DOI 10.37882/2223-2966.2023.07.15

СТРУКТУРА ОДНОРОДНЫХ РЕГИСТРОВЫХ СРЕД В ПОЛЯХ ГАЛУА

STRUCTURE OF HOMOGENOUS REGISTRY FIELDS IN THE GALUA FIELDS

Z. Kardashova

Summary: This article covers the issues of defining the concept and classification of media from homogeneous register elements, methods of their theoretical description using extended binary Galois fields GF(2^m), examples of circuit design of cells of these media and connecting them together and blocks.

Keywords: Galois field GF(2^m), homogeneous medium, register structures, logical cell, encoding and decoding, error limiting codes, digital filtering.

Кардашова Земфира Рашидовна
Аспирант, Дагестанский государственный технический университет
zeminda@yandex.ru

Аннотация. Данная статья освящает вопросы определения понятия и классификации сред из однородных регистровых элементов, способов их теоретического описания с помощью расширенных двоичных полей Галуа GF(2^m), примеров схемотехнического исполнения ячеек этих сред и соединения их в совокупности и блоки.

Ключевые слова: поле Галуа GF(2^m), однородная среда, регистровые структуры, логическая ячейка, кодирование и декодирование, коды, ограничивающие ошибки, цифровая фильтрация.

Под однородной средой понимается некоторая совокупность функциональных элементов, способных выполнять ряд логических и/или арифметических операций и, в совокупности, реализующих ту или иную математическую парадигму.

Характерными свойствами однородной среды являются: [1]

1) Однородность состава структуры, состоящего из функционально одинаковых элементов, зачастую представляющих собой аппаратные или программные аналоги существующих в реальности узлов машин и механизмов, или органов живых существ.

2) Возможность создания в такой среде из однородных элементов виртуальных структур, способных преобразовывать информацию по заданным правилам.

3) Как следствие 2-го пункта, к функциональным элементам предъявляются требования:

- наличие связи каждого элемента с другими элементами среды по входам и выходам,
- связь с входом и выходом среды,
- возможность параллельного вывода состояния среды (контроль содержимого остатка от деления — сигнатуры),
- наличие входов обеспечения синхронности процессов, настройки элементов и среды от внешних устройств и др.

Создание однородной среды, реализующей заданную математическую парадигму, предполагает: [1]

1) Во-первых, определение алгебры операций, специфичных для рассматриваемого множества элементов, которые соответствуют классическим арифметическим и логическим действиям: сложению, умножению, делению, но выполняются по правилам выбранной области математики.

2) Во-вторых, это предполагает разработку соответствующего аппаратного и схематически реализуемого устройства, обеспечивающего выполнение основных математических операций над элементами некоторого множества (либо его программного аналога).

В ряде практически важных областей, таких, как цифровая фильтрация, идентификация двоичных последовательностей, помехоустойчивое кодирование и декодирование, генерация случайных последовательностей, Фурье-подобные преобразования и прочие, находит применение алгебра математических операций, определяемая аппаратом двоичных полей Галуа $GF(2^m)$. [2]

Технические разработки однородных сред для преобразования информации в полях Галуа $GF(2^m)$ традиционно представлены регистровыми структурами, обязательными элементами которых являются сумматоры по модулю два, регистры и логические элементы.

Их характерной особенностью является жёсткость правил преобразования, ориентированность на выполнение только определённого типа операций, заданных над полем, что, с практической стороны осуществляемых такой структурой операций, приводит к кодированию с использованием только одного из образующих кодов, или фильтрации только по одному фильтрующему полиному и т.д. Целый ряд работ в области однородных регистровых сред посвящён преодолению этих ограничений и созданию программируемых структур, способных гибко перестраиваться под реализацию тех или иных задач преобразования информации. [3]

Рассматривая элементы однородных регистровых сред, следует выделить два класса регистровых структур: [3]

1) В первом из них, сумматоры располагаются между ячейками регистра на позициях, определяемых одним из сомножителей или делителем.

2) Во втором классе сумматоры располагаются вне регистра.

Для каждого из этих классов, по направлению передачи информации в однородной среде, определены подклассы: [1]

1) В первом из них, информация передаётся с входа на выход: это направление является базовым при выполнении однородной средой операций умножения, например, в устройствах помехоустойчивого кодирования.

