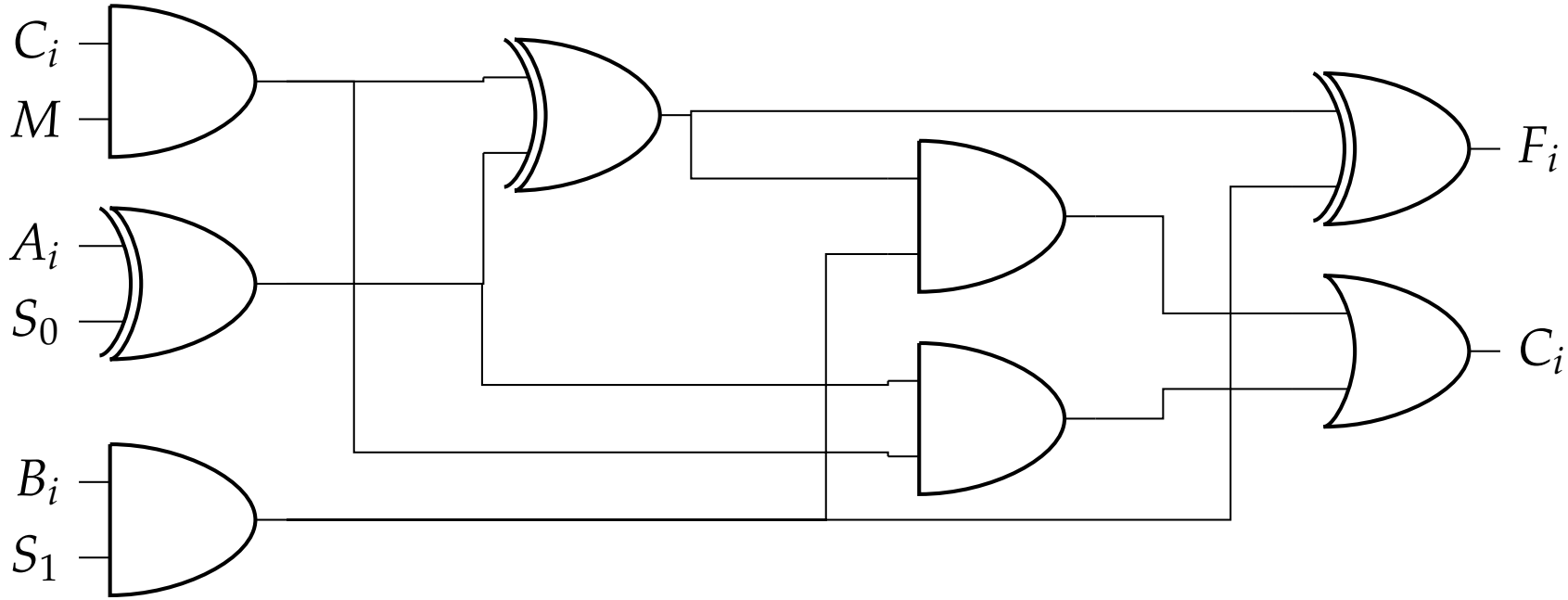
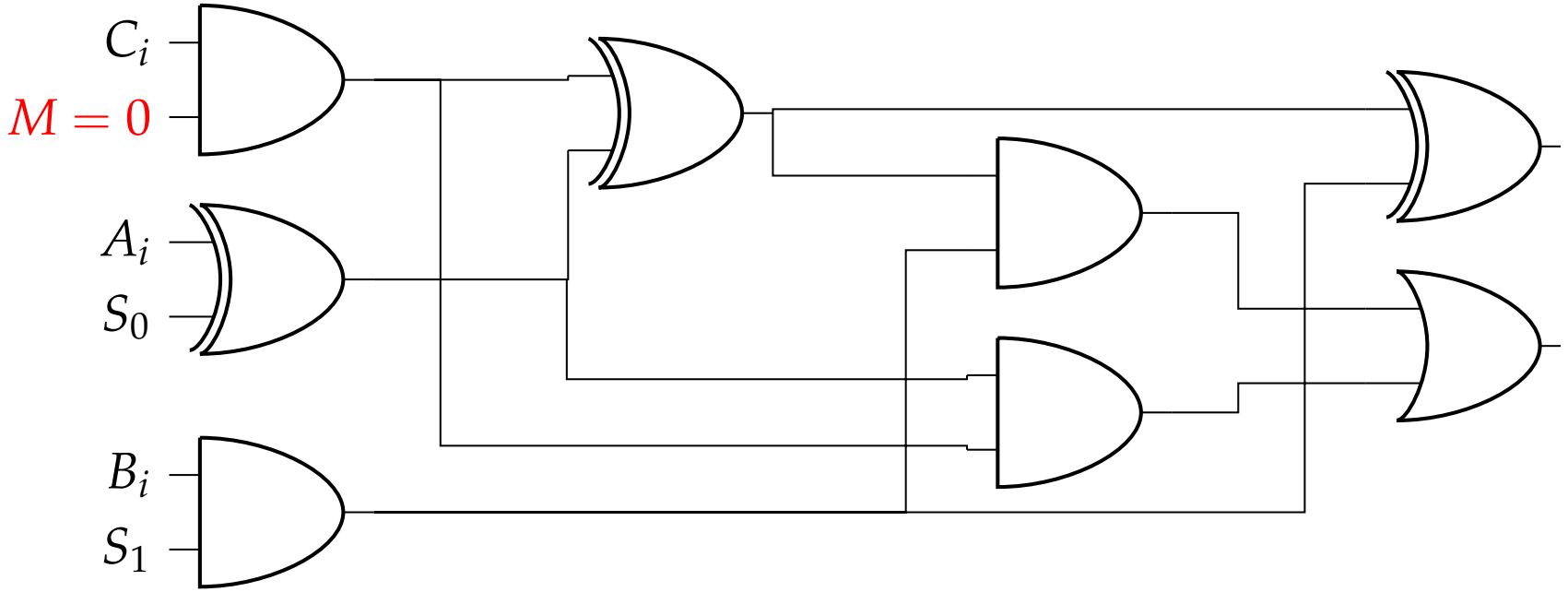
$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i$, $\quad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



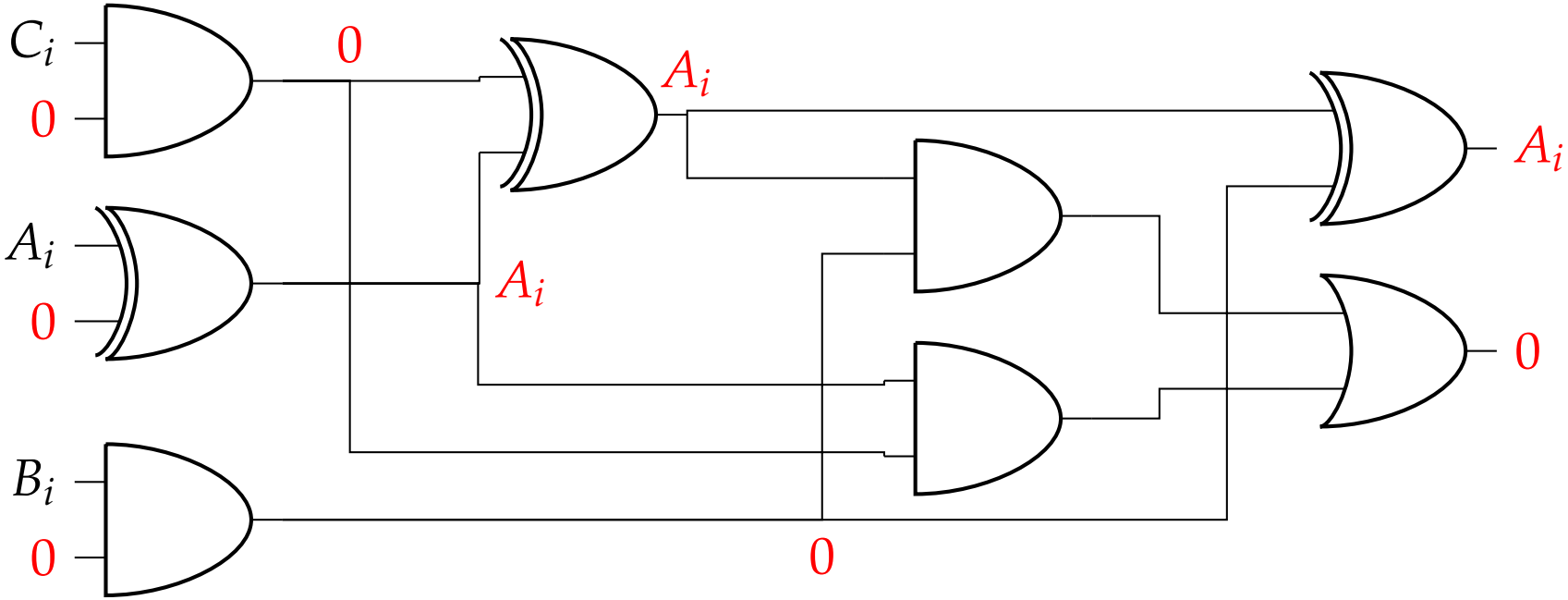
Aukeraketa.		Eragiketa logikoa $M = 0$	Eragiketa aritmetikoa $M = 1$		
S_1	S_0	F_i	F_i	C_{i+1}	Eragiketa
0	0	A_i	$A_i \oplus C_i$	$C_{i+1} = A_i C_i$	$A_i + C_i$
0	1	$\overline{A_i}$	$\overline{A_i} \oplus C_i$	$C_{i+1} = \overline{A_i} C_i$	$\overline{A_i} + C_i$
1	0	$A_i \oplus B_i$	$A_i \oplus B_i \oplus C_i$	$C_{i+1} = A_i B_i + A_i C_i + B_i C_i$	$A_i + B_i + C_i$
1	1	$\overline{A_i \oplus B_i}$	$\overline{A_i} \oplus B_i \oplus C_i$	$C_{i+1} = \overline{A_i} B_i + \overline{A_i} C_i + B_i C_i$	$\overline{A_i} + B_i + C_i$

