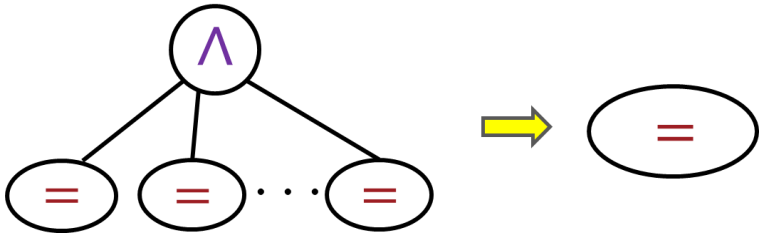
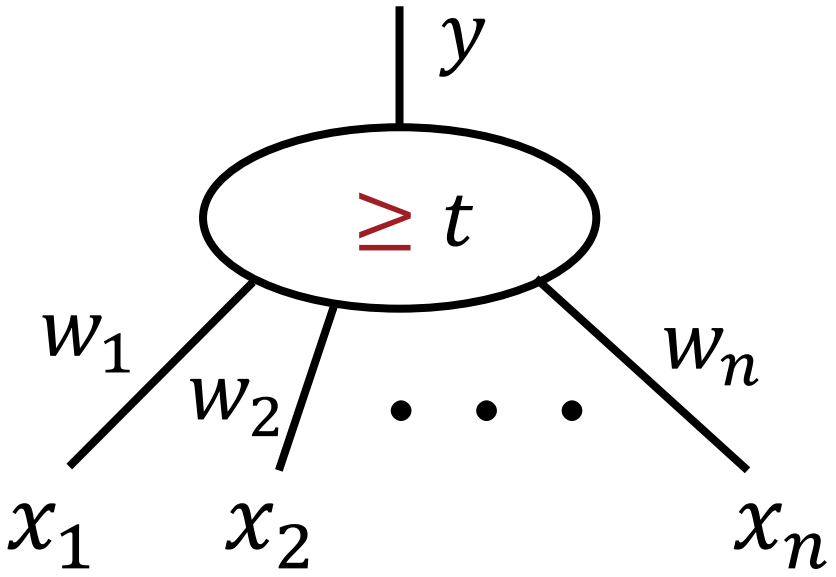
On the Size of Depth-2 Threshold Circuits for the Inner Product Mod 2 Function



Kazuyuki Amano
(Gunma Univ., Japan)

Threshold Gate (THR)

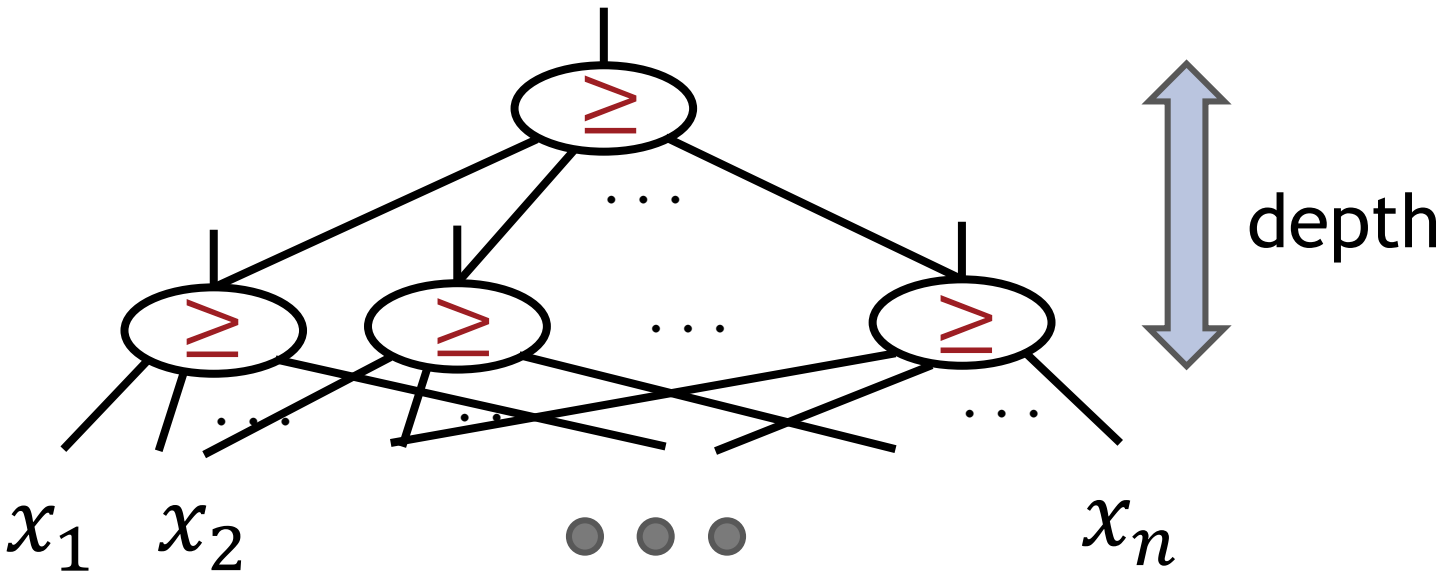


$$y = \begin{cases} 1, & \text{if } w_1x_1 + w_2x_2 + \cdots + w_nx_n \geq t \\ 0, & \text{otherwise} \end{cases}$$

Note: All weights are integer (w.l.o.g.)

