

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 1/00 (2006.01)
H03M 13/09 (2006.01)



[12] 发明专利申请公布说明书

[21] 申请号 200810173089.6

[43] 公开日 2009年4月8日

[11] 公开号 CN 101404557A

[22] 申请日 2008.11.28

[21] 申请号 200810173089.6

[71] 申请人 炬力集成电路设计有限公司

地址 519085 广东省珠海市唐家湾镇哈工大
路1号15栋1单元1号

[72] 发明人 叶院红

[74] 专利代理机构 北京同达信恒知识产权代理有限公司
代理人 李娟

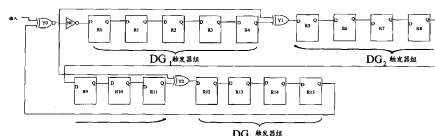
权利要求书2页 说明书9页 附图3页

[54] 发明名称

一种循环冗余校验码生成装置及方法

[57] 摘要

本发明涉及传输数据校验领域，尤其涉及采用硬件电路实现低成本的CRC校验码生成技术。一种循环冗余校验码生成装置及方法，其特征多项式为 $g(x) = \sum_{j=1}^k x^{n_j} + 1$ ，包括分别对应于 $x^{n_1} \sim x^{n_k}$ 的触发器组，触发器组由若干个触发器串接而成；触发器组依触发器组的序号顺序串接；异或门，串接于相邻两个触发器组之间；反相器，其输出端与 DG_1 触发器组的输入端相连；异或非门，另一个输入端与 DG_k 触发器组的输出端相连，其一个输入端为所述装置的输入端，其输出端与反相器的输入端、以及各异或门的输入端相连。由于将现有技术电路中的每个触发器连接的反相器去掉，并在数据输入到串接的触发器之前连接反相器进行取反，从而节省了大量的反相器，简化了CRC校验码生成电路、降低了硬件成本。



1、一种循环冗余校验码生成装置，所述循环冗余校验码的特征多项式为

$$g(x) = \sum_{j=1}^k x^{n_j} + 1, \text{ 其中 } n_1 \sim n_k \text{ 为递增顺序的自然数、} k \text{ 为自然数, 其特征在于,}$$

所述装置包括:

k 个触发器组 $DG_1 \sim DG_k$, 分别对应于 $x^{n_1} \sim x^{n_k}$, 各触发器组由若干个触发器串接而成; 其中, 对应于 x^{n_j} 的触发器组 DG_j 中的触发器个数为 $n_j - n_{j-1}$; 若 $j=1$, 则 $n_{j-1} = 0$; 触发器组依触发器组的序号顺序串接;

至少一个异或门, 分别串接于相邻的两个触发器组之间;

一个反相器, 其输出端与触发器组 DG_1 的输入端相连;

异或非门, 其一个输入端为所述装置的输入端, 另一个输入端与触发器组 DG_k 的输出端相连, 其输出端与所述反相器的输入端、以及各异或门的输入端相连。

2、如权利要求 1 所述的装置, 其特征在于, 所述触发器组中的每个触发器的复位值为 0。

3、如权利要求 1 或 2 所述的装置, 其特征在于, 所述 k 等于 3, $n_1 \sim n_3$ 分别等于 5、12、16; 以及

触发器组 DG_1 具体由 5 个触发器串接而成;

触发器组 DG_2 具体由 7 个触发器串接而成;

触发器组 DG_3 具体由 4 个触发器串接而成;

所述异或门的个数具体为 2。

4、如权利要求 1 或 2 所述的装置, 其特征在于, 所述 k 等于 14, $n_1 \sim n_{14}$ 分别等于 1、2、4、5、7、8、10、11、12、16、22、23、26、32; 以及

触发器组 $DG_1 \sim DG_{14}$ 中具体包括的触发器的个数分别为: 1、1、2、1、2、1、2、1、1、4、6、1、3、6;