2) Во втором подклассе информация передаётся с выхода на вход, что используется в преобразователях с базовой операцией деления над полем, например, при декодировании с обнаружением ошибок.

Существуют три алгебраические структуры, увязывающие множества чисел с применяемыми к ним операциями, подобных сложению/вычитанию и умножению/делению:

1) Группа, поддерживает одну пару связанных операций над элементами множества: или сложение/вычитание, или умножение/деление.

2) Кольцо поддерживает одну пару связанных операций (обычно сложение / вычитание) и одну одиночную операцию (обычно умножение).

3) Поле — структура, поддерживающая две пары операций над его элементами: сложение/вычитание и умножение/деление, за исключением деления на нуль. Поле может иметь конечное и бесконечное число элементов. Так же поле определяют как коммутативное кольцо, в котором вторая операция удовлетворяет всем пяти свойствам (замкнутость, ассоциативность, коммутативность, существование нейтрального элемента, существование инверсии), определённым для первой операции, за исключением того, что нейтральный элемент первой операции (иногда называемый нулевой элемент) не имеет инверсии.

Практическое применение в приложениях, касающихся обработки сигналов, фильтрации, кодирования и декодирования нашли только конечные поля.

В 1830 году Эварист Галуа показал, что поля, чтобы быть конечными, должны иметь число элементов p^m, где p — простое, а m — положительное целое число. А в 1893 году Элиаким Мур доказал теорему о классификации конечных полей, утверждающую, что любое конечное поле является полем Галуа. Так за конечными полями закрепилось название полей Галуа и соответствующее обозначение: $GF(p^m)$.

Простейшим двоичным полем Галуа является конечное множество из двух (p=2, m=1) значений {0; 1} с определёнными для него операциями сложения (или, через аддитивную инверсию «–a», вычитания) и умножения (или, через мультипликативную инверсию «a^{-1}», деления), как показано на рисунке 1.

Операции, определённые на данном поле имеют ряд особенностей:

- сложение, фактически, является операцией исключающего «или» (XOR),
- операция умножения, фактически, является операцией логического «и» (AND),
- операции сложения и вычитания — та же самая операция XOR,
- операции умножения и деления — та же самая операция AND.

Аналогично, можно определить поле $GF(2^2)$ из m=2-х бит, имеющее 2^2=4 элементов:

{00, 01, 10, 11}.

Операции сложения и умножения для этого поля представлены на рисунке 2.

Здесь каждое слово (2 бита) — аддитивная инверсия себя.

Каждое слово (кроме 00) имеет мультипликативную инверсию.

Мультипликативные обратные пары — (01, 01) и (10, 11).

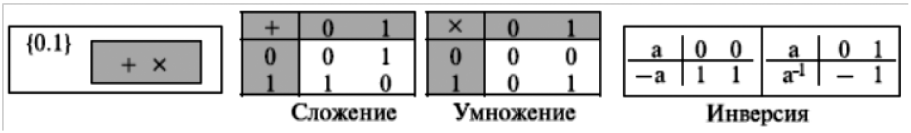

Рис. 1. Поле Галуа $GF(2^1)$

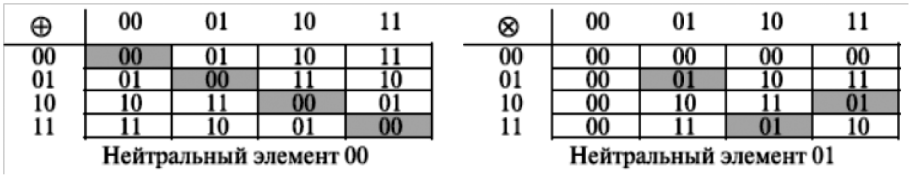

Рис. 2. Операции сложения и умножения для поля Галуа $GF(2^2)$

Поскольку компьютеры оперируют m-битовыми словами, в которых m={8; 16; 32; 64;…}, то наибольший интерес представляют поля Галуа $GF(2^8)$, $GF(2^{16})$, $GF(2^{32})$, $GF(2^{64})$ и так далее.

Примеры однородных регистровых сред

Разнообразие реализуемых однородными регистровыми средами математических парадигм предполагает широчайшее многообразие способов их аппаратной реализации. Можно отметить наличие моделей, позволяющих реализовать среды с ветвящимися структурами, среды, повышенной надёжности со скользящим структурным резервированием, позволяющие реализовать в среде виртуальные структуры преобразователей.

