Parameterized Complexity and Cryptography from Lattice Problems

Mariana Rio Costa

IST - UL

Portugal Crypto Day 2024
13th December 2024

FUNDAÇÃO CALOUSTE GULBENKIAN

Complexity of Codes and Lattice Problems

Mariana Costa, advised by João Ribeiro

Abstract

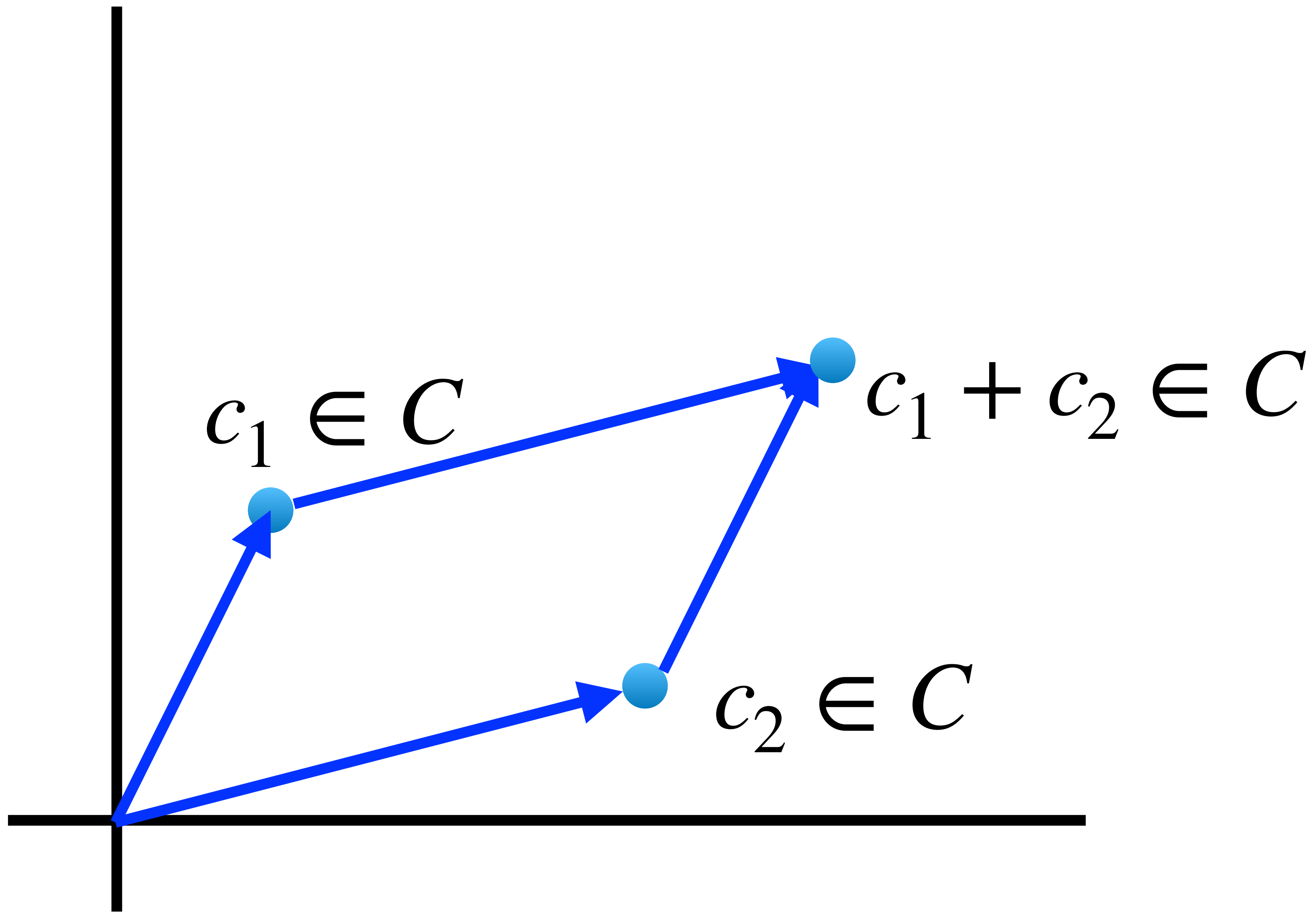
Computational problems involving point lattices are crucial in various areas of computer science, such as integer programming, coding theory, cryptanalysis, and particularly in the development of secure cryptosystems.

We work on the results left open by Huck Bennett, Mahdi Cheraghchi, Venkatesan Guruswami and João Ribeiro (STOC 2023) on the complexity of parameterized γ-SVP on the ℓ_1 norm.