Threshold Circuit

A circuit that consists of threshold gates.



Inner Product mod 2

$\mathrm{IP}_n : \{0,1\}^{2n} \to \{0,1\}$

$\mathrm{IP}_n(x_1, \ldots, x_n, y_1, \ldots, y_n) := \bigoplus_{i=1}^{n} (x_i \wedge y_i)$

(XOR of bit-wise AND of two n-bit inputs)

Question

What is the minimum size (i.e., # of gates) of a depth-two threshold circuit that computes IP_n?

Motivation

- Depth-two threshold circuit is a current frontier in circuit lower bounds

- At present, we can't refute that every Boolean function in NP can be computed by a poly-size (or even $O(n^2)$-size) depth-two threshold circuit.

- If weights are polynomially bounded, then an exponential lower bound is known, e.g., for Inner Product function.

[Hajnal et al., 1993]

So,

Inner Product function is a good candidate for proving an exponential lower bound for depth-two threshold circuit.

Best known lower bound is $\Omega(n)$.

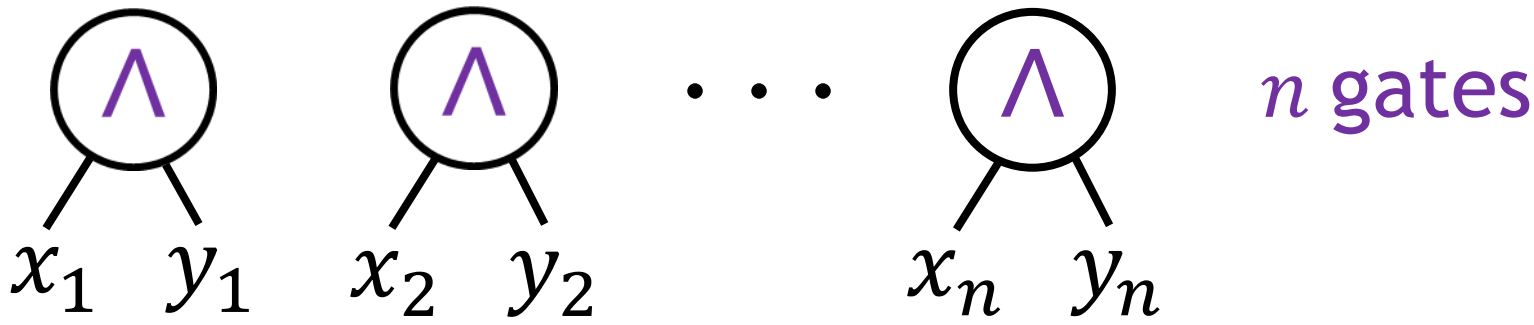
[Roychowdhury et. al, 1994]

Question:

What is the minimum size of a depth-two threshold circuit that computes IP_n?

Easy for depth 3

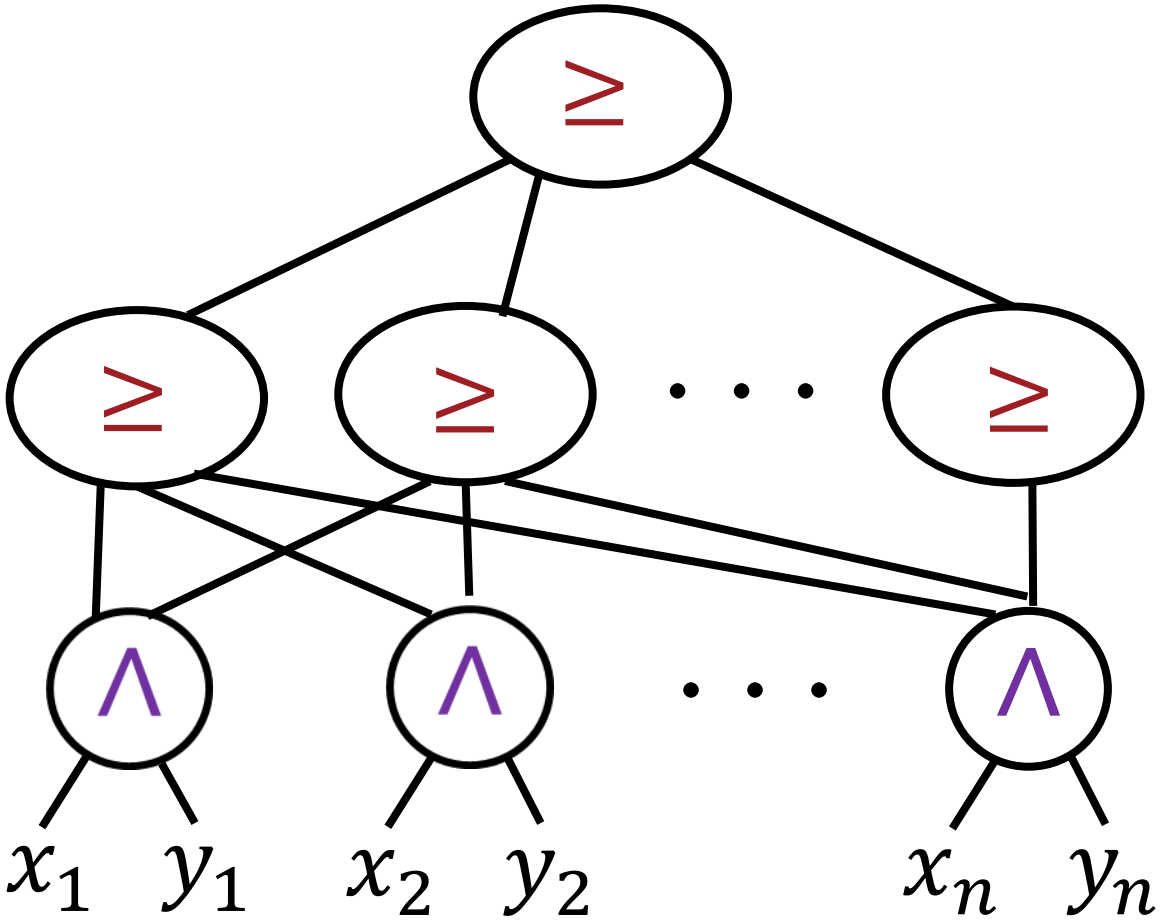
$$\mathrm{IP}_n(x_1, \ldots, x_n, y_1, \ldots, y_n) \coloneqq \bigoplus_{i=1}^{n} (x_i \wedge y_i)$$