所述异或门的个数具体为 13 个。

5、一种通过如权利要求 1-4 任一所述的装置生成循环冗余校验码的方法，用于对输入的信息码进行校验，其特征在于，包括：

将所述信息码从所述装置的输入端输入；

在所有的信息码从所述输入端输入后，各触发器的输出组成所述信息码的循环冗余校验码。

一种循环冗余校验码生成装置及方法

技术领域

本发明涉及传输数据校验领域，尤其涉及采用硬件电路实现低成本的CRC校验码生成技术。

背景技术

CRC (Cyclic Redundancy Code, 循环冗余校验码) 是数据通信中最常用的一种差错校验码，它能够发现传输数据中的单双位错误、奇数个错误，以及长度小于CRC级数的连续错误。

循环冗余校验方法的原理如下：

任意一个由二进制位串组成的代码都可以和一个系数仅为‘0’和‘1’取值的多项式一一对应，例如：代码110111对应的多项式为 $X^5 + X^4 + X^2 + X + 1$ 。

设发送方要发送的数据对应的多项式为 $V(x)$ ；

发送方和接收方约定一个特征多项式 $g(x)$ ，设该特征多项式的最高次幂为R；

在要发送的数据的末尾添加R个0，则其相应的多项式为 $M(x) = x^R V(x)$ ；

用 $M(x)$ 除以 $g(x)$ ，得到商 $Q(x)$ 和余式 $R(x)$ ，则 $M(x) = Q(x)g(x) + R(x)$ ；余式 $R(x)$ 所对应的码值按位取反即为CRC校验码值。

令 $T(x) = M(x) + R(x)$ ，发送方发送 $T(x)$ 所对应的数据；

设接收方接收到的数据对应的多项式为 $T'(x)$ ，将 $T'(x)$ 除以 $g(x)$ ，若余式为0（或者是设定的常数），则接收方认为正确接收到发送方发送的数据；否则，认为接收错误。从而达到对接收的信息流进行校验的目的。

目前可以采用两种方法来计算要发送数据的CRC校验码值：

1、采用软件方法计算接收的信息码的CRC校验码，即通过软件方法根

据特征多项式 $g(x)$ 计算将要传输的信息码的 CRC 校验码。但是，软件方法计算速度慢，且需要占用 CPU（Center Process Unit，中央处理单元）资源。

2、在现有技术中还可以将信息流通过硬件电路得到 CRC 校验码：

由于 CRC 校验码是由信息码对应的多项式 $V(x)$ 乘以 x^R ，再除以特征多项式为 $g(x)$ 后，得到的余式 $R(x)$ 所对应的码值，因此生成 CRC 校验码的硬件电路可以由多项式乘法电路和多项式除法电路综合而成：

乘以 x^R 的电路，相当于将输入序列延迟 R 位后输出，因此乘以 x^R 的电路由 R 个 DQ 触发器（或者寄存器）组成。图 1 所示为乘以 x^3 的电路。其中， R_0 - R_2 为 DQ 触发器（或者寄存器）。

除法的过程就是不断移位并与（商 \times 除数）做减法的过程，对应到电路即为一个负反馈电路。图 2 所示为除式 $x^3 + x^2 + 1$ 的除法电路。其中， Y_1 - Y_2 为异或门（逻辑异或运算电路）。

结合上述的乘除法电路，即可得到如图 3 所示的电路。

例如，对于特征多项式为 $g(x) = x^{16} + x^{12} + x^5 + 1$ 、生成 16 位 CRC 校验码的硬件电路如图 4 所示。其中， N_0 - N_{15} 为反相器（逻辑取反电路），所有信息流都从输入端输入后，寄存器 R_{15} ~ R_0 的输出值即为余式，按位取反后，就得到 16 位的 CRC 校验码。根据不同的 CRC 校验码类型的定义，在某些情况下，将触发器输出的余数作为 CRC 校验码；在某些情况下（如 CRC-CCITT16/32 类型的校验码），将触发器输出的余数取反作为 CRC 校验码。

