On the intrinsic complexity of elimination problems in effective algebraic geometry

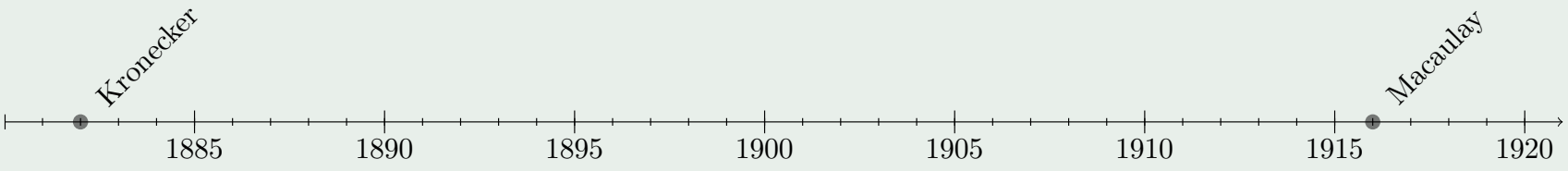
Joos Heintz

Universidad de Cantabria
Universidad de Buenos Aires

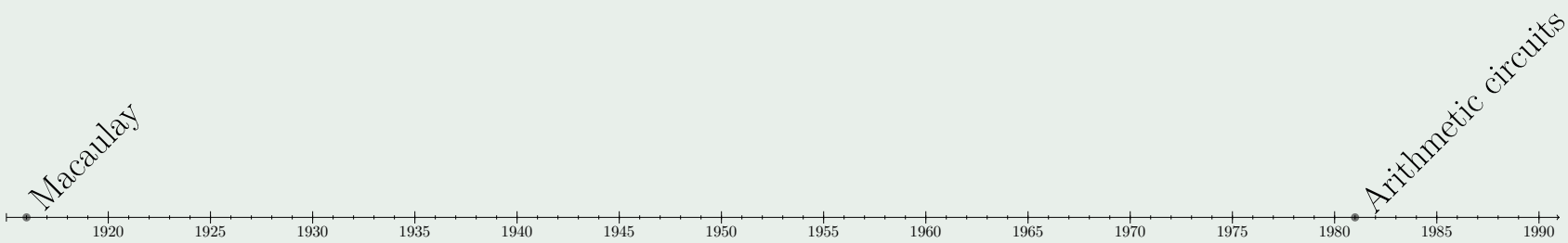
Joint work with
Bart Kuijpers (Hasselt University)
Andrés Rojas Paredes (Universidad de Buenos Aires)

Escuela Lluis Santaló, RSME and UIMP,
July 16–20, 2012, Santander, España

Previous results

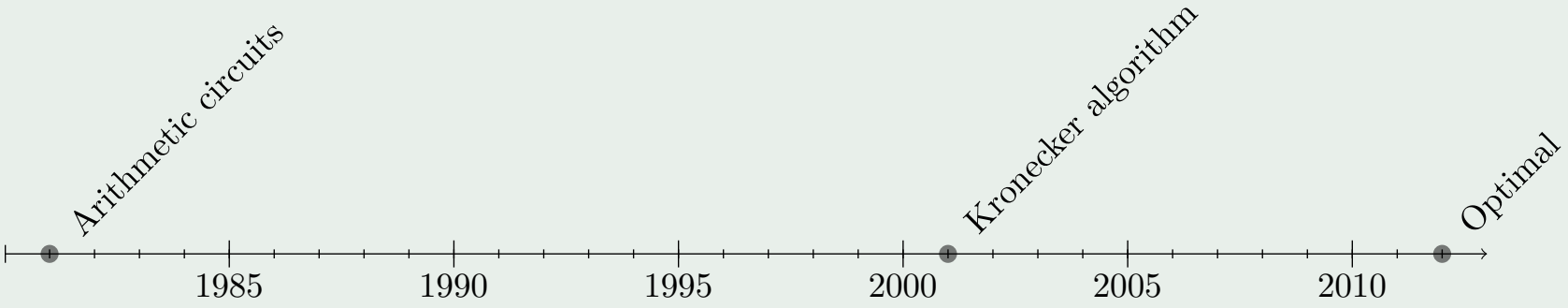


1. Modern elimination theory starts with Kronecker's 1882 paper *Grundzüge einer arithmetischen Theorie der algebraischen Grössen* (Fundamentals of an arithmetic theory of algebraic quantities).



