GDO-05 22.10.19

Es gilt: $\langle \phi(A) \rangle \leq O(n^2 \langle A \rangle)$

[Denn $\langle A^T_{*,[j]} \cdot A_{*,[j]} \rangle \leq O\left(j \cdot \langle A_{*,[j]} \rangle\right) \leq O(n\langle A \rangle)$

$\langle \det(\tilde{A}) \rangle \leq 2 \cdot \langle \tilde{A} \rangle$, siehe GLO]

Also: $\phi(A) \leq 2^{O(n^2\langle A \rangle)}$ ($\phi(A) \leq 2^{K \cdot n^2 \cdot \langle A \rangle}$ mit Konstante k).

Es genügt also, zu zeigen, dass nach Ausführung einer Vertauschung in Schritt ④

$$\phi(\tilde{B}) \leq \frac{3}{4}\phi(B)$$

ist [denn dann war nach $\left\lceil \frac{-k}{\log 3/4} \cdot n^2 \cdot \langle B_{Eingabe} \rangle \right\rceil + 1$ Iterationen

$\phi(B) < 1$, also $\phi(B) = 0$ ↯ B regulär].

Sei also $\tilde{B}_{neu}$ die Gitterbasis, die in Schritt ④ durch Vertauschen von $\tilde{b}^{j-1}$ und $\tilde{b}^j$ entstanden ist.

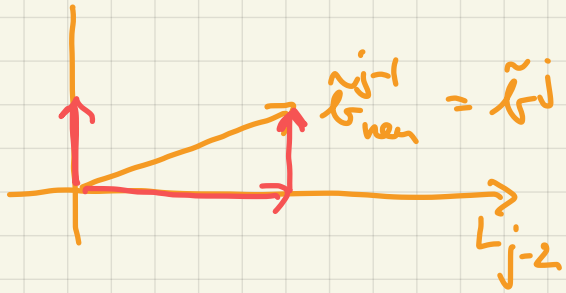
Es gilt: $V_\ell(\tilde{B}_{neu}) = V_\ell(\tilde{B})$ für alle $\ell \neq j-1$.

Also: $$\frac{\Phi(\tilde{B}_{neu})}{\Phi(\tilde{B})} = \frac{V_{j-1}(\tilde{B}_{neu})}{V_{j-1}(\tilde{B})} \qquad (***)$$

Sei $G_{neu} = [g^1_{neu}, \dots, g^n_{neu}]$ die GS-Orthogonalisierung von $\tilde{B}_{neu}$.

Es gilt $g^k_{neu} = g^k$ für $k = 1, \dots, j-2$ und

$$g^{j-1}_{neu} = \boxed{g^j + \tilde{\mu}_{j-1,j}\, g^{j-1}}$$



[denn: $g^j + \tilde{\mu}_{j-1,j}\, g^{j-1} \perp L_{j-2}$ und

$\tilde{b}^{j-1}_{neu} - (g^j + \tilde{\mu}_{j-1,j}\, g^{j-1}) = \sum_{k=1}^{j-2} \tilde{\mu}_{k,j}\, g^k \in L_{j-2}$]

$\tilde{b}^j$

Also liegen (*) und (**) in also

$$\frac{\phi(\tilde{R}_{neu})}{\phi(R)} = \frac{\| g^j + \tilde{\mu}_{j-1,j} g^{j-1} \|^2}{\| g^{j-1} \|^2} < \frac{3}{4}.$$

□