(Linear) Codes

Vector subspace of $\mathbb{F}_q^n$

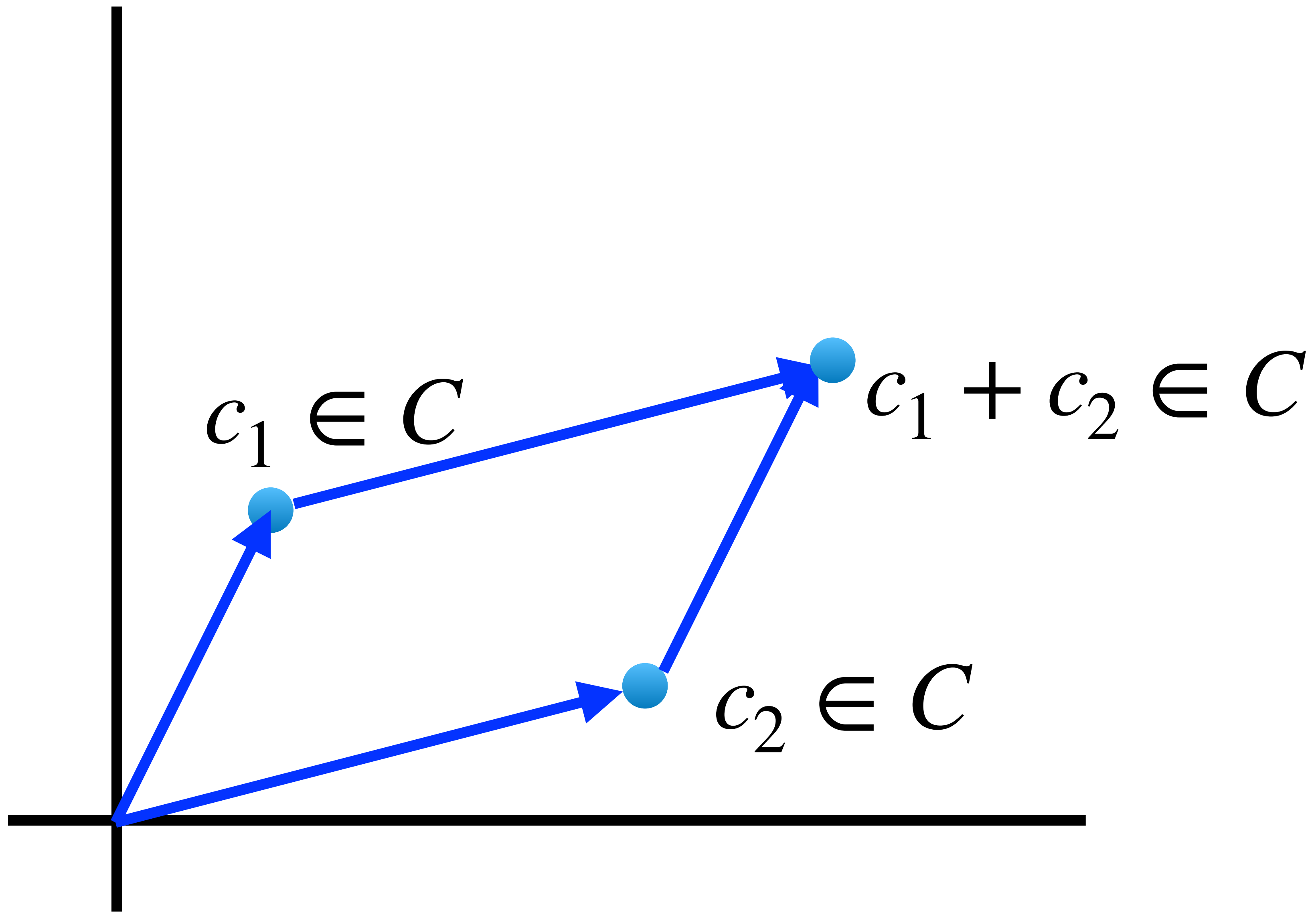
$$G \in \mathbb{F}^{n\times k},\ C = \{Gv : v \in \mathbb{F}_q^k\}$$