n gates

Easy for depth 3

$$\mathrm{IP}_n(x_1, \ldots, x_n, y_1, \ldots, y_n) := \bigoplus_{i=1}^{n} (x_i \wedge y_i)$$



$O(n)$ gates

n gates

Results

1. Non-trivial construction (of size $O(1.682^n)$) of depth-two threshold circuits that computes IP_n

2. An exponential lower bound for a special form of depth-two circuit that computes IP_n.

Naïve Construction

$$\mathrm{IP}_n(x_1, \ldots, x_n, y_1, \ldots, y_n) := \bigoplus_i (x_i \wedge y_i)$$

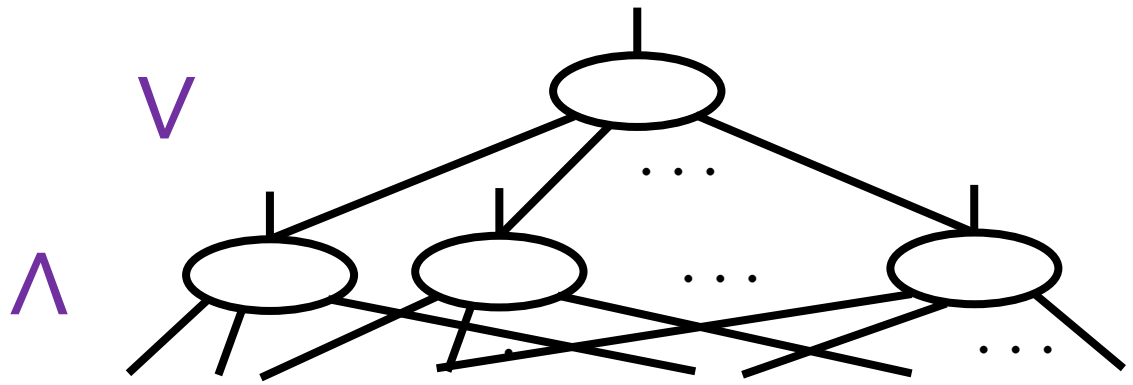
DNF (Disjunctive Normal Form)

$$= x_1 y_1 \overline{x}_2 \vee x_1 y_1 \overline{y}_2 \vee \overline{x}_1 x_2 y_2 \vee \overline{y}_1 x_2 y_2$$

(when $n = 2$)

# of gates =
# of terms

$O(3^n)$



Naïve Construction

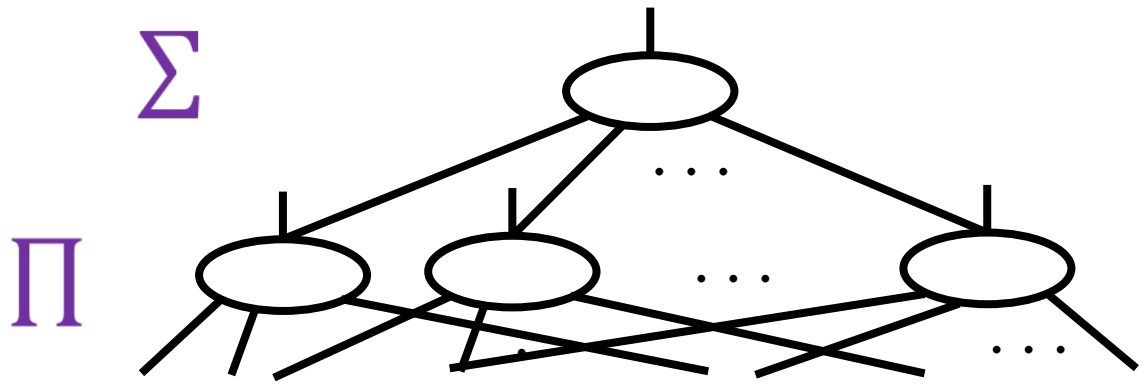
$$\mathrm{IP}_n(x_1, \ldots, x_n, y_1, \ldots, y_n) := \bigoplus_i (x_i \wedge y_i)$$

$$= \sum_{\emptyset \neq S \subseteq \{1,\ldots,n\}} (-2)^{|S|-1} \prod_{i \in S} x_i y_i.$$

