

CNS 188a Overview

- Boolean algebra as an axiomatic system
- Boolean functions and their representations using Boolean formulas and spectral methods
- Implementing Boolean functions with relay circuits, circuits of AON (AND, OR, NOT) gates and LT (Linear Threshold) gates
- Analyzing the complexity (size and depth) of circuits
- Relations (as opposed to functions) and their implementation in circuits
- Feedback and convergence in LT circuits

LT Constructions for Symmetric Functions

circuit kind	size
LT-I	$n + 1$
LT-nl, d-2	$\left\lfloor \frac{n}{2} \right\rfloor + 1$
LT-nl -XOR	$\lceil \log_2(n + 1) \rceil$

transitions

Muroga

intervals

Minnick

Binary representation

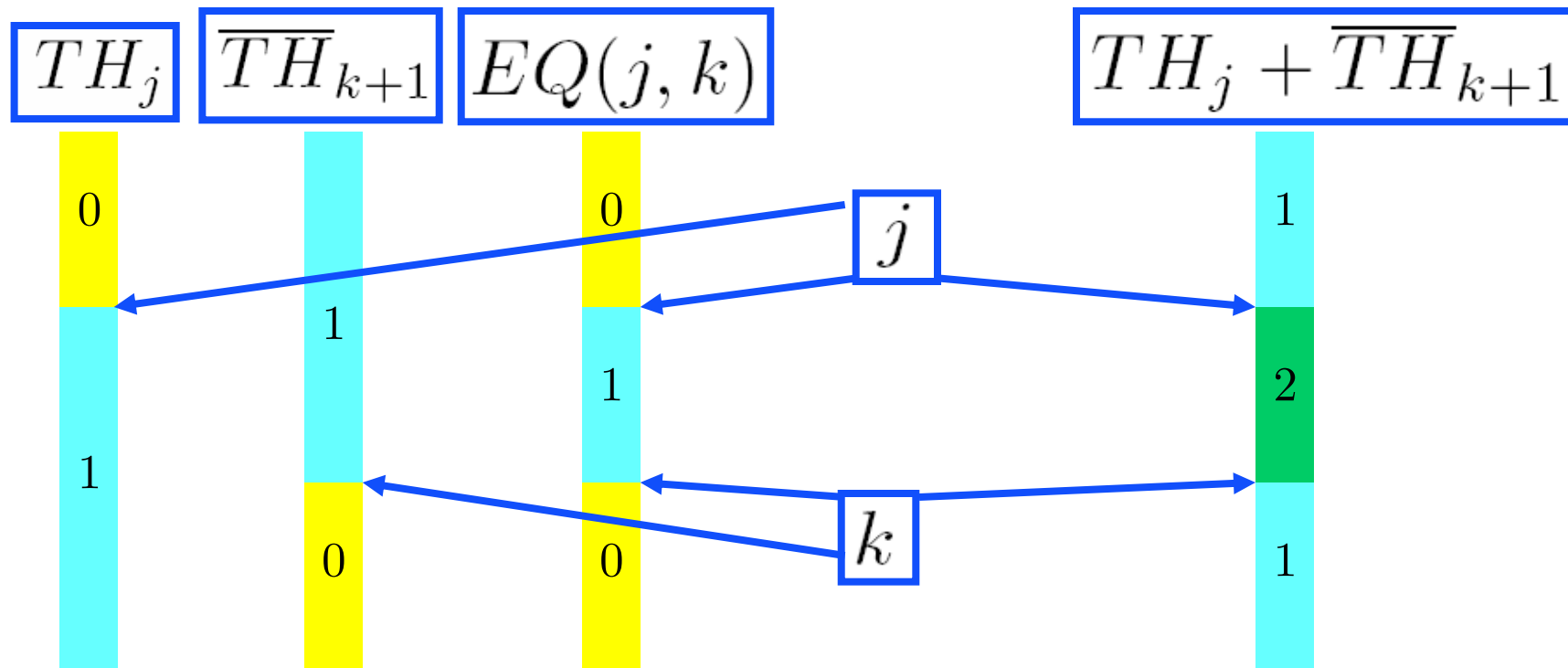
Kautz

optimal

Muroga's Idea

$$EQ(j, k) = \begin{cases} 1 & \text{if } j \leq |X| \leq k \\ 0 & \text{else} \end{cases}$$

$$EQ(j, k) = TH_j + \overline{TH}_{k+1} - 1$$



LT-I Circuit Design Algorithm for SYM

Muroga 1959

$ X $	$f(X)$	$f(X) = \overline{TH}_2 + TH_3 + \overline{TH}_5 + TH_6 - 1$	
0	1	$0 \Rightarrow 1$	$1 \Rightarrow 0$
1	1	$\overline{TH}_2$	TH_i
2	0		$\overline{TH}_i$
3	1	TH_3	
4	1	$\overline{TH}_5$	Subtract 1 for every isolated 1-block
5	0		
6	1	TH_6	
7	1		

