Direct Products in Communication Complexity

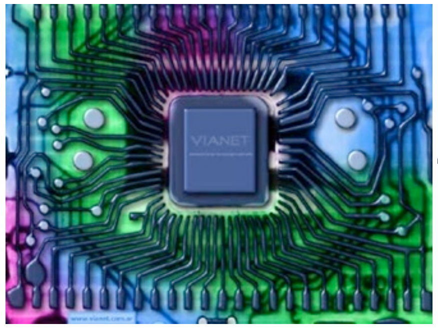



Mark Braverman, Anup Rao, Omri Weinstein, Amir Yehudayoff

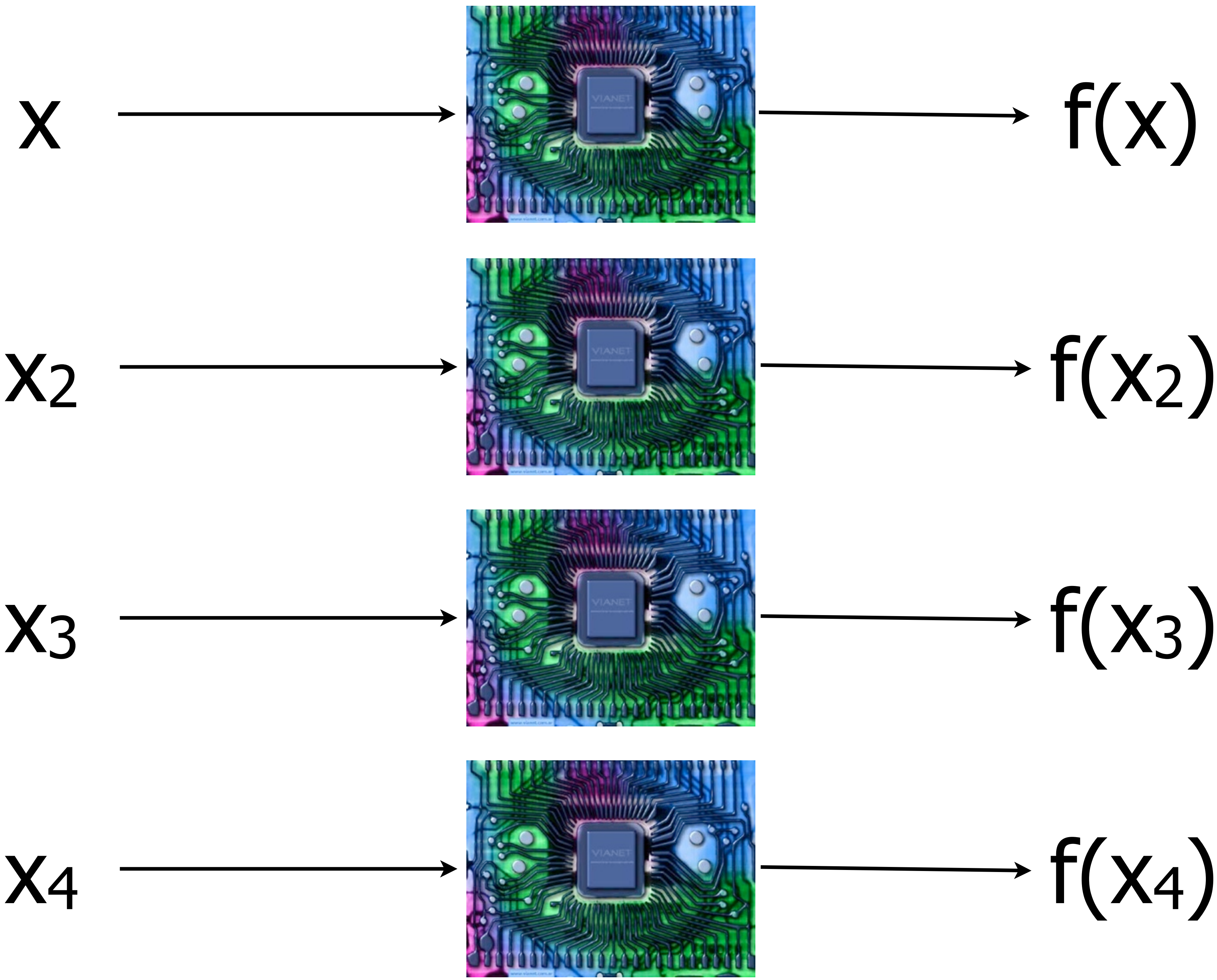
Princeton Washington Princeton Technion

Direct Sums

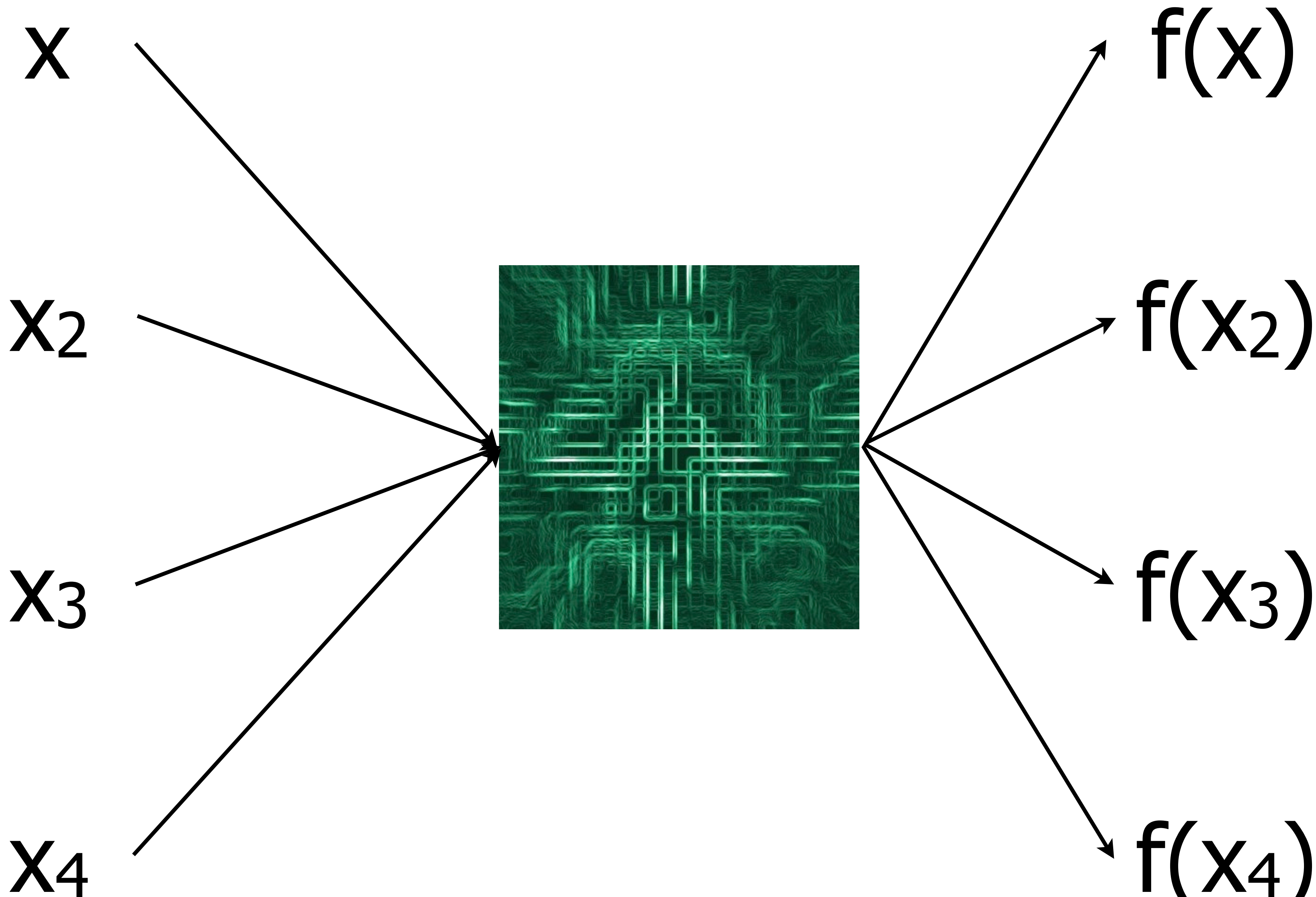
Direct Sums

x →  → f(x)

Direct Sums



Direct Sums



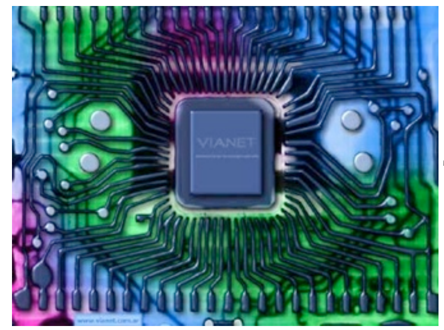
Direct Products

Success Probability

Random input

0.9

Direct Products

Random input x →  → $f(x)$

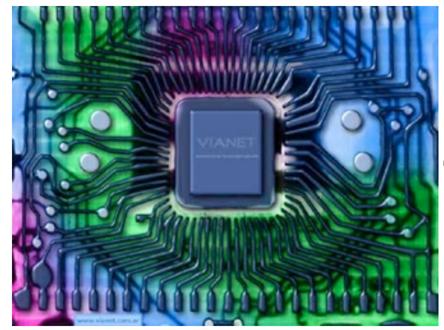
Success Probability
0.9

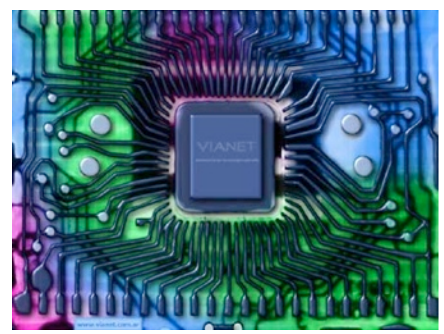
Wednesday, February 20, 13

Direct Products

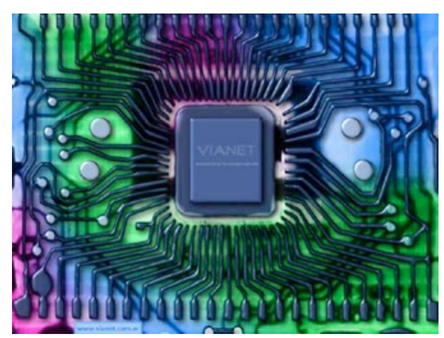
Success Probability

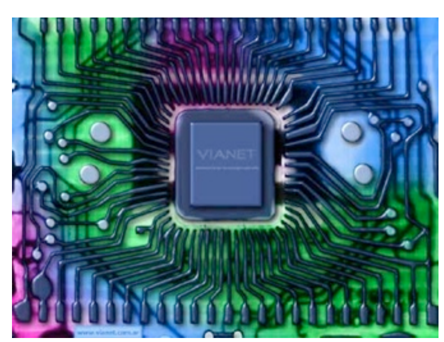
Random input

x →  → $f(x)$

x_2 →  → $f(x_2)$

0.9^n

x_3 →  → $f(x_3)$

x_4 →  → $f(x_4)$

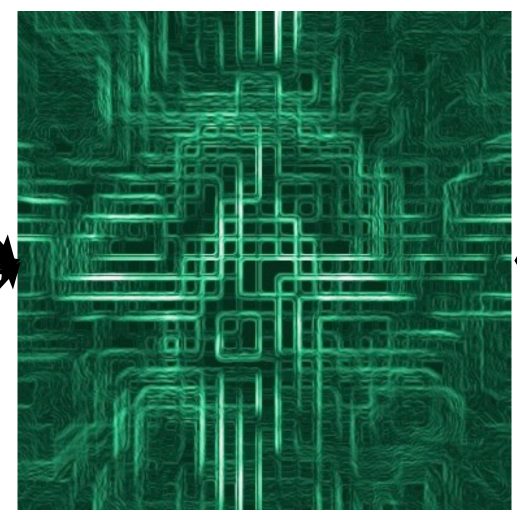
Direct Products

Success Probability

Random input

x → $f(x)$

x_2 → $f(x_2)$



x_3 → $f(x_3)$

x_4 → $f(x_4)$

0.6

Communication Complexity

Communication [Yao]

<u>Alice</u>
X

public randomness R

<u>Bob</u>
Y

private randomness R_1

private randomness R_2

Complexity: # bits exchanged
x,y drawn from some known distribution

Communication [Yao]

public randomness R

<u>Alice</u>
X

$\xrightarrow{m_1(X,R,R_1)}$

<u>Bob</u>
Y

private randomness R_1

private randomness R_2

Complexity: # bits exchanged

x,y drawn from some known distribution

Communication [Yao]

Alice

X

public randomness R

Bob

Y

$m_1(X,R,R_1)$

$m_2(Y,M_1,R,R_2)$

private randomness R_1

private randomness R_2

Complexity: # bits exchanged

x,y drawn from some known distribution

Communication [Yao]

<u>Alice</u>

X

public randomness R

<u>Bob</u>

Y

private randomness R_1

$m_1(X,R,R_1)$ →

← $m_2(Y,M_1,R,R_2)$

→

private randomness R_2

Complexity: # bits exchanged

x,y drawn from some known distribution

Communication [Yao]

