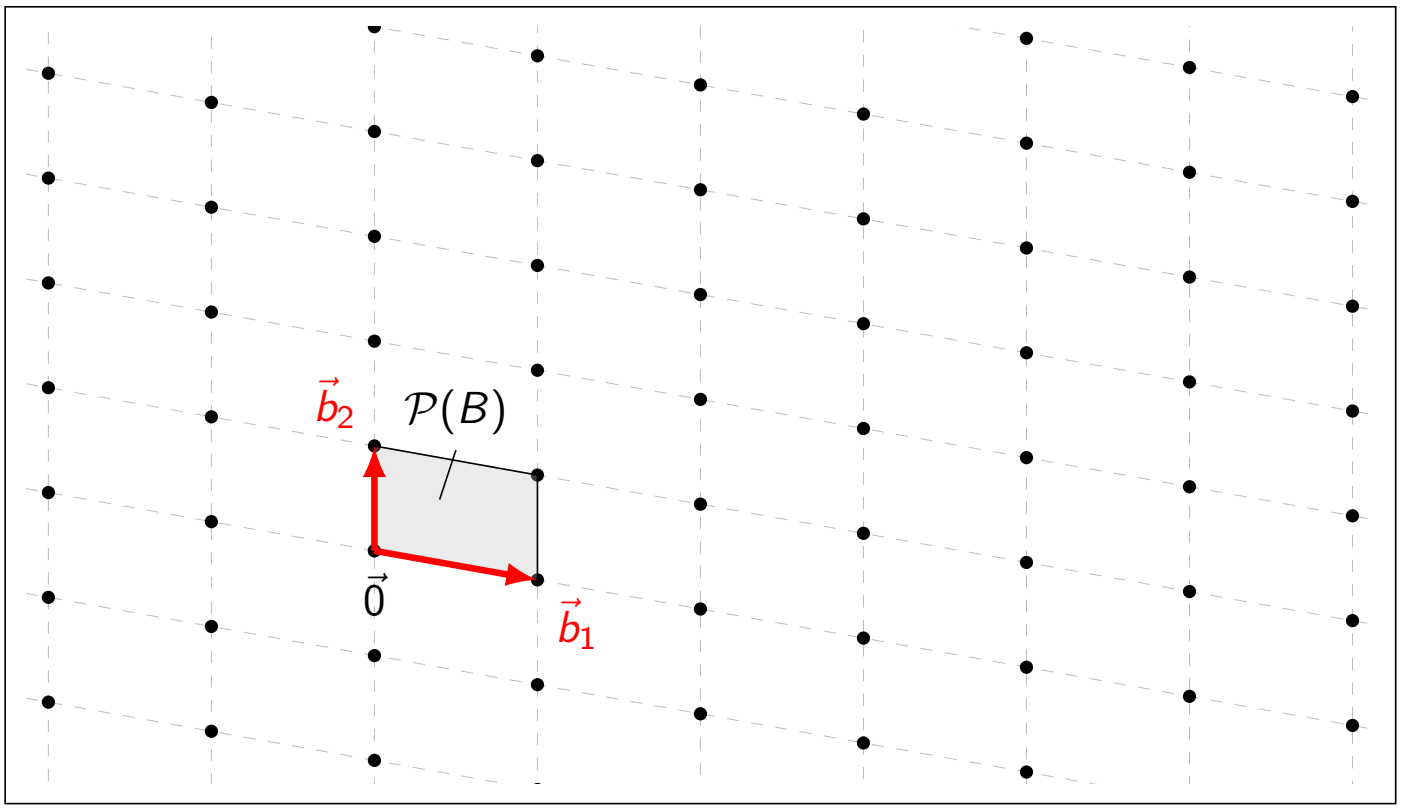


$\mathcal{L}(B')$

Äquivalent, wenn $\mathcal{L}(B) \subseteq \mathcal{L}(B')$ und $\mathcal{L}(B') \subseteq \mathcal{L}(B)$
oder $B = B' \cdot U$ mit $U \in \mathbb{Z}^{n \times n}$ und $|\det(U)| = 1$.

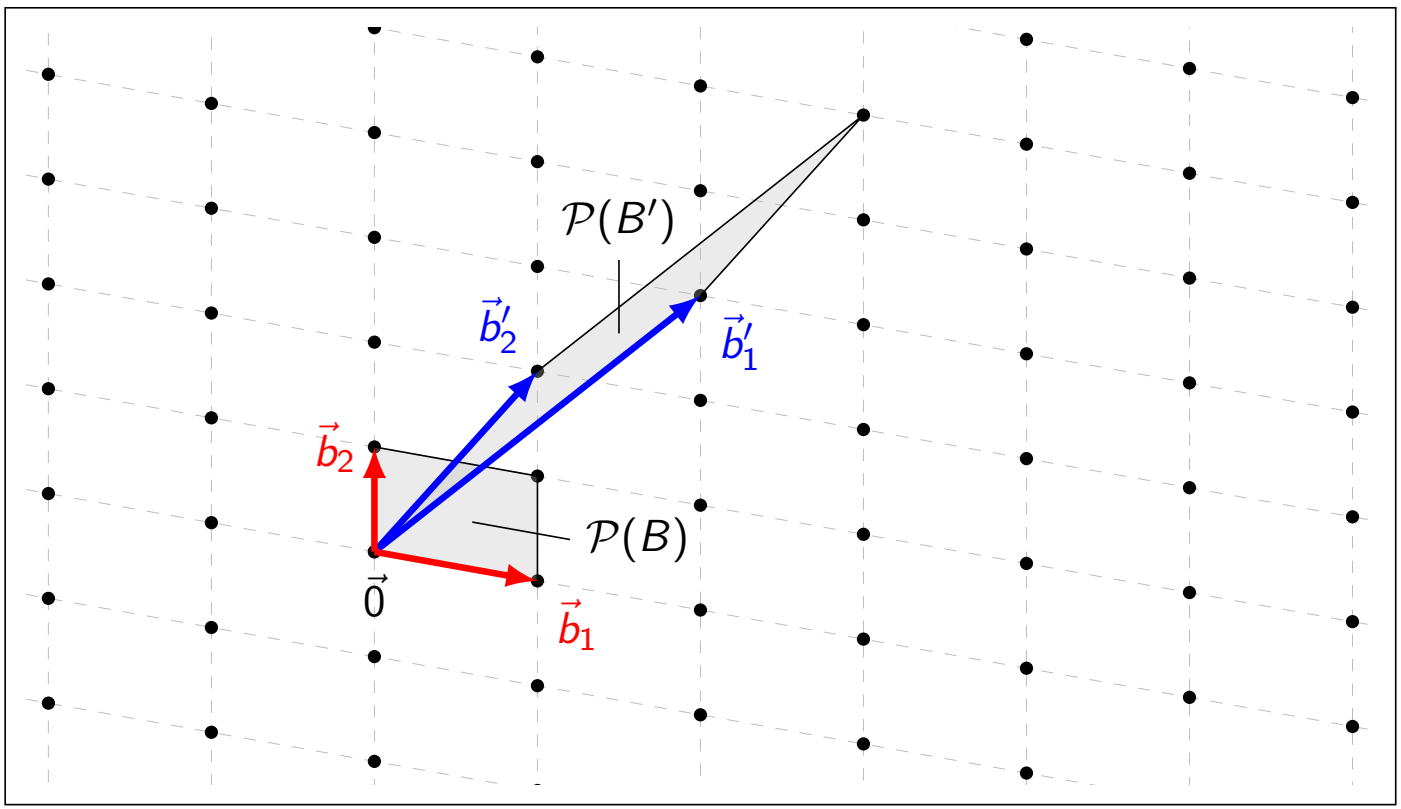
Gittertheorie: Grundmasche

$$\mathcal{P}(B) =_{\text{def}} \{s_1\vec{b}_1 + s_2\vec{b}_2 + \cdots + s_n\vec{b}_n\},\ s_1, s_2, \ldots, s_n \in [0, 1)$$



Gittertheorie: Grundmasche

$$\mathcal{P}(B) =_{\text{def}} \{s_1\vec{b}_1 + s_2\vec{b}_2 + \cdots + s_n\vec{b}_n\},\ s_1, s_2, \ldots, s_n \in [0, 1)$$



Gittertheorie: Grundmasche

Die Grundmasche hat folgende Eigenschaften:

- sie enthält stets genau einen Gittervektor
- sie spannt gemeinsam mit allen Gittervektoren die lineare Hülle des Gittes auf
- sie hat das Volumen $\sqrt{|\det(B^T \cdot B)|}$

Das Volumen der Grundmasche wird auch als Gitterdeterminante $\det(\mathcal{L}(B))$ bezeichnet.

Gittertheorie: Satz von Blichfeldt

Satz

Für jedes Gitter $\mathcal{L}(B)$ *und jede Teilmenge* $S \subseteq \text{span}(B)$ *gilt:*

Wenn S *das Volumen* $\text{vol}(S) > \det(\mathcal{L})$ *besitzt, so müssen mindestens zwei unterschiedliche Vektoren* $\vec{q}_1, \vec{q}_2 \in S$ *existieren, sodass* $\vec{q}_1 - \vec{q}_2 \in (\mathcal{L} \backslash \{\vec{0}\})$ *ist.*

Beweis.

(siehe Thesis) □

Gittertheorie: Satz von Minkowski

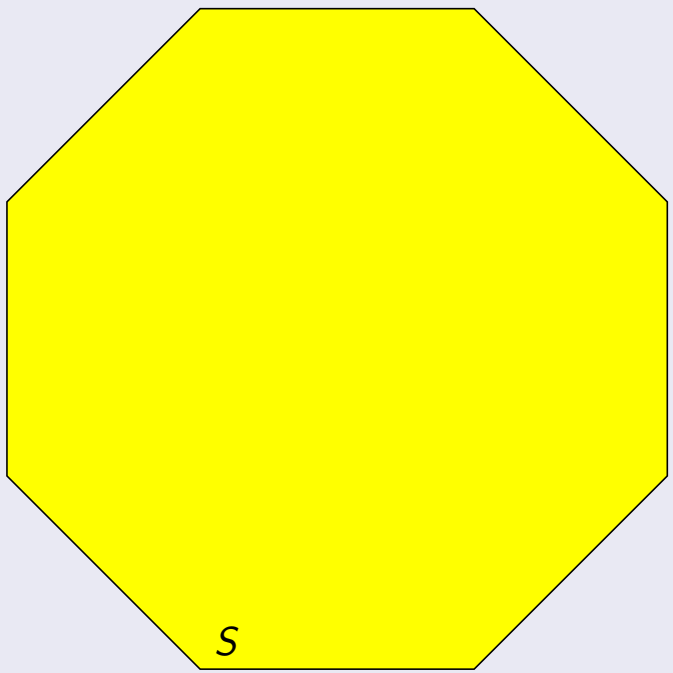
Folgerung

Für jedes Gitter $\mathcal{L}(B)$ *und jede beliebige konvexe Menge* $S \subset \text{span}(B)$, *die symmetrisch um den Ursprung des Gitters* $\mathcal{L}$ *ist, gilt:*

Wenn $\text{vol}(S) > 2^n \det(\mathcal{L})$ *ist, dann enthält* S *mindestens einen Gittervektor* $\vec{v} \in (S \cap \mathcal{L} \backslash \{\vec{0}\})$.

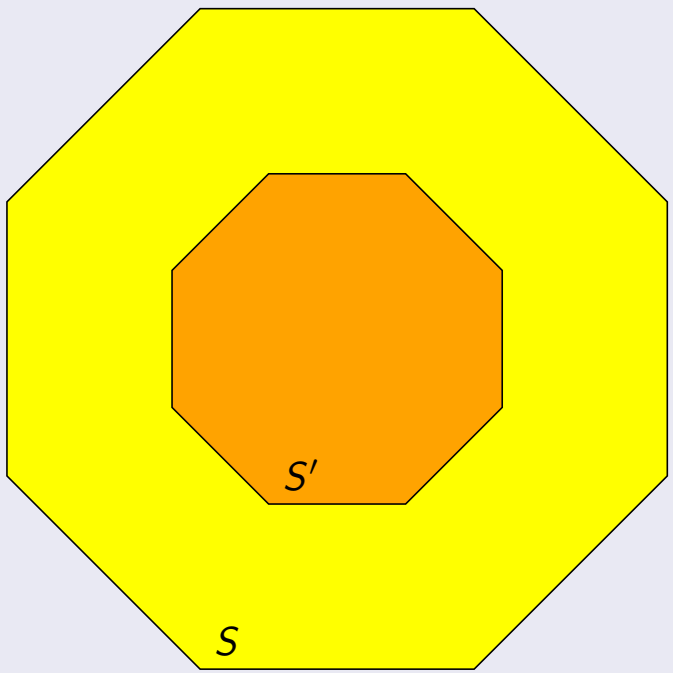
Gittertheorie: Satz von Minkowski

Beweis.