LT-nl Construction

Minnick 1959

Given a symmetric function f with k 1s in the symmetric function table

At locations: $q_1, q_2, q_3, \dots, q_k$

Construct an LT-nl circuit with $k+1$ gates

$$k = 5$$

$$q_1 = 1$$

$$q_2 = 3$$

$$q_3 = 4$$

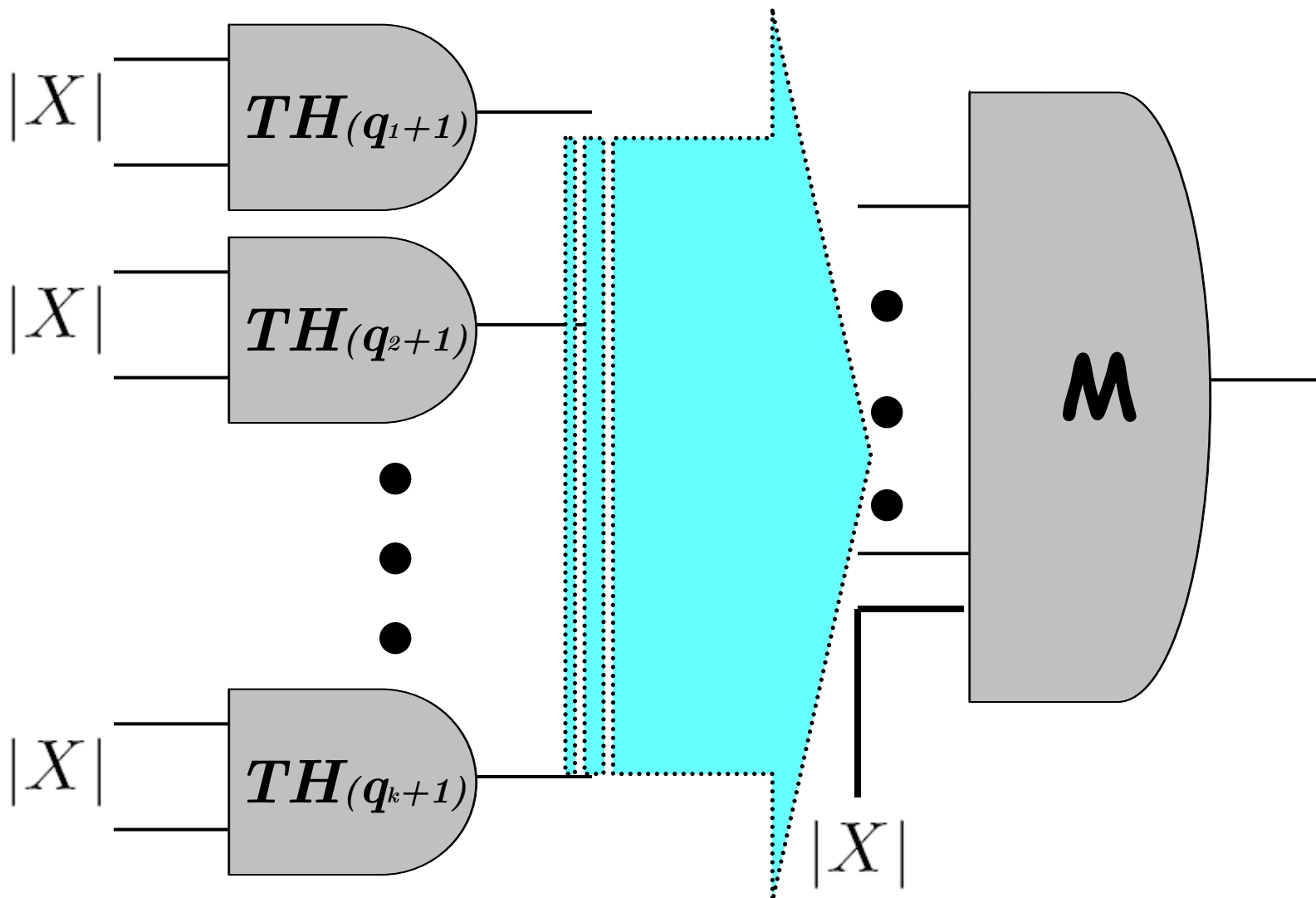
$$q_4 = 6$$

$$q_5 = 7$$

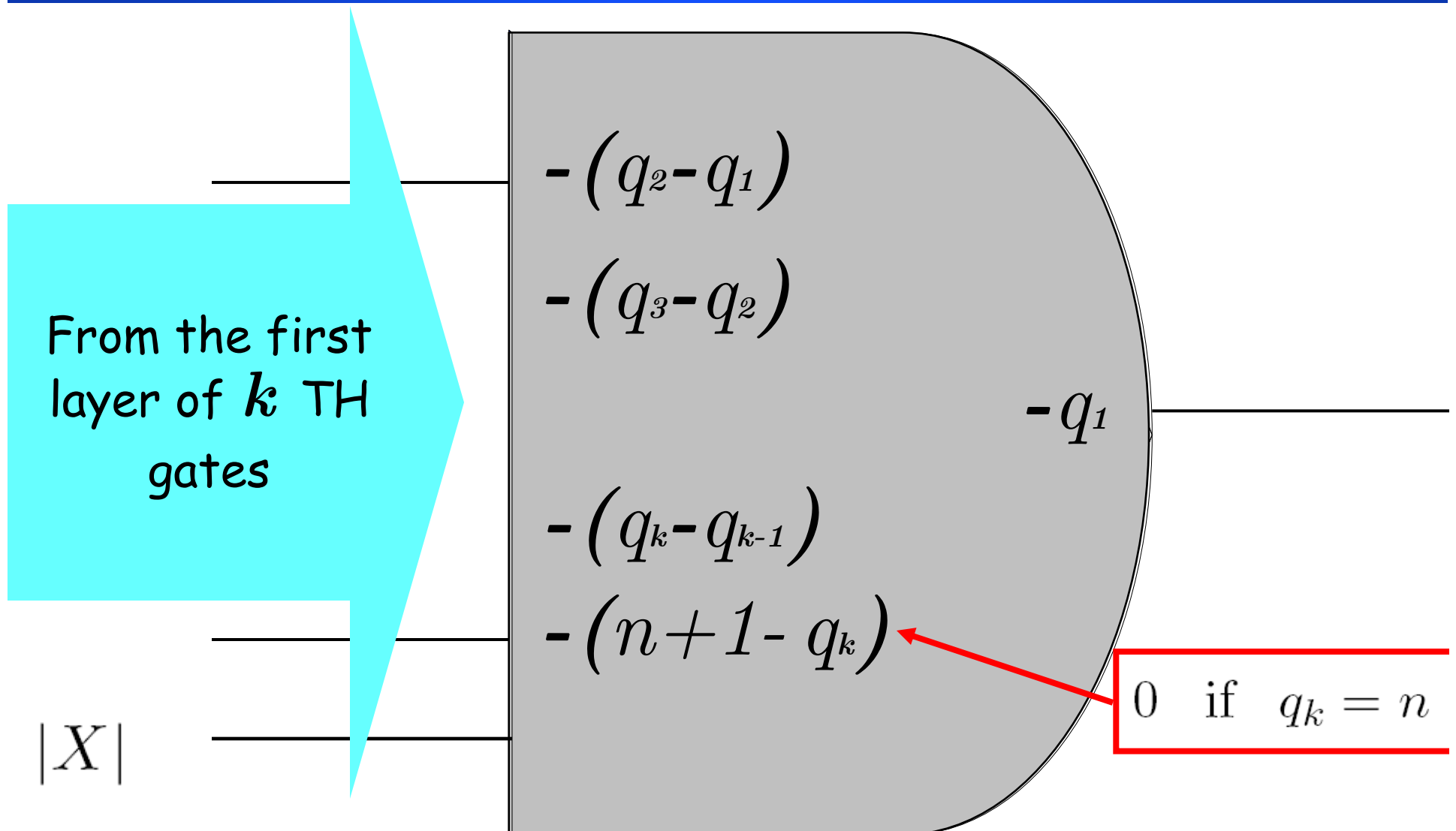
$ X $	$f(X)$
0	0
1	1
2	0
3	1
4	1
5	0
6	1
7	1

LT-nl Construction

Minnick 1959

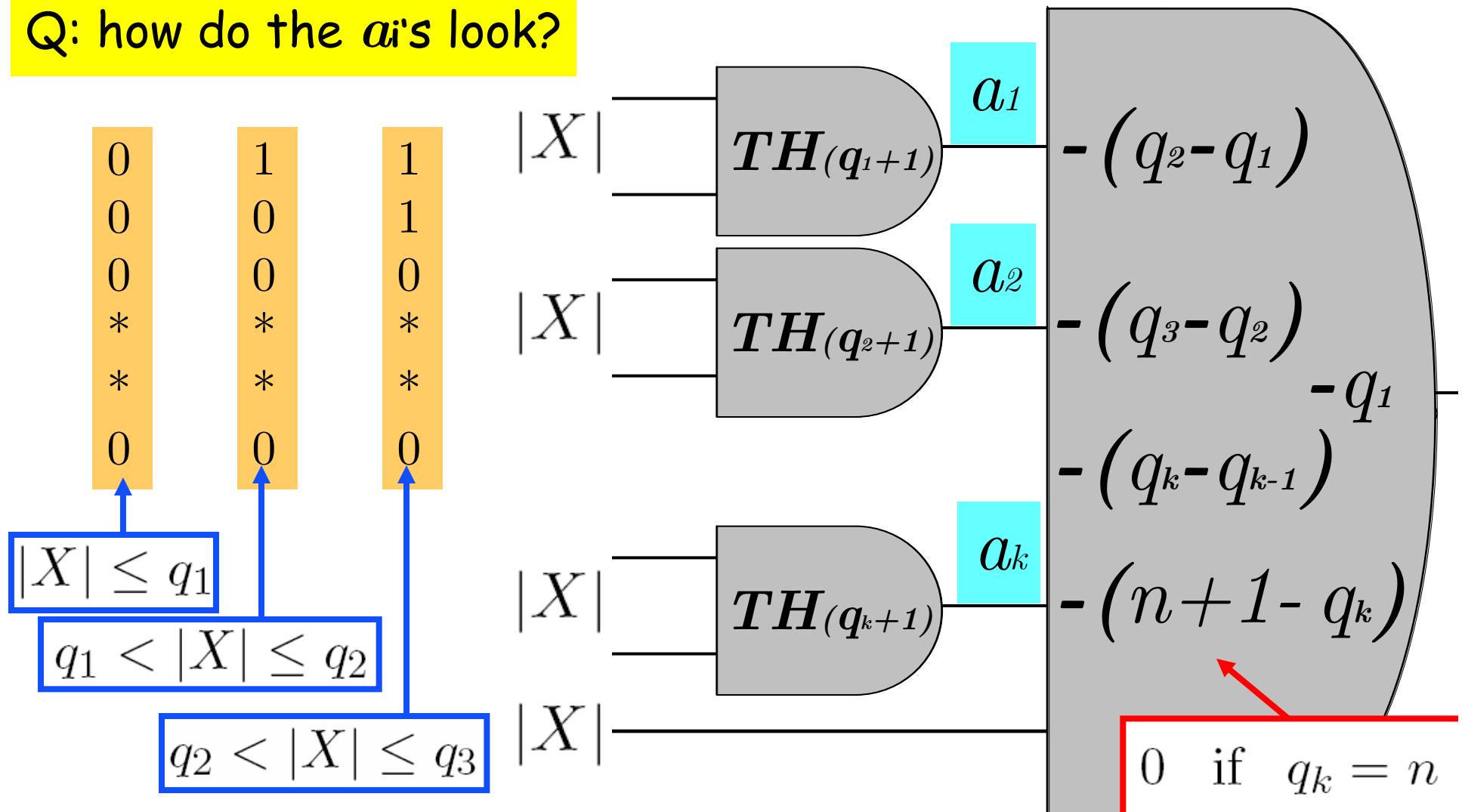


The Gate M



$$F(X) = - \left(q_1 + \sum_{i=1}^{k-1} a_i (q_{i+1} - q_i) + a_k (n + 1 - q_k) \right) + |X|$$

