On the Complexity of Tensor Formulae

Carsten Damm

Universität Trier

Aims of this talk:

- present natural algebraic problems, characterizing complexity classes like $NP, \oplus P, NL, \oplus L$
- give a new and *unified* proof for the inclusions
  - $NP/poly \subseteq \oplus P/poly$ [Valiant,Vazirani'86]
  - $SAC^1/poly \subseteq \oplus SAC^1/poly$ [Gál'95]
  - $NL/poly \subseteq \oplus L/poly$ [Wigderson'94]

1 Complexity Classes

NP — problems A of type

$\exists NP$-machine M

$$A = \{x | \#Acc_M(x) \neq 0\}$$

SAT, CLIQUE, TSP, ...

$\oplus P$ — problems A of type

$\exists NP$-machine M

$$A = \{x | \#Acc_M(x) \neq 0 \mod 2\}$$

[Papadimitriou,Zachos'83]
ODD-SAT, *odd* versions of NP-problems

NL — problems A of type

$\exists NL$-machine M

$$A = \{x | \#Acc_M(x) \neq 0\}$$

s-t-CONNECTIVITY, 2SAT, ...

$\oplus L$ — problems A of type

$\exists NL$-machine M

$$A = \{x | \#Acc_M(x) \neq 0 \mod 2\}$$

ODD-s-t-CONNECTIVITY, ...
DETERMINANT mod 2, ...

SAC^1 — problems computable by

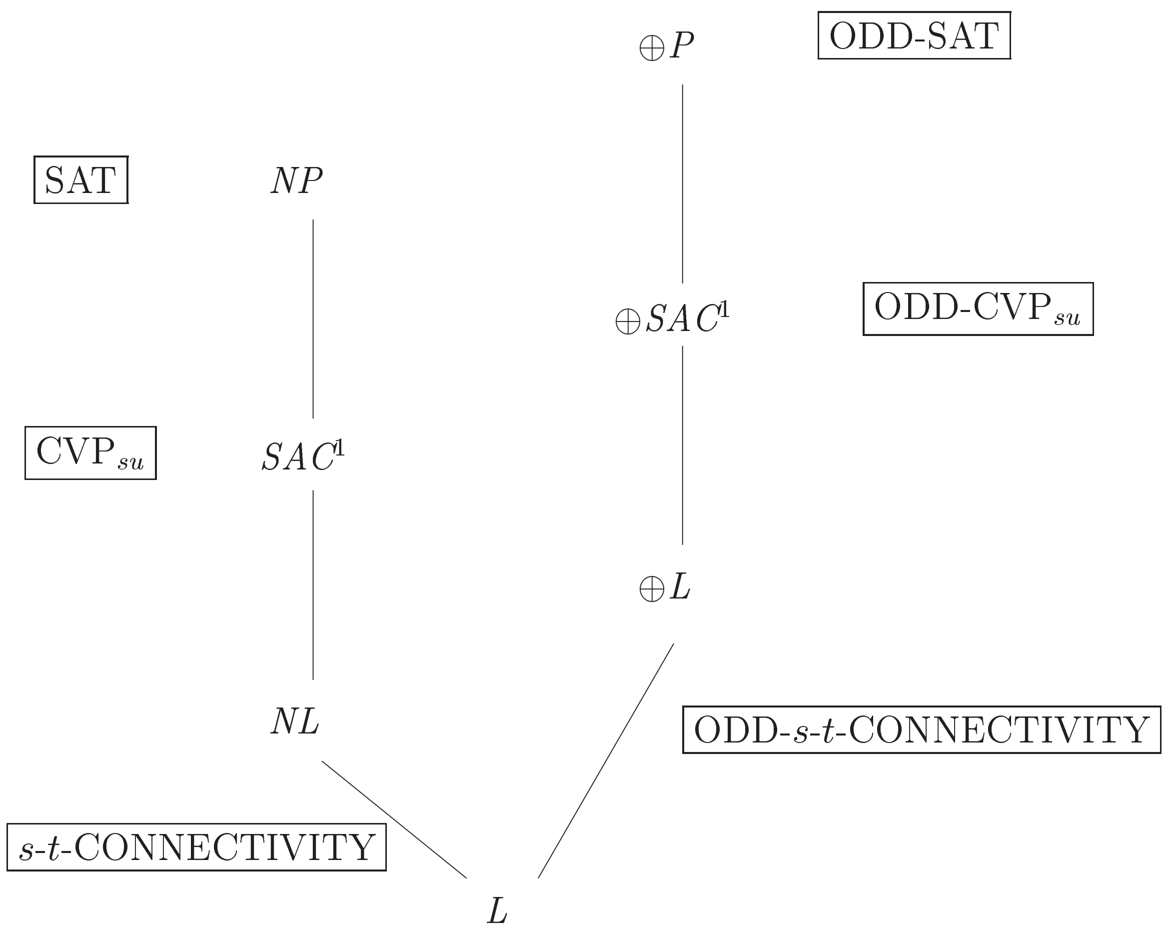
uniform log-depth, poly-size circuits with bounded fan-in AND and unbounded fan-in OR

