Formal Series and Non-Commutative Computations

Algebraic Methods, Simons Institute

Guillaume Malod

December 6, 2018

Outline

Some results in the non-commutative setting

For ABPs (Algebraic Branching Programs) :

- (Nisan 1991) Exact characterization of complexity and lower bounds
- (Limaye,M.,Srinivasan 2016) Exponential lower bounds for *skew* circuits
- (Lagarde, M., Perifel 2016) Generalization of Nisan's characterization

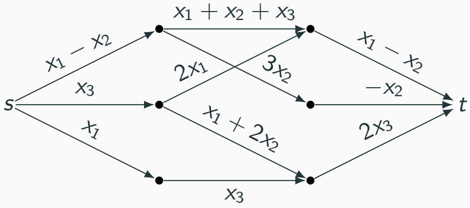
Some results in the non-commutative setting

For ABPs (Algebraic Branching Programs) :

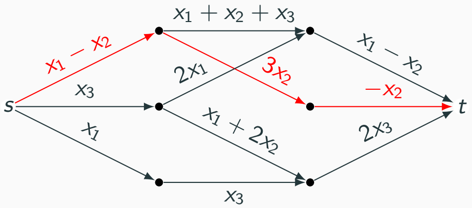
- (Nisan 1991) Exact characterization of complexity and lower bounds
- (Limaye,M.,Srinivasan 2016) Exponential lower bounds for *skew* circuits
- (Lagarde, M., Perifel 2016) Generalization of Nisan's characterization
- (Fijalkow, Lagarde, Ohlmann, Serre 2018) Show how to get those extensions from known results on formal series...

Outline

ABP (Branching programs)



ABP (Branching programs)

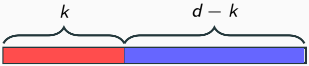


$(x_1 - x_2)(3x_2)(-x_2)$

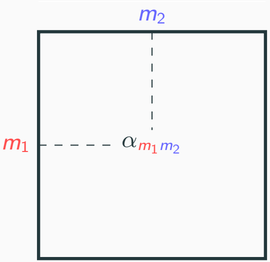
- **DAG** : source s, sink t, edges with linear forms
- **Weight of a path** : product of edge weights
- **Computed polynomial** : sum of path weights from s to t.
- **Layered**

Measure: coefficient matrices

- $\Pi = (\{1, 2, \ldots, k\}, \{k+1, k+2, \ldots, d\})$



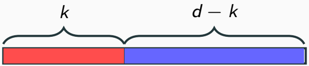
- $f = \sum_m \alpha_m . m$, homogeneous, degree d, n variables
- Define matrix $M^\Pi(f)$



- Complexity measure : $\text{rank}(M^\Pi(f))$.

Nisan's beautiful result

- $\Pi = (\{1, 2, \ldots, k\}, \{k+1, k+2, \ldots, d\})$



Theorem (Nisan, 1991)

For any homogeneous polynomial f of degree d, the size of a smallest homogeneous algebraic branching program for f is equal to

$$\sum_{k=0}^{d} \mathrm{rank}(M_k(f))$$

Corollary

Any homogeneous ABP computing the permanent has size $\geq 2^n$

Outline

Basic definitions (Berstel & Reutenauer)

- Fix a field K and a finite alphabet A
- A formal series S is a function $A^* \to K$
- Denote by (S, w) the image of w by S
- $S = \sum_{w \in A^*} (S, w) w$
- Set of formal series: $K\langle\langle A \rangle\rangle$
- Support of S: $\{w \in A^* \mid (S, w) \neq 0\}$
- Finite support: polynomials, $K\langle A \rangle$

Recognizable series

Definition

A formal series S is recognizable if there exists:

- an integer $n \geq 1$
- a morphism of monoids $\mu : A^* \to K^{n\times n}$
- two matrices $\lambda \in K^{1\times n}$ and $\gamma \in K^{n\times 1}$

such that, for all words w, $(S, w) = \lambda\mu(w)\gamma$.

