V uSVP редуцируется к SVP (решить $\lambda_1(L(B)) \le r$, "да", или $\lambda_1(L(B)) > \gamma \cdot r$, "нет").

Теорема 3 $\forall \gamma = poly(n)$ $uSVP_\gamma$ редуцируется к SVP_γ.

$\triangleleft$ $B \in \mathbb{Z}^{n \times n}$ - базис решётки с uSVP.

$s \in L(B)$, $\|s\| = \lambda_1(L)$

Мы знаем, что все вектора, не $\|$-ые s, имеют нормы $\ge \lambda_2 \ge \gamma \cdot \lambda_1$.

Идея: Построить разреженные решётки, одна из которых содержит s.

$\exists p > \gamma$ - простое

$$B_0 = [p \cdot b_1, b_2 \ldots b_n]$$

$$B_i = [b_1 + i \cdot b_2, p \cdot b_2, \ldots, b_n]$$

1. Одна из решёток, порождённая B_i $(i \ge 0)$, содержит $s = \sum x_i b_i$

(Если $x_1 \equiv 0 \mod p$, то $s \in L(B_0)$

иначе, $s \in L(B_i)$, для $i = x_2 \cdot x_1^{-1} \mod p$, т.к.

$$s = x_1 (b_1 + x_2 \cdot x_1^{-1} b_2) + \frac{x_2 - (x_2 \cdot x_1^{-1}) x}{p} \cdot p b_2 + \sum_{i \ge 3} x_i b_i)$$

2. Если $s \notin L(B_i)$, то $\lambda_1(L(B_i)) \ge \gamma \cdot \lambda_1(L)$

(Если $v \in L(B_i)$, $v \nparallel s$, то $\|v\| \ge \gamma \cdot \lambda_1(L)$.

иначе, покажем, что $\|v\| \ge p \cdot \|s\| \ge \gamma \cdot \lambda_1(L)$.

$*B = [s | b_2 | \ldots b_n]$ - базис $L(B)$, где вместо b_1 есть s

$\det(B_i) = p \cdot \det(B)$

т.к. $v \parallel s$, то $\underset{(k \ne 1)}{v = k \cdot s} \in L(B_i)$, тогда покажем, что $k \ge p$.

$* B_i = [k \cdot s | c_2 | \ldots c_n]$ - базис $L(B_i)$, где вместо $b_1 + i b_2$ есть $k \cdot s$.

$$B_i = B \cdot \left[\begin{matrix} k \\ \vdots \\ 0 \end{matrix} \; \boxed{////} \right]^{\text{неважно}} \Rightarrow \det(B_i) = \det(B) \cdot k \cdot \det[////]$$

$\det(B_i) = p \cdot \det(B) \cdot = \det(B) \cdot k \cdot \det \cancel{[\;]} \Rightarrow k \mid p \Rightarrow k = p$)

Вызываем SVP_γ на $(B_i, \ r = \underbrace{\overset{\|s\|}{\overset{\shortparallel}{\lambda_1 (L(B))}}})$.

Проблема: мы не знаем $\lambda_1(L(B))$.

Решение: Вызываем LLL $\rightsquigarrow$ 2^n-аппроксимацию к $\lambda_1(L(B))$

Запустив LLL, имеем $\lambda_1(L(B)) \le r \le 2^n \cdot \lambda_1(L(B))$

$SVP_\gamma(B_i, r)$ точно выдаст "да" для каких-то i (среди них будет i, т.ч. $s \in L(B_i)$, но, быть может, и другие i)

$SVP_\gamma(B_i, \frac{r}{2^n})$ выдаст "нет" $\forall i$

Используем бинарный поиск $r', r'' \in [\frac{r}{2^n}, r]$, т.ч. $r' < r''$,

- $SVP(B_i, r')$ возвращает "нет" $\forall i$,
- $SVP(B_i, r'')$ возвращает "да" для каких-то i.

Полагаем на след. шаге бин. поиска $r = r''$. В итоге, $SVP(B_i, r'')$ вернёт "да" только для одного i. Такое r'' – достаточная аппроксимация $\lambda_1(L)$.

Имеем, SVP_γ позволяет детектировать i, т.ч. $s \in L(B_i)$.

Повторяем редукцию для $B := B_i$.

После $\underline{\underline{k}}$ итераций, имеем $\det(\overset{\text{решётка на k-ой итерации}}{\overbrace{L_k(B)}}) = p^k \det(L(B))$

$\exists \ \widehat{L_k(B)}$. Эта решётка имеет определитель

$$\det \widehat{L_k(B)} = \frac{1}{\det L_k(B)} = \frac{1}{p^k \cdot \det(L(B))}$$

Вызвав LLL алг-м на $\widehat{L_k(B)}$, получим $\hat{b}$, т.ч. $\|\hat{b}\| \le 2^n \cdot \frac{1}{p^k \cdot (\det(L))^{\frac{1}{n}}}$

$$|\langle \hat{b}, s \rangle| \le \frac{2^n}{p^k \cdot \det(L)^{\frac{1}{n}}} \cdot \underbrace{\lambda_1(L)}_{\le \sqrt{n} \cdot \det(L)^{\frac{1}{n}}} \le \frac{2^n}{p^k} \cdot \sqrt{n} < 1 \text{ для } k = \Omega(n \cdot \lg p)$$

$= 0$

$\Rightarrow \quad S \in L \cap \hat{b}^{\perp} = \Pi(\hat{L}, \hat{b}^{\perp})$ $\Rightarrow$ решётка р-ти $n-1$.

$\Rightarrow$ Запускаем весь алг-м на $L \cap \hat{b}^{\perp}$, пока не получим решётку р-ти 1 $\Rightarrow$ знаем S.