

NON-CLOSURE PROPERTIES OF READ-ONCE OBLIVIOUS ALGEBRAIC BRANCHING PROGRAMS

Andrews, Armand, Dwivedi, Hansen, Limaye, Srinivasan, Tavenas

Cambridge University, March 2026

Available at <https://doi.org/10.4230/LIPIcs.ITCS.2026.9>

MOTIVATION & BACKGROUND

SPARSE POLYNOMIALS

$$(x^d - 1) = (x - 1) \cdot (1 + x + \cdots + x^{d-1})$$

SPARSE POLYNOMIALS

Consider the following factorisation from univariate to multivariate:

$$\underbrace{\prod_{i=1}^n (x_i^d - 1)}_f = \underbrace{\prod_{i=1}^n (x_i - 1)}_h \cdot \underbrace{\prod_{i=1}^n (1 + x_i + \dots + x_i^{d-1})}_g$$

Count sparsity (number of monomials): f has 2^n monomials, while g has d^n monomials.

Sparse polynomials are not closed under factoring.

Question: Where else is the set of polynomials not closed under factoring? How to study polynomials? \Rightarrow Computational models.

SPARSE POLYNOMIALS

Consider the following factorisation from univariate to multivariate:

$$\underbrace{\prod_{i=1}^n (x_i^d - 1)}_f = \underbrace{\prod_{i=1}^n (x_i - 1)}_h \cdot \underbrace{\prod_{i=1}^n (1 + x_i + \dots + x_i^{d-1})}_g$$

Count sparsity (number of monomials): f has 2^n monomials, while g has d^n monomials.

Sparse polynomials are not closed under factoring.

Question: Where else is the set of polynomials not closed under factoring? How to study polynomials? \Rightarrow Computational models.

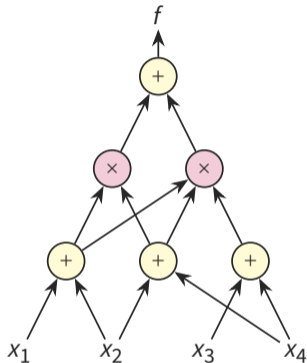
ALGEBRAIC CIRCUITS

An algebraic circuit computes polynomials in a very natural way (using $+$ and \times gates).

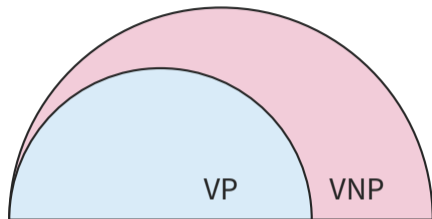
$\text{size}(f)$ = size of smallest circuit computing f .

Introduced by Valiant (1977). It defines algebraic complexity classes:

- VP: Polynomials with both degree and size bounded by $\text{poly}(n)$.
- VNP: Class containing VP. Also called **Explicit** polynomials.



ALGEBRAIC CIRCUIT CLASSES



$$\text{Det}(X) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{i=1}^n x_{i, \sigma(i)}$$

$$\text{Perm}(X) = \sum_{\sigma \in S_n} \prod_{i=1}^n x_{i, \sigma(i)}$$

Det has a $\text{poly}(n)$ -size circuit.

Valiant's conjecture: Perm is not in VP.

COMPLEXITY OF MULTIVARIATE FACTORING

The polynomial ring $\mathbb{F}[x_1, \dots, x_n]$ is a unique factorisation domain.

$$f = \prod_{i=1}^m f_i^{e_i},$$

where f_i are irreducible.

Suppose f is in some algebraic complexity class \mathcal{C} . Are the factors $f_i \in \mathcal{C}$?

If all factors f_i are in \mathcal{C} , we say that \mathcal{C} is closed under factoring.

Theorem (Kaltofen [Kal85])

VP is closed under factoring over large characteristic fields.

There is a randomized poly (size(f), deg(f))-time algorithm to compute all the irreducibles.

CLOSURE PROPERTIES OF ALGEBRAIC CIRCUITS

It is natural to ask if a computational model is robust under fundamental operations.

- Boolean circuits are studied under union and intersection.
- In the algebraic world, we can consider addition, multiplication, and crucially, **factoring**.

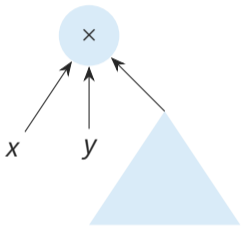
Closure under addition and multiplication is trivial, and Kaltofen classically proved closure of VP under factoring. This robust behavior extends even to larger classes:

Theorem ([BDS24; CKS19])

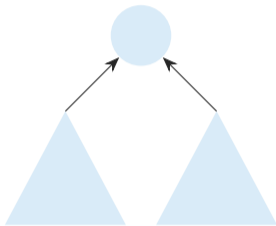
VNP is closed under factoring even over finite fields.