$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i$, $\quad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



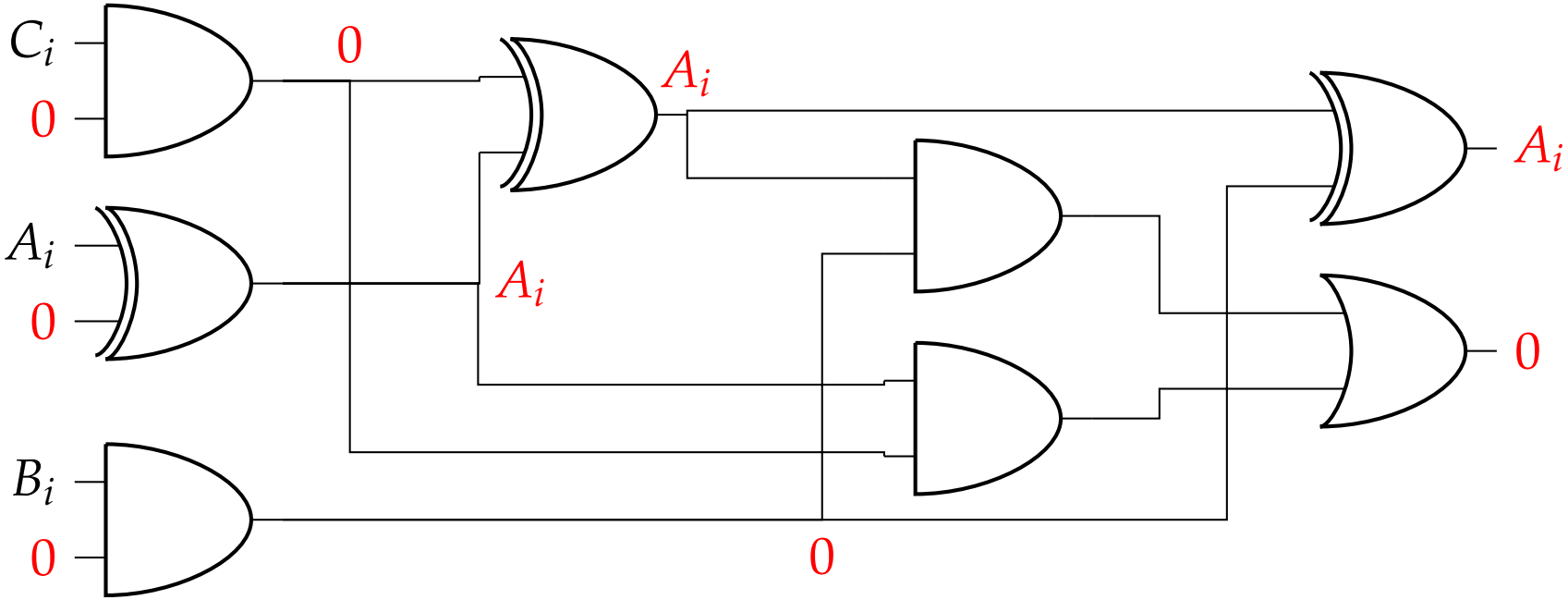
Aukeraketa.		Eragiketa logikoa $M = 0$			
S_1	S_0	F_i			

$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i$, $\quad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



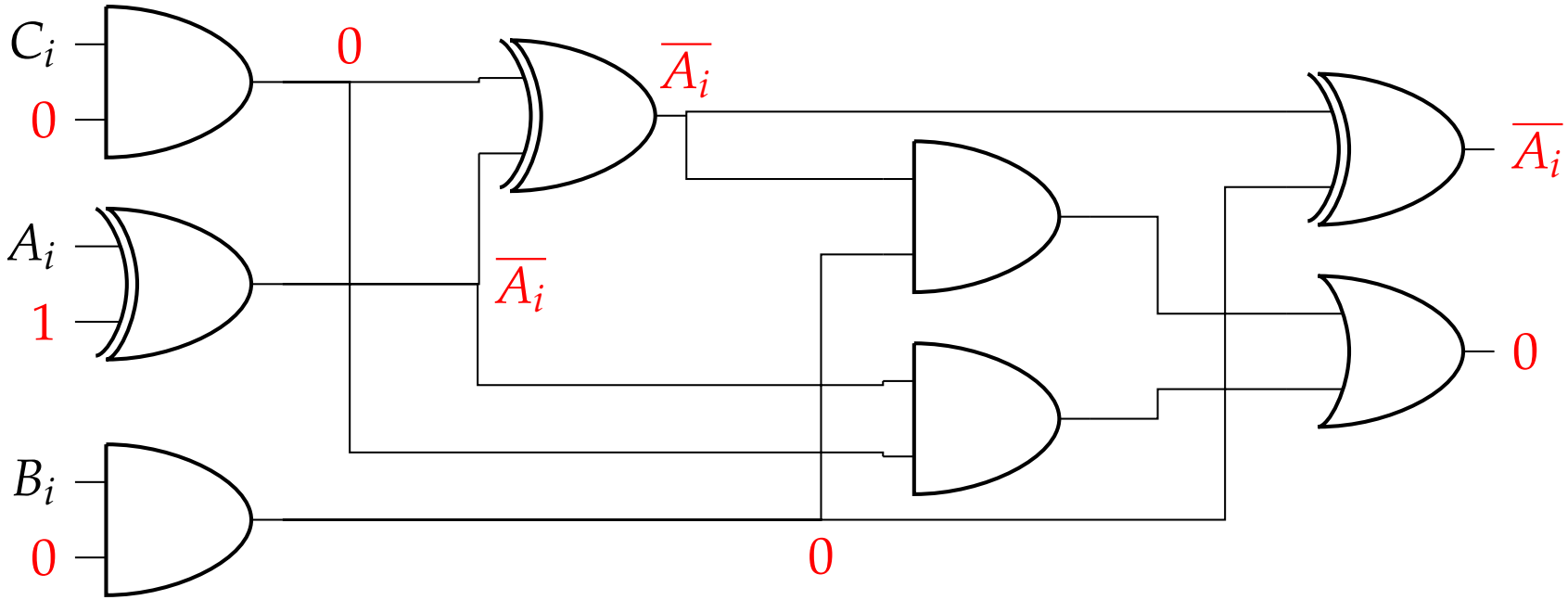
Aukeraketa.		Eragiketa logikoa $M = 0$			
S_1	S_0	F_i			
0	0				

$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i$, $\quad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