public randomness R

Alice

X

Bob

Y

private randomness R_1

private randomness R_2

$m_1(X,R,R_1)$ →

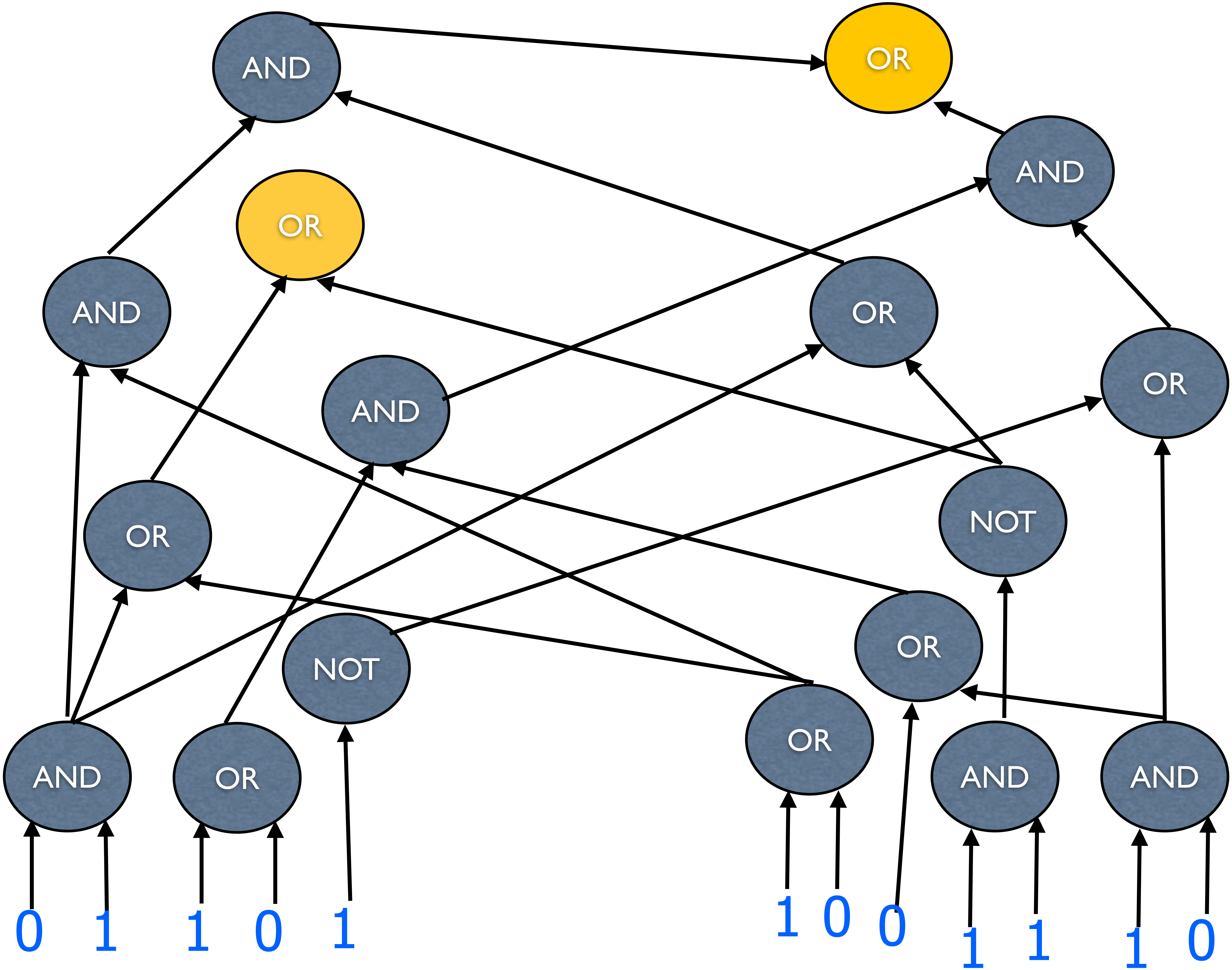
$m_2(Y,M_1,R,R_2)$ ←

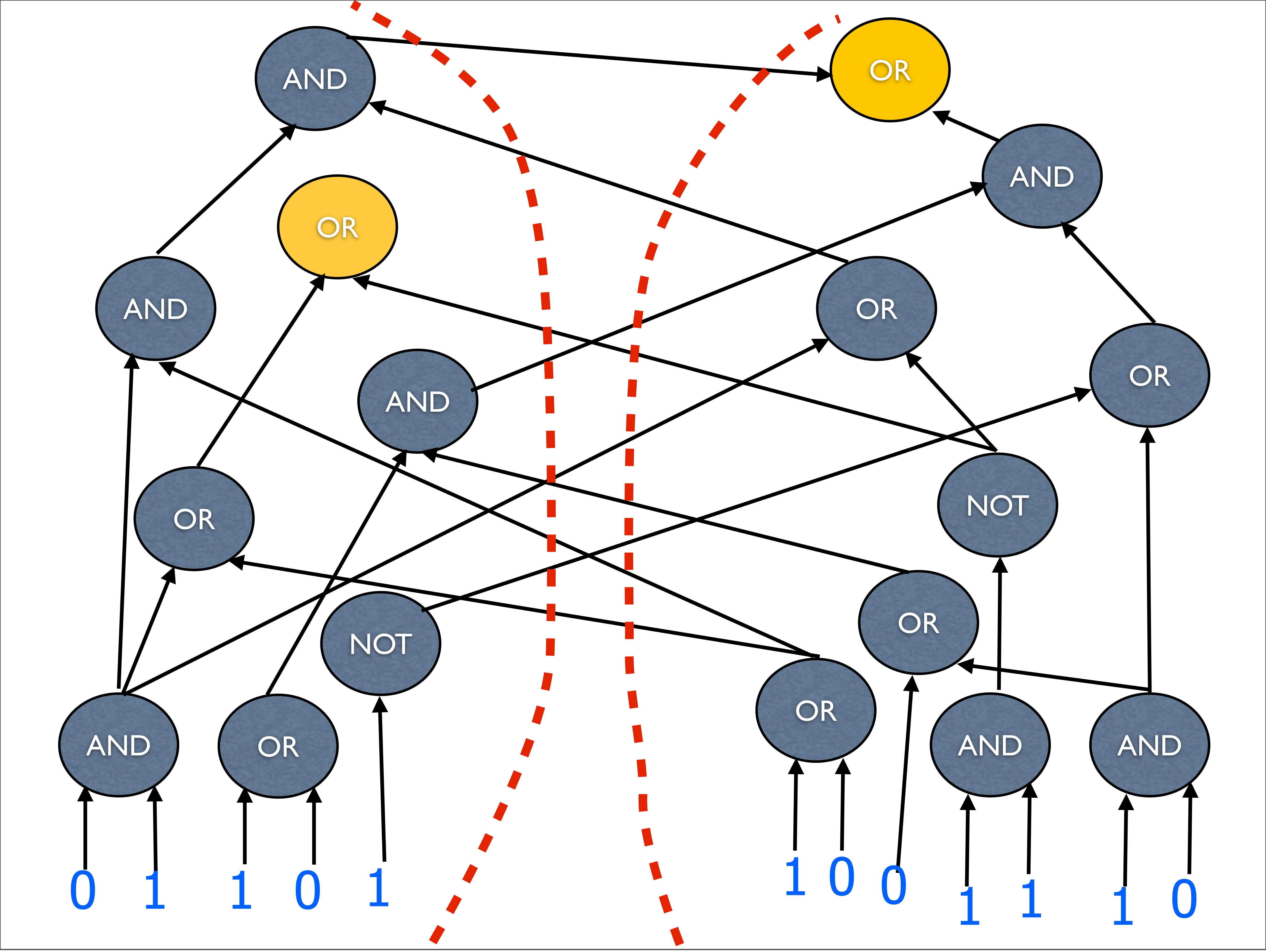
→

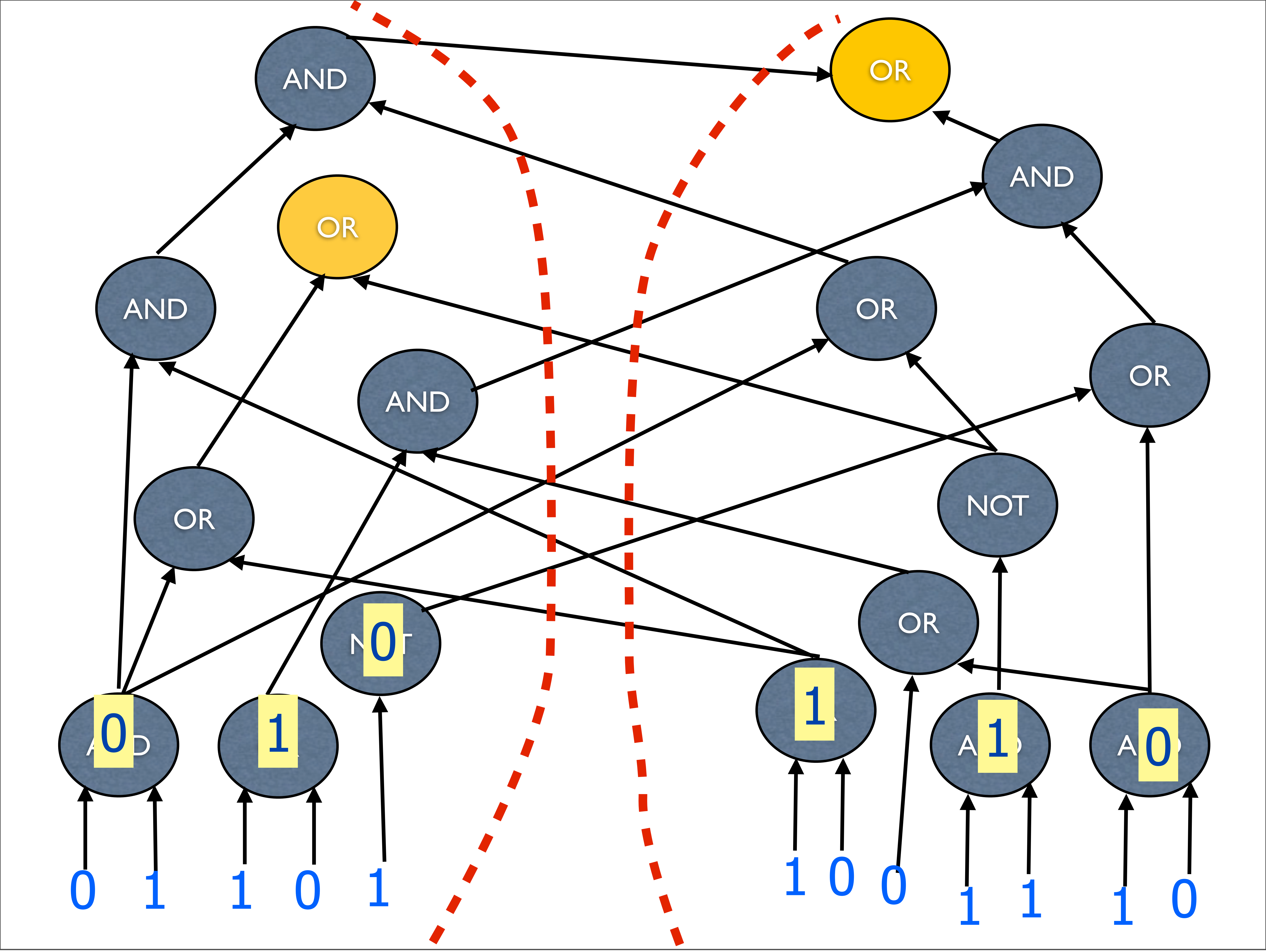
$f(X,Y)$ ←

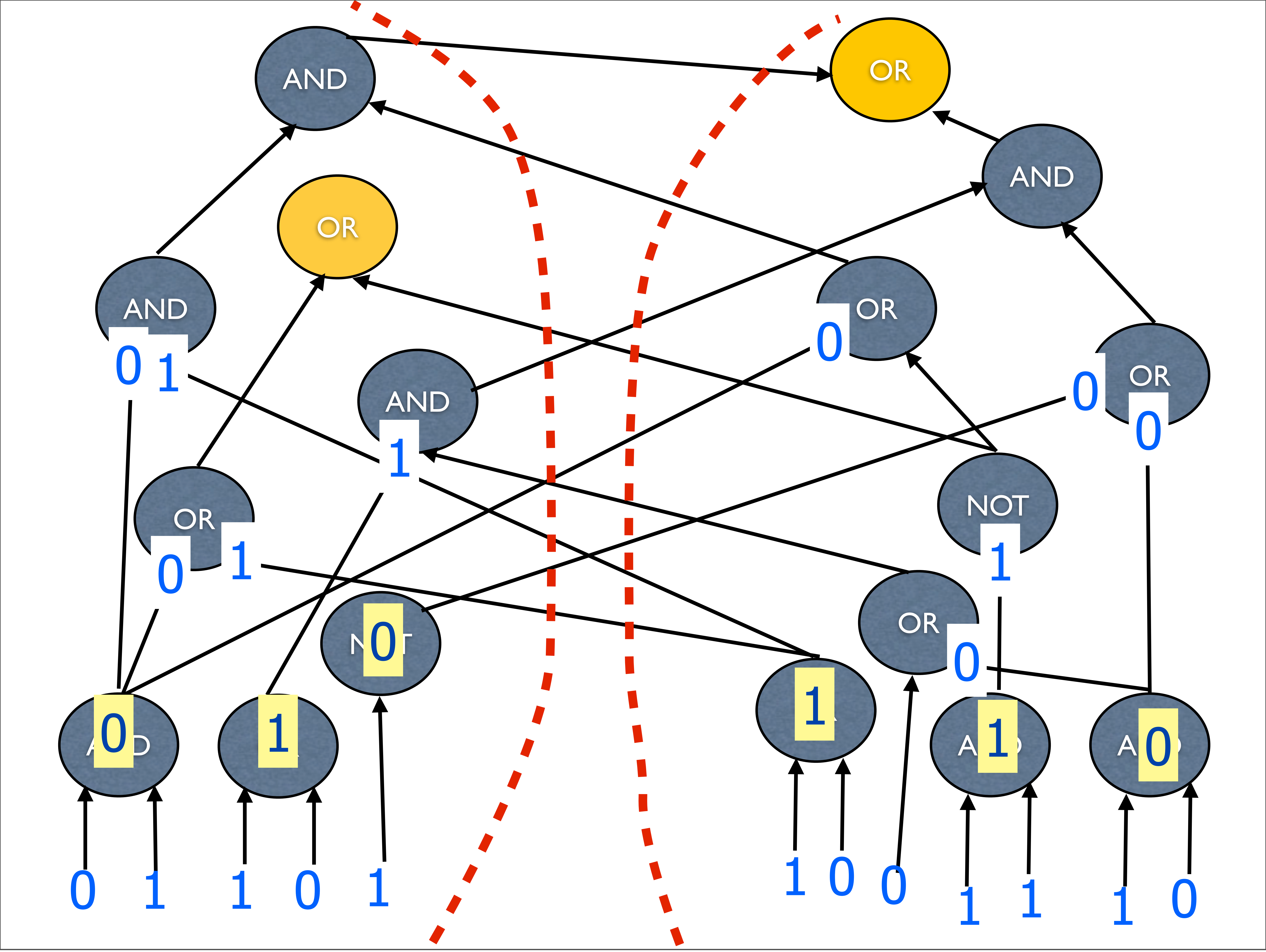
Complexity: # bits exchanged

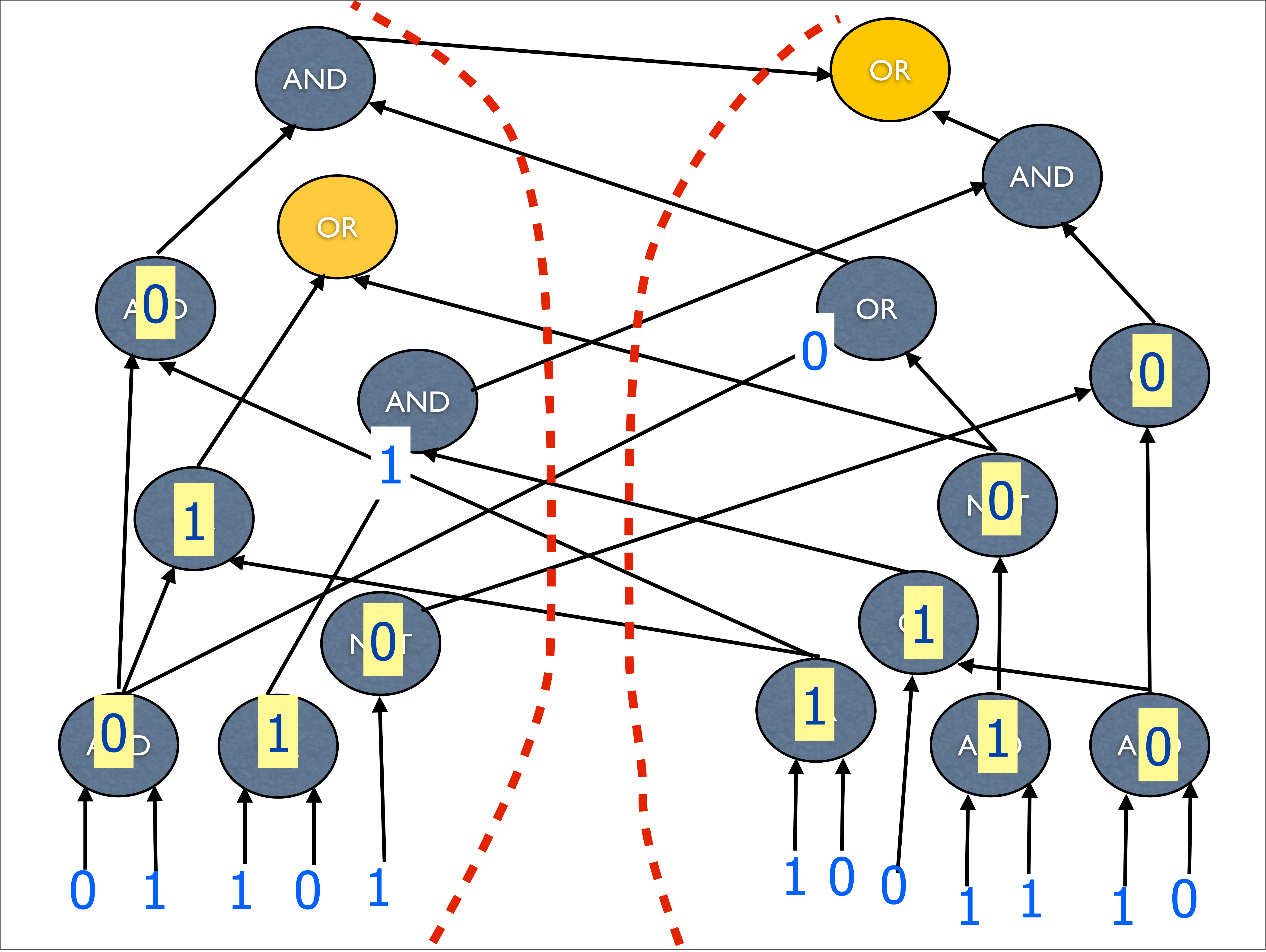
x,y drawn from some known distribution

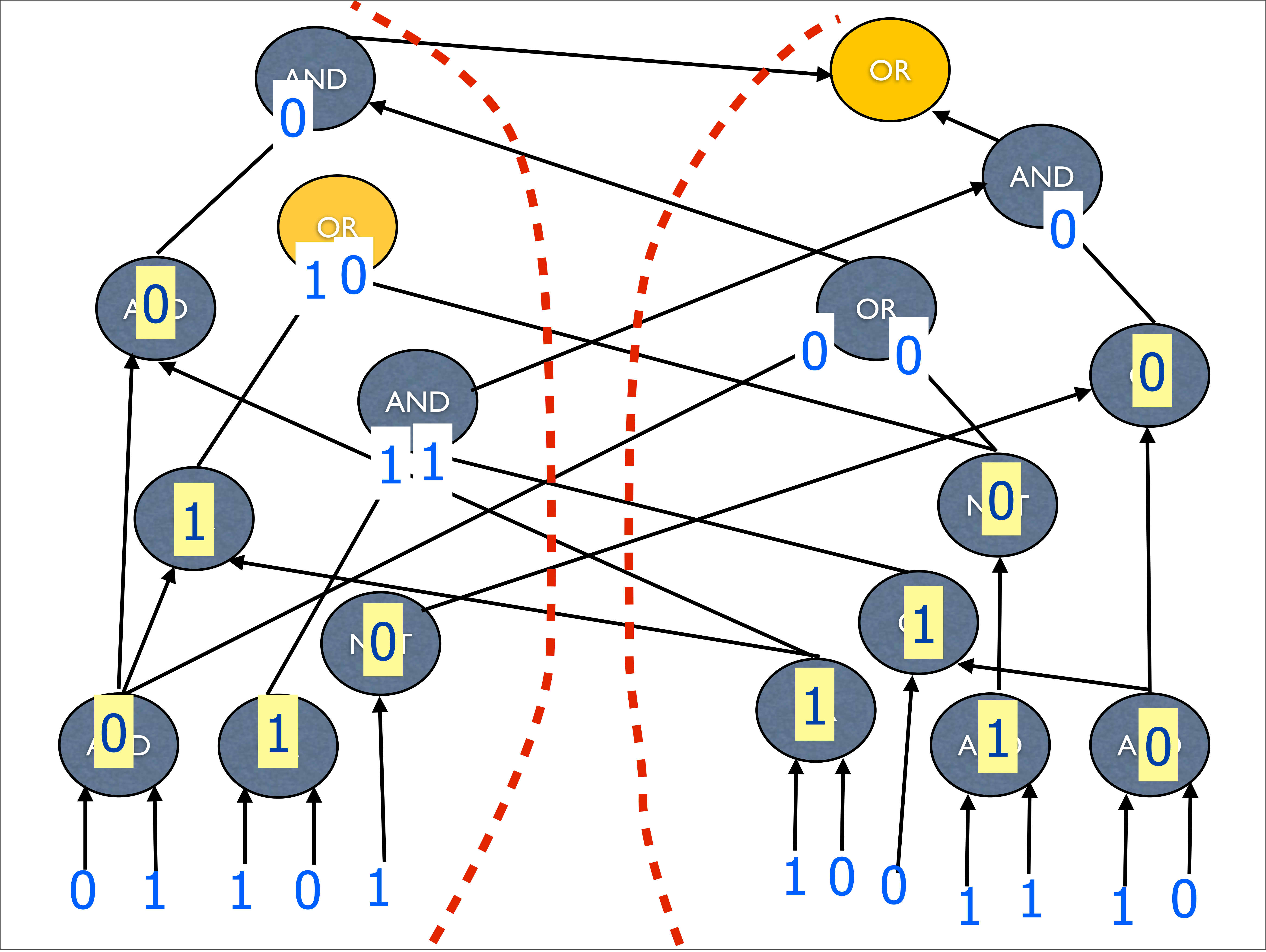

AND
OR
AND
OR
AND
OR
AND
OR
OR
NOT
OR
OR
NOT
OR
AND
OR
AND
AND
0 1 1 0 1
1 0 0 1 1 1 0


AND
OR
AND
OR
AND
OR
AND
OR
OR
NOT
OR
NOT
OR
AND
OR
NOT
OR
AND
AND
0 1 1 0 1
1 0 0 1 1 1 0

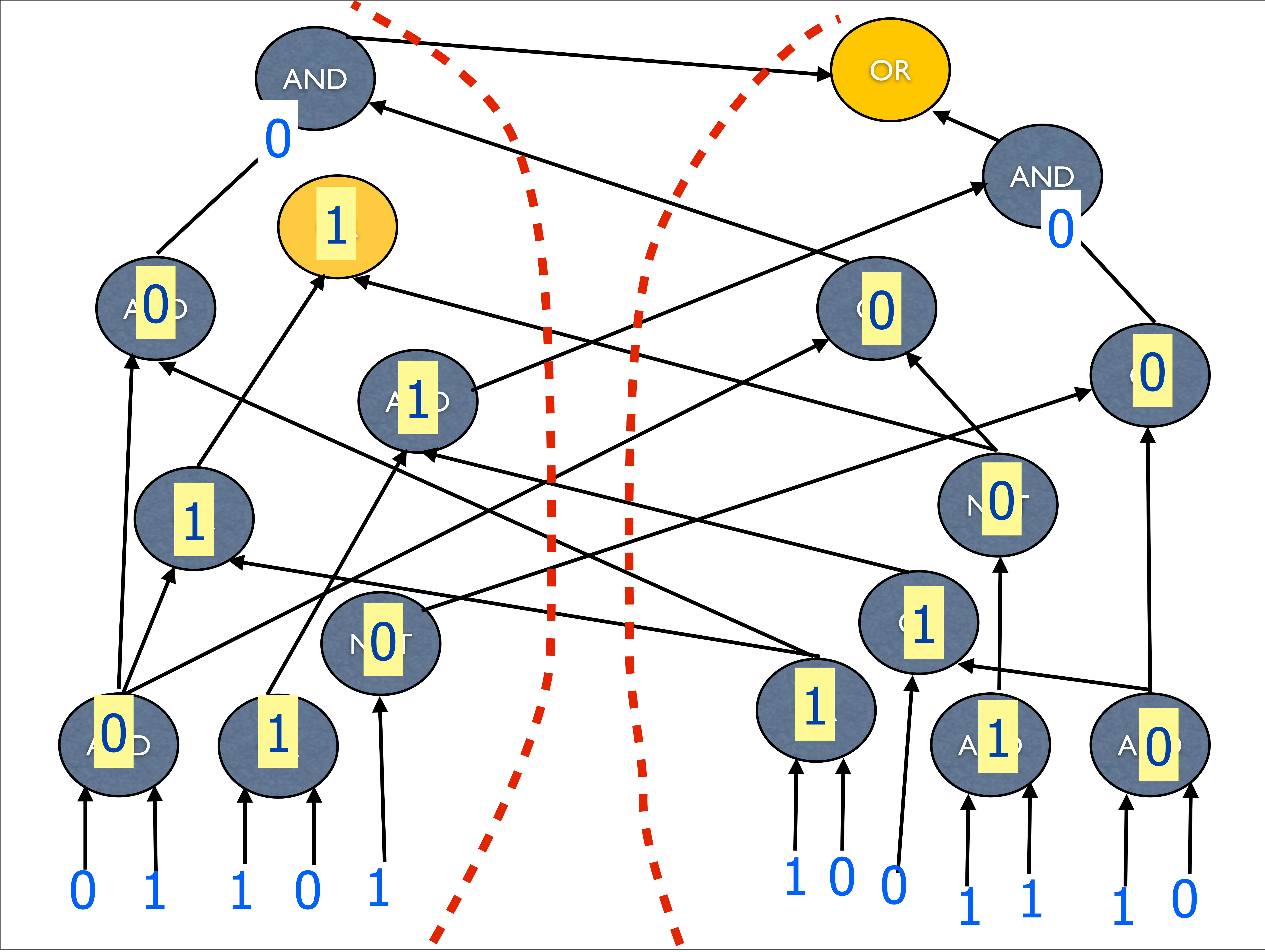

AND
OR
AND
OR
AND
OR
AND
OR
OR
NOT
OR
0
1
0
1
1
0
0 1 1 0 1
1 0 0 1 1 1 0

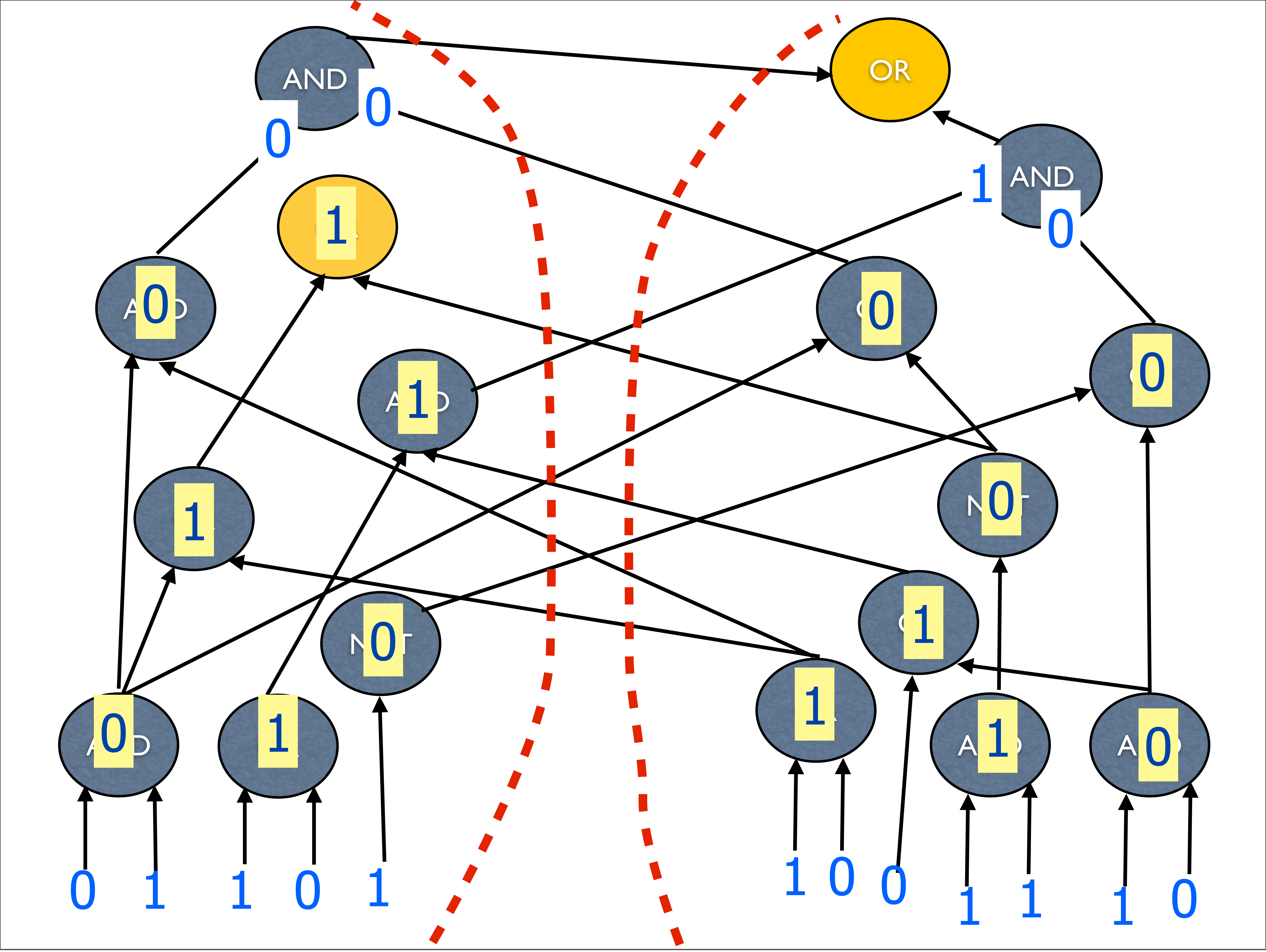

AND
OR
OR
AND
AND
OR
AND
OR
OR
NOT
OR
0
1
1
0
0
1
0
0
0
1
0
1
1
0
0
1
1
0
1
1
0
0
1
1
1
0

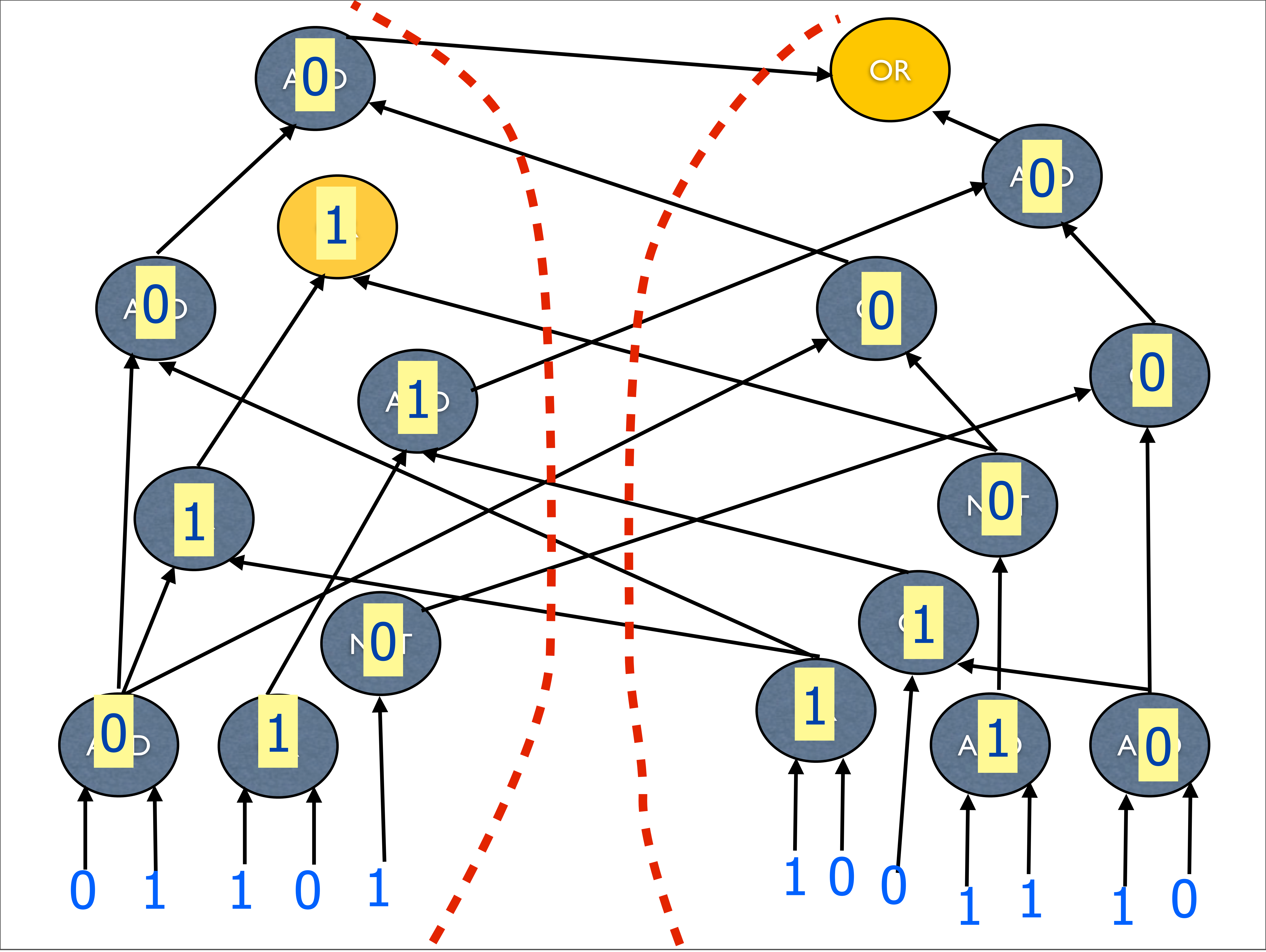

AND
OR
OR
AND
AND
OR
0 1 1 0 1
1 0 0 1 1 1 0

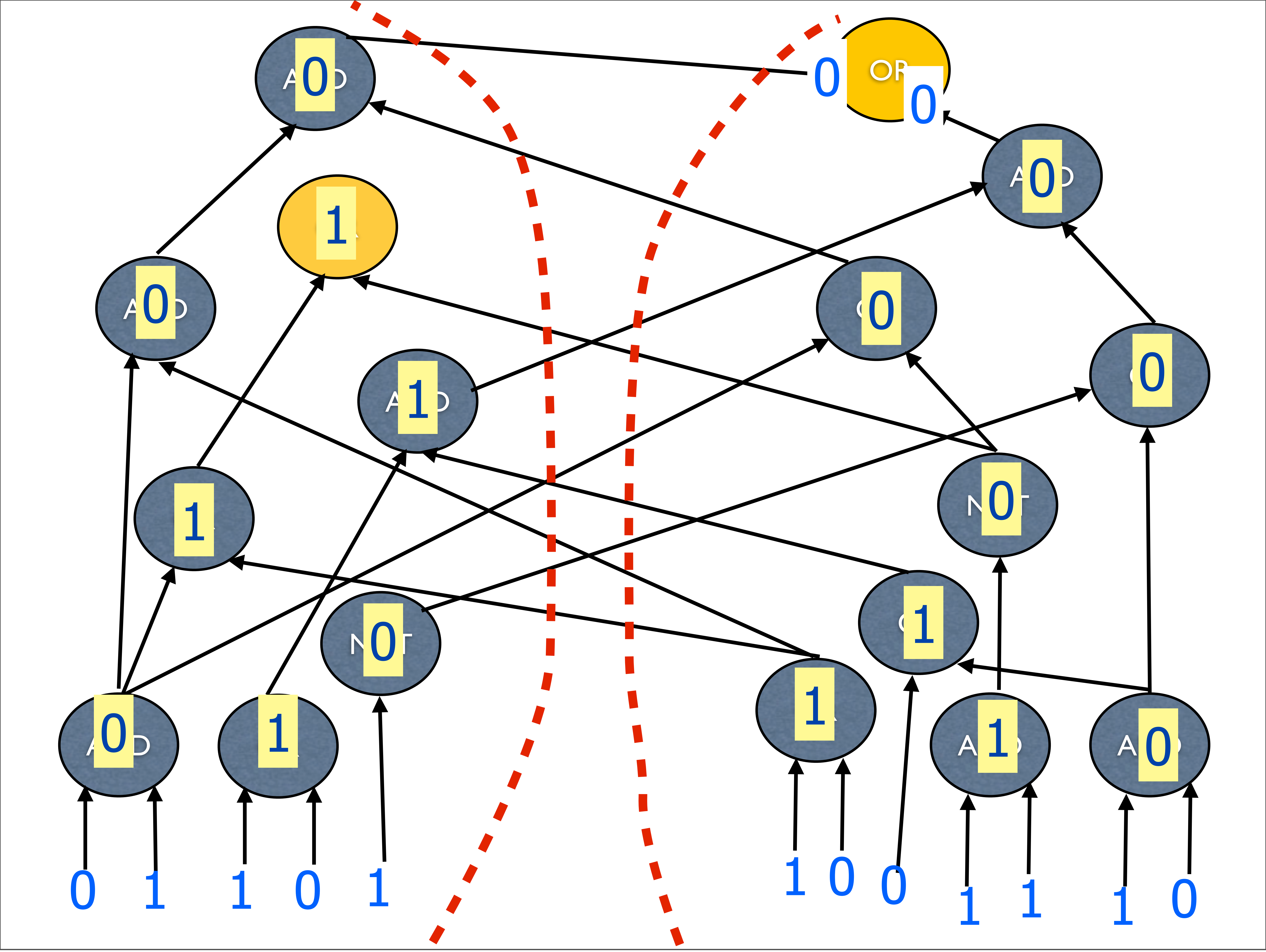


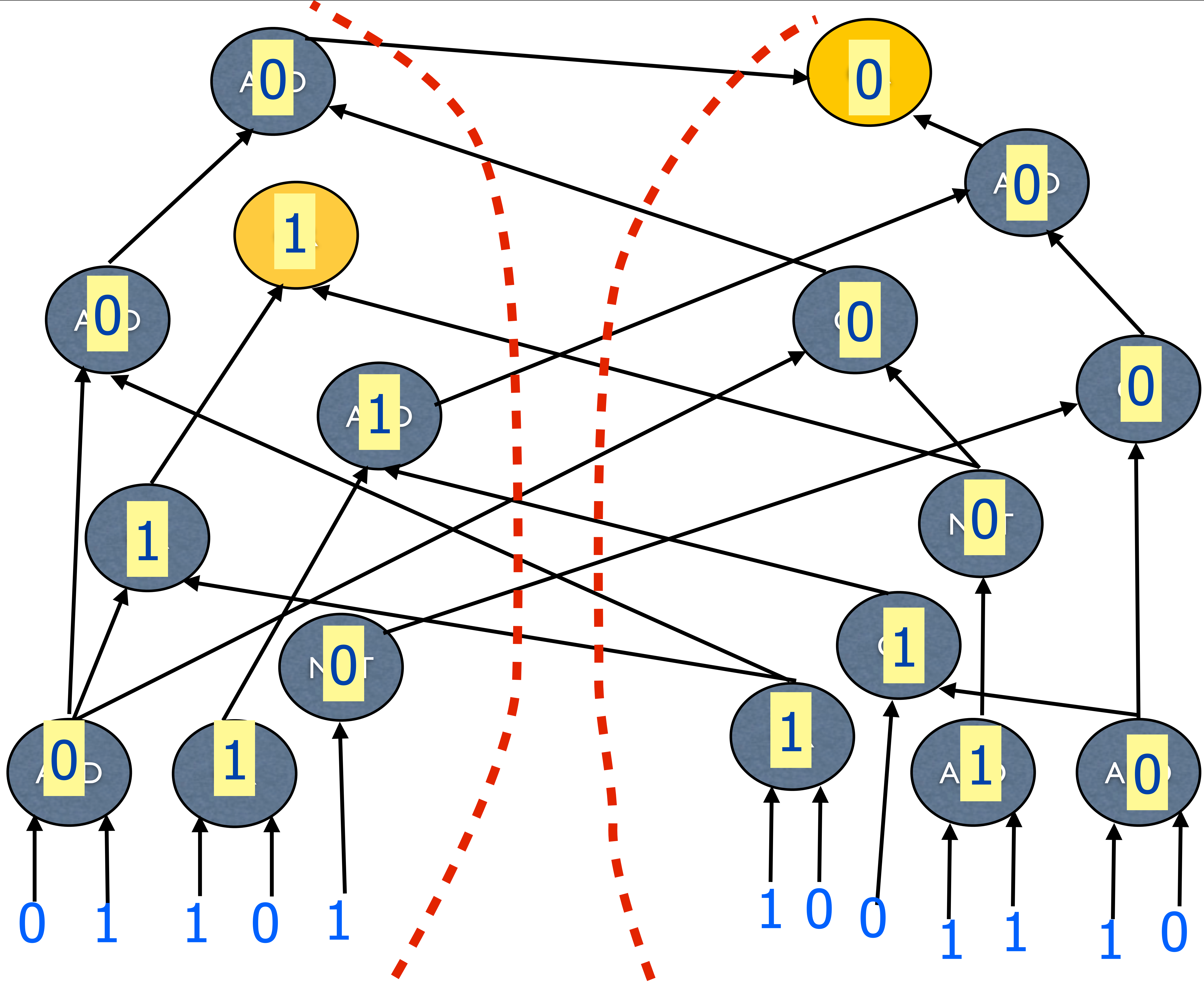
AND
OR
OR
AND
OR
AND
0 1 1 0 1
1 0 0 1 1 1 0


AND
OR
AND
0
1
0
0
0
1
1
0
0
1
0
1
1
1
0
0 1 1 0 1
1 0 0 1 1 1 0


AND
0
0
OR
1
AND
0
1
0
1
0
0
1
0
1
0
1
1
0
