Script Skeleton: Algebraic Complexity Theory*
Optimal Algorithms in Computer Algebra

Martin Ziegler

ziegler@mathematik.tu-darmstadt.de

* Synopsis to a lecture held from mid of April to mid of July 2014 at the TU Darmstadt in reverence to PETER BÜRGISSER

1 Motivating Examples for Algebraic Models of Computation

Question 1.1 *What is the least number $\ell(n)$ of multiplications to calculate X^n from given X?*

Let $\mathrm{lb}(n) := \lceil \log_2(n+1) \rceil$ denote the length of n's binary expansion and $\#_1 \mathrm{bin}(n)$ the number of 1s in it.

- upper bound $\ell(n) \le \mathrm{lb}(n) - 2 + \#_1 \mathrm{bin}(n) \le 2\log_2(n)$: by induction
- lower bound $\ell(n) \ge \lceil \log_2 n \rceil = \mathrm{lb}(n-1)$ since deg $\le 2^\ell$
- upper bound *with* division: $\ell'(n) \le \mathrm{lb}(n+1) - 1 + \#_1 \mathrm{bin}(n)/2 \le \frac{3}{2} \cdot \log_2 n$
- improved upper bound $\ell(n) \le \log_2(n) + \mathcal{O}\big(\frac{\log n}{\log\log n}\big)$: see Exercises
- improved lower bound $\ell(n) \ge \log_2 n + 0.3 \cdot \log_2\big(\#_1 \mathrm{bin}(n)\big)$:

Lemma 1.2. *Let* $F_0 := 0$, $F_1 := 1$, $F_{n+2} := F_{n+1} + F_n$, $\quad \gamma := (1+\sqrt{5})/2 \approx 1.62$.

a) $F_n = \big(\gamma^n - (-\gamma)^{-n}\big)/\sqrt{5}$, $\quad F_{n+3} \le 2 \cdot \gamma^n$.
b) *Consider an optimal sequence of multiplications* $T_k := T_{k_1} \cdot T_{k_2}$, $1 \le k \le K := \ell(n)$, *where* $T_0 := X$ *and* $0 \le k_1, k_2 < k$. *W.l.o.g. suppose* $\deg T_k < \deg T_{k+1}$ *and write* $G := \{k : \deg T_k = 2\deg T_{k-1}\}$ *for the* giant steps, $B := \{k : \deg T_k < 2\deg T_{k-1}\}$ *for the* baby steps.
Then $\#_1 \mathrm{bin}(n) \le 2^{\#B}$ *and* $n = \deg(T_K) \le 2^{\#G} \cdot \gamma^{\#B}$: *induction and example* | g | b | b |
c) $\ell(n) = K = \#G + \#B \ge (\log_2 n - \#B \cdot \log_2 \gamma) + \#B$, *where* $1 - \log_2 \gamma \ge 0.3$

See [1, EXERCISE 1.6].

Question 1.3 *Fix a polynomial $f \in \mathbb{C}[X]$. What is the least number $\ell(f)$ of arithmetic operations (additions/subtractions, multiplications) that compute $f(x)$ from given x and some complex constants?*

- upper bound $\ell(f) \le 2\deg(f) - 1$: Horner
- lower bound $\ell(f) \ge \lceil \log_2(\deg f) \rceil$
- improved upper bound $\ell(f) \le \deg(f) + \lfloor \deg(f)/2 \rfloor + 2$ (Knuth 1962):

Let $\mathbb{F}$ denote a field and $f = \sum_{j=0}^{d} \alpha_j X^j \in \mathbb{F}[X]$ a polynomial of degree d. Suppose that $h(Y) := \sum_{2j+1 \le d} \alpha_{2j+1} Y^j$ is either constant or a product of linear factors in $\mathbb{F}[Y]$. Then there exists a straight-line program computing f in $\mathbb{F}[X]$ from X and X^2 and some elements from $\mathbb{F}$ using at most $\lfloor d/2 \rfloor + 1$ multiplications and d additions/subtractions:
Write $h(Y) = (Y - \xi) \cdot h_1(Y)$ and $g(Y) = (Y - \xi) \cdot g_1(Y) + \eta$ where $g(Y) := \sum_{2j \le d} \alpha_{2j} Y^j$.
Then $f(X) = g(X^2) + X \cdot h(X^2) = (X^2 - \xi) \cdot \big(g_1(X^2) + X \cdot h_1(X^2)\big) + \eta$ can be calculated from $X, X^2, \xi, \eta, g_1(X^2) + X \cdot h_1(X^2)$ using 1 multiplication and 2 additions/subtractions.

Reminder 1.4 (Asymptotic growth) *Fix $f, g : \mathbb{N} \to \mathbb{N}$.*

- $f \in \mathcal{O}(g) \quad \Leftrightarrow \quad \limsup_n f(n)/g(n) < \infty$
- $f \in o(g) \quad \Leftrightarrow \quad \limsup_n f(n)/g(n) = 0$
- $f \in \Omega(g) \quad \Leftrightarrow \quad \limsup_n f(n)/g(n) > 0$
  (Hardy–Littlewood semantics, not *Knuth's stronger* $\liminf_n f(n)/g(n) > 0$*)*

- $f \in \Theta(g) \quad \Leftrightarrow \quad 0 < \liminf_n f(n)/g(n) \le \limsup_n f(n)/g(n) < \infty$

Question 1.5 (Polynomial Multiplication) *What is (the asymptotic growth of) the least number $\mathcal{M}(n)$ of arithmetic operations to produce (the coefficient list of) $p \cdot q$ from given (coefficient lists of any) polynomials p, q of $\deg(p), \deg(q) \le n$?*

- upper bound $(n+1)\cdot(n+2)-1$: high-school method
- lower bound $2n+1$
- upper bound $\mathcal{O}(n^{\log_2 3}) \subseteq \mathcal{O}(n^{1.585})$: Karatsuba

$$(a+b\cdot x^m)\cdot(c+d\cdot x^m) = u + v\cdot x^m + w\cdot x^{2m},$$
$$\text{where} \quad u := a\cdot c,\ w := b\cdot d,\ v := (a+b)\cdot(c+d) - u - w$$

  hence $\mathcal{M}(2n) \le 3\cdot\mathcal{M}(n)+4$ and $\mathcal{M}(2^k) \le 3^k\cdot T(1) + 4\cdot\frac{3^k-1}{3-1}$.
- upper bound $\mathcal{O}(n^{1+\varepsilon})$ for any fixed $\varepsilon > 0$: Exercises
- upper bound $\mathcal{O}(n\cdot\log n)$ over $\mathbb{C}$ using FFT

Question 1.6 (Matrix Multiplication) *What is (the asymptotic growth of) the least number of arithmetic operations to produce $A\cdot B$ from given $n\times n$–matrices?*

- upper bound $2n^3$
- lower bound n^2
- upper bound $\mathcal{O}(n^{\log_2 7}) \subseteq \mathcal{O}(n^{2.81})$:
  For $A = (A_{ij}), B = (B_{ij}) \in R^{2\times 2}$ it holds $A\cdot B = C$ where

$$C_{11} = M_1 + M_4 - M_5 + M_7, \qquad C_{12} = M_3 + M_5,$$
$$C_{21} = M_2 + M_4, \qquad C_{22} = M_1 - M_2 + M_3 + M_6$$

$$M_1 := (A_{12}+A_{22})\cdot(B_{11}+B_{22}), \quad M_2 := (A_{21}+A_{22})\cdot B_{11},$$
$$M_3 := A_{11}\cdot(B_{12}-B_{21}), \quad M_4 := A_{22}\cdot(B_{21}-B_{11}), \quad M_5 := (A_{11}+A_{12})\cdot B_{22},$$
$$M_6 := (A_{21}-A_{11})\cdot(B_{11}+B_{12}), \quad M_7 := (A_{12}-A_{22})\cdot(B_{21}+B_{22})$$

- upper bound $\mathcal{O}(n^{2.373})$: world record, de Gall `arXiv:1401.7714`

Definition 1.7 (Straight-Line Program).