- It is enough to define $\mu(a)$ for all $a \in A$
- (λ, μ, γ) is called a linear representation
- n is called the dimension
- It is an automaton

- $K\langle\langle A\rangle\rangle$ is a vector space over K
- If $u \in A^*$ and $S \in K\langle\langle A\rangle\rangle$, $u^{-1}S = \sum_{w\in A^*}(S, uw)w$ or $(u^{-1}S, w) = (S, uw)$
- $M \subseteq K\langle\langle A\rangle\rangle$ is called *stable* if $\forall u \in A^*, \forall S \in M,\ u^{-1}S \in M$

Theorem (Fliess, Carlyle & Paz)

A formal series S is recognizable iff there exists a linear subspace of $K\langle\langle A\rangle\rangle$ which:

- *contains S*
- *is stable*
- *has finite dimension*

Proof of $\Rightarrow$

- Suppose (λ, μ, γ) is a linear representation of S
- Define S_i by: $(S_i, w) = (\mu(w)\gamma)_i$, for $i = 1, \ldots, n$
- Let M be the subspace generated by the S_i (finite dimension)
- It contains S:

$$(S, w) = \lambda\mu(w)\gamma = \sum_i \lambda_i(\mu(w)\gamma)_i = \sum_i \lambda_i(S_i, w)$$

- It is stable:

$$(x^{-1}S_i, w) = (S_i, xw) = (\mu(xw)\gamma)_i = (\mu(x)\mu(w)\gamma)_i$$
$$= \sum_j (\mu(x))_{i,j}(\mu(w)\gamma)_j = \sum_j (\mu(x))_{i,j}(S_j, w)$$

Proof of $\Leftarrow$

- Let M be a stable linear subspace, containing S, generated by $S_1, \ldots, S_n$
- $S = \sum_i \lambda_i S_i$
- for $a \in A$, $i \in [n]$:

$$a^{-1} S_i = \sum_j \alpha_j S_j = \sum_j (\mu(a))_{i,j} S_j$$

- $\gamma_j = (S_j, 1)$
- Then:

$$(S_i, w) = (w^{-1} S_i, 1) = \left(\sum_j (\mu(w))_{i,j} S_j, 1 \right) = \sum_j (\mu(w))_{i,j} (S_j, 1)$$
$$= \sum_j (\mu(w))_{i,j} \gamma_j = (\mu(w)\gamma)_i$$

- Finally:

$$(S, w) = \sum_i \lambda_i (S_i, w) = (\lambda \mu(w) \gamma)$$

- Representation of dimension $n \to$ linear subspace of dimension $\leq n$
- Linear subspace of dimension $n \to$ representation of dimension n
- Hadamard products (Lemma by Arvind, Joglekar and Srinivasan)

Definition

The hadamard product of two formal series S and T is
$(S \odot T, w) = (S, w)(T, w)$

Theorem (Schützenberger 1962)

If S and T are recognizable, then $S \odot T$ also

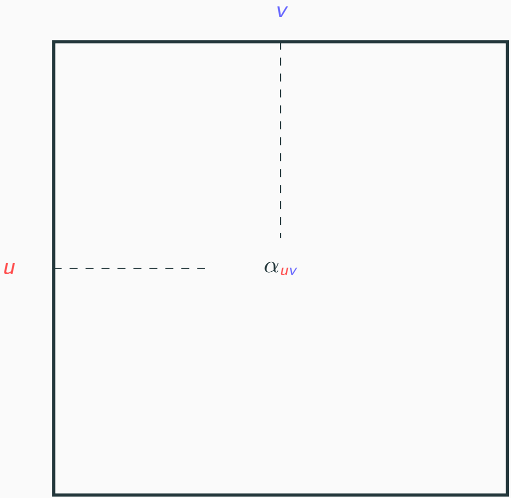
Proof.

If $S_1, \ldots, S_m$ generate a stable subspace containing S and respectively $T_1, \ldots, T_n$ for T, then the $S_i \odot T_j$ generate a stable subspace for $S \odot T$ □

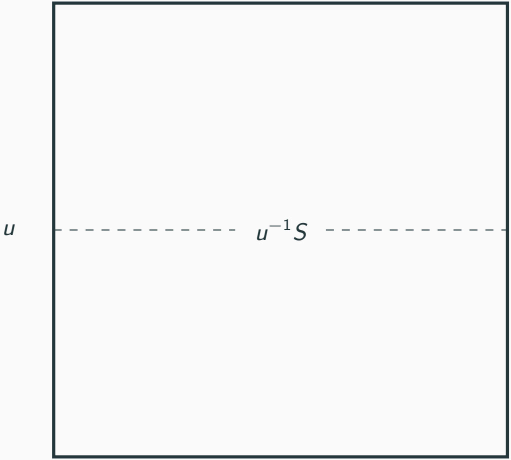
Hankel matrix

- Consider the smallest stable linear subspace containing S
- It is generated by the $u^{-1}S$ for $u \in A^*$
- S is recognizable iff this has finite dimension
- This dimension is the smallest dimension of a linear representation of S
- (The size of a smallest automaton)
- This is the rank of the Hankel matrix