2. Macaulay (1916) and van der Waerden (1950) criticize the algorithmic inefficiency of the Kronecker elimination method.

3. In elimination algorithms, polynomials become represented by circuits (and not by coefficients). H.–Sieveking 1981, H.–Schnorr 1982, Kaltofen 1988.



4. The circuit representation of polynomials becomes fully realized by the *Kronecker algorithm* for the resolution of polynomial equation systems over algebraically closed fields. Giusti–Pardo et al. 1997, 1998, H.–Matera et al. 2001, Giusti–Lecerf et al. 2001, Implementation by G. Lecerf.

5. The results presented here imply that the complexity of the *Kronecker algorithm* is asymptotically optimal under reasonable assumptions about its architecture.

Basic notions from algebraic geometry

$V \subset \mathbb{C}^n$, $W \subset \mathbb{C}^m$ closed affine varieties,
$\phi : V \dashrightarrow W$ partial map $\phi = (\phi_1, \ldots, \phi_m)$,
$\mathbb{C}[V]$ polynomial functions defined on V,
$\mathbb{C}(V)$ quotients of polynomial (i.e. *rational*) functions with dense domain.

ϕ *morphism* of affine varieties, if $\phi_1, \ldots, \phi_m \in \mathbb{C}[V]$.
A morphism is a *total* map.

ϕ *rational* map if the domain U of ϕ is Zariski open and dense in V and $\phi_1, \ldots, \phi_m$ are restrictions to U of rational functions of V.

Let $\mathcal{M} \subset \mathbb{C}^n$ and $\phi : \mathcal{M} \dashrightarrow \mathbb{C}^m$ partial map.

$\mathcal{M}$ *constructible* if $\mathcal{M}$ is definable by a Boolean combination of polynomial equations.

ϕ *constructible* if graph $\phi \subset \mathbb{C}^n \times \mathbb{C}^m$ constructible.

Remark 1.

$\phi : \mathcal{M} \dashrightarrow \mathbb{C}^m$ *constructible* $\Leftrightarrow$ ϕ *is piecewise rational.*

ϕ *constructible*
$\Rightarrow$ *there exists a Zariski open and dense subset* U *of* $\mathcal{M}$
such that $\phi|_U$ *is a rational map of* $\mathcal{M}$.

Geometrically robust constructible maps

Let $\mathcal{M} \subset \mathbb{C}^n$ constructible and $\phi : \mathcal{M} \to \mathbb{C}^m$ a (total) constructible map with components $\phi_1, \ldots, \phi_m$.

Consider $x \in \overline{\mathcal{M}}$, $\mathfrak{M}_x$ maximal ideal of coordinate functions of $\mathbb{C}[\overline{\mathcal{M}}]$ vanishing at x.

$\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}$ the local $\mathbb{C}$–algebra of $\overline{\mathcal{M}}$ at x, i.e., the localization of $\mathbb{C}[\overline{\mathcal{M}}]$ at the maximal ideal $\mathfrak{M}_x$.

The following result establishes a bridge between a topological and an algebraic notion:

Theorem–Definition 2.

(based on Zariski's Main Theorem)

$\phi : \mathcal{M} \to \mathbb{C}^m$ *geometrically robust*
if ϕ *is continuous with respect to the Euclidean topologies of* $\mathcal{M}$ *and* $\mathbb{C}^m$
or equivalently, if $\phi_1, \ldots, \phi_m$, *interpreted as rational functions of the affine variety* $\overline{\mathcal{M}}$,
satisfy at any point $x \in \mathcal{M}$ *the following two conditions:*

(i) $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}[\phi_1, \ldots, \phi_m]$ *is a finite* $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}$*–module.*

(ii) $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}[\phi_1, \ldots, \phi_m]$ *is a local* $\mathbb{C}[\overline{\mathcal{M}}]_{\mathfrak{M}_x}$*–algebra whose maximal ideal is generated by* $\mathfrak{M}_x$ *and* $\phi_1 - \phi_1(x), \ldots, \phi_m - \phi_m(x)$.

