УДК 519.6

ОБОБЩЕННЫЙ РЕГИСТР СДВИГА

В.А. Орлов, **В.А. Матвеев**

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация
e-mail: orlovaldr@mail.ru

Рассмотрен вопрос расширения элементной базы проектирования дискретных устройств с памятью. Предложено устройство (обобщенный регистр сдвига), которое существенно увеличивает возможности однонаправленного регистра сдвига с последовательным вводом и параллельным выводом, являющегося последовательным соединением триггеров. Триггер из любого состояния может перейти при подаче тактового импульса (т.е. в следующий момент времени) в любое состояние (в зависимости от значения входа). Однако n-разрядный регистр сдвига в алфавите мощности M при любом $n \geq 2$ в следующий момент времени может перейти только в M состояний. Отмечено, что такой регистр сдвига имеет M^n состояний. Известно, что устройства, в схеме которых все элементы памяти находятся в одном регистре сдвига, реализуют узкий класс отображений. Показано, что любое последовательное устройство можно реализовать схемой из функциональных элементов и одного обобщенного регистра сдвига.

***Ключевые слова*:** триггер, регистр сдвига, конечный автомат, единичная задержка, функциональный элемент.

A GENERALIZED SHIFT REGISTER

V.A. Orlov, **V.A. Matveev**

Bauman Moscow State Technical University, Moscow, Russian Federation
e-mail: orlovaldr@mail.ru

An issue of extension of hardware for designing discrete devices with memory is considered. A device (generalized shift register) is proposed that substantially increases the capability of a unidirectional shift register with the series input and parallel output, which is implemented as a series connection of triggers. When a clock pulse is supplied, the trigger (at the next moment of time) can transfer from any state to the state depending on the input value. However the n-digit shift register in the alphabet with cardinality M at any $n \geq 2$ can transfer at the next moment only to M states. This shift register is noted to have M^n states. The devices, in the circuit of which all memory elements are in the same shift register, are known to implement a narrow class of images. It is shown that any sequential device can be implemented as a circuit of functional elements and a single generalized shift register.

***Keywords*:** trigger, shift register (shifter), finite-state automation, unit delay, functional element (functor).

Устройства обработки дискретной информации широко распространены: они входят, например, даже в современные приборы учета потребления электроэнергии физическими лицами.

Разработка таких устройств, как правило, начинается с построения их схем, содержащих элементы, реализующие достаточно простые преобразования. Набор таких элементов будем называть базисом.

Наиболее востребованной областью является проектирование *последовательностных* устройств. Эти устройства преобразуют последовательности

символов входного алфавита (входные последовательности) в последовательности выходного алфавита той же длины. Символы поступают (и считываются) в дискретные моменты времени, определяемые генератором тактовых импульсов. Устройство может находиться в одном из своих (внутренних) состояний. Число состояний конечно. В каждый момент времени выходной символ и состояние в следующий момент времени однозначно определяются входным символом и текущим состоянием. Математической моделью последовательностных устройств являются конечные автоматы.

Наиболее часто последовательностные схемы строят из функциональных элементов (реализующих преобразования, не зависящие от времени) и триггеров. Значение выхода триггера при подаче тактового импульса (т.е. в следующий момент времени) равно значению его входа в текущий момент времени.

Целью работы является расширение функциональных возможностей однонаправленного регистра сдвига с последовательным вводом и параллельным выводом, являющегося последовательным соединением триггеров [1].

Регистры сдвига часто используют для обработки информации. Например, при выполнении арифметических операций операнды загружаются в регистры сдвига; значения результата операции вычисляют как функции значений выходов регистров сдвига.

