max planck institut informatik

SAARLAND UNIVERSITY
COMPUTER SCIENCE

Michael Sagraloff **Winter term 2017/18**

Computer Algebra

https://www.mpi-inf.mpg.de/departments/algorithms-complexity/teaching/winter17/comp-alg/

Assignment sheet 12 due: Monday, January 29

Exercise 1: LLL Algorithm, an Example (4 points)

Trace the LLL Algorithm to compute a "short" vector in the lattice spanned by the vectors $f_1 := (22, 11, 5)^t$, $f_2 := (13, 6, 3)^t$, and $f_3 := (-5, -2, -1)^t$. How does the computed vector compare to the shortest vector in the lattice?

Exercise 2: Bit Complexity of the LLL Algorithm (4 points)

Let $f = (f_1, \ldots, f_m)$ be a given basis with linearly independent vectors $f_i \in \mathbb{Z}^n$, and let L, with $L \geq \log n$, be an upper bound on the length of the entries of each f_i. Show that all intermediate results produced by the LLL algorithm (when applied to f) have bitsize $O(nL)$ and derive a bound on the bit complexity of the LLL algorithm that is polynomial in n and L.

Exercise 3: Evaluation Bounds (4 points)

Let f and g be coprime polynomials of degree n or less and with integer coefficients of length less than L. Show that, for any root α of f, it holds that

$$|g(\alpha)| > \frac{1}{n^n \cdot (1 + 2^L)^{3n}}.$$

Hint: Notice that $0 \neq \mathrm{res}(f, g) = u(x) \cdot f(x) + v(x) \cdot g(x)$ *for appropriate polynomials* u *and* v*. Remember how to compute* u *and* v *as determinants of Sylvester-like matrices in order to bound the bitsize of their coefficients.*

Exercise 4: Simultaneous Diophantine Approximation (2 + 4 points)

(a) Let $f := (f_1, \ldots, f_m) \in \mathbb{R}^{n \times m}$ be a basis and $D := \det(f^t \cdot f)$. Show that, for a corresponding reduced basis $\bar{f} := (\bar{f}_1, \ldots, \bar{f}_m)$, it holds that $\|\bar{f}_1\| \leq 2^{\frac{m-1}{4}} \cdot D^{1/m}$.

(b) Dirichlet's theorem states that, for arbitrary rational numbers $\alpha_1, \ldots, \alpha_n$ and an arbitrary positive integer L, there exists a positive integer N, with $N \leq 2^{L \cdot (n-1)}$, such that

$$|N \cdot \alpha_i - \lfloor N \cdot \alpha_i \rceil| \leq 2^{-L} \quad \text{for all } i. \tag{1}$$

Give a polynomial-time algorithm to compute a positive integer N, with $N \leq 2^{nL+n^2}$, such that (1) holds.

Hint: Consider the lattice spanned by the vectors $f_1 := (\alpha_1, \ldots, \alpha_n, c)^t$, $f_2 := (1, 0, , \ldots, , 0)^t$, $f_3 := (0, 1, 0, \ldots, 0)^t, \ldots, f_{n+1} := (0, \ldots, 0, 1)^t$*, with some* $c \in \mathbb{Q}^+$*, and compute a short vector* v *using the LLL algorithm. Choose* c *sufficiently small such that* $\|v\| \leq 2^{-L}$ *is guaranteed.*