

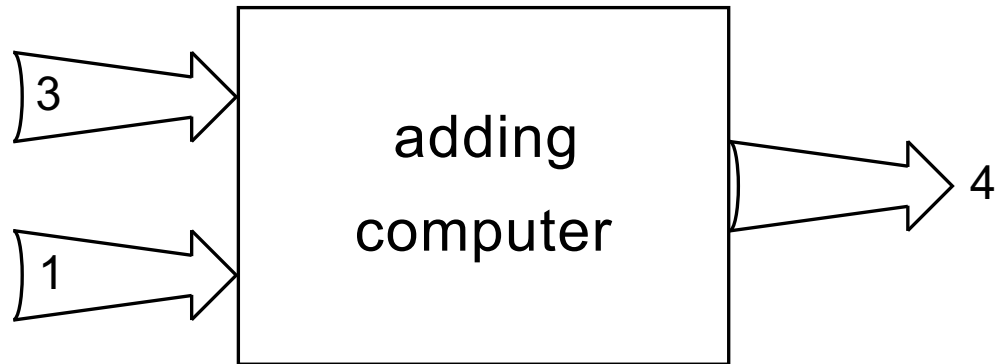
Group theory for reversible logic

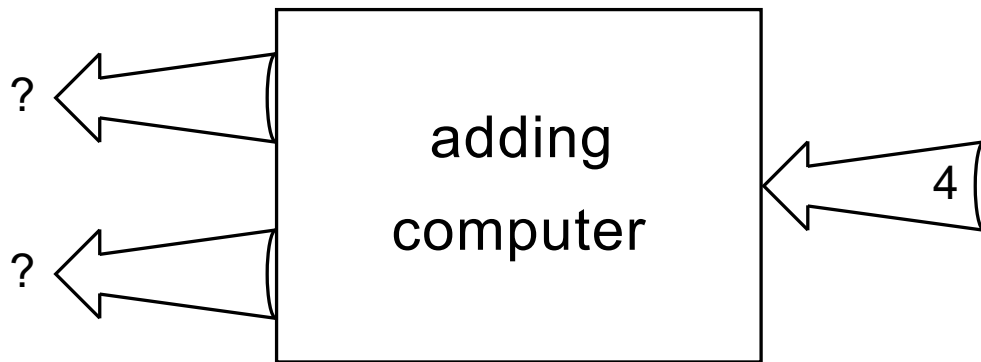
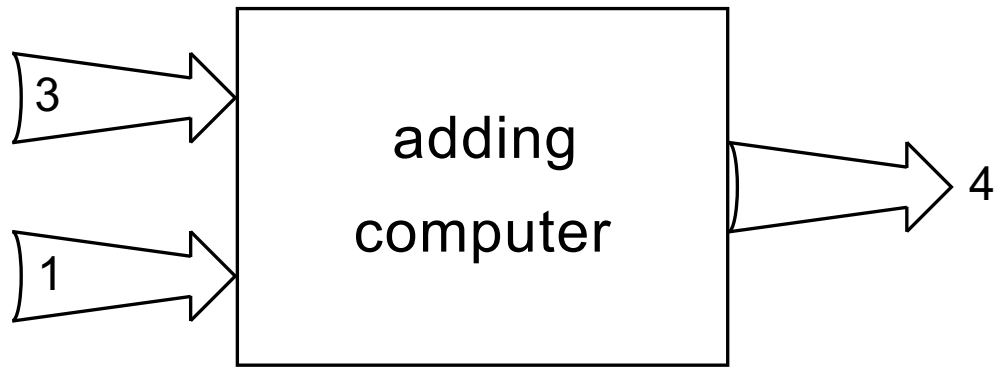
Alexis De Vos and Yvan Van Rentergem
Imec v.z.w. and Universiteit Gent
Belgium

Freiberg, 22 September 2006

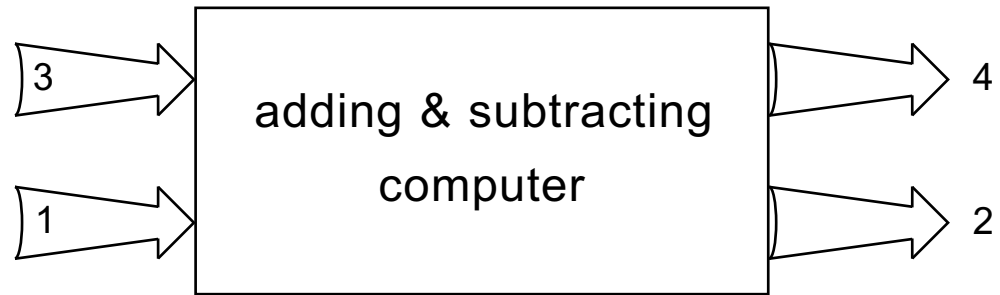


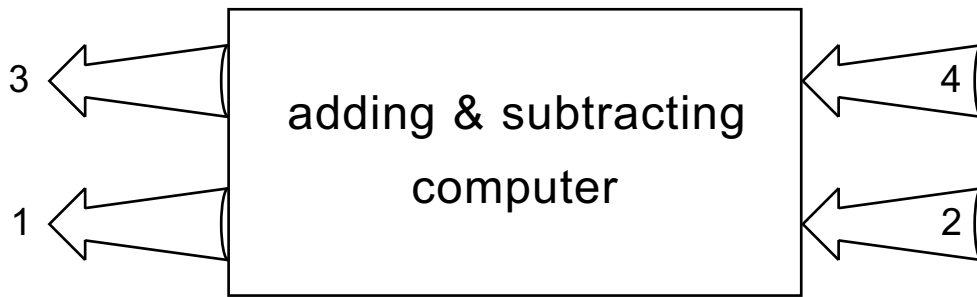
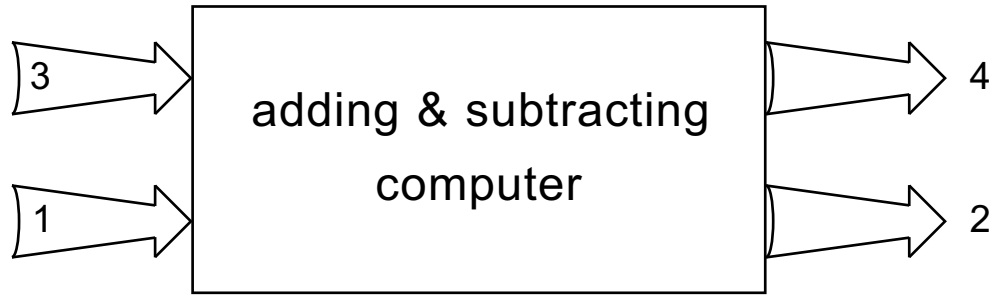
A logically irreversible computer