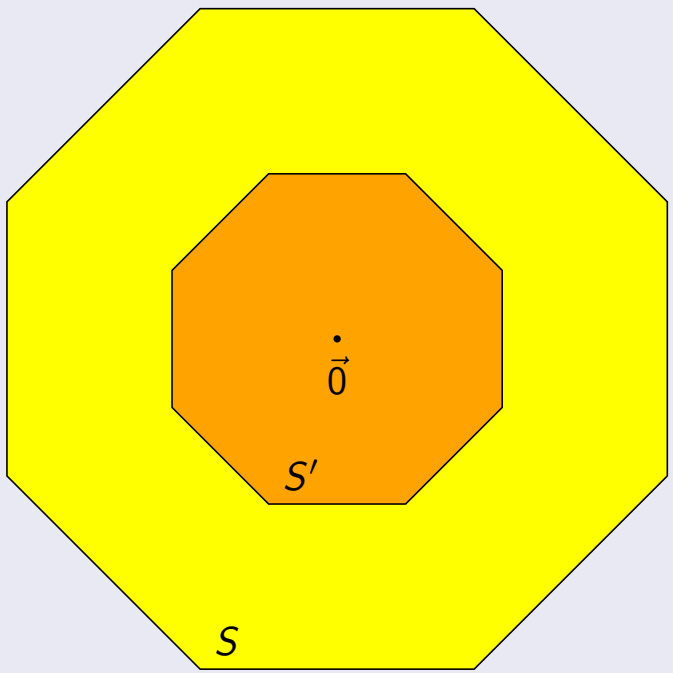
Gittertheorie: Satz von Minkowski

Beweis.



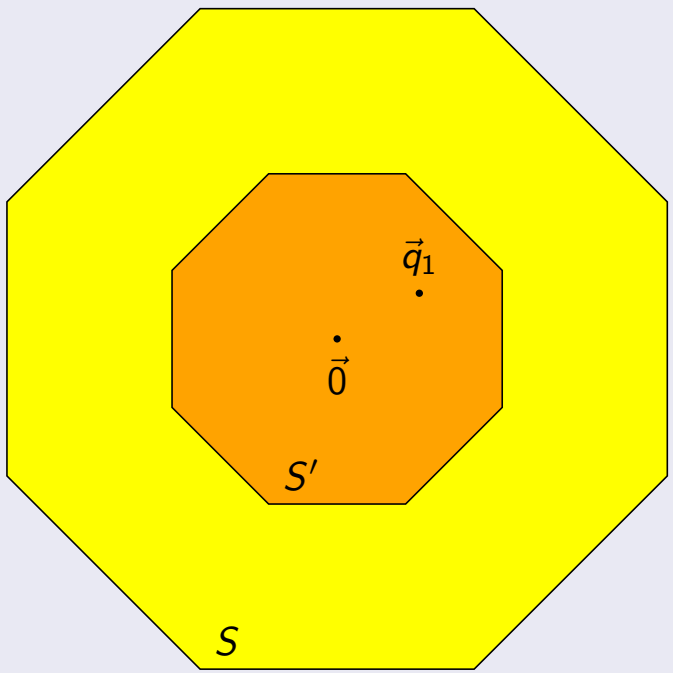
Gittertheorie: Satz von Minkowski

Beweis.



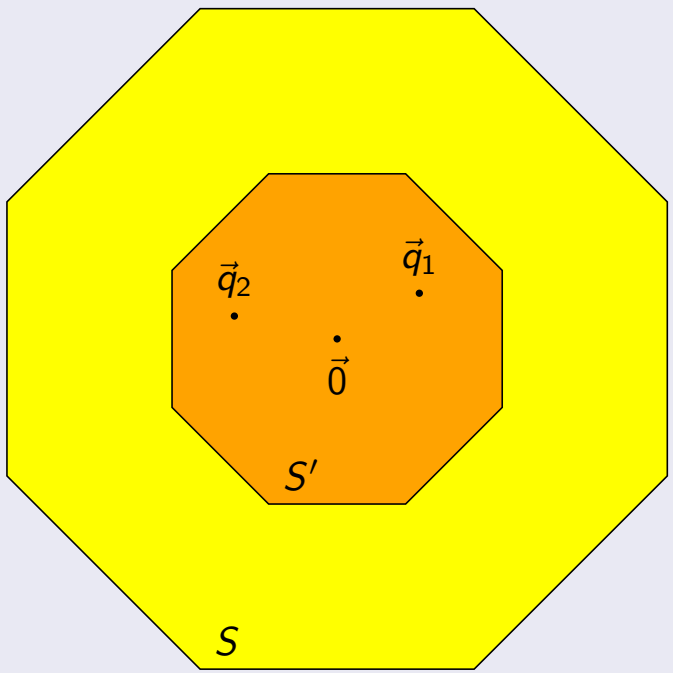
Gittertheorie: Satz von Minkowski

Beweis.



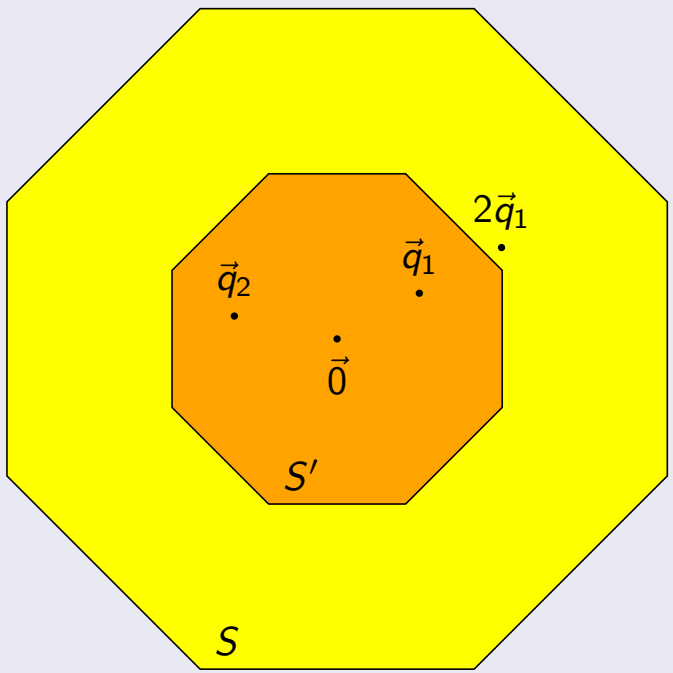
Gittertheorie: Satz von Minkowski

Beweis.



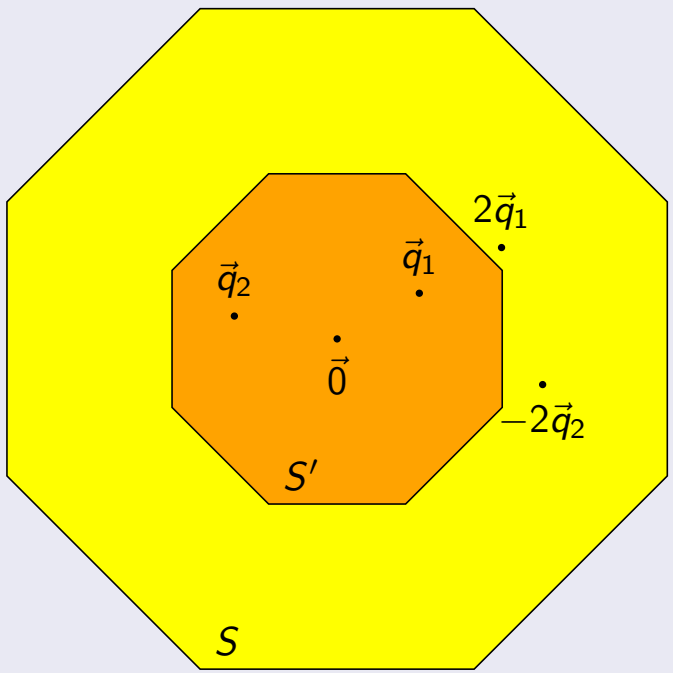
Gittertheorie: Satz von Minkowski

Beweis.



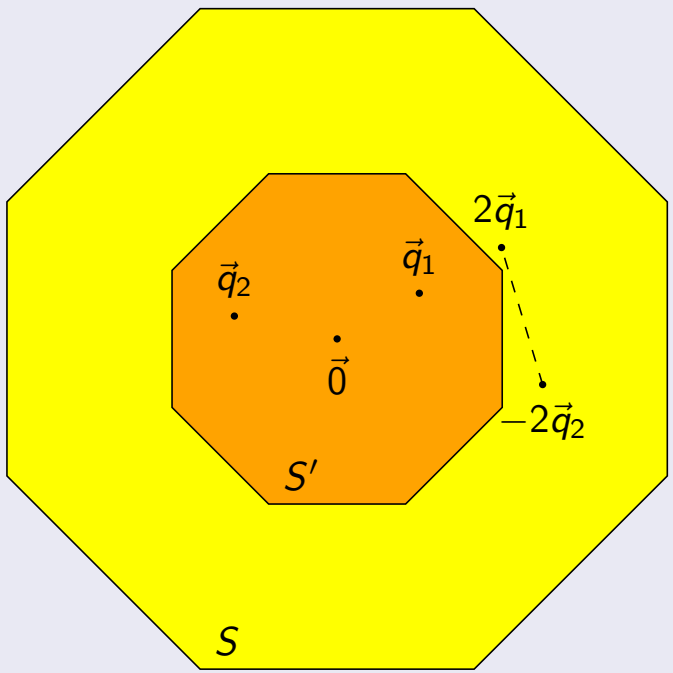
Gittertheorie: Satz von Minkowski

Beweis.



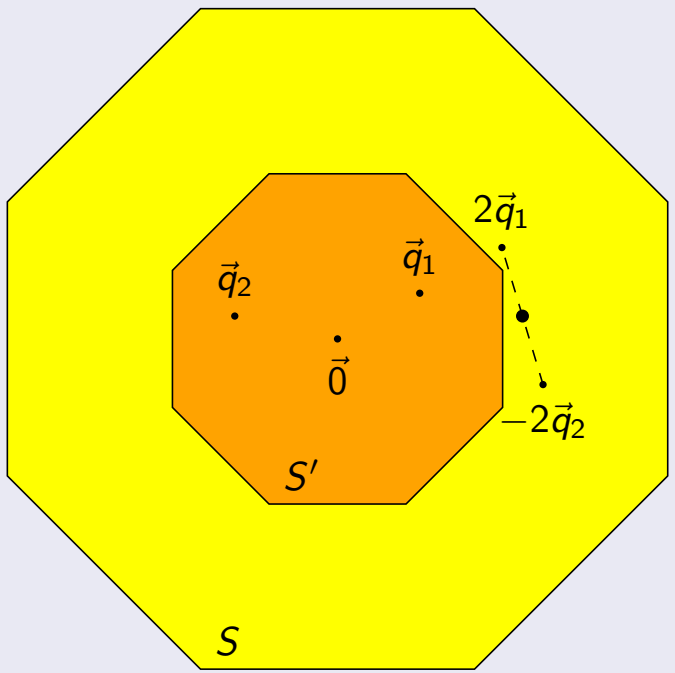
Gittertheorie: Satz von Minkowski

Beweis.



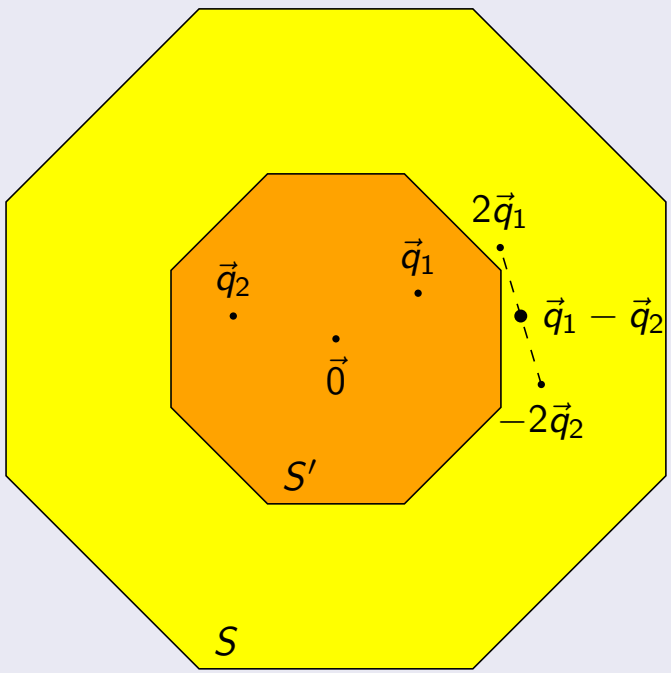
Gittertheorie: Satz von Minkowski

Beweis.



