Computationally Asymmetric Permutations and Reversible-gates Circuits

One Approach to One-Wayness

Alexey E. Zhukov
Bauman Moscow Technical University
E-mail: aez_iu8@rambler.ru

Permutations on $\mathbb{Z}_2^n$

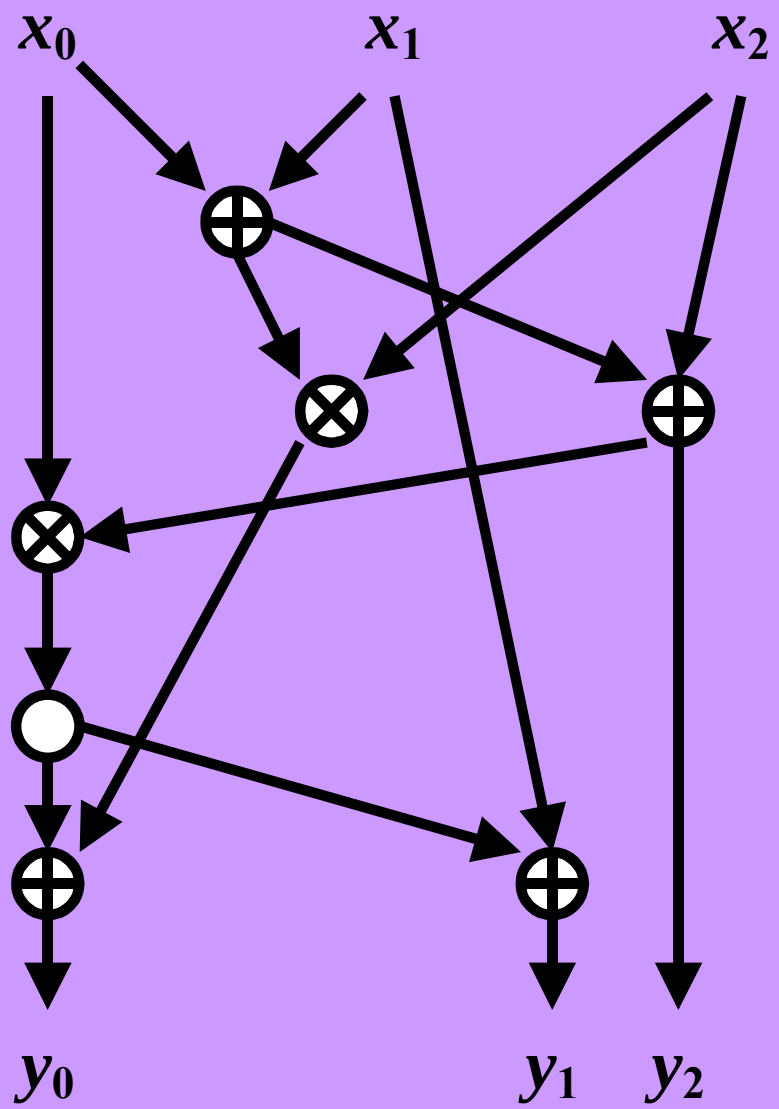
$(x_2\, x_1\, x_0)$	$(y_2\, y_1\, y_0)$
0 0 0	0 1 1
0 0 1	1 0 0
0 1 0	1 0 1
0 1 1	0 0 1
1 0 0	1 1 1
1 0 1	0 1 0
1 1 0	0 0 0
1 1 1	1 1 0

$(y_2\, y_1\, y_0)$	$(x_2\, x_1\, x_0)$
0 0 0	1 1 0
0 0 1	0 1 1
0 1 0	1 0 1
0 1 1	0 0 0
1 0 0	0 0 1
1 0 1	0 1 0
1 1 0	1 1 1
1 1 1	1 0 0

$$\mathbf{F}: \mathbb{Z}_2^3 \to \mathbb{Z}_2^3 \qquad \mathbf{F}^{-1}: \mathbb{Z}_2^3 \to \mathbb{Z}_2^3$$

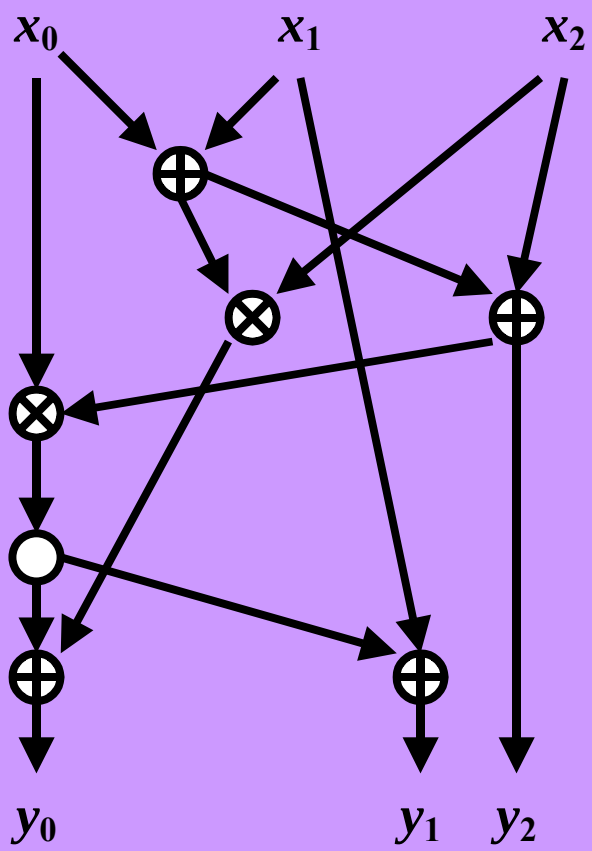
Logical Gate Circuits

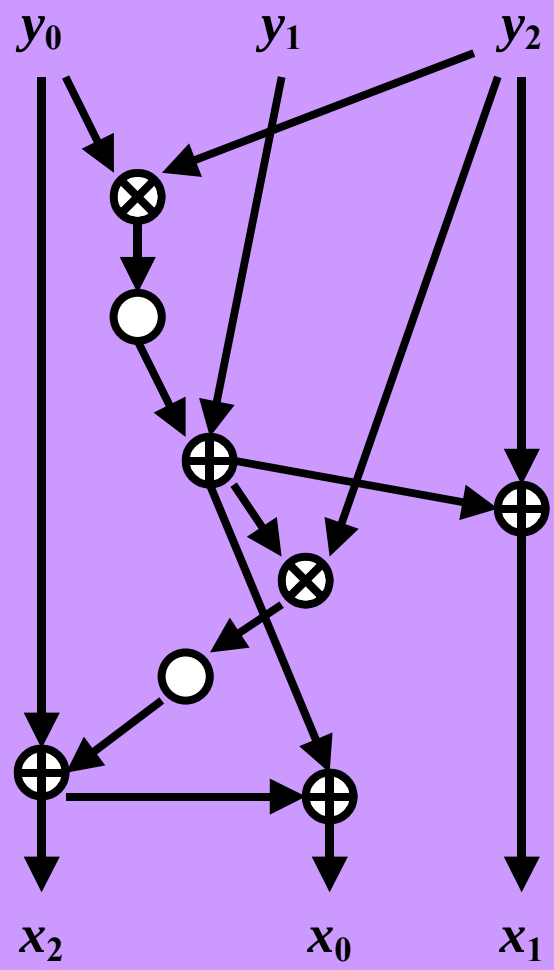
$(x_2\, x_1\, x_0)$	$(y_2\, y_1\, y_0)$
0 0 0	0 1 1
0 0 1	1 0 0
0 1 0	1 0 1
0 1 1	0 0 1
1 0 0	1 1 1
1 0 1	0 1 0
1 1 0	0 0 0
1 1 1	1 1 0