CVP_{su}, CFL

$\oplus SAC^1$ — problems computable by

uniform log-depth, poly-size circuits with bounded fan-in AND and unbounded fan-in $PARITY$

ODD-CVP_{su}



$\oplus P$
ODD-SAT
SAT
NP
$\oplus SAC^1$
ODD-CVP$_{su}$
CVP$_{su}$
SAC^1
$\oplus L$
NL
ODD-s-t-CONNECTIVITY
s-t-CONNECTIVITY
L

2 Tensor Calculus

tensors $\leftrightharpoons$ multi-dimensional matrices

Definition 1 *Let K be a field. A **tensor** is a tuple*

$$(t_{i_1,\dots,i_k}) \in \mathbb{T}_{d_1,\dots,d_k}(K)$$

of field elements.

Operations on tensors:

- addition

  $$((s+t)_{i,\dots}) := (s_{i,\dots} + t_{i,\dots})$$

  [same format]

- multiplication (tensor product)

  $$((s \cdot t)_{i,\dots,k,\dots}) := (s_{i,\dots} \cdot t_{k,\dots})$$

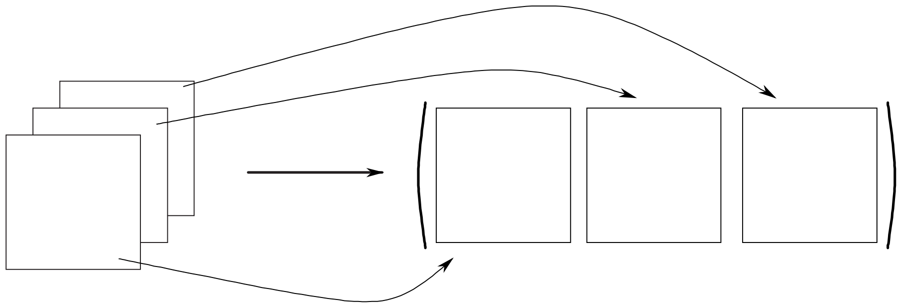
  [any format]

- junction (generalization of matrix trace)

  $$\Gamma_{k,l}(t_{i,\dots,k,\dots,j,\dots,l,\dots}) := \left(\sum_m t_{i,\dots,m,\dots,j,\dots,m,\dots} \right)$$

  [special format]

Matrix notation for tensors:



tensor operations	$\Leftrightarrow$	**matrix operations**
sum	$\Leftrightarrow$	sum
junction	$\Leftrightarrow$	product
product	$\Leftrightarrow$	Kronecker product

$$A \otimes B := \begin{pmatrix} a_{1,1} \cdot B & \dots & a_{1,l} \cdot B \\ \vdots & \ddots & \vdots \\ a_{k,1} \cdot B & \dots & a_{k,l} \cdot B \end{pmatrix}$$

Remark 2 *Operations not restricted to field! Can be considered over any semi-ring S:*

- *the Booleans* $\mathbb{B} = (\{0,1\}, \wedge, \vee)$,
- *the two-element field* $\mathbb{F}_2$,
- $\dots$

Tensor formula evaluation problem TEP_S

Given well-formed *tensor formula* $F(r, s, \dots, t)$.