若 CRC 校验码的特征多项式为 $g(x) = \sum_{j=1}^k x^{n_j} + 1$ ，其中 k 、 $n_1 \sim n_k$ 为自然数，

则现有技术的余式取反的 CRC 校验码生成电路包括： k 个触发器组、异或门、反相器。

k 个触发器组，分别对应于 $x^{n_1} \sim x^{n_k}$ ，各触发器组由若干个触发器串接而成；其中，对应于 x^{n_j} 的 DG_j 触发器组中的触发器个数为 $n_j - n_{j-1}$ ；若 $j=1$ ，则 $n_{j-1} = 0$ ；每个触发器的复位值为 1。

多个异或门，各异或门串接于各触发器组之间，并触发器组依触发器组的序号顺序串接。

此外还有一个异或门，该异或门的输入端为 CRC 校验码生成电路的输入端，其输出端与 DG_1 触发器组的输入端、以及其它异或门的一个输入端相连。

反相器的个数与触发器的个数相同，并且各反相器的输入端分别与各触发器的输出端相连。

信息码从 CRC 校验码生成电路的输入端依次输入，在所有的信息码从所述输入端输入后，各反相器的输出即为余式取反的 CRC 校验码。

本发明的发明人发现，采用软件计算信息码流的 CRC 校验码值速度慢、占用较多的 CPU 资源，而采用现有技术的生成 CRC 校验码的硬件电路采用的逻辑门较多、硬件成本较高、占用电路空间较大。

发明内容

本发明实施例提供了一种循环冗余校验码生成装置及方法，用以降低生成 CRC 校验码的电路的成本。

一种循环冗余校验码生成装置，所述循环冗余校验码的特征多项式为

$$g(x) = \sum_{j=1}^k x^{n_j} + 1, \text{ 其中 } n_1 \sim n_k \text{ 为递增顺序的自然数、} k \text{ 为自然数, 所述装置包括:}$$

k 个触发器组 $DG_1 \sim DG_k$ ，分别对应于 $x^{n_1} \sim x^{n_k}$ ，各触发器组由若干个触发器串接而成；其中，对应于 x^{n_j} 的触发器组 DG_j 中的触发器个数为 $n_j - n_{j-1}$ ；若 $j=1$ ，则 $n_{j-1} = 0$ ；触发器组依触发器组的序号顺序串接；

至少一个异或门，分别串接于相邻的两个触发器组之间；

一个反相器，其输出端与触发器组 DG_1 的输入端相连；

异或非门，其一个输入端为所述装置的输入端，另一个输入端与触发器组 DG_k 的输出端相连，其输出端与所述反相器的输入端、以及各异或门的输入端相连。

所述触发器组中的每个触发器的复位值为0。

较佳的，所述装置中所述k等于3， $n_1 \sim n_3$ 分别等于5、12、16。

较佳的，所述装置中所述k等于14， $n_1 \sim n_{14}$ 分别等于1、2、4、5、7、8、10、11、12、16、22、23、26、32。

根据上述装置生成循环冗余校验码的方法，用于对输入的信息码进行校验，包括：

将所述信息码从所述装置的输入端输入；

在所有的信息码从所述输入端输入后，各触发器的输出组成所述信息码的循环冗余校验码。

本发明实施例的CRC校验码生成电路由于将现有技术电路中的每个触发器连接的反相器去掉，并在数据输入到串接的触发器之前连接反相器进行取反，从而节省了大量的反相器，简化了CRC校验码生成电路、降低了硬件成本。

附图说明

图1为现有技术的乘法电路示意图；

图2为现有技术的多项式除法电路示意图；

图3为现有技术的乘除法电路示意图；

图4为现有技术的16位CRC校验码生成电路示意图；

图5为本发明实施例的16位CRC校验码生成电路示意图；

图6为本发明实施例的32位CRC校验码生成电路示意图。

具体实施方式

本发明实施例的CRC校验码生成电路将现有技术电路中的每个触发器连接的反相器去掉，并在数据输入到串接的触发器之前连接一个反相器进行取反，从而节省了大量的反相器，简化了电路、降低了硬件成本。

CRC 校验码的特征多项式可以表示为 $g(x) = \sum_{j=1}^k x^{n_j} + 1$, 其中 $n_1 \sim n_k$ 为递增顺序的自然数、 k 为自然数。

