Plan for today

- Lattice basis reduction
- Gaussian algorithm
- The LLL algorithm

A.K.

Lenstra, Lenstra & Lovász

$$SV(A) = \min_{v \in \Lambda(A)\setminus\{0\}} \|v\|$$

LLL : Input: $A \in \mathbb{Z}^{n\times n}$

Output: $v \in \Lambda(A)\setminus\{0\}$ s.t. $\|v\| \leq 2^{\frac{n-1}{2}} SV(A)$

Minkowski:

$\exists\ v \in \Lambda(A)\setminus\{0\}$

$\|v\|_\infty \leq \sqrt[n]{\det(\Lambda)}$

Finding such a v is open problem.

Recall

Theorem
A lattice $\Lambda \subseteq \mathbb{R}^n$ has a nonzero lattice point of length bounded by $2 \cdot \sqrt[n]{\det(\Lambda)/V_n}$.

Orthogonality defect:

- $b_1, \dots, b_n$ lattice basis.
- $B = (b_1, \dots, b_n)$
- $\gamma \in \mathbb{R}$ with $|\det(B)| = \gamma \cdot \prod_{i=1}^{n} \|b_i\|$

"orthogonality defect".

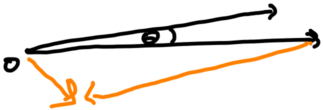
Shortest vector is of the form $B \cdot x$, $\|x\|_\infty \leq \gamma$

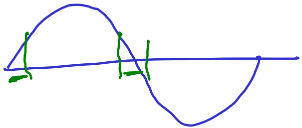
$(2\gamma + 1)^n$ candidates. Constant if n and γ are constant.

Definition

$b_1, b_2 \in \mathbb{Z}^2$ is *reduced* if enclosed angle ϕ satisfies

$$60^\circ \leq \phi \leq 120^\circ.$$





Definition

$b_1, b_2 \in \mathbb{Z}^2$ is *reduced* if enclosed angle ϕ satisfies

$30^\circ \le \phi \le 150^\circ$

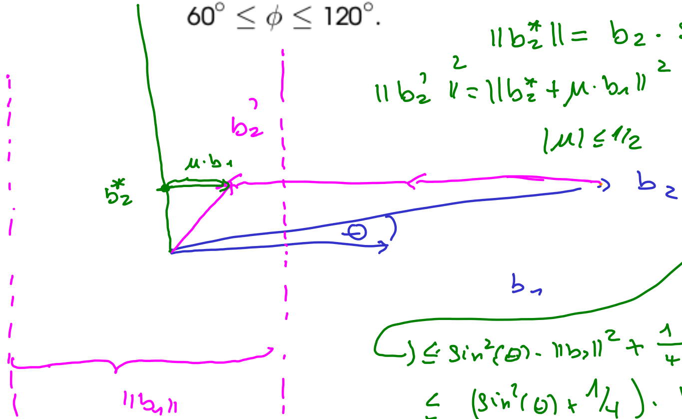
$$60^\circ \le \phi \le 120^\circ.$$

$\left(\sin^2(\theta) + \frac{1}{4}\right) < 1/2$

$\iff \sin^2(\theta) < \frac{1}{4}.$

$\|b_2^*\| = b_2 \cdot \sin(\theta)$

$\|b_2\|^2 = \|b_2^* + \mu \cdot b_1\|^2 = \|b_2^*\|^2 + \mu^2 \|b_1\|^2$



$|\mu| \le 1/2$

$\le \sin^2(\theta) \cdot \|b_2\|^2 + \frac{1}{4} \|b_1\|^2$

$\le \underbrace{\left(\sin^2(\theta) + 1/4\right)}_{<1} \cdot \|b_2\|^2$ if $(60^\circ < \phi < 120^\circ)$

Lagrange's algorithm:

- Each second iteration: $\|\cdot\|$ of larger vector is scaled with $\le 1/2$.
- $\#$ of iterations is linear in $\overset{\text{bin. enc. length.}}{\mathrm{size}(b_1,b_2)}$

Definition

$b_1, b_2 \in \mathbb{Z}^2$ is *reduced* if enclosed angle ϕ satisfies

$$60^\circ \le \phi \le 120^\circ.$$

Input: $b_1, b_2 \in \mathbb{R}^2$ (lin. indep).