a) Let $\mathcal{S} = \big(S, (c_i), (f_j)\big)$ denote a structure with constants $c_i \in S$ and (possibly partial) functions $f_j :\subseteq S^{a_j} \to S$ of arities $a_j \in \mathbb{N}$. A Straight-Line Program *P (over the signature of this structure and in variables $X_1, \ldots, X_n$) is a finite sequence of assignments $Z_k := c_i$ and $Z_k := X_\ell$ ($1 \le \ell \le n$) and $Z_k := f_j(Z_{k_1}, \ldots, Z_{k_{a_j}})$, $1 \le k_1, \ldots, k_{a_j} < k$.*

b) When assigned values $x_1, \ldots, x_n \in S$ to $X_1, \ldots, X_n$, the program computes *(the set of results consisting of $(x_1, \ldots, x_n) =: \vec{x}$ and of) $Z_1, \ldots, Z_K$; the final result is $Z_K =: P(\vec{x})$. However if any intermediate operation $f_j(Z_{k_1}, \ldots, Z_{k_{a_j}})$ happens to be undefined, then so is $P(\vec{x}) := \perp$.*

c) A cost function *C assigns to each f_j some cost $C(f_j) \ge 0$. The cost of a straight-line program P is the sum of the costs of the f_j occurring. The* length *$|P|$ of P means its cost with respect to constant cost function $f_j \mapsto 1$.*

d) The (straight-line) complexity *$\mathcal{C}_C(\mathcal{F})$ of a family $\mathcal{F}$ of functions $f :\subseteq S^{a_f} \to S$ with respect to a cost function C is the least cost of a straight-line program P over $\mathcal{S}$. computing $\mathcal{F}$.*

2 Examples of (Almost) Tight Complexity Bounds

2.1 Nonscalar Cost of Polynomial Multiplication: Interpolation and Dimension Bound

In Karatsuba's Algorithm and its generalizations, the total asymptotic cost is governed by the number of multiplications of the smaller polynomials; see Exercise 1. So we now investigate the complexity of polynomial multiplication when charging only multiplications among the coefficient algebra while additions and scaling by constants are considered free.

Theorem 2.1. *Fix some $\mathbb{F}$–algebra $\mathcal{A}$ with binary addition $+ : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ and unary scalings $\times_c : \mathcal{A} \ni a \mapsto c \cdot a \in \mathcal{A}$ by constants c from the infinite field $\mathbb{F}$.*

a) There is a straight-line program over $\mathcal{S} := \big(\mathcal{A}, (), (+, \times_c : c \in \mathbb{F})\big)$ which, for arbitrary but fixed distinct $x_1, \ldots, x_n \in \mathbb{F}$ and on input of $y_1, \ldots, y_n \in \mathcal{A}$, calculates (the unique) $a_0, \ldots, a_{n-1} \in \mathcal{A}$ with $\sum_{k=0}^{n-1} a_k \cdot x_\ell^k = y_\ell$ for $\ell = 1, \ldots, n$.

b) Consider the algebra $\mathcal{A} := \mathbb{F}[A_0, \ldots, A_n, B_0, \ldots, B_m]$ in $n+m+2$ variables $A_0, \ldots A_n, B_0, \ldots B_m$. The set $\big\{ \sum_{i+j=\ell} A_i \cdot B_j : 0 \le \ell \le n+m \big\}$ can be calculated from $A_0, \ldots, B_{m-1}$ by a straight-line program over $\mathcal{S}$ using $n+m+1$ operations "$\times$" (and arbitrary many "$+$" and "$\times_c$").

c) For $x_1, \ldots, x_N, y_1, \ldots, y_M \in \mathcal{A}$ consider the $\mathbb{F}$–vector spaces $X := \{\lambda_1 x_1 + \cdots + \lambda_N x_N : \lambda_i \in \mathbb{F}\}$ and $Y := \{\mu_1 y_1 + \cdots + \mu_M y_M : \mu_j \in \mathbb{F}\}$. Then any straight-line program over $\mathcal{S}$ computing $\{y_1, \ldots, y_M\}$ from $(x_1, \ldots, x_N)$ contains at least $\dim_{\mathbb{F}}(X + Y + \mathbb{F}) - \dim_{\mathbb{F}}(X + \mathbb{F})$ algebra multiplications "$\times$".

d) The straight-line program from Item b) is optimal!

See [1, THEOREM 2.2].

2.2 Discrete Fourier Transform: Cooley–Tukey FFT and Morgenstern's Volume Bound

Consider the N-dimensional discrete Fourier-transform

$$\mathcal{F}_N : \mathbb{C}^N \ni (x_0, \ldots, x_{N-1}) \mapsto \big(\sum_{\ell=0}^{N-1} \exp(2\pi i \cdot k \cdot \ell / N) \cdot x_\ell \big)_{k=0,\ldots,N-1} \in \mathbb{C}^N \ .$$

Theorem 2.2. *Fix $C \ge 1$ and consider the structure $\mathcal{S}_C := \big(\mathbb{C}, \mathbb{C}, (+, \times_\lambda : |\lambda| \le C)\big)$ where $\times_c : \mathbb{C} \ni z \mapsto c \cdot z \in \mathbb{C}$ denotes unary complex multiplication by constants c of modulus at most C.*

a) For $N = 2^n$, $\mathcal{F}_N$ can be computed by a straight-line program over $\mathcal{S}_1$ of length $\mathcal{O}(N \cdot \log N)$.

b) Consider a straight-line program P over $\mathcal{S}_C$ in N variables.
Each 'line' ℓ of P computes an affine linear function $\varphi_\ell : \mathbb{C}^N \to \mathbb{C}$;
and P computes an affine linear map $\Phi_P : \mathbb{C}^N \ni \vec{x} \mapsto A_P \cdot \vec{x} + \vec{b} \in \mathbb{C}^{N+|P|}$,
where $|P|$ denotes the length of P and the first N components are the identity.

c) For $\vec{a}_1, \ldots, \vec{a}_m \in \mathbb{C}^n$ with $m \ge n$ write

$$\Delta(\vec{a}_1, \ldots, \vec{a}_m) := \max\big\{ |\det(\vec{a}_{j_1}, \ldots, \vec{a}_{j_n})| : 1 \le j_1, \ldots, j_n \le m \big\} \ .$$

Then, for $1 \le k, \ell \le m$ and $\lambda \in \mathbb{C}$ with $|\lambda| \ge 1$, it holds

$$\Delta(\vec{a}_1, \ldots, \vec{a}_m, \lambda \cdot \vec{a}_k) \le |\lambda| \cdot \Delta(\vec{a}_1, \ldots, \vec{a}_m) \quad \text{and} \quad \Delta(\vec{a}_1, \ldots, \vec{a}_m, \vec{a}_k + \vec{a}_\ell) \le 2\Delta(\vec{a}_1, \ldots, \vec{a}_m) \ .$$

d) The homogeneous linear map $A_P : \mathbb{C}^n \to \mathbb{C}^{N+|P|}$ from b) satisfies $\Delta(A_P) \leq (2C)^{|P|}$.
e) Subject to scaling by $1/\sqrt{N}$, the matrix $\big(\exp(2\pi i \cdot k \cdot \ell/N)\big)_{0\leq k,\ell<N}$ is unitary and therefore has determinant of absolute value $N^{N/2}$.

See [6, §8] and [1, p.10].
The straight-line program from Item a) is thus optimal up to a constant factor!

2.3 Nonuniform Polynomial Evaluation: Transcendence Degree

Consider fields $\mathbb{F} \subseteq \mathbb{E}$ and recall that $e_1, \ldots, e_n \in \mathbb{E}$ are called *algebraically dependent (over $\mathbb{F}$)* iff there exists a non-zero polynomial $p \in \mathbb{F}[X_1, \ldots, X_n]$ with $p(e_1, \ldots, e_n) = 0$. (For example, $\{\sqrt{2\pi+1}, \pi\}$ is algebraically dependent over $\mathbb{Q}$.) A set $E \subseteq \mathbb{E}$ is algebraically *in*dependent (over $\mathbb{F}$) iff no finite subset of it is algebraically dependent. By definition, $\mathrm{trdeg}_{\mathbb{F}}(\mathbb{E})$ is the largest cardinality of any subset of $\mathbb{E}$ algebraically independent (over $\mathbb{F}$).

