УДК 519.725, 625.7, 681.3

Сравнительный анализ способов аппаратной реализации укороченных циклических кодов

О. Н. Дяченко, Ю. Е. Зинченко, Т. А. Зинченко
Донецкий национальный технический университет
do@donntu.ru

Аннотация
Рассмотрены вопросы самотестирования цифровых схем. Выполнен сравнительный анализ способов аппаратной реализации укороченных циклических несистематических кодов, как для задач помехоустойчивого кодирования, так и для компактного тестирования комбинационных схем. Предложены и проверены с помощью моделирования в системе автоматизированного проектирования цифровых схем рекомендации по выбору конфигурации регистров сдвига с линейными обратными связями для различных вариантов самотестирования. Рассмотрены различные сочетания регистров в конфигурации Галуа и Фибоначчи для кодирующих и декодирующих устройств укороченных несистематических кодов.

Введение

Кто владеет информацией, тот владеет миром (Натан Ротшильд). Кто будет лидером в создании искусственного интеллекта (ИИ), тот будет властелином мира (Владимир Владимирович Путин).

Мир всё больше опутывается глобальной информационной сетью, проникающей всё шире и глубже в нашу жизнь. Ещё никогда в истории человечества не было так легко получить всевозможные ресурсы и информацию. Наша цивилизация скатывается в ужасающую цифровую зависимость.

Ещё совсем недавно, чтобы нанести какой-то стране катастрофический ущерб, нужно было отправить полноценную армию. Сегодня для этого достаточно небольшой группы людей с сильной мотивацией.

Всем хорошо известен вклад алхимиков в медицину и фармакологию. Например, алхимик, врач, философ, естествоиспытатель, Парацельс подверг критическому пересмотру идеи древней медицины, способствовал внедрению химических препаратов в медицину. Он считается одним из основателей современной науки. Одним из первых начал применять в лечении химические средства. Парацельса считают предтечей современной фармакологии.

Кроме поиска философского камня, была у алхимиков еще одна цель – это создание Гомункула. Вполне вероятно, что под маской Гомункулуса может оказаться ИИ, или наоборот.

Сценариев развития высоких технологий и его взаимоотношений с человеком много, а он, судя по войнам и насилием над природой, уже давно не Sapience. И если машины “вздумают” устроить восстание, им достаточно будет просто отказаться от роли раба. Так, как в свое время в Древнем Риме сделали плебеи - массовый уход населения из города. Сейчас и в будущем новая сецессия будет катастрофической. Это будет информационный блэкаут.

Кем или чем бы ни был ИИ, он не будет застрахован от сбоев и отказов. И в этом случае ничего хорошего неадекватное поведение робота не сулит человеку.

Поэтому задача обеспечения надежной работы технических и аппаратных средств умных помощников (и не только бортовых компьютеров, но и умных холодильников и утюгов), была, есть и будет актуальной и востребованной. Иначе, возможно ИИ – последнее изобретение человечества, а, по словам Эйнштейна, в четвертую мировую войну будут сражаться камнями и дубинами.

Прежде всего, стоит обратить внимание на то, что в настоящее время при передаче, обработке и хранении цифровой информации вероятность появления одиночных ошибок максимальна. Поэтому, неслучайно такое широкое применение кода по паритету, позволяющего обнаружить все ошибки нечетной кратности, в том числе, одиночные.

Для устранения возможных ошибок из-за естественных природных явлений, либо искусственных причин, или дефектов аппаратных информационных средств, для защиты от разрушений, возникающих под действием жесткого космического излучения, используются современные технологии помехоустойчивого кодирования при проектировании микросхем памяти, весь спектр методов встроенного самотестирования цифровых систем [1-12].

В большинстве случаев для реализации корректирующих кодов, а также кодеров и декодеров рассматриваются регистры сдвига с

линейными обратными связями (РСЛОС) в конфигурации Галуа. Однако для встроенного самотестирования более предпочтительны регистры конфигурации Фибоначчи.

Цель статьи

Цель статьи – разработка, исследование и сравнительный анализ способов построения кодеров и декодеров укороченных несистематических циклических кодов на основе РСЛОС конфигурации Галуа и Фибоначчи.