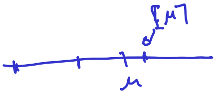
if $\|b_2\| < \|b_1\|$ swap b_2 and b_1.

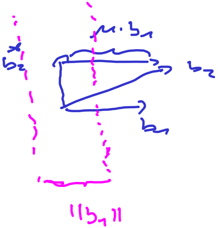
While $\sin^2(\theta) < 1/4$.

- $b_2' = b_2 - \lceil \mu \rfloor \cdot b_1$
- swap(b_1, b_2)

$\lfloor \mu \rceil$

$b_2 = b_2^* + \mu \cdot b_1$





then $b_2' = b_2^* + \lambda \cdot b_1$, with $|\lambda| \le 1/2$

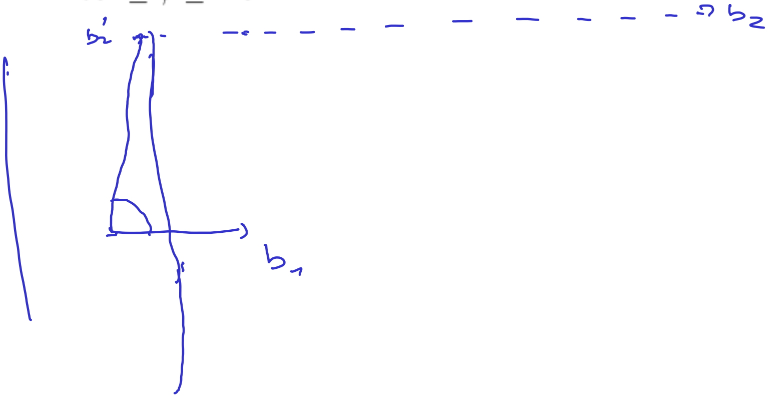
Observe that $b_2' \not\le b_2$ and $b_2' \le b_1$ unless $60^\circ \le \phi \le 120^\circ$

2D

Definition

$b_1, b_2 \in \mathbb{Z}^2$ is *reduced* if enclosed angle ϕ satisfies

$$60^\circ \leq \phi \leq 120^\circ.$$



Reduced basis

Definition

Let $f : \mathbb{N} \to \mathbb{N}$ be a function and $B \in \mathbb{Z}^{n \times n}$ be a lattice basis. B is *f-reduced* or simply *reduced* if the orthogonality defect of B is bounded by $f(n)$.

Result of research by Lagrange, Hermite & Gauss: 19th century:

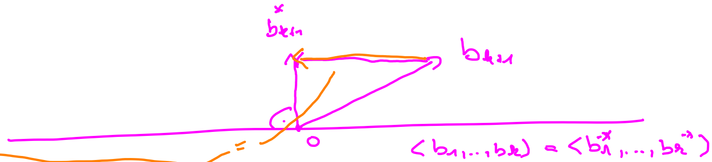
$\exists f$ such that: Each lattice $\Lambda(B) \subseteq \mathbb{R}^n$ has a reduced basis.

Gram-Schmidt orthogonalization

Given: $b_1, \ldots, b_n$, computes $b_1^*, \ldots, b_n^*$ such that

i) The vectors $b_1, \ldots, b_k$ span the same subspace as $b_1^*, \ldots, b_k^*$ for each $k = 1, \ldots, n$.

ii) The vectors $b_1^*, \ldots, b_n^*$ are pairwise orthogonal.



$$b_{k+1}^* = b_{k+1} - \boxed{\sum_{j=1}^{k} \mu_{j,k+1} \cdot b_j^*}$$

$$\left\langle b_{k+1} - \sum_{j=1}^{k} \mu_{j,k+1} b_j^*, b_i^* \right\rangle = 0 \quad \text{for each } i = 1, \ldots, k$$

$$\Leftrightarrow \quad \langle b_{k+1}, b_i^* \rangle - \sum_{j=1}^{k} \mu_{j,k+1} \langle b_j^*, b_i^* \rangle$$