Example: $\big((1,1) \cdot \big((0,1,1) \otimes (1,0)^T\big) + (1,0,1)\big) \cdot (0,1,0)^T$.

Decide whether $\mathrm{val}_S(F(r,s,\dots,t)) \neq 0_S$.

3 Completeness Results

Theorem 3
$\mathrm{TEP}_{\mathbb{B}}$ *is complete for NP.*
$\mathrm{TEP}_{\mathbb{F}_2}$ *is complete for* $\oplus P$.

Sketch: $SAT \leq^P_{\text{m-1}} \mathrm{TEP}_{\mathbb{B}}$

3CNF $F = C_1 \wedge C_2 \wedge \ldots \wedge C_m$

- encode assignments by rows and clauses by columns:
  $(a, C_i) \mapsto (\tilde{a}, \widetilde{C_i}^T)$ s.t.

  $$a \text{ satisfies } C_i \text{ iff } \tilde{a} \cdot \widetilde{C_i}^T = 1 \ (\textit{Boolean} \text{ matrix product}).$$

  Example:

  $n = 4,\ a = (1, 0, 0, 1) \mapsto \tilde{a} = (1001\ 0110)$
  $C = (x_1 \vee x_2 \vee \neg x_4) \mapsto \widetilde{C} = (1100\ 0001)$

  $$a \text{ satisfies } F \Leftrightarrow \tilde{a} \cdot (\widetilde{C_1}^T, \ldots, \widetilde{C_m}^T) = (\underbrace{1, \ldots, 1}_{m})$$

- construct "truth table matrix" TT_n containing all 2^n $\tilde{a}$ by poly-size tensor formula

  $$F \text{ satisfiable } \Leftrightarrow M_F := TT_n \cdot (\widetilde{C_1}^T, \ldots, \widetilde{C_m}^T) \text{ contains 1-row}$$

- reformulate condition

  $$M_F \text{ contains 1-row } \Leftrightarrow v \cdot M_F^{\otimes m} \cdot w^T = 1,$$

  for special vectors v, w constructable by poly-size tensor formulae

$\square$

Sketch: $SAT \leq^P_{\text{m-1}} \text{TEP}_{\mathbb{F}_2}$

similar, but more careful: a may satisfy *several* literals in a clause!

Observation 1: x, y, z literals $\Rightarrow$

$$x \vee y \vee z = x + y + z + xy + xz + yz + xyz \mod 2$$

Observation 2: $v = (v_1, \ldots, v_t) \in \{0,1\}^t \Rightarrow$

entries of $v \otimes v \otimes v$ are the products of up to 3 entries of v

- encode a by $\tilde{\tilde{a}} = \tilde{a} \otimes \tilde{a} \otimes \tilde{a}$
- encode C_i by $\overline{C_i}$, obtained from $\widetilde{\widetilde{C_i}} = \widetilde{C_i} \otimes \widetilde{C_i} \otimes \widetilde{C_i}$ by deleting duplicates

  Example:

  entries corresponding to $x_1x_1x_2, x_1x_2x_1, \ldots, x_2x_2x_1$ appear in $\widetilde{\widetilde{C_i}}$ but have same value $\Rightarrow$ replace all but the first by 0

$$a \text{ satisfies } C_i \Leftrightarrow \tilde{\tilde{a}} \cdot \overline{C_i} = 1 \mod 2$$

$\overline{TT_n} = S \cdot (TT_n \otimes TT_n \otimes TT_n)$ contains all $\tilde{\tilde{a}}$ (S = row selector matrix, constructable by poly-size tensor formula)

$$\overline{M_F} := \overline{TT_n} \cdot (\overline{C_1}^T, \ldots, \overline{C_m}^T)$$

$$F \text{ odd-satisfyable } \Leftrightarrow v \cdot \overline{M_F}^{\otimes m} \cdot w^T = 1$$