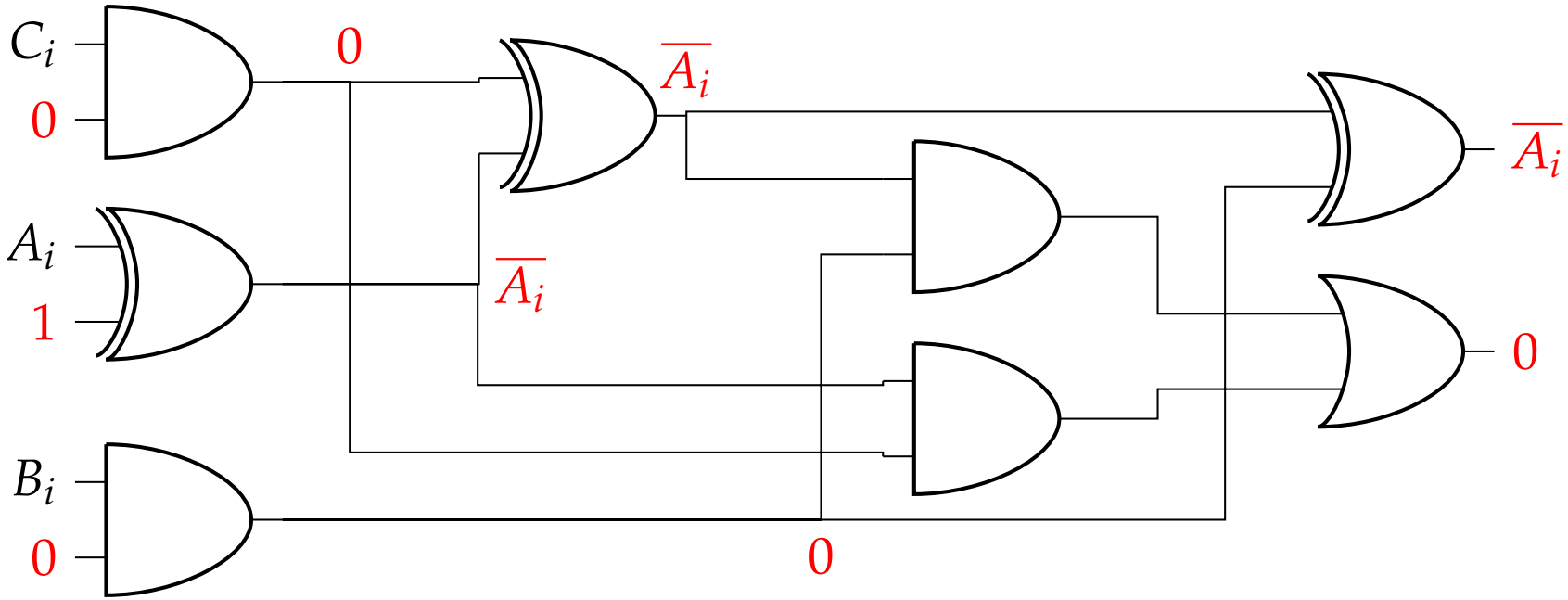
Aukeraketa.		Eragiketa logikoa $M = 0$					
S_1	S_0	F_i					
0	0	A_i					

$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i$, $\quad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



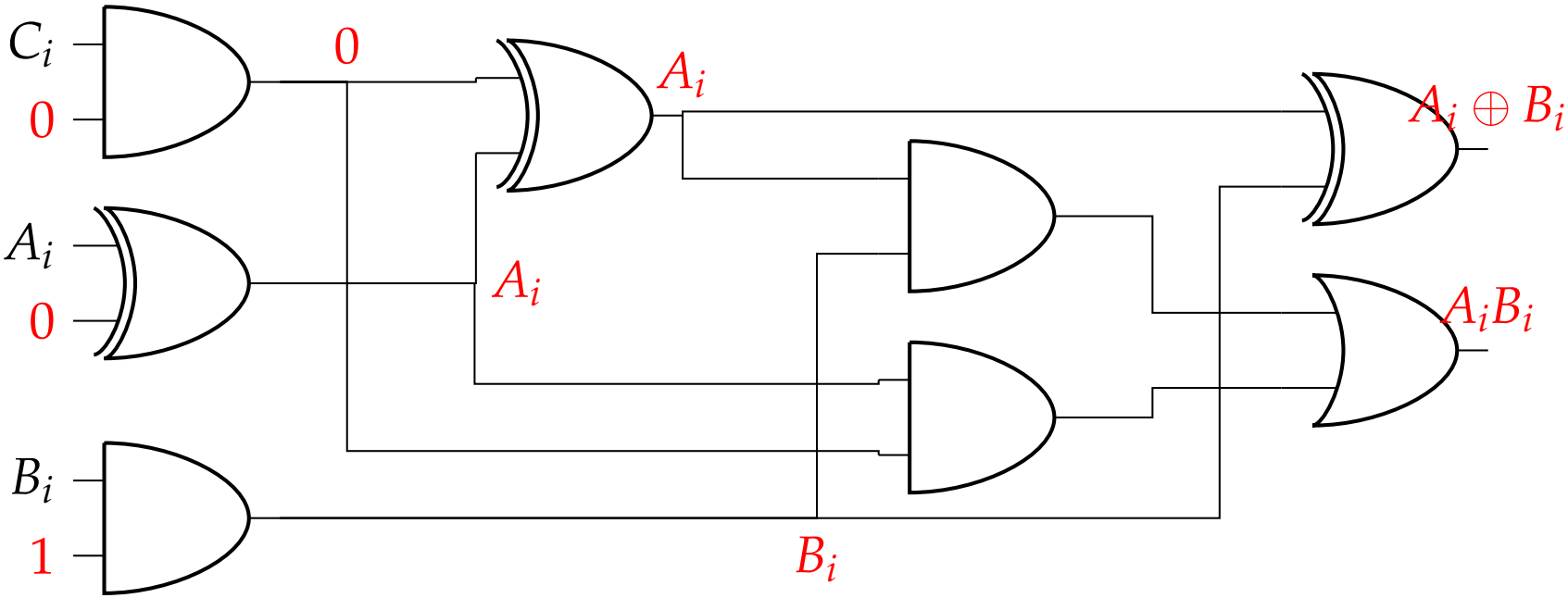
Aukeraketa.		Eragiketa logikoa $M = 0$			
S_1	S_0	F_i			
0	1				

$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i$, $\quad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



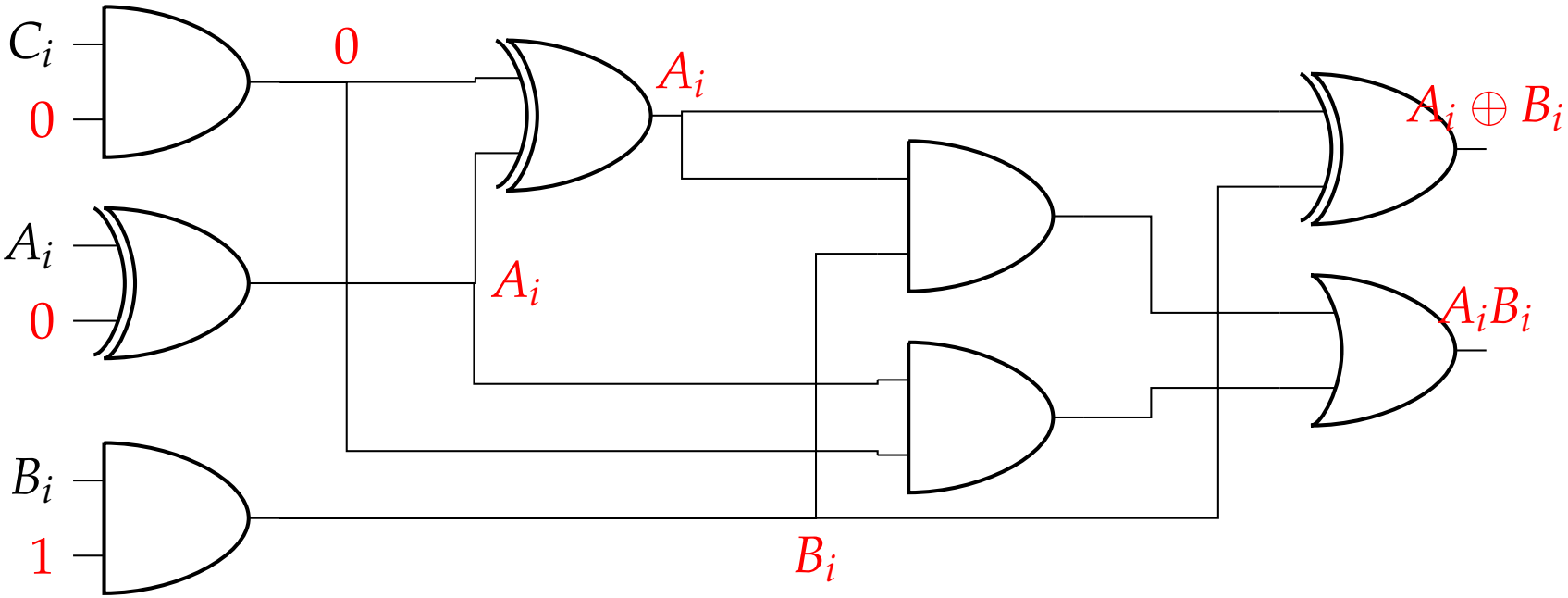
Aukeraketa.		Eragiketa logikoa $M = 0$			
S_1	S_0	F_i			
0	1	$\overline{A_i}$			