Fact 2.3 *a) Any two maximal algebraically independent subsets E, E' of $\mathbb{E}$ (over $\mathbb{F}$) have the same cardinality: exchange lemma + Zorn's Lemma.*
b) $\mathbb{E}$ is algebraic over $\mathbb{F}$ iff $\mathrm{trdeg}_{\mathbb{F}}(\mathbb{E}) = 0$.
c) π and e are transcendental. In particular $\mathrm{trdeg}_{\mathbb{Q}}\{\sqrt{2\pi+1}, \pi\} = 1$.
It is unknown whether $\{\pi, e\}$ is algebraically independent over $\mathbb{Q}$.
d) If $x_1, \ldots, x_d \in \mathbb{A}$ are linearly independent over $\mathbb{Q}$,
then $\exp(x_1), \ldots, \exp(x_d) \in \mathbb{C}$ *are algebraically independent over $\mathbb{Q}$:* Lindemann–Weierstraß
e) It holds $\mathrm{trdeg}_{\mathbb{F}}\big(\mathbb{F}(X_1, \ldots, X_n)\big) = n$,
where $\mathbb{F}(X_1, \ldots, X_n)$ denotes the field of rational functions in n variables over $\mathbb{F}$.
f) For $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{D}$ fields, it holds $\mathrm{trdeg}_{\mathbb{F}}(\mathbb{D}) = \mathrm{trdeg}_{\mathbb{F}}(\mathbb{E}) + \mathrm{trdeg}_{\mathbb{E}}(\mathbb{D})$.
In particular $\mathrm{trdeg}_{\mathbb{F}}\big(\mathbb{E}(x)\big) \leq \mathrm{trdeg}_{\mathbb{F}}(\mathbb{E}) + 1$ *for $x \in \mathbb{D}$.*
g) There exist uncountable subsets of $\mathbb{R}$ algebraically independent over $\mathbb{Q}$.

Theorem 2.4 (Motzkin'55+Belaga'61). *Let $\mathbb{F} \subseteq \mathbb{E}$ denote fields of characteristic 0 and $\mathcal{F} \subseteq \mathbb{E}(\vec{X})$ a finite set of rational functions in indeterminates $(X_1, \ldots, X_n) = \vec{X}$. For $p_j, q_j \in \mathbb{E}[\vec{X}]$ coprime over $\mathbb{F}$ and q_j monic (meaning at least one monomial has coefficient 1), define* $\mathrm{Coeff}_{\mathbb{F}}(p_1/q_1, \ldots, p_m/q_m) \subseteq \mathbb{E}$ *as the field over $\mathbb{F}$ generated by the coefficients from $p_1, \ldots, q_m$.*

a) $\mathrm{Coeff}_{\mathbb{F}}(\mathcal{F})$ *is well-defined and coincides with the field extension* $\mathbb{F}\big(\{f(\vec{x}) : \vec{x} \in \mathbb{F}^n, f \in \mathcal{F}\}\big)$.
b) For $a_j, b_j, c_j, w_j \in \mathbb{E}[\vec{X}]$ with $b_j \neq 0$, $\mathrm{Coeff}_{\mathbb{F}}(w_j + c_j \cdot a_j/b_j : j) \subseteq \mathrm{Coeff}_{\mathbb{F}}(w_j, c_j, a_j, b_j : j)$.
c) Consider the structure $\mathcal{S}' = \big(\mathbb{E}, \mathbb{F}, (\mathbb{E}, +, \times, \div)\big)$. Any straight-line program computing $\mathcal{F}$ over $\mathcal{S}'$ contains at least $\mathrm{trdeg}_{\mathbb{F}}\big(\mathrm{Coeff}_{\mathbb{F}}(\mathcal{F})\big)$ *constants from $\mathbb{E}$.*
d) Consider a straight-line program P over $\mathcal{S} := \big(\mathbb{E}, \mathbb{E}, (+, -, \times, \div)\big)$ computing (intermediate) results $f_1, \ldots, f_N \in \mathbb{E}(X_1, \ldots, X_n)$.
  i) There exist $0 \neq b_j, a_j \in \mathbb{E}[\vec{X}]$, $c_j \in \mathbb{E}$ (j=1,...,N) such that $f_j = c_j \cdot a_j/b_j$ and $\mathrm{trdeg}_{\mathbb{F}}\big(\mathrm{Coeff}_F(a_1, ..a_N, b_1, ..b_N)\big)$ *is at most the number of additions/subtractions in P.*
  ii) There exist $0 \neq v_j, u_j \in \mathbb{E}[\vec{X}]$, $w_j \in \mathbb{E}$ (j=1,...,N) such that $f_j = w_j + u_j/v_j$ and $\mathrm{trdeg}_{\mathbb{F}}\big(\mathrm{Coeff}_F(u_1, \ldots, v_N)\big)$ *is at most twice P's number of multiplications/divisions.*

e) Any straight-line program computing $\mathcal{F}$ over $\mathcal{S}$ contains at least $\operatorname{trdeg}_{\mathbb{F}}\big(\operatorname{Coeff}_{\mathbb{F}}(\mathcal{F})\big) - |\mathcal{F}|$ *additions/subtractions and* $\big(\operatorname{trdeg}_{\mathbb{F}}\big(\operatorname{Coeff}_{\mathbb{F}}(\mathcal{F})\big) - |\mathcal{F}|\big)/2$ *multiplications/divisions.*

See [1, THEOREMS 5.1+5.9].
Knuth's answer to Question 1.3 is thus optimal up to an additive constant!

3 Efficient Algorithms for Polynomials

Recall the *total* degree, $\deg(X^3 \cdot Y^2) = 5$. Let $\mathbb{F}[X]_{<d}$ denote the vector space of polynomials over $\mathbb{F}$ of total degree less than d; and $\mathbb{F}[X]_{=d}$ those homogeneous of degree d. Moreover write $\mathbb{F}[[X]]$ for the algebra of formal power series over $\mathbb{F}$.

3.1 Multivariate Derivatives

Theorem 3.1 (Baur–Strassen). *Fix a field $\mathbb{F}$ of characteristic 0, $0,1 \in C \subseteq \mathbb{F}$, and let P denote a straight-line program in n variables over $\mathcal{S} = \big(\mathbb{F}, C, (+,-,\times,\div)\big)$ computing $f \in \mathbb{F}(X_1,\ldots,X_n)$. Then there exists a straight-line program P' in n variables over $\mathcal{S}$ of length $|P'| \leq 5 \cdot |P|$ simultaneously computing all $f, \partial_1 f, \ldots, \partial_n f$.*

See [1, §7.2].

Lemma 3.2 (Taylor and Leibniz). *For $f \in \mathbb{F}(X_1,\ldots,X_N)$ define*

$$f^{(0)} := f(\vec{0}) \in \mathbb{F}, \qquad f^{(d)} := \sum_{n_1,\ldots n_d=1}^{N} \big(\partial_{n_1} \cdots \partial_{n_d} f\big)(\vec{0}) \cdot X_{n_1} \cdots X_{n_d}/d! \in \mathbb{F}[X_1,\ldots,X_N]_{=d}$$

a) For $f \in \mathbb{F}[X_1,\ldots,X_N]_{<D}$ it holds $f = \sum_{d=0}^{D-1} f^{(d)}$.
b) $(f\cdot g)^{(0)} = (f\cdot g)(\vec{0}) = f^{(0)} \cdot g^{(0)} \in \mathbb{F}$, $(f\cdot g)^{(1)} = f^{(1)} \cdot g^{(0)} + f^{(0)} \cdot g^{(1)}$,
$(f\cdot g)^{(2)} = f^{(2)} \cdot g^{(0)} + f^{(1)} \cdot g^{(1)} + f^{(0)} \cdot g^{(2)}$, and $(f\cdot g)^{(D)} = \sum_{d=0}^{D} f^{(d)} \cdot g^{(D-d)}$.
c) In case $g(\vec{0}) \neq 0$, $u := f/g$ has $u^{(0)} = f^{(0)}/g^{(0)}$, $u^{(1)} = \big(f^{(1)} - u^{(0)} \cdot g^{(1)}\big)/g^{(0)}$,
$u^{(2)} = \big(f^{(2)} - u^{(1)} \cdot g^{(1)} - u^{(0)} \cdot g^{(2)}\big)/g^{(0)}$, and $u^{(D)} = \big(f^{(D)} - \sum_{d=0}^{D-1} u^{(d)} \cdot g^{(D-d)}\big)/g^{(0)}$.

Theorem 3.3 (Strassen'73). *Let $\mathcal{A}$ denote an $\mathbb{F}$–algebra. Suppose $\mathcal{F} \subseteq \mathbb{F}[X_1,\ldots,X_N]_{<D}$ can be computed (on a Zariski–dense subset of $\mathcal{A}^N$) by a straight-line program P over $(\mathcal{A}, \mathcal{C}, +, \times, \div)$ can also be computed by a straight-line program Q over $(\mathcal{A}, \mathcal{C}, +, \times)$ of length $|Q| \leq \mathcal{O}(D^2) \cdot |P|$.*

See [1, §7.1].