$$L(F) = 7$$

Computationally Asymmetric Permutations





$L(F)=7$

$L(F^{-1})=8$

Computationally Asymmetric Linear Permutations

Boppana R.B., Lagarias J.C. ***One-way functions and circuit complexity.*** Information and Computation, vol. 74 (1987), pp. 226-240

Hiltgen A.P. ***Constructions of feebly-one-way families of permutations.*** AUSCRYPT'92, LNCS v.718 (1993), pp. 422-434

Computationally Asymmetric Linear Permutations

$$\mathbf{A}: \mathbb{Z}_2^n \to \mathbb{Z}_2^n$$

$$y_i(x_1,\ldots,x_n) = x_i \oplus x_{i+1}, \quad i = 1,\ldots,n-1;$$

$$y_n(x_1,\ldots,x_n) = x_1 \oplus x_{\lceil n/2 \rceil} \oplus x_n$$

$$L(\mathbf{A}) = n+1 \qquad L(\mathbf{A}^{-1}) = \frac{3(n-1)}{2}$$

for n = 7 :

$$L(\mathbf{A}) = 8 \qquad L(\mathbf{A}^{-1}) = 9$$

Computationally Asymmetric Linear Permutations

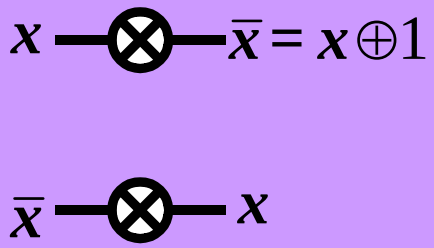
for $n = 7$ **:**

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \qquad \mathbf{A}^{-1} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

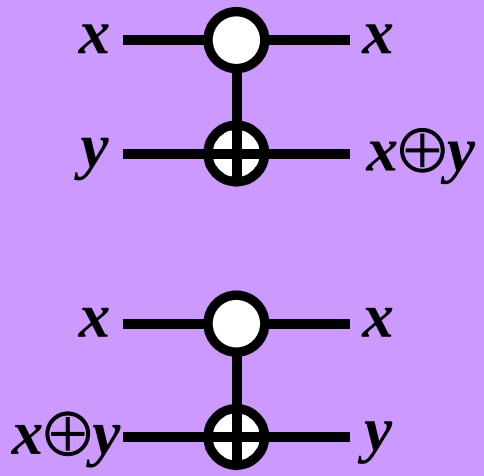
$$L(\mathbf{A}) = n+1 \underset{(n=7)}{=} 8 \qquad L(\mathbf{A}^{-1}) = \frac{3}{2}(n-1) \underset{(n=7)}{=} 9$$

Reversible Gates

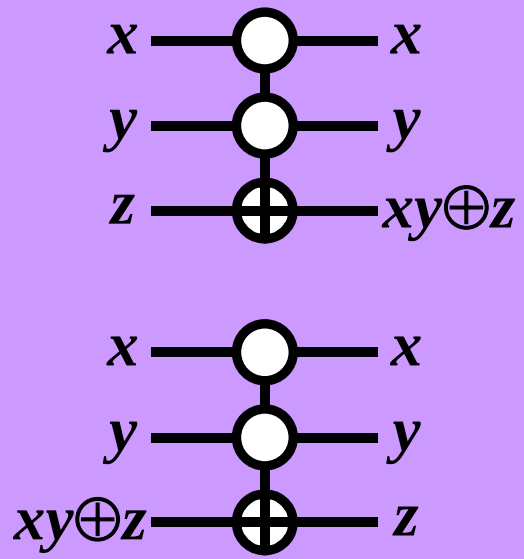
NOT



CNOT
(Controlled NOT)



Toffoli's
CCNOT
(Controlled Controlled NOT)