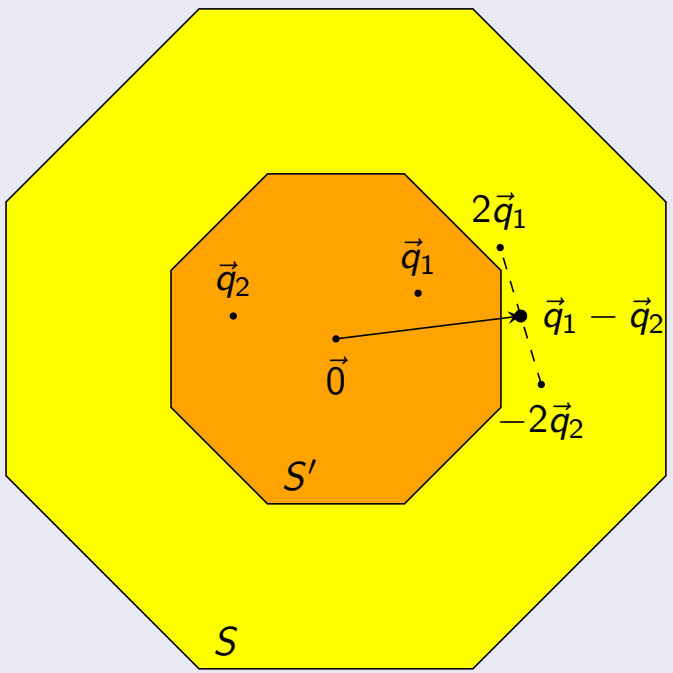
Gittertheorie: Satz von Minkowski

Beweis.



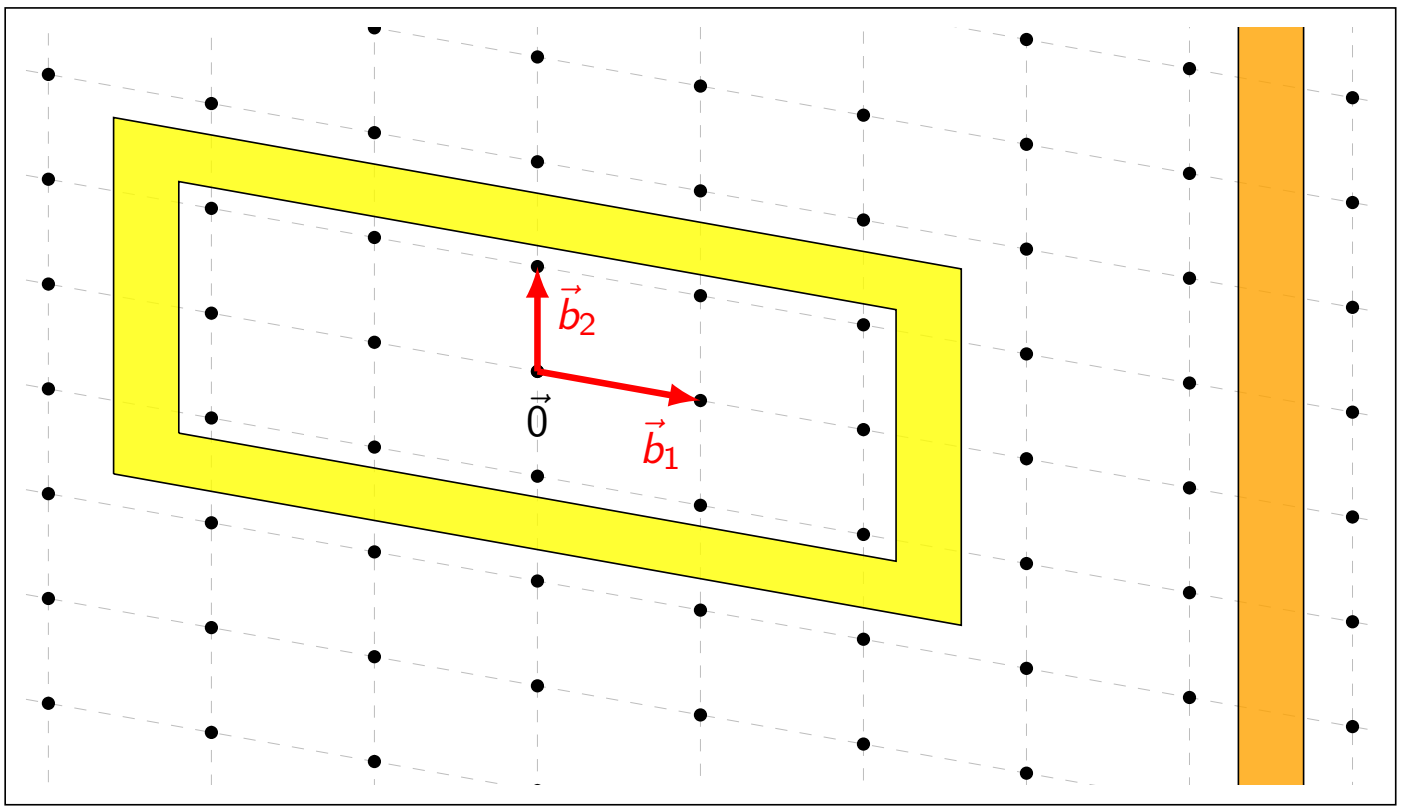
Gittertheorie: Satz von Minkowski

Beweis.



□

Satz von Minkwoski



Distanzen und Längen in Gittern

Distanz von Gittervektoren $\rightarrow$ abhängig von induzierter Norm.

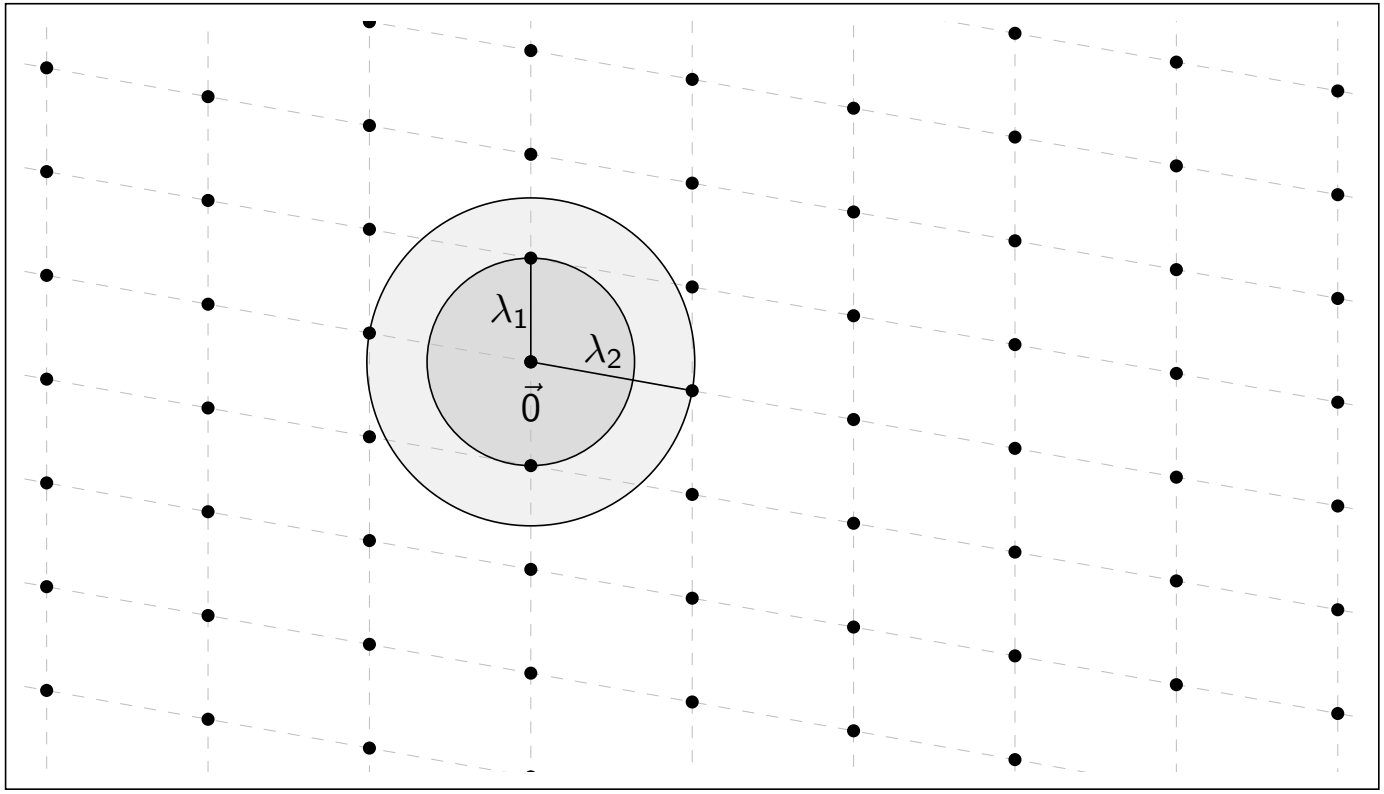
p-Norm für ein Vektor $\vec{v} \in \mathbb{R}^m$ bzw. häufige Spezialfälle:

$$\ell_1(\vec{v}) = \|\vec{v}\|_1 = \sum_{i=1}^{m} |v_i| \quad (\textit{Summennorm})$$

$$\ell_2(\vec{v}) = \|\vec{v}\| = \sqrt[2]{\sum_{i=1}^{m} |v_i|^2} \quad (\textit{Euklidische Norm})$$

$$\ell_\infty(\vec{v}) = \|\vec{v}\|_\infty = \lim_{p \to \infty} \|\vec{v}\|_p = \max_{i=1}^{m} |v_i| \quad (\textit{Maximumsnorm})$$

Die Konstanten $\lambda_1, \lambda_2, \ldots, \lambda_n$ heißen sukzessive Minima (des Gitters) und λ_1 entspricht dem kürzesten Vektor (im Gitter).



Folgerung

Sei $\mathcal{L}$ ein Gitter, so gilt: $\lambda_1 < \sqrt{n} \cdot \sqrt[n]{\det(\mathcal{L})}$.

Gram-Schmidt Orthogonalisierung

Satz

Die Basisvektoren $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n \in \mathbb{R}^m$ *des Gitters* $\mathcal{L}(\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n)$ *können durch*

$$\vec{o}_i = \vec{b}_i - \sum_{j=1}^{i-1} p_{\vec{o}_j}(\vec{b}_i)\,,\ p_{\vec{o}_j}(\vec{b}_i) = \frac{\langle \vec{b}_i, \vec{o}_j \rangle}{\langle \vec{o}_j, \vec{o}_j \rangle} \vec{o}_j \text{ und } i \in \{1, 2, \ldots, n\},$$

in eine Orthogonalbasis $\vec{o}_1, \vec{o}_2, \ldots, \vec{o}_n$ *(von* $\mathbb{R}^m$*) transformiert werden.*

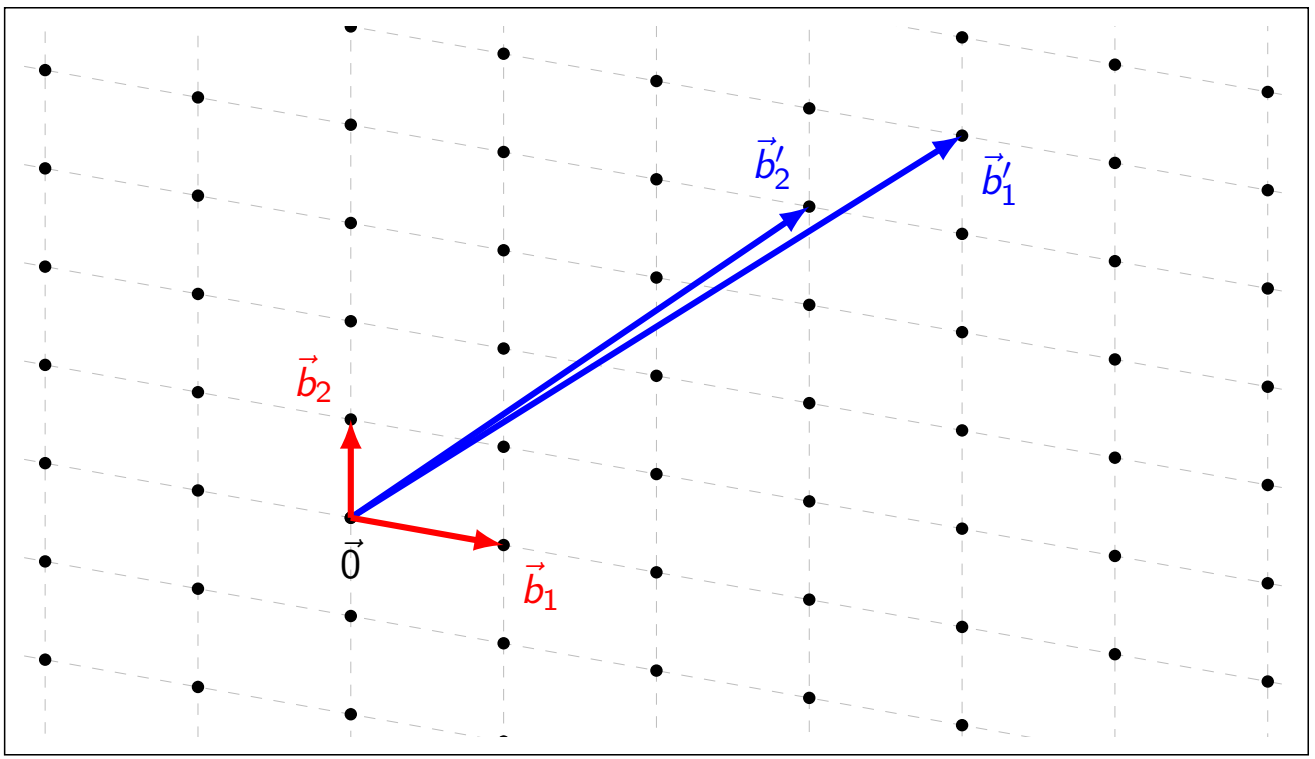
Beweis.