3.2 Univariate Polynomial Arithmetic

Abbreviate $\mathcal{S}' := \big(\mathbb{C}, \mathbb{C}, +, \times, \div\big)$.

Theorem 3.4 (Polynomial Multiplication).

a) The product of two polynomials $\bar{p},\bar{q}\in\mathbb{C}[X]$, given by their lists of coefficients (dense representation), can be computed by a straight-line program over $\mathcal{S}'$ of length $\mathcal{O}(N\cdot\log N)$, where $N:=\deg(\bar{p})+\deg(\bar{q})$.

b) The (coefficients of the) product of k given polynomials $\bar{p}_1,\ldots,\bar{p}_k\in\mathbb{C}[X]_{<d}$, can be computed by a straight-line program over $\mathcal{S}'$ of length $\mathcal{O}(N\cdot\log^2 N)$, where $N:=d\cdot k$.

See [1, §2.3].

Lemma 3.5. *a) $\bar{p}=\sum_{n\geq 0}p_nX^n\in\mathbb{F}[[X]]$ has a multiplicative inverse $1/\bar{p}\in\mathbb{F}[[X]]$ iff $p_0\neq 0$; in which case $\bar{q}=\sum_{n\geq 0}q_nX^n:=1/\bar{p}$ is given by $q_0=1/p_0$ and inductively $q_n=-\sum_{m=1}^{n}p_m\cdot q_{n-m}/p_0$.*

b) Suppose $\tilde{q}\in\mathbb{F}[[X]]$ satisfies $\bar{p}\cdot\tilde{q}\equiv 1 \pmod{X^n}$. Then $\tilde{\tilde{q}}:=\tilde{q}\cdot(2-\bar{p}\cdot\tilde{q})$ has $\bar{p}\cdot\tilde{\tilde{q}}\equiv 1 \pmod{X^{2n}}$.

c) Fix polynomials $\bar{a}=\sum_{i=0}^{n}a_iX^i$, $\bar{b}=\sum_{j=0}^{m}b_jX^j$, $\bar{q}=\sum_{k=0}^{m-n}q_kX^k$, and $\bar{r}=\sum_{\ell=0}^{m-1}r_\ell X^\ell$ with $\bar{a}=\bar{b}\cdot\bar{q}+\bar{r}$, where $n:=\deg(\bar{a})\geq\deg(\bar{b})=:m>\deg(\bar{r})$. Then

$$\left(\sum_{i=0}^{n}a_iX^{n-i}\right)/\left(\sum_{j=0}^{m}b_jX^{m-j}\right)\ \equiv\ \sum_{k=0}^{m-n}q_kX^{n-m-k}\pmod{X^{n-m+1}}$$

d) For $x_1,\ldots,x_N\in\mathbb{F}$ and $\bar{a}\in\mathbb{F}[X]$, $\bar{r}:=\bar{a}\operatorname{rem}(X-x_1)\cdots(X-x_N)$ satisfies $\bar{a}(x_n)=\bar{r}(x_n)$.

e) It holds $\bar{a}\operatorname{rem}\bar{p}=(\bar{a}\operatorname{rem}\bar{p}\cdot\bar{q})\operatorname{rem}\bar{p}$.

Theorem 3.6 (Polynomial Division and Multipoint Evaluation).

a) There exists a straight-line program over $\mathcal{S}'$ of length $\mathcal{O}(N\cdot\log N)$ computing, given (the coefficients of) $p\in\mathbb{C}[X]_{<N}$ with $p(0)\neq 0$, (the coefficients of) $1/p \bmod X^N$.

b) Given (the coefficients of) $a,b\in\mathbb{C}[X]$ of $N:=\deg(a)\geq\deg(b)=:M\geq 1$, (the coefficients of) $a \operatorname{div} b$ and $a \operatorname{rem} b$ can be computed by a straight-line program over $\mathcal{S}'$ of length $\mathcal{O}(N\cdot\log N)$.

c) A straight-line program over $\mathcal{S}'$ of length $\mathcal{O}(N\cdot\log^2 N)$ can compute, given (the coefficients of) $p\in\mathbb{C}[X]_{<N}$ and $x_1,\ldots,x_N\in\mathbb{C}$, the values $p(x_1),\ldots,p(x_N)$.

d) A straight-line program over $\mathcal{S}'$ of length $\mathcal{O}\big(Nd\cdot\log^2(Nd)\big)$ can compute, given (the coefficients of) $p_1,\ldots,p_N,q_1,\ldots,q_N\in\mathbb{C}[X]_{<d}$ and $z_1,\ldots,z_{Nd}\in\mathbb{C}$ with $q_j(z_i)\neq 0$, the values $\sum_{j=1}^{N}\frac{p_j(z_i)}{q_j(z_i)}$, $1\leq i\leq Nd$.

e) A straight-line program over $\mathcal{S}'$ of length $\mathcal{O}(N\cdot\log N+\log M)$ can compute, given $p\in\mathbb{C}[X]_{<N}$, $p^M \bmod X^N$.

See [6, §9+§10.10.1], [1, §2.4], and [10, THEOREM 2].

4 Complexity of Matrix Multiplication

4.1 Strassen's Algorithm

4.2 Complexity and Tensor Rank of Bilinear Maps

4.3 Properties of the Tensor Rank

4.4 Exponent of Matrix Multiplication, LUP-Decomposition, and Inversion

4.5 Multipoint Evaluation of Bivariate Polynomials

5 Branching Complexity

Question 5.1 (Sorting) *Given $x_1,\dots,x_n$ in a fixed linearly ordered set, how many comparisons are asymptotically sufficient and necessary to produce a permutation $\pi : [n] \to [n]$ with $x_{\pi(1)} \leq x_{\pi(2)} \leq \cdots \leq x_{\pi(n)}$?*

- upper bound $n \cdot (n+1)/2$: Bubble Sort
- upper bound $\mathcal{O}(n \cdot \log n)$: Merge Sort
- lower bound $\Omega(\log_2 n!) = \mathcal{O}(n \cdot \log n)$:

Definition 5.2 (Decision Tree). *Let $\mathcal{S} = (S, \mathcal{R})$ denote a structure with $\mathcal{R}$ a family of relations $R :\subseteq S^{a_k}$ of arities $a_R \in \mathbb{N}$ and Σ some arbitrary set. A* Decision Tree *T (over $\mathcal{S}$ and Σ and in variables $X_1,\dots,X_n$) is an ordered full binary tree with each internal node u labelled by one of the above relations R_u and by an $a_u := a_{R_u}$–tuple $(X_{u_1},\dots,X_{u_{a_u}})$ of the variables; while leaves v are labelled with elements $\sigma_v \in \Sigma$.*
When assigned values $x_1,\dots,x_n \in S$ to $X_1,\dots,X_n$, T starts at its root and for each internal node u iteratively proceeds to its left or right child depending on $R_u(x_{u_1},\dots,x_{u_{a_u}})$. Upon ending up in a leaf v it outputs $T(x_1,\dots,x_n) := \sigma_v$.

5.1 Randomized Polynomial Identity Testing

Definition 5.3. *Polynomial Identity Testing is the following decision problem:*
Given an expression p composed from variables $X_1,\dots,X_n$ and integer constants using addition $+$ and multiplication $\times$; does this p represent the zero function on $\mathbb{Q}//\mathbb{R}/\mathbb{C}$?

Any such expression p represents a multivariate integer polynomial; but expanding it into monomials can blow up its size:
For instance the determinant of a given $n \times n$–matrix $A = (a_{ij})$ is an n^2–variate polynomial of total degree n in A's entries. Expanded into monomials it consists of $n!$ terms (Leibniz Formula) yet can be evaluated (on a Zariski–dense subset of $\mathbb{F}^{n\times n}$) in $\mathcal{O}(n^3)$ steps by means of Gaussian Elimination.

