

Script Skeleton: Advanced Complexity Theory^{*}

Martin Ziegler

ziegler@mathematik.tu-darmstadt.de

Abstract. Classical computational complexity theory (last semester) has resulted in a rich variety of classes naturally capturing many practical computational problems. We also have established several relations between these classes; but not a single non-trivial lower bound (other than, e.g. $\text{Time}(n) \geq n$ and $\text{Space}(n) \geq \log n$) was obtained. The topics of this lecture describe several (more or less successful) approaches to remedy this situation.

1	Algorithmic Information Theory and Applications	1
1.1	A Lower Bound for 1-Tape Turing Machines	1
2	Time versus Space	2
2.1	Pebble Game: Time versus Space for Circuits	2
2.2	Pebble Strategies and Computation	3
3	Simple Diagonalization: Hartmanis' Hierarchy Theorems	4
4	Relativization and Priority/Injury-Diagonalization: Baker/Gill/Solovay and Friedberg/Muchnik	4
5	Straight-Line Complexity	5
5.1	Lower Bounds: Dimension, Volume, Transcendence Degree	6
5.2	Some Surprisingly Efficient Algorithms: Preconditioning, Baur-Strassen, Multipoint Evaluation	7
5.3	Matrix Multiplication and Tensor Rank	8
6	Branching Complexity	10
6.1	Hyperplane Arrangements and Combinatorial Convex Geometry	10
6.2	Linear Branching Trees	12

^{*} This is the synopsis to a lecture held in summer (mid of April to mid of July) 2011 at the TU Darmstadt.

1 Algorithmic Information Theory and Applications

0101010101010101 vs. 1011001011111001 Here $\Sigma := \{0, 1\}$.

Definition 1.1. Fix a universal Turing machine \mathcal{U} over alphabet Σ and let, for $\bar{x} \in \Sigma^*$, $K_{\mathcal{U}}(\bar{x}) := \min \{ |\langle \mathcal{M}, \bar{y} \rangle| : \mathcal{U}(\langle \mathcal{M}, \bar{y} \rangle) = \bar{x} \}$.

Lemma 1.2 (Kolmogorov Complexity).

- a) There exists $c \in \mathbb{N}$ such that, for every $\bar{x} \in \Sigma^*$, $K_{\mathcal{U}}(\bar{x}) \leq c + |\bar{x}|$.
- b) To UTM \mathcal{V} there exists $c \in \mathbb{N}$ such that every $\bar{x} \in \Sigma^*$ has $K_{\mathcal{U}}(\bar{x}) \leq c + K_{\mathcal{V}}(\bar{x})$
- c) To every n , there exists $\bar{x} \in \Sigma^n$ with $K_{\mathcal{U}}(\bar{x}) \geq n$.

Strings \bar{x} with $K(\bar{x}) \approx |\bar{x}|$ are considered *incompressible*.

1.1 A Lower Bound for 1-Tape Turing Machines

Definition 1.3 (Crossing Sequence). Let $\mathcal{M} = (Q, \Sigma, \Gamma, \delta)$ denote a deterministic 1-tape Turing machine (1-DTM) $\bar{\in} \Sigma^*$, and $s \in \mathbb{N}_0$. Then $\text{CS}_{\mathcal{M}}(\bar{x}, s)$ denotes the finite or infinite sequence (q_i) of states \mathcal{M} is in when moving from tape cell $\#s-1$ to $\#s$ or back. We write $|\text{CS}_{\mathcal{M}}(\bar{x}, s)|$ for its length.

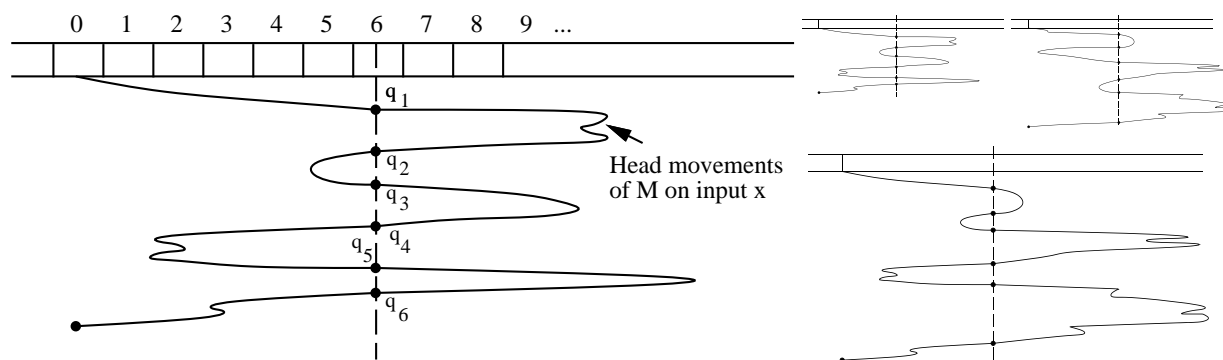


Fig. 1. a) Example of a Crossing Sequence b) Combining two computations with identical crossing sequences

Lemma 1.4 (Pumping). Let \mathcal{M} as above.

- a) Suppose both $\bar{u}\bar{v}$ and $\bar{y}\bar{z}$ are accepted by \mathcal{M} and satisfy $\text{CS}_{\mathcal{M}}(\bar{u}\bar{v}, |\bar{u}|) = \text{CS}_{\mathcal{M}}(\bar{y}\bar{z}, |\bar{y}|)$. Then \mathcal{M} accepts also $\bar{u}\bar{z}$ and $\bar{y}\bar{v}$.
- b) $\text{Time}_{\mathcal{M}}(\bar{x}) = \sum_{s=1}^{\infty} |\text{CS}_{\mathcal{M}}(\bar{x}, s)|$.
In particular, to every finite $S \subseteq \mathbb{N}_0$, there exists $s \in S$ with $|\text{CS}_{\mathcal{M}}(\bar{x}, s)| \leq \text{Time}_{\mathcal{M}}(\bar{x})/|S|$.
- c) Suppose \mathcal{M} decides $L := \{ \bar{x} 0^{|\bar{x}|} \bar{x} : \bar{x} \in \Sigma^* \}$. Then, for $m \leq s < 2m$ and $\bar{x}, \bar{y} \in \Sigma^m$ with $\bar{x} \neq \bar{y}$, it holds $\text{CS}_{\mathcal{M}}(\bar{x}0^m\bar{x}, s) \neq \text{CS}_{\mathcal{M}}(\bar{y}0^m\bar{y}, s)$.
- d) There is $c \in \mathbb{N}$ such that every $\bar{x} \in \Sigma^m$ has $K_{\mathcal{U}}(\bar{x}) \leq c + c \cdot \text{Time}_{\mathcal{M}}(\bar{x}0^m\bar{x})/m + \log_2(m)$.

