

# The LLL Algorithm for Basis Reduction

Ramesh Hariharan  
Strand Life Sciences

26 Feb 2009

## The Setting

- A set of  $n$  linearly independent vectors with integer entries.
- The lattice generated by these vectors is the set of all integer linear combinations.
- Given a vector  $p$  in this lattice, the goal is to find another whose length is at most  $2^{(n-1)/2}|p|$ .
- Basis reduction itself is a means to achieve this goal. It finds a basis (still over the integers)  $b_1 \dots b_n$  for this lattice with the following property: the associated orthogonalized basis comprising rational vectors  $b_1^* \dots b_n^*$  satisfy  $|b_{i+1}^*|^2 \geq |b_i^*|^2/2$ .
- Note that  $|b_1| \leq 2^{(n-1)/2}|p|$  because  $|p| \geq \min\{|b_1^*|, \dots, |b_n^*|\}$  and  $b_1^* = b_1$  (why?).

## The Setting

- A set of  $n$  linearly independent vectors with integer entries.
- The lattice generated by these vectors is the set of all integer linear combinations.
- Given a vector  $p$  in this lattice, the goal is to find another whose length is at most  $2^{(n-1)/2}|p|$ .
- Basis reduction itself is a means to achieve this goal. It finds a basis (still over the integers)  $b_1 \dots b_n$  for this lattice with the following property: the associated orthogonalized basis comprising rational vectors  $b_1^* \dots b_n^*$  satisfy  $|b_{i+1}^*|^2 \geq |b_i^*|^2/2$ .
- Note that  $|b_1| \leq 2^{(n-1)/2}|p|$  because  $|p| \geq \min\{|b_1^*|, \dots, |b_n^*|\}$  and  $b_1^* = b_1$  (why?).

## The Setting

- A set of  $n$  linearly independent vectors with integer entries.
- The lattice generated by these vectors is the set of all integer linear combinations.
- Given a vector  $p$  in this lattice, the goal is to find another whose length is at most  $2^{(n-1)/2}|p|$ .
- Basis reduction itself is a means to achieve this goal. It finds a basis (still over the integers)  $b_1 \dots b_n$  for this lattice with the following property: the associated orthogonalized basis comprising rational vectors  $b_1^* \dots b_n^*$  satisfy  $|b_{i+1}^*|^2 \geq |b_i^*|^2/2$ .
- Note that  $|b_1| \leq 2^{(n-1)/2}|p|$  because  $|p| \geq \min\{|b_1^*|, \dots, |b_n^*|\}$  and  $b_1^* = b_1$  (why?).

## The Setting

- A set of  $n$  linearly independent vectors with integer entries.
- The lattice generated by these vectors is the set of all integer linear combinations.
- Given a vector  $p$  in this lattice, the goal is to find another whose length is at most  $2^{(n-1)/2}|p|$ .
- Basis reduction itself is a means to achieve this goal. It finds a basis (still over the integers)  $b_1 \dots b_n$  for this lattice with the following property: the associated orthogonalized basis comprising rational vectors  $b_1^* \dots b_n^*$  satisfy  $|b_{i+1}^*|^2 \geq |b_i^*|^2/2$ .
- Note that  $|b_1| \leq 2^{(n-1)/2}|p|$  because  $|p| \geq \min\{|b_1^*|, \dots, |b_n^*|\}$  and  $b_1^* = b_1$  (why?).

## The Setting

- A set of  $n$  linearly independent vectors with integer entries.
- The lattice generated by these vectors is the set of all integer linear combinations.
- Given a vector  $p$  in this lattice, the goal is to find another whose length is at most  $2^{(n-1)/2}|p|$ .
- Basis reduction itself is a means to achieve this goal. It finds a basis (still over the integers)  $b_1 \dots b_n$  for this lattice with the following property: the associated orthogonalized basis comprising rational vectors  $b_1^* \dots b_n^*$  satisfy  $|b_{i+1}^*|^2 \geq |b_i^*|^2/2$ .
- Note that  $|b_1| \leq 2^{(n-1)/2}|p|$  because  $|p| \geq \min\{|b_1^*|, \dots, |b_n^*|\}$  and  $b_1^* = b_1$  (why?).

## The Algorithm

- Start with basis  $b_1 \dots b_n$  and associated rational orthogonal basis  $b_1^* \dots b_n^*$ .
- Set  $i = 2$  and repeat the following two steps until  $i > n$ .
- Update  $b_i$  by subtracting components along  $b_{i-1} \dots b_1$  so it is still an integer vector and additionally, it is as orthogonal as possible to each of  $b_{i-1} \dots b_1$ .
- If  $i > 1$  and  $|b_i^*| < |b_{i-1}^*|^2/2$ , then exchange  $b_{i-1}, b_i$  and update the  $b_i^*, b_{i-1}^*$  appropriately, set  $i = i - 1$ . Otherwise set  $i = i + 1$ .

## The Algorithm

- Start with basis  $b_1 \dots b_n$  and associated rational orthogonal basis  $b_1^* \dots b_n^*$ .
- Set  $i = 2$  and repeat the following two steps until  $i > n$ .
- Update  $b_i$  by subtracting components along  $b_{i-1} \dots b_1$  so it is still an integer vector and additionally, it is as orthogonal as possible to each of  $b_{i-1} \dots b_1$ .
- If  $i > 1$  and  $|b_i^*| < |b_{i-1}^*|^2/2$ , then exchange  $b_{i-1}, b_i$  and update the  $b_i^*, b_{i-1}^*$  appropriately, set  $i = i - 1$ . Otherwise set  $i = i + 1$ .