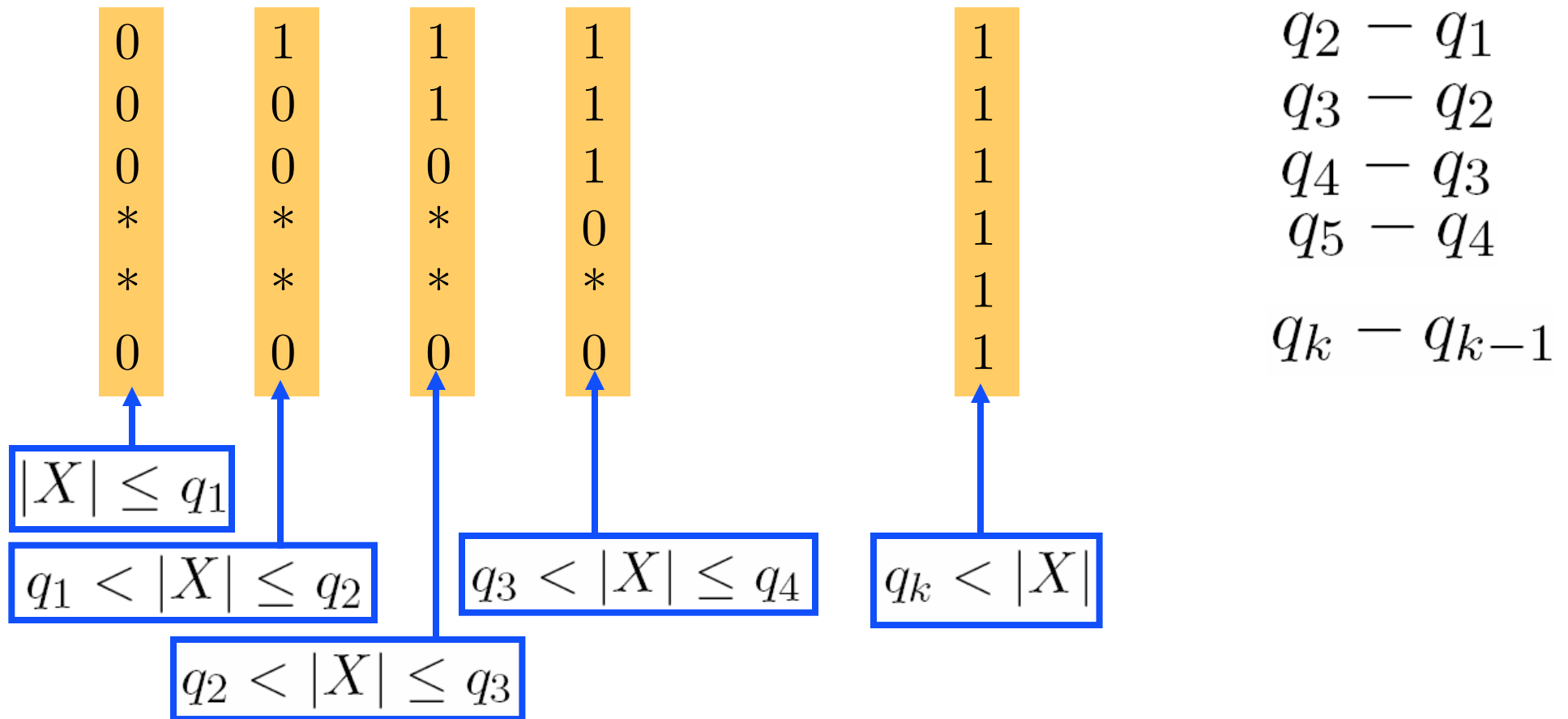
Q: how do the a_i 's look?



$$F(X) = - \left(q_1 + \sum_{i=1}^{k-1} a_i (q_{i+1} - q_i) + a_k (n + 1 - q_k) \right) + |X|$$

???

What was Minnick's key idea?



The Key: Telescopic Sum

$$q_4 < |X| \leq q_5$$

$$a_1 = 1$$

$$a_2 = 1$$

$$a_3 = 1$$

$$a_4 = 1$$

$$a_5 = 0$$

1

1

1

1

0

0

*

0

~~q_1~~

~~$q_2 - q_1$~~

~~$q_3 - q_2$~~

~~$q_4 - q_3$~~

~~$q_5 - q_4$~~

$$F(X) = -q_5 + |X|$$

We are always left with the last element in the sum

$$F(X) = - \left(q_1 + \sum_{i=1}^{k-1} a_i (q_{i+1} - q_i) + a_k (n + 1 - q_k) \right) + |X|$$

The Minnick Construction

Claim: The Minnick construction is correct

Proof:

$$F(X) = - \left(q_1 + \sum_{i=1}^{k-1} a_i (q_{i+1} - q_i) + a_k (n + 1 - q_k) \right) + |X|$$

Consider $|X|$ in each possible range:

$F(X)$ is 0 for all the upper bounds of the ranges and negative otherwise

Q

$$\begin{array}{ll} 0 \leq |X| \leq q_1 & F(X) = -q_1 + |X| \\ q_1 < |X| \leq q_2 & F(X) = -q_2 + |X| \\ q_2 < |X| \leq q_3 & F(X) = -q_3 + |X| \\ q_3 < |X| \leq q_4 & F(X) = -q_4 + |X| \\ \vdots & \\ \vdots & \\ q_{k-1} < |X| \leq q_k & F(X) = -q_k + |X| \end{array}$$

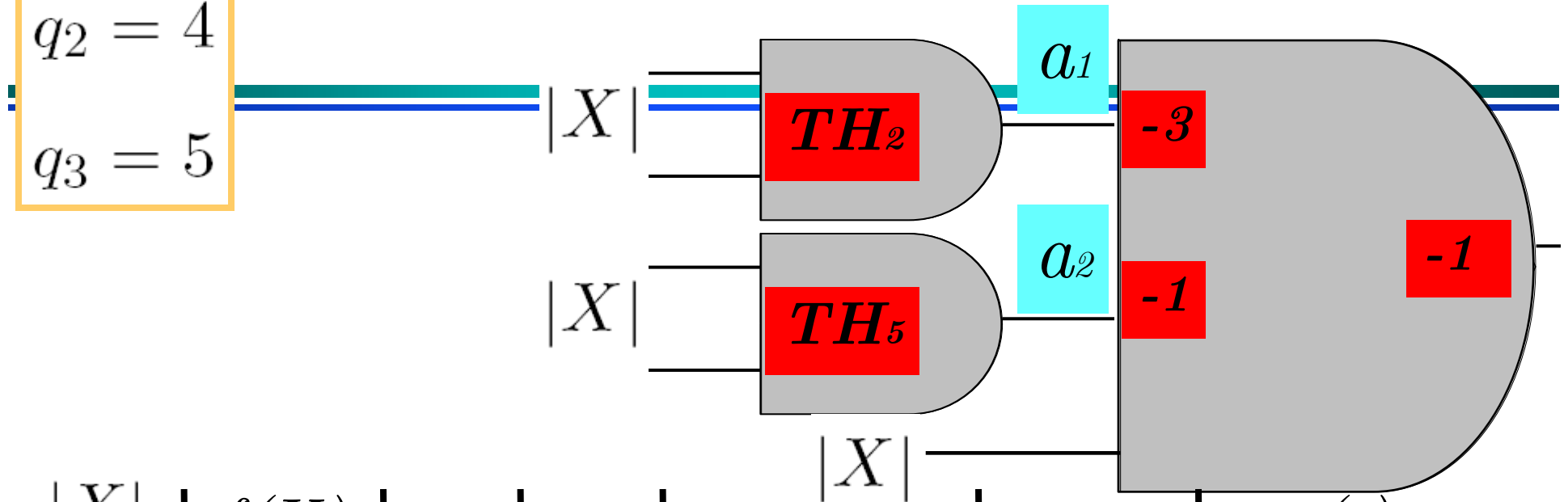
Telescopic sum

$$q_1 = 1$$

$$q_2 = 4$$

$$q_3 = 5$$

Example of Minnick's Construction



$ X $	$f(X)$	a_1	a_2	$-3a_1 - a_2 - 1$	$\dots + X $	$sgn(:)$
0	0	0	0	-1	-1	0
1	1	0	0	-1	0	1
2	0	1	0	-4	-2	0
3	0	1	0	-4	-1	0
4	1	1	0	-4	0	1
5	1	1	1	-5	0	1