1
0
1
1
1
0
0 1 1 0 1
1 0 0 1 1 1 0


OR
0 1 1 0 1
1 0 0 1 1 1 0


OR
0
0 1 1 0 1
1 0 0 1 1 1 0


0
0
1
0
0
1
0
0
1
0
1
0
1
1
0
1
1
0
0 1 1 0 1
1 0 0 1 1 1 0

Applications

- Combinatorial Auctions
- Data Structure Lower Bounds
- VLSI design/Distributed Computing
- Lower bounds for branching programs, pseudorandom generators for space.
- Streaming algorithms

The Question

suc(f,C) = max success probability for computing f with C bits CC

$f^n(x_1,\ldots,x_n,y_1,\ldots,y_n) = f(x_1,y_1),\ldots,f(x_n,y_n)$

$$\boxed{\begin{array}{c}\text{If } suc(f,C) < 2/3, \text{ is} \\ suc(f^n,nC) \leq 2^{-n/100} \text{ ??}\end{array}}$$

Prior Work

Suppose suc(f,C) < 2/3, then suc(f^n,T) ≤ $2^{-n/100}$, if

- f is disjointness [Klauck]
- f has small discrepancy [Shaltiel, Lee-Shraibman-Spalek, Sherstov] or a smooth rectangle bound [Jain-Yao]
- T < C [Pernafez-Raz-Wigderson]
- protocol has few rounds [Jain-Pereszlenyi-Yao, Molinaro-Woodruff-Yaroslavtsev]

Our Results

Our Results

Theorem (product distributions):
If suc(f,C) < 2/3, then
$suc(f^n, nC/\mathrm{polylog}(nC)) \leq 2^{-n/100}$.

Theorem (arbitrary distributions):
If suc(f,C) < 2/3, then
$suc(f^n, n^{1/2}(C-k)/\mathrm{polylog}(nC)) \leq 2^{-n/100}$.