(Linear) Codes

Vector subspace of $\mathbb{F}_q^n$

$$G \in \mathbb{F}^{n \times k},\ C = \{Gv : v \in \mathbb{F}_q^k\}$$



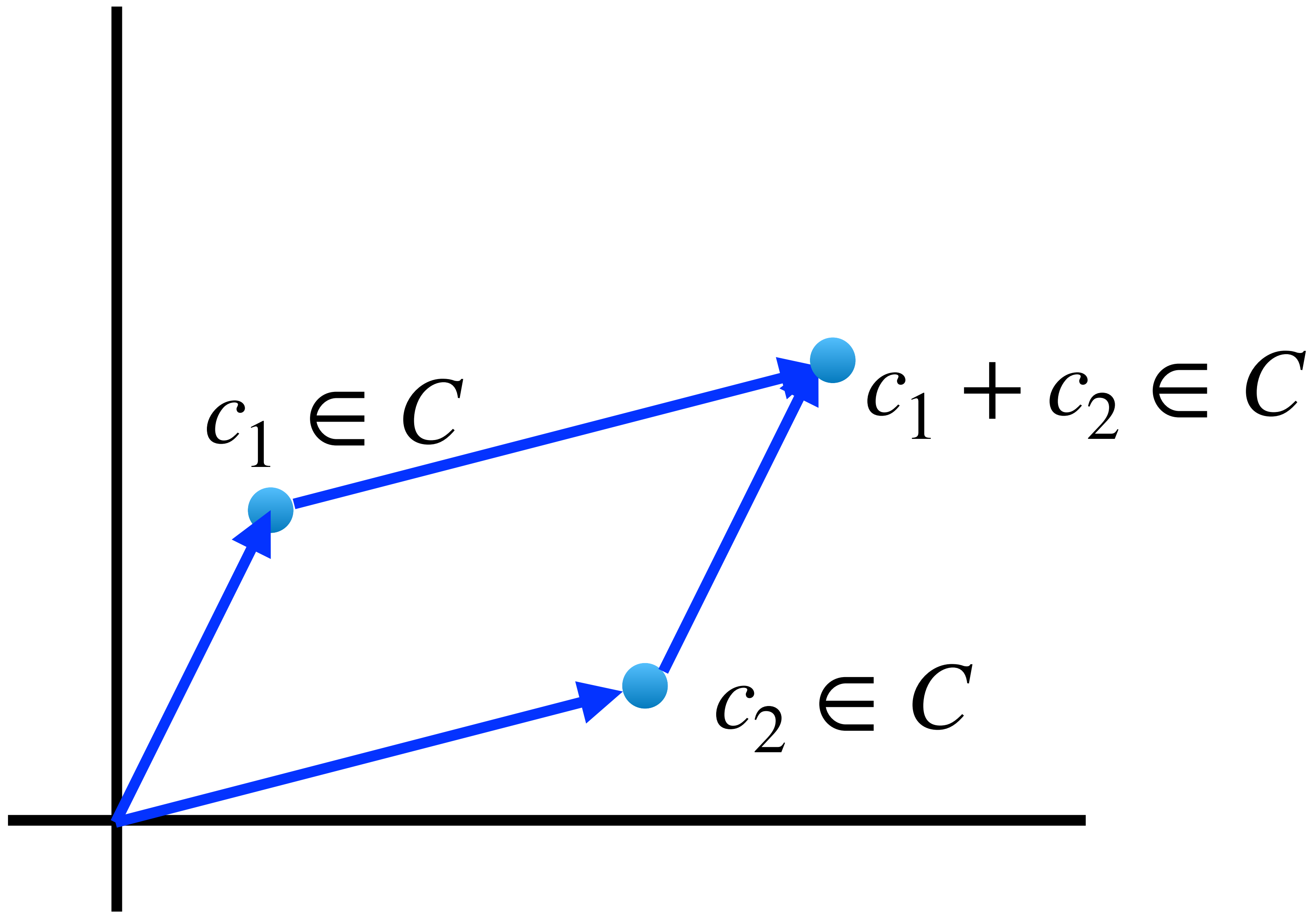
Hamming weight of v

$$\|v\|_0 = \#\{i : v_i \neq 0\}$$

(Linear) Codes

Vector subspace of $\mathbb{F}_q^n$

$$G \in \mathbb{F}^{n \times k},\ C = \{Gv : v \in \mathbb{F}_q^k\}$$



Hamming weight of v

$$\|v\|_0 = \#\{i : v_i \neq 0\}$$

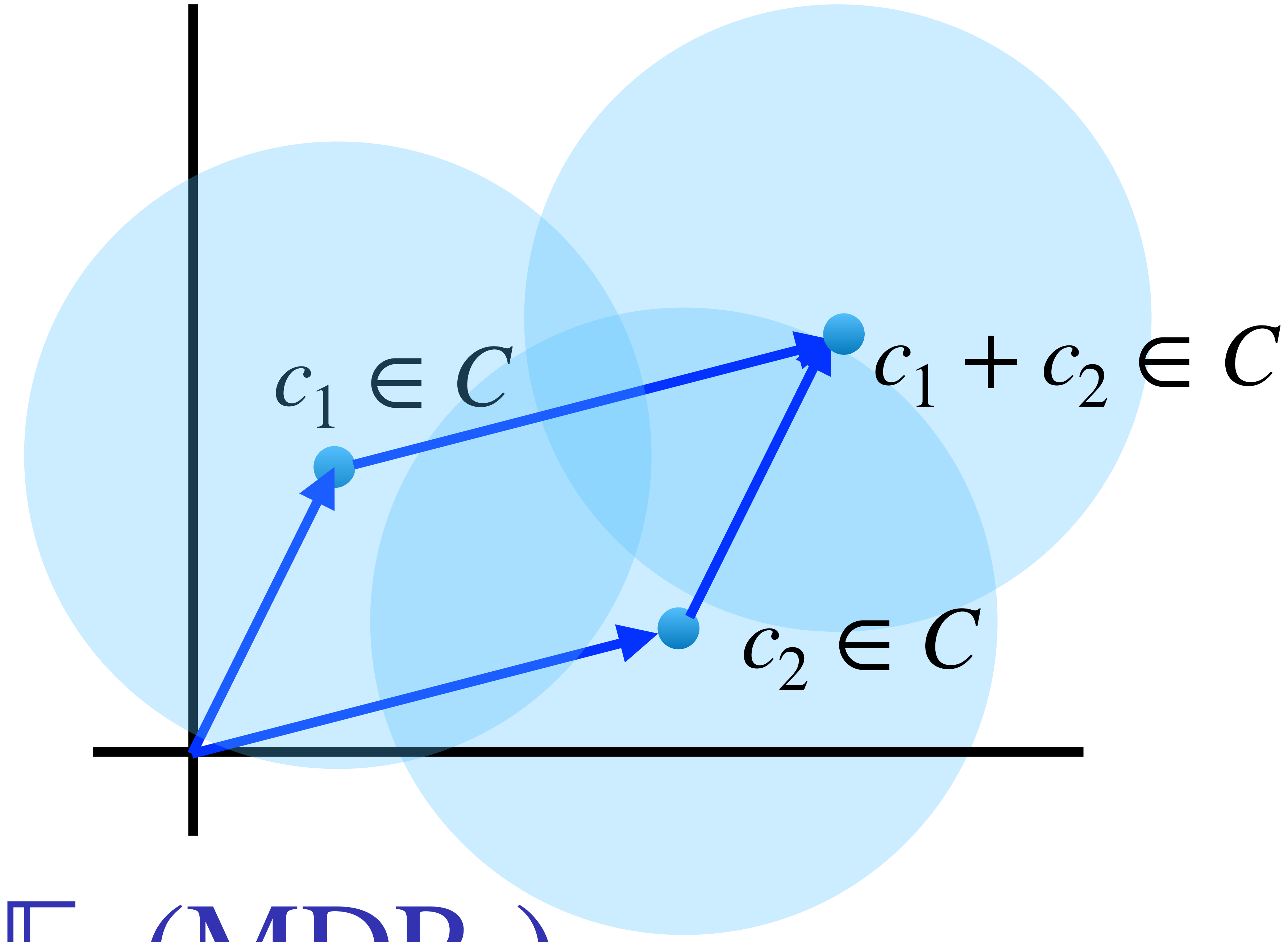
Minimum distance of C: $d(C) = \min_{c,c' \in C, c \neq c'} \|c - c'\|_0$

Nearest Codeword Problem over $\mathbb{F}_q$ (NCP$_q$)

Input: Generator matrix $G \in \mathbb{F}_q^{n\times k}$, distance bound $d \geq 0$ and target vector $t \in \mathbb{F}_q^n$