The Kautz Construction for XOR

1961

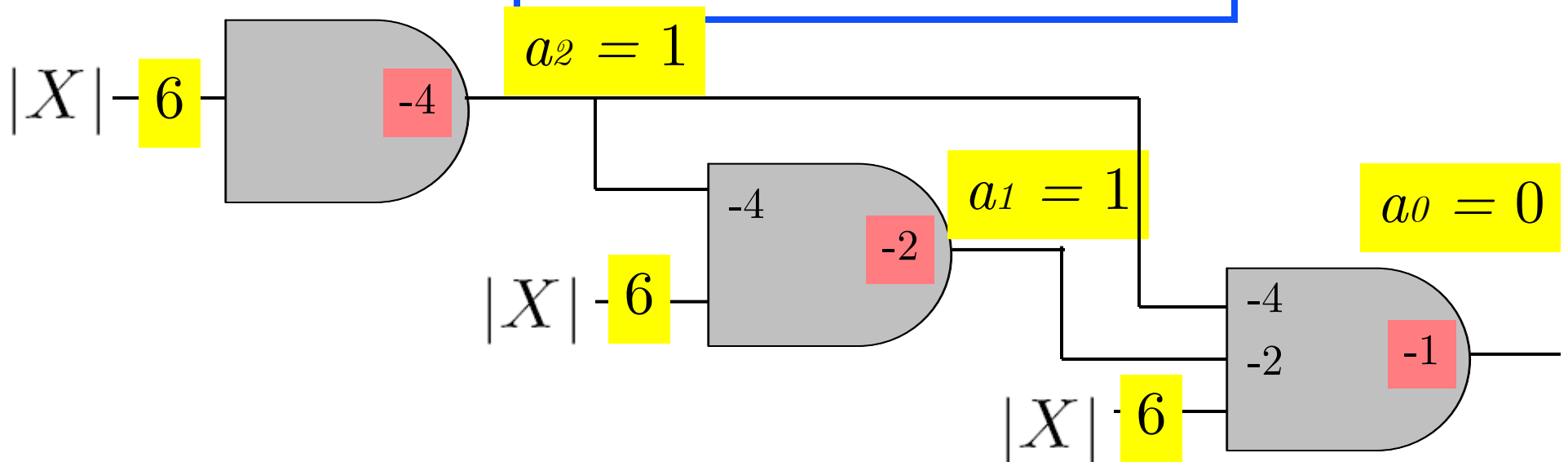
Implement the algorithm for computing the binary representation using LT gates

Algorithm: $A \leftarrow m$

For $i = j - 1$ to 0 do:

{ if $A \geq 2^i$ then $a_i = 1$
else $a_i = 0$

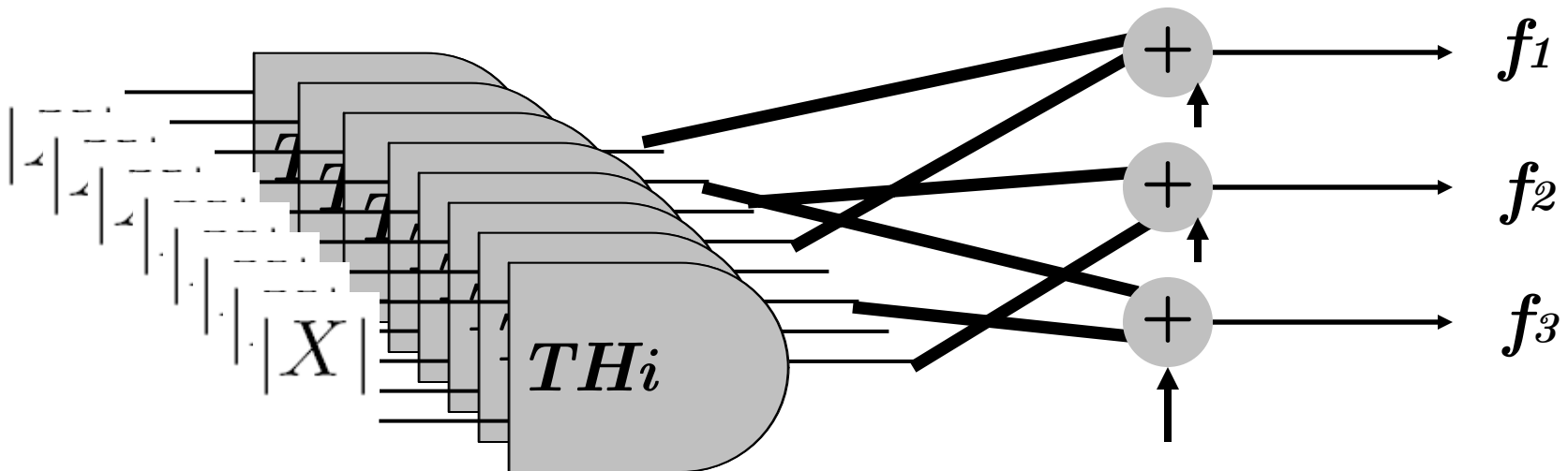
$A \leftarrow A - a_i 2^i$ }



Questions on LT Constructions

Q1: We understand how to implement a **single** symmetric function, what if we need to implement a circuit that computes a **number** of symmetric functions? Can we save in circuit size?

A1: YES - we can 'reuse' the first layer! By putting all required TH gates.



Questions on LT Constructions



Q2: Why do we care about **symmetric** functions?

What about **general** Boolean functions?

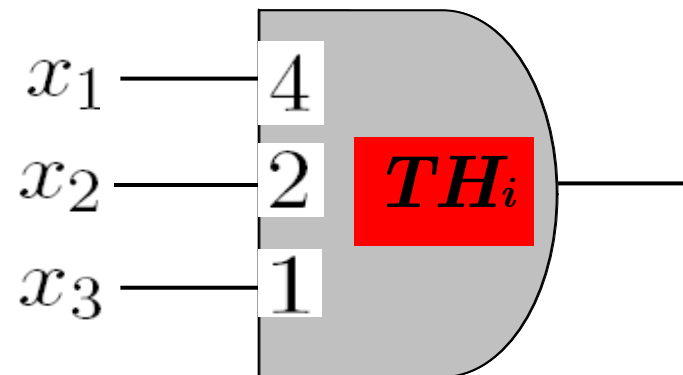
A2: A general Boolean function can be treated as a symmetric function by introducing **linear ordering**

$x_1x_2x_3$	$f(x_1, x_2, x_3)$	4 2 1
000	1	0
001	0	1
010	0	2
011	1	3
100	1	4
101	1	5
110	0	6
111	0	7

5 gates with DNF

4 gates with LT-I

3 gates with LT-nl



0	0
1	1
10	2
11	3
100	4
101	5
110	6
111	7
1000	8
1001	9
1010	10
1011	11
1100	12
1101	13
1110	14
1111	15
10000	16
10001	17
10010	18
10011	19
10100	20
10101	21
10110	22
10111	23
11000	24
11001	25
11010	26
11011	27
11100	28
11101	29
11110	30
11111	31
100000	32
etc.	etc

LT Constructions for Symmetric Functions

What do we know about
AON (AND, OR, NOT)
circuits?

circuit kind	size
LT-I	$n + 1$
LT-nl, d-2	$\left\lfloor \frac{n}{2} \right\rfloor + 1$
LT-nl -XOR	$\lceil \log_2(n + 1) \rceil$

transitions

Muroga

intervals

Minnick

Binary representations

Kautz

optimal

DNF Theorem

DNF Theorem:

Every Boolean function can be expressed in DNF.

$$\begin{aligned}\overline{(a \cdot \bar{b} + a \cdot c)} + \bar{a} &= \overline{(a \cdot \bar{b})} \cdot \overline{(a \cdot c)} + \bar{a} \\ &= (\bar{a} + b)(\bar{a} + \bar{c}) + \bar{a} \\ &= \bar{a} + b \cdot \bar{c} + \bar{a} \\ &= \bar{a} + b \cdot \bar{c}\end{aligned}$$

Absorption:

- A2. Complements:
 $a + \bar{a} = 1$ and $a \cdot \bar{a} = 0$

- T4. DeMorgan Laws:

$$\begin{aligned}\overline{(a + b)} &= \bar{a} \cdot \bar{b} \\ \overline{(a \cdot b)} &= \bar{a} + \bar{b}\end{aligned}$$

- A4. Distributivity:

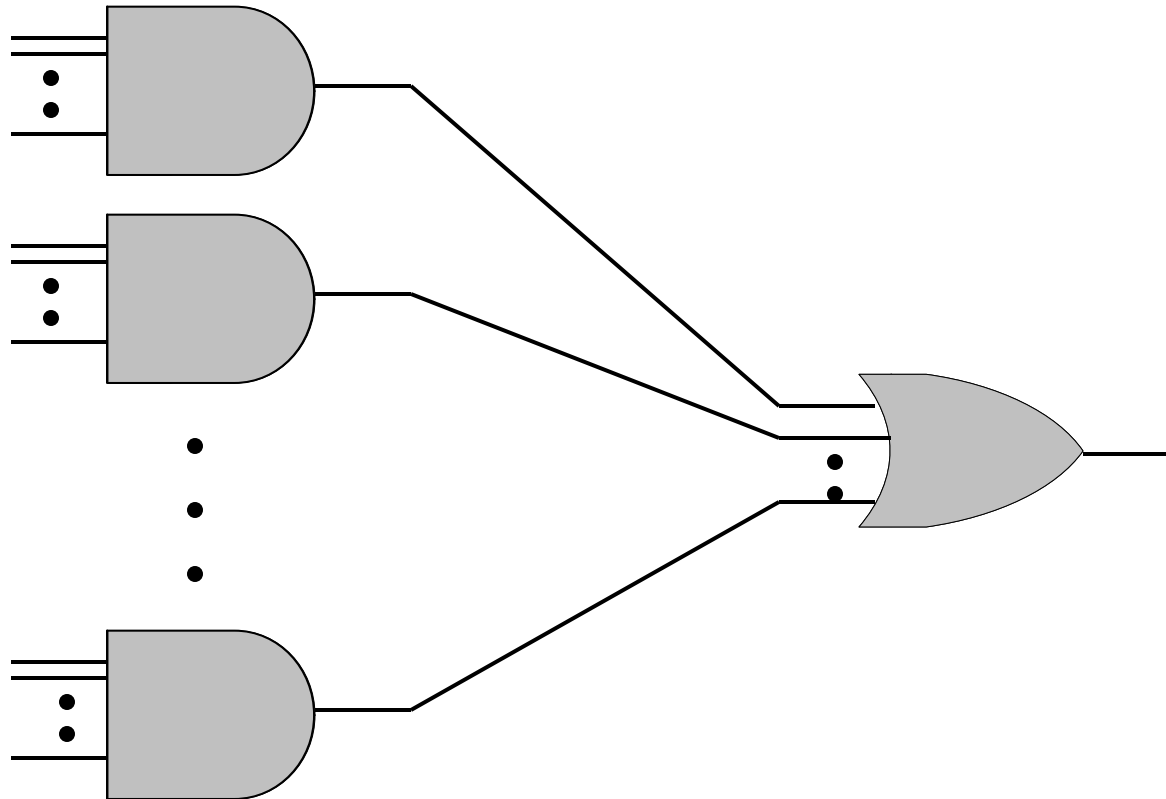
$$a + b \cdot c = (a + b) \cdot (a + c) \quad \text{and} \quad a \cdot (b + c) = a \cdot b + a \cdot c$$

$$\begin{aligned}&= \bar{a} \cdot (b + \bar{b}) \cdot (c + \bar{c}) + b \cdot \bar{c} \cdot (a + \bar{a}) \\ &= \bar{a} \cdot b \cdot c + \bar{a} \cdot b \cdot \bar{c} + \bar{a} \cdot \bar{b} \cdot c + \bar{a} \cdot \bar{b} \cdot \bar{c} + a \cdot b \cdot \bar{c} + \bar{a} \cdot b \cdot \bar{c} \\ &= \bar{a} \cdot b \cdot c + \bar{a} \cdot b \cdot \bar{c} + \bar{a} \cdot \bar{b} \cdot c + \bar{a} \cdot \bar{b} \cdot \bar{c} + a \cdot b \cdot \bar{c}\end{aligned}$$

Every 0-1 Boolean Function Can be Implemented Using A Depth Two Circuit

How?

