Combinatorial Circuits and Indiscernibility

Thomas Colcombet, Amaldev Manuel

LIAFA, Université Paris-Diderot

Motivation

- To prove hierarchy theorems for μ-calculus on data words,
- and a general technique to prove indefinability results.

Summary

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

Combinatorial Circuits

Gates – partial functions on $\mathbb{Z}, \mathbb{Z}^2, \mathbb{Z}^3, \ldots$ of two kinds,

- **binary** Those with unbounded domain and fixed arity, e.g. sum, product, isprime(), iszero(), etc.
  - Sum : $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $\mathrm{iszero}() : \mathbb{Z} \to \{0,1\}$, $\log : \mathbb{N} \to \mathbb{N}$.
- **finitary** Those with bounded domain and any arity,
  - $\bigvee_n : \{0,1\}^n \to \{0,1\}$, $\pi_n : M^n \to M$ defining the product on the monoid M.

Combinatorial Circuits

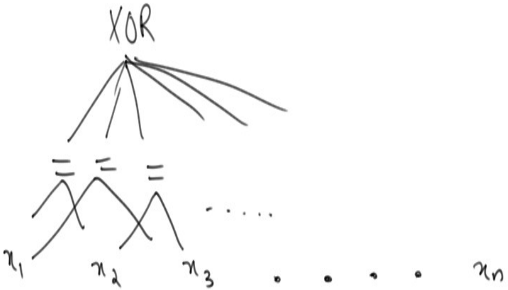
Gates – partial functions on $\mathbb{Z}, \mathbb{Z}^2, \mathbb{Z}^3, \ldots$ of two kinds,

- **binary** Those with unbounded domain and fixed arity, e.g. sum, product, isprime(), iszero(), etc.
  - Sum : $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $\mathrm{iszero}() : \mathbb{Z} \to \{0, 1\}$, $\log : \mathbb{N} \to \mathbb{N}$.
- **finitary** Those with bounded domain and any arity,
  - $\bigvee_n : \{0,1\}^n \to \{0,1\}$, $\pi_n : M^n \to M$ defining the product on the monoid M.

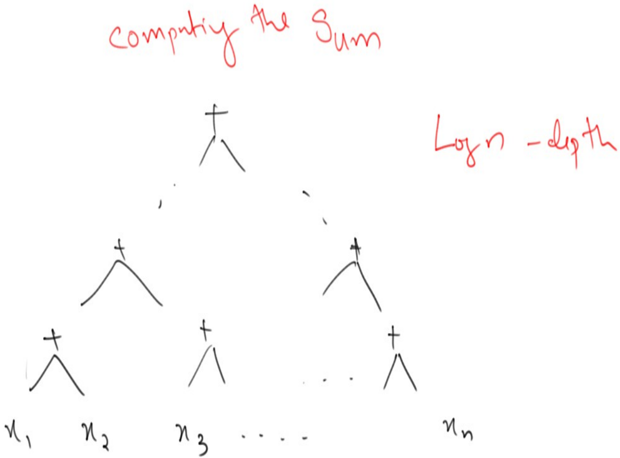
Circuits – Composition of gates of fixed height (for input of any length).

An example

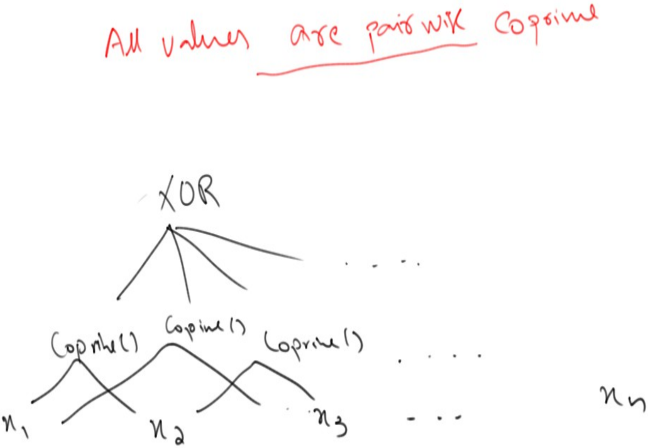
All values are different (height 2)



A non-example

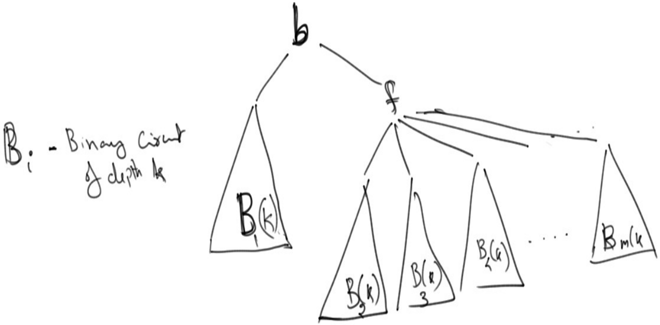


Another example

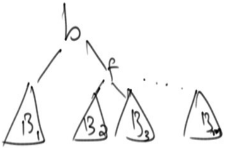


What about gcd ?

