On Arithmetic Branching Programs

Amos Beimel, Harvard University

Anna Gál, The University of Texas at Austin

DIMACS, June 1999

Motivation: Power of Algebraic Operations

Is computing the rank harder than checking independence?

Need appropriate computation models

model	operation
span programs [KW93]	rank
dependency programs [PS96]	dependency
arithmetic branching programs	independence

Goal: understand relationship between these models

Applications

Span Programs.

- Generalized Secret Sharing Schemes [BD91,KW93]
- Generalized multi-party computation [CDM98]
- Lower bounds for formulae, deterministic branching programs
- Lower bounds for Nullstellensatz proof systems [PS96]

Arithmetic Programs.

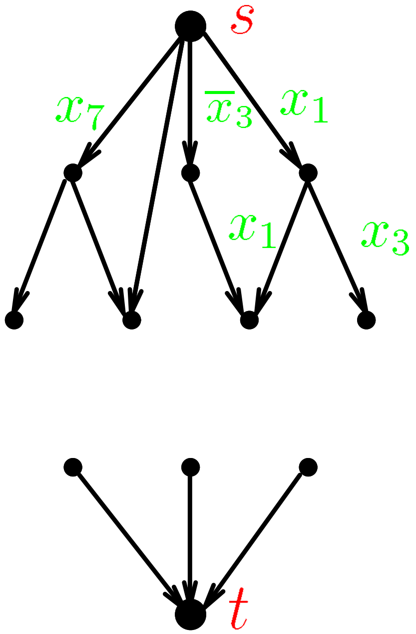
- Construction of private simultaneous protocols [IK97]

Overview of Talk

1. Definitions of the algebraic computational models
2. Previous results and new results
3. Some proofs
4. Conclusions and open problems

Part I: Definitions

Nondeterministic Branching Programs



- Directed acyclic graph
- Edges labeled by the literal:

  $\{x_1, \ldots, x_n, \overline{x}_1, \ldots, \overline{x}_n\}$

- $f(y) = 1$ iff $\exists$ path consistent with y

- size = number of edges
- complexity class: non-uniform NL

Modular Branching Programs

Nondeterministic branching programs with a different accepting criterion

mod-p branching programs:

$f(y) = 1$ iff # paths consistent with $y \neq 0 \bmod p$

Complexity class:

$\mathrm{MOD}_p\ \mathrm{L}$ [BDHM92]

p constant: poly-size span programs over $\mathrm{GF}(p)$ [KW93]

How to generalize to arbitrary fields?

Arithmetic Branching Programs

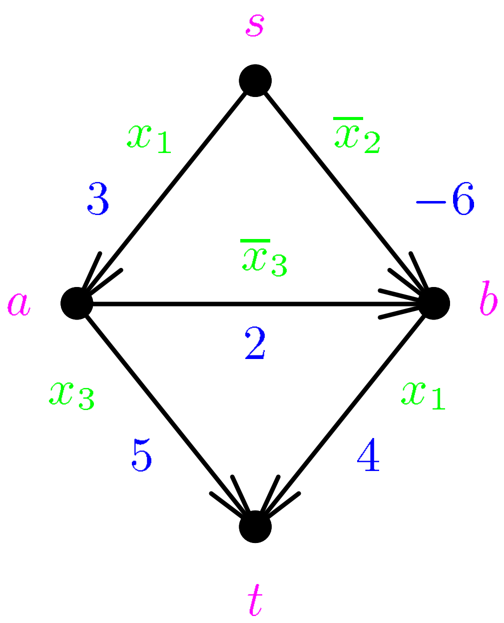
Defined over a field $\mathcal{K}$

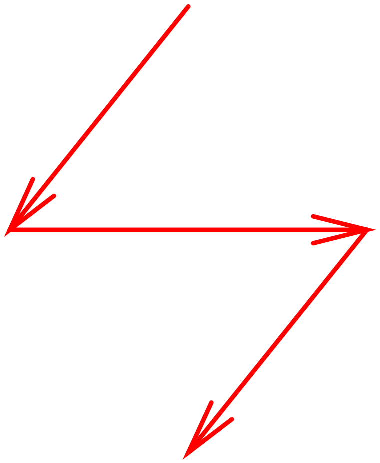
Every edge has a weight from $\mathcal{K}$