(siehe bel. Lineare Algebra-Buch) □

Berechnungsprobleme in Gittern

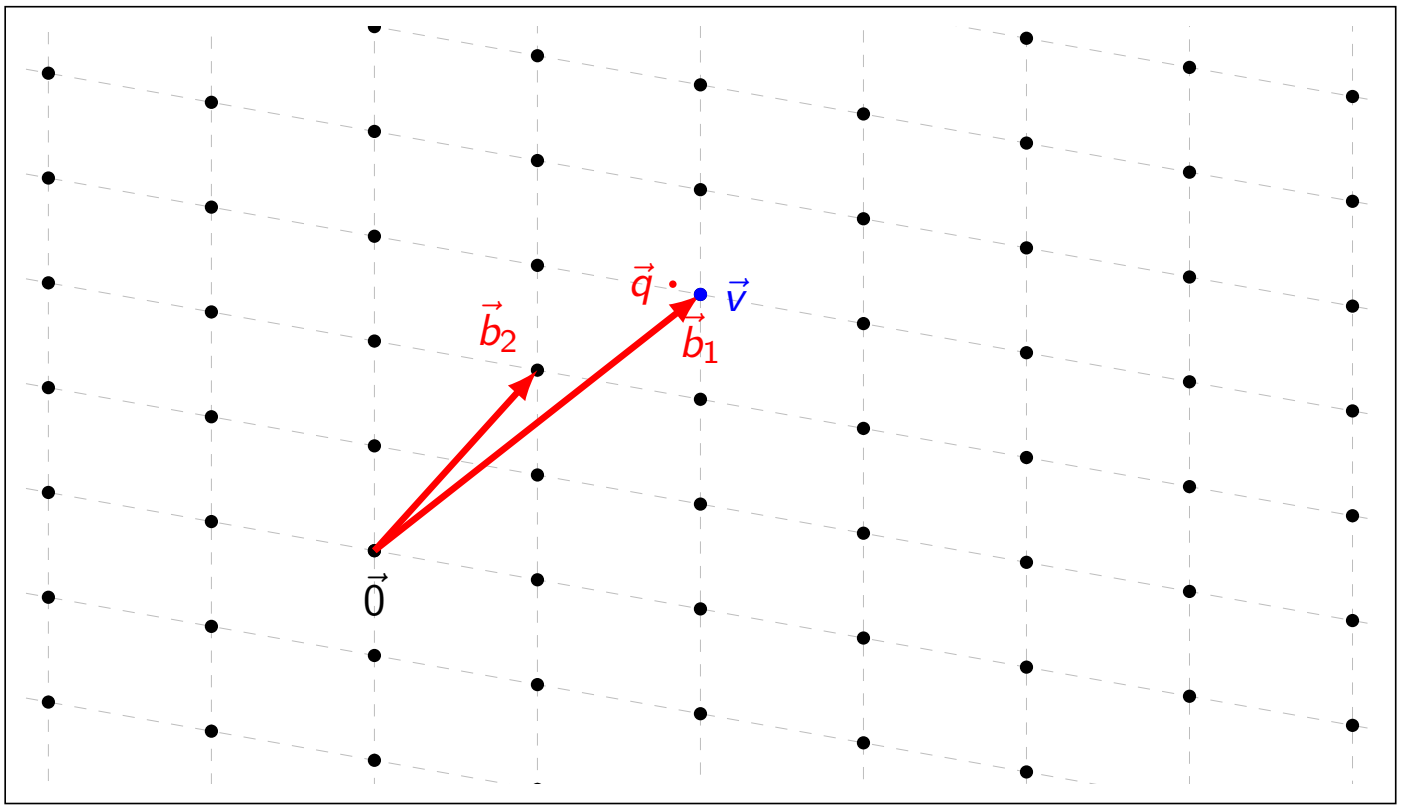
Effiziente Gitterprobleme - u. a.:

- MEMBERSHIP
- LENGTH
- DISTANCE



Das Closest Vector Problem (CVP)

Gegegeben: Basis $B \in \mathbb{Q}^{m \times n}$ mit $m \geq n$, Vektor $\vec{q} \in \text{span}(B)$.
Gesucht: Vektor $\vec{v} \in \mathcal{L}$, sodass $\|\vec{q} - \vec{v}\|$ minimal.



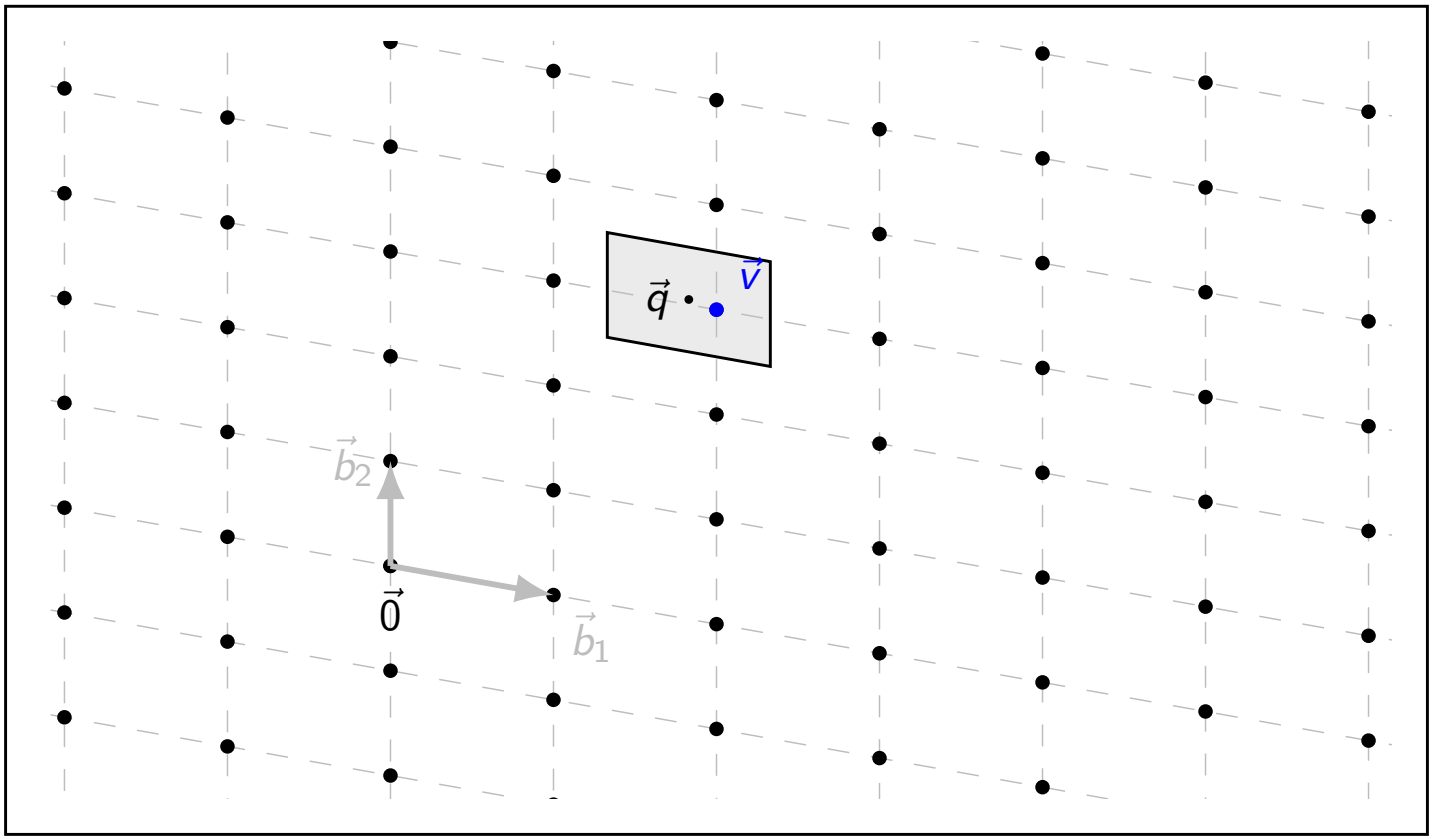
Im allgemeinen Fall ein „schwieriges“ Problem.

CVP-Approximation

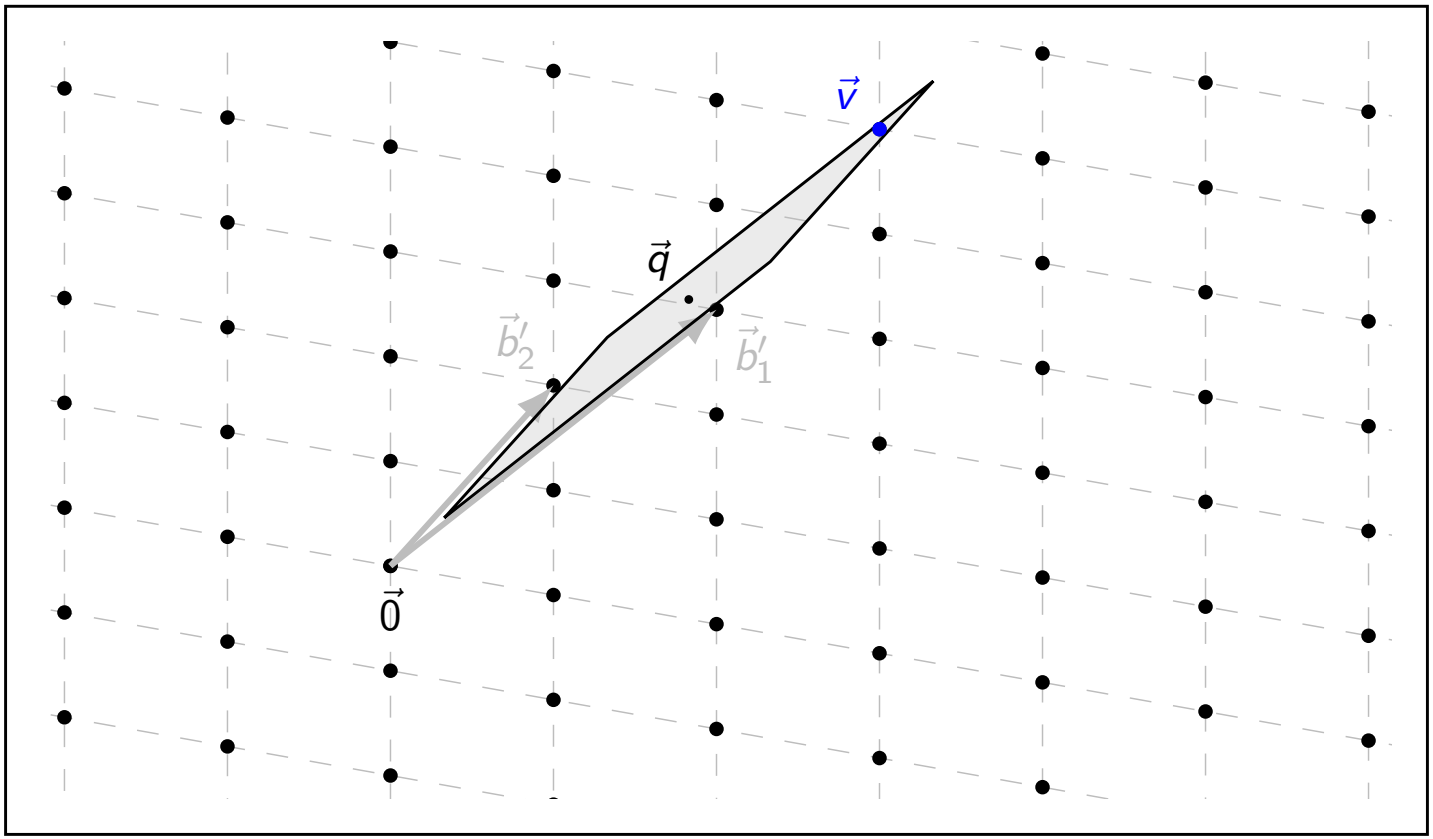
Eingabe : Basis $B \in \mathbb{Q}^{m \times n}$ mit $m \geq n$ und Vektor $\vec{q} \in \text{span}(B)$.
Ausgabe : Gittervektor $\vec{v} \in \mathcal{L}$.