Are there classes within VP that are not closed under factoring?

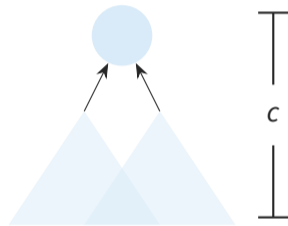
KNOWN CLOSURE RESULTS



VBP
poly-size skew circuits

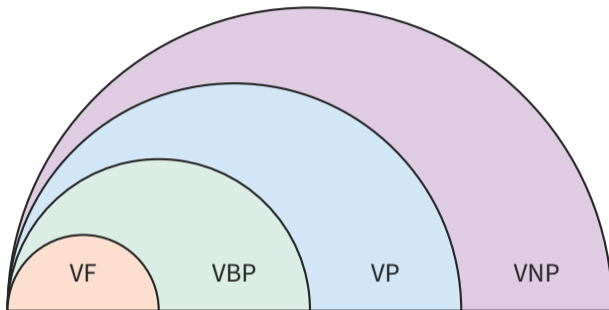


VF
poly-size formulas



Constant Depth
circuits

KNOWN CLOSURE RESULTS



[ST21] proved that VBP is closed under factoring.

[Bha+25a] proved the closure for VF and constant depth circuits.

Breakthrough: [Bha+25a] gave a unified framework to prove all the known closure results.

READ-ONCE OBLIVIOUS ABP (ROABP)

THE COMPUTATIONAL MODEL

A restricted algebraic branching program (ABP) which was alluded to earlier as skew circuits.

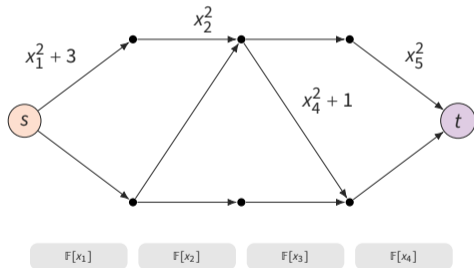
Fix a permutation $\pi : [n] \rightarrow [n]$. Model will read the variables in the order $\pi(1), \pi(2), \dots, \pi(n)$, and each variable is read at most once.

The polynomial computed by an ROABP is of the form:

$$f = \sum_{\text{path } \gamma: s \rightsquigarrow t} \text{wt}(\gamma).$$

$\text{wt}(\gamma)$ is a product of univariate polynomials on the path γ .

Subsumes many models such as sparse, set-multilinear, diagonal depth 3.



WIDTH DEPENDS ON VARIABLE ORDER

Consider the following $2n$ -variate polynomial:

$$f(\mathbf{x}, \mathbf{y}) := \prod_{i=1}^n (x_i + y_i)$$

The "Good" Order

$$(x_1, y_1, x_2, y_2, \dots, x_n, y_n)$$

Width: 2.

The "Bad" Order

$$(x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_n)$$

Width: 2^n .

FACTOR NON-CLOSURE OF ROABP

LIFTING SPARSITY HARDNESS TO ROABP

$$\underbrace{\prod_{i=1}^n (x_i^d - 1)}_f = \underbrace{\prod_{i=1}^n (x_i - 1)}_h \cdot \underbrace{\prod_{i=1}^n (1 + x_i + \dots + x_i^{d-1})}_g$$

Goal: Lift sparsity hardness to ROABP. (Both f and g are easy for ROABP).

LIFTING SPARSITY HARDNESS TO ROABP

Let $G = (V, E)$ be a graph. Define:

$$\underbrace{\prod_{(i,j) \in E} \left((x_i x_j)^d - 1 \right)}_{f_G} = \underbrace{\prod_{(i,j) \in E} (x_i x_j - 1)}_{h_G} \cdot \underbrace{\prod_{(i,j) \in E} \left(1 + x_i x_j + \dots + (x_i x_j)^{d-1} \right)}_{g_G}$$

Graph properties:

- Constant degree graph \implies monomials in $f_G = 2^{|E|} = 2^{O(n)} =: w$.
- **Induced matching**: Any large enough vertex partition S, T has an induced matching M of size $\Omega(n)$.

The first property keeps f_G easy for ROABP. The second property makes g_G hard for ROABP in every variable order.

MAIN THEOREMS

Theorem (Factor non-closure)

There is a $f := g \cdot h$ such that f is computable by an ROABP of width $w := 2^{O(n)}$ such that its factor g requires ROABP of width $w^{\Omega(\log d)}$ in every variable order.