$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i$, $\quad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



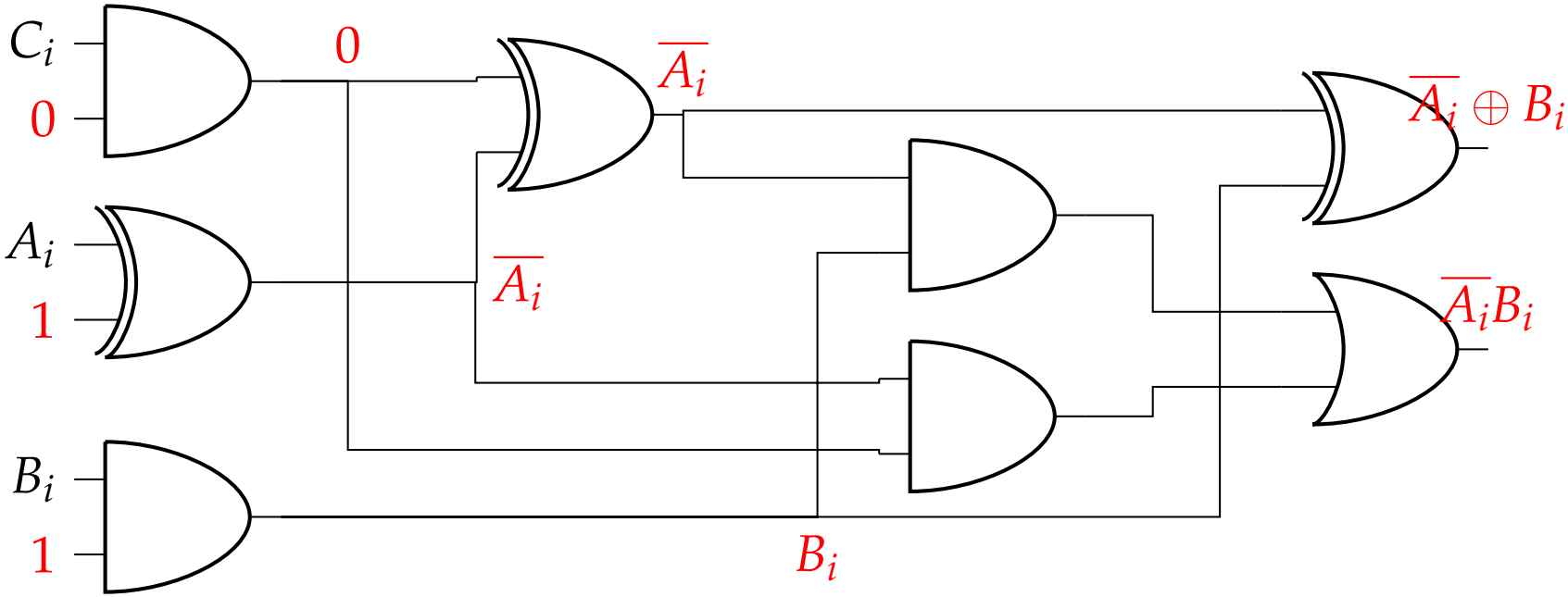
Aukeraketa.		Eragiketa logikoa $M = 0$			
S_1	S_0	F_i			
1	0				

$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i$, $\quad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



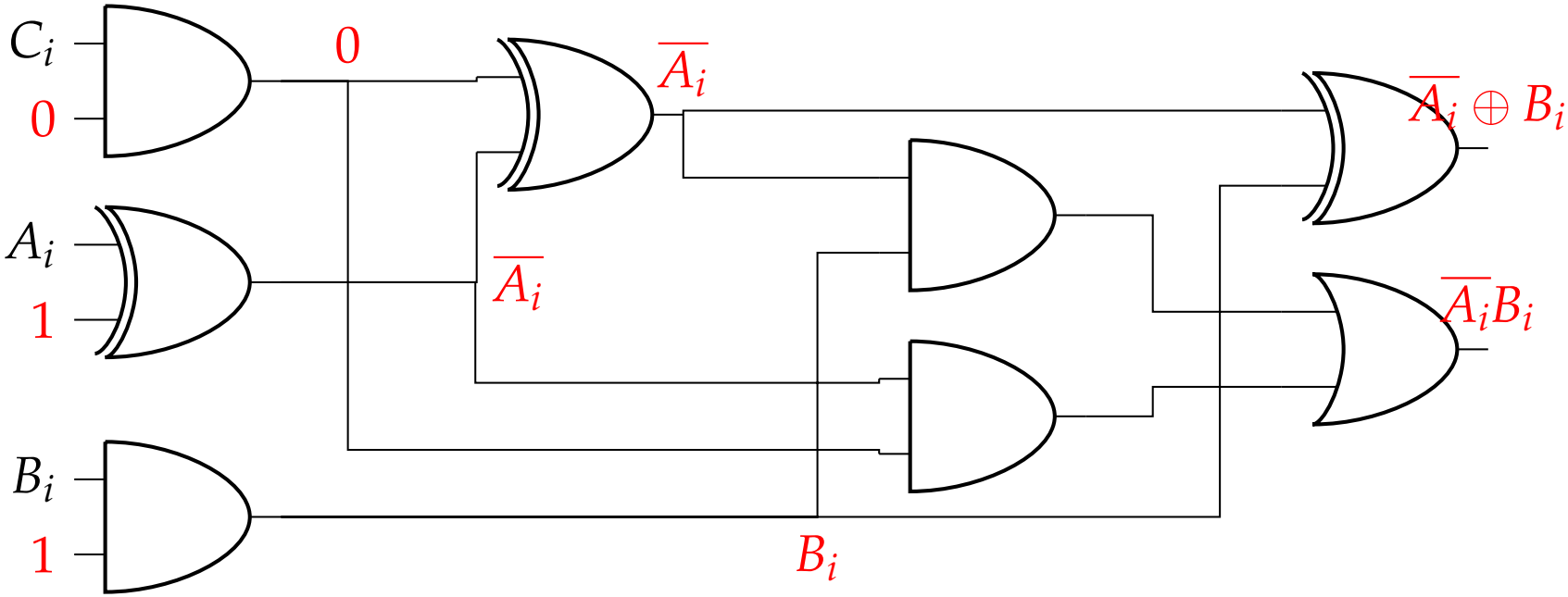
Aukeraketa.		Eragiketa logikoa $M = 0$
S_1	S_0	F_i
1	0	$A_i \oplus B_i$

$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i,$ $\quad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