Theorem 1.5. *The language L from Lemma 1.4c)*

- a) *can be decided by a deterministic 2-DTM in time $\mathcal{O}(n)$*
- b) *can be decided by a deterministic 1-DTM in time $\mathcal{O}(n^2)$*
- c) *cannot be decided by a deterministic 1-DTM in time $o(n^2)$*

2 Time versus Space

For every $f(n) \geq n$,

- a) $\text{DTIME}(f(n)) \subseteq \text{DSPACE}(f(n))$
- b) $\text{DSPACE}(f(n)) \subseteq \text{DTIME}(2^{\mathcal{O}(f(n))})$.

Improving b): \mathcal{P} versus \mathcal{NP} . This section improves a).
 $\text{DTIME}_k(f(n))$ depends on the number k of heads; $\text{DSPACE}_k(f(n))$ does not.

2.1 Pebble Game: Time versus Space for Circuits

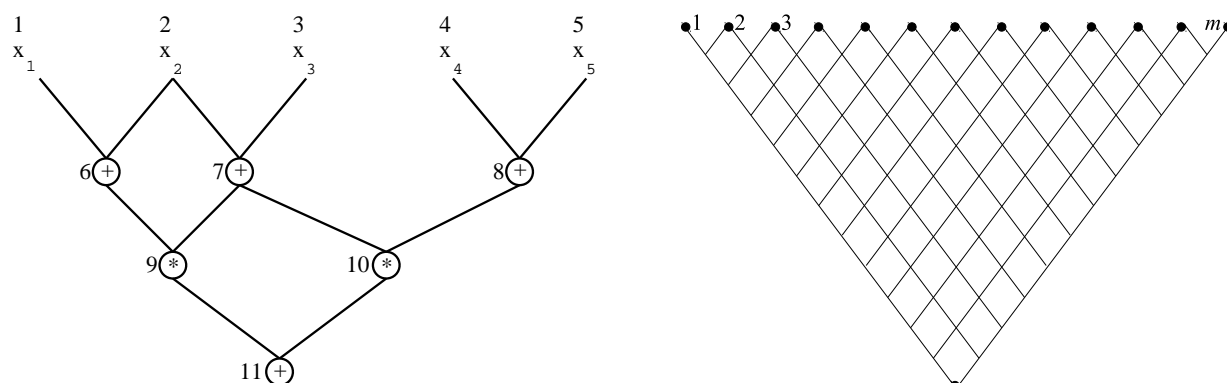


Fig. 2. a) An arithmetic circuit b) Pyramid graph P_m

Definition 2.1 (Pebble Game). *Let $G = (V, E)$ denote a directed acyclic graph (DAG) and $v \in V$. The goal of the game instance (V, E, v) is to eventually put a marker ('pebble') on v , by a sequence of moves subject to the following rules:*

- *Either remove a marker from some vertex $u \in V$*
- *Or put a marker onto a vertex $u \in V$,
provided that all direct predecessors of u are presently marked.*

We count the number of steps as well as the number of (reusable) markers employed.

Example 2.2 *The DAG in Figure 2a) can be played*

- a) *with 5 markers in 17 steps*
- b) *but not with 4 markers.*

For $m \in \mathbb{N}$, the pyramid graph P_m from Figure 2b) can be played

- c) *with $m + 1$ markers*
- d) *but not with m markers* □

Lemma 2.3. *Let (V, E) denote a DAG with indegree at most $\ell \in \mathbb{N}$ and $m := |E|$ edges. Write $S_\ell(m)$ for the least number of markers sufficient to play every DAG of indegree $\leq \ell$ having $\leq m$ edges.*

- a) *There exists $U \subseteq V$ such that $F := E \cap (U \times U)$ has $m/2 - \ell \leq |F| < m/2$ and $E \cap ((V \setminus U) \times U) = \emptyset$.*
- b) *It holds $S_\ell(m) \leq S_\ell(m/2 + \ell) + |F'|$ with the abbreviation $F' := E \cap (U \times (V \setminus U))$.*
- c) *It also holds $S_\ell(m) \leq S_\ell(m/2) + S_\ell(m/2 + \ell - |F'|) + \ell$.*
- d) *It holds $S_\ell(m) \leq \max \left\{ S_\ell(m/2 + \ell) + \frac{2m}{\log m}, S_\ell(m/2) + S_\ell(m/2 + \ell - \frac{2m}{\log m}) + \ell \right\}$ and, for fixed ℓ , $S_\ell(m) \leq \mathcal{O}(m/\log m)$.*
- e) *(V, E) can be played with $\mathcal{O}(n/\log n)$ markers for $n := |V|$ and ℓ considered fixed.*

2.2 Pebble Strategies and Computation

We encode a DAG (V, E) as a list of vertices and edges, i.e. such that $N := |\langle V, E \rangle| = \Theta(n \cdot \log n + m \cdot \log n)$ where $n := |V|$ and $m := |E|$.

Lemma 2.4. a) *A quadratically space-bounded DTM can, given $\langle V, E, v, s, t \rangle$, produce some play for (V, E, v) using $\leq s$ markers and $\leq 2^t$ steps, provided that such a play exists.*

b) *Let \mathcal{M} denote a k -tape Turing machine and $\bar{x} \in \Sigma^n$ an input on which \mathcal{M} makes T steps. Subdivide this computation into $B \in \mathbb{N}$ phases of $\lceil T/B \rceil$ steps each; and subdivide \mathcal{M} 's tapes into B blocks of $\lceil T/B \rceil$ cells each.*

i) In each phase and on each tape, \mathcal{M} visits at most 2 different blocks.

ii) The computation of $\mathcal{M}(\bar{x})$ in phase $\varphi = 1, \dots, B$ depends on the contents of blocks last modified in at most $\ell := k + 1$ different previous phases.

c) *Choosing $B := \lceil T^{1/3} \rceil$, the computation of \mathcal{M} on \bar{x} can be simulated by a Turing machine using space $\mathcal{O}(T/\log T)$.*

Theorem 2.5 (Hopcroft, Paul, Valiant 1977). *Let $t(n) \geq n$ be constructible in space $t(n)/\log t(n)$. Then $\text{DTIME}(t(n)) \subseteq \text{DSPACE}(t(n)/\log t(n))$.*

3 Simple Diagonalization: Hartmanis' Hierarchy Theorems

Example 3.1 *The following language is not semi-decidable:*

$$D := \{ \langle \mathcal{M} \rangle : \text{DTM } \mathcal{M} \text{ does not accept } \langle \mathcal{M} \rangle \} \subseteq \Sigma^*$$

We consider DTMs over arbitrary finite alphabets.