Некоторые из них рассмотрим ниже (см. рис. 3).

Этот элемент однородной регистровой среды имеет:

а) информационные входы:

2 — связи ячейки с общим входом среды;

4 — связи ячейки с выходом ячейки, предшествующей данной в среде;

7 — связи ячейки с выходом среды;

б) информационные выходы:

3 — вывода состояния ячейки в цепь обратной связи;

8 — связи с входом последующей данной в среде ячейки;

9 — вывода информации из ячейки;

в) входы настройки и синхронизации:

1 — ввода кода активизации входов и выходов элемента;

5 — ввода синхросигналов;

6 — установки элементов памяти среды в начальное состояние.

Входы и выходы ячеек среды активизируются в зависимости от выполняемых в среде функций, местоположения элемента в среде, кодов настройки, вводимых в регистр каждого из них по входу 1. По входу 5 осуществляется управление процессом синхронизации элементов среды. [3]

В работах [4], [5] предложена универсальная функциональная ячейка для формирования программируемой однородной регистровой среды, функциональная схема которой представлена на рисунке 5.

Функциональное назначение элементов этой ячейки следующее:

sm_i — логические сумматоры.

M — элемент памяти (ячейка регистра).

Рг — регистр хранения кода настройки структуры элемента среды.

XOR — сумматор по модулю поля $GF(2)$.

h_i — умножители в поле $GF(2^m)$ на скаляр — элемент поля GF(2), причём, h_i принимает значения 0 или 1, активизируя или блокируя тот или иной вход или выход ячейки.

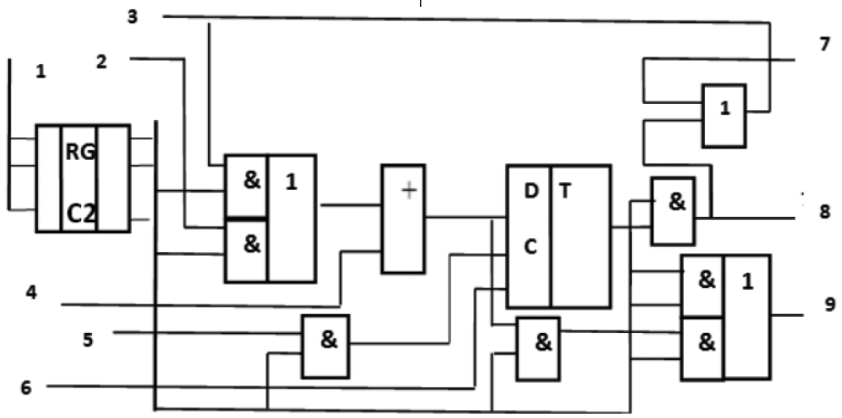

Рис. 3. Схема типового функционального элемента однородной регистровой среды [3]

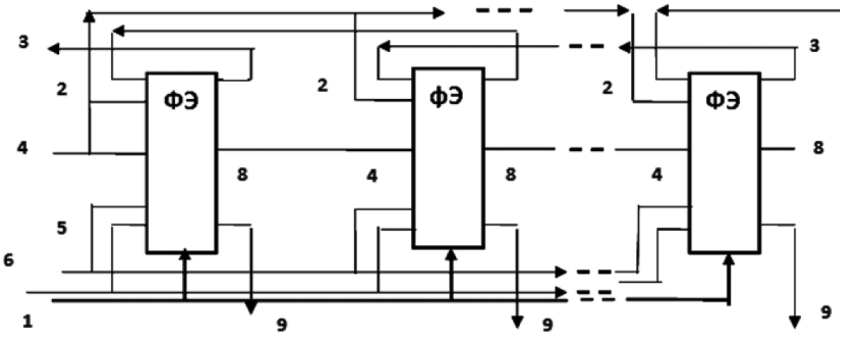

Рис. 4. Однородная регистровая среда на базе типового элемента с рисунка 3 [3]

