Circuits for Unbounded Computation

Thomas Colcombet, Amaldev Manuel

LIAFA, Université Paris-Diderot

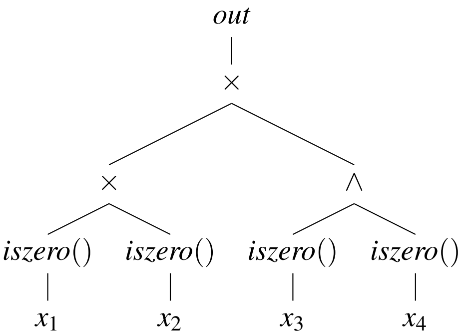
Introduction

- *Unbouded computation* is when the primitive operations are defined for arbitrary input domains, for instance $\mathbb{N}, \mathbb{Z}$.

Summary

A notion of circuits computing functions with integer domain ($\mathbb{Z}^n$) is introduced and a lowerbound is shown.

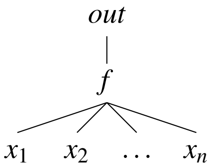
What is a circuit?



- Our gates are all partial functions of the form $f : E_1 \times E_2 \cdots \times E_k \to F$, where $E_1, \ldots, E_k, F \subseteq \mathbb{Z}$.
- The gate f has **type** $E_1 \times E_2 \cdots \times E_k \to F$ and **composition of gates respect types**.

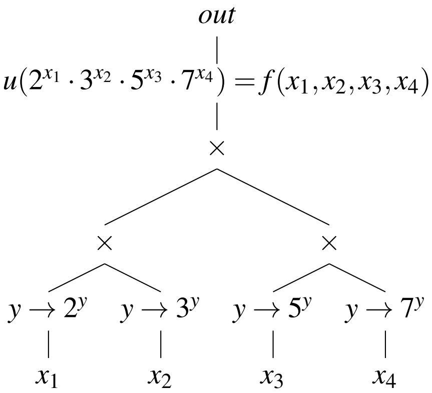
Depth vs Width

Given any $f : \mathbb{Z}^n \to \mathbb{Z}$ there is a circuit computing f with constant height and unbounded fan-in.



Depth vs Width

Given any $f : \mathbb{N}^n \to \mathbb{N}$ there is a circuit computing f with logarithmic depth and fixed fan-in.



- Any function on $\mathbb{Z}^n$ is computed by $\log$-depth, i.e. $O(\log n)$, and fixed fan-in circuits.
- Any function on $\mathbb{Z}^n$ is computed by constant-depth and unbounded fan-in circuits.

Hence,

- We need to fix the height,
- but have to see the whole input,
- while not adding too much power.

Combinatorial circuits

Observe our gates $f : E_1 \times E_2 \cdots \times E_k \to F$, where $E_1, \ldots, E_k, F \subseteq \mathbb{Z}$ are

finitary when $E_1 \times E_2 \cdots \times E_k$ is finite, examples are $\wedge, \neg, \vee$,

binary when $E_1 \times E_2 \cdots \times E_k$ is **not** finite, examples are $+, \times, \log, iszero$.

Combinatorial circuits — Circuits of **constant depth** where

- **finitary** gates, i.e. gates with finite domain, has unbounded fan-in,
- **binary** gates, i.e. gates with infinite domain, has fixed fan-in, **without loss of generality** 2.

Combinatorial circuits

Definition (Combinatorial circuits)

A combinatorial circuit C with input $x_1, \ldots, x_n$ is a directed acyclic graph with labelled vertices such that,

- **input vertices** labelled by $x_1, \ldots, x_n$,
- **finitary gates** labelled by $f : E_1 \times E_2 \cdots \times E_k \to F$ where $E_1 \times E_2 \cdots \times E_k$ is finite, has fan-in exactly k,
- **binary gates** labelled by $f : E_1 \times E_2 \to F$, has fan-in 2,
- **output vertex** labelled by out.

Combinatorial circuits – contd.

Example (All $x_1, \ldots, x_n$ are non-zero)

$$\bigwedge(zero(x_1), \ldots, zero(x_n))$$

Example (Parity: $x_1 \ldots, x_n \rightarrow \sum x_i \mod 2$)

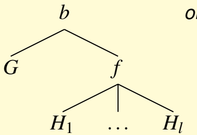
$$+_2(mod_2(x_1), \ldots, mod_2(x_n))$$

Can we compute $x_1 + x_2 \ldots + x_n$?

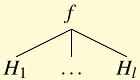
Normal form for circuits

Proposition

Every circuit $C(\bar{x})$ of depth k is equivalent to a circuit of the form ,



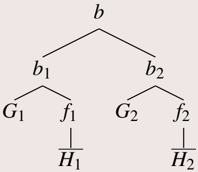
or



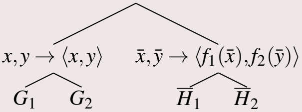
where b is a binary gate , f is a finitary gate and $G, H_1, \dots, H_l$ are binary circuits of depth k.