Proposition 3.2. *Fix $f : \mathbb{N} \rightarrow \mathbb{N}$ with $f(n) \geq 2n$.*

a) *It holds $T_f \notin \text{DTIME}(f(n))$, where*

$$T_f := \{ \langle \mathcal{M} \rangle : \text{DTM } \mathcal{M} \text{ does not accept } \langle \mathcal{M} \rangle \text{ within } f(|\langle \mathcal{M} \rangle|) \text{ steps} \}$$

b) *It also holds $S_f \notin \text{DSPACE}(f(n))$ for the language*

$$S_f := \{ \langle \mathcal{M} \rangle : \text{DTM } \mathcal{M} \text{ does not accept } \langle \mathcal{M} \rangle \text{ using } \leq f(|\langle \mathcal{M} \rangle|) \text{ tape cells} \}$$

c) *If f is computable in space $\mathcal{O}(f(n) \cdot \log n)$, then $S_f \in \text{DSPACE}(f(n) \cdot \log f(n))$.*

d) *If f is computable in time $\mathcal{O}(f(n)^3)$, then $T_f \in \text{DTIME}(f(n)^3)$.*

Corollary 3.3. $\mathcal{P} \subsetneq \text{EXP}$, $\mathcal{L} \subsetneq \text{PSPACE}$.

Theorem 3.4 (Hartmanis et. al., Fürer, Trakhtenbrot).

a) *Let $f(n) \in o(g(n))$ be computable in space $\mathcal{O}(f(n))$. Then $\text{DSPACE}(f(n)) \subsetneq \text{DSPACE}(g(n))$.*

b) *Let $f(n) \in o(g(n))$ be computable in time $\mathcal{O}(f(n))$. Then $\text{DTIME}(f(n)) \subsetneq \text{DTIME}(g(n))$.*

c) *There is a computable monotone function $f(n) \geq n$ such that $\text{DTIME}(f(n)) = \text{DTIME}(2^{f(n)})$.*

4 Relativization and Priority/Injury-Diagonalization: Baker/Gill/Solovay and Friedberg/Muchnik

Example 4.1 a) *The language*

$$H := \{ \langle \mathcal{M}, x \rangle : \text{DTM } \mathcal{M} \text{ terminates on input } x \}$$

is i) semi-decidable but ii) not decidable. Moreover iii) every semi-decidable problem is many-one reducible to H .

b) *H is trivially decidable by an ODTM with oracle H ; and so is D . But w.r.t. any oracle O , the following language is not semi-decidable by an O -oracle machine:*

$$D^O := \{ \langle \mathcal{M}^? \rangle : \text{ODTM } \mathcal{M}^O \text{ does not accept } \langle \mathcal{M}^? \rangle \} \subseteq \Sigma^*$$

c) *There is a countably infinite hierarchy $\emptyset, H, H^H =: H', H^{H^H} =: H'', \dots$ of languages; each $H^{(j)}$ semidecidable, but not decidable, relative to $H^{(j-1)}$.*

For complexity class \mathcal{C} and oracle O , generically understand \mathcal{C}^O to denote its relativization.

Scholium 4.2 For any oracle $O \subseteq \Sigma^*$, the following holds:

a) For increasing $f : \mathbb{N} \rightarrow \mathbb{N}$ O -computable in time and space $\mathcal{O}(f(n))$,

$$\text{DTIME}(f(n)) \subseteq \text{NTIME}(f(n)) \subseteq \text{DSPACE}(f(n)) \subseteq \text{DTIME}(\mathcal{O}(2)^{\log n + f(n)})$$

b) If $f(n) \in o(g(n))$ is computable in space $\mathcal{O}(f(n))$, then $\text{DSPACE}(f(n)) \subsetneq \text{DSPACE}(g(n))$.

If $f(n) \in o(g(n))$ is computable in time $\mathcal{O}(f(n))$, then $\text{DTIME}(f(n)) \subsetneq \text{DTIME}(g(n))$.

c) If $s : \mathbb{N} \rightarrow \mathbb{N}$ with $s(n) \geq \log(n)$ is O -computable in space $\mathcal{O}(s(n))$, then $\text{NSPACE}^O(s(n)) \subseteq \text{DSPACE}^O(s(n)^2)$.

d) For $s : \mathbb{N} \rightarrow \mathbb{N}$ with $s(n) \geq \log(n)$, it holds $\text{NSPACE}^O(s(n)) = \text{coNSPACE}^O(s(n))$.

e) $\text{BPP}^O \subseteq \Sigma_2\mathcal{P}^O \cap \Pi_2\mathcal{P}^O$.

In particular, $\mathcal{L}^O \subseteq \mathcal{NL}^O \subseteq \mathcal{P}^O \subseteq \mathcal{NP}^O \subseteq \text{PSPACE}^O = \text{NPSpace}^O \subseteq \text{EXP}^O$ and at least one inclusion is strict.

Theorem 4.3 (Baker, Gill, Solovay 1975).

a) There exists $A \subseteq \{0, 1\}^*$ such that $\mathcal{P}^A = \mathcal{NP}^A$.

b) There exists an oracle $B \subseteq \{0, 1\}^*$ such that $\mathcal{P}^B \neq \mathcal{NP}^B$.

Theorem 4.4 (Friedberg 1957/Muchnik 1956). There exist semidecidable $A, B \subseteq \{0, 1\}^*$ such that A is not decidable relative to B and B is not decidable relative to A .

5 Straight-Line Complexity

Definition 5.1 (Straight-Line Program). Let $\mathcal{S} = (S, (c_i), (f_j))$ denote a structure with constants $c_i \in S$ and functions $f_j : S^{a_j} \rightarrow S$ of arities $a_j \in \mathbb{N}$. A Straight-Line Program $P_{\mathcal{S}}$ (over this structure and in variables X_1, \dots, X_n) is a finite sequence of assignments $Z_k := c_i$ and $Z_k := X_\ell$ ($1 \leq \ell \leq n$) and $Z_k := f_j(Z_{k_1}, \dots, Z_{k_{a_j}})$, $1 \leq k_1, \dots, k_{a_j} < k$. When assigned values $x_1, \dots, x_n \in S$ to X_1, \dots, X_n , the program **computes** (the set of results consisting of $(x_1, \dots, x_n) =: \mathbf{x}$ and of) Z_1, \dots, Z_K ; the final result is $Z_K =: P_{\mathcal{S}}(\mathbf{x})$. However if some intermediate operation $f_j(Z_{k_1}, \dots, Z_{k_{a_j}})$ is undefined, then so is $P_{\mathcal{S}}(\mathbf{x}) := \perp$. A cost function C assigns to each f_j some cost $C(f_j) \geq 0$. The cost of a straight-line program P is the sum of the costs of the f_j occurring. The length of a straight-line program means its cost with respect to constant cost function $f_j \mapsto 1$.