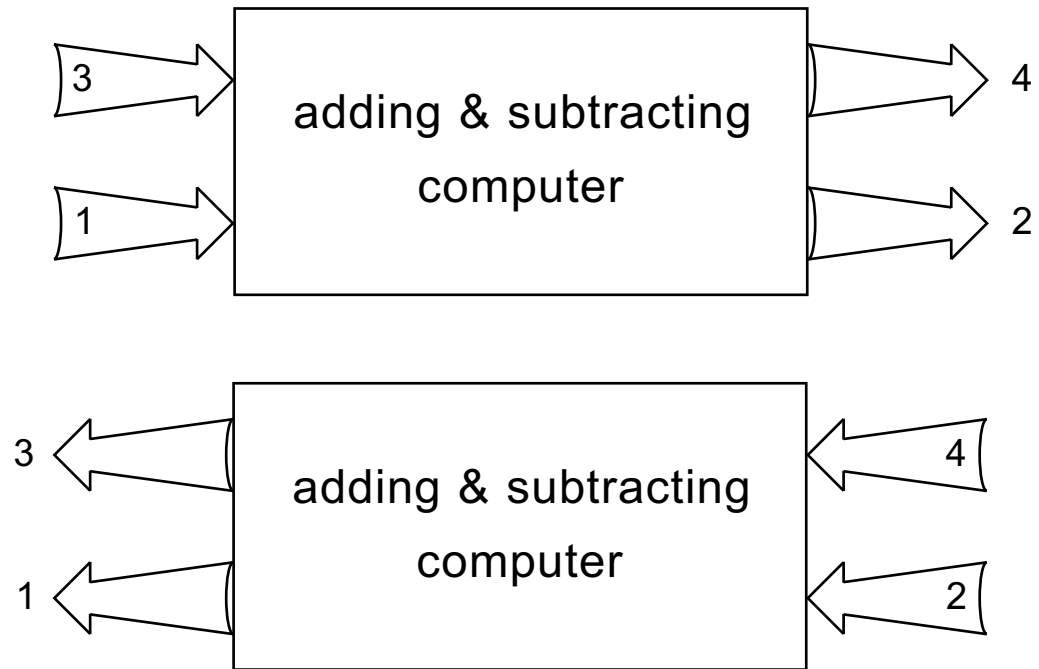




A logically reversible computer :







$$\begin{cases} P = A + B \\ Q = A - B \end{cases}$$
$$\Rightarrow \begin{cases} A = \frac{1}{2} P + \frac{1}{2} Q \\ B = \frac{1}{2} P - \frac{1}{2} Q \end{cases}$$

Groups

A group G consists of :

- a set S and
- an operation Ω .

Set and operation have to fulfil conditions :

- S has to be closed :
 $a \Omega b \in S$
- Ω has to be associative :
 $(a \Omega b) \Omega c = a \Omega (b \Omega c)$
- S has to have an identity element :
 $a \Omega i = a$
- each element of S has to have an inverse in S :
 $a \Omega a^{-1} = i$

Truth table of three reversible logic gates of width 2

(a) an arbitrary reversible gate r

(b) the identity gate i

(c) the inverse r^{-1} of r

AB	PQ
0 0	0 0
0 1	1 0
1 0	1 1
1 1	0 1

(a)

AB	PQ
0 0	0 0
0 1	0 1
1 0	1 0
1 1	1 1

(b)

AB	PQ
0 0	0 0
0 1	1 1
1 0	0 1
1 1	1 0

(c)

The group of reversible gates of width w is isomorphic to the symmetric group \mathbf{S}_{2^w} . Its order is $(2^w)!$.

Truth table of reversible logic gates ($w = 3$)

(a) a linear gate

(b) a selective gate

(c) an exchanging gate

<i>ABC</i>	<i>PQR</i>
0 0 0	1 0 0
0 0 1	0 0 0
0 1 0	0 0 1
0 1 1	1 0 1
1 0 0	1 1 1
1 0 1	0 1 1
1 1 0	0 1 0
1 1 1	1 1 0

(a)

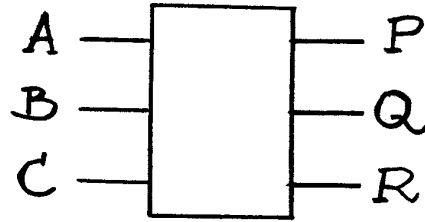
<i>ABC</i>	<i>PQR</i>
0 0 0	1 0 0
0 0 1	1 0 1
0 1 0	0 0 0
0 1 1	0 0 1
1 0 0	1 1 0
1 0 1	1 1 1
1 1 0	0 1 0
1 1 1	0 1 1

(b)

<i>ABC</i>	<i>PQR</i>
0 0 0	0 0 0
0 0 1	0 0 1
0 1 0	1 0 0
0 1 1	1 0 1
1 0 0	0 1 0
1 0 1	0 1 1
1 1 0	1 1 0
1 1 1	1 1 1

(c)

Subgroups



The subgroup of linear reversible gates

The Reed–Muller expansion

- of a non-linear reversible gate :

$$P = B \oplus AB \oplus AC$$

$$Q = A$$

$$R = C \oplus AB \oplus AC .$$

- of a linear reversible gate :

$$P = 1 \oplus B \oplus C$$

$$Q = A$$

$$R = A \oplus B .$$

$$\begin{pmatrix} P \\ Q \\ R \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \oplus \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} A \\ B \\ C \end{pmatrix} .$$

This subgroup is isomorphic to

the affine general linear group $AGL(w, 2)$.