Hankel matrix



Hankel matrix



Back to ABPs

- Automata can be seen as a computational model
- For this model we have an exact characterization of the complexity
- May be different from ABPs (cycles)
- (Fijalkow, Lagarde, Ohlmann, Serre 2018) If the polynomial S is homogeneous of degree d, the minimal automaton is an ABP (acyclic)

Back to ABPs

- Suppose $S_1, \dots, S_n$ is a basis of a stable subspace containing S
- The transition matrix μ is given by:

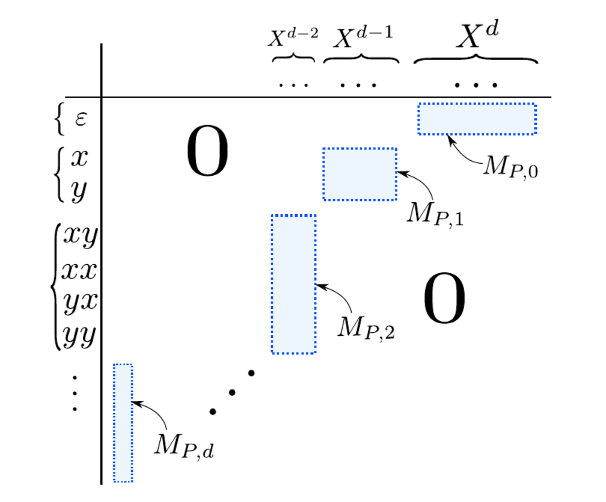
$$a^{-1}S_i = \sum_j (\mu(a))_{i,j} S_j$$

- Here we have a basis $u_1^{-1}S, \dots, u_n^{-1}S$ of the minimal stable subspace containing S
- Each $u_i^{-1}S$ is a homogeneous polynomial of degree $d - |u_i|$
- Now:

$$a^{-1}(u_i^{-1}S) = \sum_j (\mu(a))_{i,j} u_j^{-1}S$$

- $d - (|u - i| + 1) = d - |u_j|$ implies $|u_j| = |u_i| + 1$
- The "states" can be layered by length of words, transition can only go from one layer to the next
- $\rightarrow$ Nisan's homogeneous ABPs

Hankel matrix



What about non-homogenous polynomials?

- For an homogeneous polynomial, all minimal automata obtained from the Hankel matrix are ABPs

What about non-homogenous polynomials?

- For an homogeneous polynomial, all minimal automata obtained from the Hankel matrix are ABPs
- Challenge 1: find the smallest ABP for $a + ab + bb$

What about non-homogenous polynomials?

- For an homogeneous polynomial, all minimal automata obtained from the Hankel matrix are ABPs
- Challenge 1: find the smallest ABP for $a + ab + bb$
- Challenge 2: find a smallest automaton *with cycles*

What about non-homogenous polynomials?

- For an homogeneous polynomial, all minimal automata obtained from the Hankel matrix are ABPs
- Challenge 1: find the smallest ABP for $a + ab + bb$
- Challenge 2: find a smallest automaton *with cycles*
- There exists a minimal automaton defined from the Hankel matrix which is acyclic.
- Slight generalization of Nisan's result: in general, the ABP-complexity of a polynomial is the rank of the Hankel matrix

Outline

Basic definitions (Berstel & Reutenauer)

- Fix a field K and a finite ranked alphabet Σ (symbols with arities: $\Sigma = \cup \Sigma_k$)
- We consider trees over Σ, T_Σ (the free magma over Σ)
- A formal series S is a function $T_\Sigma \to K$
- Denote by (S, t) the image of t by S
- $S = \sum_{t \in T_\Sigma} (S, t) t$
- Set of formal series: $K\{\{A\}\}$
- Support of S: $\{t \in T_\Sigma \mid (S, t) \neq 0\}$
- Finite support: polynomials, $K\{A\}$

Definition

A formal tree series S is recognizable if there exists:

- an integer $n \geq 1$
- for each $a \in \Sigma_0$, a vector $\mu(a) \in K^n$
- for each $f \in \Sigma_k$, a k-linear map $\mu(f) : (K^n)^k \to K^n$
- a vector $\lambda \in K^n$

such that, for any tree t, $(S, t) = \lambda\mu(t)$, where μ is extended to a mapping from T_Σ to K^n: $\mu(f(t_1, \ldots, t_k)) = \mu(f)(\mu(t_1), \ldots, \mu(t_k))$

- (λ, μ) is called a linear representation
- n is called the dimension
- It is a weighted tree automaton