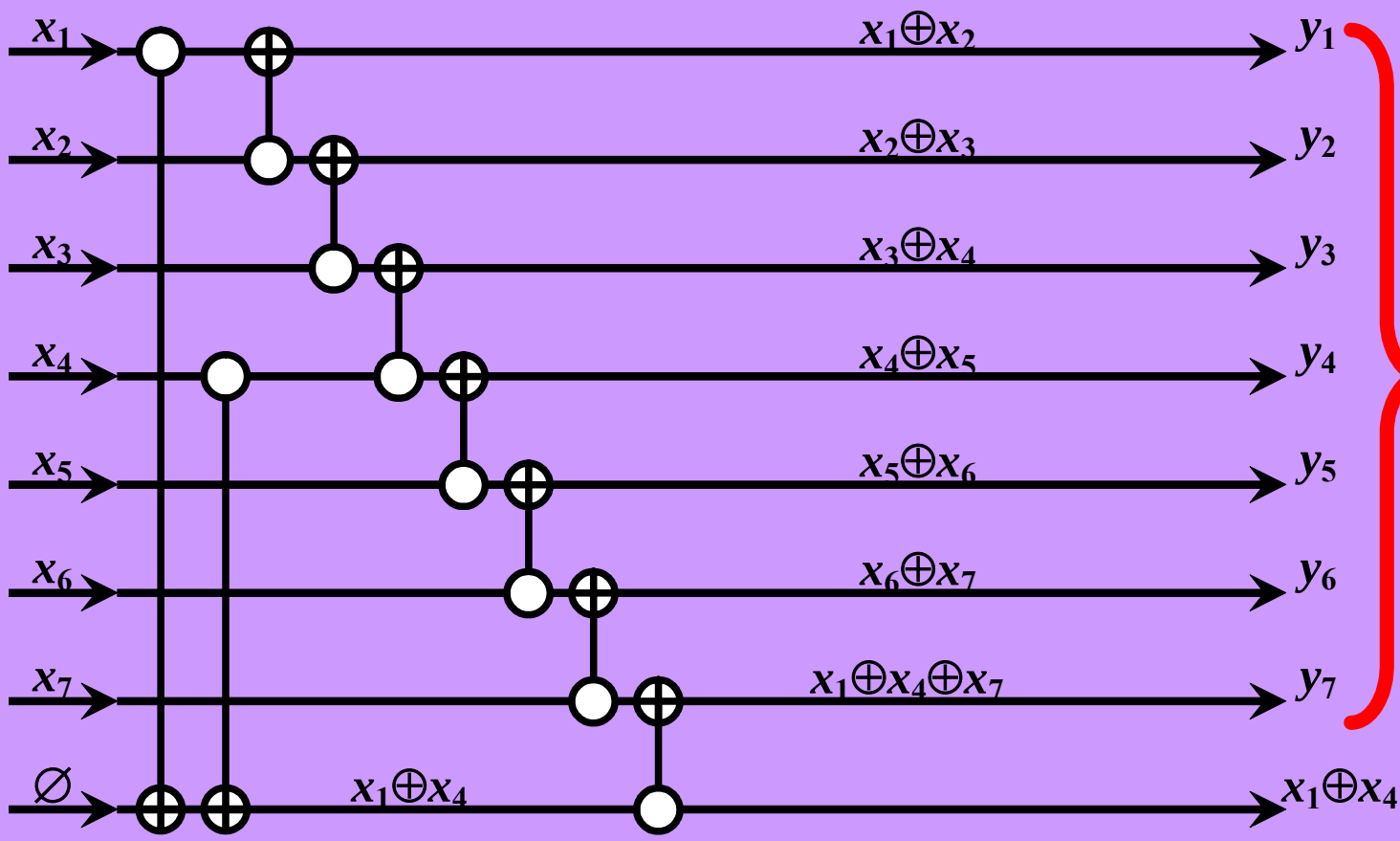


Reversible-gates Circuit

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

for odd $n \geq 7$ **:**

$$L(\mathbf{A}) = n+1 \underset{(n=7)}{=} 8$$

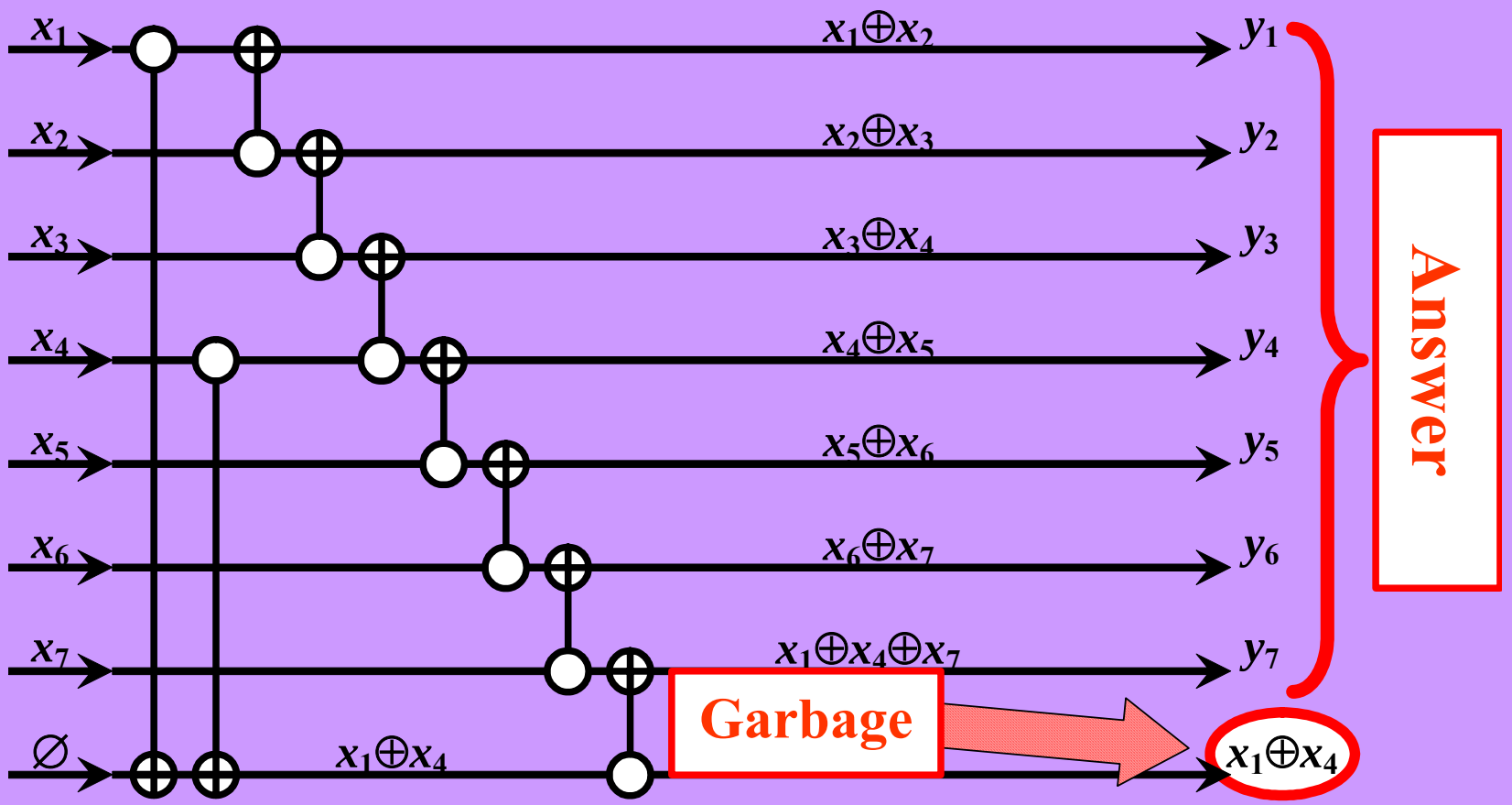