k= # bits in output of f

Our Results

Theorem (product distributions):
If suc(f,C) < 2/3, then
$suc(f^n, nC/polylog(nC)) \leq 2^{-n/100}$.

$\leq 2/3$ [BBCR]

Theorem (arbitrary distributions):
If suc(f,C) < 2/3, then
$suc(f^n, n^{1/2}(C-k)/polylog(nC)) \leq 2^{-n/100}$.

$\leq 2/3$ [BBCR]

k= # bits in output of f

Rest of the Talk

Theorem (uniform distribution):
If $suc(f,C) < 2/3$, then
$suc(f^n, nC/polylog(nC)) \leq 2^{-n/100}$.

Theorem (arbitrary distributions):
If $suc(f,C) < 2/3$, then
$suc(f^n, n^{1/2}(C-k)/polylog(nC)) \leq 2^{-n/100}$.

k = # bits in output of f

Rest of the Talk

Theorem (uniform distribution):
If suc(f,C) < 2/3, then
suc(f^n,nC/polylog(nC))$\leq 2^{-n/100}$.

$\leq$ 2/3 [BBCR]

Theorem (arbitrary distributions):
If suc(f,C) < 2/3, then
suc(f^n,$n^{1/2}$(C-k)/polylog(nC)) $\leq 2^{-n/100}$.

k= # bits in output of f

Proof by Reduction

$$\underline{\text{Alice}} \qquad \qquad \underline{\text{Bob}}$$

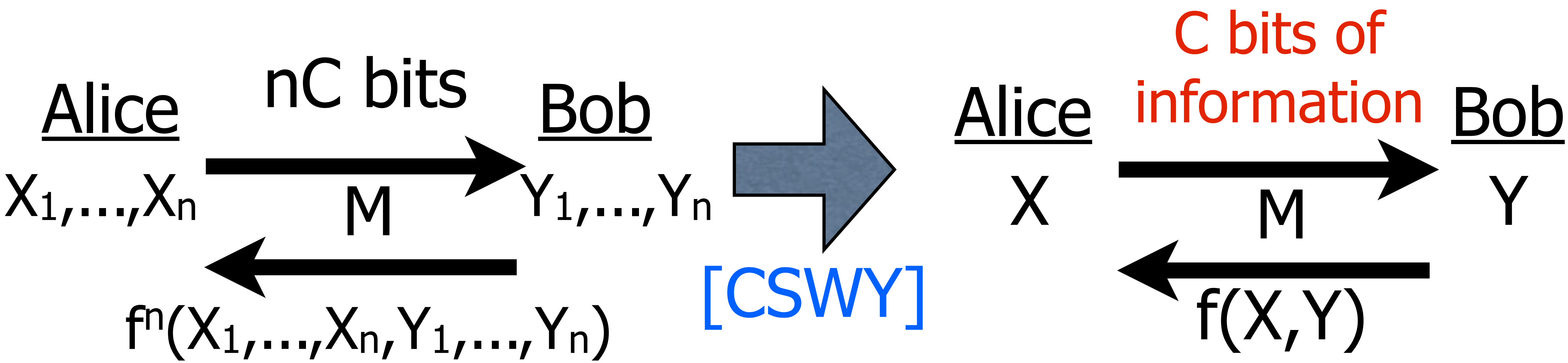
$$X_1,\ldots,X_n \xrightarrow{\text{nC bits}} Y_1,\ldots,Y_n$$

$$\xleftarrow{M}$$

$$f^n(X_1,\ldots,X_n,Y_1,\ldots,Y_n)$$

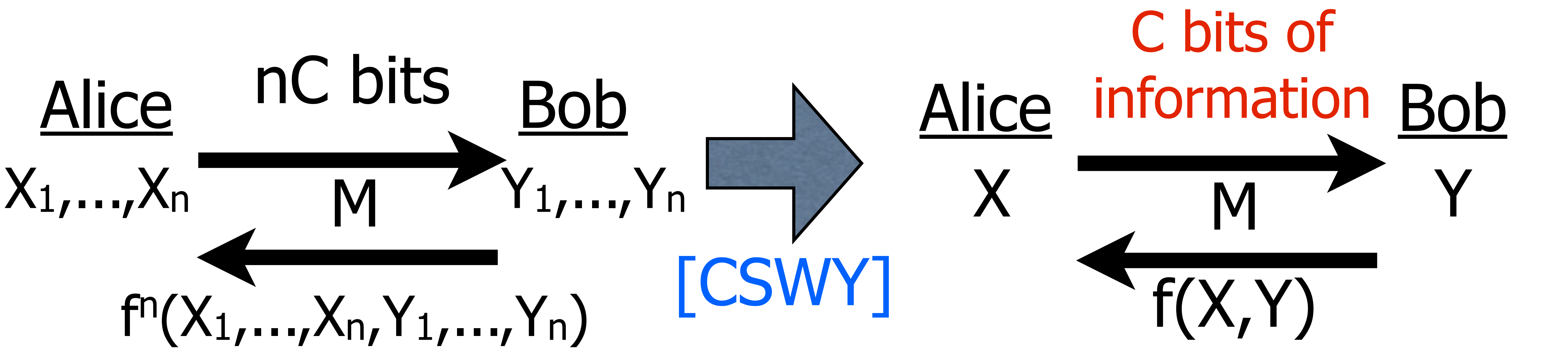
Theorem [BBCR]: If $suc(f,C) < 2/3$, then $suc(f^n,nC) \leq 2/3$.