$\square$

tensor formulae can grow fast:

$$\underbrace{(1,1)\otimes(1,1)\otimes\ldots\otimes(1,1)}_{n} = (\underbrace{1,\ldots,1}_{2^n})$$

Restricted Versions

F is *tame*, if

$$\mathrm{ord}(F) \leq 2\cdot\max\{\mathrm{ord}(G)\,|\,G \text{ is a constant sub-formula}\}$$

F is *simple*, if

$$F \text{ does not contain "}\otimes\text{"}$$

$\Longrightarrow$ **Evaluation Problems** t-TEP$_S$ and s-TEP$_S$

Theorem 4
t-TEP$_{\mathbb{B}}$ *is complete for* SAC^1.
t-TEP$_{\mathbb{F}_2}$ *is complete for* $\oplus SAC^1$.

Theorem 5
s-TEP$_{\mathbb{B}}$ *is complete for* NL.
s-TEP$_{\mathbb{F}_2}$ *is complete for* $\oplus L$.

4 Non-uniform Complexity Classes

use special algorithm (*advice* α_n) for each input length n:

- $NP/poly$ and $\oplus P/poly$

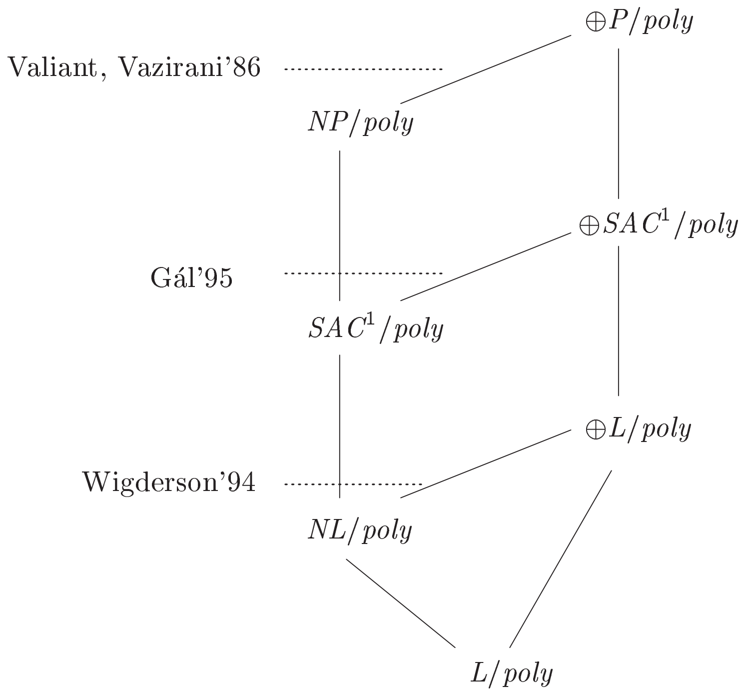
  — poly-size non-deterministic circuits

- $SAC^1/poly$ and $\oplus SAC^1/poly$

  — poly-size, log-depth semi-unbounded circuits

- $NL/poly$ and $\oplus L/poly$

  — poly-size non-deterministic branching programs


$\oplus P/poly$
Valiant, Vazirani'86
$NP/poly$
$\oplus SAC^1/poly$
Gál'95
$SAC^1/poly$
$\oplus L/poly$
Wigderson'94
$NL/poly$
$L/poly$

5 The Idea of Non-uniform Reductions

Definition 6 *$A \leq_{m\text{-}1}^{RP} B$ if there is a randomized polynomial time Turing machine M such that*

- $\forall x \,:\, x \notin A \Rightarrow M(x) \notin B$,
- $\forall x \,:\, x \in A \Rightarrow \mathbf{Pr}[M(x) \in B] \geq 1/2$.