Proof.

Inductively transform the circuit.



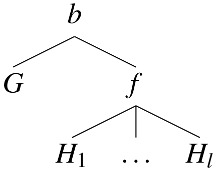
$\Rightarrow \quad \langle x_1, y_1\rangle, \langle x_2, y_2\rangle \to (b(b_1(x_1,x_2), b_2(y_1,y_2))$



□

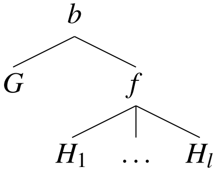
Summing $x_1, \ldots, x_n$

Assume there is a circuit of depth k computing the sum of $x_1, \ldots, x_{2^k+1}$.



Summing $x_1, \ldots, x_n$

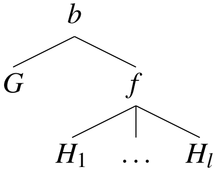
Assume there is a circuit of depth k computing the sum of $x_1, \ldots, x_{2^k+1}$.



- G has depth k so sees at most 2^k variables, choose the variable x not seen by G, w.l.o.g. the right most one.

Summing $x_1, \ldots, x_n$

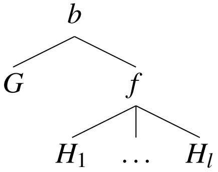
Assume there is a circuit of depth k computing the sum of $x_1, \ldots, x_{2^k+1}$.



- G has depth k so sees at most 2^k variables, choose the variable x not seen by G, w.l.o.g. the right most one.
- Remember each of H_1 to H_k maps to a finite domain w.l.o.g. E.

Summing $x_1, \ldots, x_n$

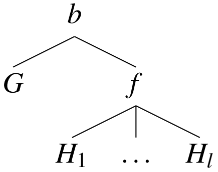
Assume there is a circuit of depth k computing the sum of $x_1, \ldots, x_{2^k+1}$.



- G has depth k so sees at most 2^k variables, choose the variable x not seen by G, w.l.o.g. the right most one.
- Remember each of H_1 to H_k maps to a finite domain w.l.o.g. E.
- Fix all other inputs $\bar{x}$ and consider $\langle \bar{x}, 0 \rangle$, $\langle \bar{x}, 1 \rangle$, $\ldots$

Summing $x_1, \ldots, x_n$

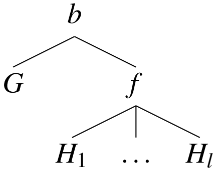
Assume there is a circuit of depth k computing the sum of $x_1, \ldots, x_{2^k+1}$.



- G has depth k so sees at most 2^k variables, choose the variable x not seen by G, w.l.o.g. the right most one.
- Remember each of H_1 to H_k maps to a finite domain w.l.o.g. E.
- Fix all other inputs $\bar{x}$ and consider $\langle \bar{x}, 0 \rangle$, $\langle \bar{x}, 1 \rangle$, $\ldots$
- The infinite set $\{\langle \bar{x}, 0 \rangle, \langle \bar{x}, 1 \rangle, \ldots\}$ is colored with finitely many colors E^l.

Summing $x_1, \ldots, x_n$

Assume there is a circuit of depth k computing the sum of $x_1, \ldots, x_{2^k+1}$.



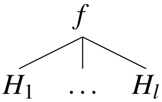
- G has depth k so sees at most 2^k variables, choose the variable x not seen by G, w.l.o.g. the right most one.
- Remember each of H_1 to H_k maps to a finite domain w.l.o.g. E.
- Fix all other inputs $\bar{x}$ and consider $\langle \bar{x}, 0 \rangle$, $\langle \bar{x}, 1 \rangle$, $\ldots$
- The infinite set $\{\langle \bar{x}, 0 \rangle, \langle \bar{x}, 1 \rangle, \ldots\}$ is colored with finitely many colors E^l.
- Hence by pigeonhole there should exist distinct $\langle \bar{x}, a \rangle$ and $\langle \bar{x}, b \rangle$ on which the finitary gate f outputs the same. Hence the circuit outputs the same value. Contradiction.

Null Sum

Let us define the function NS as

$$\text{NS} : x_1, \ldots, x_{2^k+1} \to \begin{cases} 1 & \text{if } \sum_{i=1}^{2^k+1} x_i = 0 \\ 0 & \text{otherwise} \end{cases}$$

Let us try to prove that NS is not computable in depth k. Our circuit has finite co-domain hence it is of the form,

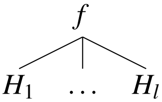


Null Sum

Let us define the function NS as

$$\text{NS} : x_1, \ldots, x_{2^k+1} \to \begin{cases} 1 & \text{if } \sum_{i=1}^{2^k+1} x_i = 0 \\ 0 & \text{otherwise} \end{cases}$$

Let us try to prove that NS is not computable in depth k. Our circuit has finite co-domain hence it is of the form,

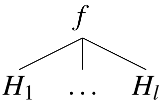


The previous argument **breaks!.**

We need two tuples $\bar{u}$ and $\bar{v}$ on which f outputs the same value but $\sum \bar{u} = 0$ and $\sum \bar{v} \neq 0$. Pigeonhole does not help.