(YES) There is $c \in C(G)$ s.t. $\|c - t\|_0 \leq d$

(NO) For all $c \in C(G)$, $\|c - t\|_0 > d$

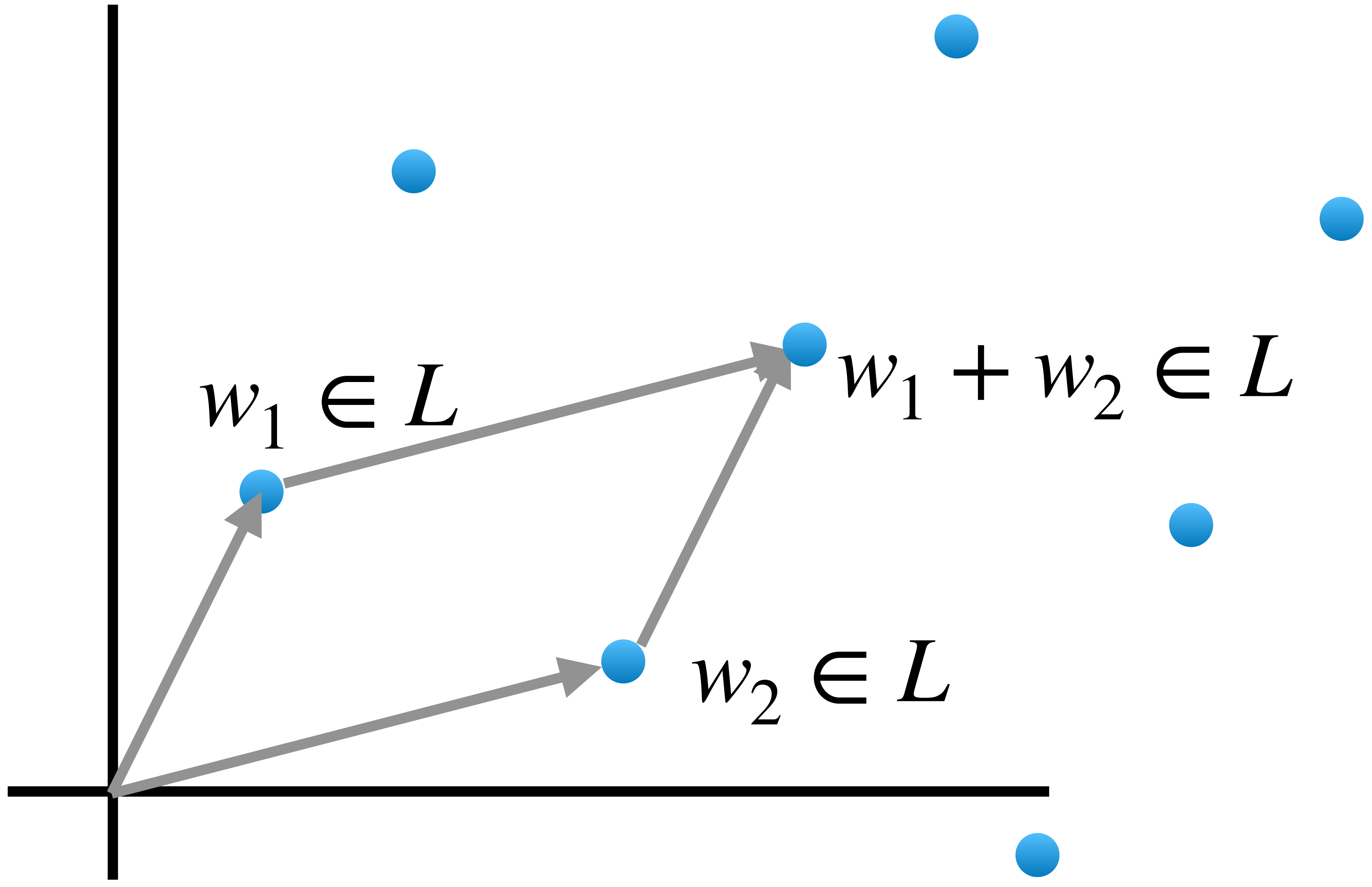


$t = 0 \implies$ Minimum Distance Problem over $\mathbb{F}_q$ (MDP$_q$)