В качестве особенности обычного регистра сдвига отметим следующее. Состоянием триггера считают значение его выхода, а состоянием регистра сдвига — упорядоченный набор состояний его элементов (триггеров). При анализе цифровых устройств с памятью часто время полагают дискретным, равным числу поданных тактовых импульсов от начала работы устройства. Триггер из любого состояния может перейти при подаче тактового импульса (т.е. в следующий момент времени) в любое состояние (в зависимости от значения входа). Однако n-разрядный регистр сдвига в алфавите мощности M при любом $n \geq 2$ в следующий момент времени может перейти только в M состояний, такой регистр сдвига имеет M^nсостояний. Известно, что устройства, в схеме которых все элементы памяти находятся в одном регистре сдвига, реализуют узкий класс последовательностных отображений.

Предлагаемое устройство назовем обобщенным регистром сдвига (ОРС). Оно может переходить в следующий (дискретный) момент времени из любого состояния в любое свое состояние. При этом при любой последовательности значений входов обобщенного регистра сдвига на его основном выходе в любой момент времени t реализуется перестановка значений его основного входа в момент времени $t - n$, где n — разрядность регистра сдвига. Отметим, что авторы хотели назвать ОРС управляемым регистром сдвига, но это понятие уже имеет другой смысл.

Поставленная задача решается следующим образом. Обобщенный регистр сдвига состоит из n триггеров и $n - 1$ функциональных элементов с двумя входами и одним выходом, реализующих функцию, которая при любом фиксированном аргументе является перестановкой другого аргумента, кроме того, среди перестановок первого аргумента имеется тождественная перестановка (такой функцией является, например, сложение по модулю

мощности алфавита регистра). Входом ОРС является вход первого триггера. Выход каждого триггера, кроме последнего, присоединяется к первому входу функционального элемента. Вторые входы функциональных элементов суть управляющие входы обобщенного регистра сдвига. Выход функционального элемента присоединяется к входу следующего триггера. Выходы триггеров, кроме последнего, являются выходами обобщенного регистра сдвига. Основным выходом обобщенного триггера является выход последнего триггера.

Нетрудно проверить, что предлагаемое устройство (n-разрядный ОРС) обладает объявленным свойством. А именно, из любого состояния он может перейти в следующий момент времени в любое другое свое состояние. Поскольку суперпозиция перестановок является перестановкой, ОРС обладает следующим свойством. При любой последовательности значений управляющих входов обобщенного регистра сдвига на основном выходе в любой момент времени t реализуется перестановка значений его основного входа в момент времени $t - n$, где n — разрядность регистра. Отметим, что если функциональные элементы ОРС реализует сумму значений их входов по модулю мощности алфавита, то при значениях управляющих входов, равных нулю, функционирование n-разрядного ОРС совпадает с функционированием обычного n-разрядного регистра сдвига.

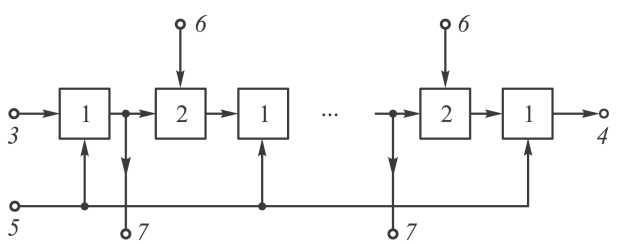
На рисунке показана схема ОРС.

Входом *3* ОРС является вход первого триггера. Выход *7* каждого триггера, кроме последнего, присоединяется к первому входу функционального элемента. Вторые входы *6* функциональных элементов суть управляющие входы ОРС. Выход функционального элемента *2* присоединяется к входу следующего триггера. Выходы *7* триггеров, кроме последнего, являются выходами ОРС. Основным выходом *4* обобщенного триггера является выход последнего триггера.

Докажем теперь еще одно свойство ОРС: любое последовательностное устройство в алфавите A мощности M, имеющее не более M^n состояний, можно реализовать с использованием функциональных элементов и одного n-разрядного ОРС в алфавите A.

Доказательство проведем с использованием теории конечных автоматов.

Для простоты изложения ограничимся рассмотрением автоматных базисов в алфавите $\{0, 1\}$, состоящих из функционально полной системы элементов с одним состоянием и элемента единичной задержки.