Example 5.2 a) Let $\mathcal{S} := (R, R, (+, \times))$ be a commutative ring and $p \in R[X]$ a polynomial. Horner's Scheme gives rise to a straight-line program computing $x \mapsto p(x)$ of length at most $2 \cdot \deg(p)$.

b) Consider the semi-group $\mathcal{S} := (\mathbb{N}, (1), (+))$. Every $N \in \mathbb{N}$ can be computed by a straight-line program over \mathcal{S} of length at most $2 \cdot \lceil \log_2 N \rceil$.

c) Consider the N -dimensional discrete Fourier-transform

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

For $N = 2^n$, \mathcal{F}_N can be computed by a straight-line program over $(\mathbb{C}, (0), (+, \times_c : c \in \mathbb{S}^1))$ of length $\mathcal{O}(N \cdot \log N)$, where $\mathbb{S}^1 = \{z \in \mathbb{C} : |z| = 1\}$ denotes the complex unit circle and $\times_c : \mathbb{C} \rightarrow \mathbb{C}, z \mapsto c \cdot z$ unary complex multiplication by c .

- d) Let F denote a field and \mathcal{A} an F -algebra. There is a straight-line program over $(\mathcal{A}, (0), (+, \times_c : c \in F))$ which, for arbitrary but fixed distinct $x_1, \dots, x_n \in F$ and on input of $y_1, \dots, y_n \in \mathcal{A}$, calculates (the unique) $a_0, \dots, a_{n-1} \in \mathcal{A}$ with $\sum_{k=0}^{n-1} a_k \cdot x_\ell^k = y_\ell$ for $\ell = 1, \dots, n$.
- e) Consider an infinite field F , $n + m$ variables $A_0, \dots, A_{n-1}, B_0, \dots, B_{m-1}$, and the algebra $\mathcal{A} = F[A_0, \dots, B_{m-1}]$ with binary operations $+$ and $\times : \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$ as well as unary $\times_c : \mathcal{A} \rightarrow \mathcal{A}$ ($c \in F$), that is the structure $(\mathcal{A}, F, (+, \times, \times_c : c \in F))$. The set $\{\sum_{i+j=\ell} A_i \cdot B_j : 0 \leq \ell \leq n+m-2\}$ can be calculated from A_0, \dots, B_{m-1} by a straight-line program using $n + m - 1$ operations “ \times ” (and arbitrary many “ $+$ ” and “ \times_c ”).

Straight-line programs as in b) are *addition chains*; c) refers to the *fast Fourier transform*.

5.1 Lower Bounds: Dimension, Volume, Transcendence Degree

Proposition 5.3. a) Any straight-line program computing $N \in \mathbb{N}$ over $(\mathbb{N}, 1, (+, -))$ has length at least $\log_2 N$. In particular the straight-line program from Example 5.2b) is optimal up to a constant factor.

b) For $\mathcal{S} = (F, F, (+, -, \times))$ a field of characteristic 0 and $0 \neq p \in F[X]$, any straight-line program computing $x \mapsto p(x)$ over \mathcal{S} contains at least $\log_2 \deg(p)$ multiplications.

Let F denote a field and $F(X)$ the field of univariate rational functions.

For coprime $p(X), q(X) \in F[X]$ define $\deg(p(X)/q(X)) := \max\{\deg(p), \deg(q)\}$.

- c) Every $r(X) \in F(X)$ can be calculated by a straight-line program over $(F, F, (+, \times, \div))$ of length at most $4 \deg(r) + 1$.
- d) Conversely, any straight-line program over $(F, F, (+, \times, \div))$ computing $r(X) \in F(X)$ has length at least $\log_2 \deg(r)$.

Theorem 5.4 (Dimension Bound). Let $F \subseteq E$ denote fields and consider $x_1, \dots, x_n, y_1, \dots, y_m \in E$ and the induced F -vector spaces $X := \{\lambda_1 x_1 + \dots + \lambda_n x_n : \lambda_i \in F\}$ and $Y := \{\mu_1 y_1 + \dots + \mu_m y_m : \mu_j \in F\}$. Moreover consider the structure $\mathcal{S} = (E, F, (+, -, \times, \times_\lambda : \lambda \in F))$ where $\times : E \times E \rightarrow E$ and $\times_\lambda : E \rightarrow E, e \mapsto \lambda \cdot e$.

- a) Any straight-line program over \mathcal{S} computing $\{y_1, \dots, y_m\}$ from (x_1, \dots, x_n) contains at least $\dim_F(X + Y + F) - \dim_F(X + F)$ multiplications “ \times ”.
- b) The straight-line program from Example 5.2e) is optimal.

Theorem 5.5 (Morgenstern’s Volume Bound). Fix $C > 0$ and consider a straight-line program P over the structure $(\mathbb{C}, \mathbb{C}, (+, \times_\lambda : |\lambda| \leq C))$ in n variables.

- a) Each ‘line’ ℓ of P computes an affine linear function $\varphi_\ell : \mathbb{C}^n \rightarrow \mathbb{C}$;
and P computes an affine linear map $\Phi_P : \mathbb{C}^n \ni \mathbf{x} \mapsto A_P \cdot \mathbf{x} + \mathbf{b} \in \mathbb{C}^{n+|P|}$,
where $|P|$ denotes the length of P and the first n components are the identity.
- b) For $\mathbf{a}_1, \dots, \mathbf{a}_m \in \mathbb{C}^n$ with $m \geq n$ write

$$\Delta(\mathbf{a}_1, \dots, \mathbf{a}_m) := \max \{ |\det(\mathbf{a}_{j_1}, \dots, \mathbf{a}_{j_n})| : 1 \leq j_1, \dots, j_n \leq m \} .$$

Then, for $1 \leq k, \ell \leq m$ and $\lambda \in \mathbb{C}$, it holds $\Delta(\mathbf{a}_1, \dots, \mathbf{a}_m, \lambda \cdot \mathbf{a}_k) \leq |\lambda| \Delta(\mathbf{a}_1, \dots, \mathbf{a}_m)$
and $\Delta(\mathbf{a}_1, \dots, \mathbf{a}_m, \mathbf{a}_k + \mathbf{a}_\ell) \leq 2\Delta(\mathbf{a}_1, \dots, \mathbf{a}_m)$.