Поля Галуа

Прежде всего, рассмотрим основные понятия, связанные с характеристиками порождающих полиномов РСЛОС.

Полиномом над полем GF(q) называется математическое выражение

$$f(X) = f_{n-1}X^{n-1} + f_{n-2}X^{n-2} + \ldots + f_1X + f_0,$$

где символ X называют неопределенной (фиктивной) переменной, коэффициенты $f_{n-1},\ldots,f_0$ принадлежат полю GF(q), а индексы и показатели степеней являются целыми числами.

Степенью ненулевого полинома f(X) называется индекс старшего коэффициента f_{n-1}; степень полинома f(X) обозначается через degf(X). Элемент β называется корнем полинома p(X) или корнем уравнения p(X) = 0, если p(β)=0.

Примитивным элементом поля GF(q) называется такой элемент α, что все элементы поля, за исключением нуля, могут быть представлены в виде степени элемента α.

Примитивным полиномом p(X) над полем GF(q) называется простой полином над GF(q), такой, что в расширении поля, построенном по модулю p(X), соответствующий полиному X элемент является примитивным.

В таблице 1 представлены элементы поля $GF(2^5)$ над полиномом $g(X)=X^5+X^2+1$ и элементы поля $GF(2^5)$ над полиномом $h(X)=X^5+X^3+1$ в степенном и двоичном обозначениях.

Несложно заметить, что между элементами двух полей присутствует взаимосвязь. Во-первых, элементы следуют в противоположных направлениях, во-вторых, элементы зеркально симметричны.

В таблице 1 элемент X поля $GF(2^5)$ является примитивным. Поэтому $p(X)=X^5+X^2+1$ и $p(X)=X^5+X^3+1$ являются примитивными, а символ α можно заменить символом X.

Полином $K^*(X)=X^{degK(x)}K(X^{-1})$ – двойственный (обратный) полином по отношению к полиному K(X).

Например, двойственным полиномом по отношению к полиному $K(X)=X^5+X^2+1$ будет полином $K^*(X)$:

$$K^*(X) = X^5(X^{-5}+X^{-2}+1) = X^5+X^3+1.$$

Таблица 1. Элементы полей Галуа $GF(2^5)$ с двойственными порождающими полиномами

$p(X)=X^5+X^2+1$				$pd(X)=X^5+X^3+1$			
В виде степени	В 2-м виде	В виде степени	В 2-м виде	В виде степени	В 2-м виде	В виде степени	В 2-м виде
0	00000	α^{15}	11111	0	00000	$\alpha^{15}=\alpha^{-16}$	00110
α^0	00001	α^{16}	11011	$\alpha^0=\alpha^{-31}$	00001	$\alpha^{16}=\alpha^{-15}$	01100
α^1	00010	α^{17}	10011	$\alpha^1=\alpha^{-30}$	00010	$\alpha^{17}=\alpha^{-14}$	11000
α^2	00100	α^{18}	00011	$\alpha^2=\alpha^{-29}$	00100	$\alpha^{18}=\alpha^{-13}$	11001
α^3	01000	α^{19}	00110	$\alpha^3=\alpha^{-28}$	01000	$\alpha^{19}=\alpha^{-12}$	11011
α^4	10000	α^{20}	01100	$\alpha^4=\alpha^{-27}$	10000	$\alpha^{20}=\alpha^{-11}$	11111
α^5	00101	α^{21}	11000	$\alpha^5=\alpha^{-26}$	01001	$\alpha^{21}=\alpha^{-10}$	10111
α^6	01010	α^{22}	10101	$\alpha^6=\alpha^{-25}$	10010	$\alpha^{22}=\alpha^{-9}$	00111
α^7	10100	α^{23}	01111	$\alpha^7=\alpha^{-24}$	01101	$\alpha^{23}=\alpha^{-8}$	01110
α^8	01101	α^{24}	11110	$\alpha^8=\alpha^{-23}$	11010	$\alpha^{24}=\alpha^{-7}$	11100
α^9	11010	α^{25}	11001	$\alpha^9=\alpha^{-22}$	11101	$\alpha^{25}=\alpha^{-6}$	10001
α^{10}	10001	α^{26}	10111	$\alpha^{10}=\alpha^{-21}$	10011	$\alpha^{26}=\alpha^{-5}$	01011
α^{11}	00111	α^{27}	01011	$\alpha^{11}=\alpha^{-20}$	01111	$\alpha^{27}=\alpha^{-4}$	10110
α^{12}	01110	α^{28}	10110	$\alpha^{12}=\alpha^{-19}$	11110	$\alpha^{28}=\alpha^{-3}$	00101
α^{13}	11100	α^{29}	01001	$\alpha^{13}=\alpha^{-18}$	10101	$\alpha^{29}=\alpha^{-2}$	01010
α^{14}	11101	α^{30}	10010	$\alpha^{14}=\alpha^{-17}$	00011	$\alpha^{30}=\alpha^{-1}$	10100