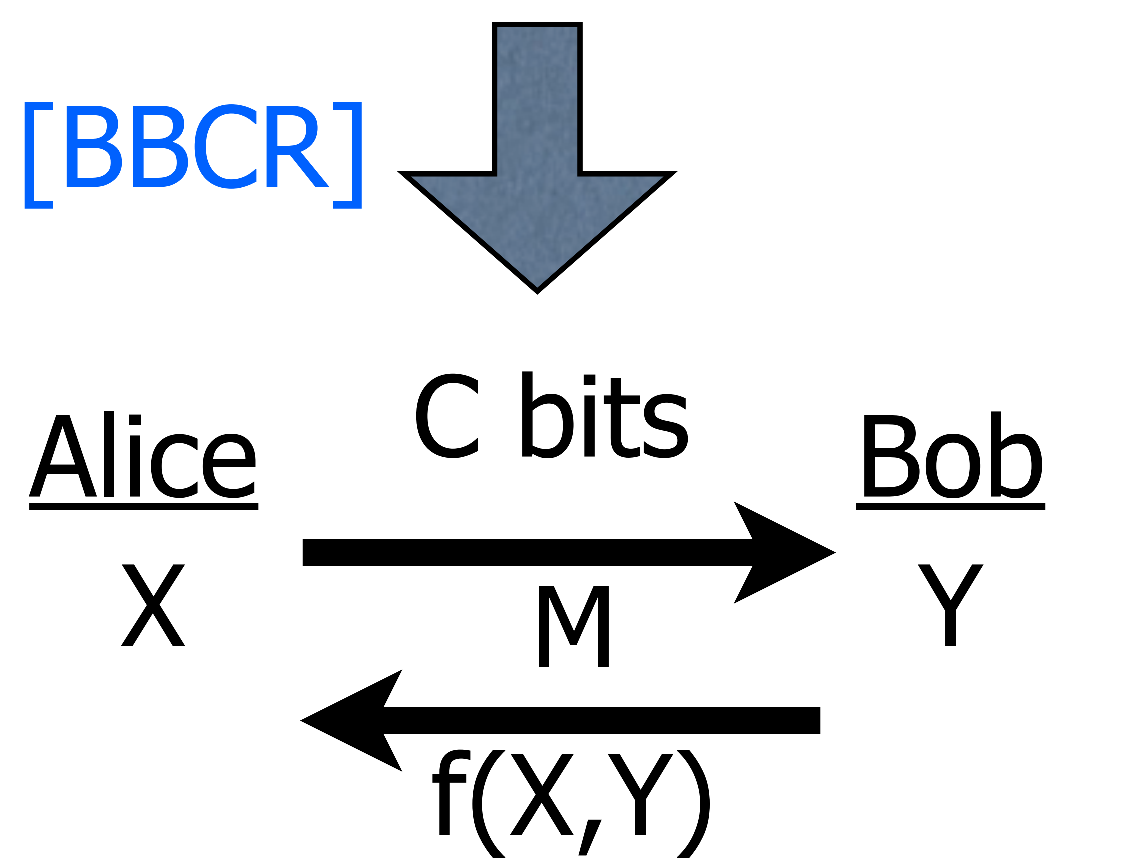
Proof by Reduction



Theorem [BBCR]: If $suc(f,C) < 2/3$, then $suc(f^n,nC) \leq 2/3$.

Proof by Reduction





Theorem [BBCR]: If $suc(f,C) < 2/3$, then $suc(f^n,nC) \leq 2/3$.

Examples

Suppose $X_1,\ldots,X_n$ are n uniform bits

$$\underline{\text{Alice}} \qquad\qquad \underline{\text{Bob}}$$

$$X_1,\ldots,X_n \xrightarrow{X_2,X_3,X_4}$$

$$\underline{\text{Alice}} \qquad\qquad \underline{\text{Bob}}$$

$$X_1 \xrightarrow[\text{0 information}]{\text{uniform bits}}$$

Examples

Suppose $X_1,\ldots,X_n$ are n uniform bits

<u>Alice</u> <u>Bob</u>

$X_1,\ldots,X_n \xrightarrow{X_2,X_3,X_4}$

<u>Alice</u> <u>Bob</u>

$X_1 \xrightarrow{\text{uniform bits}}$

0 information

<u>Alice</u> <u>Bob</u>

$X_1,\ldots,X_n \xrightarrow{\text{parity}(X_1,\ldots,X_n)}$

<u>Alice</u> <u>Bob</u>

$X_1 \xrightarrow{\text{uniform bits}}$

0 information

Examples

Suppose $X_1,\ldots,X_n$ are n uniform bits

Alice		Bob	Alice		Bob
$X_1,\ldots,X_n$	$\xrightarrow{X_2,X_3,X_4}$		X_1	$\xrightarrow{\text{uniform bits}}$	
				0 information	

Alice		Bob	Alice		Bob
$X_1,\ldots,X_n$	$\xrightarrow{\text{parity}(X_1,\ldots,X_n)}$		X_1	$\xrightarrow{\text{uniform bits}}$	
				0 information	

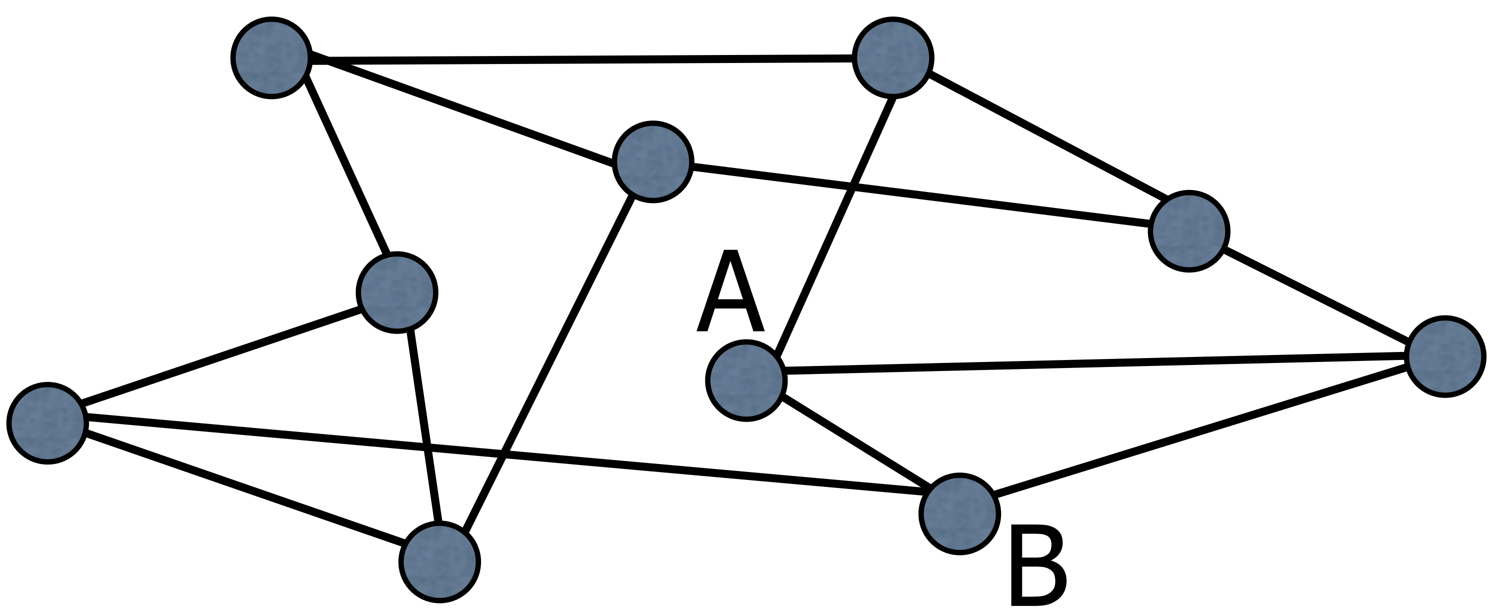
Alice		Bob	Alice		Bob
$X_1,\ldots,X_n$	$\xrightarrow{\text{majority}(X_1,\ldots,X_n)}$		X_1	$\xrightarrow{\text{majority}\mid x_1}$	
				1/n information	

Information [Shannon]

I(A;B)= $$\mathop{\mathbb{E}}_{p(a,b)}\left[\log\frac{p(a|b)}{p(a)}\right]$$

If A,B - random variables
$p(a,b)$- joint distribution

Information [Shannon]



Example:
(A,B) - random edge in d-regular graph on n vertices

I(A;B)= $$\mathop{\mathbb{E}}_{p(a,b)}\left[\log\frac{p(a|b)}{p(a)}\right]=\log\frac{1/d}{1/n}=\log\frac{n}{d}$$

Properties of Info

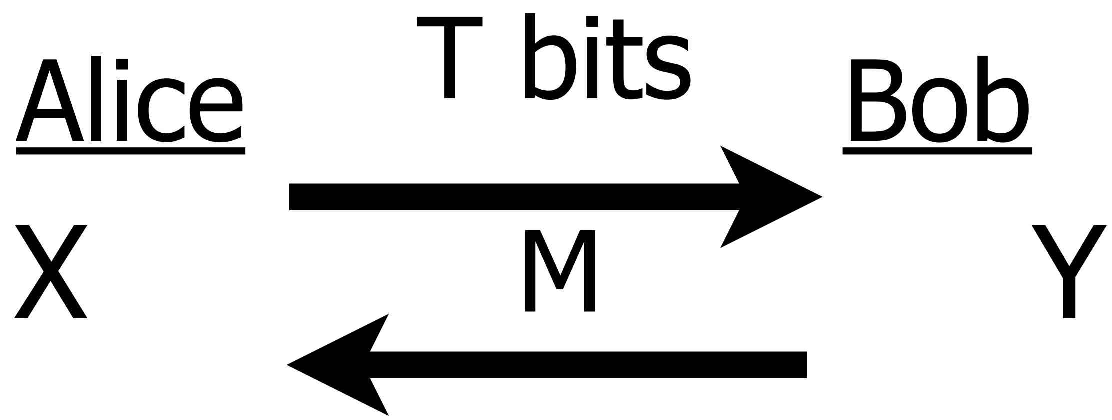
$$I(A;B|C) = E_c[I(A;B|C=c)] = \mathop{\mathbb{E}}_{p(a,b,c)}\left[\log \frac{p(a|bc)}{p(a|c)}\right]$$

$$\boxed{I(A_1A_2;B) = I(A_1; B) + I(A_2; B|A_1)}$$

If D is a T-bit string,

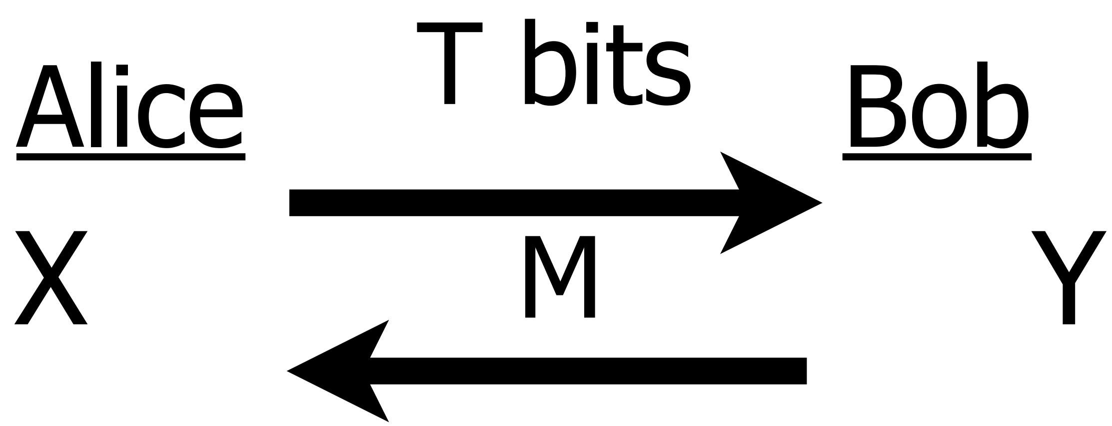
$I(C;D) \le T$

Information Cost



External information: $I(XY;M)$

Information Cost



External information: $I(XY;M) \leq T$

Low Info Protocol

$$
\begin{array}{ccc}
\underline{\text{Alice}} & \text{nC bits} & \underline{\text{Bob}} \\
X_1,\ldots,X_n & \xrightarrow[\text{M}]{} & Y_1,\ldots,Y_n \\
 & \longleftarrow & \\
 & f^n(X_1,\ldots,X_n,Y_1,\ldots,Y_n) &
\end{array}
$$

Low Info Protocol

Alice $\qquad$ nC bits $\qquad$ Bob

$$X_1,\ldots,X_n \xrightarrow[]{} \; M \; Y_1,\ldots,Y_n$$

$$\xleftarrow{}$$

$$f^n(X_1,\ldots,X_n,Y_1,\ldots,Y_n)$$

$$\begin{aligned} nC &\geq I(X_1,\ldots,X_n,Y_1,\ldots,Y_n;\, M) \\ &= I(X_1Y_1;\, M) \\ &\quad + I(X_2Y_2;M|X_1Y_1) \\ &\quad + I(X_3Y_3;M|X_1X_2Y_1Y_2) + \ldots \end{aligned}$$

Low Info Protocol

<u>Alice</u> $\xrightarrow{\text{nC bits}}$ <u>Bob</u>

$X_1,\ldots,X_n$ $\xrightarrow{M}$ $Y_1,\ldots,Y_n$

$\longleftarrow$ $f^n(X_1,\ldots,X_n,Y_1,\ldots,Y_n)$

$$
\begin{aligned}
nC &\geq I(X_1,\ldots,X_n,Y_1,\ldots,Y_n; M) \\
&= I(X_1Y_1; M) \\
&\quad + I(X_2Y_2;M|X_1Y_1) \\
&\quad + I(X_3Y_3;M|X_1X_2Y_1Y_2) + \ldots
\end{aligned}
$$

For average i,

$C \geq I(X_iY_i;M \mid X_1,\ldots,X_{i-1},Y_1,\ldots,Y_{i-1})$

Low Info Protocol

<u>Alice</u>	nC bits	<u>Bob</u>
$X_1,\ldots,X_n$	$\xrightarrow{}$ M $\xleftarrow{}$	$Y_1,\ldots,Y_n$