Corollary 3.

If we restrict a geometrically robust constructible map to a constructible subset of its domain $\mathcal{M}$ of definition, we obtain again a geometrically robust map.

The composition and the cartesian product of two geometrically robust constructible maps are geometrically robust.

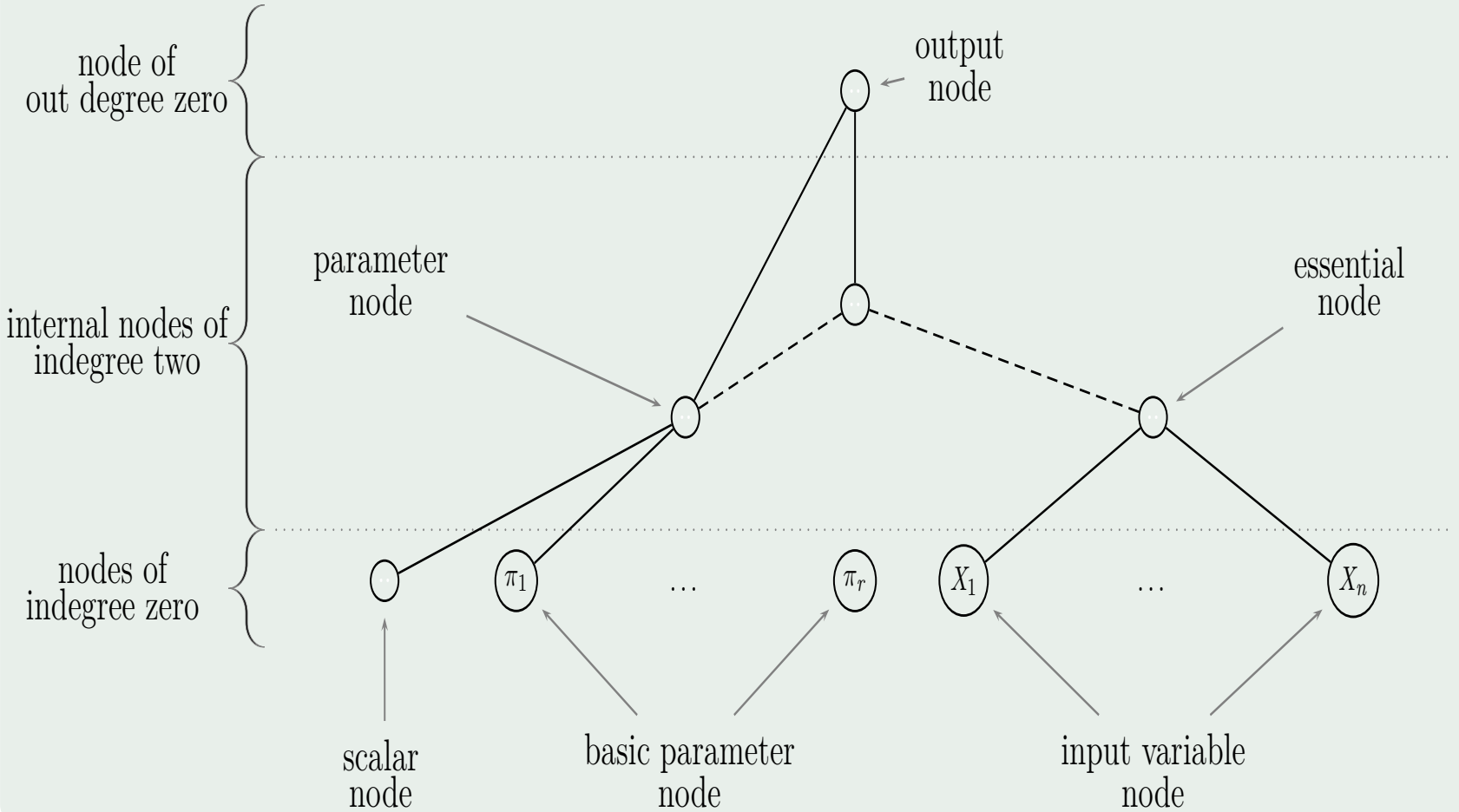
The geometrically robust constructible functions form a commutative $\mathbb{C}$–algebra which contains the polynomial functions defined on $\mathcal{M}$.