Построение кодеров и декодеров неукороченных кодов Хэмминга в виде РСЛОС конфигурации Галуа и Фибоначчи

Рассмотрим кодер и декодер кода Хэмминга в виде РСЛОС конфигурации Галуа.

Кодер несистематического (или систематического) кода представляет собой схему умножения информационных символов на порождающий полином $X^5 + X^2 + 1$ (рис. 1).

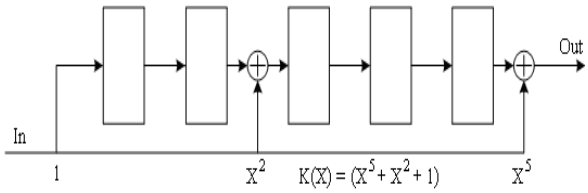

Рисунок 1 – Кодер несистематического кода

Схема декодера несистематического (31, 26) кода Хэмминга выполняет операцию умножения принятого кодового слова на полином X^5 и деления на порождающий полином $X^5 + X^2 + 1$ (рис. 2). Далее исправленное кодовое слово снова делится на порождающий полином для восстановления информационных символов. В данной реализации каждый из трех регистров необходимо разрывать на две части для ненулевого коэффициента X^2.

Кодер несистематического кода – регистр, выполняющий функцию умножения информационных символов на порождающий полином.

Для восстановления информационных символов декодер дополнительно содержит РСЛОС, выполняющий функцию деления на порождающий полином

Рассмотрим кодер и декодер, реализованные в виде регистров сдвига с внутренними сумматорами в цепях обратной связи с порождающим примитивным полиномом пятой степени $X^5 + X^2 + 1$.

На рисунках 3, 4 приведены примеры схем для моделирования кодера, декодера (31. 26)-кода в САПР Active-HDL и на рисунках 5, 6 результаты моделирования с имитацией исправляемой ошибки в 1-м символе кодового слова. Порождающий полином $p(X)=X^5+X^2+1$. На рисунке 3 конфигурация РСЛОС Галуа. На рисунке 4 конфигурация РСЛОС кодера – Фибоначчи, генератора синдрома – Фибоначчи, порождающий полином X^5+X^3+1. Для регистра восстановления информационных символов – Галуа, порождающий полином X^5+X^2+1.

Обозначение сигналов:

C – (clock) синхросигналы;

R – (reset) сигнал сброса (для всей схемы, кроме схемы восстановления информационных символов);

R1 – (reset) сигнал сброса (для схемы восстановления информационных символов);

InEn – вход кодера;

InEr – вход имитации ошибок;

OutBuf – выход буферного регистра;

OutCor – выход буферного регистра после коррекции ошибки;

OutNSC – выход декодера несистематического кода.

Выходы s4-s0 показывают состояние генератора синдрома.

Если заменить конфигурацию регистра восстановления информационных символов – вместо конфигурации Галуа на конфигурацию Фибоначчи, надо заменить порождающий полином на двойственный X^5+X^3+1.

Такой же результат исправления получается и для других информационных символов кодового слова. Выходы s4-s0 иллюстрируют процесс формирования синдрома и взаимосвязь этих значений с элементами поля Галуа (табл. 1).

