Запишем $b = b_i + \left[\sum_{j \neq i} x_j b_j + \underbrace{\left(\frac{x_i - 1}{2}\right)}_{\in \mathbb{Z}} \cdot 2 b_i \right] \in$

$b_i + L(B^{(i)})$

$\Rightarrow \operatorname{dist}(L(B^{(i)}), \underset{b_i}{\underset{\shortparallel}{t^{(i)}}}) \leq \|b\| = \lambda_1(L)$

потенциально в $L(B^{(i)}) + b_i$ могут содержаться векторы, короче b

С другой стороны, по построению $t^{(i)}, B^{(i)}$, $\operatorname{dist}(L(B^{(i)}), t^{(i)}) \geq \lambda_1(L)$

Получаем, $\operatorname{dist}(L(B^{(i)}), t^{(i)}) = \lambda_1(L) \Rightarrow \|\underbrace{c_i - b_i}_{\in L}\| = \lambda_1(L)$ ▶

Открытые вопросы

1) Редукция в Thm 2 – это редукция типа "много – к – одному"

$\uparrow$ n вызовов CVP $\qquad$ $\uparrow$ 1 решение SVP.

Вопрос: редукция 1 – к – 1. (с сохранением р-ти решётки)

2) Обратная редукция от CVP к SVP с одинаковым пар-м γ.