Lemma 5.4 (Schwartz,Zippel). *Let $\mathbb{F}$ denote a field, $S \subseteq \mathbb{F}$ finite, and $p \in \mathbb{F}[X_1,\dots,X_n]$ a non-zero polynomial of total degree $d \in \mathbb{N}$. Then, for $r_1,\dots,r_n \in S$ chosen independently and uniformly from S at random,*

$$\mathbb{P}[p(r_1,\dots,r_n) = 0] \;\leq\; d/|S| \;\; .$$

5.2 Recap on Semi-Algebraic Geometry

Definition 5.5. *Fix a ring $\mathbb{F} \subseteq \mathbb{R}$ and $d \in \mathbb{N}$.*

a) A set A of real solutions to a system of polynomial equalities (over $\mathbb{F}$) is algebraic *(over $\mathbb{F}$):*

$$\left\{\vec{x} \in \mathbb{R}^d \ : \ p_1(\vec{x}) = \ldots = p_k(\vec{x}) = 0\right\}, \quad p_1, \ldots, p_k \in \mathbb{F}[X_1, \ldots, X_d]$$

b) A constructible *set is a finite Boolean combination of algebraic sets.*
c) A set of solutions to a finite system of polynomial in-/*equalities*

$$\left\{\vec{x} \in \mathbb{R}^d \ : \ p_1(\vec{x}) = \ldots = p_k(\vec{x}) = 0 \ \wedge \ q_1(\vec{x}) > 0 \wedge \ldots \wedge q_\ell(\vec{x}) > 0\right\}$$

with $p_1, \ldots, p_k, q_1, \ldots, q_\ell \in \mathbb{F}[X_1, \ldots, X_d]$ is called basic semi-algebraic *(over $\mathbb{F}$).*
d) A subset of $\mathbb{R}^d$ semi-algebraic *is a finite union of basic semi-algebraic ones.*
e) It is countably semi-algebraic over $\mathbb{F}$ *if the union involves countably many members, all being basic semi-algebraic over $\mathbb{F}$.*

Example 5.6 *a) A circle is algebraic over $\mathbb{Z}$. A disc is basic semi-algebraic over $\mathbb{Z}$. Every integer polytope is basic semi-algebraic over $\mathbb{Z}$.*
b) Every constructible subset of $\mathbb{R}$ is finite or co-finite; every semi-algebraic subset of $\mathbb{R}$ is a finite union of intervals.
c) Every semi-algebraic set is the projection of a constructible set.

Fact 5.7 (Tarski–Seidenberg) *The projection of a semi-algebraic set is again semi-algebraic!*

5.3 Recap on Projective Geometry

Definition 5.8. *Fix a field $\mathbb{F} \supseteq \mathbb{Q}$ and $d \in \mathbb{N}$.*

a) Projective space $\mathbb{P}^d(\mathbb{F})$ is the set $\{\ [\vec{v}] : \vec{0} \neq \vec{v} \in \mathbb{F}^{d+1}\}$ of lines through the origin, where $[\vec{v}] := \{\lambda\vec{v} : \lambda \in \mathbb{F}\}$ denotes a projective point.
b) The Grassmannian $\mathrm{Gr}_k(\mathbb{F}^d)$ is the set of k–dimensional linear subspaces of $\mathbb{F}^d$; $\mathrm{Gr}(\mathbb{F}^d) := \bigcup_k \mathrm{Gr}_k(\mathbb{F}^d)$. (So $\mathrm{Gr}_1(\mathbb{F}^{d+1}) = \mathbb{P}^d(\mathbb{F})\ldots$)
c) For $(\vec{a}_1, \ldots, \vec{a}_d)^\dagger = B = (\vec{b}_1, \ldots, \vec{b}_k) \in \mathbb{F}^{d\times k}$ a matrix of full rank, the family of its maximal minors

$$\mathrm{Det}\left(\mathrm{span}(B)\right) \ := \ \left(\det(\vec{a}_{i_1}, \ldots, \vec{a}_{i_k})\right)_{1\leq i_1<i_2<\ldots<i_k\leq d}$$

is called the Plücker Coordinates *of* $\mathrm{span}(B) \in \mathrm{Gr}_k(\mathbb{F}^d)$.

Lemma 5.9. $\mathrm{Det} : \mathrm{Gr}_k(\mathbb{F}^d) \to \mathbb{P}^{\binom{d}{k}-1}(\mathbb{F})$ *is well-defined and injective (but not surjective).*

See [17, PROPOSITION 14.2].

6 $\mathcal{NP}$–Completeness over the Reals

A BCSS machine $\mathcal{M}$ (over $\mathbb{R}$) can in each step add, subtract, multiply, divide, and branch on the result of comparing two reals. Its memory consists of an infinite sequence of cells, each capable of holding a real number and accessed through an index register (similar to a one-head Turing machine). A program for $\mathcal{M}$ may store a finite number of real constants. The notions of *decidability* and *semi-decidability* translate straightforwardly from discrete $L \subseteq \{0,1\}^*$ and $L \subseteq \mathbb{N}^*$ to real languages $\mathbb{L} \subseteq \mathbb{R}^*$. Computing a function $f :\subseteq \mathbb{R}^* \to \mathbb{R}^*$ means that the machine, given $\vec{x} \in \mathrm{dom}(f)$, outputs $f(\vec{x})$ within finitely many steps and terminates while diverging on inputs $\vec{x} \notin \mathrm{dom}(f)$.

Example 6.1 *a)* $\mathrm{rank} : \mathbb{R}^{n\times m} \to \mathbb{N}$ *is uniformly BCSS–computable in time* $\mathcal{O}(n^3 + m^3)$
b) The graph of the square root function is BCSS–decidable.
c) $\mathbb{Q}$ *is BCSS semi-decidable; and so is the set* $\mathbb{A}$ *of algebraic reals.*
d) The algebraic degree function $\deg : \mathbb{A} \to \mathbb{N}$ *is BCSS–computable.*
e) A language $\mathbb{L} \subseteq \mathbb{R}^*$ *is BCSS semi-decidable iff* $\mathbb{L} = \mathrm{range}(f)$ *for some total computable* $f : \mathbb{R}^* \to \mathbb{R}^*$.
f) The real Halting problem $\mathbb{H}$ *is* not *BCSS–decidable, where*

$$\mathbb{H} := \left\{ \langle \mathcal{M}, \vec{x} \rangle : \textit{BCSS machine } \mathcal{M} \textit{ terminates on input } \vec{x} \right\}$$

g) Every discrete language $L \subseteq \{0,1\}^*$ *is BCSS–decidable!*
h) The following discrete problems (i) $\mathrm{FEAS}^0_{\mathbb{R}}$ *and (ii)* $\mathrm{QUART}^0_{\mathbb{R}}$ *can be* verified *in polynomial time by a BCSS machine without constants:*
  i) Given (the degrees and coefficients in binary of) a system of multivariate polynomial in-/equalities with integer coefficients, does it admit a real solution?
  ii) Given a multivariate polynomial of total degree at most 4, does it admit a real root?

Definition 6.2. *Let* $\mathcal{NP}^0_{\mathbb{R}}$ *denote the family of discrete decision problems of the form*

$$\left\{ \vec{x} \in \{0,1\}^n : n \in \mathbb{N}, \exists \vec{y} \in \mathbb{R}^{p(n)} : \langle \vec{x}, \vec{y} \rangle \in \mathbb{V} \right\}$$

where $p \in \mathbb{N}[N]$ *and* $\mathbb{V} \subseteq \mathbb{R}^*$ *can be decided in polynomial time by a BCSS machine without constants.*

Theorem 6.3. $\mathrm{FEAS}^0_{\mathbb{R}}$ *and* $\mathrm{QUART}^0_{\mathbb{R}}$ *are complete for* $\mathcal{NP}^0_{\mathbb{R}}$
(with respect to many-one reduction by a polynomial-time Turing machine).

Fact 6.4 (Grigoriev'88,Canny'88,Heintz&Roy&Solernó'90,Renegar'92)
$\mathcal{NP} \subseteq \mathcal{NP}^0_{\mathbb{R}} \subseteq$ *PSPACE*.