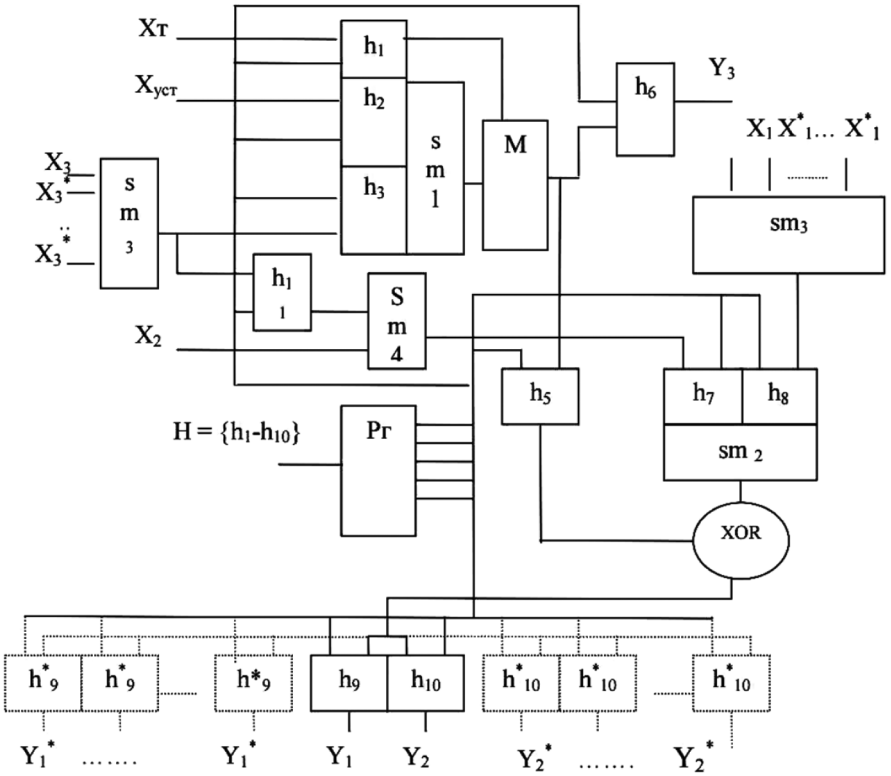

Рис. 5. Ячейка однородной ветвящейся полиномиальной среды [5]

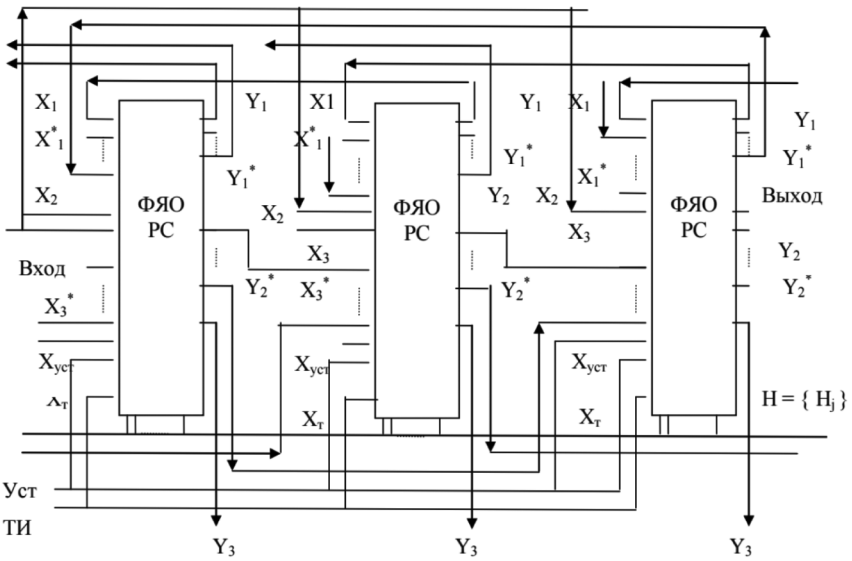

Рис. 6. Структура однородной ветвящейся полиномиальной среды [5]

*h**— элементы ячеек, для организации связей по информационным входам и выходам с ячейками, предшествующими и стоящими в среде после данной ячейки. При создании однородной среды без дополнительных связей, расширяющих функциональные возможности среды, эти элементы в её структуре отсутствуют.

$H = (h_1, h_2, \ldots, h_n)$ — двоичный вектор настройки ячейки, формируется и вводится в процессе формирования в среде структуры виртуальных преобразователей информации.

Однородная среда, построенная на базе ячейки рисунка 5, может быть функционально представлена схемой рисунка 6.

Одной из целей разработки и совершенствования однородных регистровых структур является возможность замены ими программируемых логических матриц (ПЛМ), широко применяемых в схемах аппаратного преобразования кодовых последовательностей.