Блок-схема ОРС:
1 — триггер; *2* — функциональный элемент; *3* — вход; *4* — основной выход; *5* — тактовый вход; *6* — управляющие входы; *7* — выходы

Конечный автомат является имеющим вход и выход устройством, которое может находиться в одном из своих состояний. Конечный автомат осуществляет преобразование информации в дискретные моменты времени $0, 1, 2, \ldots, t, \ldots$ На вход автомата поступает последовательность символов входного алфавита $\mathbf{X} = \{X_1, X_2, \ldots, X_N\}$; эту последовательность называют входным словом. Функционирование конечного автомата осуществляется в соответствии с системой из NS команд, где S – мощность алфавита состояний $\mathbf{Q} = \{Q_1, Q_2, \ldots, Q_S\}$. Значение выхода автомата является элементом выходного алфавита $\mathbf{Y} = \{Y_1, Y_2, \ldots, Y_M\}$. Каждая команда имеет следующий вид: $X_i Q_j \to Y_k Q_l$, где X_i — входная буква, Q_j — текущее состояние, Y_k — выходная буква и Q_l — состояние в следующий за текущим моментом момент времени (следующее состояние).

Функционирование конечного автомата задают также кортежем

$$< \mathbf{X}, \mathbf{Y}, \mathbf{Q}, V, P >,$$

где V: $\mathbf{X} \times \mathbf{Q} \to \mathbf{Y}$ (функция выхода); P: $\mathbf{X} \times \mathbf{Q} \to \mathbf{Q}$ (функция переходов).

Конечный автомат с определенным состоянием в начальный момент времени называется инициальным автоматом. В соответствии со своей системой команд инициальный автомат реализует автоматную функцию, которая произвольное входное слово преобразует в выходное слово той же длины.

Трахтенброт Б.А. [2, 3] показал, что любой конечный автомат можно реализовать схемой, элементами которой являются функциональные элементы и элементы единичной задержки. При некоторых соотношениях между параметрами конечного автомата (N, M и S) эта реализация является асимптотически наилучшей. Отметим, что в случае произвольных автоматных базисов реализация существенно усложняется [4–6]. Возможна зависимость сложности реализации от весов нескольких элементов базиса; задача нахождения асимптотически наилучшей реализации алгоритмически неразрешима.

Для реализации автомата M в рассматриваемом базисе буквы алфавитов $\mathbf{X}$, $\mathbf{Y}$ и $\mathbf{Q}$ кодируют двоичными наборами длин n, m и s соответственно. При этом кодировании функции V (функции P) соответствует система m (система s) булевых функций от $n + s$ переменных.

Имеющую k входов и r входов схему называют (k, r)-блоком.

Согласно Б.А. Трахтенброту, схема S, реализующая автомат M, имеет n входов $x_1, x_2, \ldots, x_n$, m выходов $y_1, y_2, \ldots, y_m$ и состоит из $(n + s, m)$-блока A, $(n + s, s)$-блока B и s элементов задержки. Здесь $n =]\log_2 N[$, $m =]\log_2 M[$ и $s =]\log_2 S[$. Блок A (блок B) реализует функцию выхода (функцию переходов). Входы схемы S соединены с первыми входами блоков A и B. Остальные входы этих блоков соединены с выходами s элементов задержки. Входы элементов задержки соединены с последними s выходами блока B. Выходами схемы S являются выходы блока A.

Покажем, что любой конечный автомат можно реализовать схемой, в которой все элементы памяти находятся в одном ОРС.

Через Z обозначим (2, 1)-блок, состоящий из (2, 1)-элемента D, реализующего сложение по модулю два, и элемента задержки. Выход элемента

D соединен с входом элемента задержки. Входами блока Z являются входы элемента D. Выходом блока Z является выход элемента задержки.