Weight of a path: product of weights of edges

$f(y) = 1$ iff sum of weights of consistent paths $\neq 0$

Example: Arithmetic Branching Programs

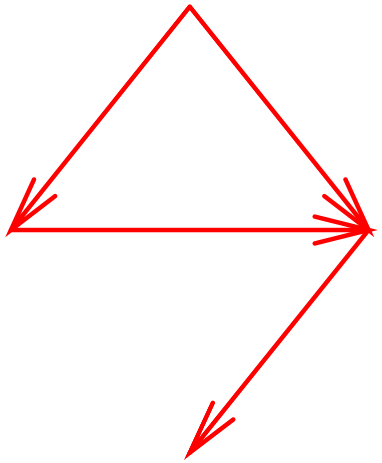




$y_1 = 1,\ y_2 = 1,\ y_3 = 0$

Consistent paths	weight
$s \to a \to b \to t$	$3 \cdot 2 \cdot 4 = 24$

Accepted



$y_1 = 1, \; y_2 = 0, \; y_3 = 0$

Consistent paths	weight
$s \to a \to b \to t$	24
$s \to b \to t$	-24

Rejected

DEF: Dependency Programs [PS96]

M matrix over field $\mathcal{K}$

Each row of M is labeled by a literal from $\{x_1, \ldots, x_n, \overline{x}_1, \ldots, \overline{x}_n\}$

Input $y \in \{0,1\}^n \Longrightarrow$ submatrix M_y – rows with consistent labels

Dependency programs accepts $y \Longleftrightarrow$ rows of M_y are dependent

size = number of rows in M

Example: Dependency Program

x_1	1	2	4	0
$\overline{x}_1$	0	0	0	1
x_2	1	1	1	0
x_2	1	3	7	0

$y_1 = 1,\ y_2 = 1$ Accept

$y_1 = 0,\ y_2 = 1$ Reject

/Span Program

Dependency prog. Span prog.

Reject

Accept

DEF: Span Programs [KW93]

Original Motivation:

proving lower bounds for modular branching programs

Like dependency programs

Span program accepts $y \iff \vec{1} \in \mathrm{span}(M_y)$

Notation

$\mathrm{NBP}(f)$ – size of smallest nondeterministic branching program

$\mathrm{AP}_{\mathcal{K}}(f)$ – size of smallest arithmetic branching program

$\mathrm{DP}_{\mathcal{K}}(f)$ – size of smallest dependency program

$\mathrm{SP}_{\mathcal{K}}(f)$ – size of smallest span program

Part II: Previous and New Results

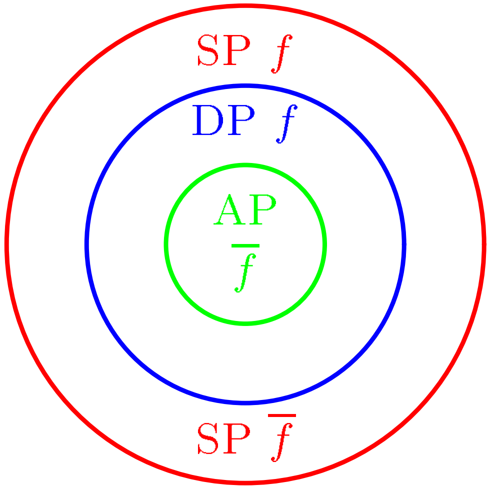
Previous Results

[PS96] + This work

$\frac{1}{n} \cdot \mathrm{SP}_{\mathcal{K}}(f) \leq \mathrm{DP}_{\mathcal{K}}(f) \leq 2 \cdot \mathrm{AP}_{\mathcal{K}}\left(\overline{f}\right)$

[Gál95,PS96]

$\mathrm{SP}_{\mathcal{K}}(f) = \mathrm{SP}_{\mathcal{K}}\left(\overline{f}\right)$



[BDHM92]

$$\mathrm{AP}_{GF(q)}(f) \leq (q-1) \cdot \mathrm{AP}_{GF(q)}(\overline{f})$$

[KW93]

$$\mathrm{AP}_{GF(q)}(f) \leq \mathrm{poly}\left(q \cdot \mathrm{SP}_{GF(q)}(f)\right)$$

Main Results

- Arithmetic programs are closed under disjunction, conjunction
- $\mathrm{AP}_{\mathcal{K}}\left(\overline{f}\right) \leq \mathrm{poly}\left(\mathrm{DP}_{\mathcal{K}}(f)\right)$

$\Longrightarrow$ with [PS96]

f has small dependency prog. iff $\overline{f}$ has small arithmetic prog.