$f^n(X_1,\ldots,X_n,Y_1,\ldots,Y_n)$

$$\boxed{C \geq I(X_iY_i;M \mid X_1,\ldots,X_{i-1}\ Y_1,\ldots,Y_{i-1})}$$

---

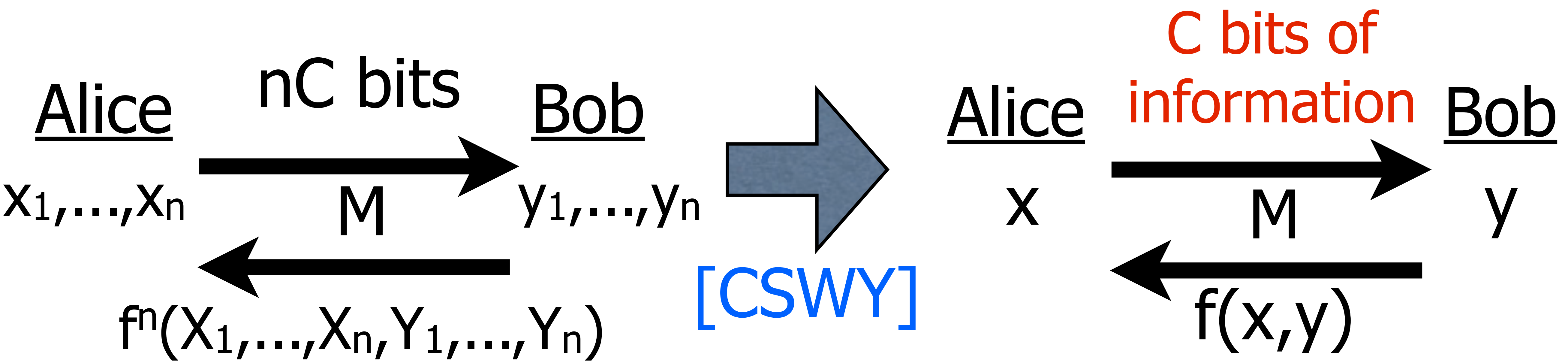
publicly sample: $X_1,\text{-},X_{i-1}\ Y_1,\text{-},Y_{i-1}$

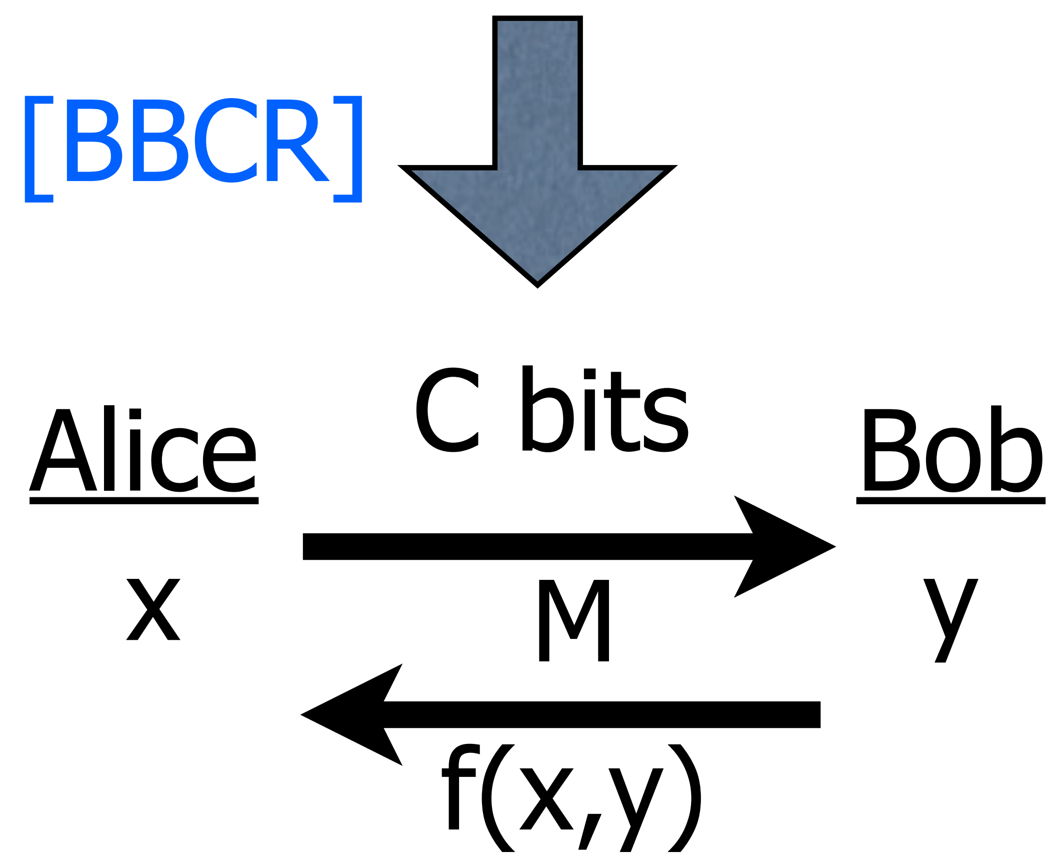
<u>Alice</u>		<u>Bob</u>
X_i	$\xrightarrow{}$ M $\xleftarrow{}$	Y_i

$f^n(X_1,\ldots,X_n,Y_1,\ldots,Y_n)$

$$\boxed{\text{Information} \leq C}$$

Reduction

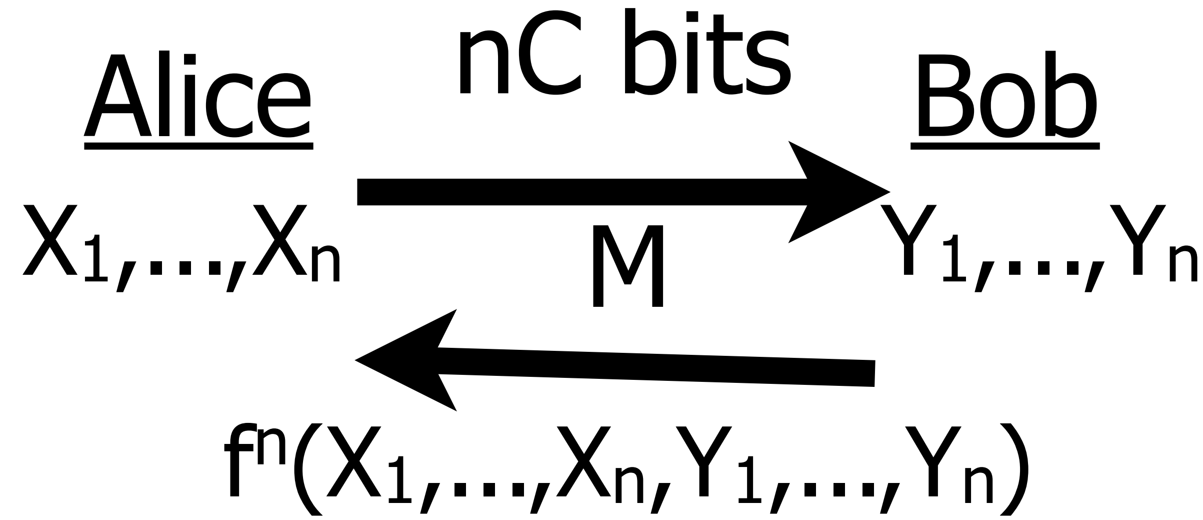




Theorem [BBCR]: If $suc(f,C) < 2/3$, then $suc(f^n,nC) \leq 2/3$.

Theorem: If $\mathrm{suc}(f,C) < 2/3$, then $\mathrm{suc}(f^n, nC) \leq 2^{-n/100}$.

Theorem: If suc(f,C) < 2/3, then suc(f^n,nC)$\leq 2^{-n/100}$.



Theorem: If suc(f,C) < 2/3, then $suc(f^n, nC) \leq 2^{-n/100}$.

Alice — nC bits — Bob

$X_1,\dots,X_n \xrightarrow{M} Y_1,\dots,Y_n$

$\xleftarrow{\quad}$

$f^n(X_1,\dots,X_n,Y_1,\dots,Y_n)$

W: event that output is correct

Theorem: If $\mathrm{suc}(f,C) < 2/3$, then $\mathrm{suc}(f^n,nC) \leq 2^{-n/100}$.

Alice	nC bits	Bob
$X_1,\ldots,X_n$	$\xrightarrow{\quad M \quad}$	$Y_1,\ldots,Y_n$

$f^n(X_1,\ldots,X_n,Y_1,\ldots,Y_n)$

W: event that output is correct

Alice	C bits	Bob
X_i	$\xrightarrow{\quad M' \quad}$	Y_i

$$M'X_iY_i \sim MX_iY_i|W$$

Theorem: If $suc(f,C) < 2/3$, then $suc(f^n, nC) \leq 2^{-n/100}$.

Alice $\xrightarrow{\text{nC bits}}$ Bob

$X_1,\ldots,X_n$ M $Y_1,\ldots,Y_n$

$f^n(X_1,\ldots,X_n,Y_1,\ldots,Y_n)$

W: event that output is correct

Challenges:

- $M|W$ is not a protocol, e.g.

Alice $\xrightarrow{M}$ Bob

$X_1,\ldots,X_n$ $Y_1,\ldots,Y_n$

E: $M=h(X_1,\ldots,X_n,Y_1,\ldots,Y_n)$

Simulating $M|E$ with a protocol naively requires a lot of communication!

Alice $\xrightarrow{\text{C bits}}$ Bob

X_i M' Y_i

$M'X_iY_i \sim MX_iY_i|W$

Theorem: If suc(f,C) < 2/3, then $\mathrm{suc}(f^n, nC) \leq 2^{-n/100}$.

Alice

$X_1,\ldots,X_n$

nC bits

M

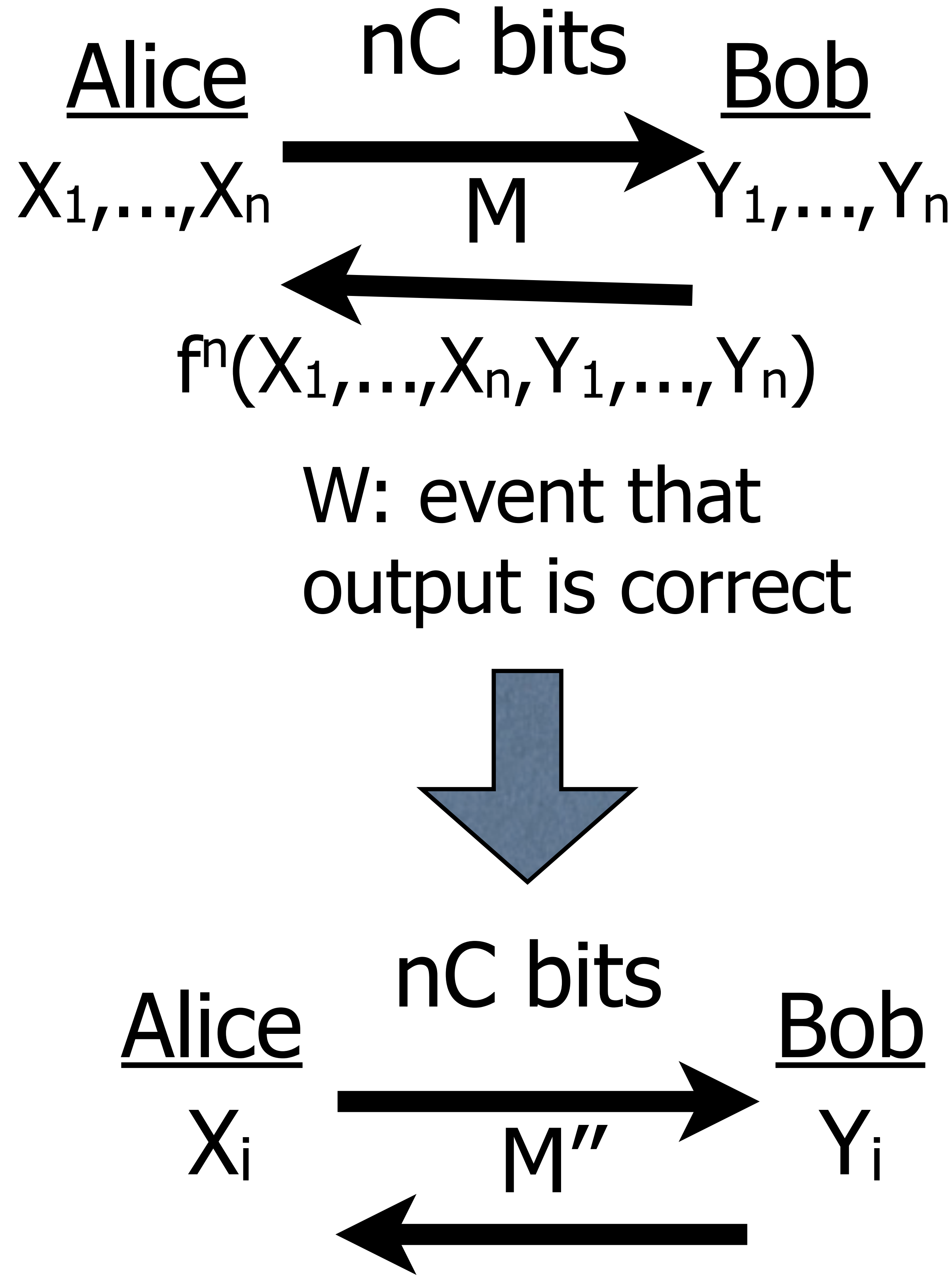
Bob

$Y_1,\ldots,Y_n$

$f^n(X_1,\ldots,X_n,Y_1,\ldots,Y_n)$

W: event that output is correct

Theorem: If suc(f,C) < 2/3, then $\mathrm{suc}(f^n, nC) \leq 2^{-n/100}$.



$$M''X_iY_i \sim MX_iY_i|W$$

Theorem: If suc(f,C) < 2/3, then $\mathrm{suc}(f^n, nC) \leq 2^{-n/100}$.

Alice	nC bits	Bob
$X_1,\ldots,X_n$	M	$Y_1,\ldots,Y_n$

$f^n(X_1,\ldots,X_n,Y_1,\ldots,Y_n)$

W: event that output is correct

Alice	nC bits	Bob
X_i	M″	Y_i

$M''X_iY_i \sim MX_iY_i|W$

Alice	C bits	Bob
X_i	M′	Y_i

$M'X_iY_i \sim MX_iY_i|W$

Theorem: If $suc(f,C) < 2/3$, then $suc(f^n,nC) \leq 2^{-n/100}$.

Alice $X_1,\ldots,X_n$ — nC bits, M — Bob $Y_1,\ldots,Y_n$

$f^n(X_1,\ldots,X_n,Y_1,\ldots,Y_n)$

W: event that output is correct

Intuition: W cannot simultaneously affect all n inputs or messages about all n inputs.