Parameterized arithmetic circuit

$n, r \in \mathbb{N}$, $X_1, \ldots, X_n$ indeterminates,
$\mathcal{M} \subset \mathbb{C}^r$ constructible,
$\pi_1, \ldots, \pi_r : \mathcal{M} \to \mathbb{C}$ canonical projections.

A *(by $\mathcal{M}$) parameterized arithmetic circuit* β
(with *basic parameters* $\pi_1, \ldots, \pi_r$ and *inputs* $X_1, \ldots, X_n$)
is a labelled directed acyclic graph (labelled DAG):

Parameterized arithmetic circuit



Intermediate results

We consider β as a syntactical object which we wish to equip with a certain semantics.

A canonical evaluation procedure of β assigns to each node a rational function of $\mathcal{M} \times \mathbb{C}^n$ (if this works β is called *consistent*).

In case of a parameter node, the evaluation procedure assigns a rational function of $\mathcal{M}$.

In either situation we call such a rational function an *intermediate result* of β.

Final results, parameters and essential parameters

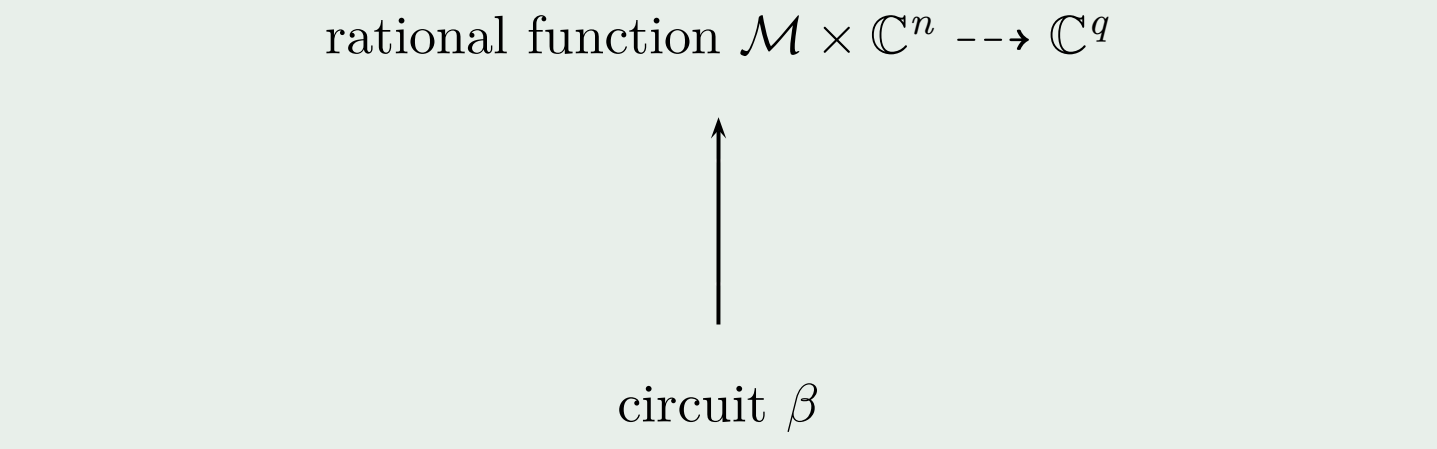
Intermediate results associated with output nodes will be called *final results* of β.