Reversible-gates Circuit

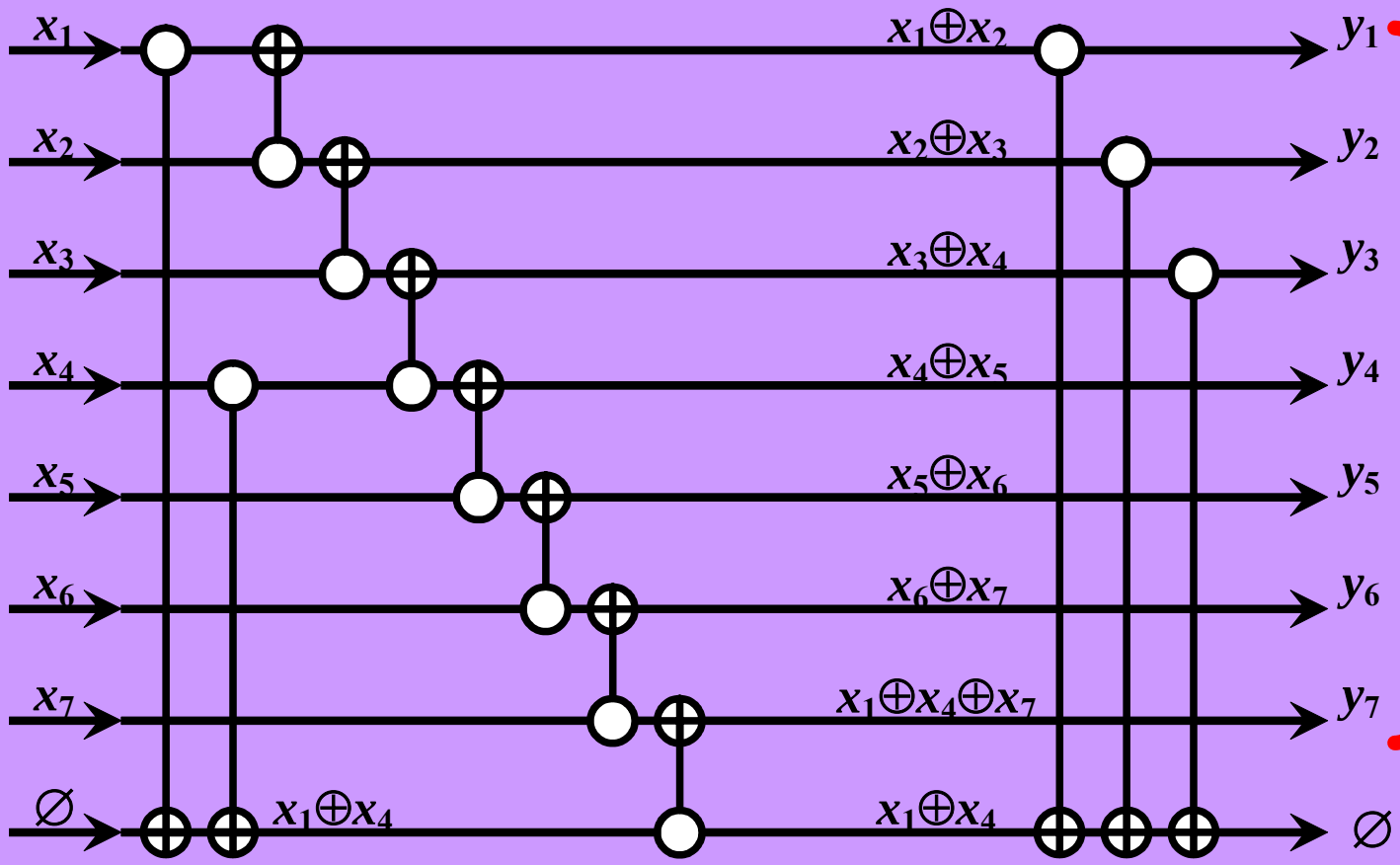
$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

for odd $n \geq 7$ **:**

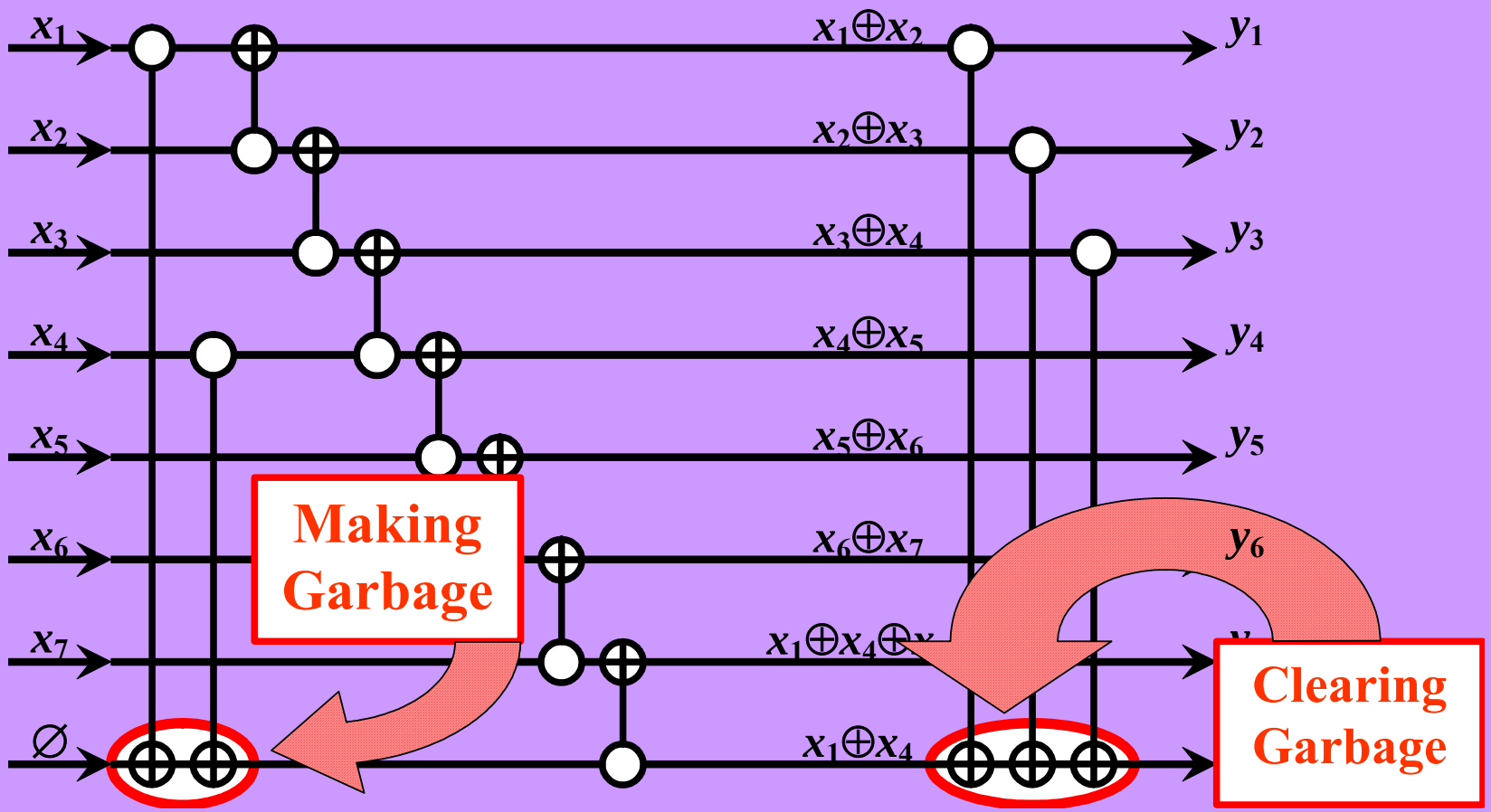
$$L(\mathbf{A}) = n + 1 \underset{(n=7)}{=} 8$$