Недостатками ПЛМ являются: [6]
- — большое время программирования;
- — невозможность перепрограммирования для использования ПЛМ в других целях, так как программирование осуществляется электрическим пережиганием специальных плавких участков;
- — невозможность исправить (восстановить) связи, пережжённые ошибочно.

В отличие от ПЛМ, программируемые регистровые структуры содержат блок управления и настройки, и блок, представляющий собой среду, состоящую из одинаковых функциональных элементов — ячеек, соединённых между собой гибкими, управляемыми программными связями, образующими однородную программируемую регистровую структуру, которая позволяют осуществлять приём сигналов каждым из её элементов, как от внешней среды — общего входа, так и по цепи обратной связи. [7]

Универсальная логическая ячейка с программируемой структурой, способная заменить собой элементы логических матриц, содержит: [7]
- — синхронный D-триггер (T),
- — сумматор по модулю два (XOR),
- — восемь логических элементов И (AND),
- — три логических элемента ИЛИ (OR).

В данной конструкции ячейки однородной среды предусмотрены: [7]
- — информационные входы элементов — X0, X1, X2,
- — управляющие сигналы — 1,2,3,4,5,6,8,9,
- — а также информационные выходы элементов — Y1, Y2, Y3.

Приведённая схема ячейки позволяет менять в однородной среде, построенной на её основе менять выполняемые средой функции и менять структуру связей между ячейками управляя направлением информационных потоков.

В [8] предложена однородная регистровая среда, представляющих системный аппаратный ресурс, в котором, в процессе эксплуатации системы, могут быть программно сформированы структуры виртуальных преобразователей информации, выполняющие функции генерации псевдослучайных чисел, кодирование и декодирование в кодах, обнаруживающих ошибки, функции цифровой фильтрации, функции операций умножения и деления в расширенных двоичных полях Галуа, функции хранения информации, сравнения кодов.

Установка в начальное состояние и настройка однородной регистровой среды с программируемой структурой сводятся к вводу данных о формируемом в среде виртуальном устройстве в блок управления и настройки и ввод этим блоком кодов настройки в регистры настройки регистровых ячеек блока, представленного на рисунке 8. От внешнего устройства в устройство управления и настройки вводится сигнал, определяющий характери-

