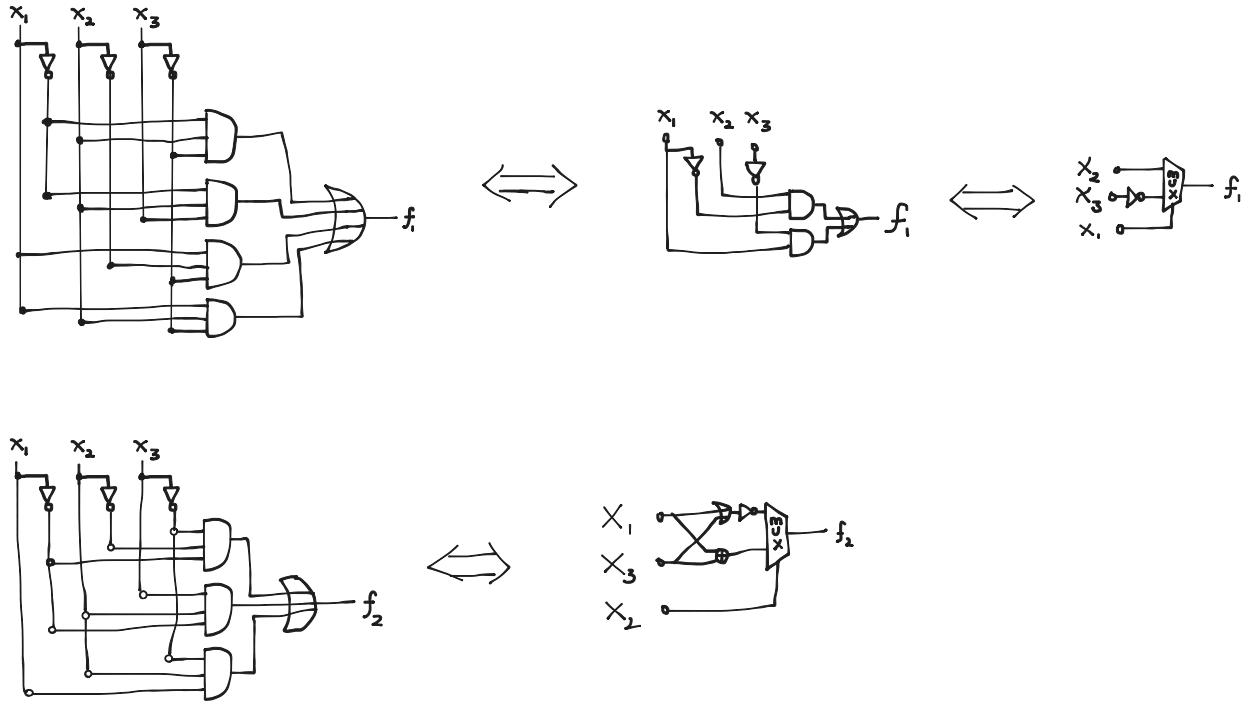


1.



2. Given

$$y[i] = \begin{cases} 1 & i = \langle x \rangle \bmod 2^n, x[n-1] = 0 \\ 0 & i \neq \langle x \rangle \bmod 2^n \end{cases} \quad 0 \leq i \leq 2^{n-1} - 1$$

$$y[i + 2^{n-1}] = \begin{cases} 1 & i = \langle x \rangle \bmod 2^{n-1}, x[n-1] = 1 \\ 0 & i \neq \langle x \rangle \bmod 2^{n-1} \end{cases} \quad 0 \leq i \leq 2^{n-1} - 1$$

we can say that

$$y[i] = \begin{cases} 1 & i = \langle x \rangle \bmod 2^{n-1} + x[n-1] \cdot 2^{n-1} \\ 0 & i \neq \langle x \rangle \bmod 2^{n-1} + x[n-1] \cdot 2^{n-1} \end{cases} \quad 0 \leq i \leq 2^n - 1$$

$$\Downarrow$$

$$y[i] = \begin{cases} 1 & i = \langle x \rangle \\ 0 & i \neq \langle x \rangle \end{cases} \quad 0 \leq i \leq 2^n - 1$$

$$\Downarrow$$

$$\langle y \rangle = 2^{\langle x \rangle} \iff y[\langle x \rangle] = 1$$

It is clear that this is a decoder.

3.

$$\begin{aligned}
\langle x_0 \rangle + \langle c_0 \rangle &= \langle c_1 s_0 \rangle \\
\langle x_1 \rangle + \langle c_1 \rangle &= \langle c_2 s_1 \rangle \\
\langle x_1 0 \rangle + \langle c_1 0 \rangle &= \langle c_2 s_1 0 \rangle \\
\langle x_1 0 \rangle + \langle c_1 0 \rangle + \langle s_0 \rangle &= \langle c_2 s_1 s_0 \rangle \\
\langle x_1 0 \rangle + \langle c_1 s_0 \rangle &= \langle c_2 s_1 s_0 \rangle \\
\langle x_1 0 \rangle + \langle x_0 \rangle + \langle c_0 \rangle &= \langle c_2 s_1 s_0 \rangle \\
\langle x_1 x_0 \rangle + \langle c_0 \rangle &= \langle c_2 s_1 s_0 \rangle \\
\langle x_1 x_0 \rangle + 1 &= \langle c_2 s_1 s_0 \rangle,
\end{aligned}$$

$$\begin{aligned}
\langle c_2 s_1 s_0 \rangle &= \langle x_1 x_0 \rangle + 1 \\
\langle c_2 \rangle \cdot 4 + \langle s_1 \rangle \cdot 2 + \langle s_0 \rangle &= \langle x_1 \rangle \cdot 2 + \langle x_0 \rangle + 1 \\
\langle s_1 \rangle \cdot 2 + \langle s_0 \rangle \bmod 4 &= \langle x_1 \rangle \cdot 2 + \langle x_0 \rangle + 1 \\
\langle s_1 s_0 \rangle \bmod 4 &= \langle x_1 x_0 \rangle + 1
\end{aligned}$$

4.

$$\langle h^0 . R \rangle = 0$$

$$\begin{aligned}
\langle h^{t+1} . R \rangle &= \langle h^t . R \rangle + 1 \bmod 4 \\
&= (t \bmod 4) + 1 \bmod 4 \\
&= t + 1 \bmod 4
\end{aligned}$$

$$\langle h^{t+1} . R \rangle = t + 1 \bmod 4 \iff h^{t+1} . R = \text{bin}_2(t + 1 \bmod 4)$$