例如, 取值 $k=3$ 、 $n_1=5$ 、 $n_2=12$ 、 $n_3=16$ 时, 则 CRC 校验码的特征多项式为 $g(x) = x^{16} + x^{12} + x^5 + 1$ (此为 CRC-CCITT16 类型的校验码的特征多项式)。

本发明实施例的 CRC 校验码生成电路根据 CRC 校验码的特征多项式 $g(x) = \sum_{j=1}^k x^{n_j} + 1$ 生成, 具体包括: k 个触发器组、异或门、反相器、异或非门。

其中, k 个触发器组为 $DG_1 \sim DG_k$ 触发器组, 分别对应于特征多项式中的单项式 $x^{n_1} \sim x^{n_k}$, 各触发器组由若干个触发器串接而成; 其中, 对应于 x^{n_j} 的 DG_j 触发器组中的触发器个数为 $n_j - n_{j-1}$; 若 $j=1$, 则 $n_{j-1} = 0$; k 个触发器组共包括 16 个触发器 (R0~R15)。

触发器组依触发器组的序号顺序串接; 也就是说, 触发器组串接的顺序与触发器组的序号相同。比如 DG_1 触发器组后面是 DG_2 触发器组, DG_2 触发器组后面是 DG_3 触发器组……

对于生成 CRC-CCITT16/32 类型的校验码现有技术的触发器的复位值为 1, 则对应的本发明实施例中的 CRC 校验码生成电路的触发器组中的每个触发器的复位值为 0; 但是对于其它有些类型的 CRC 校验码, 若现有技术电路的触发器的复位值为 0, 则本发明实施例中的电路的触发器的复位值则相应变为 1, 也就是说, 本发明实施例的电路的触发器的复位值与现有技术的相反。

异或门, 串接于相邻的两个触发器组之间。比如, 在 DG_1 触发器组与 DG_2 触发器组之间串接有异或门 Y1, 在 DG_2 触发器组与 DG_3 触发器组之间串接有异或门 Y2……依次类推, 直到将所有的相邻的触发器组之间串接了异或门。

反相器, 其输出端与 DG_1 触发器组的输入端相连。

异或非门, 其一个输入端为所述 CRC 校验码生成电路的输入端, 另一个输入端与 DG_k 触发器组的输出端相连, 其输出端与所述反相器的输入端, 以及

各异或门的一个输入端相连。

在生成信息码的 CRC 校验码的过程中，将信息码从 CRC 校验码生成电路的输入端，即异或非门的一个输入端依次输入，则在所有的信息码从所述输入端输入后，触发器组的各触发器的输出即为信息码的余式取反后的 CRC 校验码。

当 CRC 校验码的特征多项式 $g(x) = \sum_{j=1}^k x^{n_j} + 1$ 中的 $k=3$ 、 $n_1=5$ 、 $n_2=12$ 、 $n_3=16$ 时，特征多项式为 $g(x) = x^{16} + x^{12} + x^5 + 1$ ，本发明实施例提供的对应的一个具体 CRC 校验码生成电路如图 5 所示，包括：3 个触发器组（ $DG_1 \sim DG_3$ ）、异或门（Y1 和 Y2）、反相器（N0）、异或非门（Y0）。

由于多项式的 $k=3$ ，因此 CRC 校验码生成电路包括 3 个触发器组，其中 DG_1 对应于单项式 x^5 ， DG_2 对应于单项式 x^{12} ， DG_3 对应于单项式 x^{16} 。触发器组中的每个触发器的复位值根据实际情况对 CRC 校验码的定义可以全部为 0，也可以全部为 1。例如，对于本发明实施例生成 CRC-CCITT16/32 类型的校验码的电路中的触发器的复位值全部为 0。

DG_1 触发器组中的触发器个数为： $n_1 - n_0 = 5 - 0 = 5$ ； DG_2 触发器组中的触发器个数为： $n_2 - n_1 = 12 - 5 = 7$ ； DG_3 触发器组中的触发器个数为： $n_3 - n_2 = 16 - 12 = 4$ ；