Normal form for depth-k circuits



gcd is not computable



B_i – binary circuit of depth k

- Assume there is a circuit of depth k computing gcd of $2^k + 1$ values $x_1, x_2, \ldots, x_{2^k+1}$
- B_1 does not see a value, WLOG x_{2^k+1}.
- $B_2, \ldots, B_m$ induces a finite coloring of $x_1, x_2, \ldots, x_{2^k+1}$ (say with colors $[r]$).
- Consider the set $(2^{r+1}, 2^{r+1}, \ldots, 2), (2^{r+1}, 2^{r+1}, \ldots, 2^2), \ldots, (2^{r+1}, 2^{r+1}, \ldots, 2^{r+1})$.
- Using **pigeonhole** conclude that there are two tuples on which the circuit gives the same value.

What about gcd=1 ?

Formally, Show that there is no constant-depth circuit

$$C(x_1,\ldots,x_n) = \begin{cases} 1 & \text{if } \gcd(x_1,\ldots,x_n) = 1 \\ 0 & \end{cases}$$

Previous proof does not work.

Indiscernibility

Fix an r-coloring χ of $\mathbb{N}^k$,

$$\chi : \mathbb{N}^k \to [r]$$

Two tuples $(u_1, u_2, \ldots, u_m), (v_1, v_2, \ldots, v_m) \in \mathbb{N}^m$ are **χ-indiscernible** if **for every window $W = i_1 i_2 \ldots i_k \in [m]^k$ the χ-colorings of $(u_{i_1}, u_{i_2}, \ldots, u_{i_k})$ and $(v_{i_1}, v_{i_2}, \ldots, v_{i_k})$ are the same.**

Indiscernibility

Fix an r-coloring χ of $\mathbb{N}^k$,

$$\chi : \mathbb{N}^k \to [r]$$

Two tuples $(u_1, u_2, \ldots, u_m), (v_1, v_2, \ldots, v_m) \in \mathbb{N}^m$ are **χ-indiscernible** if **for every window $W = i_1 i_2 \ldots i_k \in [m]^k$ the χ-colorings of $(u_{i_1}, u_{i_2}, \ldots, u_{i_k})$ and $(v_{i_1}, v_{i_2}, \ldots, v_{i_k})$ are the same.**

Definability Theorem

Circuits cannot distinguish between indiscernible tuples.

Indefinability

A property $\mathbf{P} \subseteq \mathbb{N}^*$ is not definable by circuits

iff

for any r-coloring χ there are two χ-indiscernible tuples, one in P, other not in P.

Hales-Jewett Theorem

Fix a finite alphabet A.
A **Combinatorial line** is a word w in $(A \cup \{x\})^* \setminus A^*$ identified with the set $\{w[x/a] \mid a \in A\}$.

Let $A = \{a, b, c\}$ then $w = axc$ corresponds to $\{aac, abc, acc\}$.

Hales-Jewett Theorem

Fix a finite alphabet A.
A **Combinatorial line** is a word w in $(A \cup \{x\})^* \setminus A^*$ identified with the set $\{w[x/a] \mid a \in A\}$.

Let $A = \{a, b, c\}$ then $w = axc$ corresponds to $\{aac, abc, acc\}$.

Hales-Jewett Theorem
For every alphabet A and colors $[r]$ there is a length $n = \mathrm{HJ}(|A|, r)$ such that any r-coloring of A^n has a monochromatic combinatorial line.

A game-theoretic example

Generalized tic-tac-toe has three parameters, number of players r, size of the board m and dimension n.
Usual tic-tac-toe is when $r = 2$, $m = 3$ and $d = 2$.
Rows, columns, diagonals are combinatorial lines.

HJ says that for any number of players and size of the board, there is a large enough dimension such that the game wont end in a draw!

Example

Van der Warden Theorem For any k and colors $[r]$ there is a number $n = \mathbf{VW}(k, r)$ such that any r-coloring of $[n]$ has a monochromatic arithmetic progression of length k.

Example

Van der Warden Theorem For any k and colors $[r]$ there is a number $n = \mathbf{VW}(k,r)$ such that any r-coloring of $[n]$ has a monochromatic arithmetic progression of length k.

- Take $A = \{1,\ldots,k\}$ and colors $[r]$ and get $m = \mathbf{HJ}(k,r)$.
- Identify each word $a_1 a_2 \ldots a_m$ in A^m with the word $a_1 + a_2 \ldots + a_m$. (A combinatorial line corresponds to some $a + \lambda x$ where a is a sum of elements of A and $\lambda \in [m]$ is an integer.)
- Apply the r-coloring to the numbers A^m.
- $a + \lambda \times 1, a + \lambda \times 2, \ldots, a + \lambda$ is an AP of length k.

Example

Applying the same proof,

Gallai-Witt Theorem

For any finite $F \subseteq \mathbb{N}^k$ and colors $[r]$ there is a number $n = \mathbf{GW}(k,r,F)$ such that any r-coloring of $[n]^k$ has a monochromatic homothetic copy (i.e. $a + \lambda \times F$) of F.

Enough to prove indefinability of modular sum.

Conclusion

- Notion of circuits are useful for data words.
- Lowerbounds depend on deep theorems from combinatorics.
- Reductions, hardness, completeness etc.