Claim 7
If A and B are complete for $\mathcal{C}_1$ and $\mathcal{C}_2$ under $\leq_{m\text{-}1}^{P}$ and both classes are closed under $\leq_{m\text{-}1}^{P/poly}$, then

$$A \leq_{m\text{-}1}^{RP} B \;\Rightarrow\; \mathcal{C}_1/poly \subseteq \mathcal{C}_2/poly.$$

Proof: A counting argument. □

If A and B are complete for $\mathcal{C}_1$ and $\mathcal{C}_2$ under $\leq_{m\text{-}1}^{L}$ and both classes are closed under $\leq_{m\text{-}1}^{L/poly}$, then

$$A \leq_{m\text{-}1}^{RL} B \;\Rightarrow\; \mathcal{C}_1/poly \subseteq \mathcal{C}_2/poly.$$

wanted:

- 3SAT $\leq^{RP}_{\text{m-1}}$ ODD-3SAT
- $\text{CVP}_{su} \leq^{RL}_{\text{m-1}} \text{ODD-CVP}_{su}$
- s-t-CONNECTIVITY $\leq^{RL}_{\text{m-1}}$ ODD-s-t-CONNECTIVITY

Solution 1

Uniqueness Lemmas[a][b]:
Given instance x of *Boolean* problem A ($x \in A$ iff $\mathrm{Cert}_A(x) \neq \emptyset$), consider alteration A' of A and do a random change $x \mapsto x_r$, such that

- $(x, r) \mapsto x_r$ is "easy to compute".
- If $\mathrm{Cert}_A(x) = \emptyset$, then $\mathrm{Cert}_{A'}(x_r) = \emptyset$, regardless of r.
- If $\mathrm{Cert}_A(x) \neq \emptyset$, then *probably* $\#\mathrm{Cert}_{A'}(x_r) = 1$ for some A' related to A.

[a] Valiant,Vazirani's Lemma
[b] Mulmuley,Vazirani,Vazirani's Isolating Lemma

Simulation: Translate uniqueness into "parity computation".

Technical differences:

- NP vs. $\oplus P$: $A = A' = SAT$ (essentially)
  NL vs. $\oplus L$: $A = s$-t-CONNECTIVITY
  $A' =$ UNIQUE-MINIMAL-s-t-PATH
- Valiant,Vazirani's Lemma does not seem applicable to NL or SAC^1-problems
- diversity of complete problems

6 The Arithmetization Approach

Solution 2

Arithmetization:

Let K be a finite field. Given instance x of *Boolean* problem A ($x \in A$ iff $\mathrm{Cert}_A(x) \neq \emptyset$), assign polynomial

$$p_x(z) = \sum_{c \in \mathrm{Cert}_A(x)} m_c(z) \in K[z_1, \ldots, z_t],$$

such that $p_x(z) = \mathbf{0}$ if and only if $\mathrm{Cert}_A(x) = \emptyset$.

Polynomial Testing[a]:

For random $r \in K^t$ holds:

- If $p_x(z) = \mathbf{0}$, then $p_x(r) = 0$, regardless of r.
- If $p_x(z) \neq \mathbf{0}$, then