Its order is $2^{(w+1)w/2} w!_2$,

where $w!_2$ is the bifactorial of w :

$$w!_2 = 1(1+2)(1+2+2^2)\dots(1+2+2^2+\dots+2^{w-1}) .$$

The number r of reversible gates
the number l of linear reversible gates

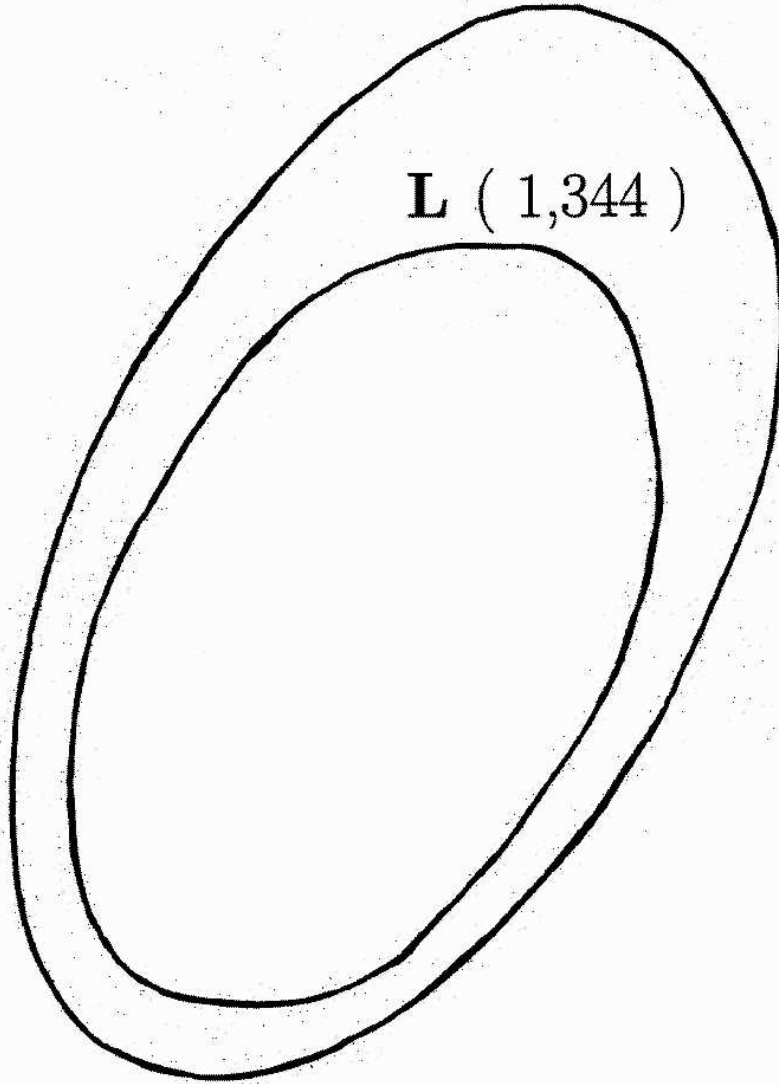
w	r	l
1	2	2
2	24	24
3	40,320	1,344
4	20,922,789,888,000	322,560

$$r(w) = (2^w)!$$

$$l(w) = 2^{(w+1)w/2} w!_2$$

R (40,320)

L (1,344)



The subgroup of univariate linear reversible gates

Each output is only function of one input :

$$P = 1 \oplus B$$

$$Q = A$$

$$R = C .$$

This group isomorphic to the indirect product $\mathbf{S}_w : \mathbf{S}_2^w$.

The subgroup of exchangers

Each output equals one input :

$$P = B$$

$$Q = A$$

$$R = C .$$

This group isomorphic to the symmetric group \mathbf{S}_w .

A trivial subgroup

Each output equals its corresponding input :

$$P = A$$

$$Q = B$$

$$R = C .$$

This results in the trivial subgroup \mathbf{I} .

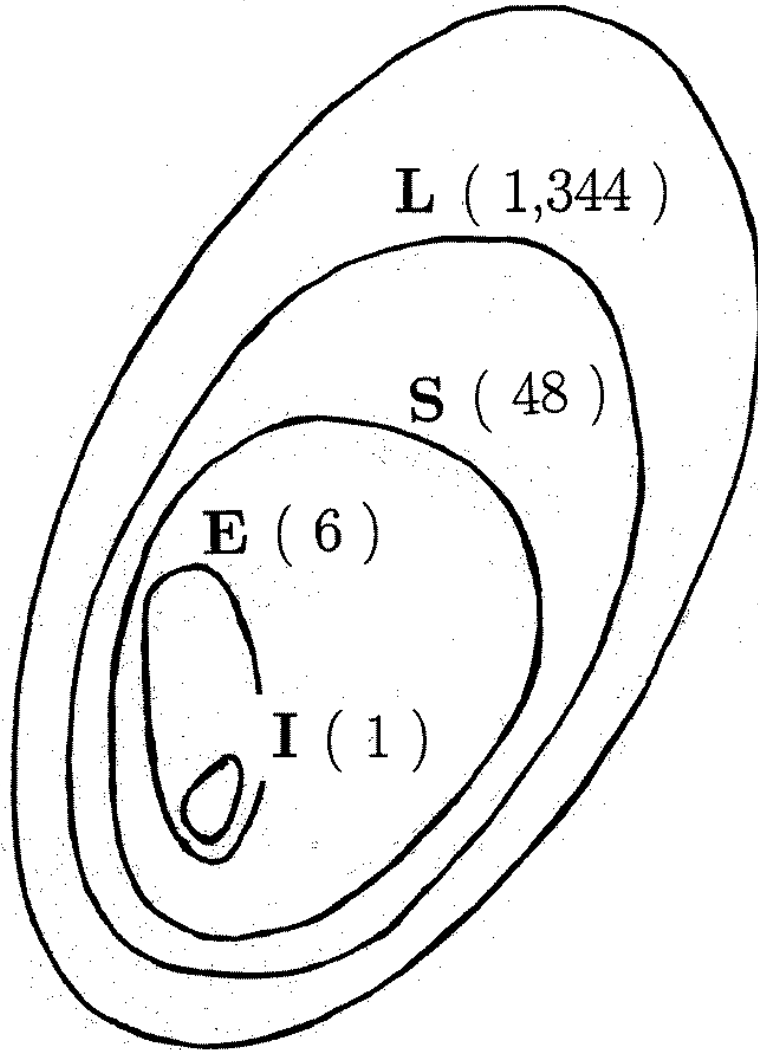
R (40,320)

L (1,344)

S (48)

E (6)

I (1)