1 *Berechne* $r_1, r_2, \ldots, r_n \in \mathbb{R}$, *sodass* $\vec{q} = r_1\vec{b}_1 + r_2\vec{b}_2 + \cdots + r_n\vec{b}_n$.
2 $\vec{v} \leftarrow \vec{0}$
3 **for** $i = 1, 2, \ldots, n$ **do**
4 $\quad \vec{v} \leftarrow \vec{v} + \lfloor r_i \rceil \cdot \vec{b}_i$
5 **end for**

Babais ROUNDING OFF PROCEDURE

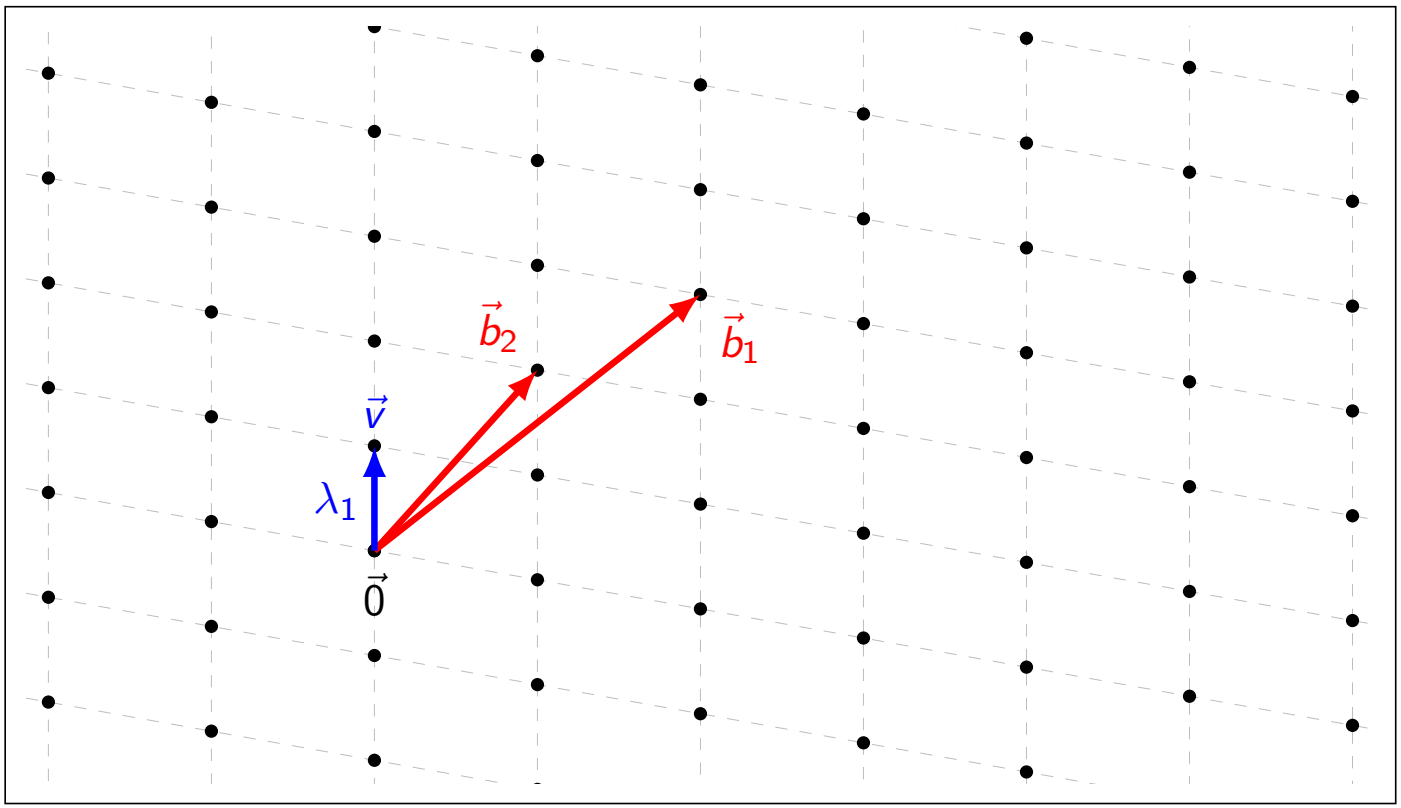


Babais ROUNDING OFF PROCEDURE



Das Shortest Vector Problem (SVP)

Gegegeben: Basis $B \in \mathbb{Q}^{m \times n}$ mit $m \geq n$.
Gesucht: Vektor $\vec{v} \in \mathcal{L}$, sodass $\|\vec{v}\| = \lambda_1$.



Im allgemeinen Fall auch ein „schwieriges“ Problem.

SVP-Approximation

Idee: lange nichtorthogonale Basisvektoren
$\rightarrow$ kurze orthogonale Basisvektoren.

Längenreduziertheit

Basisvektoren $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n$, Gram-Schmidt Basisvektoren $\vec{o}_1, \vec{o}_2, \ldots, \vec{o}_n$ und $0 < j < i \leq n$:

$$\left| \frac{\langle \vec{b}_i, \vec{o}_j \rangle}{\langle \vec{o}_j, \vec{o}_j \rangle} \right| \leq \frac{1}{2}$$

. . . äquivalent zu . . .

$$\|\vec{b}_i\| \leq \|\vec{b}_i \pm \vec{o}_j\|$$

Längenreduktion

Eingabe : Basisvektoren $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n \in \mathbb{Q}^m$ und Gram-Schmidt Basisvektoren $\vec{o}_1, \vec{o}_2, \ldots, \vec{o}_n \in \mathbb{Q}^m$

Ausgabe : Längenreduzierte Basis $\vec{b}'_1, \vec{b}'_2, \ldots, \vec{b}'_n \in \mathbb{Q}^m$

1 **for** $i = 2, 3, \ldots, n$ **do**
2 **for** $j = (i-1), (i-2), \ldots, 1$ **do**
3 $\vec{b}_i \leftarrow \vec{b}_i - \left\lceil \frac{\langle \vec{b}_i, \vec{o}_j \rangle}{\langle \vec{o}_j, \vec{o}_j \rangle} \right\rfloor \cdot \vec{b}_j$
4 **end for**
5 **end for**

SVP-Approximation

Idee: Erweiterung der Längenreduziertheit um eine Längenbegrenzung.

LLL-Reduziertheit ...

...enthält neben Längenreduziertheit noch:

$$\left\| \vec{o}_i + \frac{\langle \vec{b}_i, \vec{o}_{i-1} \rangle}{\langle \vec{o}_{i-1}, \vec{o}_{i-1} \rangle} \vec{o}_{i-1} \right\|^2 \geq \frac{3}{4} \|\vec{o}_{i-1}\|^2$$

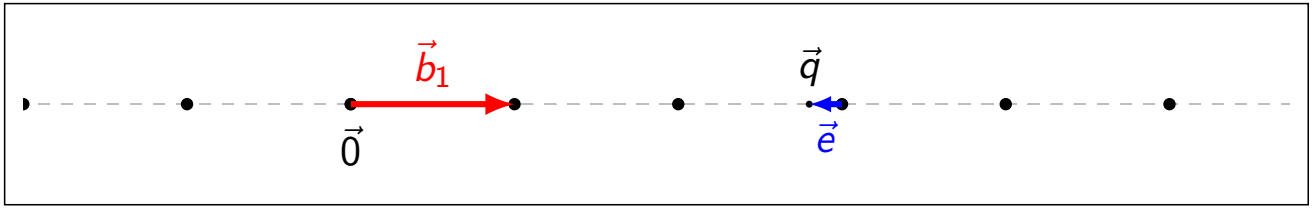
...äquivalent zu ...

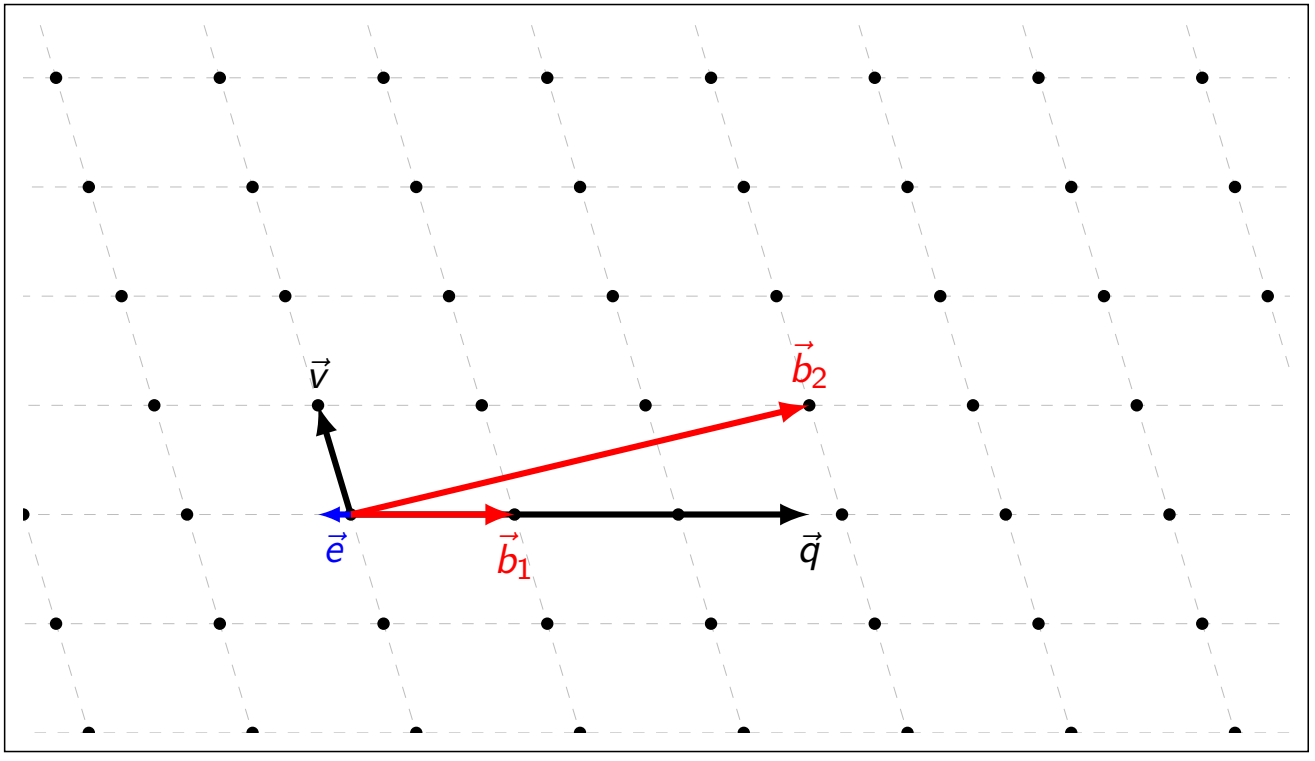
$$\|\vec{o}_i\|^2 \geq \left(\frac{3}{4} - \left(\frac{\langle \vec{b}_i, \vec{o}_{i-1} \rangle}{\langle \vec{o}_{i-1}, \vec{o}_{i-1} \rangle} \right)^2 \right) \|\vec{o}_{i-1}\|^2$$

Eingabe : Basisvektoren $\vec{b}_1, \vec{b}_2, \ldots, \vec{b}_n \in \mathbb{Q}^m$.
Ausgabe : LLL-reduzierte Basisvektoren $\vec{b}'_1, \vec{b}'_2, \ldots, \vec{b}'_n \in \mathbb{Q}^m$.