(Inclusion-Exclusion formula)

# of gates :

2^n



Result

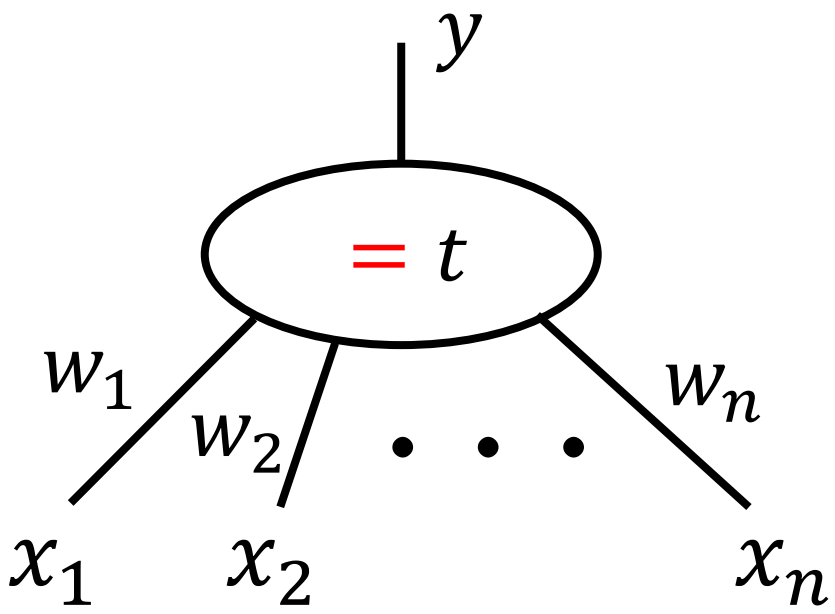
IP_n has a depth-two threshold circuit of size $O(1.682^n)$

Outline

Step 1: Construct an efficient THR of ETHR circuit that computes IP_k for small k.

Step 2: Use this as a building block to construct a circuit for IP_n for general n.

ETHR (Exact Threshold Gate)



$$y = \begin{cases} 1, & \text{if } w_1x_1 + w_2x_2 + \cdots + w_nx_n = t \\ 0, & \text{otherwise.} \end{cases}$$

Key Fact 1

- An ETHR gate can be simulated by two THR gates

$$[\![\ell(x) = t]\!] = [\![\ell(x) \geq t]\!] - [\![\ell(x) \geq t+1]\!]$$

- Conversely, a THR gate can be simulated by polynomial number of ETHR gates

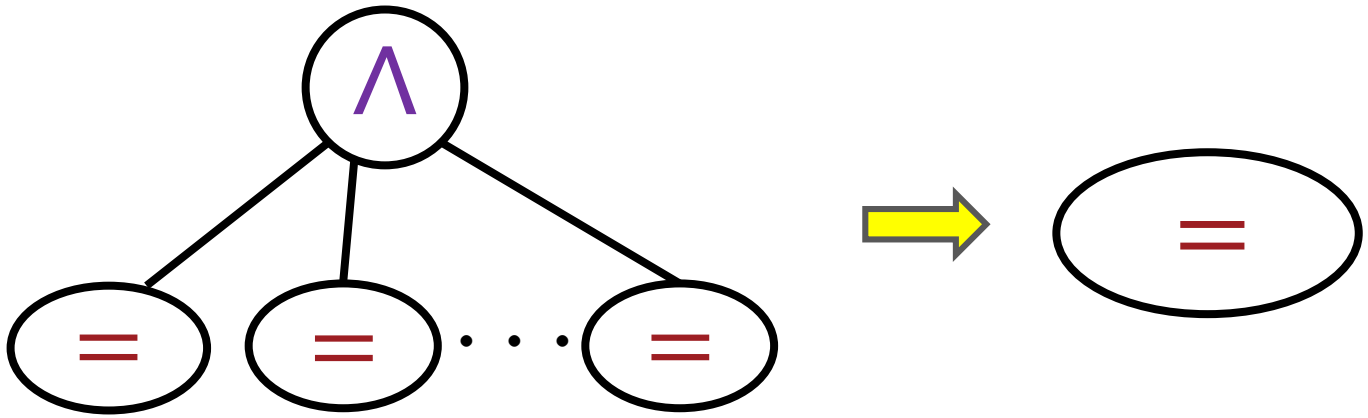
[Hansen, Podolskii,'10]

but we don't need this today…

Key Fact 2

- ETHR gates is closed under AND operation

[Hansen, Podolskii,'10]



e.g.,

$$[\![\ell_1(x) = t_1]\!] \wedge [\![\ell_2(x) = t_2]\!]$$

$$= [\![10000\ell_1(x) + \ell_2(x) = 10000t_1 + t_2]\!]$$

Step 1

With the help of computers, we found that

IP_4 can be represented by
the sign of the linear combination of 8 ETHR gates

Step 1

With the help of computers, we found that

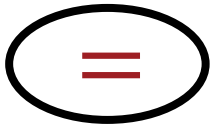
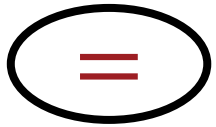
IP_4 can be represented by
the sign of the linear combination of 8 ETHR gates

$$\mathrm{IP}_4(x_1, \ldots, x_4, y_1, \ldots, y_4) = \operatorname{sgn}\left(-3 + 2\sum_{i\in[7]} g_i(z_1, z_2, z_3, z_4)\right).$$

