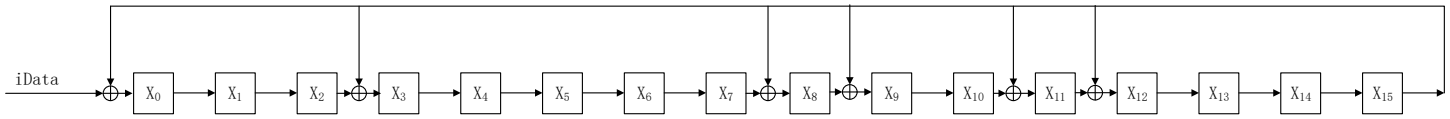
本文以 CRC16 为例进行 64bit 并行电路实现原理的推导过程。

CRC16(0x1B09)，生成多项式：

$$G(x) = x^{16} + x^{12} + x^{11} + x^9 + x^8 + x^3 + 1$$

生成多项式对应的串行实现电路如下：



根据串行电路可得到如下矩阵方程，该方程表示触发器X_0~X_{15}，在t时刻和$t+1$时刻的关系。

$$\begin{pmatrix} X_{15}(t+1) \\ X_{14}(t+1) \\ X_{13}(t+1) \\ X_{12}(t+1) \\ X_{11}(t+1) \\ X_{10}(t+1) \\ X_9(t+1) \\ X_8(t+1) \\ X_7(t+1) \\ X_6(t+1) \\ X_5(t+1) \\ X_4(t+1) \\ X_3(t+1) \\ X_2(t+1) \\ X_1(t+1) \\ X_0(t+1) \end{pmatrix} = \begin{bmatrix} 0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0 \\ 1&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0 \\ 1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{bmatrix} \cdot \left(\begin{pmatrix} X_{15}(t) \\ X_{14}(t) \\ X_{13}(t) \\ X_{12}(t) \\ X_{11}(t) \\ X_{10}(t) \\ X_9(t) \\ X_8(t) \\ X_7(t) \\ X_6(t) \\ X_5(t) \\ X_4(t) \\ X_3(t) \\ X_2(t) \\ X_1(t) \\ X_0(t) \end{pmatrix} + \begin{pmatrix} d(t) \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right)$$

令

$$X(t+1) = \begin{pmatrix} X_{15}(t+1) \\ X_{14}(t+1) \\ X_{13}(t+1) \\ X_{12}(t+1) \\ X_{11}(t+1) \\ X_{10}(t+1) \\ X_9(t+1) \\ X_8(t+1) \\ X_7(t+1) \\ X_6(t+1) \\ X_5(t+1) \\ X_4(t+1) \\ X_3(t+1) \\ X_2(t+1) \\ X_1(t+1) \\ X_0(t+1) \end{pmatrix} \qquad F = \begin{bmatrix} 0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0 \\ 1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1 \\ 1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \end{bmatrix}$$

则

$$X(t+1) = F \cdot X(t) + F \cdot \begin{pmatrix} d(t) \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

由此可推得

$$X(t+2) = F^2 \cdot X(t) + F^2 \cdot \begin{pmatrix} d(t) \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + F \cdot \begin{pmatrix} d(t+1) \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

又由于F矩阵得特殊性，可得

$$F \cdot \begin{pmatrix} d(t+1) \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = F^2 \cdot \begin{pmatrix} 0 \\ d(t+1) \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

则

$$(t+2) = F^2 \cdot X(t) + F^2 \cdot \begin{pmatrix} d(t) \\ d(t+1) \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

继续递推

$$X(t+16) = F^{16} \cdot X(t) + F^{16} \cdot \begin{pmatrix} d(t) \\ d(t+1) \\ d(t+2) \\ d(t+3) \\ d(t+4) \\ d(t+5) \\ d(t+6) \\ d(t+7) \\ d(t+8) \\ d(t+9) \\ d(t+10) \\ d(t+11) \\ d(t+12) \\ d(t+13) \\ d(t+14) \\ d(t+15) \end{pmatrix}$$

继续

$$X(t+17) = F^{17} \cdot X(t) + F^{17} \cdot \begin{pmatrix} d(t) \\ d(t+1) \\ d(t+2) \\ d(t+3) \\ d(t+4) \\ d(t+5) \\ d(t+6) \\ d(t+7) \\ d(t+8) \\ d(t+9) \\ d(t+10) \\ d(t+11) \\ d(t+12) \\ d(t+13) \\ d(t+14) \\ d(t+15) \end{pmatrix} + F \cdot \begin{pmatrix} d(t+16) \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

最后得出

$$X(t+64) = F^{64} \cdot X(t) + F^{64} \cdot \begin{pmatrix} d(t) \\ d(t+1) \\ d(t+2) \\ d(t+3) \\ d(t+4) \\ d(t+5) \\ d(t+6) \\ d(t+7) \\ d(t+8) \\ d(t+9) \\ d(t+10) \\ d(t+11) \\ d(t+12) \\ d(t+13) \\ d(t+14) \\ d(t+15) \end{pmatrix} + F^{48} \cdot \begin{pmatrix} d(t+16) \\ d(t+17) \\ d(t+18) \\ d(t+19) \\ d(t+20) \\ d(t+21) \\ d(t+22) \\ d(t+23) \\ d(t+24) \\ d(t+25) \\ d(t+26) \\ d(t+27) \\ d(t+28) \\ d(t+29) \\ d(t+30) \\ d(t+31) \end{pmatrix} + F^{32} \cdot \begin{pmatrix} d(t+32) \\ d(t+33) \\ d(t+34) \\ d(t+35) \\ d(t+36) \\ d(t+37) \\ d(t+38) \\ d(t+39) \\ d(t+40) \\ d(t+41) \\ d(t+42) \\ d(t+43) \\ d(t+44) \\ d(t+45) \\ d(t+46) \\ d(t+47) \end{pmatrix} + F^{16} \cdot \begin{pmatrix} d(t+48) \\ d(t+49) \\ d(t+50) \\ d(t+51) \\ d(t+52) \\ d(t+53) \\ d(t+54) \\ d(t+55) \\ d(t+56) \\ d(t+57) \\ d(t+58) \\ d(t+59) \\ d(t+60) \\ d(t+61) \\ d(t+62) \\ d(t+63) \end{pmatrix}$$

推导结束

注：利用该方法可推导任一位宽得 CRC 计算，但硬件实现时需要注意增加并行度的同时会带来逻辑级数的增加，即会增加路径延迟。