Reversible Circuit

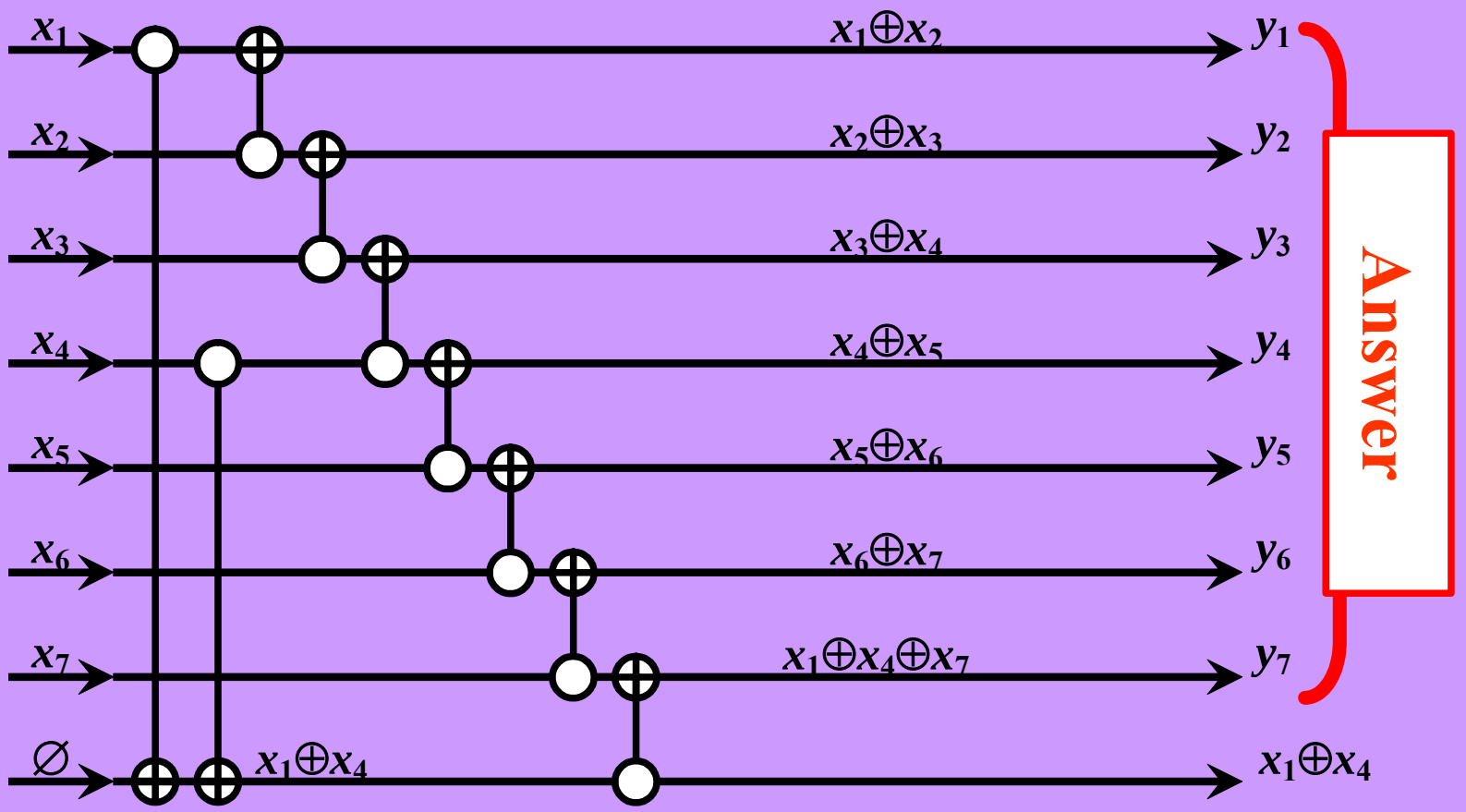


Reversible Circuit



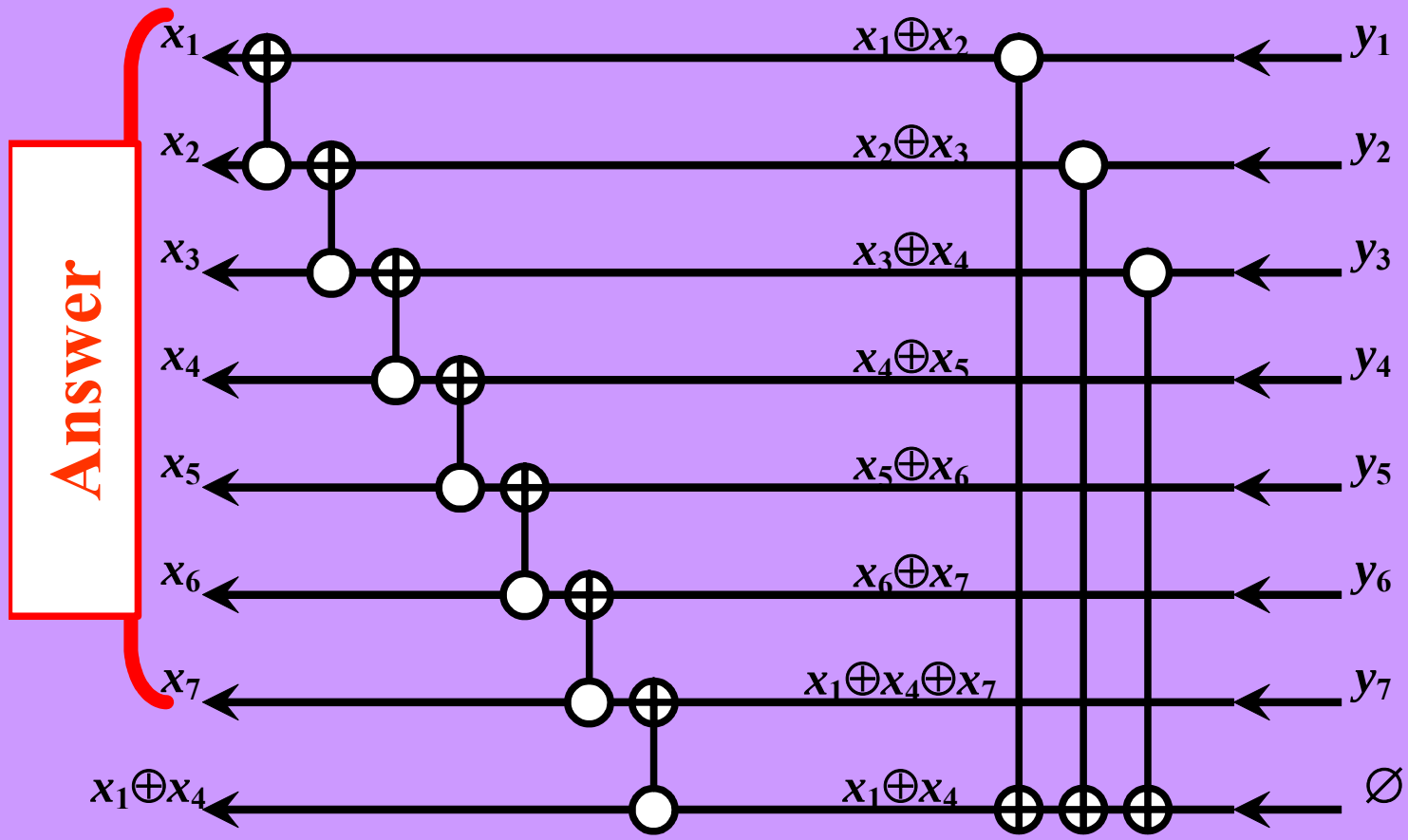
for odd $n \geq 7$ **:**

$$L(\mathbf{A}) = n+1 \underset{(n=7)}{=} 8$$



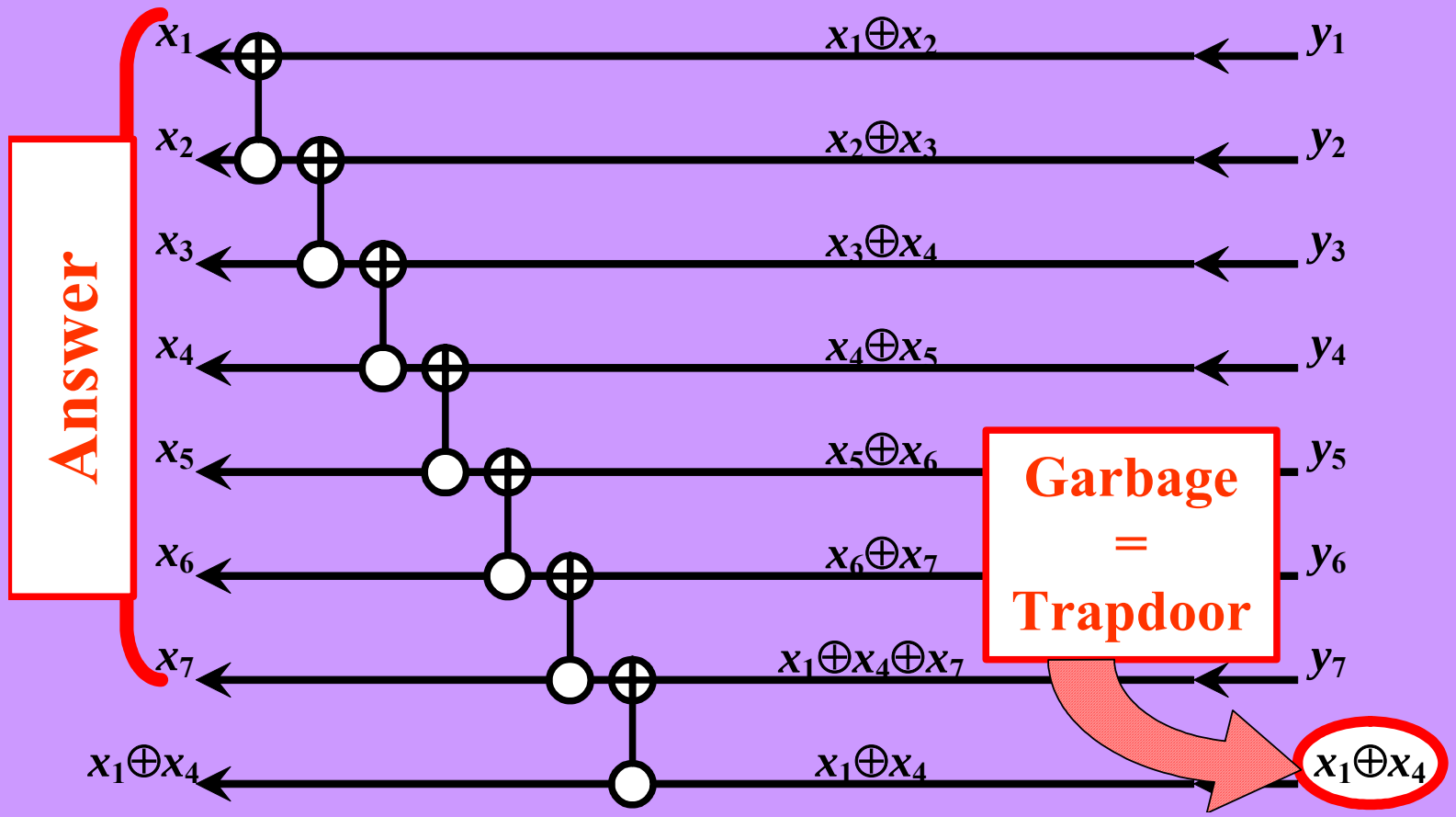