$\Longrightarrow$ Dependency programs are closed under conjunction

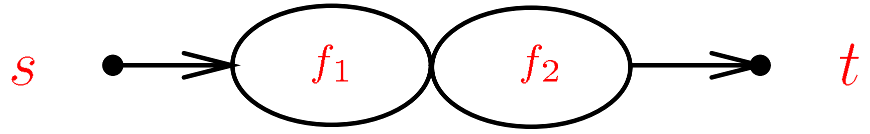
(open problem in [PS96])

- $\mathrm{AP}_{\mathcal{K}}(f) \leq \tilde{O}\left(n^2 \cdot \mathrm{NBP}(f)\right)$

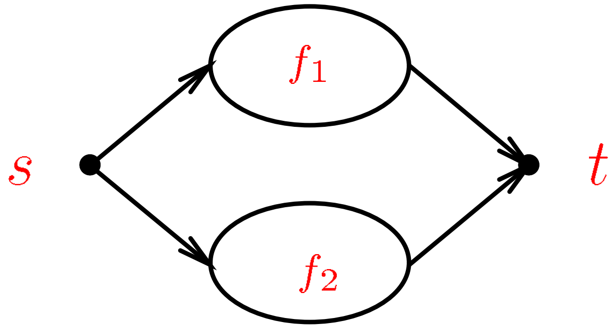
Part III: Some Proofs

Properties of Arithmetic Programs

- Closed under conjunction $f_1 \wedge f_2$



- Closed under disjunction $f_1 \vee f_2$



over infinite fields

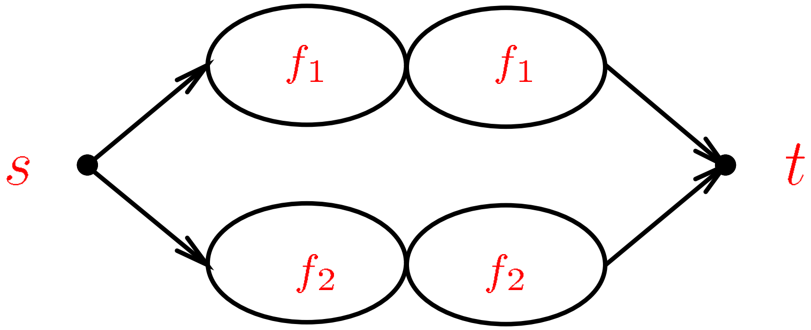
α

Sum of accepting paths: $x + \alpha y$

There are $\leq 2^n$ accepting assignments $\Longrightarrow \exists \alpha \in \mathcal{K}$ that is good.

Disjunction: Finite Fields

Example $\Re$: $x^2 + y^2 = 0$ iff $x = y = 0$



Every finite field has a polynomial of degree 2

$$Q(x, y) = 0 \text{ iff } x = y = 0$$

Conclusion: $\forall \mathcal{K}$ $\mathrm{AP}_{\mathcal{K}}(f_1 \vee f_2) \leq 2 \cdot (\mathrm{AP}_{\mathcal{K}}(f_1) + \mathrm{AP}_{\mathcal{K}}(f_2))$

Arithmetic Program $\Longrightarrow$ Dependency Programs [PS96]

Stage I (following [BDHM92])

Graph of arithmetic program computing $f \Longrightarrow$ matrix $B(x)$

$B(x)$ entries – $a \cdot x_i$, $a \cdot \overline{x}_i$, or a

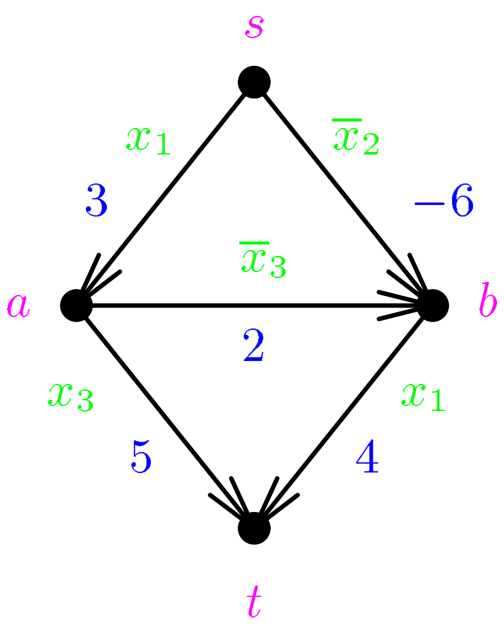
THM [BDHM92]

$\det(B(y)) =$ sum of weights of consistent paths

$\Longrightarrow f(y) = 1$ iff rows of $B(y)$ are independent

Stage II: Transform $B(x)$ to a dependency program computing $\overline{f}$

Example: Arithmetic Programs $\Longrightarrow$ Dependency Program



	s	a	b	t
s	-1	$3x_1$	$-6\overline{x}_2$	0
a	0	-1	$2\overline{x}_3$	$5x_3$
b	0	0	-1	$4x_1$
t	0	0	0	-1

Dependency Program $\Longrightarrow$ Arithmetic Programs

Labeled matrix $A(x)$ – each entry $a \cdot x_i$, $a \cdot \overline{x}_i$, or a

Lemma:

For every matrix $A(x)$ with s rows and every integer r $(0 \leq r \leq s)$
$\exists$ arithmetic prog. of size $\text{poly}(s)$ that accepts y iff $\text{rank}(A(y)) \geq r$

Proof uses [BGH82,Mul87,Ber84,MV97] and closure properties.