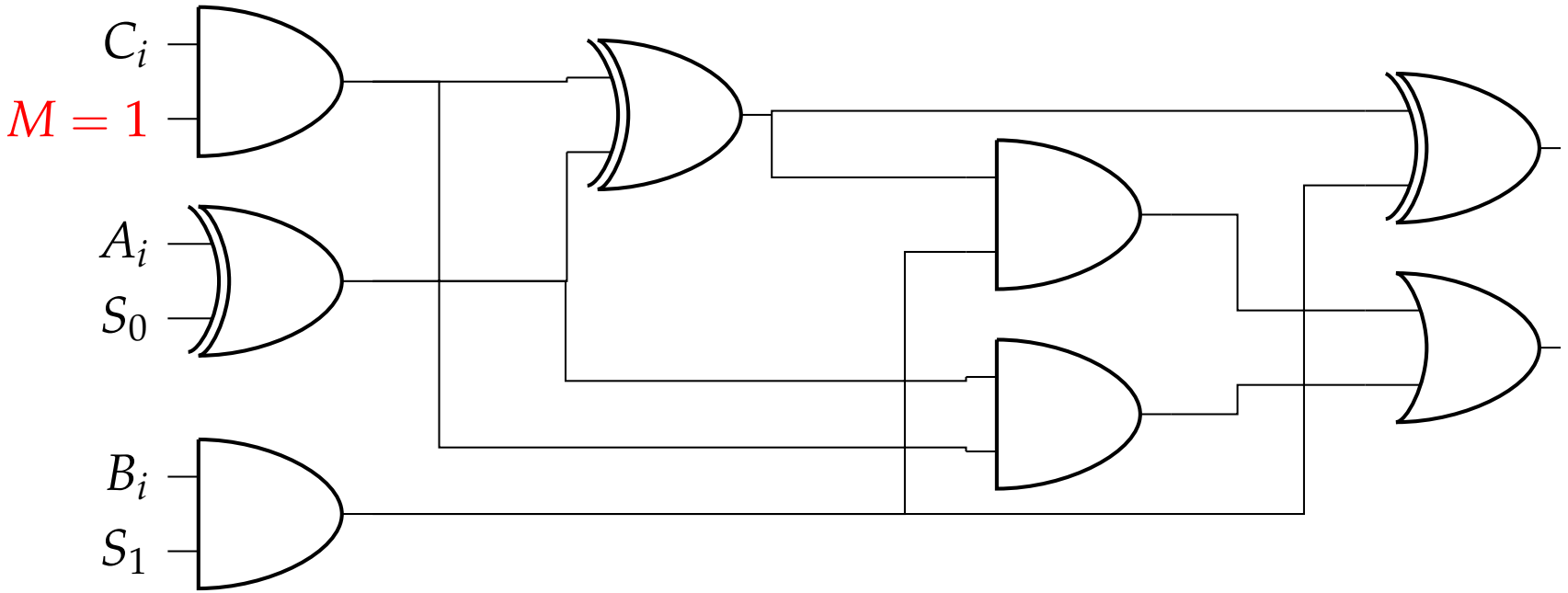
Aukeraketa.		Eragiketa logikoa $M = 0$			
S_1	S_0	F_i			
1	1				

$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i,$ $\quad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



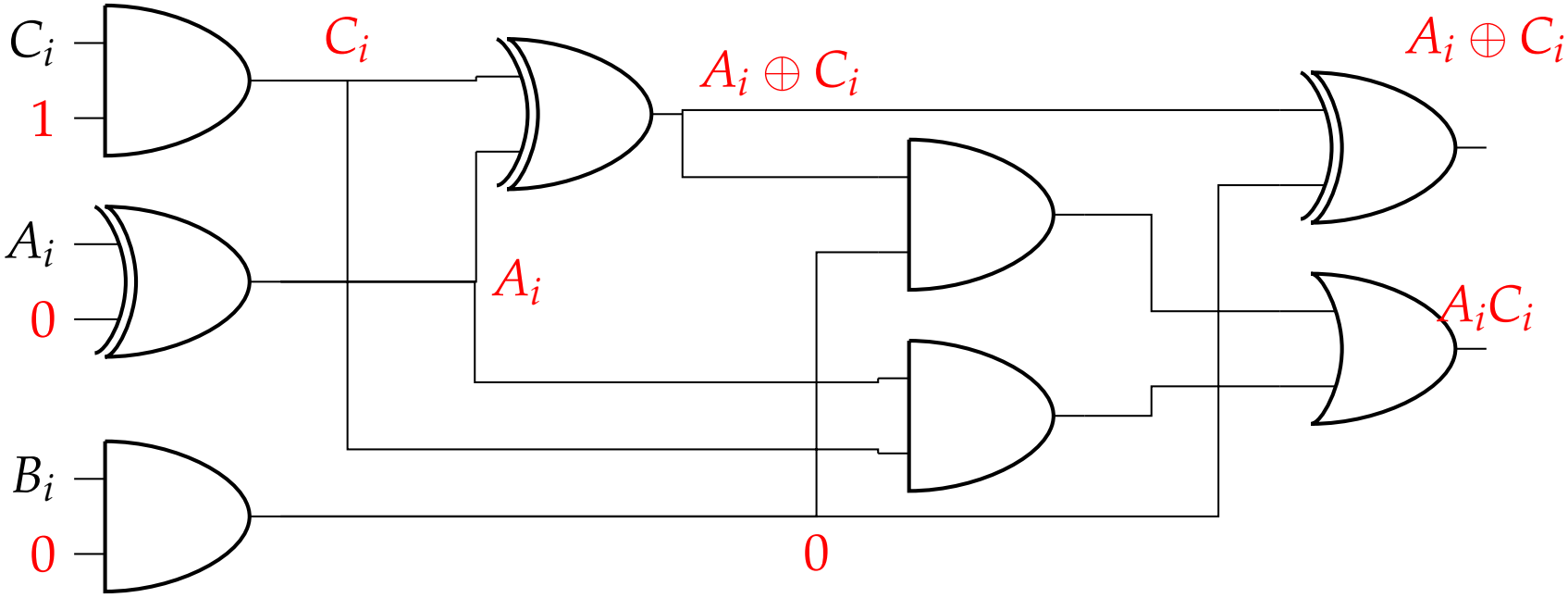
Aukeraketa.		Eragiketa logikoa $M = 0$			
S_1	S_0	F_i			
1	1	$\overline{A_i \oplus B_i}$			

$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i,$ $\quad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



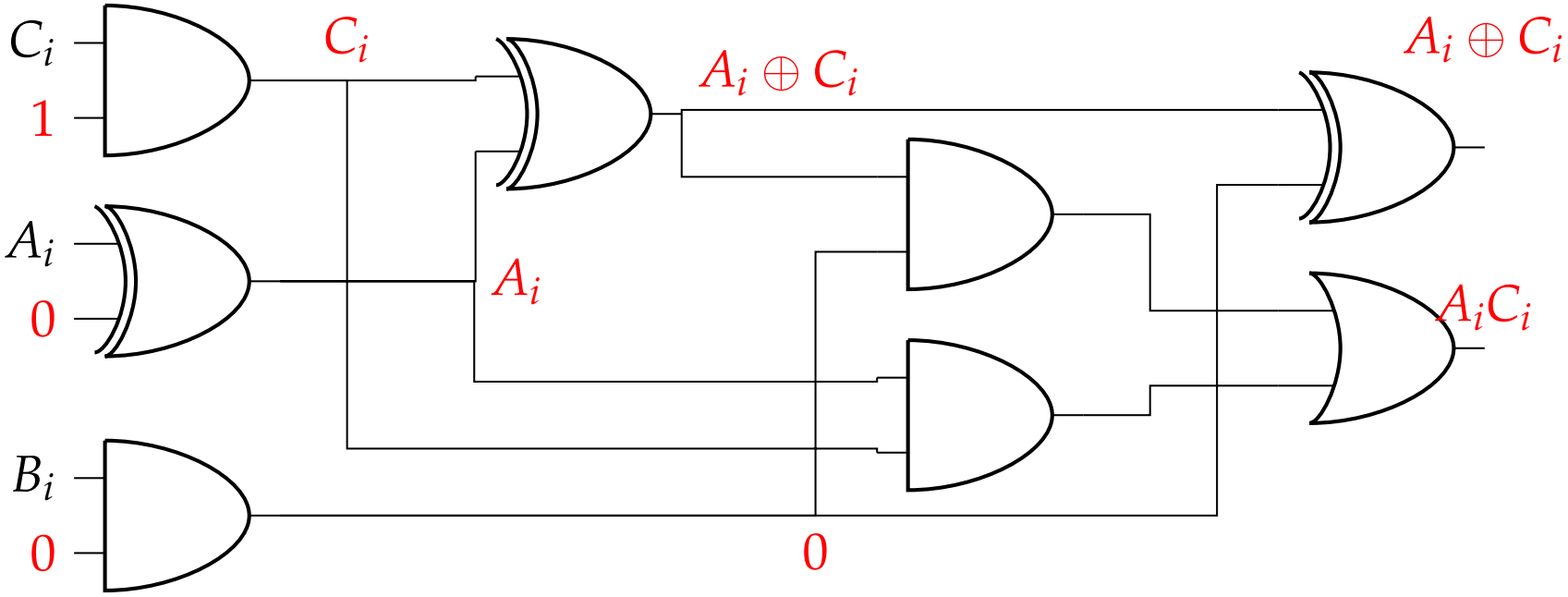
Aukeraketa.			Eragiketa aritmetikoa $M = 1$		
S_1	S_0		F_i	C_{i+1}	Eragiketa