Intermediate results associated with parameter nodes will be called *parameters* of β and will be interpreted as rational functions of $\mathcal{M}$.

A parameter associated with a node which has an outgoing edge into a node which depends on some input of β is called *essential*.

q is the number of output nodes of β.

β is a syntactical object which represents the final results, i.e., the rational functions of $\mathcal{M} \times \mathbb{C}^n$ assigned to its output nodes:



Robust circuit

Suppose β is consistent, has K nodes and
there is a total constructible map $\Omega : \mathcal{M} \times \mathbb{C}^n \to \mathbb{C}^K$
extending the rational map $\mathcal{M} \times \mathbb{C}^n \dashrightarrow \mathbb{C}^K$
given by the intermediate results of β.

The pair (β, Ω) is called a *robust* parameterized arithmetic circuit if Ω is geometrically robust.

Such a geometrically robust constructible map Ω is uniquely determined by β. If it exists we call β *robust*.

Totally/essentially division–free

The parameterized arithmetic circuit β is *totally division–free* if any division node of β corresponds to a division by a non–zero complex scalar.

β is *essentially division–free* if only parameter nodes are labelled by divisions.

Complexity measure

Our basic complexity measure is the *non–scalar* one over the ground field $\mathbb{C}$.

This means that we count, at unit costs, only essential multiplications and divisions ($\mathbb{C}$–linear operations are free).

Lemma 4.

If β is robust, then all intermediate results of β are polynomials in $X_1, \ldots, X_n$ over the $\mathbb{C}$–algebra of geometrically robust constructible functions defined on $\mathcal{M}$.

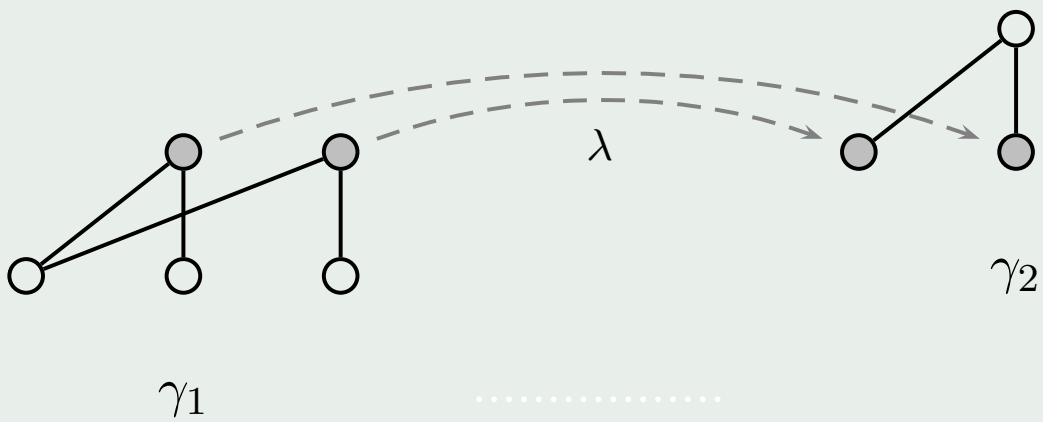
In other words,
the intermediate results of β are polynomials in $X_1, \ldots, X_n$
(we do not restrict the type of arithmetic operations contained in β!).

Operations with robust parameterized arithmetic circuits

Join

γ_1 and γ_2 two robust parameterized arithmetic circuits with parameter domain $\mathcal{M}$,
λ : outputs $\gamma_1 \rightarrow$ inputs γ_2, identification of nodes.

Connect γ_1 with γ_2 by λ.



Join

The (consistent) circuit $\gamma_2 *_\lambda \gamma_1$ is called the (consistent) *join* of γ_1 with γ_2.