- c) The homogeneous linear map $A_P : \mathbb{C}^n \rightarrow \mathbb{C}^{n+|P|}$ from a) satisfies $\Delta(A_P) \leq (2C)^{|P|}$.
- d) The matrix $(\exp(2\pi i \cdot k \cdot \ell/n))_{0 \leq k, \ell < n}$ has determinant of absolute value $n^{n/2}$.
- e) The straight-line program from Example 5.2c) is asymptotically optimal.

Theorem 5.6 (Transcendence Degree Bound, Motzkin+Belaga). Let $F \subseteq E$ denote fields of characteristic 0 and $\mathcal{F} \subseteq E(\mathbf{X})$ a finite set of rational functions in indeterminates $(X_1, \dots, X_n) = \mathbf{X}$. For $p_j, q_j \in E[\mathbf{X}]$ coprime over F and q_j monic, define $\text{Coeff}_F(p_1/q_1, \dots, p_m/q_m)$ as the field over F generated by the coefficients from p_1, \dots, q_m .

- a) $\text{Coeff}_F(\mathcal{F})$ is well-defined and coincides with $F(\{f(\mathbf{x}) : \mathbf{x} \in F^n, f \in \mathcal{F}\})$.
- b) For $a_j, b_j, c_j, w_j \in E[\mathbf{X}]$ with $b_j \neq 0$, $\text{Coeff}_F(w_j + c_j \cdot a_j / b_j : j) \subseteq \text{Coeff}_F(w_j, c_j, a_j, b_j : j)$.
- c) Consider the structure $\mathcal{S}' = (E, F, (E, +, \times, \div))$. Any straight-line program computing \mathcal{F} over \mathcal{S}' contains at least $\text{trdeg}_F(\text{Coeff}_F(\mathcal{F}))$ constants from E .
- d) Consider a straight-line program P over $\mathcal{S} := (E, E, (+, \times, \div))$ computing (intermediate) results f_1, \dots, f_N .
 - i) There exist $0 \neq b_j, a_j \in E[\mathbf{X}]$, $c_j \in E$ ($j=1, \dots, N$) such that $f_j = c_j \cdot a_j / b_j$ and $\text{trdeg}_F(\text{Coeff}_F(a_1, \dots, b_N))$ is at most the number of additions in P .
 - ii) There exist $0 \neq v_j, u_j \in E[\mathbf{X}]$, $w_j \in E$ ($j=1, \dots, N$) such that $f_j = w_j + u_j / v_j$ and $\text{trdeg}_F(\text{Coeff}_F(u_1, \dots, v_N))$ is at most twice P ’s number of multiplications/divisions.
- e) Any straight-line program computing \mathcal{F} over \mathcal{S} contains at least $\text{trdeg}_F(\text{Coeff}_F(\mathcal{F})) - |\mathcal{F}|$ additions and $(\text{trdeg}_F(\text{Coeff}_F(\mathcal{F})) - |\mathcal{F}|)/2$ multiplications.

5.2 Some Surprisingly Efficient Algorithms:

Preconditioning, Baur-Strassen, Multipoint Evaluation

Proposition 5.7 (Horner is not optimal with preconditioning).

Let E denote a field and $f = \sum_{j=0}^n \alpha_j X^j \in E[X]$ a polynomial of degree n .

- a) Suppose $f = (X^2 - \xi) \cdot f_1(X) + \eta \in E[X]$ with $\xi, \eta \in E$. Then f can be calculated from $X, X^2, \xi, \eta, f_1(X)$ (the latter of degree $n - 2$) using 1 multiplication and 2 additions/subtractions.
- b) Suppose that $h := \sum_{2\ell+1 \leq n} \alpha_{2\ell+1} X^\ell$ is either constant or a product of linear factors in $E[X]$. Then there is a straight-line program computing f in $E[X]$ from X and X^2 and some elements from E using at most $\lfloor n/2 \rfloor + 2$ multiplications and n additions/subtractions.

c) Suppose E is algebraically closed (or real closed). Then there is a straight-line program computing f in $E[X]$ from X and some elements of E using at most $\lfloor n/2 \rfloor + 3$ multiplications and $n + 1$ additions/subtractions; and for $\alpha_0, \dots, \alpha_n$ algebraically independent, this is optimal up to an additive constant.

Theorem 5.8 (Baur-Strassen). Fix a field F of characteristic 0, $0, 1 \in C \subseteq F$, and let P denote a straight-line program in n variables over $\mathcal{S} = (F, C, (+, -, \times, \div))$ computing $f \in F(X_1, \dots, X_n)$.

Then there exists a straight-line program P' in n variables over \mathcal{S} of length $|P'| \leq 5 \cdot |P|$ simultaneously computing all $f, \partial_1 f, \dots, \partial_n f$.

Theorem 5.9 (Multipoint Evaluation). Let $\mathcal{S} = (\mathbb{C}, \mathbb{S}^1, (+, \times, \div))$.

- a) Let \mathbb{F} denote a field of characteristic 0 and $\bar{u}, \bar{v} \in \mathbb{F}[X]$ such that $\bar{u} \cdot \bar{v} \equiv 1 \pmod{X^n}$. Then $\bar{u} \cdot (2\bar{v} - \bar{u} \cdot \bar{v}^2) \equiv 1 \pmod{X^{2n}}$.
- b) There is a straight-line program over \mathcal{S} of length $\mathcal{O}(n \cdot \log n)$ which, given $u_0, u_1, \dots, u_{n-1} \in \mathbb{C}$ with $u_0 \neq 0$, calculates the unique $v_0, \dots, v_{n-1} \in \mathbb{C}$ such that $(\sum_{k=0}^{n-1} u_k X^k) \cdot (\sum_{k=0}^{n-1} v_k X^k) \equiv 1 \pmod{X^n}$.
- c) Let $n \geq m$. There is a straight-line program over \mathcal{S} of length $\mathcal{O}(n \cdot \log n)$ which, given $a_0, \dots, a_n \in \mathbb{C}$ and $b_0, \dots, b_m \in \mathbb{C}$ with $b_m \neq 0$, calculates the unique $q_0, \dots, q_{n-m} \in \mathbb{C}$ and $r_0, \dots, r_{m-1} \in \mathbb{C}$ such that

$$\sum_{k=0}^n a_k X^k = \left(\sum_{k=0}^m b_k X^k \right) \cdot \left(\sum_{k=0}^{n-m} q_k X^k \right) + \left(\sum_{k=0}^{m-1} r_k X^k \right)$$

- d) There is a straight-line program over \mathcal{S} of length $\mathcal{O}(n \cdot \log^2 n)$ which, given $a_0, \dots, a_{n-1} \in \mathbb{C}$ and $x_1, \dots, x_n \in \mathbb{C}$, simultaneously calculates all $\sum_{k=0}^{n-1} a_k x_\ell^k$, $1 \leq \ell \leq n$.