A chain of subgroups

We have thus constructed a chain of subgroups :

$$\mathbf{S}_{2^w} \supset \mathit{AGL}(w, 2) \supset \mathbf{S}_w : \mathbf{Z}_2^w \supset \mathbf{S}_w \supset \mathbf{I} ,$$

with subsequent orders

$$(2^w)! > 2^{(w+1)w/2} w!_2 > w!2^w > w! > 1 .$$

Example $w = 3$:

$$\mathbf{S}_8 \supset \mathit{AGL}(3, 2) \supset \mathbf{S}_3 : \mathbf{S}_2^3 \supset \mathbf{S}_3 \supset \mathbf{I} ,$$

with subsequent orders

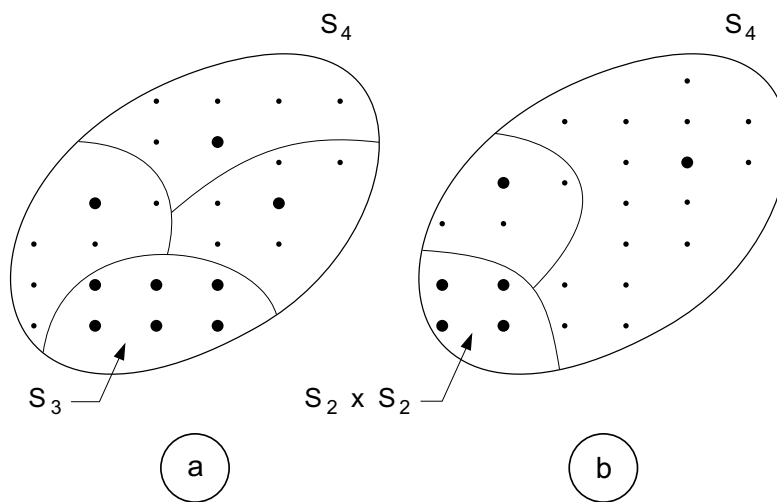
$$40,320 > 1,344 > 48 > 6 > 1 .$$

Cosets

Let a be a member of the group \mathbf{G} .

The coset of a is the set $b \Omega a$,

where b is a member of the subgroup \mathbf{H} .



The symmetric group \mathbf{S}_4 partitioned
(a) as the four left cosets of \mathbf{S}_3 .

Cosets

The coset of a is the set $b \Omega a$,
where b is a member of the subgroup \mathbf{H} .

Maslov and Dueck apply the following
chain of subgroups :

$$\mathbf{S}_8 \supset \mathbf{S}_7 \supset \mathbf{S}_6 \supset \mathbf{S}_5 \supset \mathbf{S}_4 \supset \mathbf{S}_3 \supset \mathbf{S}_2 \supset \mathbf{S}_1 = \mathbf{I} .$$

with subsequent orders

$$40,320 > 5,040 > 720 > 120 > 24 > 6 > 2 > 1 .$$

For synthesizing all 40,320 members of \mathbf{S}_8 ,
they need a library of only 28 elements.

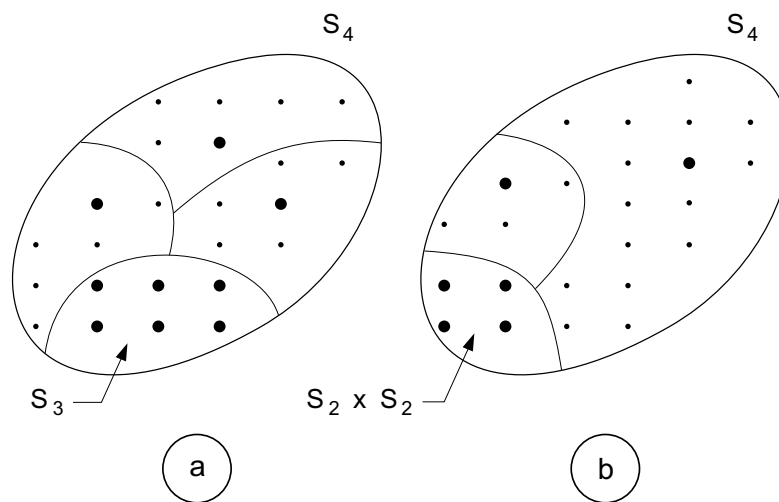
The synthesis is a cascade with length of 7 or less.

Double cosets

Let a be a member of the group \mathbf{G} .

The double coset of a is $b_1 \Omega a \Omega b_2$,

where both b_1 and b_2 are members of subgroup \mathbf{H} .



The symmetric group \mathbf{S}_4 partitioned

(a) as the four left cosets of \mathbf{S}_3

(b) as the three double cosets of $\mathbf{S}_2 \times \mathbf{S}_2$.

Double cosets

The double coset of a is $b_1 \Omega a \Omega b_2$,
where both b_1 and b_2 are members of subgroup \mathbf{H} .

Van Rentergem et al. apply the following
chain of subgroups :

$$\mathbf{S}_8 \supset \mathbf{S}_4^2 \supset \mathbf{S}_2^4 \supset \mathbf{S}_1^8 = \mathbf{I} .$$

with subsequent orders

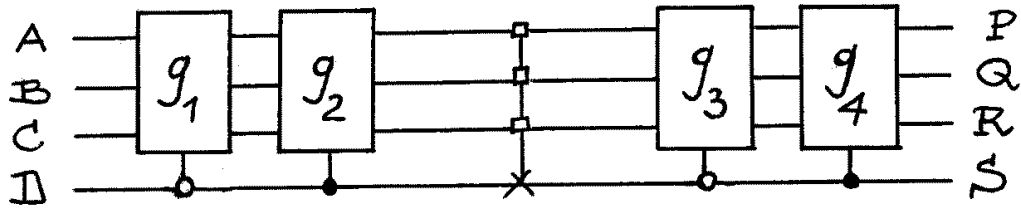
$$40,320 > 576 > 16 > 1 .$$

For synthesizing all 40,320 members of \mathbf{S}_8 ,
they need a library of only 7 elements.

The synthesis is a cascade with length of 7 or less.