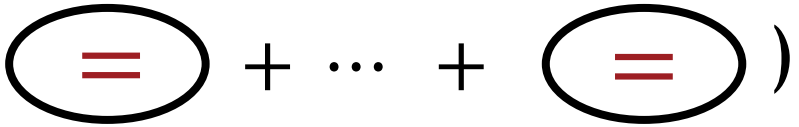
$g_1, \ldots, g_7$

$$[\![-z_1 + z_2 + z_3 + z_4 = 1]\!], \quad [\![z_1 - z_2 + z_3 + z_4 = 1]\!],$$
$$[\![z_1 + z_2 - z_3 + z_4 = 1]\!], \quad [\![z_1 + z_2 + z_3 - z_4 = 1]\!],$$
$$[\![z_1 - z_2 - z_3 + z_4 = 0]\!], \quad [\![z_1 - z_2 + z_3 - z_4 = 0]\!],$$
$$[\![z_1 + z_2 - z_3 - z_4 = 0]\!].$$

$$z_i := x_i + y_i$$

IP_4 = sign ( + ⋯ + )

8

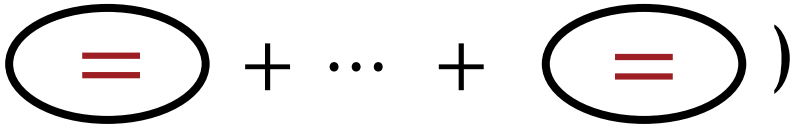
IP_4 = sign ( + ⋯ +)

8

If we assume that

"+" represents 0 and "—" represents 1,

then sign(x) ⊕ sign(y) = sign(x·y)

IP_4 = sign ()

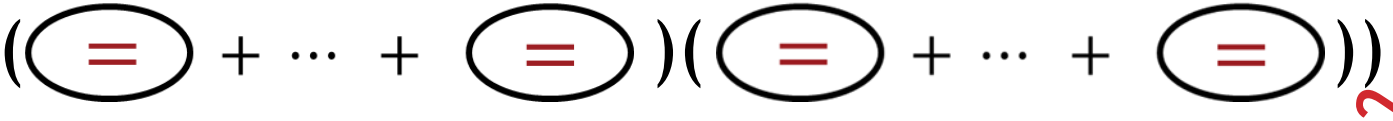
8

If we assume that

"+" represents 0 and "—" represents 1,

then sign(x) $\oplus$ sign(y) = sign(x·y)

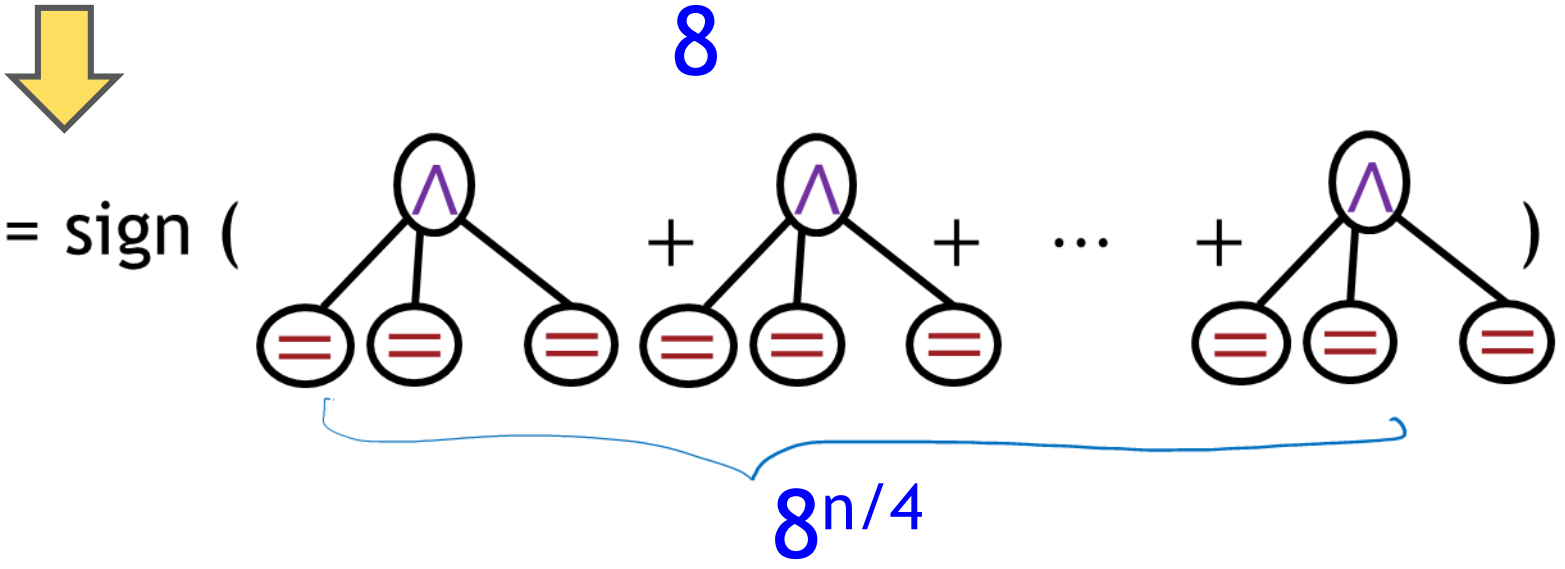
$IP_8 = IP_4 \oplus IP_4$

= sign (())

$$IP_n = \text{sign}\left(\left(\bigcirc\!\!= + \cdots + \bigcirc\!\!= \right)^{n/4} \right)$$