Являющуюся (s, s)-блоком схему, состоящую из элемента задержки и $s-1$ блоков Z, назовем (Z, s)-цепочкой. Первым входом (выходом) (Z, s)-цепочки является вход (выход) элемента задержки, выход которого соединен с входом первого блока Z. Выход блока Z соединен с входом следующего блока Z. Остальными входами (выходами) (Z, s)-цепочки являются входы (выходы) блоков Z. Нетрудно проверить, что (Z, s)-цепочка является моделью s–разрядного ОРС.

Состоянием конечного автомата является набор значений выходов его элементов задержки. Через $z_1, z_2, \ldots, z_s$ обозначим значения входов (Z, s)-цепочки, а через $u_1, u_2, \ldots, u_s$ — значения ее выходов.

Нетрудно проверить, что из состояния $(u_1, u_2, \ldots, u_s)$ (Z, s)-цепочка перейдет в состояние

$$z_1, u_1 \oplus z_2, \ldots, u_{s-1} \oplus z_s,$$

где символом $\oplus$ обозначена операция сложения по модулю 2.

Покажем теперь, что любой конечный автомат можно реализовать схемой T, в которой все элементы задержки находятся в одном ОРС.

Эта схема T, реализующая автомат М, имеет n входов $x_1, x_2, \ldots, x_n$, m выходов $y_1, y_2, \ldots, y_m$ и состоит из $(n + s, m)$-блока A, $(n + s, s)$-блока C и (s, s)-блока R, являющегося (Z, s)-цепочкой.

Блок A (как и в схеме S) реализует функцию выхода. Входы схемы T соединены с первыми входами блоков A и C. Остальные входы этих блоков соединены с выходами блока R. Входы блока R соединены с последними s выходами блока C. Выходами схемы T являются выходы блока A.

Опишем функционирование блока C. Значения выходов блока R обозначим через $q_1, q_2, \ldots, q_s$.

Пусть $p_i(x_1, \ldots, x_n, q_1, \ldots, q_s)$, $\quad 1 \le i \le s$, — булева функция, реализуемая на i-м выходе блока B (из схемы S).

Пусть $z_i(x_1, \ldots, x_n, q_1, \ldots, q_s)$, $\quad 1 \le i \le s$, — булева функция, реализуемая на i-м выходе блока C. Положим

$$z_1(x_1, \ldots, x_n, q_1, \ldots, q_s) = p_1(x_1, \ldots, x_n, q_1, \ldots, q_s)$$

и

$$z_i(x_1, \ldots, x_n, q_1, \ldots, q_s) = p_i(x_1, \ldots, x_n, q_1, \ldots, q_s) \ \oplus q_{i-1}, \quad 2 \le i \le s.$$

Нетрудно проверить, что схема T реализует автомат М. Поскольку блоки B и C реализуют различные системы булевых функций, схема T может иметь более простую реализацию.

Отметим, что в ОРС элементы задержки почти образуют цепочку, что может иметь значение в ряде приложений.

В заключение отметим, что предлагаемый авторами ОРС может быть использован при построении универсальных и специализированных устройств обработки дискретной информации.

ЛИТЕРАТУРА

1. *Джон Ф. Уэйкерли*. Проектирование цифровых устройств. Т. 1, 2 / пер. с англ. Е.В. Воронова, А.Л. Ларина. М.: ПОСТМАРКЕТ, 2002. 1088 с.
2. *Трахтенброт Б.А.* Асимптотическая оценка сложности логических сетей с памятью // Докл. АН СССР. 1959. Т. 127. № 2. С. 281–284.
3. *Трахтенброт Б.А.* О сложности схем, реализующих многопараметрические семейства операторов: Сб. “Проблемы кибернетики”. М.: Наука, 1964. Вып. 12. С. 99–112.
4. *Орлов В.А.* Алгоритмическая неразрешимость задачи нахождения асимптотического поведения функции Шеннона при реализации ограниченно-детерминированных операторов схемами в произвольном базисе // Докл. АН СССР. 1971. Т. 196. № 5. С. 1036–1039.
5. *Орлов В.А.* Об особенностях поведения функции Шеннона в случае автоматных базисов // Математические заметки. 1972. Т. 11. Вып. 1. С. 73–82.
6. *Орлов В.А.* О реализации функций схемами и формулами в функционально полных базисах // Докл. РАН. 1999. Т. 365. № 6. С. 734–735.