在 $DG_1 \sim DG_3$ 触发器组之间串接有异或门 Y1、Y2。并且 $DG_1 \sim DG_3$ 触发器组的串接顺序按照触发器组的序号进行串接的，也就是，串接顺序为 DG_1 、 DG_2 、 DG_3 。

反相器，其输出端与 DG_1 触发器组的输入端相连。

异或非门，其一个输入端为所述 CRC 校验码生成电路的输入端，另一个输入端与 DG_3 触发器组的输出端相连，其输出端与所述反相器的输入端、以及各异或门（Y1 和 Y2）的一个输入端相连。

信息码从如图 5 所示的 CRC 校验码生成电路的输入端，即异或非门的一个输入端依次输入，则在所有的信息码从所述输入端输入后，触发器组的各

触发器的输出即为信息码的余式取反后的 CRC 校验码。

从图 5 中可以看出,本发明实施例提供的 CRC 校验码生成电路比现有技术的如图 4 所述的 CRC 校验码生成电路减少了 15 个反相器,从而节省了电路成本、电路空间。而且,当需要生成的校验码的位数越高的时候,节省的逻辑门(反相器)的数量就更多,节省的电路空间也就更大。

再例如,32 位的 CRC 校验码的生成电路如图 6 所示,其特征多项式为 $g(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$ 。(此为 CRC-CCITT32 类型的校验码的特征多项式)电路包括 32 个触发器(R0~R31),分属于 14 个触发器组(DG₁~DG₁₄),还包括:异或门(Y1~Y13)、反相器(N0)、异或非门(Y0)。

根据上述方法,可以计算出每个触发器组中的触发器个数。DG₁~DG₁₄ 的触发器组的触发器个数分别为:1、1、2、1、2、1、2、1、1、4、6、1、3、6。由于为 CRC-CCITT32 类型的校验码的生成电路,因此电路的触发器组中的每个触发器的复位值为 0。触发器组依触发器组的序号顺序串接。

在各触发器组之间还串接有异或门 Y1~Y13。异或门 Y1~Y13 分别串接于相邻的两个触发器组之间。

反相器 N0 的输出端与 DG₁ 触发器组的输入端相连。

异或非门 Y0 的一个输入端为 32 位 CRC 校验码生成电路的输入端,另一个输入端与 DG₁₄ 触发器组的输出端相连,其输出端分别与反相器 N0 的输入端、以及各异或门(Y1~Y13)的输入端相连。

信息码从如图 6 所示的 CRC 校验码生成电路的输入端,即异或非门的一个输入端依次输入,则在所有的信息码从所述输入端输入后,触发器组的各触发器的输出即为信息码的余式取反后的 CRC 校验码。

上述以生成 CRC-CCITT16/32 类型的 CRC 校验码为例的电路中的触发器的复位值为 0,而对于应用本发明原理生成的其它类型的 CRC 校验码的电路中的触发器,本领域技术人员可以根据实际情况将其设置为 0 或者 1。

下面以如图 5 所示的电路为例来说明本发明实施例的 CRC 校验码生成电路输出的 CRC 校验码与现有技术的 CRC 校验码生成电路输出的 CRC 校验码相同。

在如图 5 所示的电路中，假设各触发器的复位值（即初始值）为 $C_0 \sim C_{15}$ ，
5 由于各触发器的复位值与现有技术图 4 所示的触发器的复位值相反，则图 4 电路中的各触发器的初始值为 $\overline{C_0} \sim \overline{C_{15}}$ 。

经过一个时钟周期后，信息码的第一个数据 D_0 输入到如图 4、图 5 所示的电路中，则图 4、图 5 所示的电路中的各触发器输出值如下表所示：

10

表 1

	R0	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15
图 4 电路	$C_{15} \wedge D_0$	C_0	C_1	C_2	C_3	$C_4 \wedge C_{15} \wedge D_0$	C_5	C_6	C_7	C_8	C_9	C_{10}	$C_{11} \wedge C_{15} \wedge D_0$	C_{12}	C_{13}	C_{14}
图 5 电路	$\sim C_{15} \wedge D_0$	$\sim C_0$	$\sim C_1$	$\sim C_2$	$\sim C_3$	$\sim C_4 \wedge C_{15} \wedge D_0$	$\sim C_5$	$\sim C_6$	$\sim C_7$	$\sim C_8$	$\sim C_9$	$\sim C_{10}$	$\sim C_{11} \wedge C_{15} \wedge D_0$	C_{12}	$\sim C_{13}$	$\sim C_{14}$