$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i,$ $\quad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



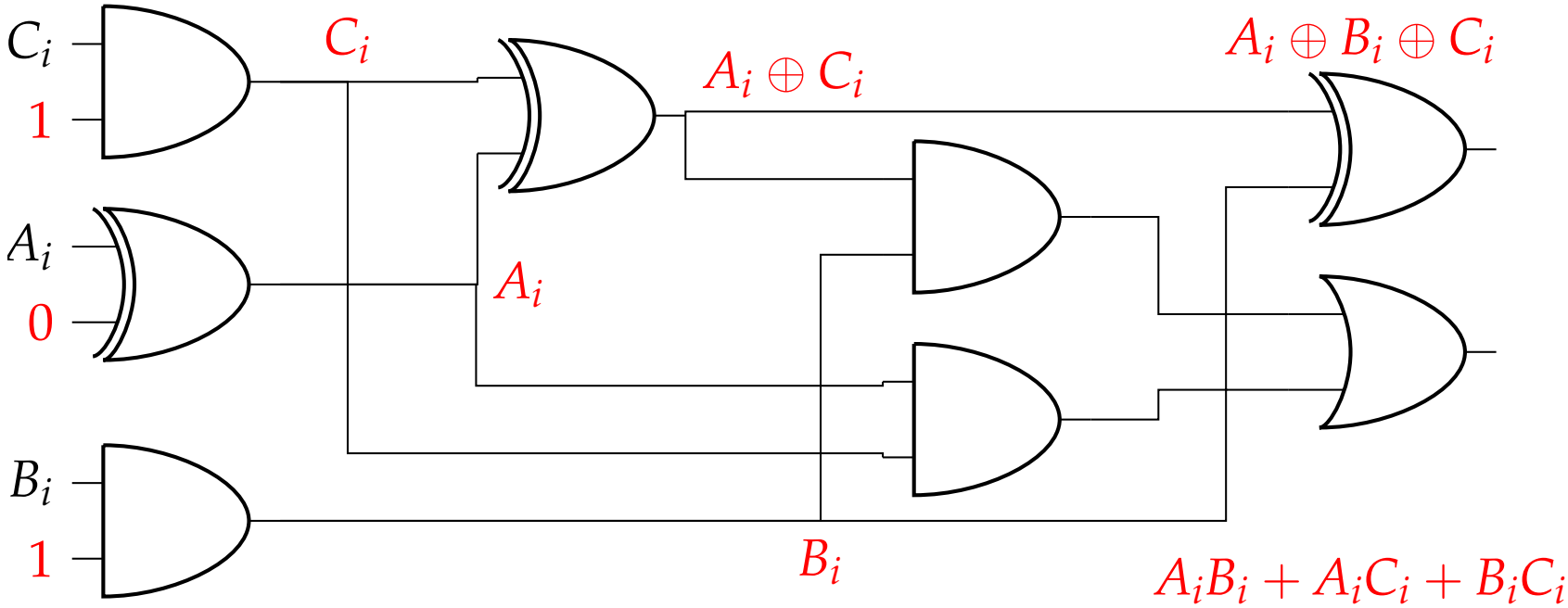
Aukeraketa.			Eragiketa aritmetikoa $M = 1$		
S_1	S_0		F_i	C_{i+1}	Eragiketa
0	0				

$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i,$ $\quad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



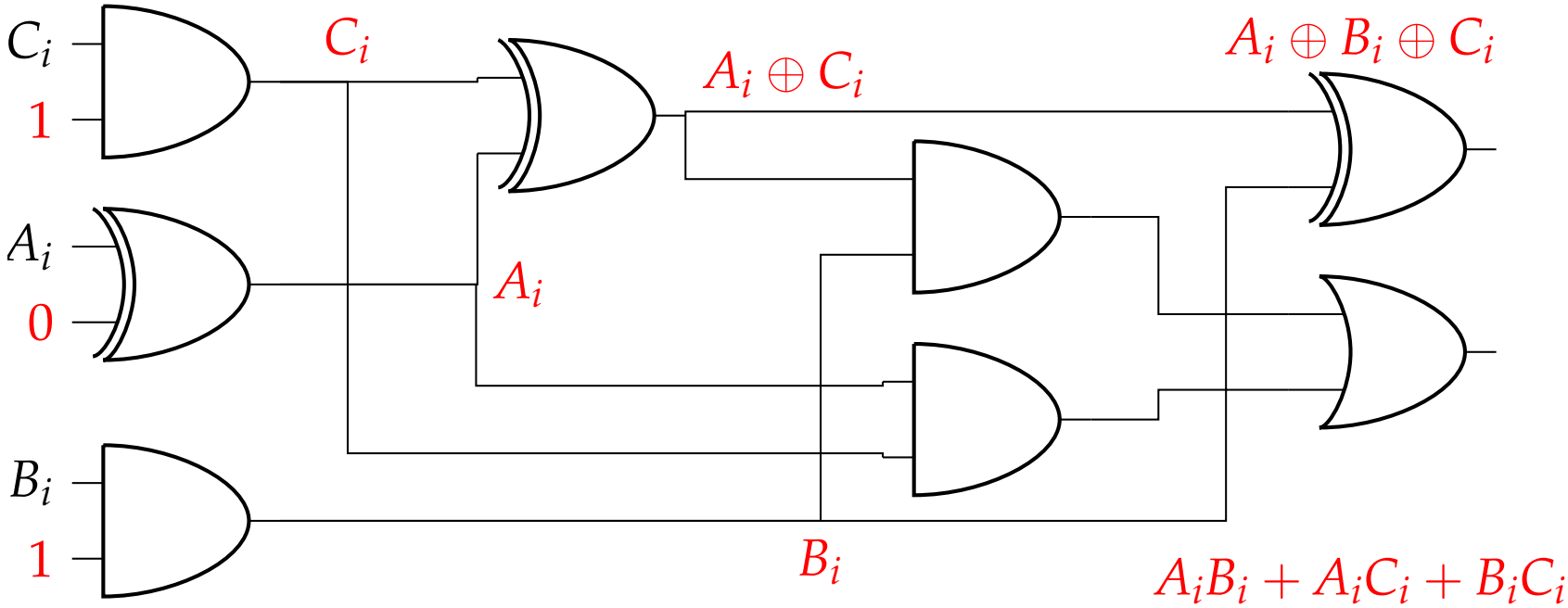
Aukeraketa.			Eragiketa aritmetikoa $M = 1$		
S_1	S_0		F_i	C_{i+1}	Eragiketa
0	0		$A_i \oplus C_i$	$C_{i+1} = A_i C_i$	$A_i + C_i$

$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i$, $\quad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