REFERENCES

[1] Wakerly J.F. Digital Design: Principles and Practices. 3rd Ed. Prentice Hall, 1999. 949 p. (Russ. Ed.: Dzhon F. Ueykerli. Proektirovanie tsifrovykh ustroystv. V 2 t. Moscow, POSTMARKET Publ., 2002. 543 p. (vol. 1), 528 p. (vol. 2).

[2] Trakhtenbrot B.A. An asymptotic estimate of the complexity of logical networks with memory. *Dokl. Akad. Nauk SSSR* [Proc. Acad. Sci. USSR], 1959, vol. 127, no. 2, pp. 281–284 (in Russ.).

[3] Trakhtenbrot B.A. On the complexity of circuits implementing multiparameter families of operators. *Sb. “Problemy kibernetiki”* [Collect. Pap. “Cybernetics problems”]. Moscow, Nauka Publ., 1964. iss. 12, pp. 99–112 (in Russ.).

[4] Orlov V.A. Algorithmic undecidability of the detecting problem of the asymptotic behavior of the Shannon function in implementing bounded-deterministic operators using schemes in an certain basis. *Dokl. Akad. Nauk SSSR* [Proc. Acad. Sci. USSR], 1971, vol. 196, no. 5, pp. 1036–1039 (in Russ.).

[5] Orlov V.A. Singularities of Shannon functions in the case of automation bases. *Matematicheskie zametki* [Mathematical Notes, pp. 48–53], 1972, vol. 11, no. 1, pp. 73–82 (in Russ.).

[6] Orlov V.A. On the functions implementation by circuits and formulas in functionally complete basis *Dokl. RAN* [Proc. Russ. Acad. Sci.], 1999, vol. 365, no. 6, pp. 734–735 (in Russ.).

Статья поступила в редакцию 06.01.2013

Валентин Александрович Орлов — д-р физ.-мат. наук, профессор кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана. Автор более 60 научных работ в области синтеза оптимальных управляющих систем, моделей и алгоритмов обработки дискретной информации, интеллектуальных информационных систем, информационной безопасности и криптографии.
МГТУ им. Н.Э. Баумана, Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5.

V.A. Orlov — Dr. Sci. (Phys.–Math.), professor of of “Information Security” department of the Bauman Moscow State Technical University. Author of more than 60 publications and two inventions in the field of synthesis of optimal control systems, models and algorithms of discrete data processing, intelligent information systems, information security and cryptography.
Bauman Moscow State Technical University, Vtoraya Baumanskaya ul. 5, Moscow, 105005 Russian Federation.

Валерий Александрович Матвеев — д-р техн. наук, профессор, руководитель Научно-учебного комплекса “Информатика и системы управления”, заведующий кафедрой “Информационная безопасность” МГТУ им. Н.Э. Баумана. Заслуженный деятель науки РФ, лауреат Государственных премий СССР и РФ, лауреат премий Правительства РФ в области науки и образования. Автор более 200 научных работ и 25 патентов в области приборостроения и высокотемпературной сверхпроводимости.
МГТУ им. Н.Э. Баумана, Российская Федерация, 105005, Москва, ул. 2-я Бауманская, д. 5.

V.A. Matveev — Dr. Sci. (Eng.), professor, head of “Information security” department, chief of Scientific and Educational Complex for Informatics and Control Systems of the Bauman Moscow State Technical University. Honored Scientist of the Russian Federation, Laureate of the State Prizes of the USSR and Russian Federation, Laureate of the RF Government Prize in Science and Education. Author of more than 200 publications and 25 patents in the field of instrument engineering and high-temperature superconductivity.
Bauman Moscow State Technical University, Vtoraya Baumanskaya ul. 5, Moscow, 105005 Russian Federation.