1 $i \leftarrow 2$
2 $\vec{o}_1 \leftarrow \vec{b}_1$
3 **while** $i \leq n$ **do**
4 **for** $j = (i-1), (i-2), \ldots, 1$ **do**
5 $\vec{b}_i = \vec{b}_i - \left\lfloor \langle \vec{b}_i, \vec{o}_j \rangle / \langle \vec{o}_j, \vec{o}_j \rangle \right\rceil \cdot \vec{b}_j$
6 **end for**
7 **if** $\left\| \vec{o}_i + \langle \vec{b}_i, \vec{o}_{i-1} \rangle / \langle \vec{o}_{i-1}, \vec{o}_{i-1} \rangle \vec{o}_{i-1} \right\|^2 \geq \frac{3}{4} \|\vec{o}_{i-1}\|^2$ **then**
8 $i \leftarrow i + 1$
9 **else**
10 *tausche* $\vec{b}_{i-1}$ *mit* $\vec{b}_i$
11 $i \leftarrow \max(i-1, 2)$
12 **end if**
13 **end while**

Einbettungstechnik ($\mathrm{CVP}^n \rightarrow \mathrm{SVP}^{n+1}$)





Komplexität der Gitterprobleme

Komplexitätstheoretische Analyse (Zusammenfassung)

Komplexitätstheoretische Ergebnisse (u. a.):

- CVP ist NP-hart
- SVP_∞ ist NP-hart (offen für beliebige Norm)
- SVP ist NP-hart (unter randomisierten Reduktionen)

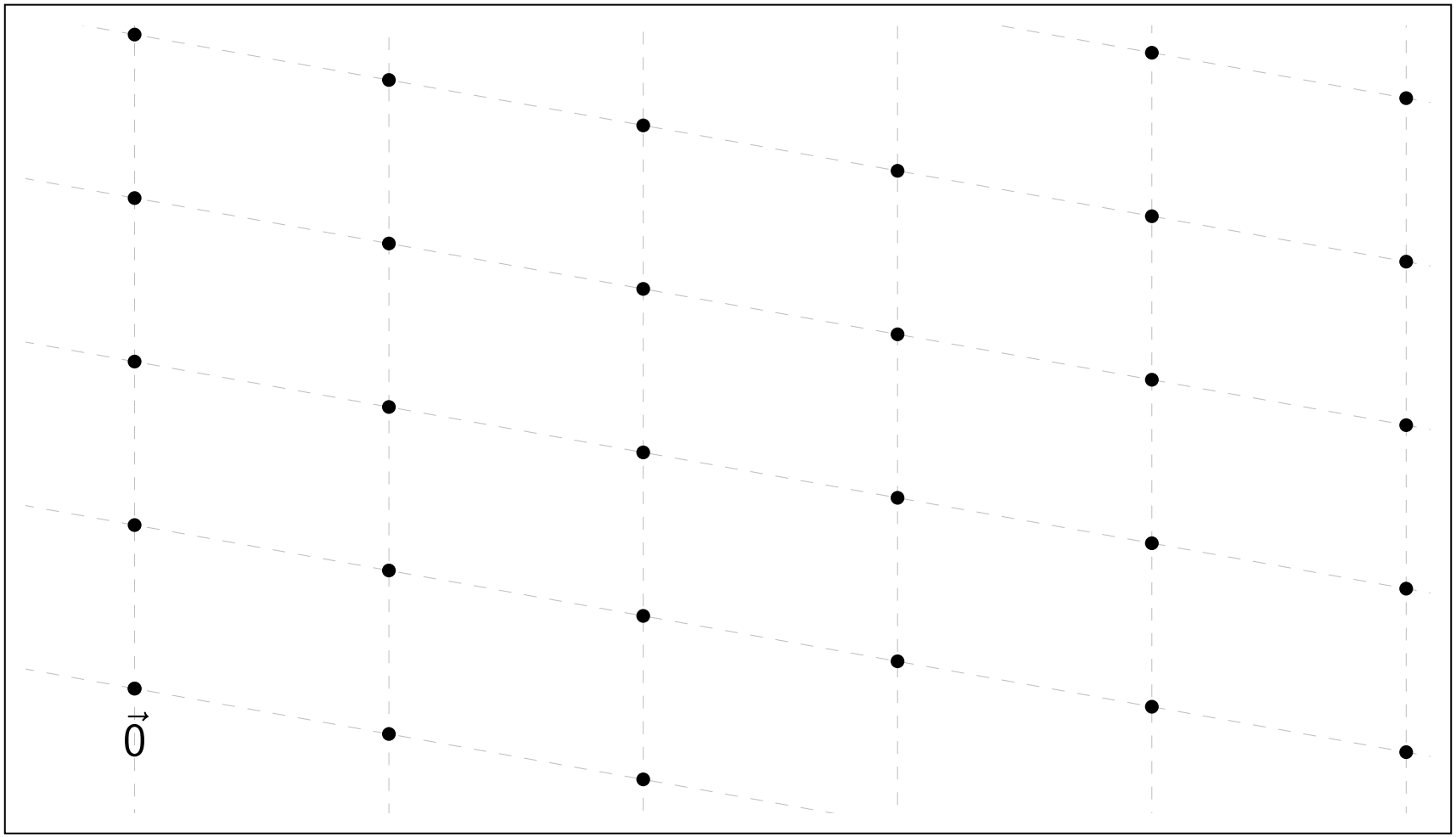
Miklos Ajtai hat 1996 folgende Reduktion gezeigt:

Satz

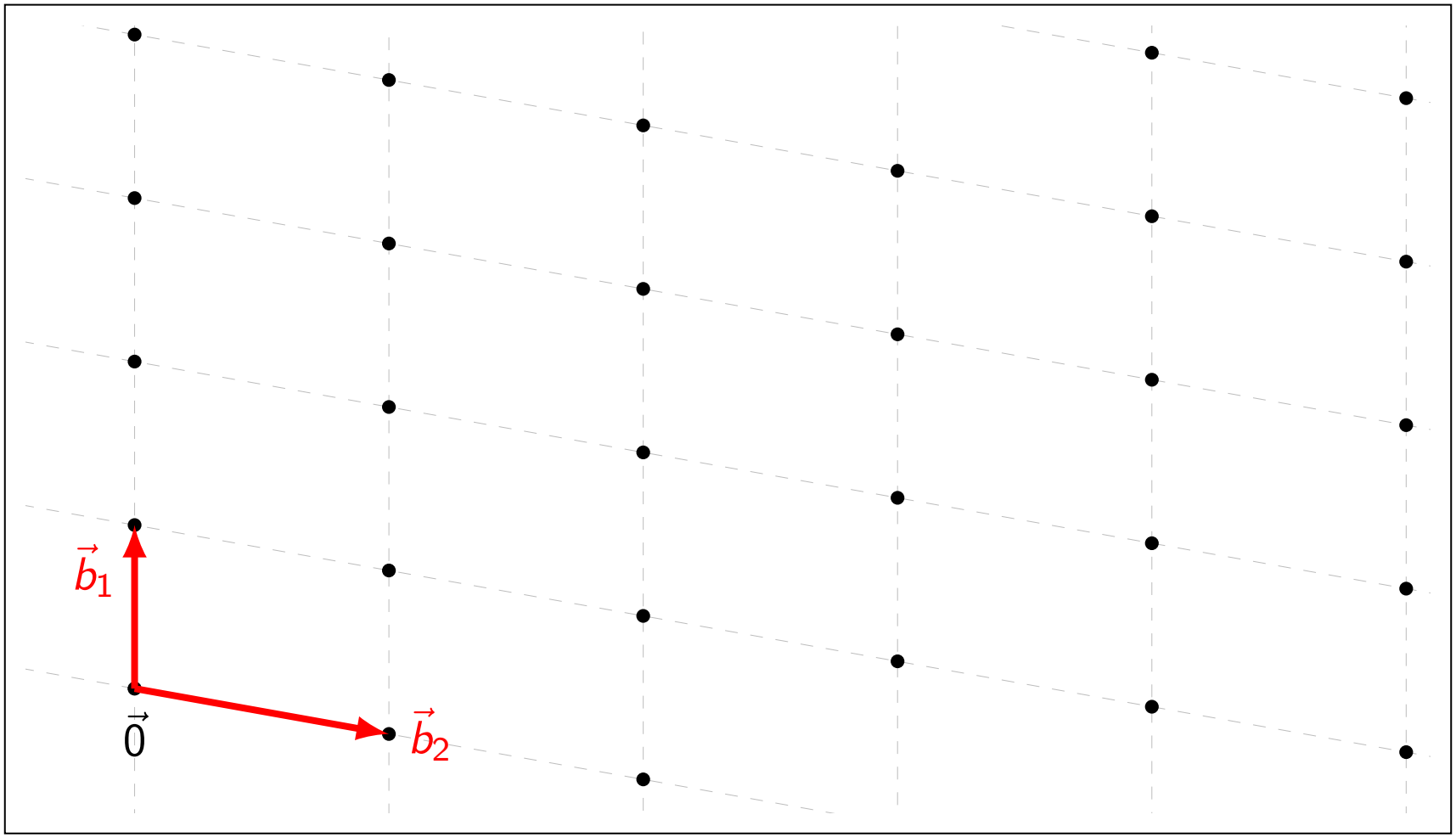
Sei $m, n, q \in \mathbb{N}$ *mit* $n \log(q) < m < \frac{q}{2n^4}$ *und* $q \in \mathcal{O}(n^c)$, *wobei* $c > 0$ *eine Konstante ist, dann erzeugt die Menge* $\{\vec{v} : M\vec{v} \equiv 0 \mod q\}$, *wobei* $M \in \mathbb{Z}_q^{n \times m}$ *mit* $m \geq n$ *eine bestimmte Klasse von Gittern* $\mathcal{L}(B)$, *in denen* ${}^*SIVP^n_{p(n)} \leq_t^p 1SVP^m$ *mit* $\gamma(n) \in \mathcal{O}(n^d)$, *wobei* d *eine Konstante ist, gilt.*