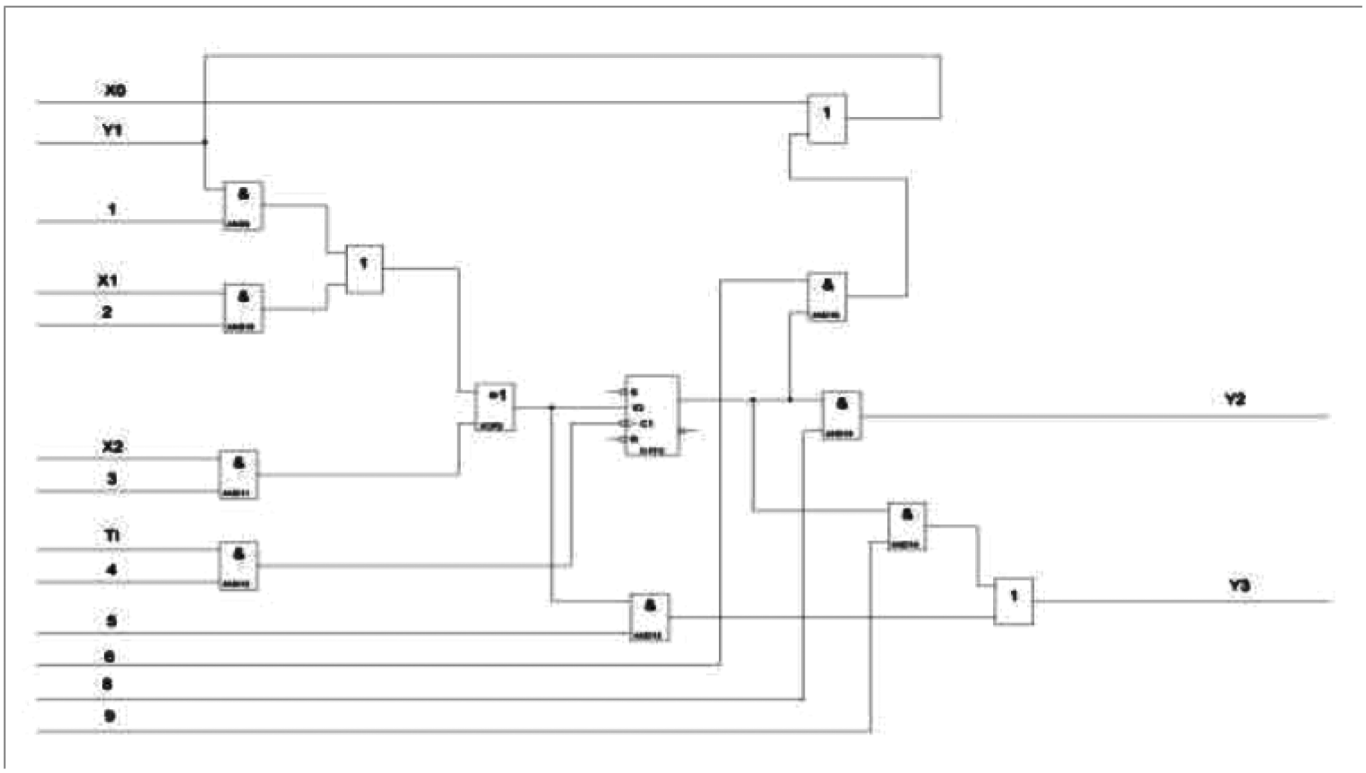

Рис. 7. Схема универсальной логической ячейки программируемой однородной среды [7]

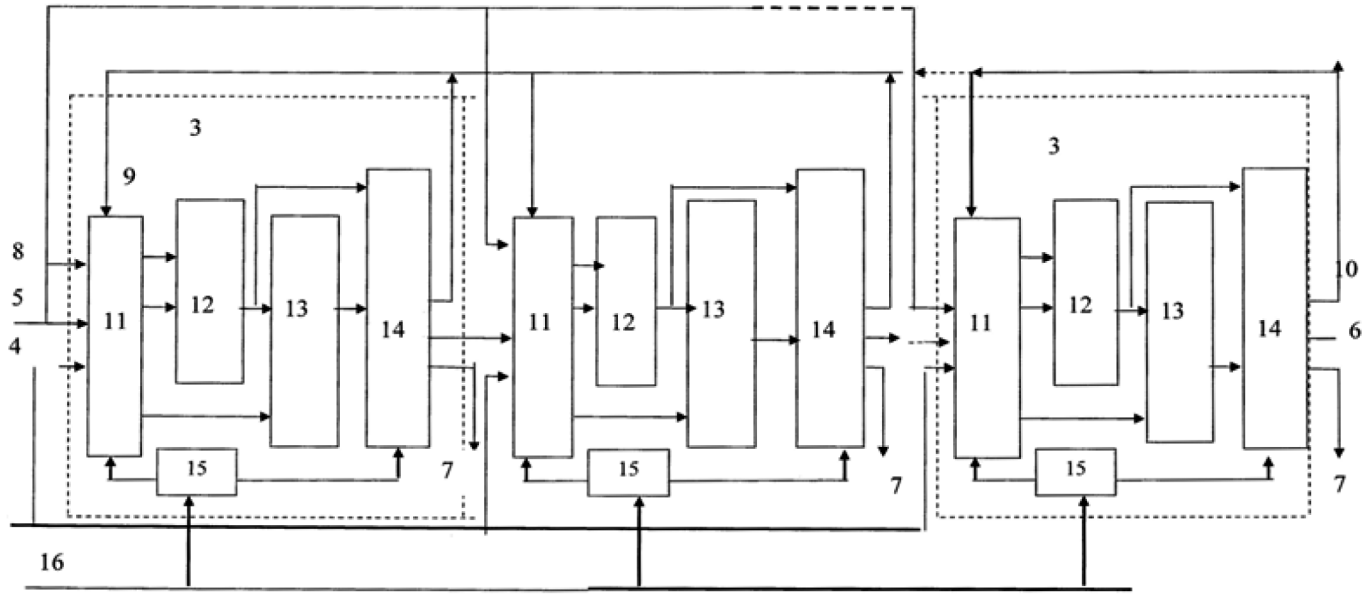

Рис. 8. Структура регистрового блока программируемой однородной среды [8]

стики входного сигнала и число тактов, выполнения операций по его преобразованию. При этом, устройством управления и настройки все регистры кодов настройки ячеек устанавливаются в начальное состояние. [8]