for odd $n \geq 7$ **:**

$$L(\mathbf{A}^{-1}) = \frac{3}{2}(n-1) \underset{(n=7)}{=} 9$$



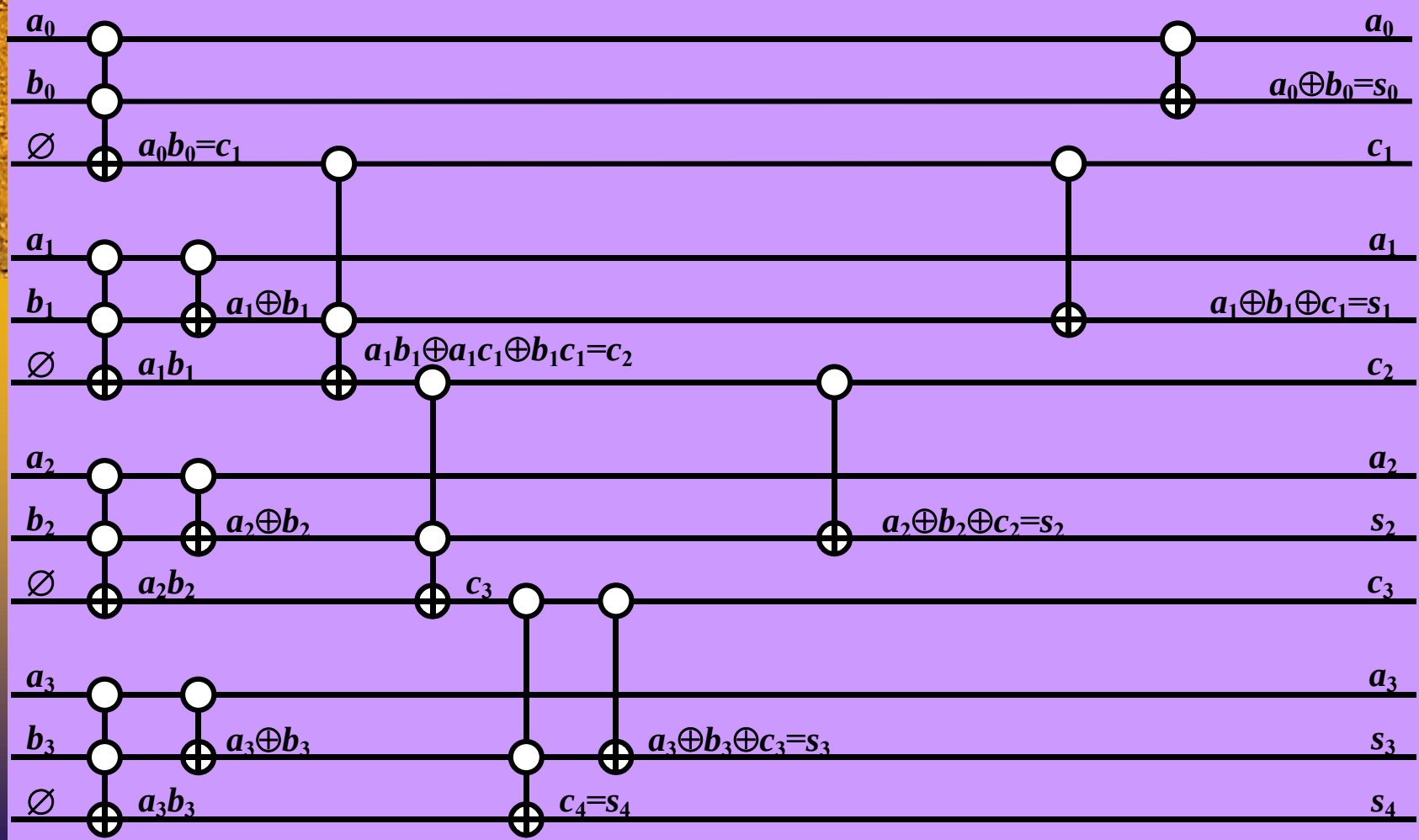
for odd $n \geq 7$ **:**

$$L(\mathbf{A}^{-1}) = n \underset{(n=7)}{=} 7$$