6.1 Equations over the Cross Product

The cross product in $\mathbb{R}^3$ is well-known due to its many applications in physics such as torque or electromagnetism. Mathematically it constitutes the mapping

$$\times : \mathbb{R}^3 \times \mathbb{R}^3 \ni \big((v_0,v_1,v_2),(w_0,w_1,w_2)\big) \mapsto (v_1w_2 - v_2w_1, v_2w_0 - v_0w_2, v_0w_1 - v_1w_0) \in \mathbb{R}^3 \quad (1)$$

It is bilinear (thus justifying the name "product") but anti-commutative $\vec{v}\times\vec{w} = -\vec{w}\times\vec{v}$ and non-associative and fails the cancellation law:

$$\vec{v}\times w = \vec{u}\times w \;\not\Rightarrow\; \vec{v} = \vec{u} \;\not\Leftarrow\; \vec{w}\times\vec{v} = \vec{w}\times\vec{u}\ .$$

Fact 6.5 *a) For linearly independent $\vec{v},\vec{w}$, their cross product $\vec{v}\times\vec{w} =: \vec{u}$ is uniquely determined by the following: $\vec{u}\perp\vec{v}$, $\vec{u}\perp\vec{w}$ (where "$\perp$" denotes orthogonality), the triplet $\vec{v},\vec{w},\vec{u}$ is right-handed, and lengths satisfy $\|\vec{u}\| = \|\vec{v}\|\cdot\|\vec{w}\|\cdot\cos\angle(\vec{v},\vec{w})$.*
In particular, anti-/parallel $\vec{v},\vec{w}$ are mapped to $\vec{0}$.
b) Cross products commute with simultaneous orientation preserving orthogonal transformations: For $O\in\mathbb{R}^{3\times3}$ with $O\cdot O^\dagger = \mathrm{id}$ and $\det(O) = 1$ it holds $(O\cdot\vec{v})\times(O\cdot\vec{w}) = O\cdot(\vec{v}\times\vec{w})$, where $O^\dagger$ denotes the transposed matrix.

Definition 6.6. *a) A term $t(V_1,\dots,V_n)$ (over "$\times$", in variables $V_1,\dots,V_n$) is either one of the variables, or $(s\times t)$ for terms s,t (in variables $V_1,\dots,V_n$).*
b) For $\vec{v}_1,\dots,\vec{v}_n\in\mathbb{R}^3$ the value $t(\vec{v}_1,\dots,\vec{v}_n)$ is defined inductively via Equation (1).
c) Fix a field $\mathbb{F}\subseteq\mathbb{Q}$ and recall from Definition 5.8 that $\mathbb{P}^2(\mathbb{F}) = \{\,[\vec{v}] : \vec{0}\neq\vec{v}\in\mathbb{F}^3\}$ denotes the projective plane (over $\mathbb{F}$), where $[\vec{v}] := \{\lambda\vec{v} : \lambda\in\mathbb{F}\}$.
For distinct $[\vec{v}],[\vec{w}]\in\mathbb{P}^2(\mathbb{F})$ (well-)define $[\vec{v}]\times[\vec{w}] := [\vec{v}\times\vec{w}]$; $[\vec{v}]\times[\vec{v}]$ is undefined.
d) For a term $t(V_1,\dots,V_n)$ and $[\vec{v}_1],\dots,[\vec{v}_n]\in\mathbb{P}^2(\mathbb{F})$, the value $t([\vec{v}_1],\dots,[\vec{v}_n])$ is defined inductively via c), provided all sub-terms are defined.

Definition 6.7. *a)* $\mathsf{XNONTRIV}^0_{\mathbb{F}^3} := \big\{\langle t(V_1,\dots V_n)\rangle \,\big|\, n\in\mathbb{N},\ \exists\vec{v}_1,\dots\vec{v}_n\in\mathbb{F}^3 : t(\vec{v}_1,\dots\vec{v}_n)\neq\vec{0}\big\}$.
b) $\mathsf{XNONTRIV}^0_{\mathbb{P}^2(\mathbb{F})} := \big\{\langle t(V_1,\dots,V_n)\rangle \,\big|\, n\in\mathbb{N},\ \exists[\vec{v}_1],\dots,[\vec{v}_n]\in\mathbb{P}^2(\mathbb{F}) : t([\vec{v}_1],\dots,[\vec{v}_n])\ \textit{defined}\big\}$.
c) $\mathsf{XUVEC}^0_{\mathbb{F}^3} := \big\{\langle t(V_1,\dots,V_n)\rangle \,\big|\, n\in\mathbb{N},\ \exists\vec{v}_1,\dots,\vec{v}_n\in\mathbb{F}^3 : t(\vec{v}_1,\dots,\vec{v}_n) = \vec{e}_3 := (0,0,1)\big\}$.
d) $\mathsf{XNONEQUIV}^0_{\mathbb{P}^2(\mathbb{F})} := \big\{\langle s(V_1,\dots,V_n), t(V_1,\dots,V_n)\rangle \,\big|$
$n\in\mathbb{N},\ \exists[\vec{v}_1],\dots,[\vec{v}_n]\in\mathbb{P}^2(\mathbb{F}) : s([\vec{v}_1],\dots,[\vec{v}_n])\neq t([\vec{v}_1],\dots,[\vec{v}_n])$, *both sides defined*$\big\}$.
e) $\mathsf{XSAT}^0_{\mathbb{F}^3} := \big\{\langle t_1(V_1,\dots,V_n)\rangle \,\big|\, n\in\mathbb{N},\ \exists\vec{v}_1,\dots,\vec{v}_n\in\mathbb{F}^3 : t(\vec{v}_1,\dots,\vec{v}_n) = \vec{v}_1\neq\vec{0}\big\}$.
f) $\mathsf{XSAT}^0_{\mathbb{P}^2(\mathbb{F})} := \big\{\langle t_1(V_1,\dots,V_n)\rangle \,\big|\, n\in\mathbb{N},\ \exists[\vec{v}_1],\dots,[\vec{v}_n]\in\mathbb{P}^2(\mathbb{F}) : t([\vec{v}_1],\dots,[\vec{v}_n]) = [\vec{v}_1]\big\}$.

Following JOHN VON NEUMANN (who in turn credits KARL VON STAUDT), express arithmetic over $\mathbb{F}$ as geometric operations on $\mathbb{F}^3$ by identifying $r\in\mathbb{F}$ with the line $\big\{\binom{x}{rx} : x\in\mathbb{F}\big\}$.

Lemma 6.8. *Fix a subfield $\mathbb{F}$ of $\mathbb{R}$. Let $\vec{v}_1,\vec{v}_2,\vec{v}_3$ denote an orthogonal basis of $\mathbb{F}^3$. Then $V_j := \mathbb{F}\vec{v}_j$ satisfies $V_1\times V_2 = V_3$, $V_2\times V_3 = V_1$, and $V_3\times V_1 = V_2$. Moreover abbreviating $V_{12} := \mathbb{F}(\vec{v}_1-\vec{v}_2)$ and $V_{23} := \mathbb{F}(\vec{v}_2-\vec{v}_3)$ and $V_{13} := \mathbb{F}(\vec{v}_1-\vec{v}_3)$, we have for $r,s\in\mathbb{F}$:*

a) $\mathbb{F}(\vec{v}_1 - rs\vec{v}_2) \;=\; V_3\times\big[\mathbb{F}(\vec{v}_3 - r\vec{v}_2)\times\mathbb{F}(\vec{v}_1 - s\vec{v}_3)\big]$

b) $\mathbb{F}(\vec{v}_1 - s\vec{v}_3) \;=\; V_2 \times \big[V_{23} \times \mathbb{F}(\vec{v}_1 - s\vec{v}_2)\big]$
c) $\mathbb{F}(\vec{v}_3 - r\vec{v}_2) \;=\; V_1 \times \big[V_{13} \times \mathbb{F}(\vec{v}_1 - r\vec{v}_2)\big]$
d) $\mathbb{F}\big(\vec{v}_1 - (r-s)\vec{v}_2\big) \;=\; V_3 \times \big[\big([V_{23} \times \mathbb{F}(\vec{v}_1 - r\vec{v}_2)] \times [V_2 \times \mathbb{F}(\vec{v}_1 - s\vec{v}_3)]\big) \times V_3\big]$
e) $V_{13} \;=\; V_2 \times (V_{12} \times V_{23})$.
f) *For* $W \in \mathbb{P}^2(\mathbb{F})$, *the expression* $\imath(W) := (W \times V_3) \times \Big(\big((W \times V_3) \times V_3\big) \times V_2\Big)$ *is defined precisely when* $W = \mathbb{F}(\vec{v}_1 - r\vec{v}_2 + s\vec{v}_3)$ *for some* $s \in \mathbb{F}$ *and a unique* $r \in \mathbb{F}$; *and in this case* $\imath(W) = \mathbb{F}(\vec{v}_1 - r\vec{v}_2)$. *Moreover, if* $W = \mathbb{F}(\vec{v}_1 - r\vec{v}_2)$ *then* $\imath(W) = W$.