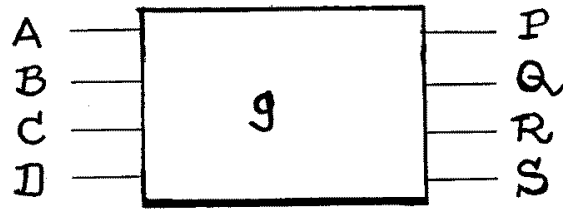


$$\in S_{16}$$

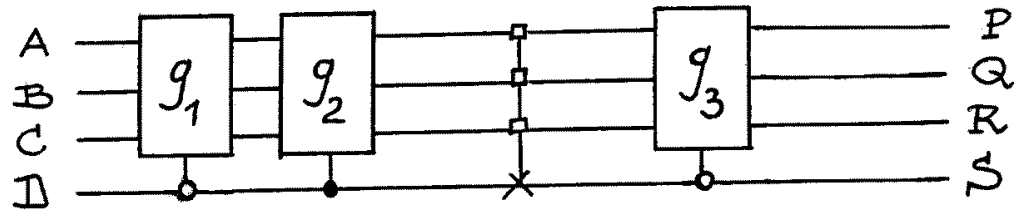


$$\underbrace{\hspace{10em}}_{\in S_8 \times S_8} \quad \underbrace{\hspace{5em}}_{\in S_2^8} \quad \underbrace{\hspace{10em}}_{\in S_8 \times S_8}$$

Synthesis according to
 double coset space
 $S_8 \times S_8 \setminus S_{16} / S_8 \times S_8$

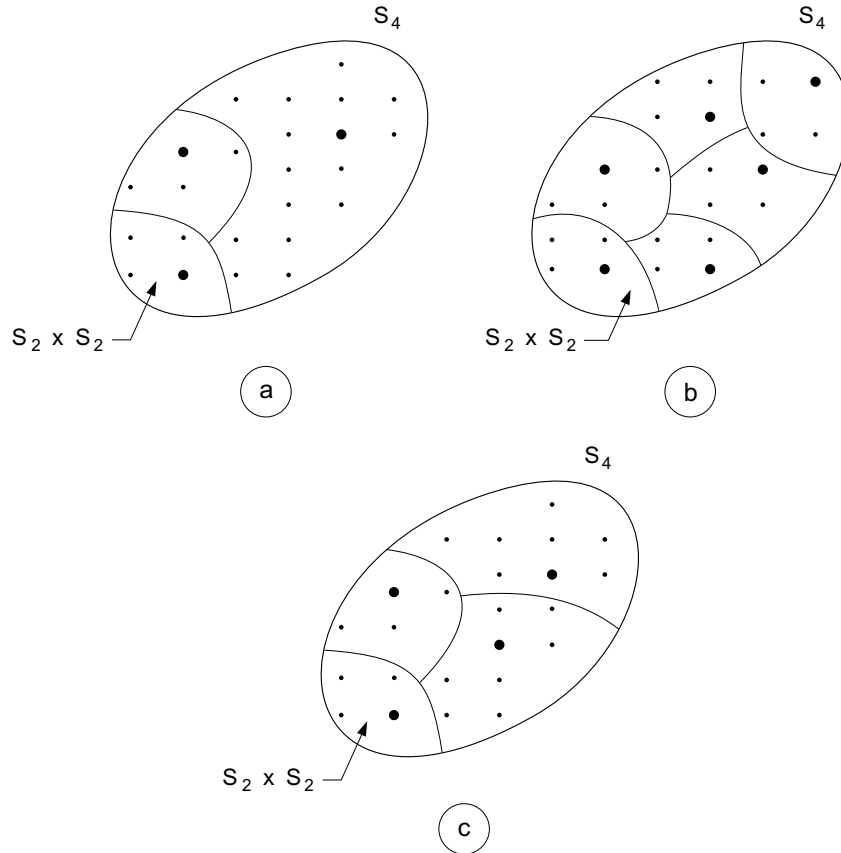


$\in S_{16}$



$\in S_8 \times S_8$ $\in S_2^8$ $\in S_8$

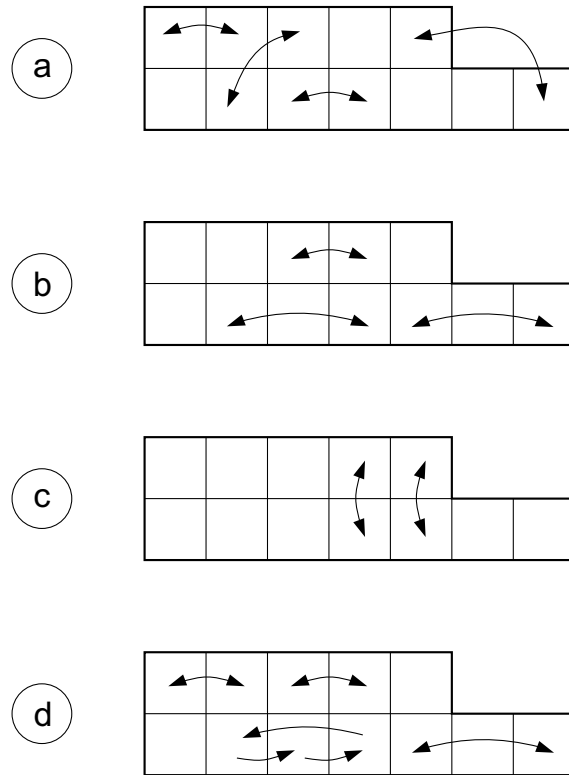
Synthesis according to
 double coset space
 $S_8 \times S_8 \setminus S_{16} / S_8$



Partitioning of \mathbf{S}_4 according to

- (a) double coset space $\mathbf{S}_2 \times \mathbf{S}_2 \backslash \mathbf{S}_4 / \mathbf{S}_2 \times \mathbf{S}_2$,
- (b) right coset space $\mathbf{S}_4 / \mathbf{S}_2 \times \mathbf{S}_2$, and
- (c) double coset space $\mathbf{S}_2 \backslash \mathbf{S}_4 / \mathbf{S}_2 \times \mathbf{S}_2$.

$$\mathbf{S}_{12} = \mathbf{S}_{5+7}$$



Mappings:

(a) arbitrary mapping $a \in \mathbf{S}_{12}$

(b-d) its decomposition into three mappings :