Gitterbasierte Kryptografieverfahren

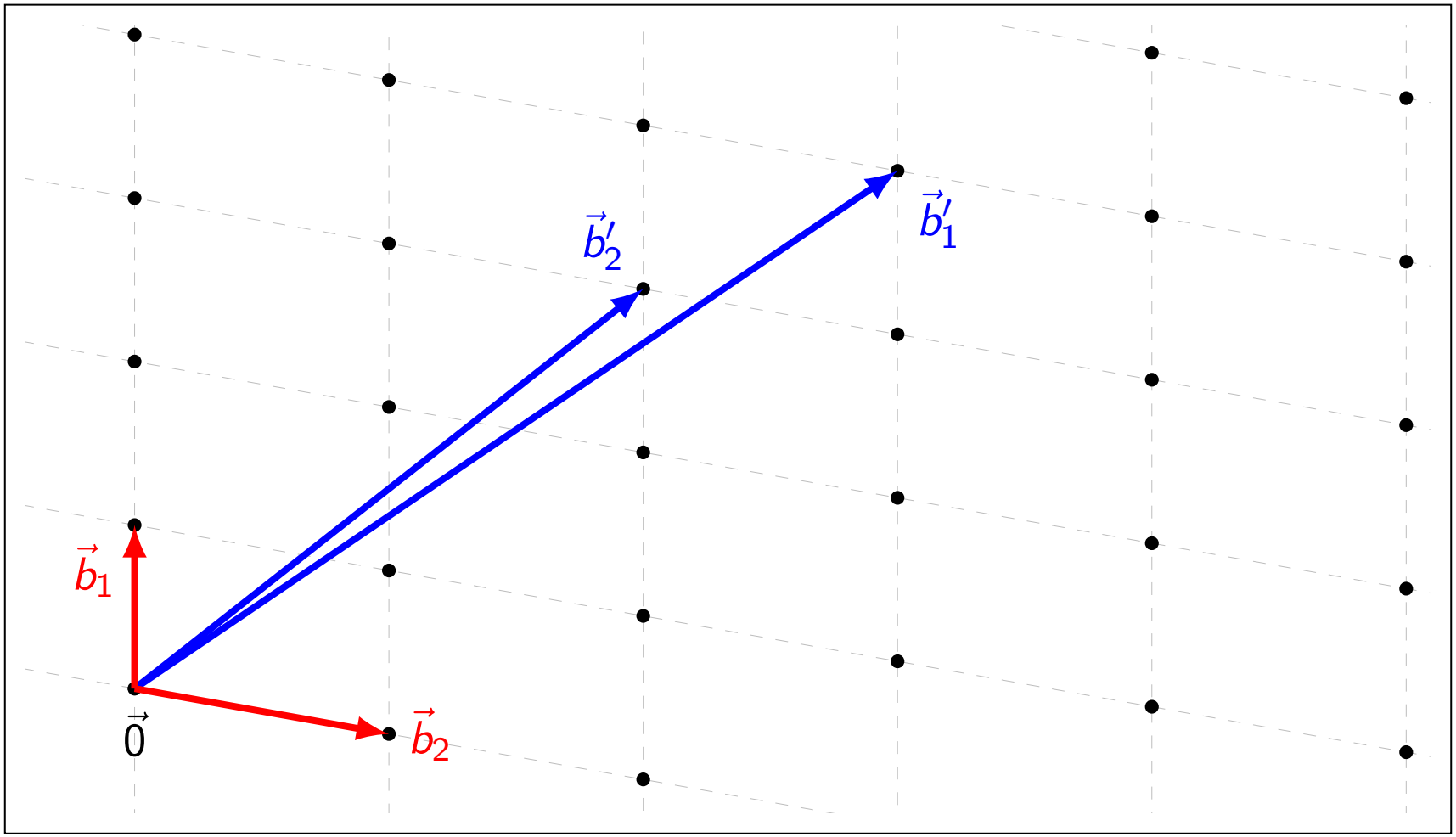
GGH-Kryptografieverfahren



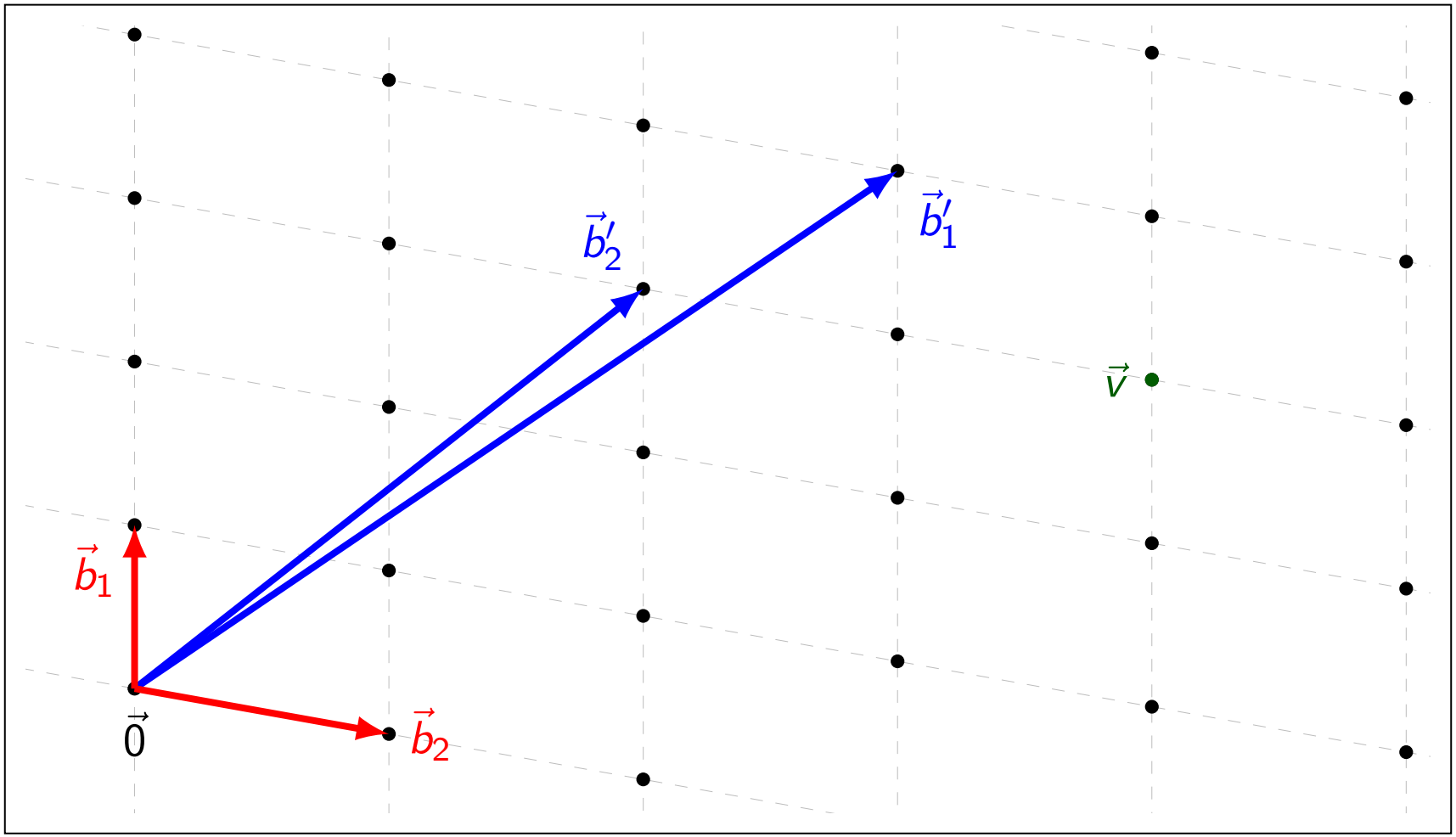
GGH-Kryptografieverfahren



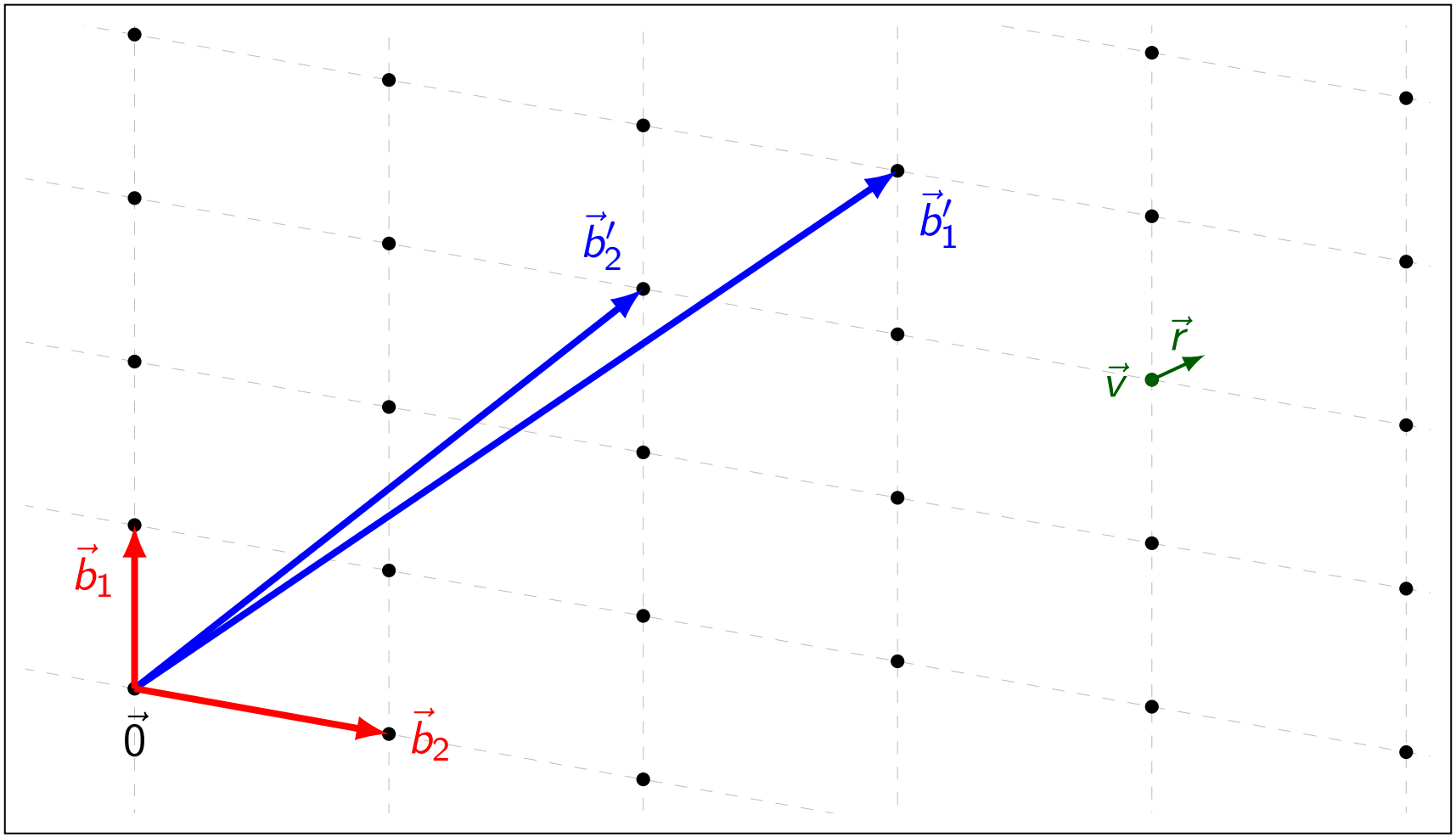
GGH-Kryptografieverfahren



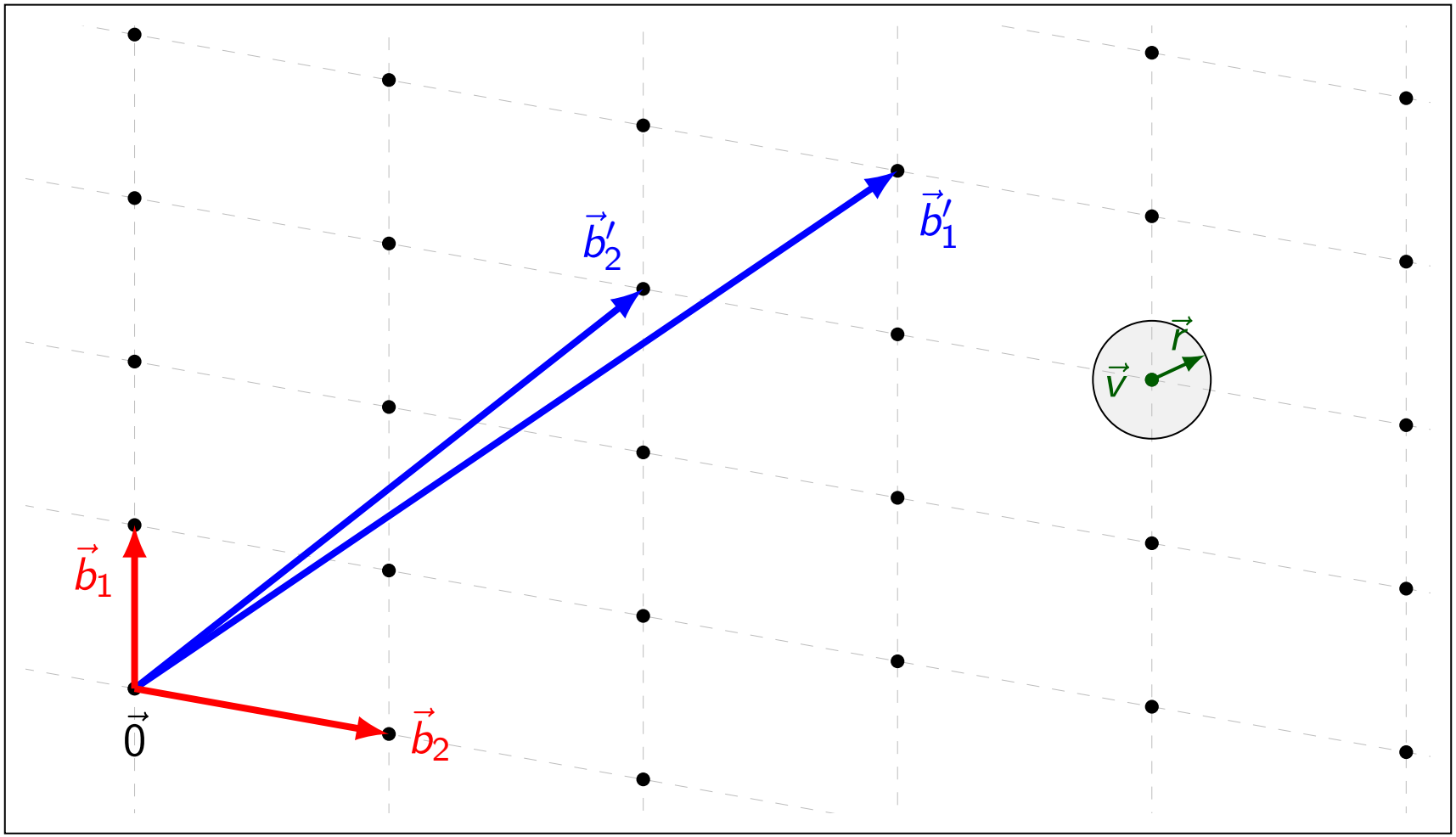
GGH-Kryptografieverfahren



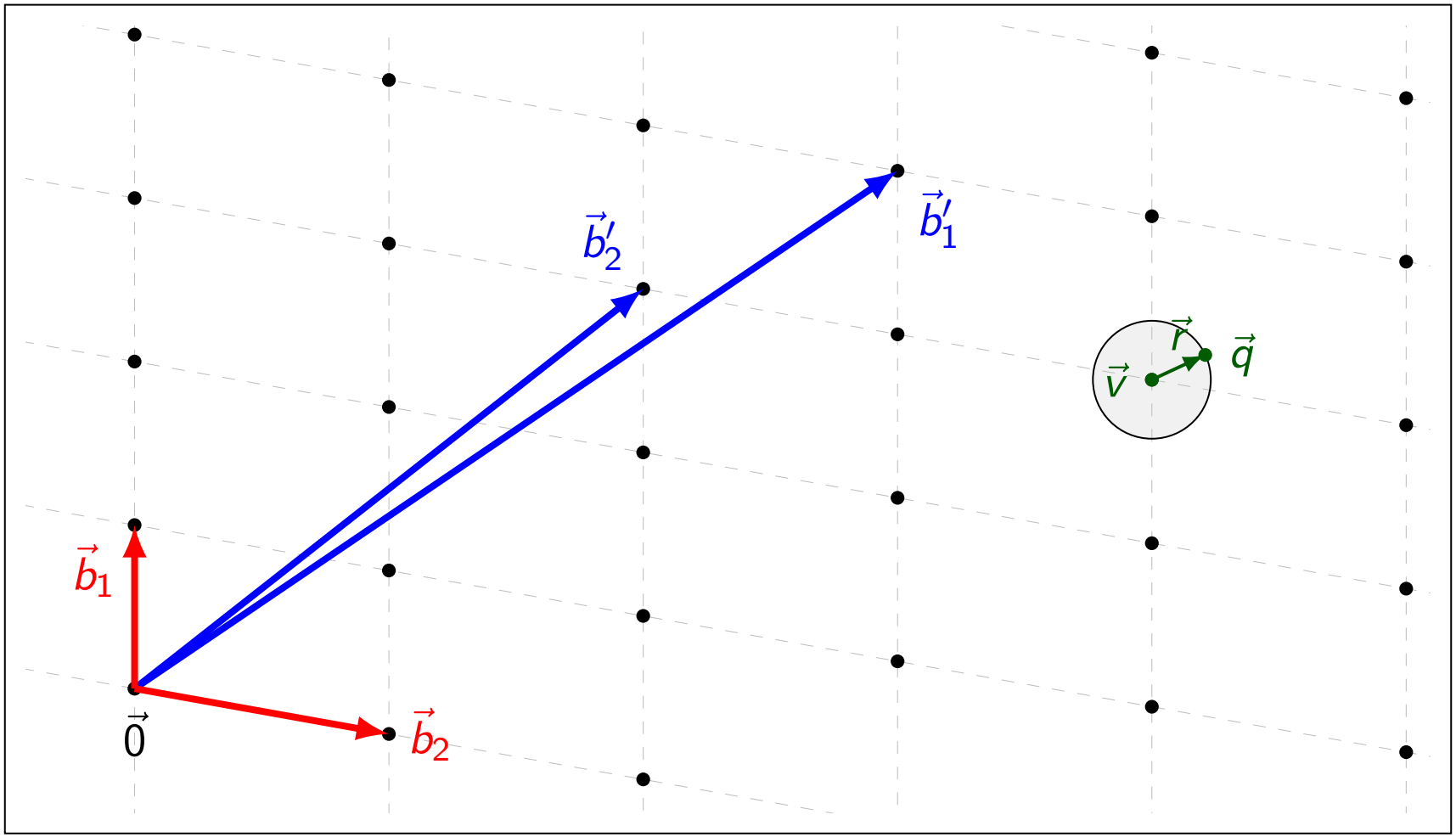
GGH-Kryptografieverfahren



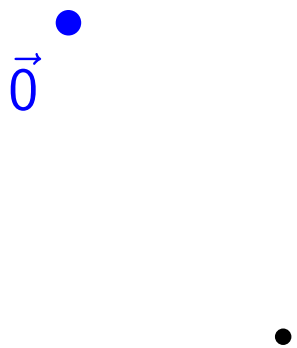
GGH-Kryptografieverfahren



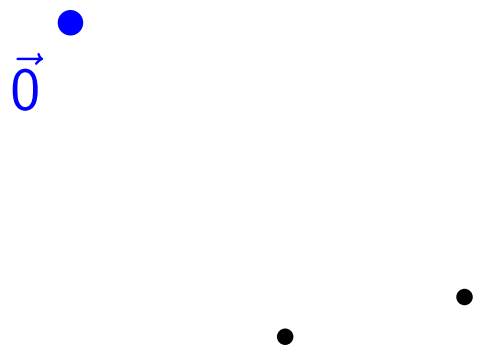
GGH-Kryptografieverfahren



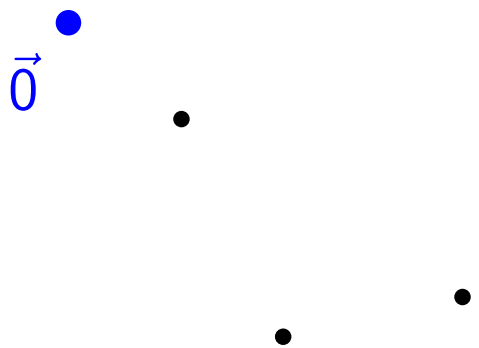
GGH-Signaturverfahren



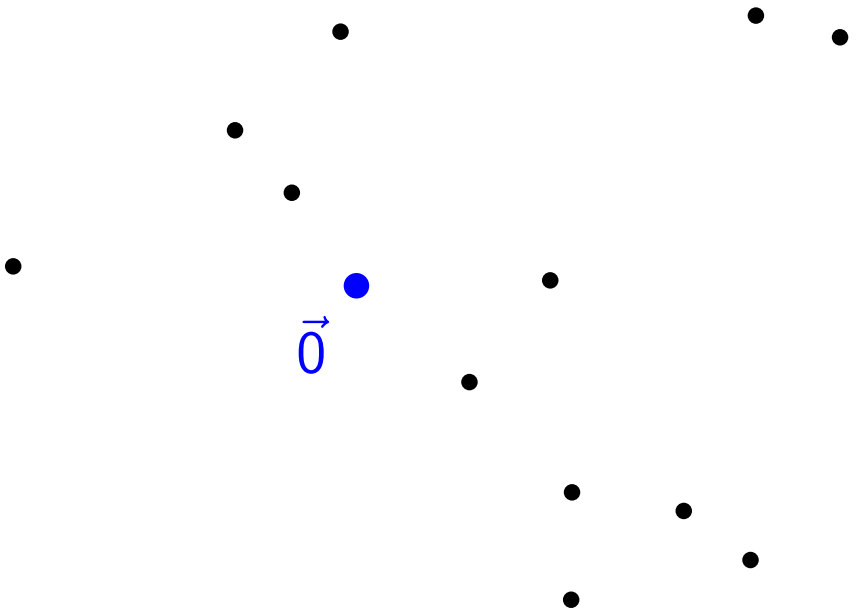
GGH-Signaturverfahren



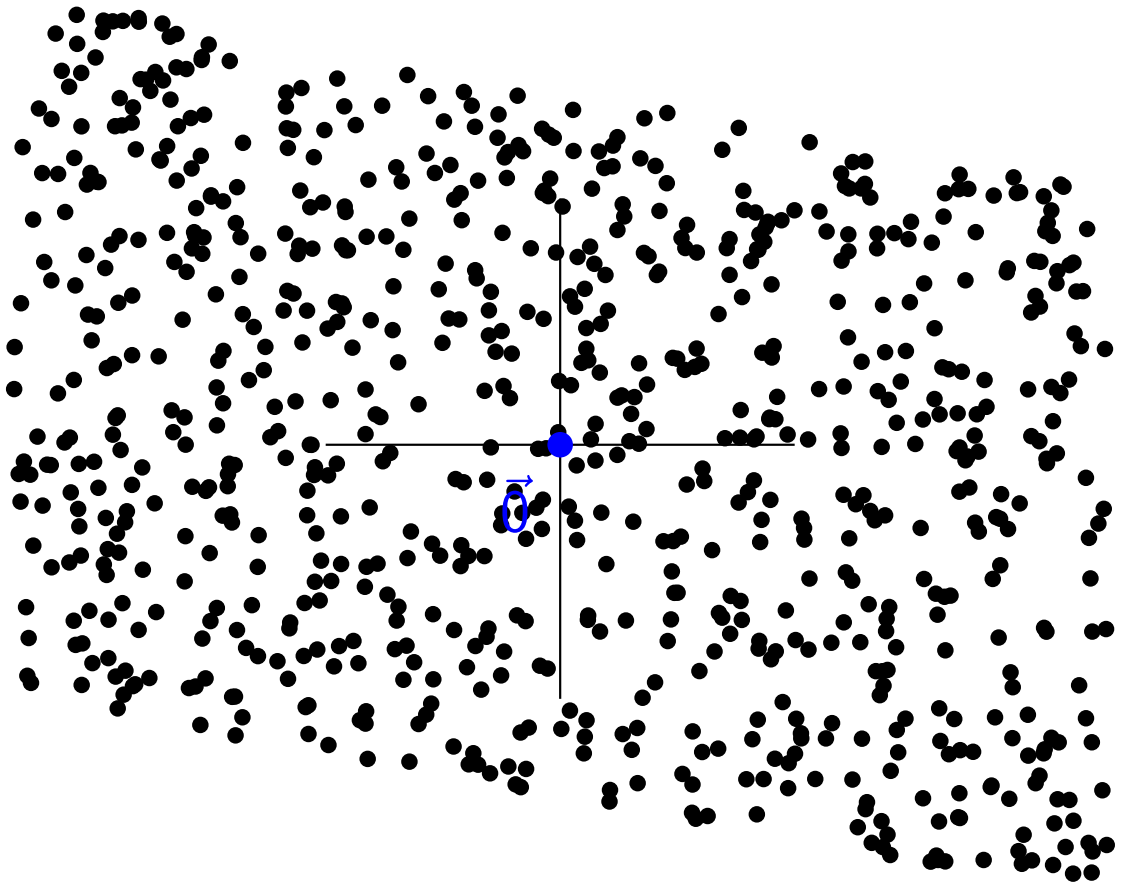
GGH-Signaturverfahren



GGH-Signaturverfahren



GGH-Signaturverfahren



Idee: honest-verifier perfect zero-knowledge interactive proof system

Sei $(B, \vec{q}, d)$ eine Instanz von $\text{GapCVP}_{\gamma(n)}$ mit $B \in \mathbb{Q}^{m \times n}$, $\vec{q} \in \text{span}(B)$, $d \in \mathbb{Q}$ und $\forall \vec{w} \in \mathcal{L}(B) : \|\vec{w} - \vec{q}\| > \gamma(n) \cdot d$.