5.3 Matrix Multiplication and Tensor Rank

Example 5.10 (Strassen) Let $\mathcal{S} = (R, (0, 1), (+, \times))$ denote a ring.

- a) For $A = (A_{ij}), B = (B_{ij}) \in R^{2 \times 2}$ it holds $A \cdot B = C$ where

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

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

- b) Since $R' := R^{n \times n}$ is itself a ring, two matrices over $R^{2n \times 2n}$ can be multiplied using 7 multiplications and a constant number of additions of $n \times n$ -matrices.
- c) $N \times N$ matrix multiplication over R can be performed by a straight-line program over \mathcal{S} of length $\mathcal{O}(n^{\log_2 7}) \leq \mathcal{O}(n^{2.81})$.

Example 5.11 (Matrix Rank and Tensors) Fix a field \mathbb{F} of characteristic 0.

a) For finite-dimensional \mathbb{F} -vector spaces X and Y and a linear map $T : X \rightarrow Y$, it holds

$$\text{rank}(T) = \min \left\{ r \in \mathbb{N} \mid \exists \mathbf{a}_1, \dots, \mathbf{a}_r \in X \exists \mathbf{b}_1, \dots, \mathbf{b}_r \in Y : T = \sum_{j=1}^r \mathbf{b}_j \cdot \mathbf{a}_j^\dagger \right\} .$$

b) Consider $N, M, K \in \mathbb{N}$ and, for $\mathbf{a} \in \mathbb{F}^N, \mathbf{b} \in \mathbb{F}^M, \mathbf{c} \in \mathbb{F}^K$, the $(N \times M \times K)$ -hypermatrix $T = (t_{n,m,k})_{1 \leq n \leq N, 1 \leq m \leq M, 1 \leq k \leq K}$ with $t_{n,m,k} := a_n \cdot b_m \cdot c_k$.

c) Fix finite-dimensional \mathbb{F} -vector spaces X, Y, Z with respective bases $(\mathbf{x}_1, \dots, \mathbf{x}_N), (\mathbf{y}_1, \dots, \mathbf{y}_M)$, and $(\mathbf{z}_1, \dots, \mathbf{z}_K)$ and algebraic duals X^*, Y^*, Z^* . A $(N \times M \times K)$ -hypermatrix $T \in \mathbb{F}^{N \times M \times K}$ gives rise to a bilinear map $T : X^* \times Y^* \rightarrow Z$ via

$$X^* \times Y^* \ni (\mathbf{x}^*, \mathbf{y}^*) \mapsto \sum_{n=1}^N \sum_{m=1}^M \sum_{k=1}^K t_{n,m,k} \cdot \mathbf{x}^*[\mathbf{x}_n] \cdot \mathbf{y}^*[\mathbf{y}_m] \cdot \mathbf{z}_k .$$

And, conversely, any bilinear map $T : X^* \times Y^* \rightarrow Z$ has a representation (w.r.t. fixed bases) as a $N \times M \times K$ -hypermatrix.

Definition 5.12 (Tensor Rank). Fix a field \mathbb{F} of characteristic 0 and finite-dimensional F -vector spaces X, Y, Z with algebraic duals X^*, Y^*, Z^* . A tensor is a bilinear map from $X^* \times Y^*$ to Z . A simple tensor is of the form

$$\mathbf{x} \otimes \mathbf{y} \otimes \mathbf{z} : X^* \times Y^* \ni (\mathbf{u}^*, \mathbf{v}^*) \mapsto \mathbf{u}^*[\mathbf{x}] \cdot \mathbf{v}^*[\mathbf{y}] \cdot \mathbf{z}, \quad \mathbf{x} \in X, \mathbf{y} \in Y, \mathbf{z} \in Z$$

and has $\text{rank} \leq 1$; $\text{rank} = 0$ iff $(\mathbf{x}, \mathbf{y}) = 0$ or $\mathbf{z} = 0$. We denote by $X \otimes Y \otimes Z$ the set of tensors $T : X^* \times Y^* \rightarrow Z$. The rank of such a T is the least $r \in \mathbb{N}$ such that T can be written as the sum of r simple tensors.

Lemma 5.13. a) Each trilinear functional $\hat{T} : X^* \times Y^* \times Z^* \rightarrow \mathbb{F}$ corresponds to a unique tensor $T : X^* \times Y^* \rightarrow Z$ and vice versa. (In the sequel we tacitly identify \hat{T} with $T \dots$)

b) $T \in X \otimes Y \otimes Z$ has the same rank as

$$T' \in Y \otimes Z \otimes X, \quad (\mathbf{y}^*, \mathbf{z}^*) \mapsto (X^* \ni \mathbf{x}^* \mapsto \mathbf{z}^*[T(\mathbf{x}^*, \mathbf{y}^*)] \in F) \in X .$$

c) Each $T \in X \otimes Y \otimes Z$ has $\text{rank}(T) \leq \dim(X) \dim(Y)$ and $\text{rank}(T) \geq \dim \text{range}(T)$.

d) For $X^* := Y^* := Z := \mathbb{F}^{n \times n}$, the tensor of $n \times n$ -matrix multiplication

$$\mathcal{M}_n : X \times Y \rightarrow Z, \quad (A, B) \mapsto A \cdot B$$

has $\text{rank}(\mathcal{M}_2) \leq 7$ and $\text{rank}(\mathcal{M}_{2n}) \leq 7 \cdot \text{rank}(\mathcal{M}_n)$, hence $\text{rank}(\mathcal{M}_n) \leq n^{\lceil \log_2 7 \rceil}$.

e) Let $T \in X \otimes Y \otimes Z$ and $S \in X' \otimes Y' \otimes Z'$. Then

$$\begin{aligned} T \oplus S : (X \oplus X') \times (Y \oplus Y') &\rightarrow Z \oplus Z', & ((\mathbf{x}^*, \mathbf{x}'^*), (\mathbf{y}^*, \mathbf{y}'^*)) &\mapsto T(\mathbf{x}^*, \mathbf{y}^*) \oplus S(\mathbf{x}'^*, \mathbf{y}'^*), \\ T \otimes S : (X \otimes X') \times (Y \otimes Y') &\rightarrow Z \otimes Z', & ((\mathbf{x}^* \otimes \mathbf{x}'^*), (\mathbf{y}^* \otimes \mathbf{y}'^*)) &\mapsto T(\mathbf{x}^*, \mathbf{y}^*) \otimes S(\mathbf{x}'^*, \mathbf{y}'^*) \end{aligned}$$

have $\text{rank}(T \oplus S) \leq \text{rank}(T) + \text{rank}(S)$ and $\text{rank}(T \otimes S) \leq \text{rank}(T) \cdot \text{rank}(S)$.