Lattices

Discrete subgroup of $\mathbb{R}^n$

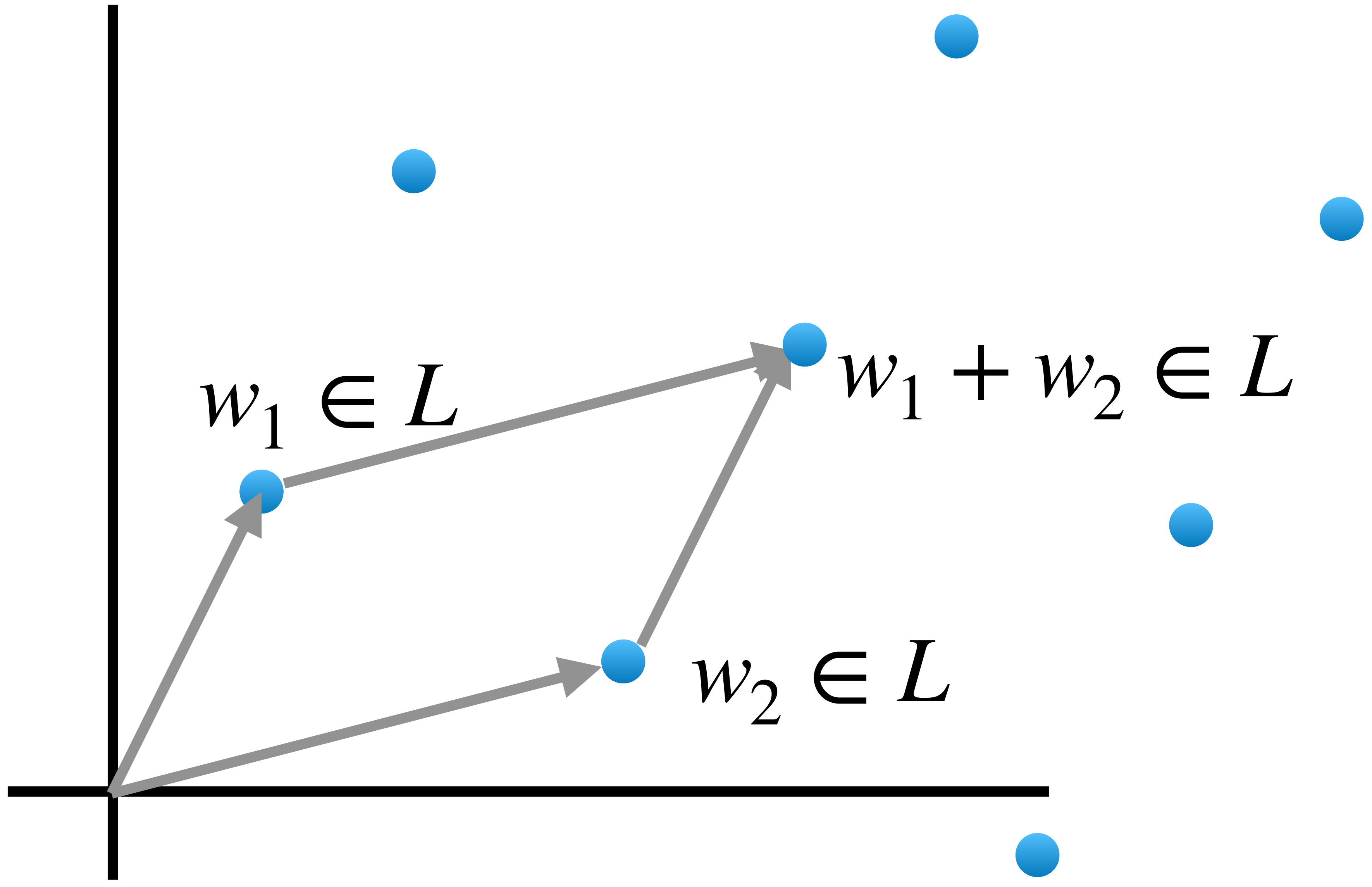
$$B \in \mathbb{R}^{n\times k},\ L = \{Bv : v \in \mathbb{Z}^k\}$$