从上表可以直接看出，经过一个时钟周期后，图 4 电路中的触发器 $R_1 \sim R_4$ 、
15 $R_6 \sim R_{11}$ 、以及 $R_{13} \sim R_{15}$ 输出的值与图 5 电路中的触发器 $R_1 \sim R_4$ 、 $R_6 \sim R_{11}$ 、
以及 $R_{13} \sim R_{15}$ 输出的值相反。

而图 4 电路中的触发器 R_0 输出值为 $C_{15} \wedge D_0$ ，图 5 电路中的触发器 R_0 输出值为 $\sim C_{15} \wedge D_0$ 。根据公式 $A \wedge B = \sim \overline{A \wedge B}$ ，则有 $C_{15} \wedge D_0 = \sim \overline{\sim C_{15} \wedge D_0}$ ，因此图 4 电路中的 R_0 与图 5 电路中的 R_0 输出值也相反。

同理，图 4 电路中的 R_5 、 R_{12} 的输出值也与图 5 电路中的 R_5 、 R_{12} 的输出值相反。因此，图 4 电路中的 $R_0 \sim R_{15}$ 输出值经反相器反向后即与图 5 电路
20

的 R0~R15 输出值相同。

再经过一个时钟周期后，重复上个时钟周期的推导过程，可发现图 4 电路中 R0~R15 输出值与图 5 电路的 R0~R15 输出值仍相反。

依次类推，经过 N 个时钟周期，串行输入了 N 位数据流后，图 4 电路中 R0~R15 输出值与图 5 电路的 R0~R15 输出值仍相反。而图 4 电路中 R0~R15 输出值经反相器反向后即与图 5 电路的 R0~R15 输出值相同，从而图 4 和图 5 电路得到相同的 CRC 校验码。

因此，本发明实施例提供的如图 5 所示的电路生成的 CRC 校验码与现有技术如图 4 所示的电路生成的 CRC 校验码相同。类似的，对于采用本发明实施例的方法生成的其它电路生成的 CRC 校验码也会与现有技术的电路生成的 CRC 校验码相同，此处不再对各种电路进行一一证明，本领域技术根据本发明实施例公开的技术内容可以轻而易举实现。

本发明实施例的 CRC 校验码生成电路由于将现有技术电路中的每个触发器连接的反相器去掉，并在数据输入到串接的触发器之前连接反相器进行取反，从而节省了大量的反相器，简化了 CRC 校验码生成电路、降低了硬件成本。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分步骤是可以通程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，如：ROM/RAM、磁碟、光盘等。

还可以理解的是，附图或实施例中所示的装置结构仅仅是示意性的，表示逻辑结构。其中作为分离部件显示的模块可能是或者可能不是物理上分开的，作为模块显示的部件可能是或者可能不是物理模块。

以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以作出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