$$\mathbf{Pr}[p_x(r) \neq 0] \geq 1 - \frac{\deg p_x(z)}{|K|}.$$

[a] e.g., Schwartz, Zippel, …

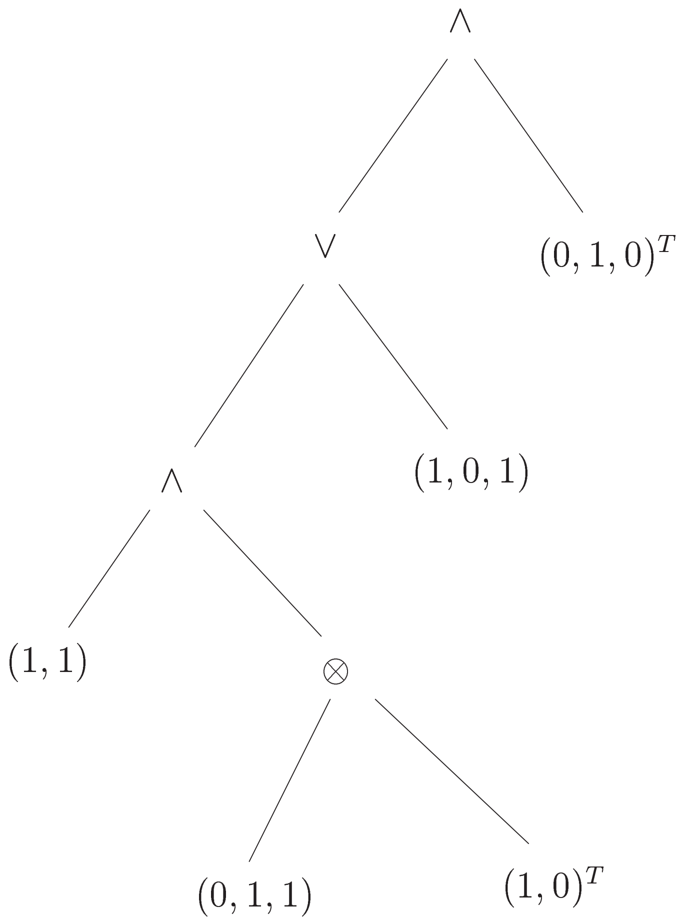
Simulation:

Choose $K = GF(2^d)$ and translate testing $p_x(r) = 0$ into "parity computation".

Application

- $\mathrm{TEP}_{\mathbb{B}} \leq^{RP}_{\text{m-1}} \mathrm{TEP}_{\mathbb{F}_2}$

  Example: $\big((1,1) \wedge \big((0,1,1) \otimes (1,0)^T\big) \vee (1,0,1)\big) \wedge (0,1,0)^T$.



Certificate: *minimal* collection $C = \{(G,i,j),\dots\}$ of entries of sub-formulae, s.t.

- root $\in S$
- each entry evaluates to 1

Observation 1:
For each sub-formula G holds $\mathrm{ord}(G) \leq 2^{O(|F|)}$

$\Longrightarrow$ each entry can be encoded by $s = O(|F|)$ bits

consider variables $z_G^1, \dots, z_G^s$

$$G_{i,j} \mapsto m_{(G,i,j)}(z) := \prod_{\mathrm{bin}_l(i,j)=1} z_G^l$$

$$p_F(z) := \sum_{C \in \mathrm{Cert}(F)} \prod_{(G,i,j) \in C} m_{(G,i,j)}.$$

$t = \#$ variables $= O(|F|^2)$,

$\Longrightarrow K = \mathbb{F}_{2^d}, d \leq 2 \log |F|$ sufficient for polynomial testing

choose $r \in K^t$, test for $p_F(r) \neq 0$

simulate computation of $p_F(r)$ by tensor formula over $\mathbb{F}_2$

Observation 2:
by field arithmetic

- sum of K-tensors — d-tupel of sums of $\mathbb{F}_2$-tensors
- product of K-tensors — sum of d-tupel of products of $\mathbb{F}_2$-tensors
- tensor product of K-tensors — sum of d-tupel of tensor products of $\mathbb{F}_2$-tensors

$\Longrightarrow$

$$\mathrm{TEP}_{\mathbb{B}} \leq^{RP}_{\text{m-1}} \mathrm{TEP}_{\mathbb{F}_2}$$

$$\text{t-TEP}_{\mathbb{B}} \leq^{RP}_{\text{m-1}} \text{t-TEP}_{\mathbb{F}_2}$$

$$\text{s-TEP}_{\mathbb{B}} \leq^{RP}_{\text{m-1}} \text{s-TEP}_{\mathbb{F}_2}$$

7 Discussion

Buntrock, D., Hertrampf, Meinel'90:
standard problems of linear algebra over finite fields complete for log-space *MOD*-classes:

- determinant
- solving linear equations
- computing rank
- ...

Is there a similar characterization of *multi-linear* algebra by polynomial time *MOD*-classes?

Probably not!!

- evaluation problems for tensor formulae strongly depend on ground field:

$$\mathrm{TEP}_{\mathbb{F}_p} \text{ complete for } MOD_p\text{-}P$$

- computing tensor rank over *any field* is *NP*-hard [Håstad'90]