Lattices

Discrete subgroup of $\mathbb{R}^n$

$$B \in \mathbb{R}^{n \times k},\ L = \{Bv : v \in \mathbb{Z}^k\}$$



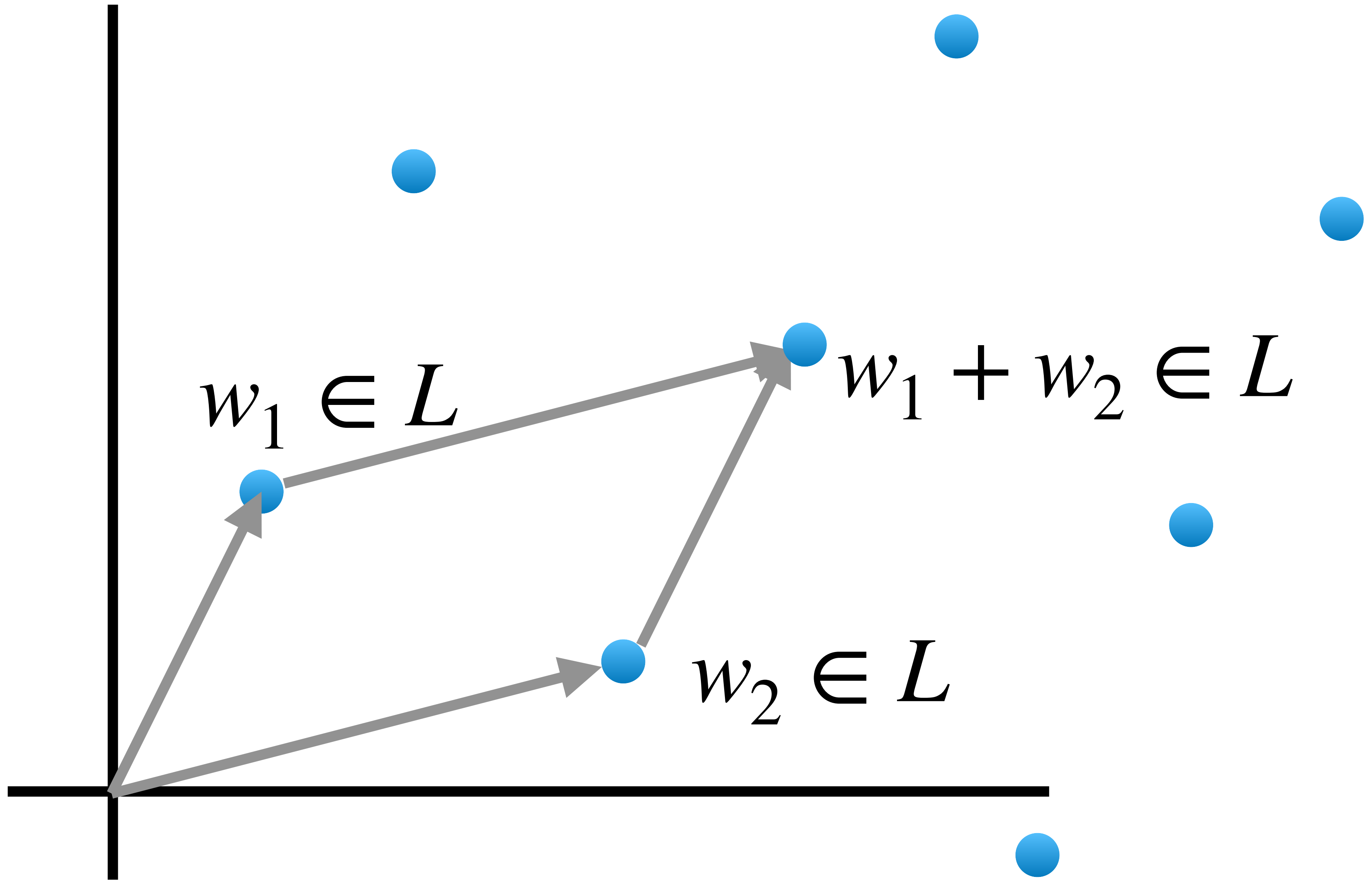
ℓ_p**-norm of** v**,** $p \geq 1$

$$\|v\|_p = \left(\sum_{i=1}^{n} |v_i|^p \right)^{1/p}$$

Lattices

Discrete subgroup of $\mathbb{R}^n$

$B \in \mathbb{R}^{n \times k},\ L = \{Bv : v \in \mathbb{Z}^k\}$



ℓ_p**-norm of** v**,** $p \geq 1$

$$\|v\|_p = \left(\sum_{i=1}^{n} |v_i|^p \right)^{1/p}$$

Minimum distance of L: $\lambda_1(L) := \min_{v \in L \setminus \{0\}} \|v\|_p$

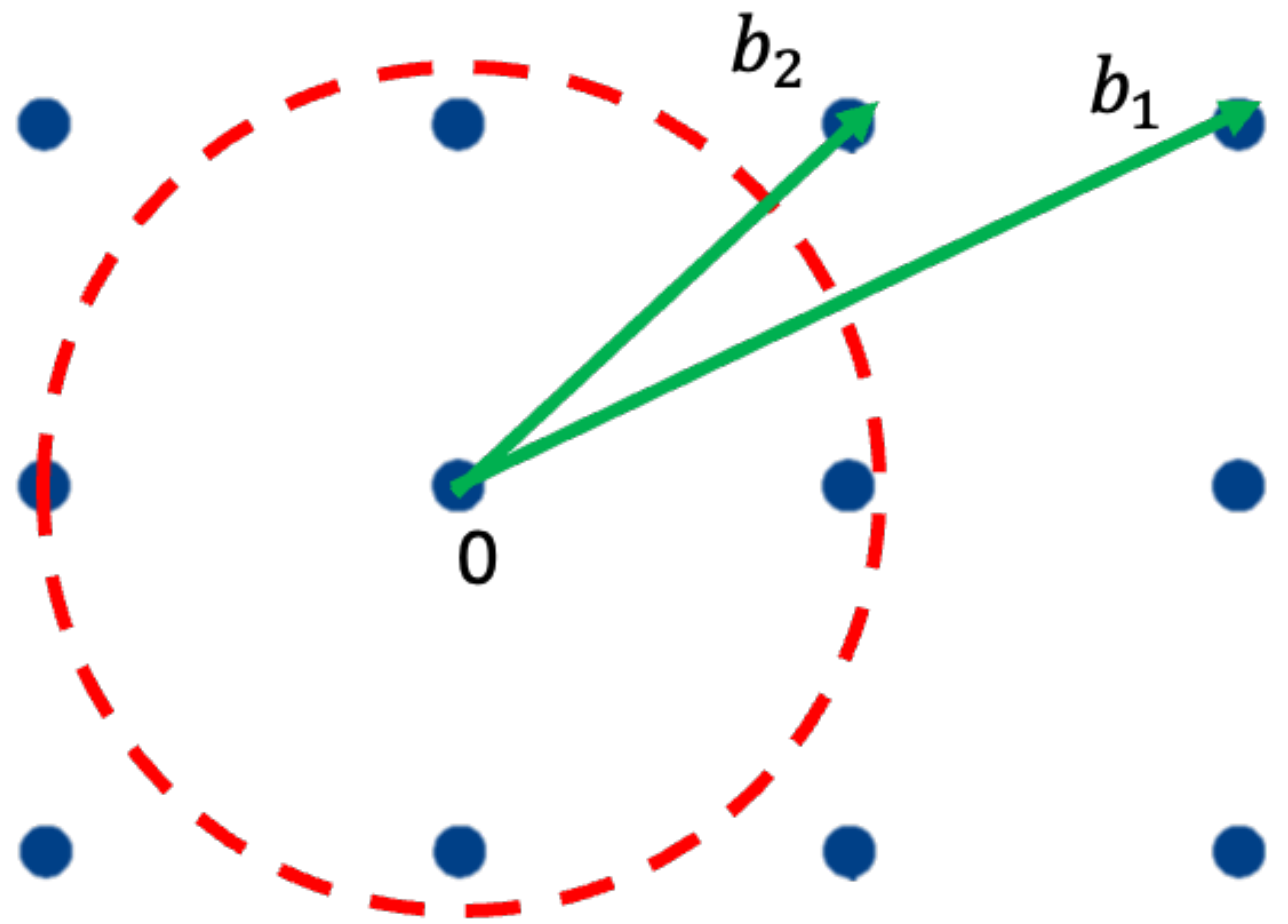
γ-GapSVP, $\gamma \geq 1$

Input: Base $B \in \mathbb{Z}^{n \times k}$ of a lattice L and $d > 0$

(YES) There is $v \in L(B)$ s.t. $\|v\|_p \leq d$

(NO) Every $v \in L(B)$ satisfies $\|v\|_p > \gamma d$

$\gamma = 1 \implies$ GapSVP



How hard are these problems?

SVP:

NP-hard for arbitrary γ, Micciancio '00; Khot '05; Haviv, Regev '12 ($p \geq 1$)

MDP:

NP-hard for arbitrary γ, Håstad '01, Dumer, Micciancio, Sudan '03

How hard are these problems?