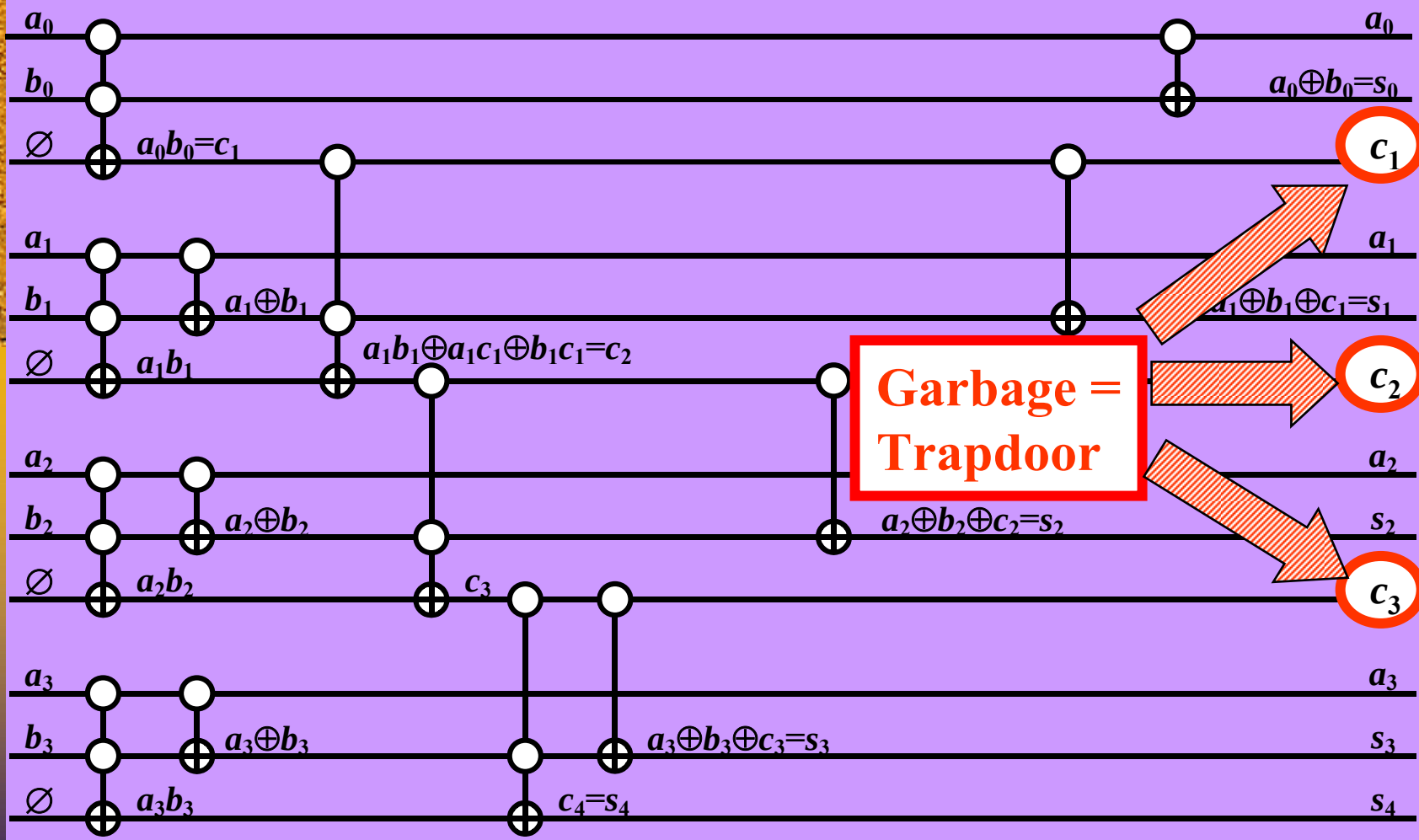


Reversible-gates Circuit for Two-number Adder

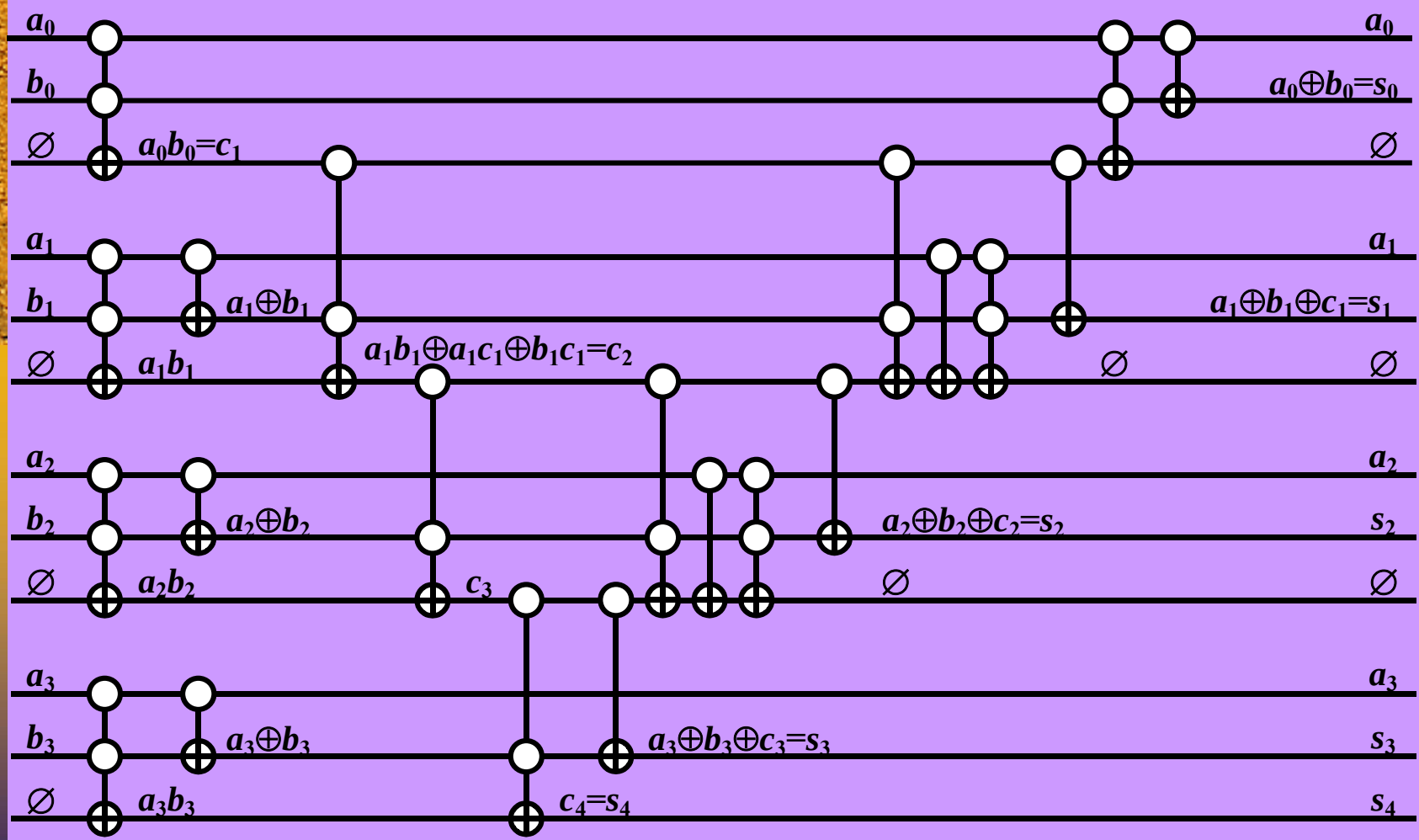
$L = 5n - 3$: Red'kin N.L. *Minimal realization of a binary adder.* Probl. Kibern., 38 (1981), pp. 181-216