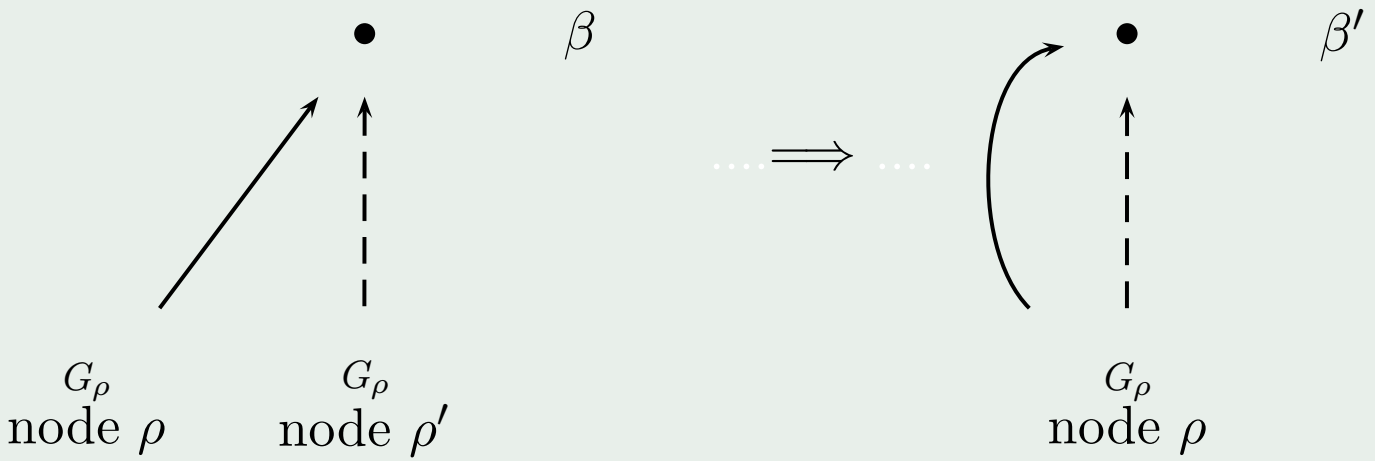
Consistent joins:

- are robust
- represent a composition of the rational maps defined by γ_1 and γ_2

Reduction

Rewrite a given parameterized arithmetic circuit β as a new circuit which computes the same final results.

β computes at two different nodes ρ and ρ', the same intermediate result G_ρ, ρ does not depend on ρ'.



Reduction

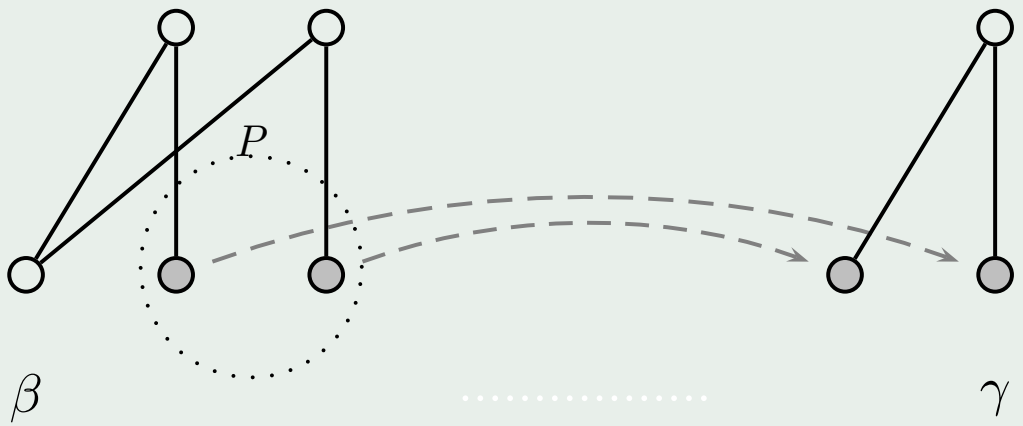
By erasing the node ρ', we obtain the parameterized arithmetic circuit β'

We call β' a *reduction* of β.

The way we obtained β' from β is a *reduction step*. A *reduction procedure* is a sequence of successive reduction steps.