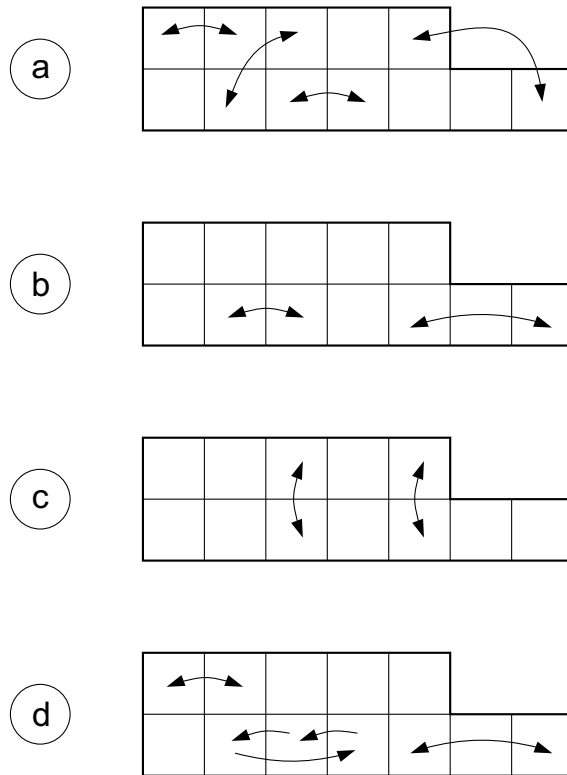
$$a = h_1 v h_2 \quad \text{with}$$

$$h_1 \in \mathbf{S}_5 \times \mathbf{S}_7$$

$$v \in \mathbf{S}_2 \times \mathbf{S}_2 \times \mathbf{S}_2 \times \mathbf{S}_2 \times \mathbf{S}_2 \quad \text{and}$$

$$h_2 \in \mathbf{S}_5 \times \mathbf{S}_7$$

$$\mathbf{S}_{12} = \mathbf{S}_{5+7}$$



Mappings:

(a) arbitrary mapping $a \in \mathbf{S}_{12}$

(b-d) its decomposition into three mappings :

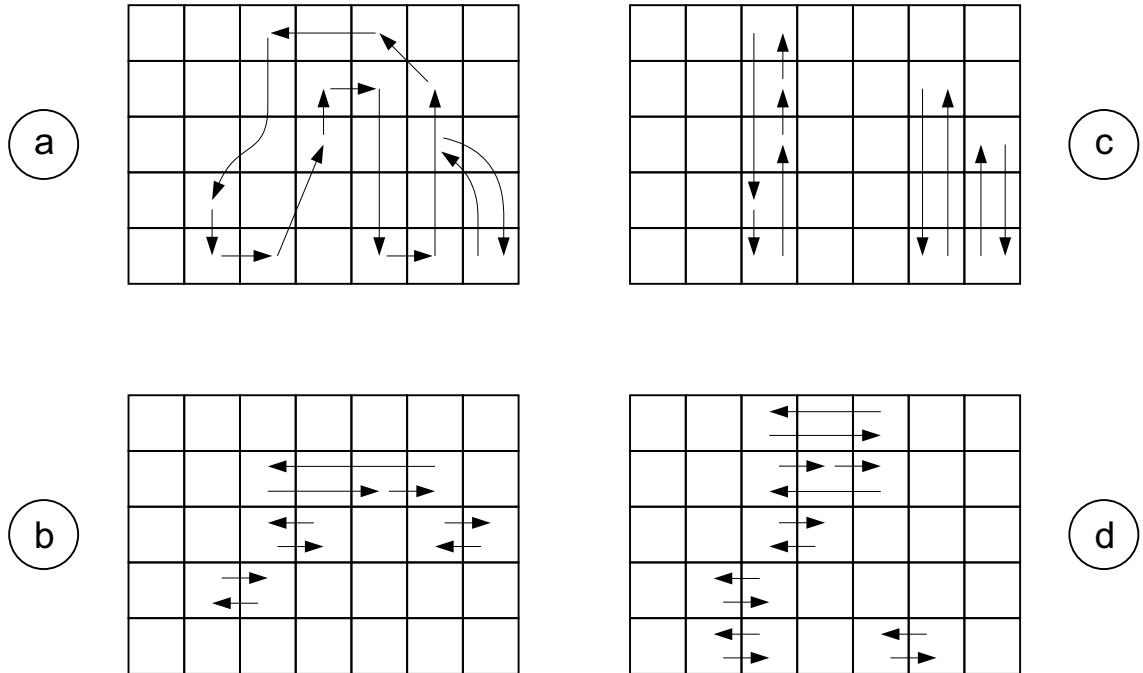
$$a = h_1 v h_2 \quad \text{with}$$

$$h_1 \in \mathbf{S}_7$$

$$v \in \mathbf{S}_2 \times \mathbf{S}_2 \times \mathbf{S}_2 \times \mathbf{S}_2 \times \mathbf{S}_2 \quad \text{and}$$

$$h_2 \in \mathbf{S}_5 \times \mathbf{S}_7$$

$$\mathbf{S}_{35} = \mathbf{S}_{5 \times 7}$$



Mappings:

(a) arbitrary mapping $a \in \mathbf{S}_{12}$

(b-d) its decomposition into three mappings :

$$a = h_1 v h_2 \quad \text{with}$$

$$h_1 \in \mathbf{S}_7 \times \mathbf{S}_7 \times \mathbf{S}_7 \times \mathbf{S}_7$$

$$v \in \mathbf{S}_5 \times \mathbf{S}_5 \times \mathbf{S}_5 \times \mathbf{S}_5 \times \mathbf{S}_5 \times \mathbf{S}_5 \times \mathbf{S}_5 \quad \text{and}$$

$$h_2 \in \mathbf{S}_7 \times \mathbf{S}_7 \times \mathbf{S}_7 \times \mathbf{S}_7 \times \mathbf{S}_7$$

Young subgroups of a symmetric group.

A **Young subgroup** of the symmetric group \mathbf{S}_a is any subgroup isomorphic to

$$\mathbf{S}_{a_1} \times \mathbf{S}_{a_2} \times \dots \times \mathbf{S}_{a_k}$$

with (a_1, a_2, \dots, a_k) a partition of the number a ,

i.e. with $a_1 + a_2 + \dots + a_k = a$.

