

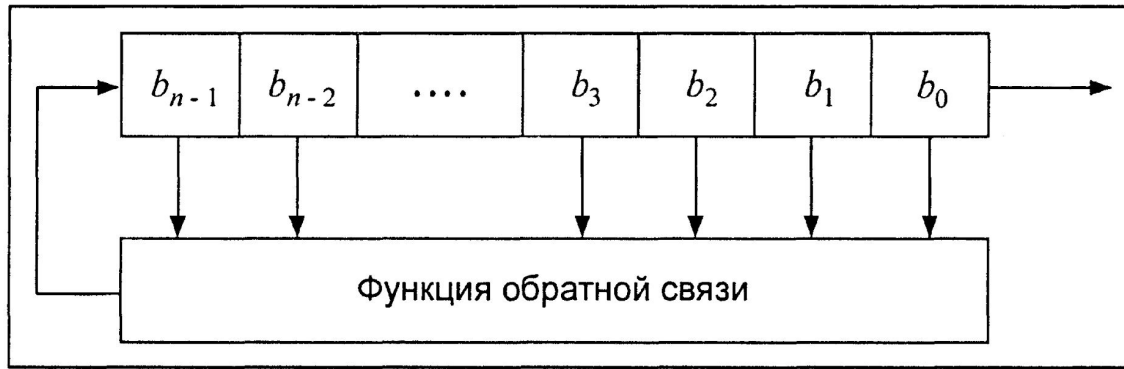


Рис. 16.1. Регистр сдвига с обратной связью

Регистр сдвига представляет собой последовательность битов. **Длина регистра сдвига выражается числом битов.** Если длина регистра равна n битам, регистр называют n -битовым регистром сдвига.

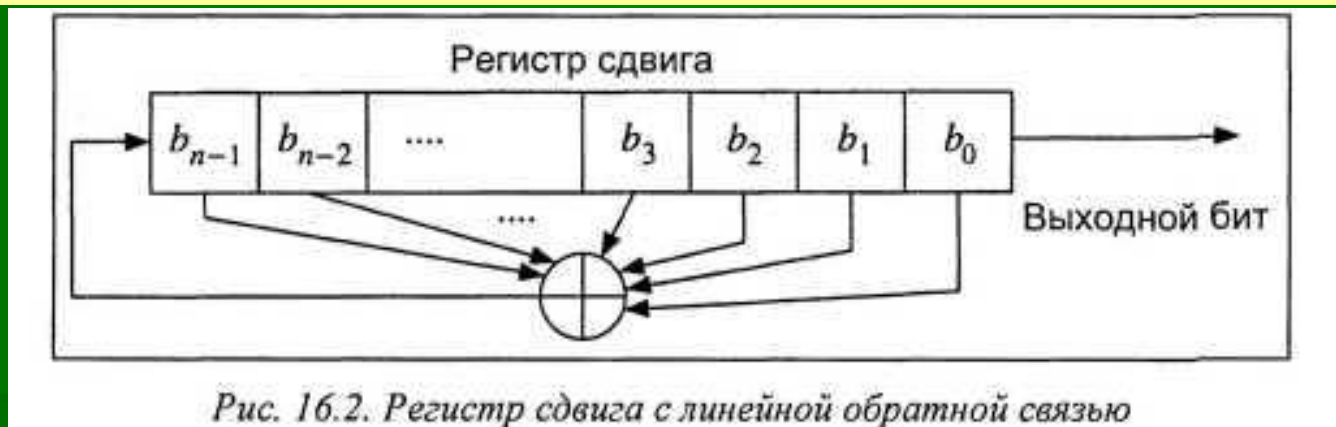
При каждом извлечении бита все биты регистра сдвига сдвигаются вправо на 1 позицию.

Новый старший бит рассчитывается как функция от всех остальных битов регистра.

На выходе регистра сдвига оказывается 1 бит, обычно младший значащий бит.

Периодом регистра сдвига называют длину получаемой последовательности до начала ее повторения.

К простейшему типу регистра сдвига с обратной связью относится **регистр сдвига с линейной обратной связью** (РСЛОС) (*Linear Feedback Shift Register, LFSR*) (см. Рис. 16.2). Обратная связь представляет собой просто операцию XOR над некоторыми битами регистра; перечень этих битов называется **последовательностью отводов** (или точек съема).



Иногда такую схему называют **конфигурацией Фибоначчи**.

$$b_{k+n} = \left(\sum_{i=0}^{n-1} c_i \cdot b_{k+i} \right)_{\text{mod } 2}, \quad k \geq 0.$$

$$x^{32} + x^7 + x^5 + x^3 + x^2 + x + 1$$

Высшая степень является длиной РСЛОС - n .

Биты нумеруются от $n - 1$ до 0.

Все степени, за исключением старшей, задают последовательность отводов, отсчитываемую от правого (младшего) края регистра сдвига.

Член x^n обозначает вход, который подается на левый (старший) край регистра.

Запись (32, 7, 5, 3, 2, 1, 0) означает, что для данного 32-битового регистра сдвига новый бит генерируется с помощью операции XOR над **седьмым, пятым, третьим, вторым, первым и нулевым битами** (см. Рис. 16.4). Период итогового РСЛОС будет максимальным, циклически проходя последовательность $2^{32} - 1$ значений до ее повторения.

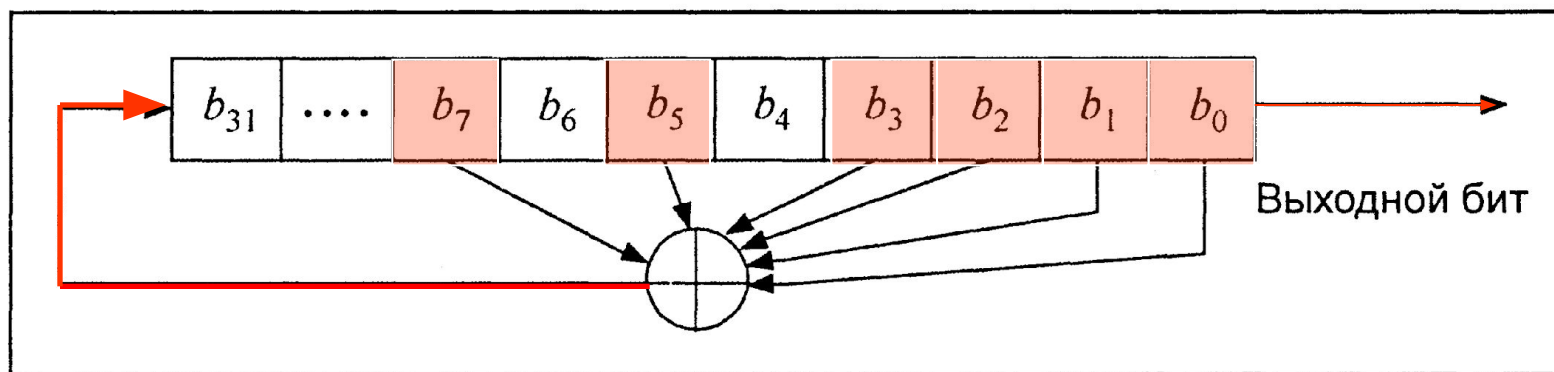


Рис. 16.4. 32-битовый РСЛОС с максимальной длиной