Observation: Let $b_1^*,\dots,b_i^*,b_{i+1}^*,b_{i+2}^*,\dots,b_n^*$ be the

GSO. of $b_1,\dots,b_i,b_{i+1},\dots,b_n$. and let $c_1^*,\dots,c_i^*,c_{i+1}^*,\dots,c_n^*$

be GSO of $b_1,\dots,b_{i+1},b_i,b_{i+2},\dots b_n$. Then

$$c_k^* = b_k^* \quad \text{for } k \in \{1,\dots,i-1\} \cup \{i+2,\dots,n\}$$

Gram-Schmidt orthogonalization

Given: $b_1, \ldots, b_n$, computes $b_1^*, \ldots, b_n^*$ such that

i) The vectors $b_1, \ldots, b_k$ span the same subspace as $b_1^*, \ldots, b_k^*$ for each $k = 1, \ldots, n$.

ii) The vectors $b_1^*, \ldots, b_n^*$ are pairwise orthogonal.

$$\langle b_{k+1}, b_i^* \rangle - \sum_{j=1}^{k} \mu_{k+1,j} \underbrace{\langle b_j^*, b_i^* \rangle}_{=0 \text{ if } i \neq j} = \langle b_{k+1}, b_i^* \rangle - \mu_{k+1,i} \langle b_i^*, b_i^* \rangle$$

$$\Rightarrow \mu_{k+1,i} = \frac{\langle b_{k+1}, b_i^* \rangle}{\langle b_i^*, b_i^* \rangle}.$$

G.S.O.

Lower bound on $SV(\Lambda)$

$b_1^* \leftarrow b_1$
For $j = 2, \dots, k$
  $b_j^* \leftarrow b_j - \sum_{i=1}^{j-1} \mu_{ji} b_i^*$
  where $\mu_{ji} = \langle b_j, b_i^* \rangle / \underbrace{\|b_i^*\|^2}_{\langle b_i^*, b_i^* \rangle}$.

$$b_j = \sum_{i=1}^{j-1} \mu_{ji} \cdot b_i^* + b_j^*.$$

$$(b_1, \dots, b_n) = (b_1^*, \dots, b_n^*) \cdot \underbrace{\begin{pmatrix} 1 & & \mu \\ & \ddots & \\ 0 & & 1 \end{pmatrix}}_{R}$$

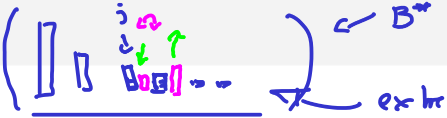
$$B = B^* \cdot R$$

Question.

$SV(\Lambda(B))$

If $B = B^*$. $SV(\Lambda(B))$ is shortest column of B.

Quality of Approximation



product of norms is invariant.

extremely rapid decay.

Lemma

Let $B = B^* \cdot R$ be the GSO of B. The length of a shortest column of B^* is a lower bound on the length of a shortest vector of $\Lambda(B)$.

Proof: Let $v = B \cdot x$, $x \in \mathbb{Z}^n \setminus \{0\}$ be a shortest vector. $x = \begin{bmatrix} x_1 \\ \vdots \\ x_k \neq 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$

$$v = B \cdot x = B^* \cdot \begin{bmatrix} 1 & \cdots & \mu \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_k \\ 0 \\ \vdots \\ 0 \end{bmatrix} = B^* \cdot \begin{pmatrix} \vdots \\ x_k \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$= \ldots \cdot b_1^* + \ldots b_2^* + \ldots + x_k \cdot b_k^* + 0$$

$$\Rightarrow \|v\| \geq \underbrace{|x_k|}_{\geq 1} \cdot \|b_k^*\| \geq \|b_k^*\| \geq \min_j \|b_j^*\|$$

Quality of Approximation

$$\det(B_1)^2 = \det\left(B_1^T \cdot B_1\right) = \det\left(\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}^T B_1^{*T} \cdot B_1^* \cdot \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} \right)$$

$$= \det\left(B_1^{*T} \cdot B_1^* \right) = \prod_{i=1}^{n} \|b_i^*\|$$

Lemma

Let $B = B^* \cdot R$ be the GSO of B. The length of a shortest column ~~i=~~ of B^* is a lower bound on the length of a shortest vector of $\Lambda(B)$.

$B_1 = B_2 \cdot U \Leftrightarrow U$ is unimod.