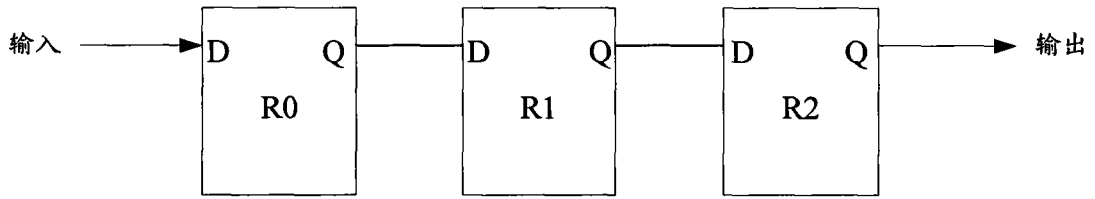


图 1

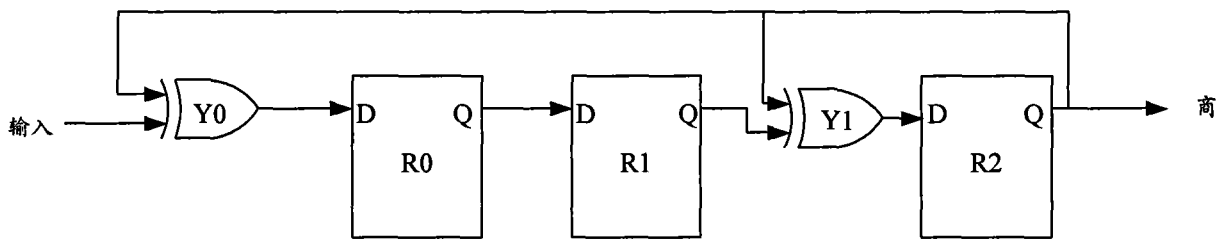


图 2

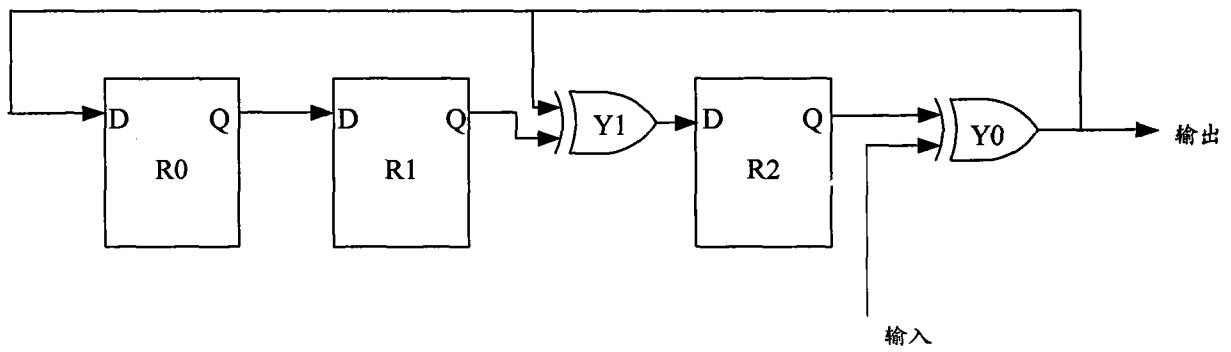


图 3