Theorem 5.14 (Exponent of Matrix Multiplication). Fix a field F of characteristic 0 and $\omega \geq 2$ as well as the structure $\mathcal{S} = (F, F, (+, \times))$. The following are equivalent:

- i) To every $\epsilon > 0$ there exists a family P_n of straight-line programs over \mathcal{S} of length $\mathcal{O}(n^{\omega+\epsilon})$ which, given $A, B \in F^{n \times n}$, calculate $A \cdot B$.
- ii) To every $\epsilon > 0$, it holds $\text{rank}(\mathcal{M}_n) \leq \mathcal{O}(n^{\omega+\epsilon})$.

6 Branching Complexity

Definition 6.1. Let $\mathcal{S} = (S, (c_i), (f_j), (P_k))$ denote a structure with relations $P_k \subseteq S^{b_k}$ or arities $b_k \in \mathbb{N}$.

- a) A **Branching Tree** $T_{\mathcal{S}}$ (over this structure and in variables X_1, \dots, X_n) is basically a straight-line program with the additional capability to branch based on whether a predicate P_k , applied to previously calculated results, holds or not. More formally, it is a rooted binary tree whose outdegree-1 nodes $u \in T_{\mathcal{S}}$ are each labelled with either a variable, a constant c_i from \mathcal{S} , or with a function f_j applied to results from a_j outdegree-1 predecessor nodes of u ; and each outdegree-2 node is labelled with a predicate P_k applied to b_k degree-1 predecessor nodes. Each leaf (=outdegree-0 node) is labelled either with some symbol $\sigma \in \Sigma$ or with some finite tuple of degree-1 predecessor nodes.
- b) When assigned values $x_1, \dots, x_n \in S$ to X_1, \dots, X_n the tree calculates, starting from the root, in outdegree-1 nodes intermediate results; and in outdegree-2 nodes branches according to whether the predicate holds. $T_{\mathcal{S}}$ **accepts** input $\mathbf{x} \in S^n$ if this process ends in a leaf labelled $+\in \Sigma$; it **rejects** if the leaf is labelled $-\in \Sigma$; otherwise it **computes** the specified (tuple of intermediate) value(s).
- c) The size of a branching tree is its total number of nodes; similarly for the depth.

Example 6.2 (Sorting) Consider some totally ordered set S and the structure $\mathcal{S} = (S, (), (), (<))$. We say that a branching tree over \mathcal{S} on n variables **sorts** if it computes some function $(f_1, \dots, f_n) = f : S^n \rightarrow S^n$ such that, for every $\bar{x} = (x_1, \dots, x_n) \in S^n$,

$$f_1(\bar{x}) \leq f_2(\bar{x}) \leq \dots \leq f_n(\bar{x}) \quad \text{and} \quad \forall y \in S : \#\{j : x_j = y\} = \#\{j : f_j(x_1, \dots, x_n) = y\} \quad (1)$$

- a) For each $n \in \mathbb{N}$, both **Bubble Sort** and **Quicksort** give rise to branching trees over \mathcal{S} in n variables of depth $\mathcal{O}(n^2)$.
- b) **Heap Sort** gives rise to a branching tree over \mathcal{S} in n variables of depth $\mathcal{O}(n \cdot \log n)$.
- c) If $|S| \geq n$, then any branching tree over \mathcal{S} in n variables has at least $n!$ different leaves. In particular, **Heap Sort** is asymptotically optimal.

6.1 Hyperplane Arrangements and Combinatorial Convex Geometry

Definition 6.3. Fix $d \in \mathbb{N}$.

- a) A set $X \subseteq \mathbb{R}^d$ is **convex** if

$$\forall \mathbf{x}, \mathbf{y} \in X : \lambda \mathbf{x} + (1 - \lambda) \mathbf{y} \in X \quad (2)$$

holds for every $0 \leq \lambda \leq 1$. X is **affine** if Equation (2) holds for every $\lambda \in \mathbb{R}$; equivalently: $X \neq \emptyset$ and $X - \mathbf{y} := \{\mathbf{x} - \mathbf{y} : \mathbf{x} \in X\}$ is a vector space for some/every $\mathbf{y} \in X$.

- b) We call $\mathbf{h} \in \mathbb{S}^d = \{\mathbf{y} \in \mathbb{R}^{d+1} : \|\mathbf{y}\| = 1\}$ an **oriented hyperplane**. Its **open halfspace** $H_{<\mathbf{h}}$ is the set $\{\mathbf{x} \in \mathbb{R}^d : \sum_j x_j \cdot h_j < h_0\}$; the topological closure $H_{\leq \mathbf{h}} := \overline{H_{<\mathbf{h}}}$ its **closed halfspace**. Finally write $H_{=\mathbf{h}} := H_{\leq \mathbf{h}} \cap H_{\leq -\mathbf{h}}$ for its **affine hyperplane**.

- c) The *dimension* of $X \subseteq \mathbb{R}^d$, $\dim(X)$, is the affine dimension of $\text{ahull}(X) := \{\lambda \cdot \mathbf{x} + (1 - \lambda) \cdot \mathbf{y} : \mathbf{x}, \mathbf{y} \in X, \lambda \in \mathbb{R}\}$; $\dim(\emptyset) := -\infty$. A (convex) **polytope** $P \subseteq \mathbb{R}^d$ is the finite intersection of finitely many open/closed halfspaces.
- d) The **membership problem** associated with a finite family \mathcal{H} of affine hyperplanes in \mathbb{R}^d is the question of whether a given $\mathbf{x} \in \mathbb{R}^d$ belongs to $\bigcup \mathcal{H}$ or not.
- e) For $\mathbf{h} \in \mathbb{S}^d$ and $\mathbf{x} \in \mathbb{R}^d$, write $\text{sgn}(\mathbf{x}, \mathbf{h}) := \text{sgn}(\sum_j x_j \cdot h_j - h_0) \in \{+, 0, -\}$.
- f) The **point location problem** associated with a finite family $\mathcal{H} = \{\mathbf{h}^{(1)}, \dots, \mathbf{h}^{(n)}\}$ of oriented hyperplanes is the function

$$\mathbb{R}^d \ni \mathbf{x} \mapsto \text{sgn}(\mathbf{x}, \mathcal{H}) := (\text{sgn}(\mathbf{x}, \mathbf{h}^{(k)}))_{1 \leq k \leq n} \in \{+, 0, -\}^n .$$