Q: Let B_1 and B_2 be bases of $\Lambda \leq \mathbb{Z}^n$ with

GSOs: $B_1 = (b_1^*, \ldots, b_n^*) \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}$ $\quad B_2 = (c_1^*, \ldots, c_n^*) \begin{pmatrix} 1 & \mu' \\ 0 & 1 \end{pmatrix}$

$$\prod_{i=1}^{n} \|b_i^*\| = \prod_{i=1}^{n} \|c_i^*\| = \det(\mathcal{L}(B_1))$$

$$\prod_{i=1}^{n} \|b_i^*\| = |\det(B_1)|, \qquad \prod_{i=1}^{n} \|c_i^*\| = |\det(B_2)|$$

$$B = B^{*} \underbrace{\begin{bmatrix} 1 & 1001 & 503 & 12 \\ 0 & 1 & 13 & 105 \\ 0 & 0 & 1 & \underline{20000{,}8} \\ 0 & 0 & 0 & 1 \end{bmatrix}}_{R}$$

$\cdot 20000$ –

$\rightsquigarrow B_{\text{normal}}$

$$\to B^{*} \cdot \begin{bmatrix} 1 & 1001 & 503 & \sim \\ 0 & 1 & |\cdot| \le 1/2 & |\cdot| \le 1/2 \\ 0 & 0 & 1 & -0{,}2 \\ 0 & 0 & 0 & 1 \end{bmatrix} = B^{*} \cdot \begin{pmatrix} 1 & & |\cdot| \le 1/2 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

$\to$ not touched!

Normalization

- Let r_{ij} be the j-th entry of the i-th row of R.
- Subtracting $\lfloor r_{ij} \rceil$ times the i-th column of R from the j-th column, the new entry r'_{ij} at position ij will satisfy $-1/2 < r'_{ij} \leq 1/2$
- Entries in a row below the i-th row of R remain unchanged.
- Thus working our way from the last to the first row, we obtain a basis $B' = B^* \cdot R'$ with

$$-1/2 < r'_{ij} \leq 1/2, \text{ for } 1 \leq i < j \leq n. \tag{10}$$

This procedure is called a *normalization step*.

$b_j^{\prime *}$ (next slide)

$\shortparallel$

this is put back!

Normalize (B)

Repeat the following two steps, as long as there exists a j, $1 \le j \le n-1$ with

$$\underbrace{\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2}_{= c_j^*} < 3/4\, \|b_j^*\|^2 : \qquad (11)$$

- Normalize B
- Swap b_j and b_{j+1}

$= c_j^*$ if $[c_1^*, \dots, c_n^*] \cdot \begin{pmatrix} 1 & \dots & * \\ & & 1 \end{pmatrix}$ is

GSO of $[b_1, \dots, b_{j-1}, b_{j+1}, b_j, \dots, b_n]$

Recall: $c_1^* = b_1^*$, $c_2^* = b_2^*$, $c_{j-1}^* = b_{j-1}^*$, $c_j^* = b_{j+1}^* + \mu_{j+1} \cdot b_j^*$, $c_{j+1}^* = ?$,

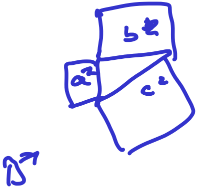
$c_{j+2}^* = b_{j+2}^*, \dots, c_n^* = b_n^*$

And thus $\|c_j^*\| \cdot \|c_{j+1}^*\| = \|b_j^*\| \cdot \|b_{j+1}^*\|$

Suppose Alg on Input $A\in\mathbb{Z}^{n\times n}$ terminates with Bases $B\in\mathbb{Z}^{n\times n}$.

$$B=(b_1,\dots,b_n) = (b_1^* \cdots b_n^*)\begin{pmatrix}1 & & \mu\\ & \ddots & \\ 0 & & 1\end{pmatrix}$$