SVP:

NP-hard for arbitrary γ, Micciancio ’00; Khot ’05; Haviv, Regev ’12 ($p \geq 1$)

MDP:

NP-hard for arbitrary γ, Håstad ’01, Dumer, Micciancio, Sudan ’03

Does this mean that “real-world” instances of these problems are computationally intractable?

Example

VERTEX COVER PROBLEM:

Input: n-vertex graph G and parameter k

YES if G has vertex cover of size $\leq k$, **NO** otherwise.

NP-hard (Karp '72), **but** there's an algorithm running in time $O(2^k n)$ (Fellows '88)

Parameterized complexity

Complexity in terms of the input size n and a parameter of interest k

Fixed-Parameter Tractable (FPT): A problem is **FPT** iff there is an algorithm running in time:

$$f(k) \cdot n^c$$

For some function f.

Parameterized complexity

A parameterized problem Π is $W[1]$**-hard** if there is an FPT reduction from Clique to Π.

FPT reduction:

(G, k)
Clique instance

algorithm running in time $f(k) \cdot n^c$ $\longrightarrow$

(x, k')
Π instance

YES/**NO** instances mapped to **YES**/**NO** instances & $k' = g(k)$

γ-approximate Shortest Vector Problem, $\gamma \geq 1$

Bennett, Cheraghchi, Guruswami, Ribeiro '23:

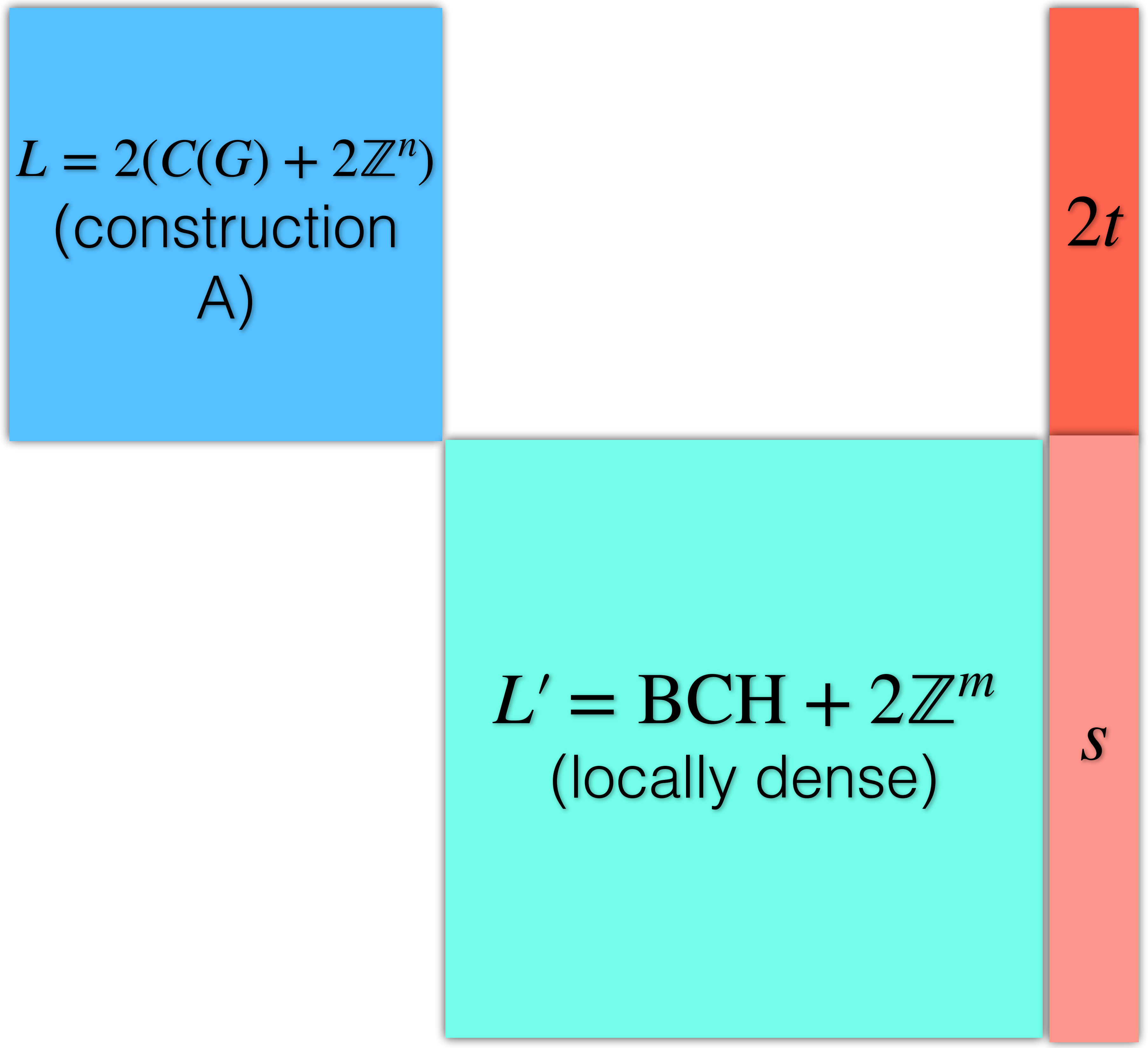
- γ-SVP$_p$ is $W[1]$-hard for $p > 1$ and **all** $\gamma > 1$
- γ-SVP$_1$ is $W[1]$**-hard** for $\gamma < 2$

Parameterized Inapproximability of the
Minimum Distance Problem over all Fields and the
Shortest Vector Problem in all ℓ_p Norms*