We need stronger arguments.

Reformulation



- The finitary gate f sees the input through a 2^k sized **window** via the binary circuits H_i by mapping it to a color in E^l.
- Let us call the coloring $\chi : \mathbb{Z}^{2^k} \to E^l$.
- Two inputs $\bar{u}$ and $\bar{v}$ appear the same to f if for any window $i_1, \dots, i_{2^k} \in \{1, \dots, n\}^{2^k}$,

$$\chi(u_{i_1}, \dots, u_{i_k}) = \chi(v_{i_1}, \dots, v_{i_k}).$$

- We say $\bar{u}$ and $\bar{v}$ are **χ-indiscernible** in which case.

If we can prove that **for every χ there are two χ-indiscernible tuples $\bar{u}$ and $\bar{v}$ such that $\sum \bar{u} = 0$ and $\sum \bar{v} \neq 0$**, then we are done.

Reformulation contd.

- We saw for any window $i_1, \ldots, i_{2^k} \in \{1, \ldots, n\}^{2^k}$, the coloring function χ defines you a coloring.
- Let us define in one shot all the colorings of all the windows, i.e, big coloring Ψ defines all the colors given by χ for all the windows , that is $\Psi(\bar{u}) : \{1, \ldots, n\}^{2^k} \to E^l$, where

$$\Psi(\bar{u}) : \text{a window } w \to \text{coloring } \chi(w) \text{ of the window}$$

Now $\bar{u}$ and $\bar{v}$ are **χ-indiscernible** iff $\Psi(\bar{u}) = \Psi(\bar{v})$.

Restating our aim,

If we can prove that **for every χ there are two χ-indiscernible tuples $\bar{u}$ and $\bar{v}$ such that $\sum \bar{u} = 0$ and $\sum \bar{v} \neq 0$**, then we are done.

Gallai-Witt

Theorem (Gallai-Witt)

- *Fix a finite set of colors C,*
- *Choose a finite set of points $F \subseteq \mathbb{N}^k$,*
- *Gallai-Witt will give you an n such that,*
  - *for any coloring of $[n]^k$ with C colors, you can find a monochromatic* ***scaled translated copy of F*** *inside.*

Scaled translated copy of F is $\bar{a} + \lambda F$ for some $\bar{a} \in \mathbb{N}^k$ and a positive integer λ.

Applying Gallai-Witt

For every $\chi : \mathbb{Z}^k \to C$ there are two χ-indiscernible tuples $\bar{u}$ and $\bar{v}$ of length $k+1$ such that $\sum \bar{u} = 0$ and $\sum \bar{v} \neq 0$.

- Choose the set of colors to be $windows \to C$.
- Take $F \subseteq \mathbb{N}^k$ as $\{(0,\ldots,0),(1,0,\ldots,0),(0,1,\ldots,0),\ldots,(0,0,\ldots,1)\}$.
- Gallai-Witt gives an n.
- Apply the following coloring to $[n]^k$ as

$$color(x_1,\ldots,x_k) = \Psi(x_1,\ldots,x_k,-\sum x_i)$$

  and obtain $\bar{a} \in \mathbb{N}^k$ and a positive integer λ.

Choose

$$\bar{u} = (a_1,\ldots,a_k,-\sum a_i) \qquad \bar{v} = (a_1,\ldots,a_k,-\sum a_i + \lambda)$$

They are χ-indiscernible.

Lowerbound

Let us define the function NSM as

$$\text{NSM} : x_1, \ldots, x_n, x_{n+1} \to \begin{cases} 1 & \text{if } \sum_{i=1}^{n} x_i = 0 \mod x_{n+1} \\ 0 & \text{otherwise} \end{cases}$$

Theorem

NSM *is not recognizable. (More precisely* NSM_{2^k+2} *is not recognized by depth* k*-circuits).*

Theorem (Definability)

A language L *is recognizable if and only if* $\forall n \in \mathbb{N}$ *there is a finite set of colors* C *and a coloring* $\chi : \mathbb{N}^{2^k} \to C$ *such that*

$$\forall \bar{u}, \bar{v} \in \mathbb{N}^n, \text{ if } \bar{u} \sim_\chi \bar{v} \text{ then } \bar{u} \in L \Leftrightarrow \bar{v} \in L$$

Thanks to **Holger** and **Thomas** for helping me to prepare.

Thank you for your attention.