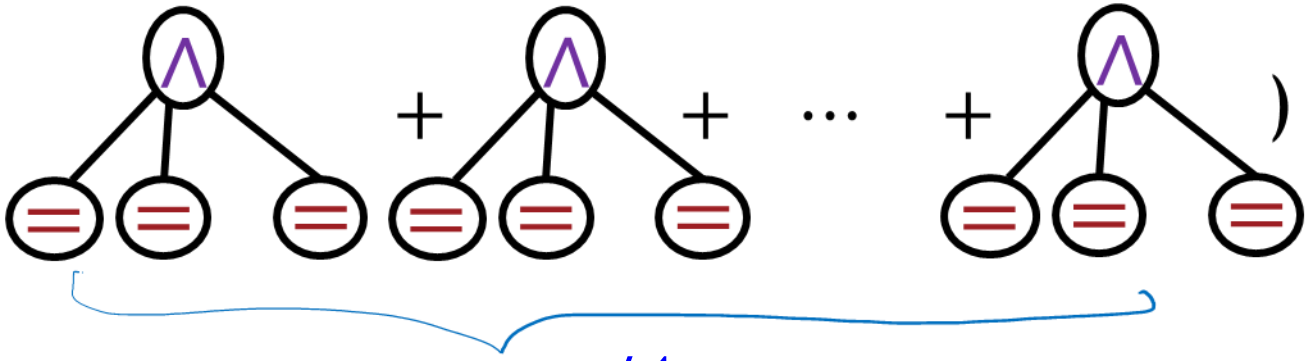
8

$IP_n = \text{sign}\left(\left(= + \cdots + = \right)^{n/4} \right)$



$IP_n = \text{sign}\left(\left(= + \cdots + = \right)^{n/4} \right)$

$IP_n = \text{sign}\left(\right.$



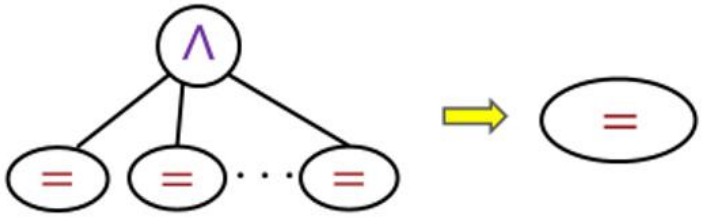
$\left. \right)$

$8^{n/4}$

Key Fact 2

- ETHR gates is closed under AND operation

[Hansen, Podolskii, '10]



$IP_n = \text{sign}\left(\left(= + \cdots + = \right)^{n/4} \right)$

8

$IP_n = \text{sign}\left(\wedge + \wedge + \cdots + \wedge \right)$

$8^{n/4}$

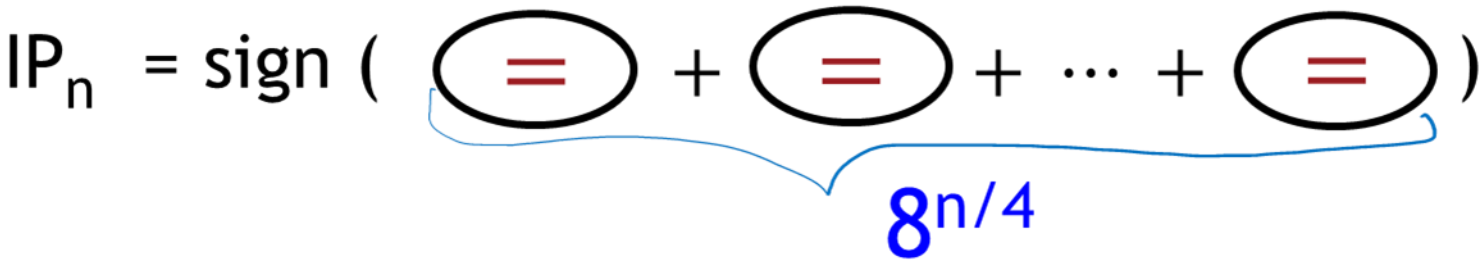
$IP_n = \text{sign}\left(= + = + \cdots + = \right)$