ZK-Protokoll

1. *Verifier* wählt zufällig ein $\sigma \in \{0, 1\}$, einen zufälligen Gittervektor $\vec{v} \in \mathcal{L}(B)$ in einer „sehr großen“ Kugel und gleichverteilt zufällig einen Fehlervektor $\vec{r}$ (innerhalb einer Kugel mit Radius $\frac{\gamma(n) \cdot d}{2}$). Sendet $x =_{\text{def}} \vec{v} + \sigma\vec{q} + \vec{r}$ an den *Prover*.
2. *Prover* antwortet mit $\tau = 0$, wenn $\forall \vec{w} \in \mathcal{L}(B) : \|\vec{w} - \vec{x}\| < \|(\vec{w} + \vec{v}) - \vec{x}\|$, sonst mit $\tau = 1$.
3. *Verifier* akzeptiert, gdw. $\tau = \sigma$.

Fazit

- Interessanter Post-Quantum Kandidat
- Eigenschaft der „beweisbaren“ Sicherheit einzigartig
- Heute: Komplexere Gitter - NTRU (Zyklische Gitter) und LWE (Ideale Gitter) - die (nicht offensichtlich) Gitter als Grundlage verwenden
- (Noch) viele offene Fragen bzgl. Komplexität von Gitterproblemen und im Besonderen der Gitterbasisreduktion

Vielen Dank für die Aufmerksamkeit.