Huck Bennett† Mahdi Cheraghchi‡ Venkatesan Guruswami§ João Ribeiro¶

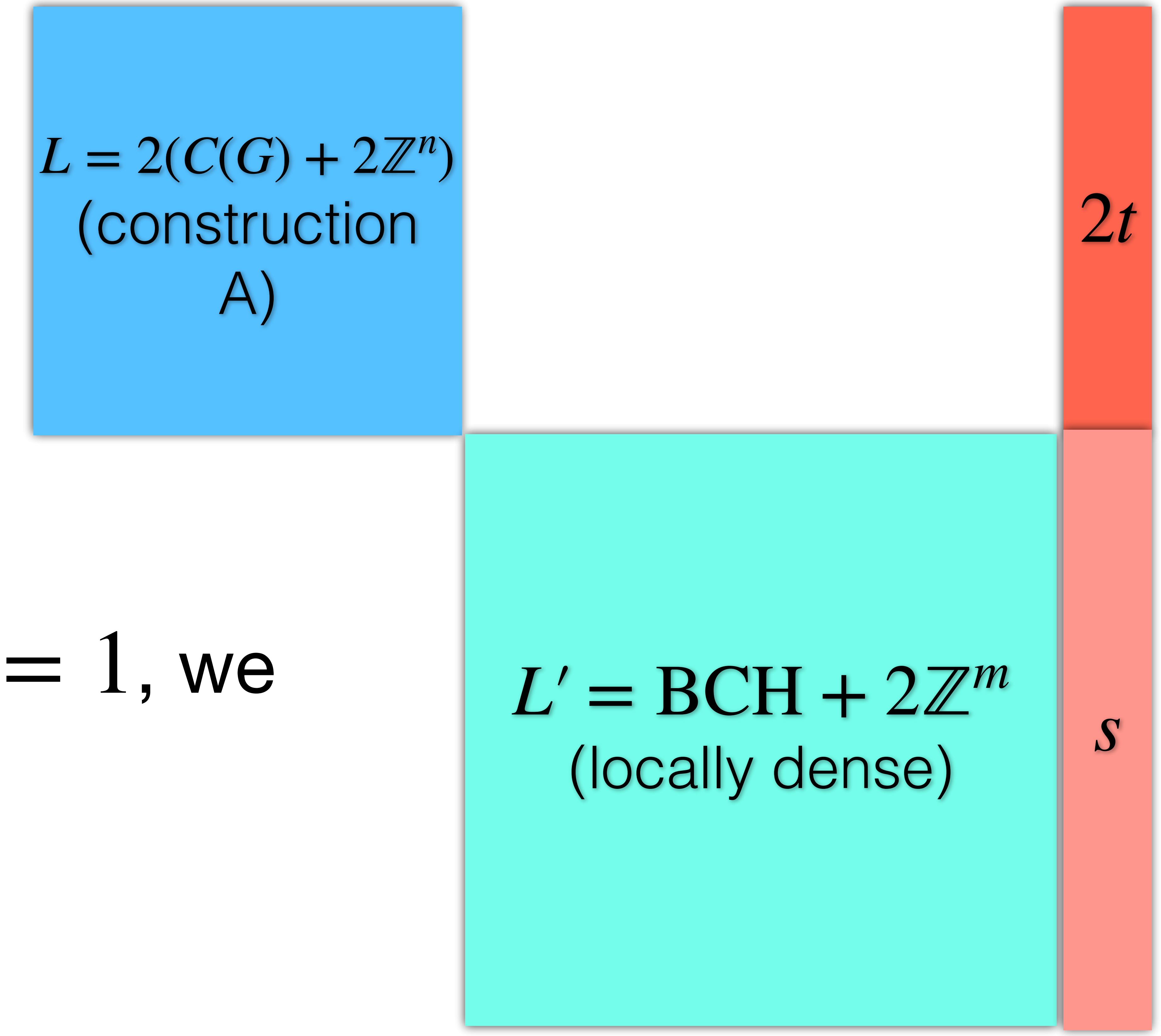
W[1] hardness of γ-SVP$_p$

In Bennet *et al.* ’23, the reduction applied is based on **Khot’s reduction from NCP$_2$ to SVP$_p$**, while ensuring **Haviv-Regev’s** Tensoring conditions



W[1] hardness of γ-SVP$_p$

In Bennet *et al.* ’23, the reduction applied is based on **Khot’s reduction from NCP$_2$ to SVP$_p$**, while ensuring **Haviv-Regev’s** Tensoring conditions



To use the reduction in Bennet *et al.* ’23 with $p = 1$, we need codes that are “better than BCH”

BUT there are none (so far!) for Z_p with p prime

W[1] hardness of γ-SVP$_1$

Our work: We extended the Haviv-Regev tensoring conditions to Z_4

Costa, Ribeiro '24:

Fix an integer $c \geq 1$ and real numbers $p, \gamma \geq 1$. Suppose that (B, k) with $B \in \mathbb{Z}^{m \times n}$ and $k \in \mathbb{Z}^+$ is an instance of γ-SVP$_p$ with the additional property that if (B, k) is a NO instance of γ-SVP$_p$, then every nonzero vector $w \in \mathscr{L}(B)$ satisfies at least one of the following conditions, where $d = \gamma k$:

- $\|w\|_0 > d^p$
- $w \in 4\mathbb{Z}^m$ e $\|w\|_0 > d^p/4^p$
- $w \in 4\mathbb{Z}^m$ e $\|w\|_p > d^{c+3p/2}$

Then, $(B^{\otimes c}, k^c)$ is a **YES** (resp. **NO**) instance of γ^c-SVP_p if (B, k) is a **YES** (resp. **NO**) instance of γ-SVP_p, where $B^{\otimes c}$ denotes the c-fold tensor product of B with itself.

References

Bennett, H., Cheraghchi, M., Guruswami, V., & Ribeiro, J. (2023). Parameterized Inapproximability of the Minimum Distance Problem over All Fields and the Shortest Vector Problem in All ℓ_p Norms. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing* (pp. 553-566).

Costa, M. & Ribeiro, J. (2024). Complexity of Codes and Lattice Problems. Not Published.