$8^{n/4}$

Key Fact 1

- An ETHR gate can be simulated by two THR gates

$$[\![\ell(x) = t]\!] = [\![\ell(x) \geq t]\!] - [\![\ell(x) \geq t+1]\!]$$



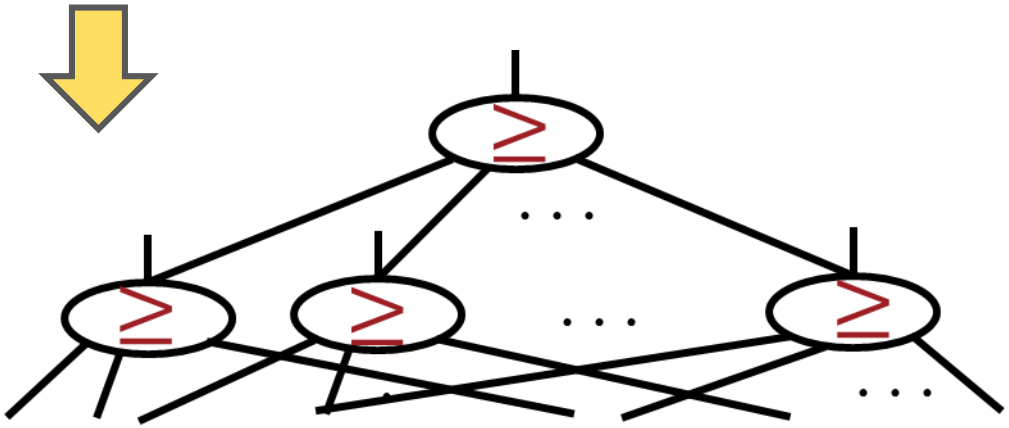
Key Fact 1

- An ETHR gate can be simulated by two THR gates

$$[\![\ell(x) = t]\!] = [\![\ell(x) \geq t]\!] - [\![\ell(x) \geq t+1]\!]$$

IP_n = sign ($=$ + $=$ + ⋯ + $=$)

$8^{n/4}$



# of gates:

$$2 \cdot 8^{n/4} = O(1.682^n)$$

q.e.d

Some generalization

IP_k can be represented by the sign of the linear combination of m ETHR gates

A THR of THR circuit of size $O((m^{1/k})^n)$

Our construction:

$$(k, m) = (4, 8) \rightarrow O(1.682^n)$$

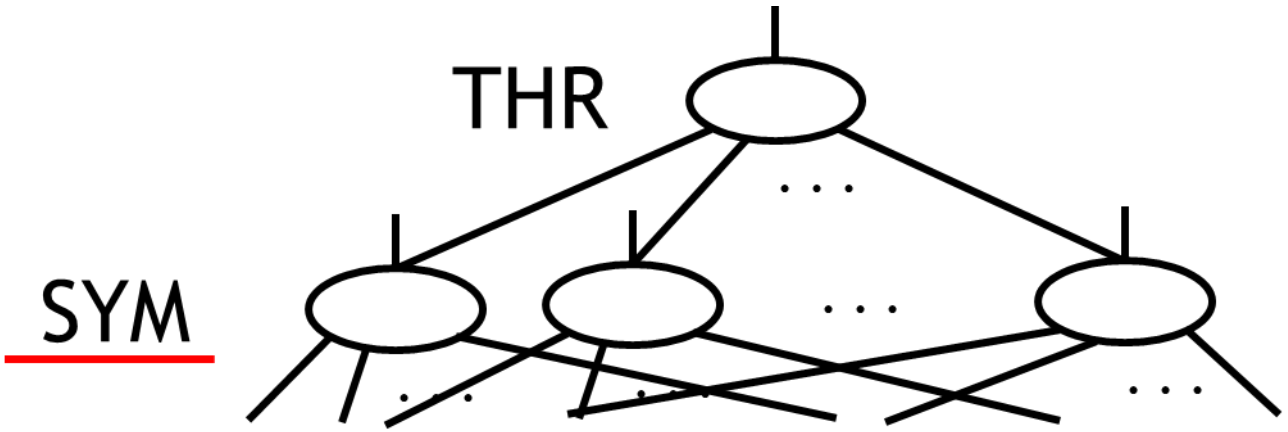
For example,

$(k, m) = (5, 13)$ would imply $O(1.6803^n)$ bound

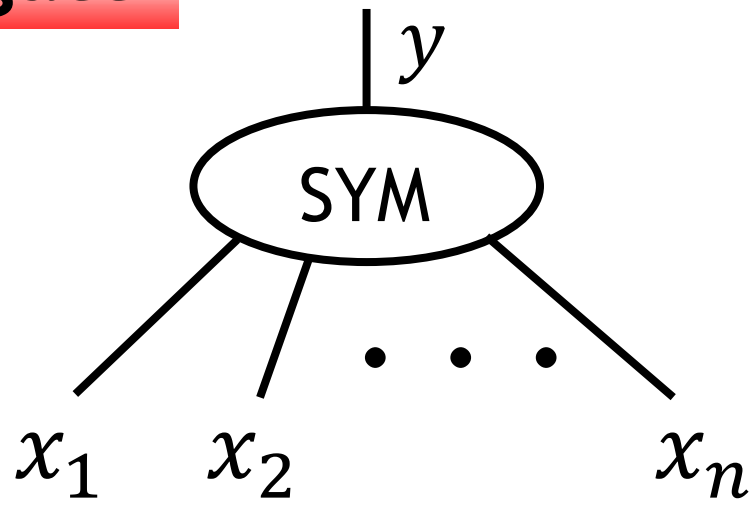
Results

1. Non-trivial construction (of size $O(1.682^n)$) of depth-two threshold circuits that computes IP_n

2. An exponential lower bound for a special form of depth-two circuit that computes IP_n.



SYM gate



A gate that computes a symmetric function, i.e., its output $y \in \{0,1\}$ depends only on the # of ones in inputs $x_1, \ldots, x_n$.