- g) A **face** of \mathcal{H} is a subset of \mathbb{R}^d of the form

$$\mathcal{H}(\bar{\sigma}) := \{\mathbf{x} \in \mathbb{R}^d : \text{sgn}(\mathbf{x}, \mathcal{H}) = \bar{\sigma}\}, \quad \bar{\sigma} \in \{+, 0, -\}^n .$$

A face of dimension 0 is called a **vertex**; an **edge** is a face of dimension 1; a face of dimension d is a **cell**; a **facet** is a face of dimension $d - 1$; a face of dimension $d - 2$ is called **ridge**.

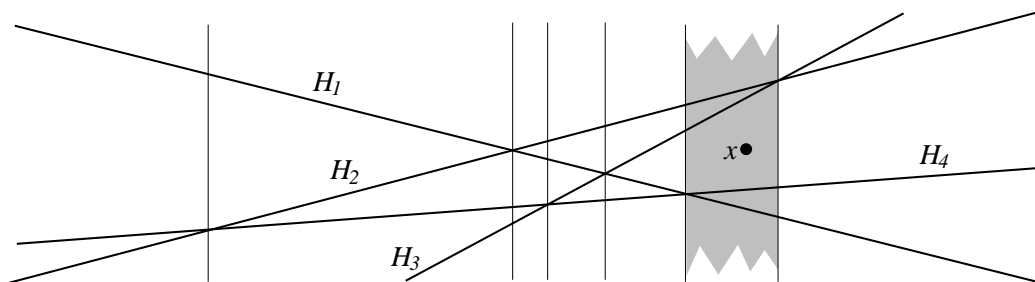


Fig. 3. An arrangement of 4 lines in the plane inducing 6 intersections (=vertices), 16 line segments (=edges=ridges=facets), and 11 cells.

Lemma 6.4. Fix a finite family \mathcal{H} of n oriented hyperplanes in \mathbb{R}^d .

- a) Each face of \mathcal{H} is a polytope.
- b) Each vertex of \mathcal{H} is determined by (at least) d hyperplanes.
In particular, \mathcal{H} has at most $\binom{n}{d}$ vertices.
- c) For an arrangement of n hyperplanes in dimension d , the number of k -dimensional faces is at most $\sum_{j=0}^k \binom{d-j}{k-j} \cdot \binom{n}{d-j}$
- d) and these numbers are attained by almost every arrangement.

Example 6.5 For $2 < N \in \mathbb{N}$, the following 2D arrangement has a cell with N facets:

$$\mathbf{h}_n := (1, \cos \frac{2\pi n}{N}, \sin \frac{2\pi n}{N}) / \sqrt{2}, \quad 0 \leq n < N .$$

6.2 Linear Branching Trees

Definition 6.6. A *Linear Branching Tree* for dimension $d \in \mathbb{N}$ is a branching tree over the structure $\mathcal{S} := (\mathbb{R}^d, (), (), (H_{=\mathbf{h}}, H_{<\mathbf{h}} : \mathbf{h} \in \mathbb{S}^d))$.

Example 6.7 To each n -element family \mathcal{H} of oriented hyperplanes in \mathbb{R}^d , there exists a *Linear Branching Tree* of depth $\mathcal{O}(n)$ deciding the membership problem associated with \mathcal{H} .

Lemma 6.8. Let T denote a linear branching tree for dimension d and v a vertex of T . Write $T(v)$ for the set of inputs $\mathbf{x} \in \mathbb{R}^d$ which, according to the semantics of Definition 6.1b), passes through v .

- a) $T(v)$ is a polytope. Each facet corresponds to an oriented hyperplanes queried by T on the path from the root up to v .
- b) For the leaves v_1, \dots, v_N of T , $(T(v_j))_{j=1, \dots, N}$ constitutes a partition of \mathbb{R}^d .
- c) For any linear branching tree T over \mathcal{S} solving membership to \mathcal{H} , and for each leaf v of T , $T(v)$ is either a subset of some $H_{=\mathbf{h}}$ with $\mathbf{h} \in H$ or of $\mathcal{H}(\bar{\sigma})$ for some $\bar{\sigma} \in \{+, -\}^{\mathcal{H}}$.

Theorem 6.9 (Ukkonen'83, Dobkin/Lipton'74, Meiser'93).

Fix an n -element family \mathcal{H} of oriented hyperplanes in dimension d .

- a) Suppose \mathcal{H} has N distinct cells. Then any linear branching tree over \mathcal{S} deciding membership to \mathcal{H} has depth at least $\log N$.
- b) Let $\mathcal{H}(\bar{\sigma})$ denote a cell having m facets. Then any linear branching tree over $(\mathbb{R}^d, (), (), (H_{=\mathbf{h}}, H_{<\mathbf{h}} : \mathbf{h} \in \mathcal{H}))$ deciding membership to \mathcal{H} has depth at least m .
- c) There exists a linear branching tree over \mathcal{S} of depth $\mathcal{O}(\log n)$ solving the point location problem for \mathcal{H} .
- d) There exists a linear branching tree over \mathcal{S} of depth $\mathcal{O}(d^5 \log n)$ solving the point location problem for \mathcal{H} .

References

1. M. LI, P. VITÁNYI: “An Introduction to Kolmogorov Complexity and its Applications”, Springer
2. F. MEYER AUF DER HEIDE: “Skript zu Komplexitätstheorie II”, <http://www.upb.de/cs/ag-madh/vor1/KomplexII99> (1999)
3. C. PAPADIMITRIOU: “Computational Complexity”, Addison-Wesley (1995).
4. K.R. REISCHUK: “Komplexitätstheorie”, Teubner (1999)
5. U. SCHÖNING, R. PRUIM: “Gems of Theoretical Computer Science”, Springer (1998).
6. P. BÜRGISSER, M. CLAUSEN, A. SHOKROLLAHI: “Algebraic Complexity Theory”, Springer (1997).
7. H. EDELSBRUNNER: “Algorithms in Combinatorial Geometry”, Springer EATCS Monographs vol.10 (1987).