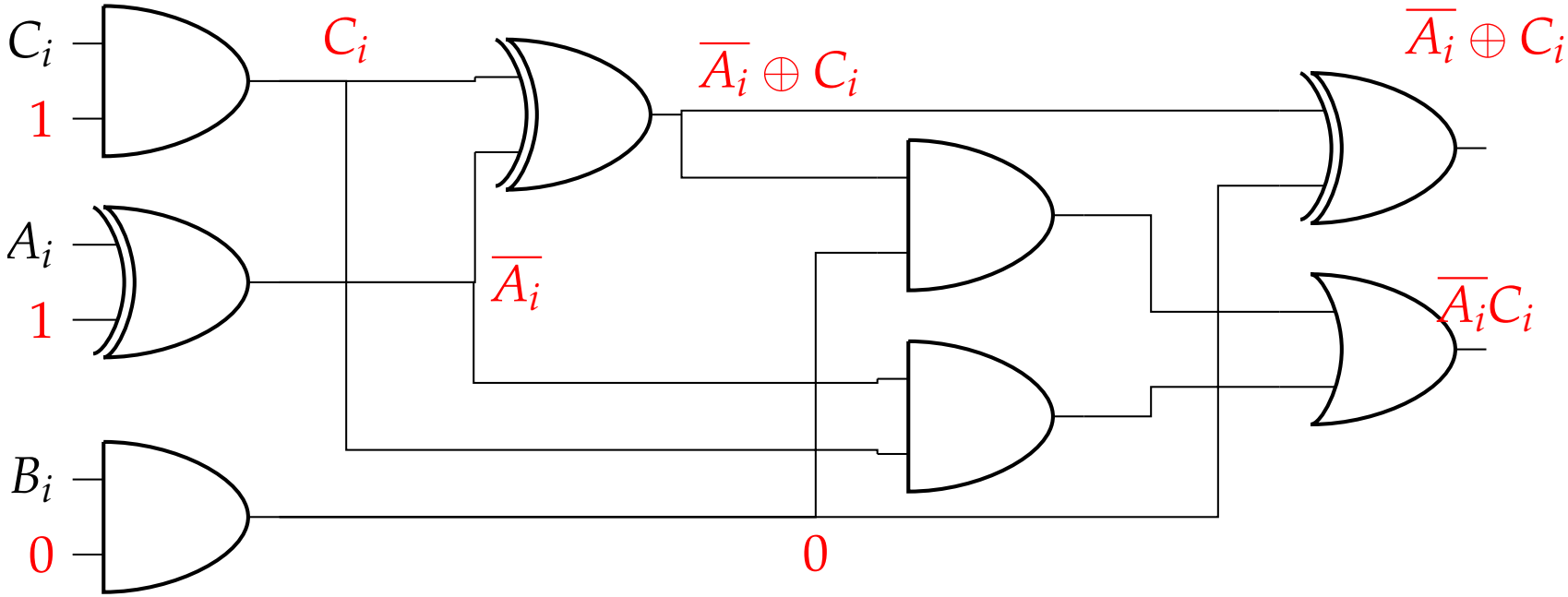
Aukeraketa.			Eragiketa aritmetikoa $M = 1$		
S_1	S_0		F_i	C_{i+1}	Eragiketa
0	1				

$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i$, $\quad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



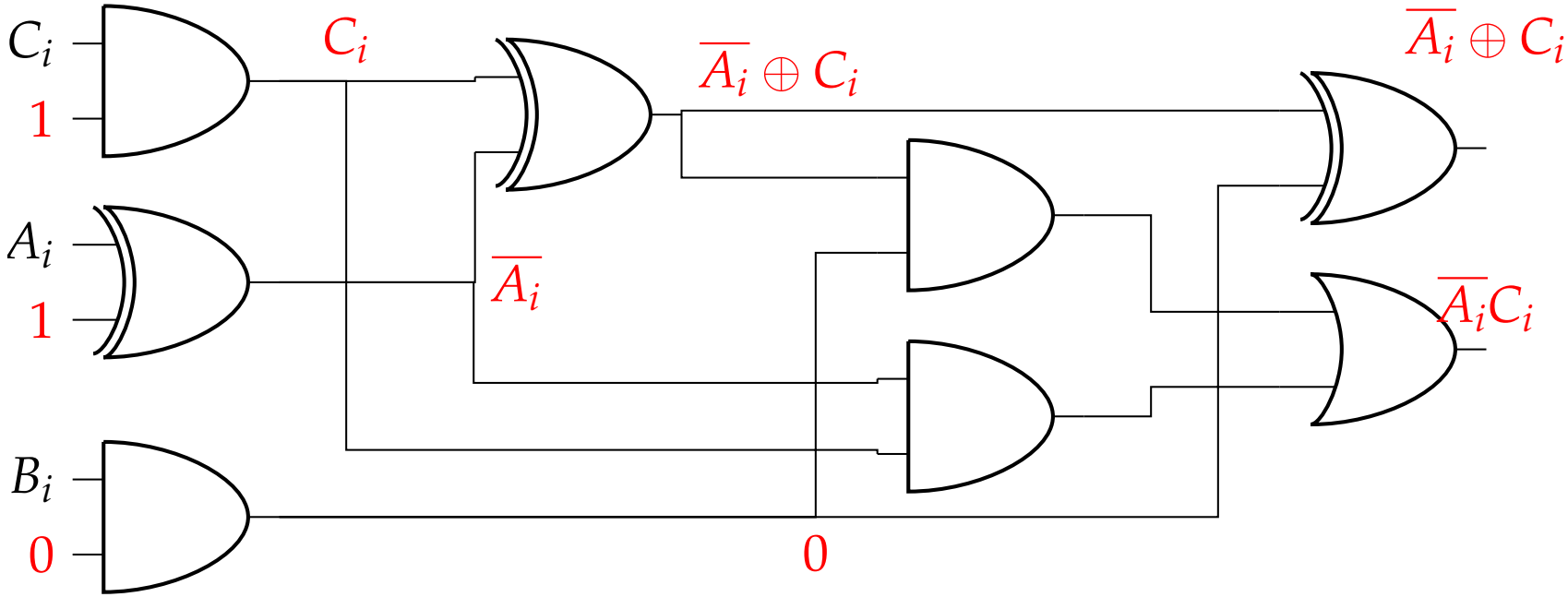
Aukeraketa.			Eragiketa aritmetikoa $M = 1$		
S_1	S_0		F_i	C_{i+1}	Eragiketa
0	1	$\overline{A_i}$	$\overline{A_i} \oplus C_i$	$C_{i+1} = \overline{A_i}C_i$	$\overline{A_i} + C_i$

$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i$, $\quad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



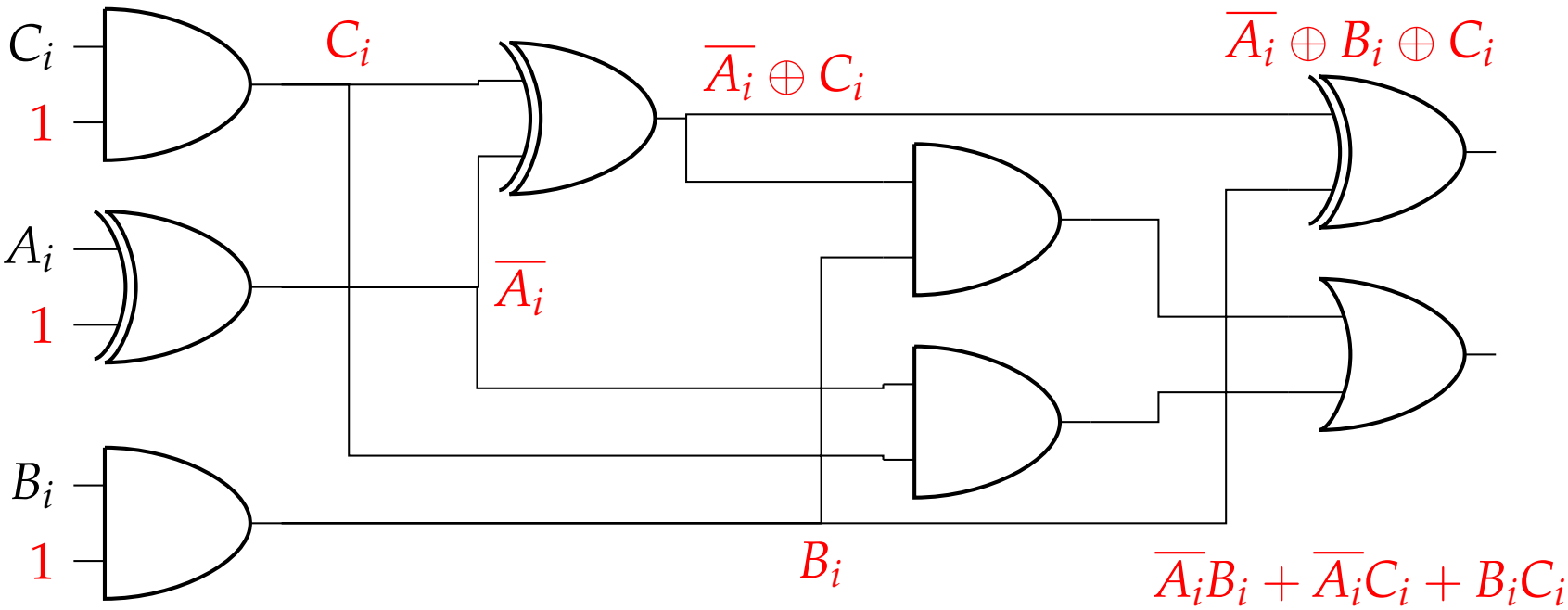
Aukeraketa.			Eragiketa aritmetikoa $M = 1$		
S_1	S_0		F_i	C_{i+1}	Eragiketa
1	0				