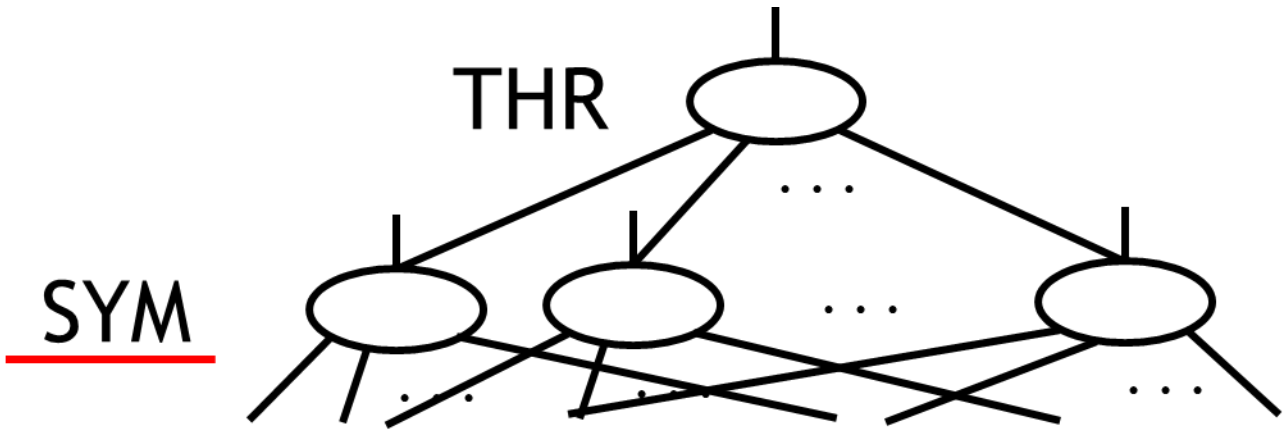
A SYM gate can emulate PARITY, MOD, unweighted MAJORITY, etc.

Result

Theorem

Every THR-SYM circuit computing IP_n has size $\Omega(1.5^n)$

improving $\Omega(1.414^n)$ bound by Forster et al. (2001)



Linear Programming

Theorem [A, MFCS '05]

The obj. of the following LP gives a lower bound on the size of THR-SYM circuit for IP_n

$$\text{Minimize} \quad \sum_{T \subseteq X_k} q_T,$$

$$\text{Subject to} \quad \sum_{T: v \in T} q_T \geq z_{k-1} \quad (v \in X_k),$$

$$\sum_{T: |\{u,v\} \cap T| = 1} q_T \geq z_{k-2} \quad \left(\begin{array}{l} i, j \in [k], i \neq j \\ u \in \{x_{2i-1}, x_{2i}\}, v \in \{x_{2j-1}, x_{2j}\} \end{array} \right),$$

$$q_T \geq 0 \quad (T \subseteq X_k).$$

… and It's Dual

$$\text{Maximize} \quad z_{k-1} \sum_{v \in [2k]} s_v + z_{k-2} \sum_{\{u,v\} \in Z_k} t_{u,v},$$

$$\text{Subject to} \quad \sum_{v \in [2k]: x_v = 1} s_v + \sum_{\{u,v\} \in Z_k : x_u \neq x_v} t_{u,v} \leq 1 \qquad (\boldsymbol{x} \in \{0,1\}^{2k}),$$

$$s_v \geq 0 \qquad (v \in [2k]),$$

$$t_{u,v} \geq 0 \qquad (\{u,v\} \in Z_k).$$

LP duality theorem says that any feasible solution to this dual problem gives a lower bound.

… and It's Dual

$$\text{Maximize} \quad z_{k-1} \sum_{v \in [2k]} s_v + z_{k-2} \sum_{\{u,v\} \in Z_k} t_{u,v},$$

$$\text{Subject to} \quad \sum_{v \in [2k]: x_v = 1} s_v + \sum_{\{u,v\} \in Z_k : x_u \neq x_v} t_{u,v} \leq 1 \qquad (\boldsymbol{x} \in \{0,1\}^{2k}),$$

$$s_v \geq 0 \qquad (v \in [2k]),$$

$$t_{u,v} \geq 0 \qquad (\{u,v\} \in Z_k).$$

LP duality theorem says that any feasible solution to this dual problem gives a lower bound.

Theorem

Every THR-SYM circuit computing IP_n has size $\Omega(1.5^n)$

Summary & Future work

1. $O(1.682^n)$ upper bound on the size of a depth-two threshold circuit for IP_n.
   - Find a small circuit by a computer and then blow-up.
   - A constant may be improved.
   - Sub-exponential bound seems to be challenging.

Summary & Future work

1. $O(1.682^n)$ upper bound on the size of a depth-two threshold circuit for IP_n.
   - Find a small circuit by a computer and then blow-up.
   - A constant may be improved.
   - Sub-exponential bound seems to be challenging.

2. $\Omega(1.5^n)$ lower bound on the size of a THR-SYM circuit for IP_n
   - Give a solution to the dual of LP whose obj. gives a lower bound on circuit size.
   - Can we extend the method to THR-THR circuits?

Fin. Thank you.