The subgroups

$$\mathbf{S}_2^{\frac{a}{2}} = \mathbf{S}_2 \times \mathbf{S}_2 \times \dots \times \mathbf{S}_2 \quad \left(\frac{a}{2} \text{ factors}\right) \text{ and}$$

$$\mathbf{S}_{\frac{a}{2}}^2 = \mathbf{S}_{\frac{a}{2}} \times \mathbf{S}_{\frac{a}{2}} \quad (2 \text{ factors}) \text{ are called}$$

dual Young subgroups of \mathbf{S}_a

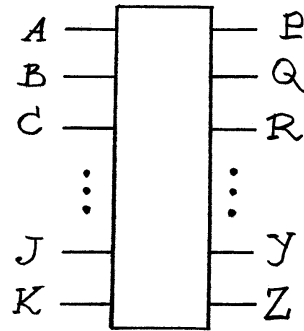
as they are based on

two dual partitions of the number a :

$$a = 2 + 2 + \dots + 2 \quad \left(\frac{a}{2} \text{ terms}\right) \text{ and}$$

$$a = \frac{a}{2} + \frac{a}{2} \quad (2 \text{ terms}).$$

Electronics



Electronic implementation is based on the subgroup of control gates :
 w inputs A, B, C, \dots, J , and K and
 w outputs P, Q, R, \dots, Y , and Z , such that :

$$\begin{aligned}P &= A \\Q &= B \\R &= C \\&\dots = \dots \\Y &= J \\Z &= f(A, B, C, \dots, J) \oplus K ,\end{aligned}$$

where f is an arbitrary boolean function of the $w - 1$ variables A, B, C, \dots, J .

The subgroup is isomorphic to $\mathbf{S}_2^{2^{w-1}}$ of order $2^{2^{w-1}}$.

Three special examples:

- If $f = 0$, then $Z = K$.
Then the gate is the identity gate i .
- If $f = 1$, then $Z = 1 \oplus K = \overline{K}$.
Then the gate is the inverter or NOT gate.
- If $f(A, B, C, \dots, J) = ABC\dots J$,
then the gate is the CONTROLLED ^{$w-1$} NOT gate
or TOFFOLI gate.

R (40,320)

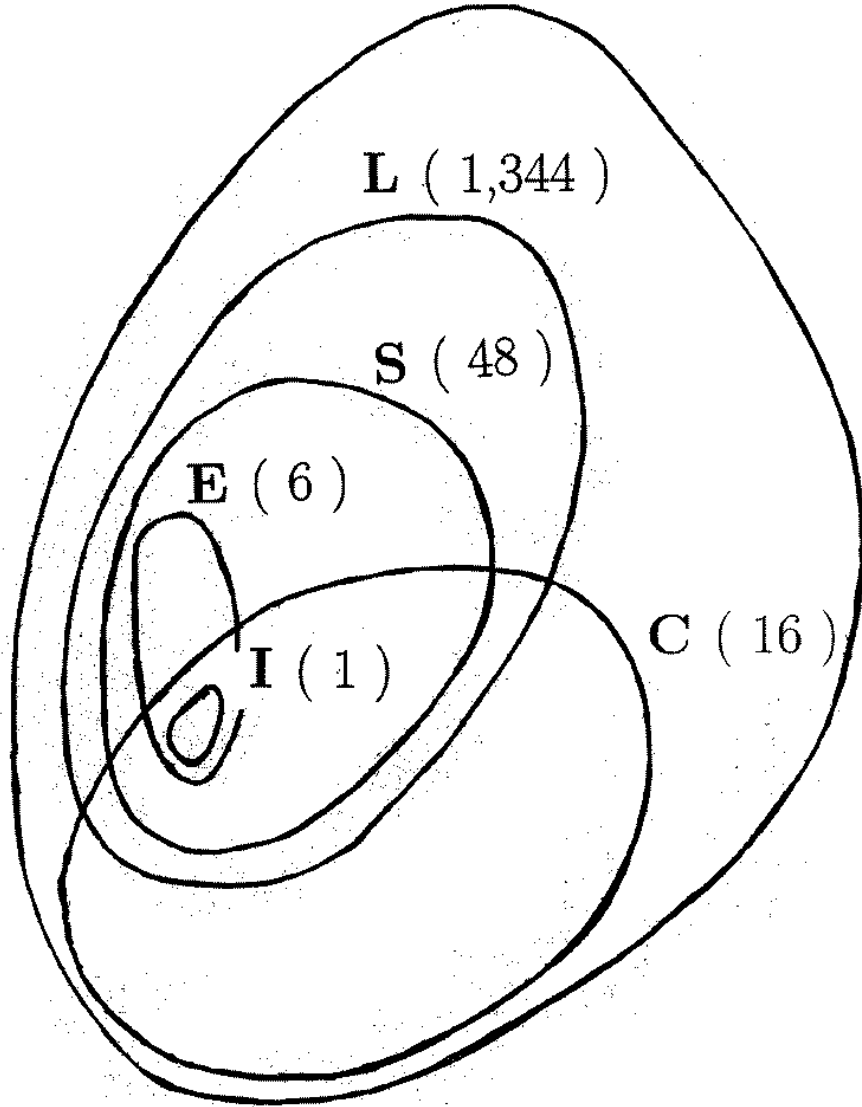
L (1,344)

S (48)

E (6)

I (1)

C (16)



The NOT gate:

$$P = \overline{A}$$

The CONTROLLED NOT gate:

$$\begin{aligned} P &= A \\ Q &= A \oplus B . \end{aligned}$$

is equivalent with

$$\begin{aligned} P &= A \\ Q &= \text{if } (A = 0) \text{ then } B \text{ else } \overline{B} . \end{aligned}$$

The CONTROLLED CONTROLLED NOT gate or TOFFOLI gate:

$$\begin{aligned} P &= A \\ Q &= B \\ R &= AB \oplus C . \end{aligned}$$

is equivalent with

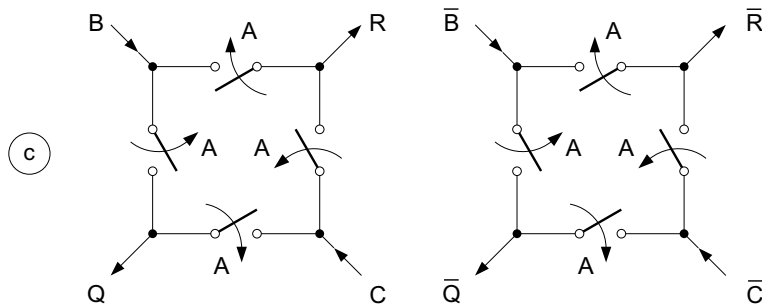
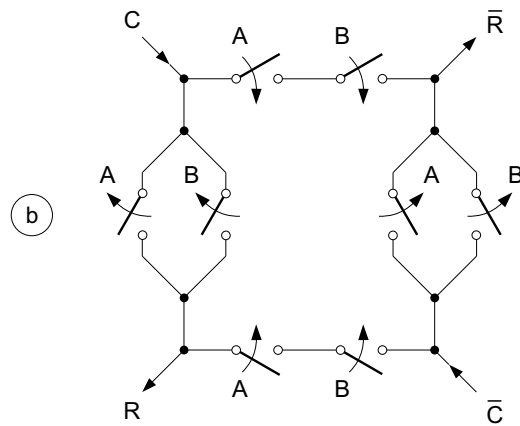
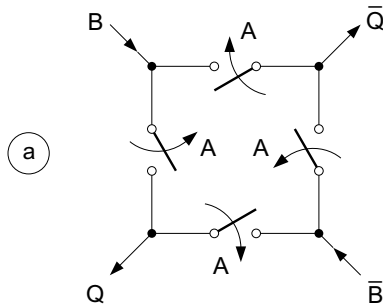
$$\begin{aligned} P &= A \\ Q &= B \\ R &= \text{if } (AB = 0) \text{ then } C \text{ else } \overline{C} . \end{aligned}$$

Schematic for

(a) CONTROLLED NOT gate

(b) CONTROLLED CONTROLLED NOT gate

(c) CONTROLLED SWAP gate



The CONTROLLED SWAP gate or FREDKIN gate :

$$P = A$$

$$Q = B \oplus AB \oplus AC$$

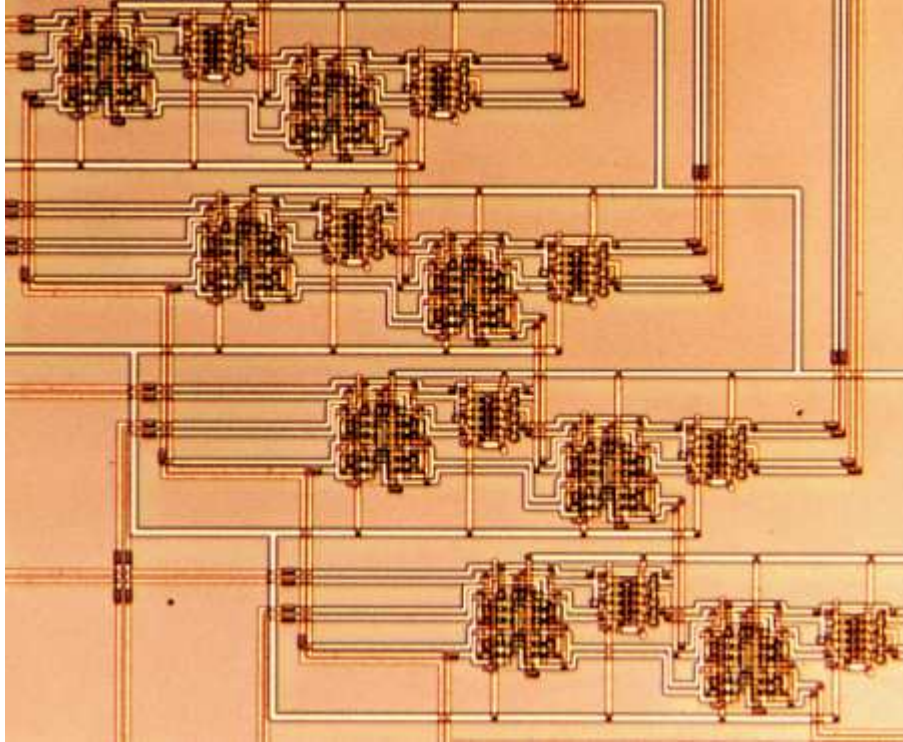
$$R = C \oplus AB \oplus AC .$$

is equivalent with

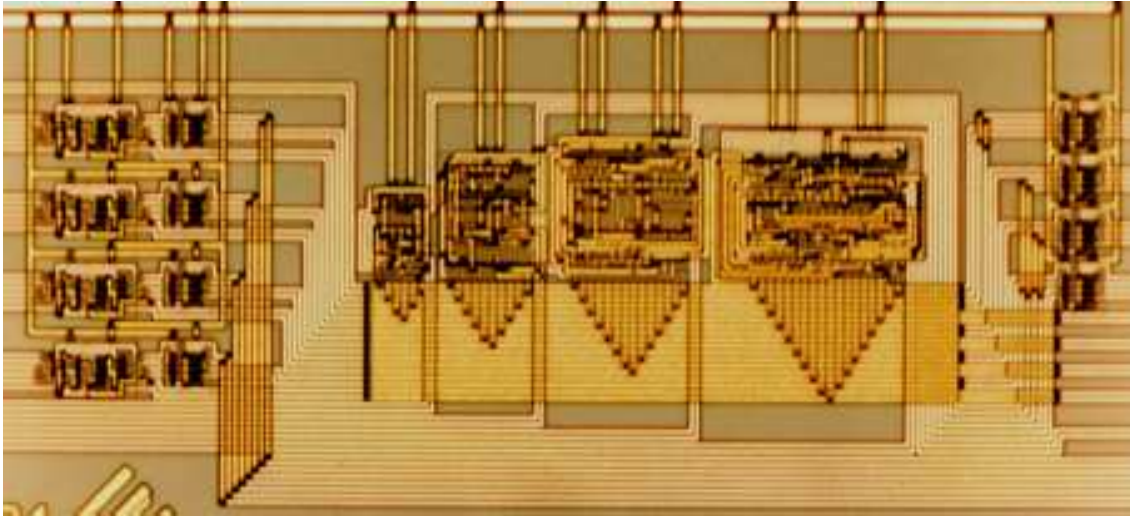
$$P = A$$

$$Q = B$$

$$R = \text{if } (A = 0) \text{ then } C \text{ else } B .$$



Microscope photograph ($140\ \mu\text{m} \times 120\ \mu\text{m}$) of $2.4\text{-}\mu\text{m}$ 4-bit reversible ripple adder.



Microscope photograph ($610 \mu\text{m} \times 290 \mu\text{m}$) of $0.8\text{-}\mu\text{m}$ 4-bit reversible carry-look-ahead adder.