Broadcasting

β and γ two robust parameterized arithmetic circuits,
P set of nodes of β
replace each input of γ by the corresponding node in P



Broadcasting and reducing a robust parameterized arithmetic circuit means rewriting it using only valid polynomial identities.

A family of hard elimination polynomials

$T, U_1, \ldots, U_n$ and $X_1, \ldots, X_n$ indeterminates
$U := (U_1, \ldots, U_n)$, $X := (X_1, \ldots, X_n)$.

For given $n \in \mathbb{N}$
$H^{(n)} := \sum_{1 \leq i \leq n} 2^{i-1} X_i + T \prod_{1 \leq i \leq n} (1 + (U_i - 1)X_i)$.

$H^{(n)}$ can be evaluated using $O(n)$ arithmetic operations.

$\mathcal{O} := \{\sum_{1 \leq i \leq n} 2^{i-1} X_i + t \prod_{1 \leq i \leq n} (1 + (u_i - 1)X_i);$
$(t, u_1, \ldots, u_n) \in \mathbb{C}^{n+1}\}$
is contained in a finite–dimensional $\mathbb{C}$–linear subspace of $\mathbb{C}[X]$ and therefore $\mathcal{O}$ and $\overline{\mathcal{O}}$ are constructible sets.

There exist $K := 16n^2 + 2$ integer points $\xi_1, \ldots, \xi_K \in \mathbb{Z}^n$ of bit length at most $4n$ such that for any two polynomials $f, g \in \overline{\mathcal{O}}$ the equalities $f(\xi_k) = g(\xi_k), 1 \leq k \leq K$, imply $f = g$.

$$\Rightarrow$$

The polynomial map $\Xi : \overline{\mathcal{O}} \to \mathbb{C}^K$ defined for $f \in \overline{\mathcal{O}}$ by $\Xi(f) := (f(\xi_1), \ldots, f(\xi_K))$ is injective,
$\mathcal{M} := \Xi(\mathcal{O})$ is an irreducible constructible subset of $\mathbb{C}^K$ with $\overline{\mathcal{M}} = \Xi(\overline{\mathcal{O}})$ and $\Xi : \overline{\mathcal{O}} \to \overline{\mathcal{M}}$ a finite morphism of affine varieties.

$$\Rightarrow$$

The bijective constructible map $\phi := \Xi^{-1} : \mathcal{M} \to \mathcal{O}$, is geometrically robust.

$\epsilon \in \{0,1\}^n$, $\phi_\epsilon : \overline{\mathcal{M}} \to \mathbb{C}^1$
ϕ_ϵ assigns to each point $v \in \overline{\mathcal{M}}$ the value $\phi(v)(\epsilon)$

$P^{(n)} := \prod_{\epsilon \in \{0,1\}^n}(Y - \phi_\epsilon)$
$P^{(n)}$ is a geometrically robust constructible function
$\mathcal{M} \times \mathbb{C} \to \mathbb{C}$.

Consider $F^{(n)} := \prod_{\epsilon \in \{0,1\}^n}(Y - H^{(n)}(T, U, \epsilon)) =$
$\prod_{0 \le j \le 2^n - 1}(Y - (j + T \prod_{1 \le i \le n} U_i^{[j]_i}))$

$[j]_i$ denotes the i–th digit of the binary representation of the integer j, $0 \le j \le 2^n - 1$, $1 \le i \le n$.

We have for $t \in \mathbb{C}^1$ and $u \in \mathbb{C}^n$ the identities:
$P^{(n)}(\Xi(H^{(n)}(t,u,X)),Y) =$
$\prod_{\epsilon\in\{0,1\}^n}(Y - \phi_\epsilon(\Xi(H^{(n)}(t,u,X)))) =$
$\prod_{\epsilon\in\{0,1\}^n}(Y - H^{(n)}(t,u,\epsilon)) = F^{(n)}(t,u,Y)$

