On the Structure of Reduced Kernel Lattice Bases

Karen Aardal Frederik von Heymann Andrea Lodi Laurence Wolsey

Consider the integer linear problem

$$\max\{\boldsymbol{c}\boldsymbol{x} \mid A\boldsymbol{x} = \boldsymbol{b}, \boldsymbol{x} \in \mathbb{Z}^n_+\}$$

where $A \in \mathbb{Z}^{m\times n}$ with $\mathrm{HNF}(A) = [I, 0]$.

Reformulation:

$$\boldsymbol{x} = \boldsymbol{x}^0 + Q\boldsymbol{\lambda}, \text{ where}$$

$\boldsymbol{x}^0 \in \mathbb{Z}^n$ satisfies $A\boldsymbol{x}^0 = \boldsymbol{b}$, $\boldsymbol{\lambda} \in \mathbb{Z}^{n-m}$ and $Q \in \mathbb{Z}^{n\times n-m}$ is an LLL-reduced Basis of $\ker_{\mathbb{Z}}(A)$.

Why do we do this?

- Q has some structure we can use for branching;
- (rounding) cuts are only limited by feasible points.

What does Q look like?

Observation: There is some dense interaction in some variables (whose number seems very stable and almost independent of the total number of variables), and otherwise substitutions.

Why is this happening?

Assumptions:

- $A = \boldsymbol{a} = (a_1, \dots, a_n)$;
- $a_1, \dots, a_n \in \{l, l+1, \dots, u\}$ with $0 < l < u$;
- $\ker_{\mathbb{Z}}(A)$ is given by a basis where $\boldsymbol{b}_1\mathbb{Z} + \cdots + \boldsymbol{b}_k\mathbb{Z} = \ker_{\mathbb{Z}}(\boldsymbol{a}) \cap (\mathbb{Z}^{k+1} \times 0^{n-k-1})$.

Theorem: With increasing k, the probability that $\boldsymbol{b}_k$ and $\boldsymbol{b}_{k+1}$ are switched during the LLL-reduction goes to zero.

Tools:

- $Pr(\gcd(a_1, \dots, a_k) > 1) \lesssim \frac{u}{2^{k-1}}$.
- $\|\boldsymbol{b}^*_k\|^2 = \dfrac{\sum_{i=1}^{k+1} a_i^2}{\sum_{i=1}^{k} a_i^2}$.
- $1 - \Theta(\frac{1}{k}) \le \mathbb{E}\left[\|\boldsymbol{b}^*_{k+1}\|^2 / \|\boldsymbol{b}^*_k\|^2\right] \le 1 + \Theta(\frac{1}{k})$.
- $Pr\left(\|\boldsymbol{b}^*_{k+1}\|^2 / \|\boldsymbol{b}^*_k\|^2 < y\right) \to 0$ when $y \in (1/4, 1)$.

Conclusion: $\|\boldsymbol{b}^*_{k+1} + \mu_{k+1,k}\boldsymbol{b}^*_k\|^2 \ge y\|\boldsymbol{b}^*_k\|^2$ with high probability, which is the ordering criterion of LLL.

# var	$l,u = 100, 1000$			$l,u = 15000, 150000$		
	avg # dense	min # dense	max # dense	avg # dense	min # dense	max # dense
50	22.4	18	28	28.6	26	32
100	24.1	19	33	30.2	26	36
200	26.7	20	40	31.1	27	44