## The Algorithm

- Start with basis  $b_1 \dots b_n$  and associated rational orthogonal basis  $b_1^* \dots b_n^*$ .
- Set  $i = 2$  and repeat the following two steps until  $i > n$ .
- Update  $b_i$  by subtracting components along  $b_{i-1} \dots b_1$  so it is still an integer vector and additionally, it is as orthogonal as possible to each of  $b_{i-1} \dots b_1$ .
- If  $i > 1$  and  $|b_i^*| < |b_{i-1}^*|^2/2$ , then exchange  $b_{i-1}, b_i$  and update the  $b_i^*, b_{i-1}^*$  appropriately, set  $i = i - 1$ . Otherwise set  $i = i + 1$ .

## The Algorithm

- Start with basis  $b_1 \dots b_n$  and associated rational orthogonal basis  $b_1^* \dots b_n^*$ .
- Set  $i = 2$  and repeat the following two steps until  $i > n$ .
- Update  $b_i$  by subtracting components along  $b_{i-1} \dots b_1$  so it is still an integer vector and additionally, it is as orthogonal as possible to each of  $b_{i-1} \dots b_1$ .
- If  $i > 1$  and  $|b_i^*| < |b_{i-1}^*|^2/2$ , then exchange  $b_{i-1}, b_i$  and update the  $b_i^*, b_{i-1}^*$  appropriately, set  $i = i - 1$ . Otherwise set  $i = i + 1$ .

## Analysis

- If  $b_i$  is as orthogonal as possible to each of  $b_{i-1} \dots b_1$ , then its component along each of  $b_{i-1} \dots b_1$  has length at most  $1/2$ . (Why?)
- If  $b_{i-1}, b_i$  are exchanged then  $|b_{i-1}^{**}|^2 < 3/4|b_{i-1}^*|^2$  and  $|b_i^{**}| \leq |b_i^*|$ , where the double-star superscript denotes the updated values of the orthogonalized vectors. (Why?)
- If the process converges, then we have what we want, i.e.,  $|b_{i+1}^*|^2 \geq |b_i^*|^2/2$ .
- And the process does converge (Why? Hint consider  $\prod_{1 \leq i \leq n} (\prod_{1 \leq j \leq i} |b_j^*|^2)$ ).
- How large do the numbers grow?

## Analysis

- If  $b_i$  is as orthogonal as possible to each of  $b_{i-1} \dots b_1$ , then its component along each of  $b_{i-1} \dots b_1$  has length at most  $1/2$ . (Why?)
- If  $b_{i-1}, b_i$  are exchanged then  $|b_{i-1}^{**}|^2 < 3/4|b_{i-1}^*|^2$  and  $|b_i^{**}| \leq |b_i^*|$ , where the double-star superscript denotes the updated values of the orthogonalized vectors. (Why?)
- If the process converges, then we have what we want, i.e.,  $|b_{i+1}^*|^2 \geq |b_i^*|^2/2$ .
- And the process does converge (Why? Hint consider  $\prod_{1 \leq i \leq n} (\prod_{1 \leq j \leq i} |b_j^*|^2)$ ).
- How large do the numbers grow?

## Analysis

- If  $b_i$  is as orthogonal as possible to each of  $b_{i-1} \dots b_1$ , then its component along each of  $b_{i-1} \dots b_1$  has length at most  $1/2$ . (Why?)
- If  $b_{i-1}, b_i$  are exchanged then  $|b_{i-1}^{**}|^2 < 3/4|b_{i-1}^*|^2$  and  $|b_i^{**}| \leq |b_i^*|$ , where the double-star superscript denotes the updated values of the orthogonalized vectors. (Why?)
- If the process converges, then we have what we want, i.e.,  $|b_{i+1}^*|^2 \geq |b_i^*|^2/2$ .
- And the process does converge (Why? Hint consider  $\prod_{1 \leq i \leq n} (\prod_{1 \leq j \leq i} |b_j^*|^2)$ ).
- How large do the numbers grow?

## Analysis

- If  $b_i$  is as orthogonal as possible to each of  $b_{i-1} \dots b_1$ , then its component along each of  $b_{i-1} \dots b_1$  has length at most  $1/2$ . (Why?)
- If  $b_{i-1}, b_i$  are exchanged then  $|b_{i-1}^{**}|^2 < 3/4|b_{i-1}^*|^2$  and  $|b_i^{**}| \leq |b_i^*|$ , where the double-star superscript denotes the updated values of the orthogonalized vectors. (Why?)
- If the process converges, then we have what we want, i.e.,  $|b_{i+1}^*|^2 \geq |b_i^*|^2/2$ .
- And the process does converge (Why? Hint consider  $\prod_{1 \leq i \leq n} (\prod_{1 \leq j \leq i} |b_j^*|^2)$ ).
- How large do the numbers grow?

## Analysis

- If  $b_i$  is as orthogonal as possible to each of  $b_{i-1} \dots b_1$ , then its component along each of  $b_{i-1} \dots b_1$  has length at most  $1/2$ . (Why?)
- If  $b_{i-1}, b_i$  are exchanged then  $|b_{i-1}^{**}|^2 < 3/4|b_{i-1}^*|^2$  and  $|b_i^{**}| \leq |b_i^*|$ , where the double-star superscript denotes the updated values of the orthogonalized vectors. (Why?)
- If the process converges, then we have what we want, i.e.,  $|b_{i+1}^*|^2 \geq |b_i^*|^2/2$ .
- And the process does converge (Why? Hint consider  $\prod_{1 \leq i \leq n} (\prod_{1 \leq j \leq i} |b_j^*|^2)$ ).
- How large do the numbers grow?