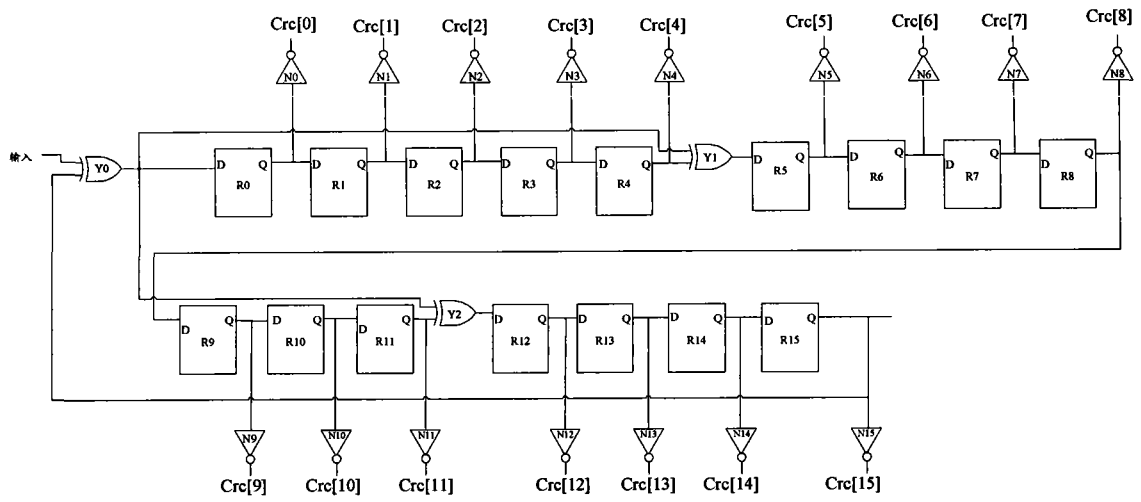


图 4

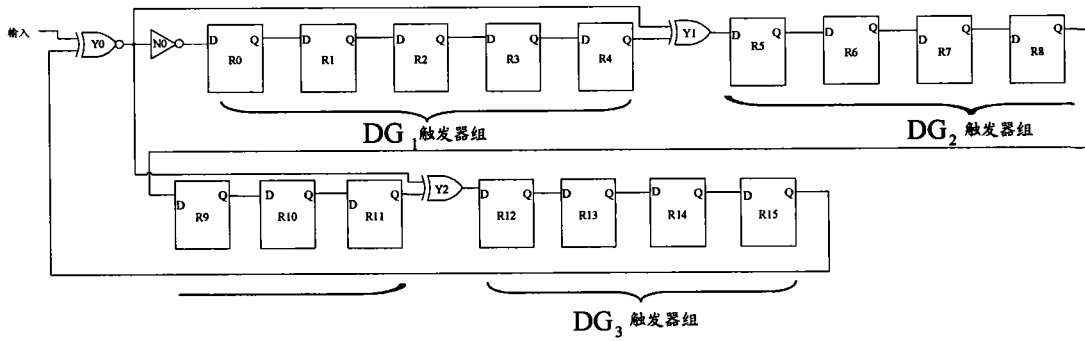


图 5

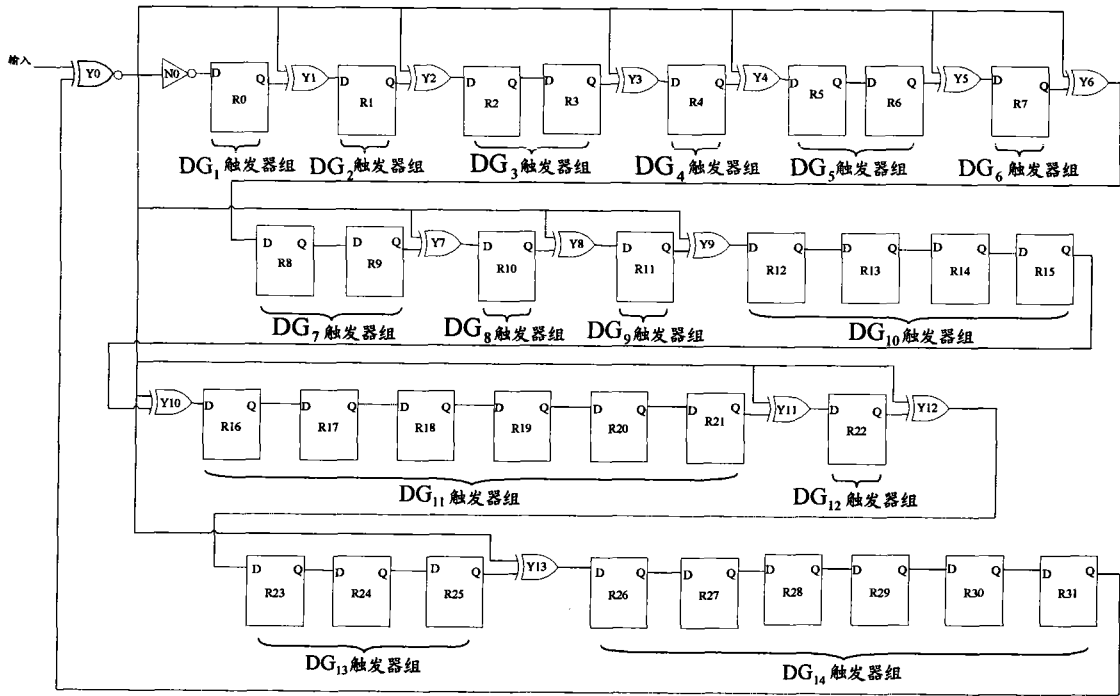


图 6