$b_1=b_1^*$. Lets compare $\|b_2^*\|$ with $\|b_1^*\|$



$$\|b_2^*+\mu_{2,1}b_1^*\|^2 \ge 3/4\cdot\|b_1^*\|^2$$

$$\|b_2^*\|^2+\underbrace{\mu_{21}^2}_{\le 1/4}\|b_1^*\|^2 \ge 3/4\,\|b_1^*\|^2$$

$$\|b_2^*\|^2 \ge \frac{1}{2}\cdot\|b_1^*\|^2$$

$$\|b_3^*+\mu_{32}b_2^*\|^2 \ge 3/4\cdot\|b_2^*\|$$

$$\|b_3^*\|^2\ge\frac{1}{2}\|b_2^*\|^2 \Rightarrow \|b_2^*\|^2\ge\left(\frac{1}{2}\right)^2\|b_1^*\|^2$$

$$\Rightarrow \|b_i^*\|^2 \ge \left(\frac{1}{2}\right)^{i-1}\|b_1^*\|^2$$

$$\Rightarrow \|b_n^*\|^2 \le (SV)^2\cdot 2^{n-1}.$$

$$\Rightarrow \|b_1\| \le 2^{\frac{n-1}{2}}\cdot SV(A)$$

The *potential* of a lattice basis B is defined as

$$\phi(B) = \|b_1^*\|^{2n} \|b_2^*\|^{2(n-1)} \|b_3^*\|^{2(n-2)} \cdots \|b_n^*\|^2 \tag{12}$$

What happens after a swap.

$c_1^*, \ldots, c_{j-1}^*, c_j^*, c_{j+1}^*, \ldots, c_n^*$

$$\frac{\phi(C)}{\phi(B)} = \frac{\|c_1^*\|^{2n} \, \|c_2^*\|^{2(n-1)} \cdots \|c_j^*\|^{2(n-j+1)} \, \|c_{j+1}^*\|^{2(n-j)} \cdots\cdots}{\|b_1^*\|^{2n} \, \|b_2^*\|^{2(n-1)} \cdots \|b_j^*\|^{2(n-j+1)} \, \|b_{j+1}^*\|^{2(n-j)} \cdots}$$

equal.

$$= \boxed{\frac{\|c_j^*\|^{2(n-j+1)} \cdot \|c_{j+1}^*\|^{2(n-j)}}{\|b_j^*\|^{2(n-j+1)} \cdot \|b_{j+1}^*\|^{2(n-j)}} \cdot \frac{\|b_j^*\|^2}{\|c_j^*\|^2}} \cdot \frac{\|c_j^*\|^2}{\|b_j^*\|^2} \leq \left(\frac{3}{4}\right)$$

Potential is an integer

$B_i = B^* \cdot \begin{pmatrix} 1 & \mu \\ & 1 \\ 0 & \end{pmatrix}$

Let B_i be the matrix consisting of the first i columns of B. Then we have

$$\det(B_i^T \cdot B_i) = \|b_1^*\|^2 \cdots \|b_i^*\|^2 \in \mathbb{N} \tag{14}$$

Consequently we have

$$\phi(B) = \prod_{i=1}^{n} \det(B_i^T \cdot B_i) \in \mathbb{N}. \tag{15}$$

$B_i^T \cdot B_i = \left[\begin{array}{c|c} 1 & \\ \mu & 1 \end{array}\,\middle|\, 0\right] \cdot B^{*T} \cdot B^* \cdot \begin{bmatrix} 1 \cdots \mu \\ 1 \\ \hline 0 \end{bmatrix}$

$= \left[\begin{array}{c|c} 1 & \\ \mu & 1 \end{array}\,\middle|\, 0\right] \begin{bmatrix} \|b_1^*\|^2 & & \\ & \ddots & \\ & & \|b_n^*\|^2 \end{bmatrix} \cdot \begin{bmatrix} 1 \cdots \mu \\ 1 \\ \hline 0 \end{bmatrix}$

$= \left[\begin{array}{c|c} 1 & \\ \mu & 1 \end{array}\,\middle|\, 0\right] \cdot \begin{bmatrix} \|b_1^*\|^2 & & \\ & \ddots & \\ & & \|b_i^*\|^2 \\ \hline & 0 & \end{bmatrix} \begin{bmatrix} 1 \cdots \mu \\ 1 \\ \hline 0 \end{bmatrix}$

$= \begin{bmatrix} 1 & \\ \mu & 1 \end{bmatrix} \cdot \begin{bmatrix} \|b_1^*\|^2 & \\ & \|b_i^*\|^2 \end{bmatrix} \cdot \begin{pmatrix} 1 & \mu \\ & 1 \end{pmatrix}$

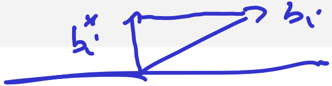
$\det(B_i^T \cdot B_i) \in \mathbb{Z}$

$\|$

$\|b_1^*\|^2 \cdots \|b_i^*\|^2$

$\Rightarrow \phi(B) \in \mathbb{N}_{\geq 1}$ if $B \in \mathbb{Z}^{n \times n}$ (non-sing.)