Alice X_i — nC bits, M″ — Bob Y_i

$M''X_iY_i \sim MX_iY_i|W$

Alice $\xrightarrow[M]{nC \text{ bits}}$ **Bob**

$X_1,\ldots,X_n$ $\quad$ $Y_1,\ldots,Y_n$

$f^n(X_1,\ldots,X_n,Y_1,\ldots,Y_n)$

W: event that output is correct

Alice $\xrightarrow[M'']{nC \text{ bits}}$ **Bob**

X_i $\quad$ Y_i

$M''X_iY_i \sim MX_iY_i|W$

Alice $\xrightarrow[M']{C \text{ bits}}$ **Bob**

X_i $\quad$ Y_i

$M'X_iY_i \sim M''X_iY_i$

$$
\begin{aligned}
nC &\geq I(X_1,\ldots,X_n,Y_1,\ldots,Y_n;\, M|W) \\
&= I(X_1Y_1;\, M|W) \\
&\quad + I(X_2Y_2; M|WX_1Y_1) \\
&\quad + I(X_3Y_3; M|WX_1X_2Y_1Y_2)\ldots
\end{aligned}
$$

<u>Alice</u> nC bits <u>Bob</u>

$X_1,\ldots,X_n$ M $Y_1,\ldots,Y_n$

$f^n(X_1,\ldots,X_n,Y_1,\ldots,Y_n)$

W: event that output is correct

<u>Alice</u> nC bits <u>Bob</u>

X_i M″ Y_i

$M''X_iY_i \sim MX_iY_i|W$

<u>Alice</u> C bits <u>Bob</u>

X_i M′ Y_i

$M'X_iY_i \sim M''X_iY_i$

$$\begin{aligned} nC &\geq I(X_1,\ldots,X_n,Y_1,\ldots,Y_n;\, M|W) \\ &= I(X_1Y_1;\, M|W) \\ &\quad + I(X_2Y_2; M|WX_1Y_1) \\ &\quad + I(X_3Y_3; M|WX_1X_2Y_1Y_2)\ldots \end{aligned}$$

$$\boxed{\begin{array}{l}\text{For average } i, \\ C \geq I(X_iY_i; M|X_1,\ldots,X_{i-1},Y_1,\ldots,Y_{i-1}W)\end{array}}$$

<u>Alice</u> nC bits <u>Bob</u>

$X_1,\ldots,X_n$ $\xrightarrow{M}$ $Y_1,\ldots,Y_n$

$f^n(X_1,\ldots,X_n,Y_1,\ldots,Y_n)$

W: event that output is correct

<u>Alice</u> nC bits <u>Bob</u>

X_i $\xrightarrow{M''}$ Y_i

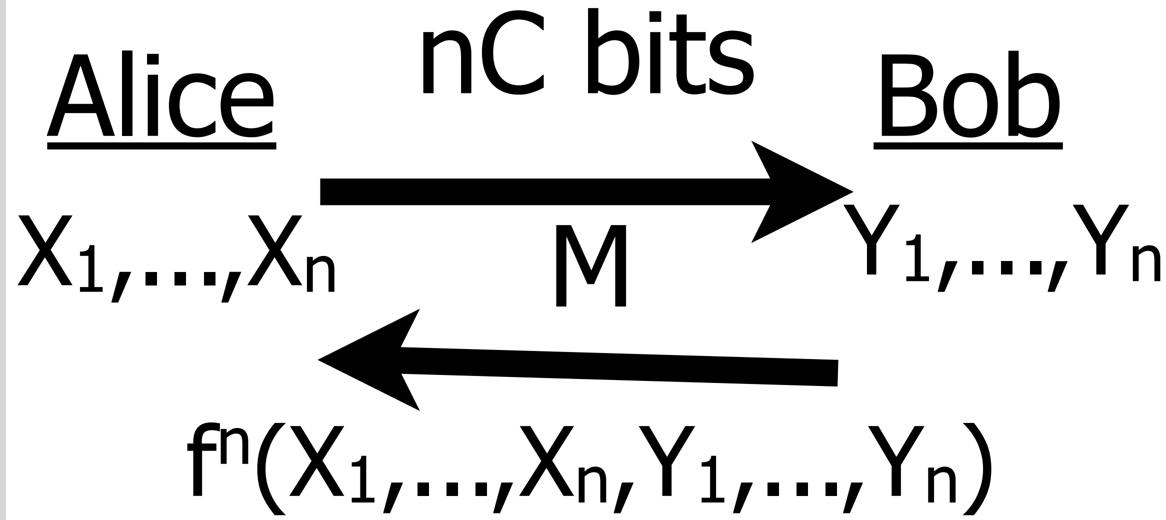
$M''X_iY_i \sim MX_iY_i|W$

<u>Alice</u> C bits <u>Bob</u>

X_i $\xrightarrow{M'}$ Y_i

$M'X_iY_i \sim M''X_iY_i$

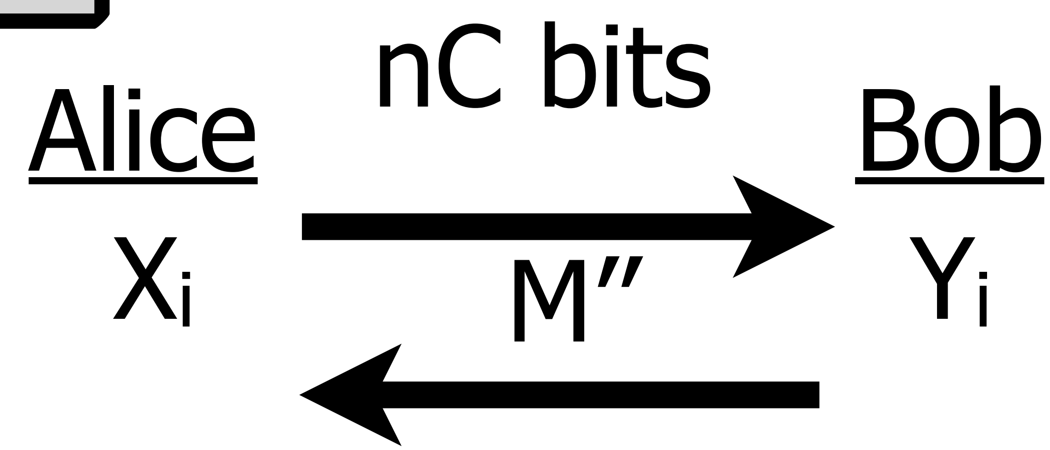
$$nC \geq I(X_1,\ldots,X_n,Y_1,\ldots,Y_n;\, M|W)$$
$$= I(X_1Y_1;\, M|W)$$
$$+ I(X_2Y_2;M|WX_1Y_1)$$
$$+ I(X_3Y_3;M|WX_1X_2Y_1Y_2)\ldots$$



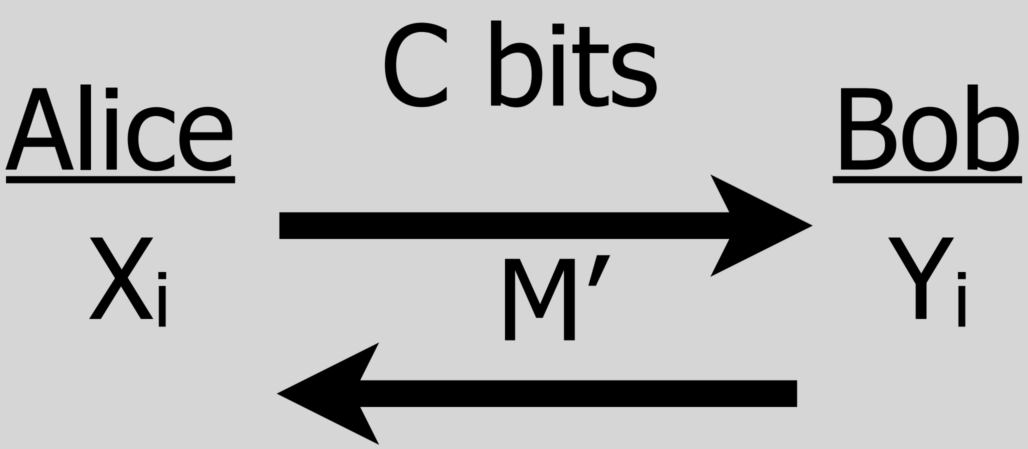
For average i,
$C \geq I(X_iY_i;M|X_1,\ldots,X_{i-1},Y_1,\ldots,Y_{i-1}W)$

W: event that output is correct

WANT: For average i,
$C \geq I(X_iY_i;M''|X_1,\ldots,X_{i-1},Y_1,\ldots,Y_{i-1})$



$M''X_iY_i \sim MX_iY_i|W$



$M'X_iY_i \sim M''X_iY_i$

Cannot use BBCR:

$$\underline{\text{Alice}} \xrightarrow{M} \underline{\text{Bob}}$$

x

$$M = \begin{cases} x, \text{ with } \varepsilon \text{ prob.} \\ \text{random, } 1-\varepsilon \text{ prob.} \end{cases}$$

Cannot use BBCR:

Alice $\xrightarrow{M}$ Bob

x

$$M = \begin{cases} x, \text{ with } \varepsilon \text{ prob.} \\ \text{random, } 1-\varepsilon \text{ prob.} \end{cases}$$

M is ε close to having 0 information, but has very large information

Cannot use BBCR:

Alice (x) $\xrightarrow{M}$ Bob

$$M = \begin{cases} x, & \text{with } \varepsilon \text{ prob.} \\ \text{random}, & 1-\varepsilon \text{ prob.} \end{cases}$$

M is ε close to having 0 information, but has very large information

However: can modify protocol to obtain low info protocol!

Cannot use BBCR:

Alice $\xrightarrow{M}$ Bob

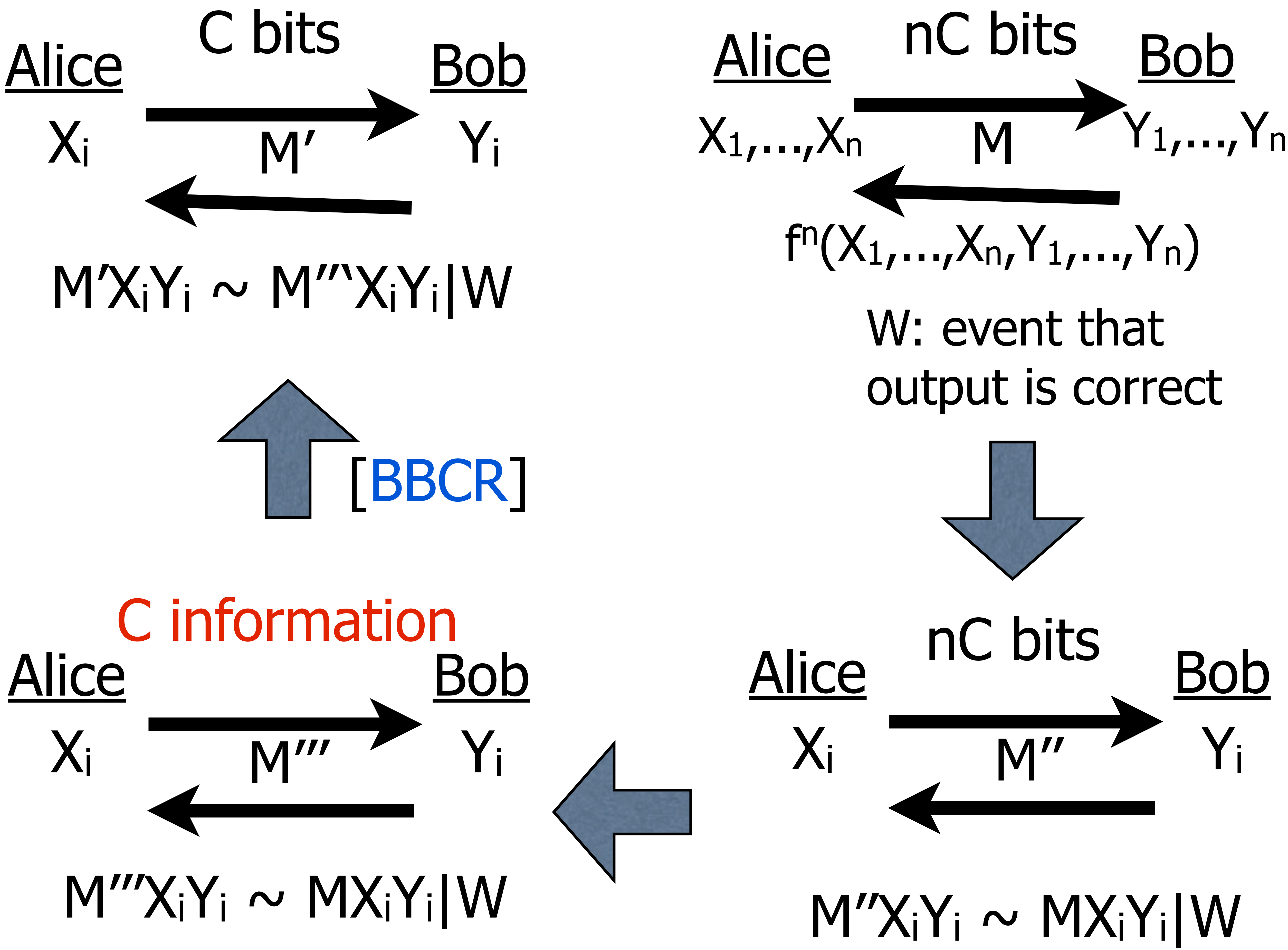
x

$$M = \begin{cases} x, \text{ with } \varepsilon \text{ prob.} \\ \text{random, } 1-\varepsilon \text{ prob.} \end{cases}$$

M is ε close to having 0 information, but has very large information

However: can modify protocol to obtain low info protocol!

Theorem: If a protocol is statistically close to low information, then it can be simulated by a low information protocol


C bits
Alice
Bob
X_i
M'
Y_i
$M'X_iY_i \sim M''X_iY_i|W$
nC bits
Alice
Bob
$X_1,\ldots,X_n$
M
$Y_1,\ldots,Y_n$
$f^n(X_1,\ldots,X_n,Y_1,\ldots,Y_n)$
W: event that output is correct
[BBCR]
C information
Alice
Bob
X_i
M'''
Y_i
$M'''X_iY_i \sim MX_iY_i|W$
nC bits
Alice
Bob
X_i
M''
Y_i
$M''X_iY_i \sim MX_iY_i|W$

Results

Theorem (product distributions):
If suc(f,C) < 2/3, then
$suc(f^n, nC/\mathrm{polylog}(nC)) \leq 2^{-n/100}$.

Theorem (arbitrary distributions):
If suc(f,C) < 2/3, then
$suc(f^n, n^{1/2}(C-k)/\mathrm{polylog}(nC)) \leq 2^{-n/100}$.

k= # bits in output of f

Open Challenges

Open Challenges

- Simulating a protocol with information I and communication C currently takes $(I.C)^{1/2}$ [BBCR]. Is it possible to do better?

Open Challenges

- Simulating a protocol with information I and communication C currently takes $(I.C)^{1/2}$ [BBCR]. Is it possible to do better?
- Direct products in other computational models (like circuits)? Strong counterexamples known for circuits, but the full truth is still not known.

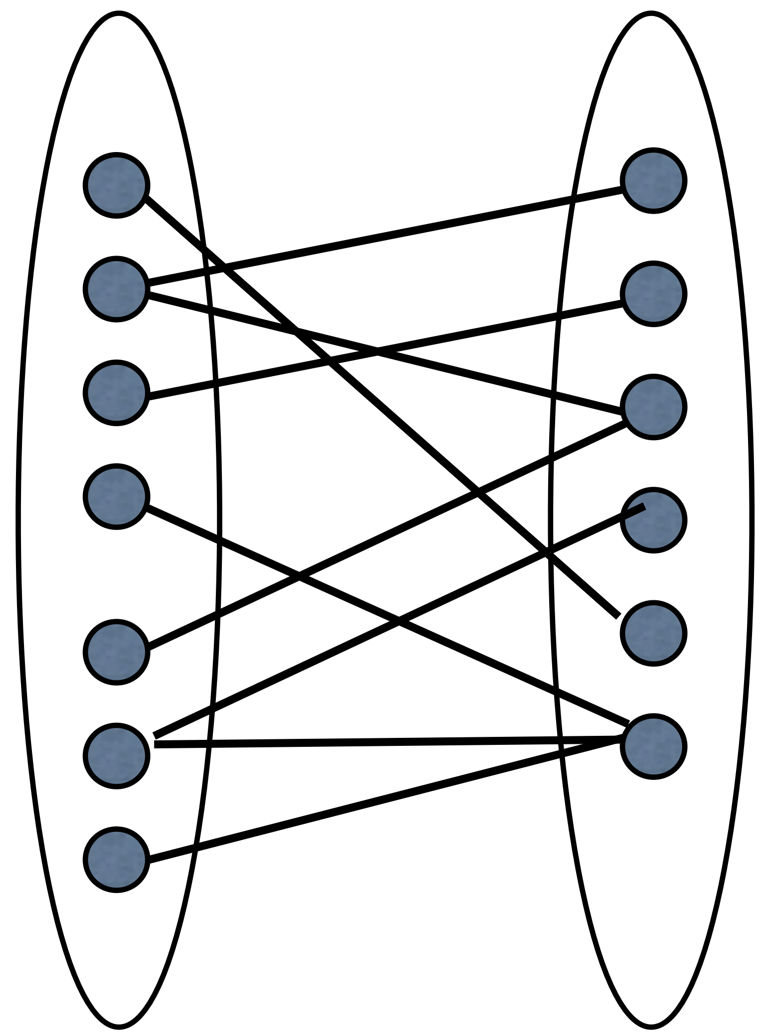
Questions?