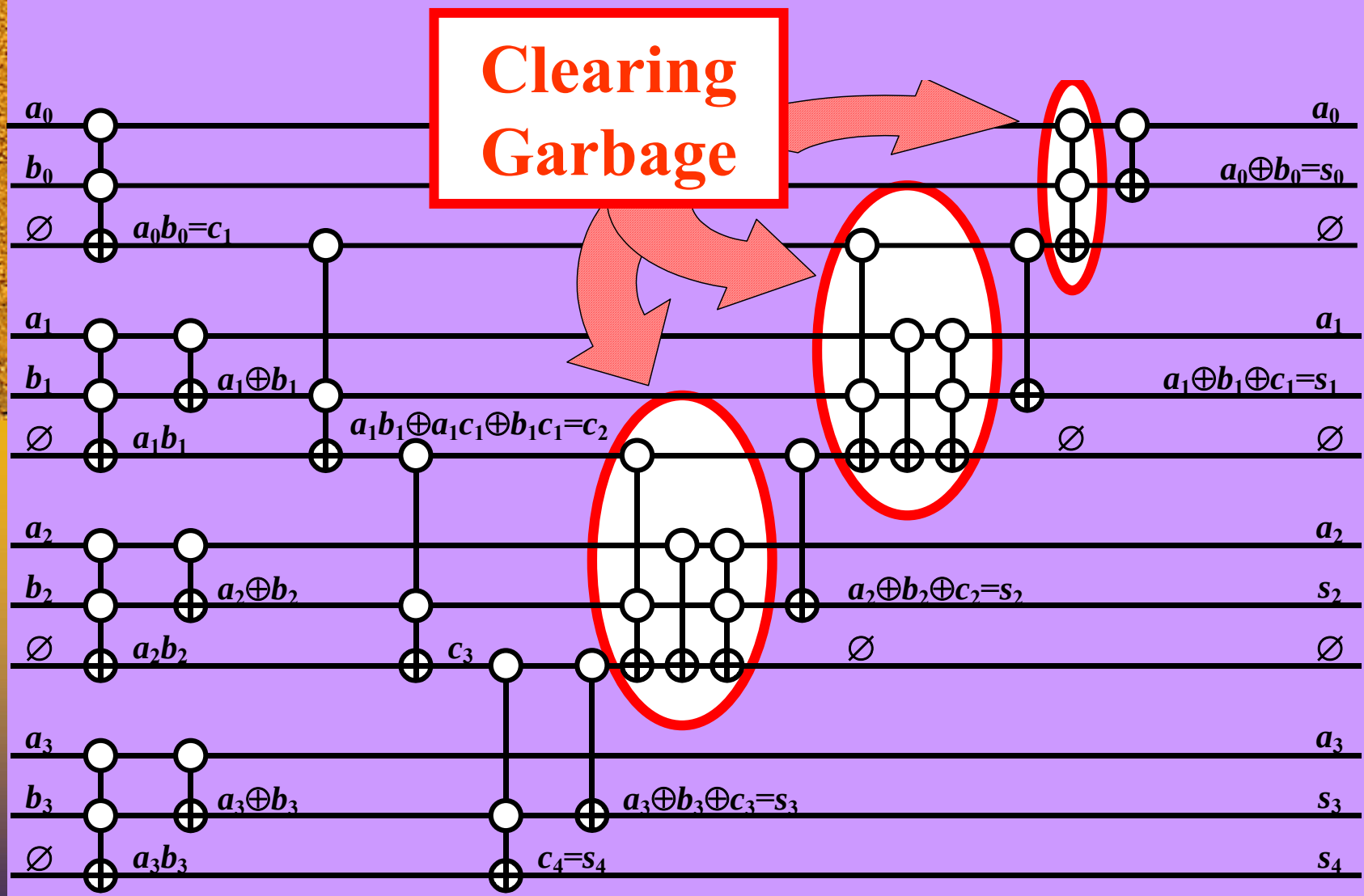
Reversible-gates Circuit for Two-number Adder



Reversible Circuit for Two-number Adder



Reversible Circuit for Two-number Adder



Reversible Circuit for Two-number Adder