Implement the DNF representation: *OR* of many *AND*s



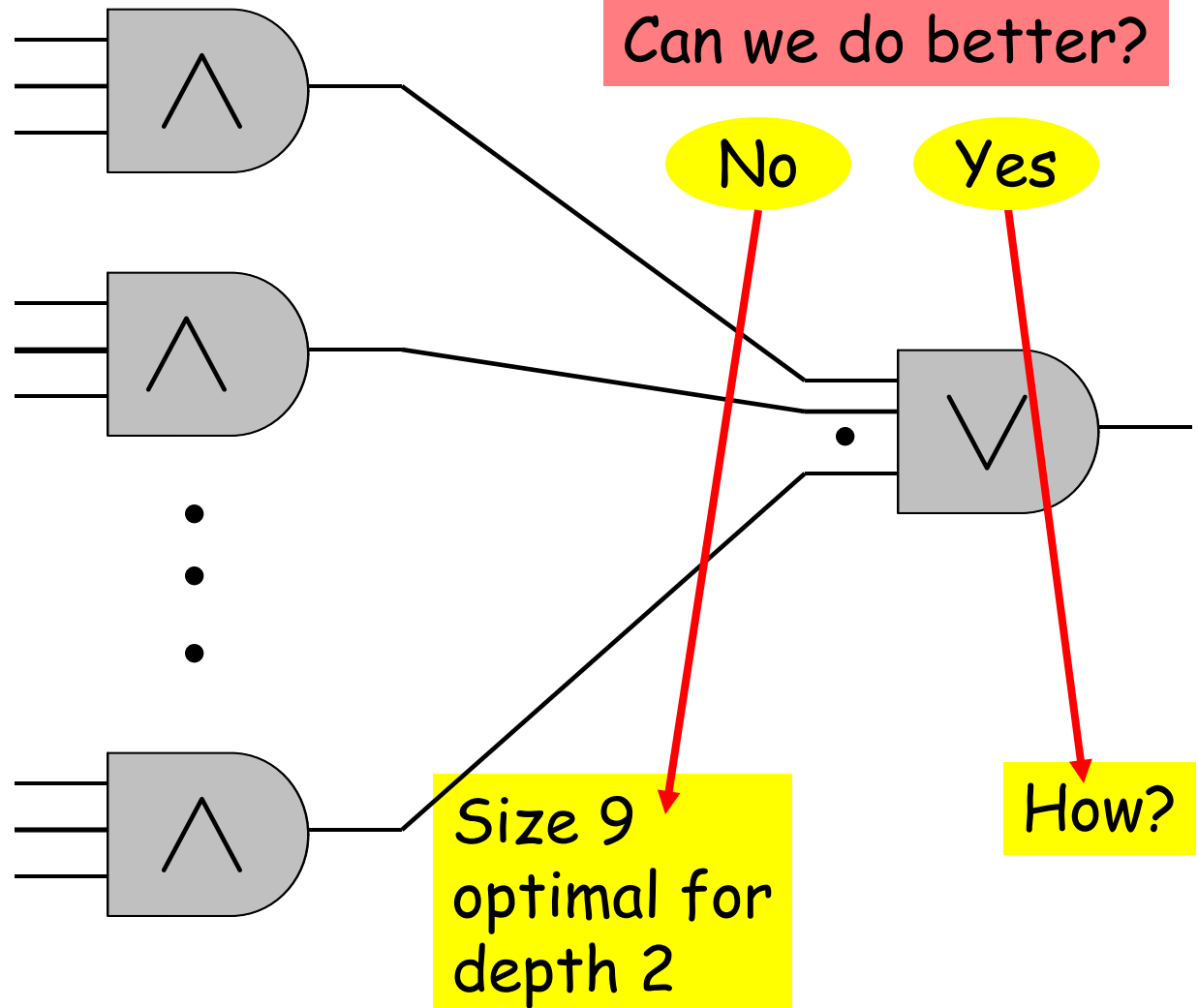
XOR of Four Variables with AON

Depth = 2

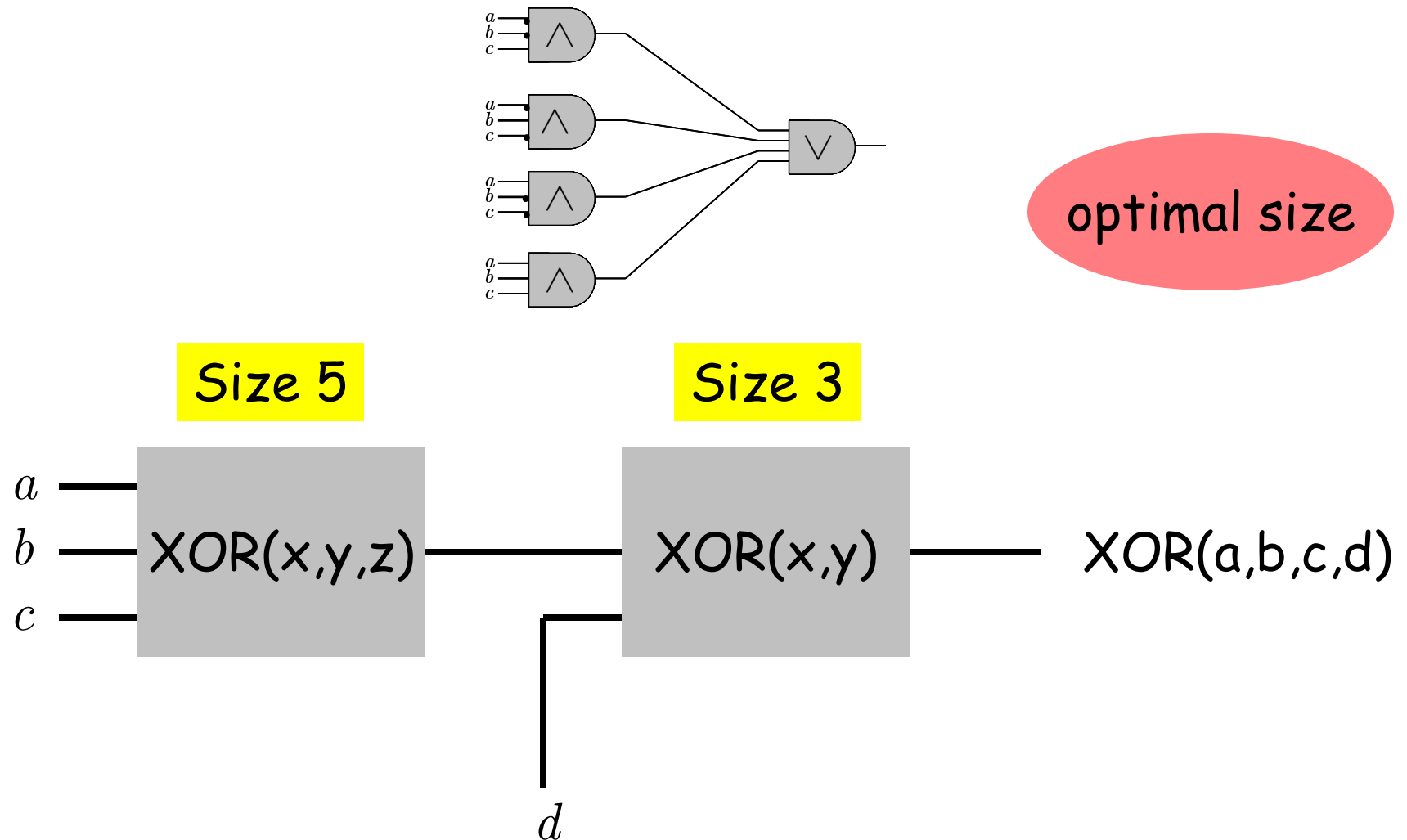
Size = 9

4 *AND*s for $|X| = 1$

4 *AND*s for $|X| = 3$



Size 8 AON Circuit for XOR of Four Variables



AON Constructions for XOR

$n=4$

	circuit kind	size	
9	AON, d-2	$2^{n-1} + 1$	optimal
8	AON	$\lceil 2.5(n-1) \rceil$	

lower bound: $2n - 1$

maybe optimal

Dept-2 AON Circuit for XOR

Theorem: An optimal size depth-2 AON circuit for $XOR(x_1, x_2, \dots, x_n)$ has $2^{n-1} + 1$ gates

Proof:

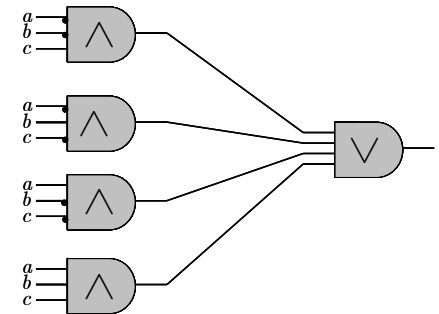
The construction follows from the DNF representation:
 2^{n-1} normal terms + one OR gate

Lower bound: **WLOG** 

???

(i) Every **AND** gate must have all n inputs

(ii) Every **AND** gate computes a normal term
DNF is a representation, hence,
there are 2^{n-1} **AND** gates



Depth-2 AON Circuit for XOR

Theorem: An optimal size depth-2 AON circuit for $XOR(x_1, x_2, \dots, x_n)$ has $2^{n-1} + 1$ gates

Proof (cont):

Need to prove: (i) Every **AND** gate must have all n inputs

By contradiction: Assume that there is a gate G with $n-1$ inputs. Say x_1 is missing From G

Assume that: $G(\hat{x}_2, \hat{x}_2, \hat{x}_3, \dots, \hat{x}_n) = 1$

Hence, the output of the circuit is 1 (the **OR** gate has 1-input)

Note that for both assignments the output of the circuit is 1:

Q

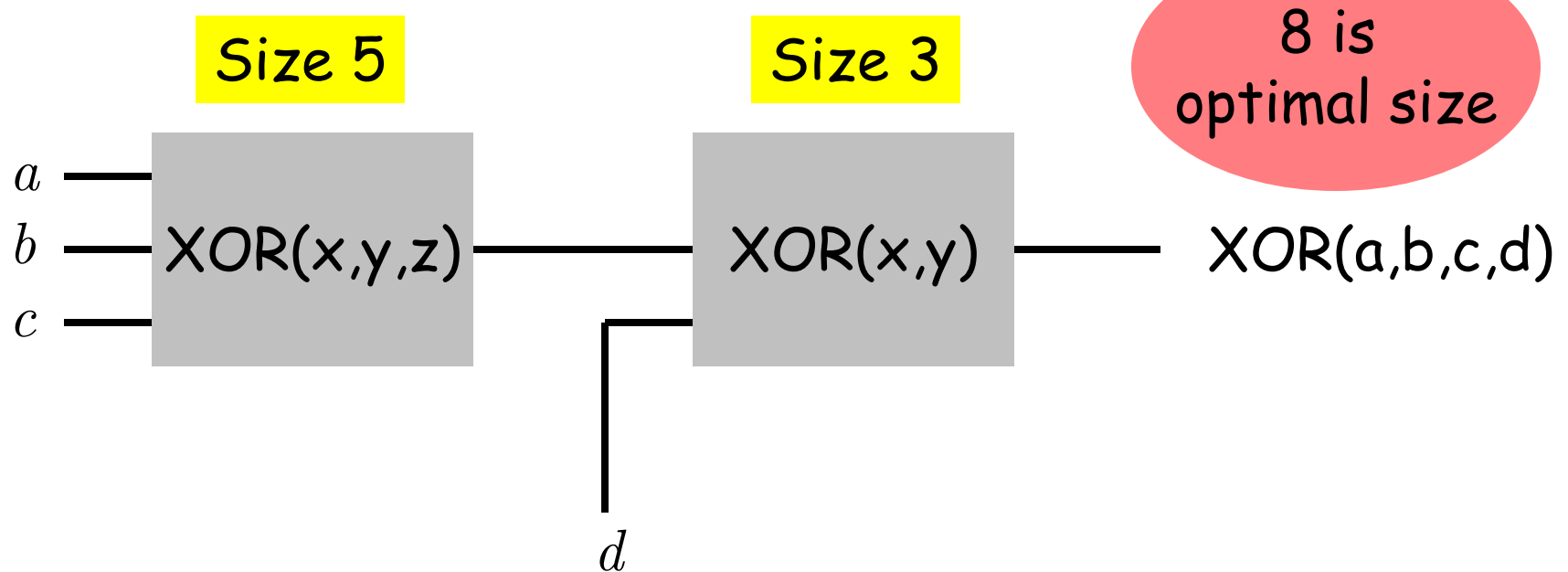
$(0, \hat{x}_2, \hat{x}_2, \hat{x}_3, \dots, \hat{x}_n)$ $(1, \hat{x}_2, \hat{x}_2, \hat{x}_3, \dots, \hat{x}_n)$

Contradiction!! Those assignments have different parities

AON Constructions for XOR

n=4	circuit kind	size	
9	AON, d-2	$2^{n-1} + 1$	optimal
8	AON	$\lceil 2.5(n-1) \rceil$	
	lower bound:	$2n - 1$	maybe optimal

Size 8 AON Circuit for XOR of Four Variables



Idea:

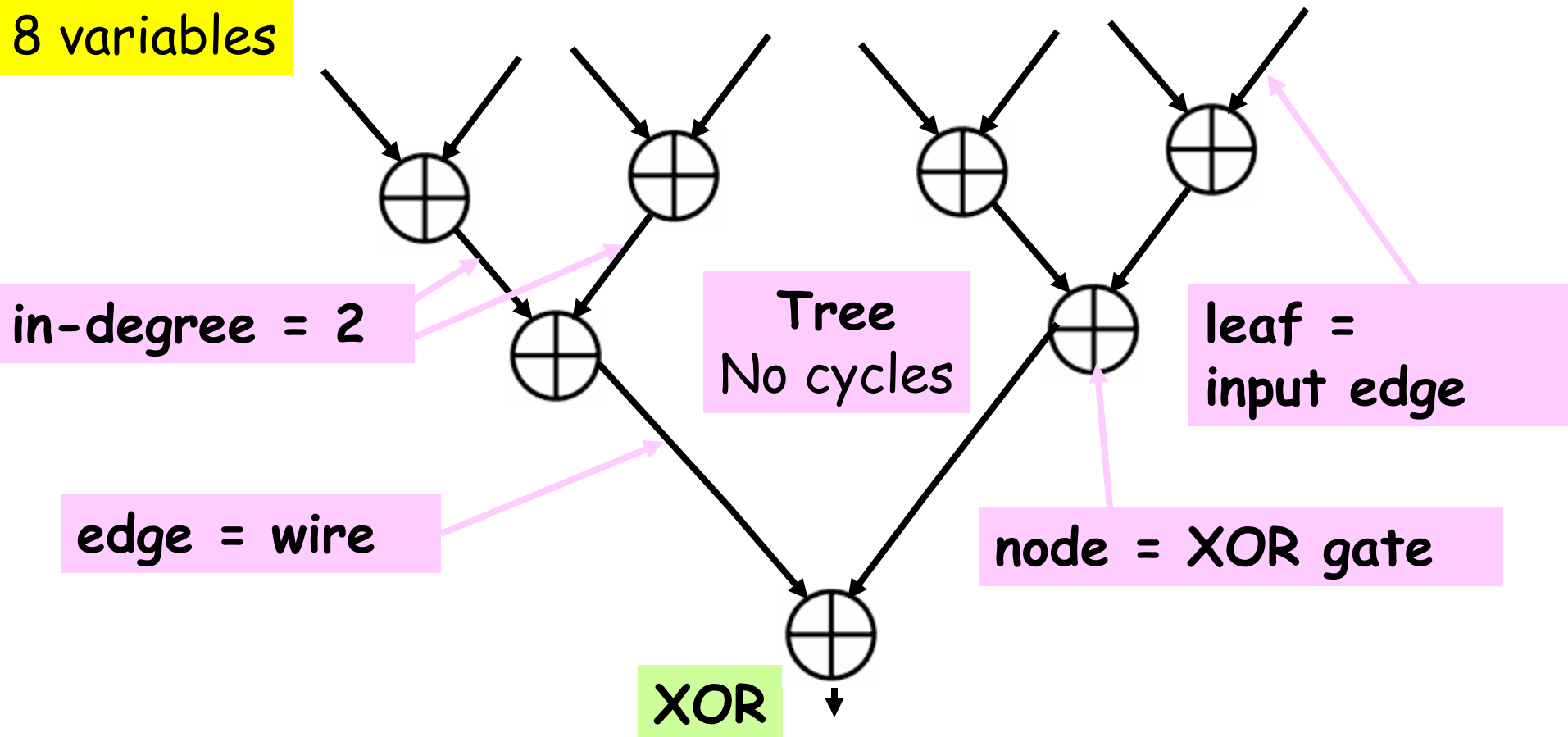
Compute a large XOR by using a circuit of small XOR gates

AON Circuit for XOR

Idea:

Compute a **large** XOR by using a circuit of **small** XOR gates

8 variables



AON Circuit for XOR

Idea:

Compute a **large** XOR by using a circuit of **small** XOR gates

8 variables

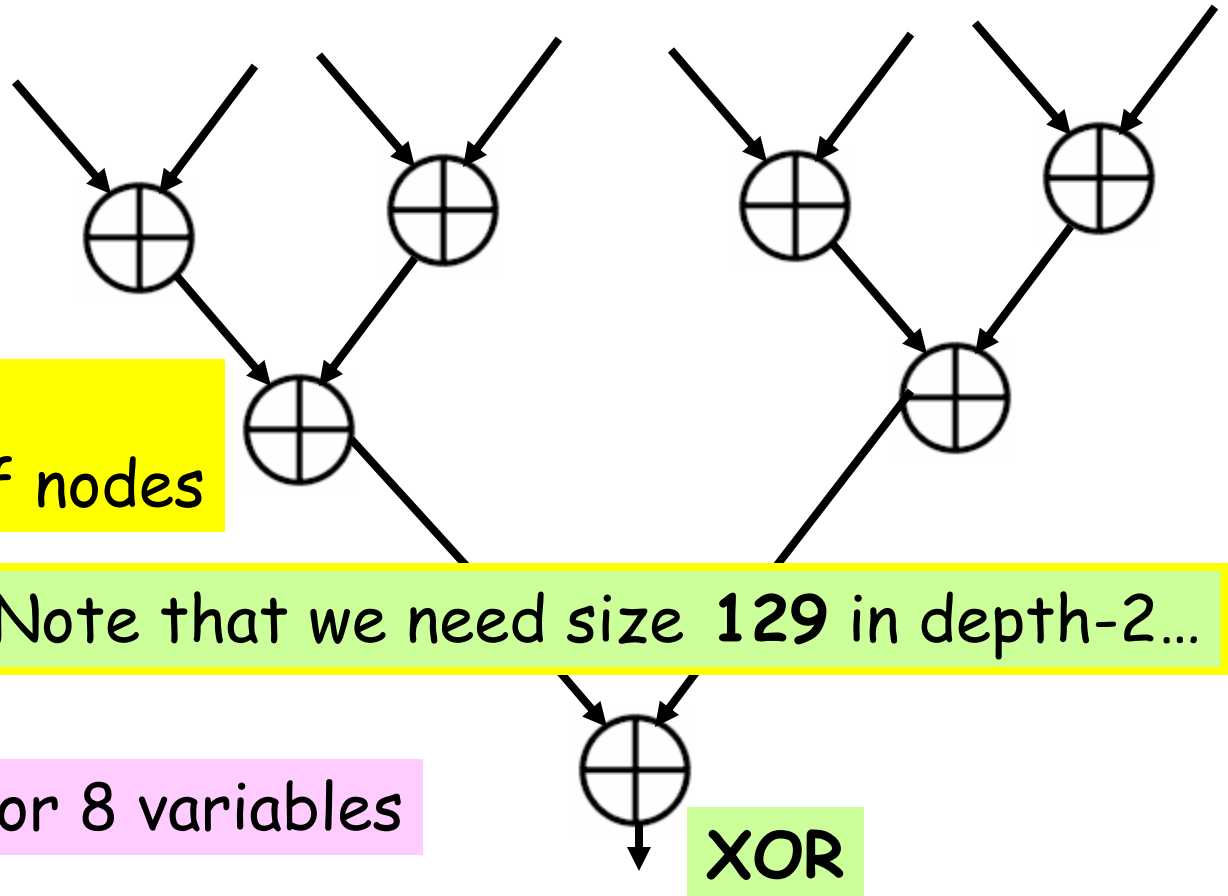
Circuit **size**
in AON gates?

Size =
Node size **X** number of nodes

$$3 \times 7 = 21$$

Note that we need size **129** in depth-2...

Q: Can we do better for 8 variables



AON Circuit for XOR

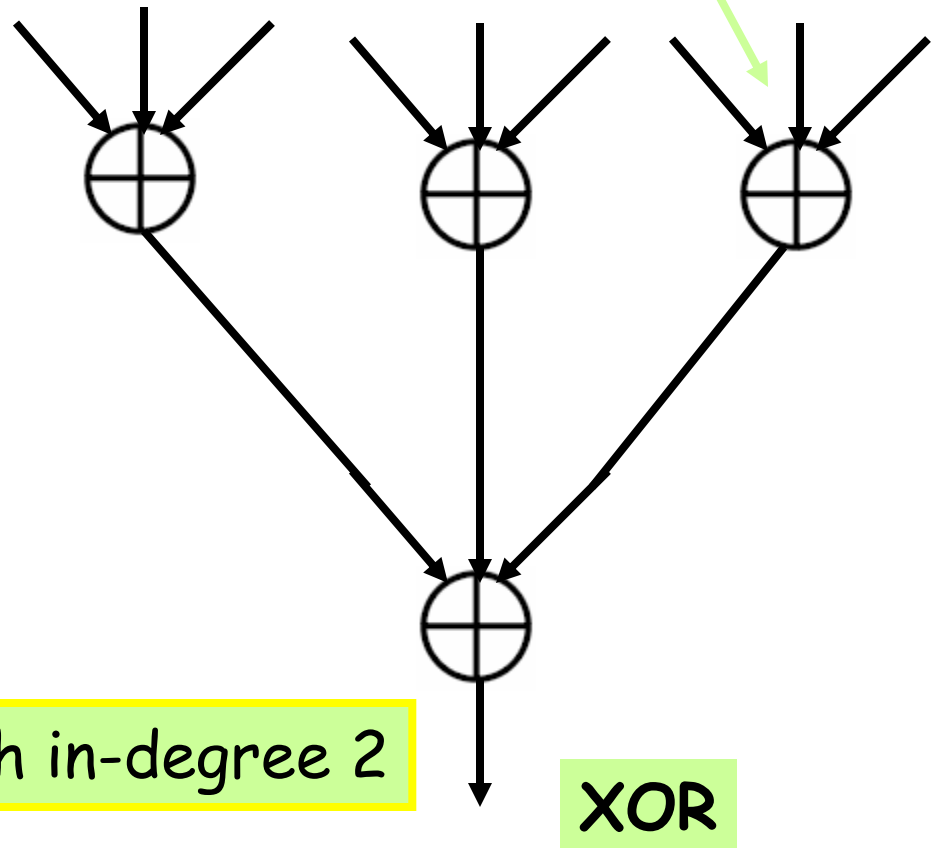
Idea: Use a larger in-degree?