Obviously...

$$\boxed{\text{suc}(f^n, nC) \leq \text{exponentially small}}$$

Watch Out [Feige]

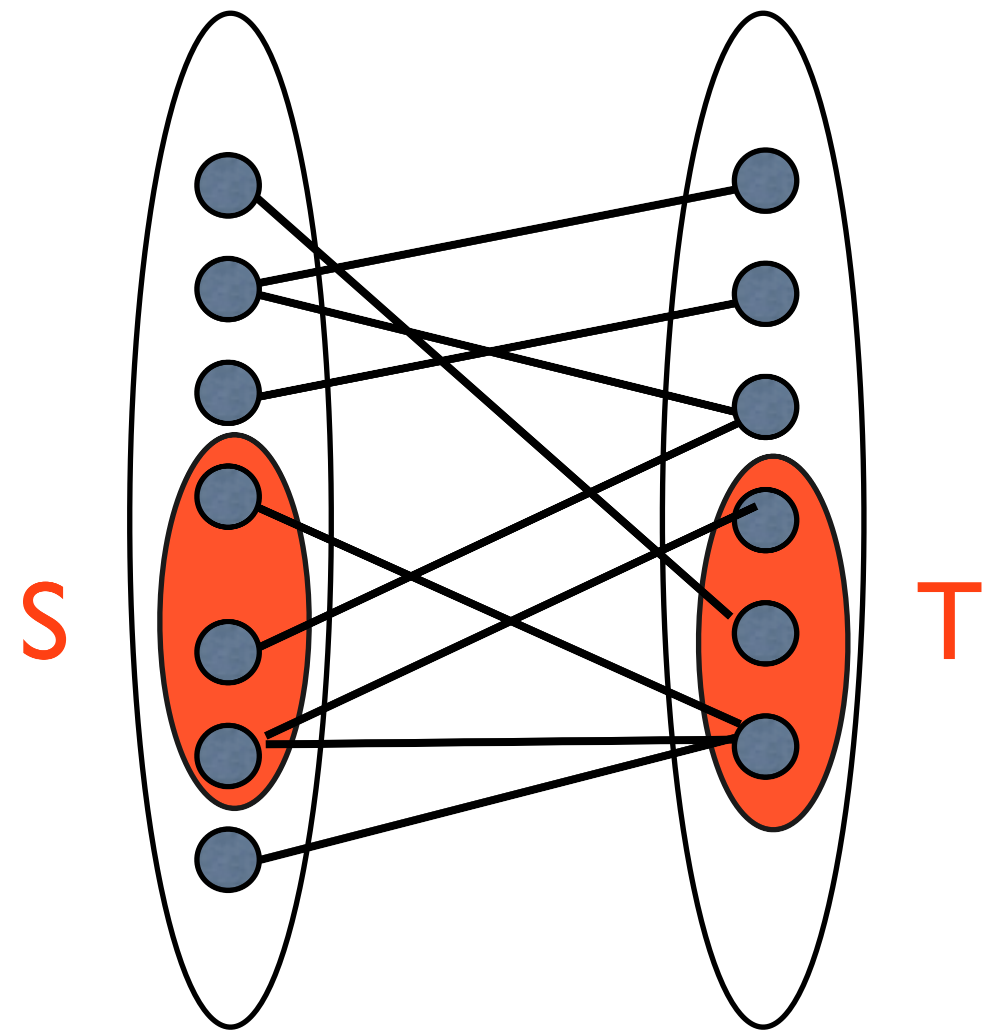
Uniformly random graph, K vertices on each side.



Watch Out [Feige]

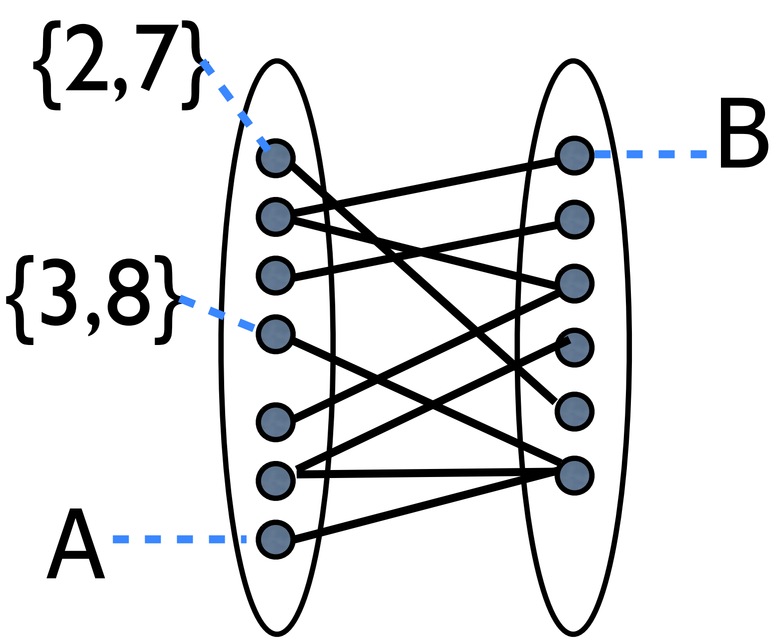
Uniformly random graph, K vertices on each side.

If |S|,|T| >2(log K), edge density between S,T ~ 0.5



Watch Out [Feige]

Random graph, edge density = 0.5

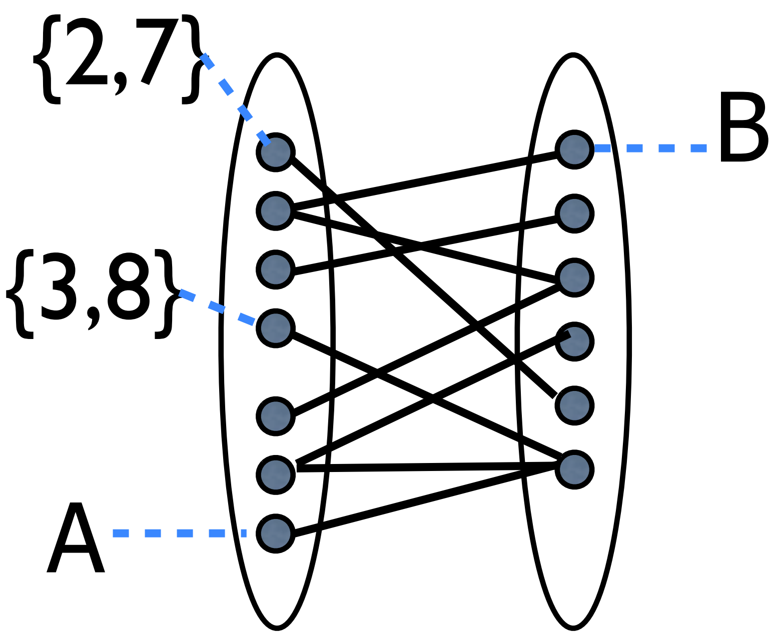


A,B ⊂ {1,2,...,k}

|A|,|B|=2

Watch Out [Feige]

Random graph, edge density = 0.5



$A,B \subset \{1,2,\ldots,k\}$

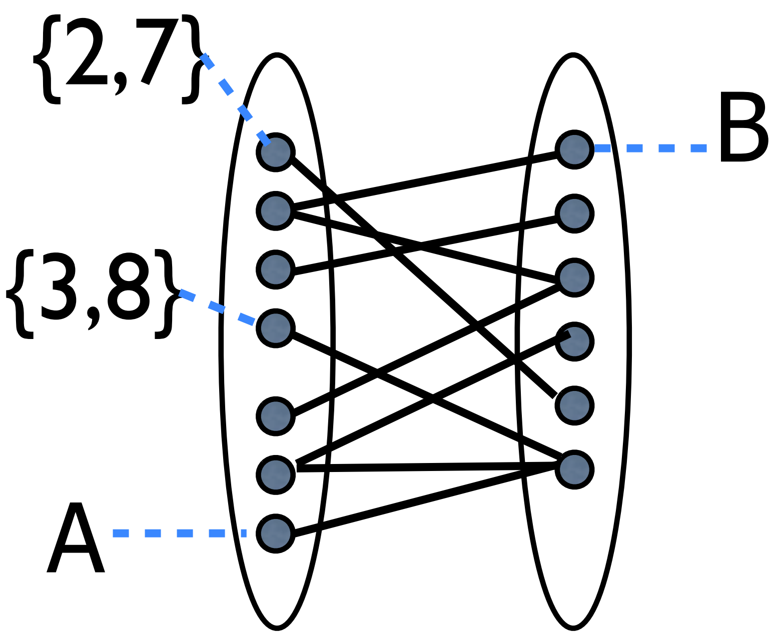
$|A|,|B|=2$

Alice	Bob
$x \in [k]$	$y \in [k]$
Output $A \ni x$	Output $B \ni y$

Goal: Output (A,B) that is an edge

Watch Out [Feige]

Random graph, edge density = 0.5



$A,B \subset \{1,2,\ldots,k\}$

$|A|,|B|=2$

<u>Alice</u>

$x \in [k]$

Output $A \ni x$

<u>Bob</u>

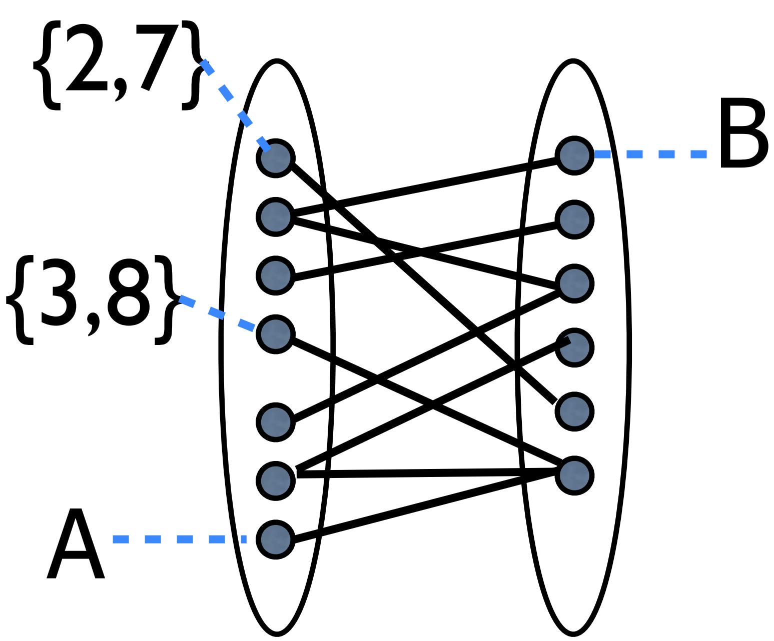
$y \in [k]$

Output $B \ni y$

Lemma: Pr[(A,B) is an edge] ~ 0.5

Watch Out [Feige]

Random graph, edge density = 0.5



A,B $\subset$ {1,2,...,k}
|A|,|B|=2

Alice

x$\in$[k]

Bob

y$\in$[k]

0.1 log k bits

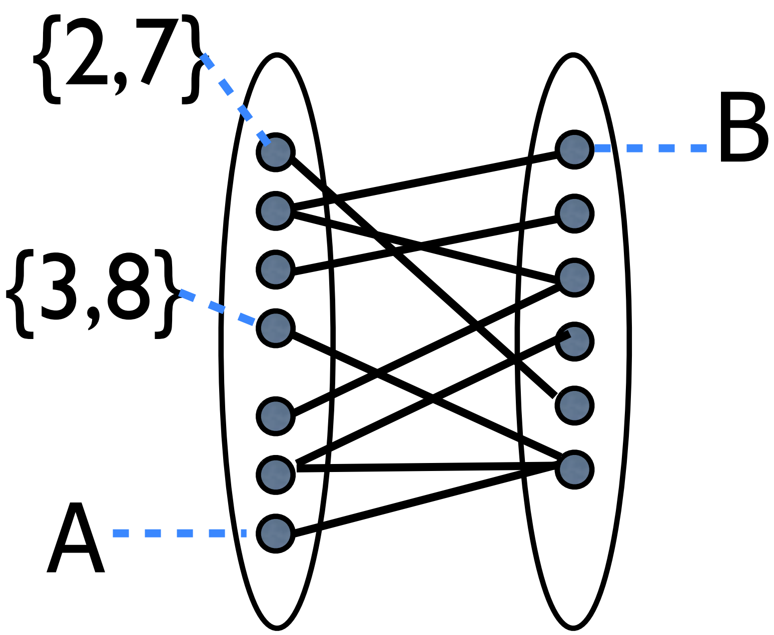
Output A$\ni$x

Output B$\ni$y

Lemma: Pr[(A,B) is an edge] ~ 0.5

Watch Out [Feige]

Random graph, edge density = 0.5



$A, B \subset \{1,2,\ldots,k\}$

$|A|,|B|=2$

<u>Alice</u> <u>Bob</u>

$x \in [k]$ $\xrightarrow{\text{0.1 log k bits}}$ $y \in [k]$

Output $A \ni x$ Output $B \ni y$

Lemma: Pr[(A,B) is an edge] ~ 0.5

<u>Alice</u> <u>Bob</u>

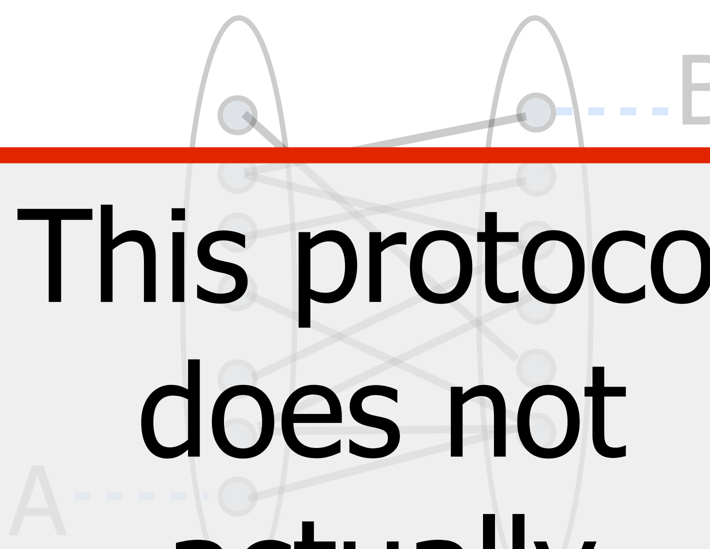
$x_1, x_2 \in [k]$ $y_1, y_2 \in [k]$

$A=\{x_1,x_2\}$ $B=\{y_1,y_2\}$

Lemma: Pr[(A,B) is an edge] ~ 0.5

Wait wait...

Random graph, edge density = 0.8



|A|,|B|=2

Alice		Bob
$x \in [k]$	$\xrightarrow{}$ 0.1 log k bits $\xleftarrow{}$	$y \in [k]$
Output $A \ni x$		Output $B \ni y$

Lemma: Pr[(A,B) is an edge] ~0.5

This protocol does not actually transmit A,B!

Alice	Bob
$x_1, x_2 \in [k]$	$y_1, y_2 \in [k]$
$A = \{x_1, x_2\}$	$B = \{y_1, y_2\}$

Lemma: Pr[(A,B) is an edge] ~ 0.5