Dependency Program $\Longrightarrow$ Arithmetic Programs (cont.)

$$M \qquad \Longrightarrow \qquad N(x)$$

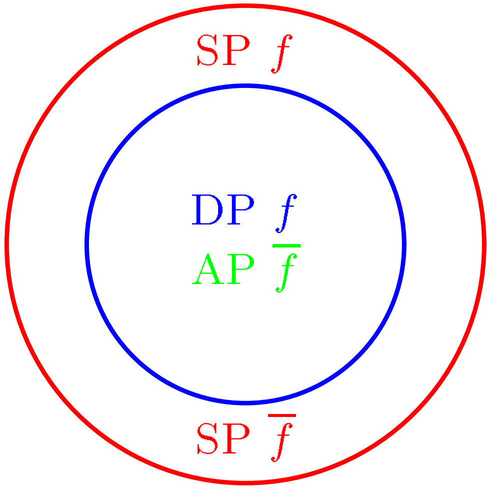
r $rows$ r $rows$

$$\begin{array}{c|ccc} x_1 & 1 & 2 & 4 \\ \overline{x}_1 & 0 & 0 & 1 \\ x_2 & 1 & 1 & 1 \\ x_2 & 1 & 3 & 7 \end{array} \quad \Longrightarrow \quad \begin{array}{ccc|cccc} 1 \cdot x_1 & 2 \cdot x_1 & 4 \cdot x_1 & \overline{x}_1 & 0 & 0 & 0 \\ 0 & 0 & 1 \cdot \overline{x}_1 & 0 & x_1 & 0 & 0 \\ 1 \cdot x_2 & 1 \cdot x_2 & 1 \cdot x_2 & 0 & 0 & \overline{x}_2 & 0 \\ 1 \cdot x_2 & 3 \cdot x_2 & 7 \cdot x_2 & 0 & 0 & 0 & \overline{x}_2 \end{array}$$

$f(y) = 0 \Longleftrightarrow M_y$ full rank $\Longleftrightarrow N(y)$ full rank $\Longleftrightarrow \mathrm{rank}(N(y)) \geq r$

Part IV: Conclusions and Open Problems

Conclusions



Over every field

$$\frac{1}{n} \cdot \mathrm{SP}_{\mathcal{K}}(f) \leq \mathrm{DP}_{\mathcal{K}}(f) \leq 2 \cdot \mathrm{AP}_{\mathcal{K}}\left(\overline{f}\right)$$

$$\mathrm{SP}_{\mathcal{K}}(f) = \mathrm{SP}_{\mathcal{K}}\left(\overline{f}\right)$$

$$\mathrm{AP}_{\mathcal{K}}(f) \leq \mathrm{poly}\left(\mathrm{DP}_{\mathcal{K}}\left(\overline{f}\right)\right)$$

Over infinite field

$$\mathrm{SP}_{\mathcal{K}}(f) \leq \mathrm{DP}_{\mathcal{K}}(f) \leq 2 \cdot \mathrm{AP}_{\mathcal{K}}\left(\overline{f}\right) \leq 2 \cdot \mathrm{NBP}\left(\overline{f}\right)$$

Open Problems

1. Closure of arithmetic programs under complement?
2. Simulating span programs by arithmetic programs?
3. Arithmetic program that accepts y iff $\mathrm{rank}(A(y)) = r$?

The Open Problems are Equivalent!!!

$(2) \Longrightarrow (1)$

Simulate arithmetic program for f by span program

construct span program for $\overline{f}$

simulate span program by arithmetic program

$(3) \Longrightarrow (2)$

A span program M accepts y iff $\mathrm{rank}\begin{pmatrix} M(y) \\ \vec{1} \end{pmatrix} = \mathrm{rank}(M(y))$

$(1) \Longrightarrow (3)$

$\mathrm{rank}(A(y)) = r$ iff $\mathrm{rank}(A(y)) \geq r$ and $\mathrm{rank}(A(y)) < r + 1$.