Theorem 6.9. *a)* $\mathsf{XNONTRIV}^0_{\mathbb{R}^3}$, $\mathsf{XNONTRIV}^0_{\mathbb{P}^2(\mathbb{R})}$, $\mathsf{XUVEC}^0_{\mathbb{R}^3}$, *and* $\mathsf{XNONEQUIV}^0_{\mathbb{P}^2(\mathbb{R})}$ *are polytime equivalent to* Polynomial Identity Testing *(Definition 5.3).*
b) $\mathsf{XSAT}^0_{\mathbb{R}^3}$ *and* $\mathsf{XSAT}^0_{\mathbb{P}^2(\mathbb{R})}$ *are* $\mathcal{NP}^0_{\mathbb{R}}$*–complete.*
c) *There is a term* $t(V_1,\ldots,V_n)$ *s.t.* $\vec{0} \neq t(V_1,\ldots,V_n) = V_1$ *is satisfiable over* $\mathbb{R}^3$ *but not over* $\mathbb{Q}^3$.

6.2 Satisfiability in Quantum Logic

Definition 6.10. *a) For a vector space* V, *the Grassmannian* $\mathrm{Gr}_k(V)$ *is the set of* k*–dimensional linear subspaces of* V*;*
$\mathrm{Gr}(V) := \bigcup_k \mathrm{Gr}_k(V)$, $\boldsymbol{1} := V$ *is called (strong) truth, every* $X \neq \boldsymbol{0} := \{\vec{0}\}$ *is* weakly true.
b) For a finite-dimensional inner product space V, *equip* $\mathrm{Gr}(V)$ *with the operations*

$$X \wedge Y := X \cap Y, \quad X \vee Y := X + Y, \quad \text{and } \neg X := X^{\perp} = \{\vec{v} \in V : \forall \vec{a} \in X : \vec{v} \perp \vec{a}\} \ .$$

c) A lattice term *is an expression over variables and* $\vee, \wedge$*;*
an (ortho) term *may in addition involve* $\neg$.
d) For a term t *with variables* $X_1,\ldots,X_n$ *and for an assignment* $x_1,\ldots,x_n \in \mathrm{Gr}(V)$, *the* value $t_V(x_1,\ldots,x_n)$ *is defined inductively according to b).*
We may omit the subscript V *if it is clear from the context.*
e) $C(X,Y) := (X \wedge Y) \vee (X \wedge \neg Y) \vee (\neg X \wedge Y) \vee (\neg X \wedge \neg Y)$ *is called* commutator *(of* X *and* Y*).*
f) $\mathsf{SAT}_V := \{\langle t(X_1,\ldots,X_n)\rangle : \exists x_1,\ldots,x_n \in \mathrm{Gr}(V) : t_V(x_1,\ldots,x_n) = \boldsymbol{1}\}$,
$\mathsf{sat}_V := \{\langle t(X_1,\ldots,X_n)\rangle : \exists x_1,\ldots,x_n \in \mathrm{Gr}(V) : t_V(x_1,\ldots,x_n) \neq \boldsymbol{0}\}$.
g) For a term $t(X_1,\ldots,X_n)$ *and a field* $\mathbb{F} \subseteq \mathbb{C}$ *let*

$$\mathrm{maxdim}_{\mathbb{F}}(t,d) \;:=\; \max\big\{\dim\big(t_{\mathbb{F}^d}(x_1,\ldots,x_n)\big) : x_1,\ldots,x_n \in \mathrm{Gr}(\mathbb{F}^d)\big\} \ .$$

h) A d*–diamond in* V *is a* $(d+1)$*–tuple* $D_0, D_1, \ldots, D_d \in \mathrm{Gr}(V)$ *such that* $V = D_1 \oplominus \ldots \oplominus D_d = D_0 \oplus D_j$ *for all* $1 \leq j \leq d$, *where* $\oplominus$ *and* $\oplus$ *denote orthogonal and direct sum, respectively.*

So $\mathsf{SAT}_{\mathbb{F}^1} = \mathsf{sat}_{\mathbb{F}^1}$ coincides with the classical, Boolean satisfiability problem;
$\langle t\rangle \in \mathsf{SAT}_{\mathbb{F}^d} \Leftrightarrow \mathrm{maxdim}_{\mathbb{F}}(t,d) = d$, $\langle t\rangle \in \mathsf{sat}_{\mathbb{F}^d} \Leftrightarrow \mathrm{maxdim}_{\mathbb{F}}(t,d) > 0$.

Lemma 6.11. *a)* $\mathrm{Gr}(V)$ *satisfies* de Morgan's Rules $\neg(X \vee Y) = (\neg X) \wedge (\neg Y)$ *and* $\neg(X \wedge Y) = (\neg X) \vee (\neg Y)$; *but* $\mathrm{Gr}(\mathbb{R}^2)$ *violates the distributive law* $(X \vee Y) \wedge Z = (X \wedge Z) \vee (Y \wedge Z)$.

b) $\mathrm{Gr}(V)$ *satisfies the* modular laws

$$x \subseteq y \quad \Rightarrow \quad x \vee (y \wedge z) = y \wedge (x \vee z), \qquad x \supseteq y \quad \Rightarrow \quad x \wedge (y \vee z) = y \vee x \wedge z)$$

and in particular the orthomodular laws

$$u \subseteq v \quad \Rightarrow \quad u \vee (v \wedge \neg u) = v, \qquad u \supseteq v \quad \Rightarrow \quad u \wedge (v \vee \neg u) = v$$

c) For $a, b \in \mathrm{Gr}(V)$ *it holds:* $C(a,b) = \mathbf{1} \Leftrightarrow a = (a \vee b) \wedge (a \vee \neg b) \Leftrightarrow: aCb$.
In particular $aCb \Leftrightarrow \neg aCb \Leftrightarrow bCa$.
d) Suppose $x, y, z \in \mathrm{Gr}(V)$ *have* $C(x,y) = \mathbf{1} = C(x,z)$.
Then $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ *and* $C(x, y \vee z) = \mathbf{1}$.
e) If $x_1, \ldots, x_n \in \mathrm{Gr}(V)$ *satisfy* $C(x_i, x_j) = \mathbf{1}$ *and* $t(x_1, \ldots, x_n) \neq 0$,
then there exist $y_1, \ldots, y_n \in \{\mathbf{0}, \mathbf{1}\}$ *with* $t(y_1, \ldots, y_n) = \mathbf{1}$.
f) For any field $\mathbb{F} \subseteq \mathbb{C}$, *if* $t(X_1, \ldots, X_n)$ *admits a weakly/strongly satisfying assignment in* $\mathrm{Gr}(\mathbb{F}^2)$, *it also admits one in* $\mathcal{MO}_n := \{\mathbf{0}, \mathbf{1}, \mathbb{Q}\binom{1}{1}, \mathbb{Q}\binom{-1}{1}, \ldots, \binom{1}{n}, \binom{-n}{1}\}$.

Proposition 6.12. *Fix a field* $\mathbb{F} \subseteq \mathbb{C}$ *and* $3 \leq d \in \mathbb{N}$. *Let* $\vec{e}_1, \ldots, \vec{e}_d \in \mathbb{F}^d$ *denote a basis and abbreviate* $\Theta : \mathbb{F} \ni a \mapsto \mathbb{F}(\vec{e}_1 - a\vec{e}_2) \in \mathrm{Gr}_1(\mathbb{F}^d)$ *and* $E_j := \mathbb{F}\vec{e}_j$ *and* $E_{ij} := \mathbb{F}(\vec{e}_i - \vec{e}_j)$.

a) $\big(\mathbb{F}(\vec{e}_1 - b\vec{e}_3) \vee \mathbb{F}(\vec{e}_3 - a\vec{e}_2)\big) \wedge (E_1 \vee E_2) \;=\; \Theta(a \cdot b)$;
b) $\mathbb{F}(\vec{e}_i - a\vec{e}_k) \;=\; \big(\mathbb{F}(\vec{e}_i - a\vec{e}_j) \vee E_{jk}\big) \wedge (E_i \vee E_k)$ *for pairwise distinct* $1 \leq i, j, k \leq d$;
c) $\mathbb{F}(\vec{e}_j - a\vec{e}_k) \;=\; \big(\mathbb{F}(\vec{e}_i - a\vec{e}_j) \vee E_{ik}\big) \wedge (E_j \vee E_k)$ *for pairwise distinct* $1 \leq i, j, k \leq d$;
d) $\Big(\big[\big(\mathbb{F}(\vec{e}_1 - b\vec{e}_3) \vee E_2\big) \wedge \big(\Theta(a) \vee E_{23}\big)\big] \vee E_3\Big) \cap (E_1 \vee E_2) \;=\; \Theta(a - b)$;
f) For pairwise distinct $1 \leq i, j, k \leq d$ *it holds:* $\bigvee_{i=1}^{d} E_i = \mathbf{1}$, $E_i \wedge \bigvee_{j \neq i} E_j = \mathbf{0}$, $E_{ij} \vee E_j = E_i \vee E_j$, $E_{ij} \wedge E_j = \mathbf{0}$, $E_{ik} = E_{ki} = (E_i \vee E_k) \wedge (E_{ij} \vee E_{jk})$.
g) Conversely every choice of $E_i, E_{ij} \in \mathrm{Gr}(\mathbb{F}^d)$ *satisfying the conditions expressed in f) arise from a basis* e_i.