Characterizing recognizable tree series

- $K\{\{A\}\}$ is a vector space over K
- A context is a tree with one leaf labelled $\square$
- If c is a context and $S \in K\{\{A\}\}$, $c^{-1}S = \sum_{t \in T_\Sigma}(S, c[t])t$ or $(c^{-1}S, t) = (S, c[t])$
- $M \subseteq K\{\{A\}\}$ is called *stable* if, for all context c and for all $S \in M$, $c^{-1}S \in M$

Theorem

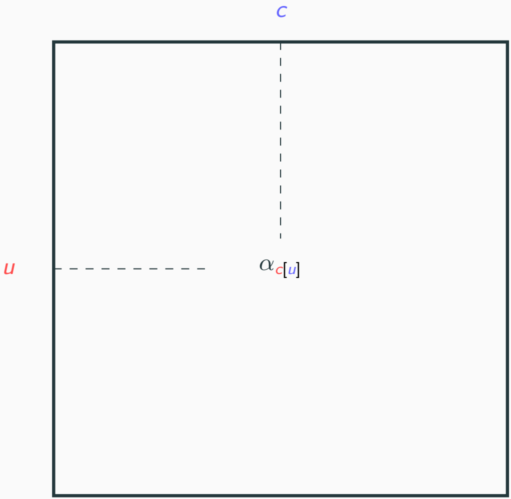
A formal tree series S is recognizable iff there exists a linear subspace of $K\{\{A\}\}$ which:

- *contains S*
- *is stable*
- *has finite dimension*

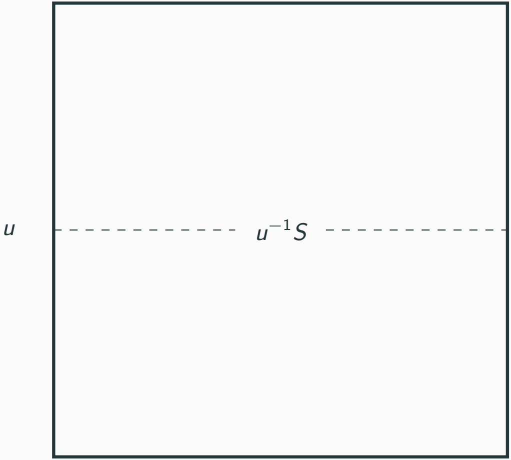
Hankel matrices

- OK for $\Rightarrow$
- I don't have a direct proof of $\Leftarrow$ ☹
- Suppose there is a stable linear subspace of finite dimension containing S
- The smallest such subspace V (generated by the $c^{-1}S$) also has finite dimension
- Consider the space U generated by the $t^{-1}S$, where t is a *tree* (in the space of formal *context* series)
- It is a linear subspace of formal context series over A
- U and V have the same dimension (Hankel matrix)
- From the fact that U has finite dimension, define a representation of S
- Size of the smallest automaton is the rank of the Hankel matrix (Bozapalidis & Louscou-Bozapalidou)

Hankel matrix



Hankel matrix



Back to circuits

- Σ_0 is the set of variables, there is only one other symbol, of arity 2
- Binary tree over the variables $\rightarrow$ non-commutative non-associative monomial
- non-commutative, non-associative series and polynomials
- Automata can be seen as a (non-commutative, non-associative) computational model
- For this model we have an exact characterization of the complexity
- May be different from circuits (cycles)
- (Fijalkow, Lagarde, Ohlmann, Serre 2018) If the polynomial S is homogeneous of degree d, all minimal automata are acyclic (circuit)
- (M) In general, there is always a minimal automaton which is acyclic

Non-commutative Hadamard product of an ABP and a circuit

- Formal tree series: if S and T have small linear representations, so does $S \odot T$
- (Arvind & Srinivasan 2009) If f has a small circuit and g has a small ABP, then $f \odot g$ has a small circuit (non-commutative, but associative setting)
- Follows from simple observation: there is a small circuit computing all the monomials of g with all possible associative structures: $\tilde{g}$
- Then $f \odot \tilde{g}$ as a non-associative polynomial projects down to $f \odot g$

Conclusion

- Exact characterization of circuit complexity for non-associative, non-commutative polynomials
- Showing lower bounds in the associative setting means considering all the possible Hankel matrices which can define a given associative polynomial
- We can express this as linear constraints on the coefficients of the matrix

Conclusion

- Exact characterization of circuit complexity for non-associative, non-commutative polynomials
- Showing lower bounds in the associative setting means considering all the possible Hankel matrices which can define a given associative polynomial
- We can express this as linear constraints on the coefficients of the matrix
- Exact characterization of circuit complexity for non-associative polynomials