Theorem (Powering non-closure)

There is a quadratic polynomial f computable by $O(n)$ width ROABP such that for any d , f^d requires ROABP of width **at least**

$$\binom{d + n/2}{n/2}$$

in every variable order.

ROABP COMPLEXITY OF SYMMETRIC COMPOSITION

FUNDAMENTAL THEOREM OF SYMMETRIC POLYNOMIALS

The degree- d elementary symmetric polynomial in n variables is defined as:

$$e_d(x_1, \dots, x_n) \quad := \quad \sum_{1 \leq i_1 < \dots < i_d \leq n} x_{i_1} \dots x_{i_d}$$

The Fundamental Theorem

For any symmetric polynomial $f_{\text{sym}}(x_1, \dots, x_n)$ there is a unique polynomial f such that:

$$f_{\text{sym}}(x_1, \dots, x_n) \quad = \quad f(e_1, \dots, e_n)$$

How does $\text{size}(f)$ relate to $\text{size}(f_{\text{sym}})$?

[BJ19] showed they are polynomially related for circuits. [Bha+25b] proved the same for formulas and constant depth circuits.

MAIN THEOREMS

Theorem (f_{sym} is easy, f is hard)

There exists f such that $f_{sym} = f(e_1, \dots, e_n)$ has constant-width ROABP, but f requires width $2^{\Omega(n)}$.

Candidate: $f_{sym} = \sum_{i=0}^n e_i(x_1^k, \dots, x_n^k)$ for prime $k \in [n/2, n]$.

f_{sym} has a constant width ROABP, while f is the **Circulant Polynomial**.

Theorem (f is easy, f_{sym} is hard)

There exists f with constant-width ROABP such that f_{sym} requires width $2^{\Omega(n)}$.

Candidate: $f(x_1, \dots, x_n) = x_k^k$ where $k = \lfloor n/2 \rfloor$.

OPEN PROBLEMS

ROABP is **not closed** under **factoring, powering, or symmetric composition**. Where else is it not closed?

Exponential Factor Separation: Is there a polynomial which is easy for ROABP but has a factor that is exponentially harder for ROABP?

Universality of Hardness Lifting: Given a polynomial f with sparsity s , can we always find a gadget ϕ such that $f(\phi \circ \mathbf{x})$ requires ROABP size $\Omega(s)$ in every order?

Hard Roots of Easy Powers: Is there a polynomial $f = g^d$ that is easy for ROABP, but whose root g is hard?

REFERENCES [1]

- [BDS24] C. S. Bhargav, Prateek Dwivedi, and Nitin Saxena. “Learning the Coefficients: A Presentable Version of Border Complexity and Applications to Circuit Factoring”. In: *Proceedings of the 56th Annual ACM Symposium on Theory of Computing, STOC 2024, Vancouver, BC, Canada, June 24-28, 2024*. ACM, 2024, pp. 130–140 (cited on page 9).
- [Bha+25a] Somnath Bhattacharjee, Mrinal Kumar, Shanthanu S. Rai, Varun Ramanathan, Ramprasad Saptharishi, and Shubhangi Saraf. “Closure under factorization from a result of Furstenberg”. In: *CoRR abs/2506.23214* (2025). arXiv: 2506.23214 (cited on page 11).

REFERENCES [2]

- [Bha+25b] Somnath Bhattacharjee, Mrinal Kumar, Shanthanu S. Rai, Varun Ramanathan, Ramprasad Saptharishi, and Shubhangi Saraf. “Constant-depth circuits for polynomial GCD over any characteristic”. In: *CoRR* abs/2506.23220 (2025). arXiv: 2506.23220 (cited on page 20).
- [BJ19] Markus Bläser and Gorav Jindal. “On the Complexity of Symmetric Polynomials”. In: *10th Innovations in Theoretical Computer Science Conference (ITCS 2019)*. Vol. 124. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2019, 47:1–47:14 (cited on page 20).
- [CKS19] Chi-Ning Chou, Mrinal Kumar, and Noam Solomon. “Closure Results for Polynomial Factorization”. In: *Theory Comput.* 15 (2019), Paper No. 13, 34 (cited on page 9).

REFERENCES [3]

- [Kal85] Erich Kaltofen. “Polynomial-Time Reductions from Multivariate to Bi- and Univariate Integral Polynomial Factorization”. In: *SIAM J. Comput.* 14.2 (1985), pp. 469–489 (cited on page 8).
- [ST21] Amit Sinhababu and Thomas Thierauf. “Factorization of Polynomials given by Arithmetic Branching Programs”. In: *Comput. Complexity* 30.2 (2021), Paper No. 15, 47 (cited on page 11).