Theorem 6.13. *a) For any field* $\mathbb{F} \subseteq \mathbb{C}$, *both* $\mathsf{SAT}_{\mathbb{F}^2}$ *and* $\mathsf{sat}_{\mathbb{F}^2}$ *are* $\mathcal{NP}$*–complete.*
b) For every $d \geq 3$, $\mathsf{SAT}_{\mathbb{R}^d}$ *and* $\mathsf{sat}_{\mathbb{R}^d}$ *are* $\mathcal{NP}_{\mathbb{R}}$*–complete*
c) and so are $\mathsf{SAT}_{\mathbb{C}^d}$ *and* $\mathsf{sat}_{\mathbb{C}^d}$*!*
d) There exists a term t *that is (weakly/strongly) satisfiable over* $\mathrm{Gr}(\mathbb{R}^3)$ *but not over* $\mathrm{Gr}(\mathbb{Q}^3)$ *and a term* s *(weakly/strongly) satisfiable over* $\mathrm{Gr}(\mathbb{C}^3)$ *but not over* $\mathrm{Gr}(\mathbb{R}^3)$.

Lemma 6.14. *a) For terms* $s(X_1, \ldots, X_n)$ *and* $t(Y_1, \ldots, Y_m)$ *it holds*
$\mathrm{maxdim}(s \vee t, d) = \min\{\mathrm{maxdim}(s,d) + \mathrm{maxdim}(t,d), d\}$.
b) Fix $V \in \mathrm{Gr}(W)$ *and a term* $t(X_1, \ldots, X_n)$.
For $x_1, \ldots, x_n \in \mathrm{Gr}(V)$ *it holds* $t_V(x_1, \ldots, x_n) = t_W(x_1, \ldots, x_n) \cap V$.
c) For terms $s(X_1, \ldots, X_n) = s(\bar{X})$ *and* $t(\bar{Y})$ *abbreviate* $\big(s|_t\big)(\bar{X}, \bar{Y}) := s\big(X_1 \wedge t(\bar{Y}), \ldots, X_n \wedge t(\bar{Y})\big) \wedge t(\bar{Y})$. *Then* $\mathrm{maxdim}(s|_t, d) = \mathrm{maxdim}\big(s, \mathrm{maxdim}(t,d)\big)$.
d) Every d–diamond $D_0, D_1, \ldots, D_d \in \mathrm{Gr}(V)$, $d := \dim(V)$, *weakly satisfies the following term* $g_d(Z_0, Z_1, \ldots, Z_d) = g_d(\bar{Z})$:

$$\neg Z_0 \wedge \bigwedge\nolimits_{j=1}^{d} \big(Z_0 \vee g_{d,j}(\bar{Z})\big), \quad \text{where } g_{d,j}(\bar{Z}) := Z_j \wedge \bigwedge\nolimits_{i \neq j > 0} \neg Z_i \ . \tag{2}$$

e) For $d := \dim(V)$, every weakly satisfying assignment $D_0, D_1, \ldots, D_d \in \mathrm{Gr}(V)$ of Equation (2) constitutes a d-diamond.
Moreover, in this case, $g_{d,j}(D_0, D_1, \ldots, D_d) = D_j$ and $\dim\big(g_d(D_0, D_1, \ldots, D_d)\big) = 1$.

f) If t is weakly satisfiable over $\mathrm{Gr}(V)$, there exists some $W \in \mathrm{Gr}_{|t|}(V)$ such that t is weakly satisfiable over $\mathrm{Gr}(W)$, where $|t|$ denotes the syntactic length of t.

Definition 6.15. *Call $t(X_1, \ldots, X_n)$ weakly/strongly satisfiable over $\mathrm{Gr}(\mathbb{F}^*)$ if there exists some $d \in \mathbb{N}$ and a weakly/strongly satisfying assignment $x_1, \ldots, x_n \in \mathrm{Gr}(\mathbb{F}^d)$.*

6.3 Realizability of Oriented Matroids

6.4 Stretchability of Pseudolines

References

1. P. BÜRGISSER, M. CLAUSEN, A. SHOKROLLAHI: *Algebraic Complexity Theory*, Springer (1997).
2. L. BLUM, F. CUCKER, M. SHUB, S. SMALE: *Complexity and Real Computation*, Springer (1998).
3. P. BÜRGISSER: *Completeness and Reduction in Algebraic Complexity Theory*, Springer (2000).
4. F. CUCKER: "On the Complexity of Quantifier Elimination: the Structural Approach", pp.400–408 in *The Computer Journal* vol.**36:5** (1993).
5. M.R. GAREY, D.S. JOHNSON: "*Computers and Intractability: A Guide to the Theory of $\mathcal{NP}$–completeness*", Freeman (1979).
6. J. VON ZUR GATHEN, J. GERHARD: *Modern Computer Algebra* 3rd Edition, Cambridge (2013).
7. A. GERASOULIS: "A Fast Algorithm for the Multiplication of Generalized Hilbert Matrices with Vectors", pp.179–188 in *Mathematics of Computation* vol.**50:181** (1988).
8. C. HERRMANN: "The free orthomodular word problem is solved" (review of the paper by G. KALMBACH), in *Zentralblatt für Mathematik* **Zbl 0585.06004** and *Mathematical Reviews* **MR 87K:06023** (1987).
9. W.M. KOOLEN, M. ZIEGLER: "Kolmogorov Complexity Theory over the Reals", pp.153–169 in *Proc. 5th Int. Conf. on Computability and Complexity in Analysis*, Electronic Notes in Theoretical Computer Science vol.**221** (2008).
10. M. ZIEGLER: "Fast Relative Approximation of Potential Fields", pp.140–149 in *Proc. 8th Int. Workshop on Algorithms and Data Structures* (WADS'2003), Springer LNCS vol.**2748**.
11. C. HERRMANN, M. ZIEGLER: "Computational Complexity of Quantum Satisfiability", pp.175–184 in *Proc. 26th Ann. IEEE Sympo. on Logic in Computer Science* (LiCS'11).
12. K. MEER, C. MICHAUX: "A Survey on Real Structural Complexity Theory", pp.113–148 in *Bulletin of the Belgian Mathematical Society* vol.**4** (1997).
13. M. SCHAEFER: "Complexity of Some Geometric and Topological Problems", pp.334–344 in *Proc. 17th Int. Symp. on Graph Drawing*, Springer LNCS vol.**5849** (2010).
14. S. SMALE: "Mathematical Problems for the Next Century", pp.7–15 in *Math. Intelligencer* vol.**20:2** (1998).
15. C. HERRMANN, J. SOKOLI, M. ZIEGLER: "Satisfiability of cross product terms is complete for real nondeterministic polytime Blum-Shub-Smale machines", pp.85–92 in *Proc. 6th Int. Conf. Machines, Computations and Universality*, Electronic Proceedings in Theoretical Computer Science vol.**128** (2013).
16. N. SAXENA: "Progress on Polynomial Identity Testing", pp.49–79 in *Bulletin of the EATCS* no.**99** (2009).
17. E. MILLER, B. STURMFELS *Combinatorial Commutative Algebra*, vol.**227** in Springer Graduate Texts in Mathematics (2005).
18. T.J. HAGGE: "$QL(\mathbb{C}^n)$ Determines n", pp.1194–1196 in *Journal of Symbolic Logic* vol.**72:4** (2007).