$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i$, $\quad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



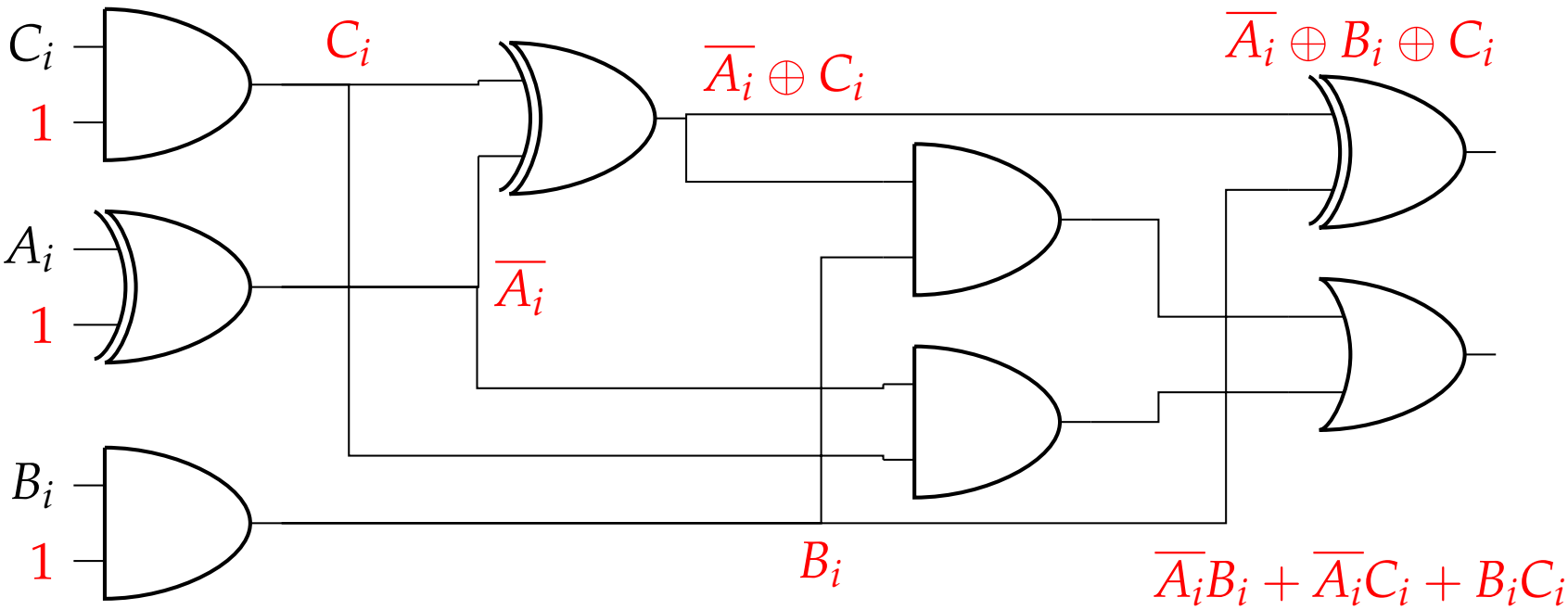
Aukeraketa.			Eragiketa aritmetikoa $M = 1$		
S_1	S_0		F_i	C_{i+1}	Eragiketa
1	0		$A_i \oplus B_i \oplus C_i$	$C_{i+1} = A_iB_i + A_iC_i + B_iC_i$	$A_i + B_i + C_i$

$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i, \qquad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



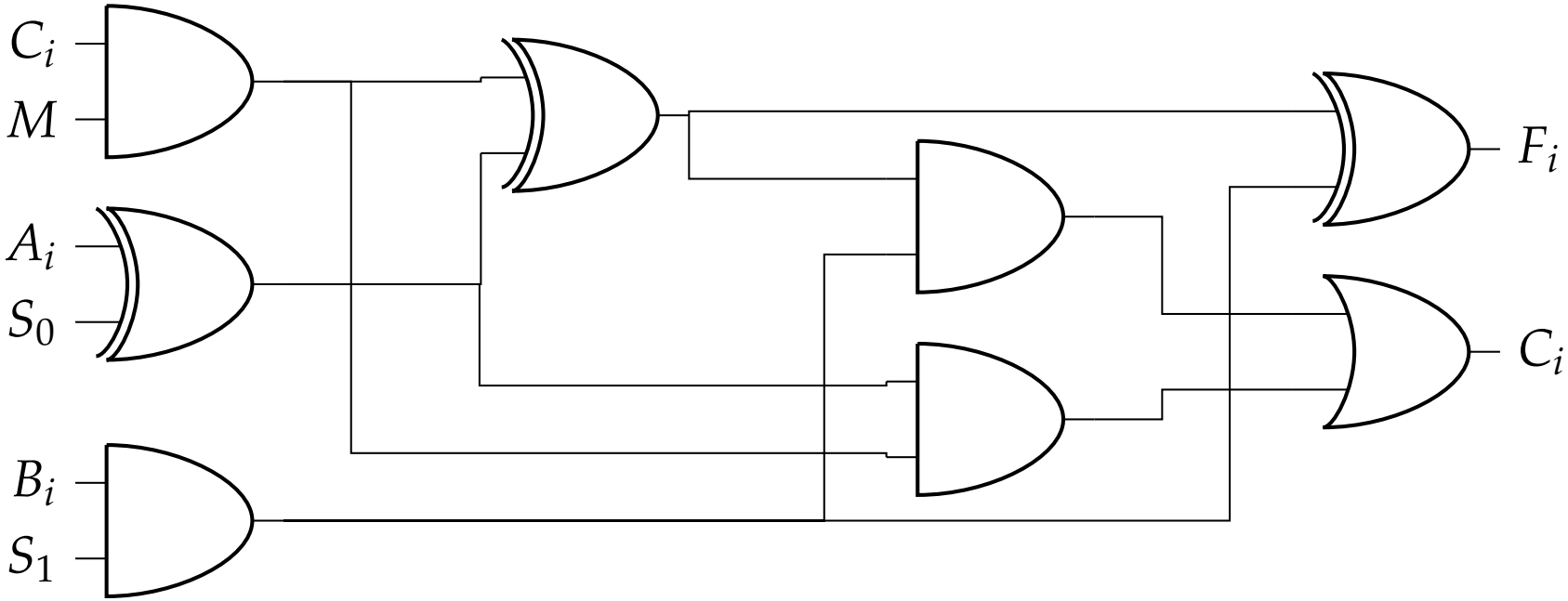
Aukeraketa.			Eragiketa aritmetikoa $M = 1$		
S_1	S_0		F_i	C_{i+1}	Eragiketa
1	1				

$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i, \qquad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



Aukeraketa.			Eragiketa aritmetikoa $M = 1$		
S_1	S_0		F_i	C_{i+1}	Eragiketa
1	1		$\overline{A_i} \oplus B_i \oplus C_i$	$C_{i+1} = \overline{A_i}B_i + \overline{A_i}C_i + B_iC_i$	$\overline{A_i} + B_i + C_i$

$F_i = ((S_0 \oplus A_i) \oplus MC_i) \oplus S_1 B_i$, $\quad C_{i+1} = MC_i(S_0 \oplus A_i) + S_1 B_i((S_0 \oplus A_i) \oplus MC_i)$



Aukeraketa.		$M = 0$	Eragiketa aritmetikoa $M = 1$		
S_1	S_0	F_i	F_i	C_{i+1}	Eragiketa
0	0	A_i	$A_i \oplus C_i$	$C_{i+1} = A_i C_i$	$A_i + C_i$
0	1	$\overline{A_i}$	$\overline{A_i} \oplus C_i$	$C_{i+1} = \overline{A_i} C_i$	$\overline{A_i} + C_i$
1	0	$A_i \oplus B_i$	$A_i \oplus B_i \oplus C_i$	$C_{i+1} = A_i B_i + A_i C_i + B_i C_i$	$A_i + B_i + C_i$
1	1	$\overline{A_i \oplus B_i}$	$\overline{A_i} \oplus B_i \oplus C_i$	$C_{i+1} = \overline{A_i} B_i + \overline{A_i} C_i + B_i C_i$	$\overline{A_i} + B_i + C_i$