Bounding the number of iterations



Theorem

The LLL-algorithm terminates in $O(n^2(\log n + s))$ iterations, where s is the largest binary encoding length of a coefficient of $B \in \mathbb{Z}^{n \times n}$.

Proof: $\ln(\phi(B))$ is upper bound (forget constant)

$$\left(\tfrac{3}{4}\right)^i \cdot \phi(B) \leq 1 \iff i = O(\ln(\phi(B)))$$

$\|b_i^*\| \leq \|b_i\| \leq M \cdot \sqrt{n}$, M is upper bound on abs value of coeff of B.. 2^s

$$\Rightarrow \phi(B) \leq \left[\left(M \cdot \sqrt{n}\right)^{2n}\right]^n = \left(M \cdot \sqrt{n}\right)^{2n^2}$$

log: $O(n^2 \cdot [\overbrace{\log(M)} + \log(n)])$

Warning : We did not yet show that LLL-Alg

~~runs~~ runs in poly-time, because the numbers in

intermediate bases have to remain of polynomial

encoding length. This however can be

done, we do not do it here!

Ex.

Show that LLL-reduced basis has orthogonality defect

of $2^{?n^2}$

b_1^* approximates SV

Theorem

Let $B \in \mathbb{Z}^{n \times n}$ be LLL-reduced. Then

$$\underline{\|b_1\|^2 = \|b_1^*\|^2} \leq \underline{2^{n-1}}\, \underline{SV(\Lambda(B))}.$$

Proof

- Upon termination: $\mu_{j+1,j}^2 \leq 1/4$
- Since also $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 \geq 3/4\, \|b_j^*\|^2$ and since $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 = \|b_{j+1}^*\|^2 + \mu_{j+1,j}^2 \|b_j^*\|^2$ we have

$$\|b_{j+1}^*\|^2 \geq 1/2 \|b_j^*\|^2 \tag{16}$$

Proof

- Upon termination: $\mu_{j+1,j}^2 \leq 1/4$
- Since also $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 \geq 3/4\, \|b_j^*\|^2$ and since $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 = \|b_{j+1}^*\|^2 + \mu_{j+1,j}^2 \|b_j^*\|^2$ we have

$$\|b_{j+1}^*\|^2 \geq 1/2 \|b_j^*\|^2 \tag{16}$$

Proof

- Upon termination: $\mu_{j+1,j}^2 \leq 1/4$
- Since also $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 \geq 3/4\, \|b_j^*\|^2$ and since $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 = \|b_{j+1}^*\|^2 + \mu_{j+1,j}^2 \|b_j^*\|^2$ we have

$$\|b_{j+1}^*\|^2 \geq 1/2 \|b_j^*\|^2 \tag{16}$$

Proof

- Upon termination: $\mu_{j+1,j}^2 \leq 1/4$
- Since also $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 \geq 3/4\, \|b_j^*\|^2$ and since $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 = \|b_{j+1}^*\|^2 + \mu_{j+1,j}^2 \|b_j^*\|^2$ we have

$$\|b_{j+1}^*\|^2 \geq 1/2 \|b_j^*\|^2 \tag{16}$$

Proof

- Upon termination: $\mu_{j+1,j}^2 \leq 1/4$
- Since also $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 \geq 3/4\,\|b_j^*\|^2$ and since $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 = \|b_{j+1}^*\|^2 + \mu_{j+1,j}^2\|b_j^*\|^2$ we have

$$\|b_{j+1}^*\|^2 \geq 1/2\|b_j^*\|^2 \tag{16}$$

Proof

- Upon termination: $\mu_{j+1,j}^2 \leq 1/4$
- Since also $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 \geq 3/4\,\|b_j^*\|^2$ and since $\|b_{j+1}^* + \mu_{j+1,j}\, b_j^*\|^2 = \|b_{j+1}^*\|^2 + \mu_{j+1,j}^2 \|b_j^*\|^2$ we have

$$\|b_{j+1}^*\|^2 \geq 1/2\|b_j^*\|^2 \tag{16}$$