В зависимости от выбранного способа ввода кодов настройки выполняется настройка ячеек среды путём ввода по входам 16 кодов настройки в регистры ячеек. По окончании процесса настройки элементов среды осуществляются ввод преобразуемого входного сигнала и вывод результатов по тактовым импульсам, формируемым устройством управления и настройки. При этом, число тактовых импульсов зависит от выполняемых виртуальным устройством преобразований. [8]

Блок регистровых ячеек среды с программируемой структурой состоит из настраиваемых функциональных элементов-ячеек 3. Элемент-ячейка 3 содержит:

— логический блок входа 11,
— сумматор по модулю два 12,
— синхронный D-триггер 13,
— логический блок выхода 14,
— регистр кода настройки элемента 15.

Вход 5 первой ячейки блока связан с входом регистровой среды, а входы 5 остальных ячеек связаны с выходами 6 предшествующих ячеек.

Вход 8 всех ячеек связан с входом среды и служит для ввода преобразуемых данных.

Вход 4 связан с выходом тактирования устройства управления и настройки.

Входы 9 всех ячеек связаны с выходом регистрового блока цепью обратной связи.

Выходы 10 всех ячеек являются выходами в цепь обратной связи.

Выходы 7 являются выходами ячеек из среды.

Входы 16 являются входами настройки ячеек от устройства управления и настройки.

Код настройки каждой ячейки вводится и хранится на время выполнения функций виртуальным преобразователем информации в регистре 15. Выходы регистра определяют активные цепи логических блоков 11 и 14. На входы сумматора по модулю два 12, в зависимости от настройки, могут быть поданы сигналы с входа среды, выхода предшествующей ячейки или из цепи обратной связи. Выход сумматора связан с входом синхронного триггера 13, результат суммирования может быть записан в триггер, если настройка предполагает такую запись, либо результат может быть выведен на один из выходов ячейки через выходной логический блок 14.

Выводы

1) В области аппаратной реализации устройств цифровой фильтрации, преобразования кодов, кодирования и декодирования кодами, обнаруживающими ошибки, существует запрос на разработку гибких программируемых однородных регистровых сред и замену ими узлов на базе одноразово программируемых логических матриц.

2) Теоретическим аппаратом, описывающим функционирование однородных регистровых сред, являются поля Галуа различной степени m $GF(2^m)$ с характеристикой p=2, позволяющие ввести и необходимые алгебры операций над элементами поля, проводимые в регистровой среде.

3) Ячейки однородных регистровых сред могут быть очень сложными по своей структуре, но формируются на базе простых элементов: D-триггеров, сумматоров по основанию 2, логических элементов И, ИЛИ, НЕ.

4) Структурно, однородные регистровые среды состоят из блока управления и настройки и регистрового блока из настраиваемых логических ячеек.

5) Многообразие выполняемых однородными регистровыми средами функций подразумевает разнообразие их схемотехнических реализаций.

ЛИТЕРАТУРА

1. Аладьев В.З. Однородные структуры. — Таллинн: Изд-во АН ЭССР, 1988
2. Блейхут Р. Теория и практика кодов, контролирующих ошибки. / Пер. с англ. под ред. К.Ш. Зигангирова. — М.: Мир, 1986
3. Кадиев И.П., Кадиев П.А. Однородные регистровые среды с программируемой структурой. Вестник Дагестанского государственного технического университета. Технические науки, 2014, № 4(35)
4. Кадиев П.А., Губа А.В., Кадиев И.П. Ячейка однородной среды. Патент РФ № 2059284. Бюл. № 12,1996.
5. Кадиев П.А., Губа А.В., Кадиев И.П. Ячейка однородной ветвящейся полиномиальной среды. Патент РФ № 2129297. Бюл. № 11,1999.
6. Угрюмов Е.П. Цифровая схемотехника. Учеб. пособие для вузов. Изд. 2. — СПб.: БХВ-Петербург, 2004. С. 357.
7. Амаева Д.К. Моделирование однородных регистровых сред с программируемой структурой. Доклад. ФГБОУ «Дагестанский государственный технический университет».
8. Кадиев П.А., Кадиев И.П. Однородные регистровые среды с программируемой структурой. Патент RU2449347C2, 2010.

Журнал «Современная наука: актуальные проблемы теории и практики»