9 variables

Size =
Node size $\times$ number of nodes

$$5 \times 4 = 20$$

Size 18 for 8 variables



Note that we need size 21 with in-degree 2

AON Circuit for XOR

Idea: Use a larger in-degree?

$$2^{d-1} + 1$$

$$k = \frac{n - 1}{d - 1}$$

Circuit size = (node size in AON gates) $\times$ (number of nodes)

Both are functions of the in-degree d and the number of variables n (leaves)

Lemma: a tree with in-degree d and with k nodes has
 $n = k(d-1) + 1$ leaves

Proof:

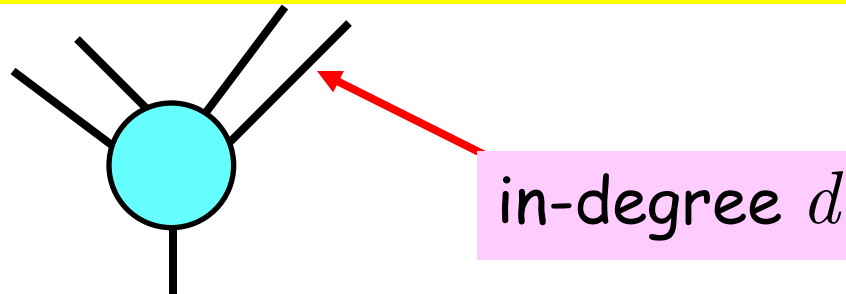
Idea: induction on k ; the number of nodes in the tree

AON Circuit for XOR

Lemma: a tree with in-degree d and with k nodes has
 $n = k(d-1) + 1$ leaves

Proof: **Idea:** induction on k ; the number of nodes in the tree

$k=1$



in-degree d

Assume true for $k=m$: $n = m(d-1) + 1$

How many leaves we add when we attach a new node? $(d-1)$

Hence, for $k=m+1$: $n = m(d-1) + 1 + (d-1)$
 $= (m+1)(d-1) + 1$

Q

AON Circuit for XOR

Lemma: a tree with in-degree d and with k nodes has
 $n = k(d-1) + 1$ leaves

Circuit size = (node size in AON gates) $\times$ (number of nodes)

$$2^{d-1} + 1$$

$$k = \frac{n-1}{d-1}$$

$$\text{Circuit size} = (2^{d-1} + 1) \times \frac{n-1}{d-1} = \frac{2^{d-1} + 1}{d-1} \times (n-1)$$

Optimal for $d=3$

d	
2	3
3	2.5
4	3
5	4.25

Number of inputs is given

Find an optimal d

AON Circuit for XOR

Claim: Given a **regular XOR circuit** (same in-degree for all XOR gates), the optimal circuit size for XOR of n variables is: $\lceil 2.5(n - 1) \rceil$

d	$\frac{2^{d-1} + 1}{d - 1}$
2	3
3	2.5
4	3
5	4.25

Q: Is it optimal?

A1: maybe? We do not know...

A2: we know how to prove a lower bound of $2n-1$ using the **forcing-elimination-reverse** induction approach

AON Circuit for XOR

We have a construction of size $\lceil 2.5(n - 1) \rceil$
we know how to prove a lower bound of $2n - 1$

n	$2n - 1$	$\lceil 2.5(n - 1) \rceil$
2	3	3
3	5	5
4	7	8
5	9	10
6	11	13
7	13	15
8	15	18

Matt Cook proved that an
AON circuit of **size 7**
for XOR does not exist
he used a **computer search**

AON Circuit for XOR

We have a construction of size $\lceil 2.5(n - 1) \rceil$
we know how to prove a lower bound of $2n - 1$

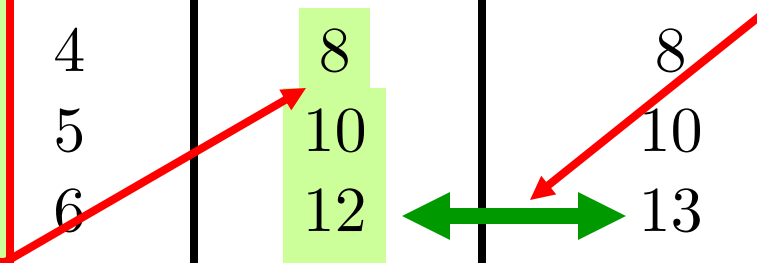
Matching upper/lower
bounds = **MSc in CS**

Matt Cook proved that an
AON circuit of size 7
for XOR does not exist
he used a computer search

Prove Matt's result
wo/computer search
and get A+ in class

n	$2n - 1$	$\lceil 2.5(n - 1) \rceil$
2	3	3
3	5	5
4	8	8
5	10	10
6	12	13
7	14	15
8	16	18

next gap



AON/ LT Constructions for Symmetric Functions

XOR		circuit kind	size
circuit kind	size	LT-I	$n + 1$
AON, d-2	$2^{n-1} + 1$	LT-nl, d-2	$\left\lfloor \frac{n}{2} \right\rfloor + 1$
AON	$\lceil 2.5(n-1) \rceil$	LT-nl-XOR	$\lceil \log_2(n+1) \rceil$

Exponential improvement in size using LT gates

AON/ LT Constructions for Arithmetic Functions

Q: for polynomial size circuit, what is the smallest depth?

For the details, see paper on class web site: Siu and B., 1990

For integers with n bits	Function	AON	LT
	Addition: $A+B$	3	2
	Product: $A \times B$	$O(\log_2 n)$	3
n integers	Sorting	$O(\log_2 n)$	3

CNS 188a Overview

- Boolean algebra as an axiomatic system
- Boolean functions and their representations using Boolean formulas and spectral methods
- Implementing Boolean functions with relay circuits, circuits of AON (AND, OR, NOT) gates and LT (Linear Threshold) gates
- Analyzing the complexity (size and depth) of circuits
- Relations (as opposed to functions) and their implementation in circuits
- Feedback and convergence in LT circuits

Spectral Analysis of Boolean Functions

Q: why bother?

- Upper and lower bounds on the size of LT circuits
- Synthesis techniques for LT circuits
- Linear vs. Polynomial threshold functions
- Best known learning algorithm for Boolean functions

Representations of Boolean Functions

We will represent the 0 element by 1
and the 1 element by -1

$$a \mapsto (-1)^a$$

$$f : \{1, -1\}^n \mapsto \{1, -1\}$$

The AND function of two variables:

DNF: $f(x_1, x_2) = x_1 \cdot x_2$

Truth table:

x_1x_2	$f(x_1, x_2)$
11	1
1-1	1
-11	1
-1-1	-1

LT function:

$$f(x_1, x_2) = \text{sgn}(1 + x_1 + x_2)$$

x_1x_2	$\downarrow$
11	3
1-1	1
-11	1
-1-1	-1

The star of the Show: Polynomial Representation

$$f(x_1, x_2) = \frac{1}{2}(1 + x_1 + x_2 - x_1x_2)$$

$$f(1, 1) = \frac{1}{2}(1 + 1 + 1 - 1) = 1$$

$$f(1, -1) = \frac{1}{2}(1 + 1 - 1 + 1) = 1$$

$$f(-1, 1) = \frac{1}{2}(1 - 1 + 1 + 1) = 1$$

$$f(-1, -1) = \frac{1}{2}(1 - 1 - 1 - 1) = -1$$

AND

The star of the Show: Polynomial Representation

$$f(x_1, x_2) = \frac{1}{2}(1 + x_1 + x_2 - x_1x_2)$$

$$\frac{1}{2} \quad \frac{1}{2} \quad \frac{1}{2} \quad -\frac{1}{2}$$

The spectrum
is the set of the coefficients of the polynomial representation

Important fact: it works for arbitrary Boolean functions