On the other hand:
$(\exists X_1)\ldots(\exists X_n)(\exists T)(\exists U_1)\ldots(\exists U_n)$
$(X_1^2 - X_1 = 0 \wedge \cdots \wedge X_n^2 - X_n = 0 \wedge \bigwedge_{1\le j\le K} S_j =$
$H^{(n)}(T,U,\xi_j) \wedge Y = H^{(n)}(T,U,X))$
describes
$\{(s,y) \in \mathbb{C}^{K+1}; s \in \mathcal{M}, y \in \mathbb{C}, P^n(s,y) = 0\}$

$\Rightarrow$
$P^{(n)} \in \mathbb{C}(\overline{\mathcal{M}})[Y]$ is a (by $\mathcal{M}$ parameterized) *elimination polynomial*.

Theorem 5.

Let γ be an essentially division–free, robust parameterized arithmetic circuit with domain of definition $\mathcal{M}$ such that γ evaluates the elimination polynomial $P^{(n)}$.
Then γ performs at least $\Omega(2^{\frac{n}{2}})$ essential multiplications and at least $\Omega(2^n)$ multiplications with parameters.

Proof (sketch)

$F^{(n)} := Y^{2^n} + \varphi_1 Y^{2^n-1} + \cdots + \varphi_{2^n}$,
$\varphi_\kappa \in \mathbb{C}[T, U], 1 \leq \kappa \leq 2^n$
$\varphi := (\varphi_1, \ldots, \varphi_{2^n})$, $\lambda := (\lambda_1, \ldots, \lambda_{2^n}) := \varphi(0, U)$
independent of U.

Proof (sketch)

$$\varphi_\kappa := \lambda_\kappa + TL_\kappa + \text{higher order terms in } T \ , 1 \leq \kappa \leq 2^n \qquad (1)$$

$$L_1, \ldots, L_{2^n} \in \mathbb{C}[U] \textit{ linearly independent over } \mathbb{C} \qquad (2)$$

Let γ be the robust circuit with parameter domain $\mathcal{M}$ and m essential parameters which evaluates $P^{(n)}$

Transform γ in a robust circuit with parameter domain $\mathbb{C}^{n+1}$ and m essential parameters $\mu_1, \ldots, \mu_m \in \mathbb{C}[T, U]$,
$\mu := (\mu_1, \ldots, \mu_m)$, which evaluates $F^{(n)}$.

Proof (sketch)

There exists a polynomial map $\omega : \mathbb{C}^m \to \mathbb{C}^{2^n}$ with $\omega \circ \mu = \varphi$

Robustness of γ *implies* $\nu := \mu(0, U)$ *is independent of* U.
(This relies strongly on Theorem–Definition 2)

For $u \in \mathbb{C}^n$, let $\epsilon_u : \mathbb{C} \to \mathbb{C}^m$ defined by $\epsilon_u(t) := \mu(t, u), t \in \mathbb{C}$.

$\epsilon_u(0) = \nu$ independently of u

$\varphi = \omega \circ \mu$ and (1) imply

$$(L_1(u), \ldots, L_{2^n}(u)) = \frac{\partial \varphi}{\partial t}(0, u) = (D\omega)_\nu(\epsilon'(0)) \qquad (3)$$

$(D\omega)_\nu$ = complex $(m \times 2^n)$–matrix M which is independent of u.

Proof (sketch)

Choose $u_1, \ldots, u_{2^n} \in \mathbb{C}^n$ such that
$N := (L_\kappa(u_l))_{1 \leq \kappa, l \leq 2^n}$ has rank 2^n (see (2))

$$K := \begin{pmatrix} \epsilon'_{u_1}(0) \\ \vdots \\ \epsilon'_{u_{2^n}}(0) \end{pmatrix}$$

(3) implies $N = K \cdot M$

$$\mathrm{rk} N = 2^n \text{ implies } \mathrm{rk} M \geq 2^n \text{ and finally } m \geq 2^n$$
$$\Rightarrow \gamma \text{ performs at least } \Omega(2^{\frac{n}{2}}) \text{ essential multiplications.}$$

Next lecture:

- A computation model with robust circuits.
- Approximative computations.