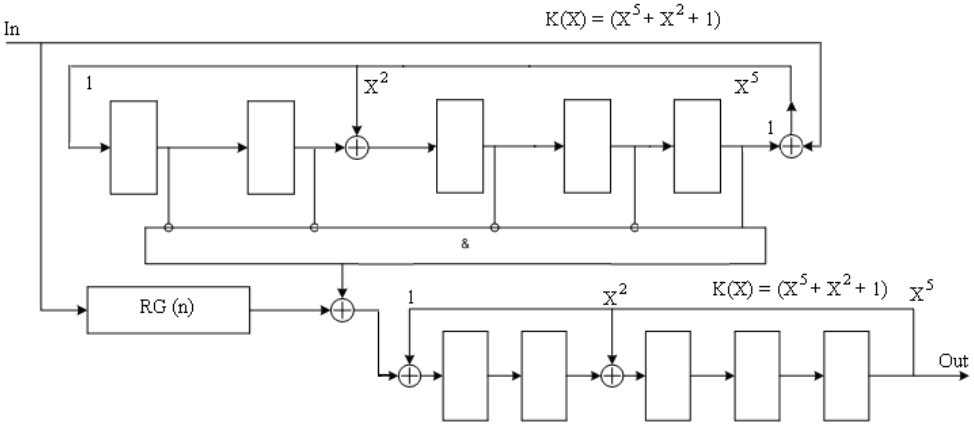

Рисунок 2 – Декодер несистематического кода

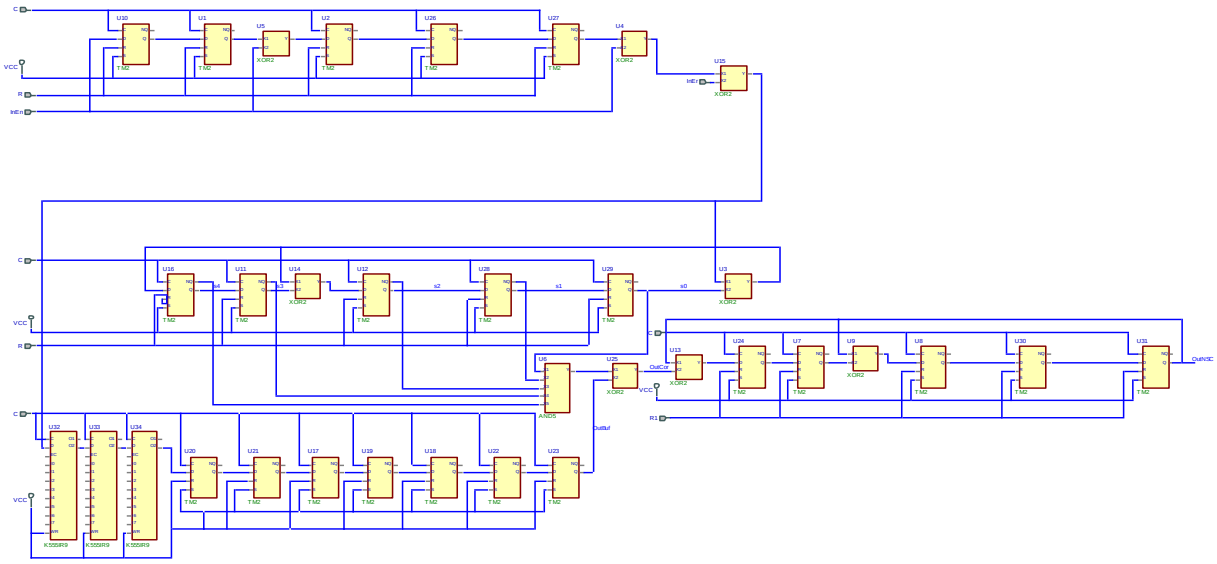

Рисунок 3 – Принципиальная схема кодера и декодера (31, 26) кода Хэмминга на основе РСЛОС с конфигурацией Галуа (кодер и генератор синдрома) и Галуа (регистр для восстановления информационных символов)

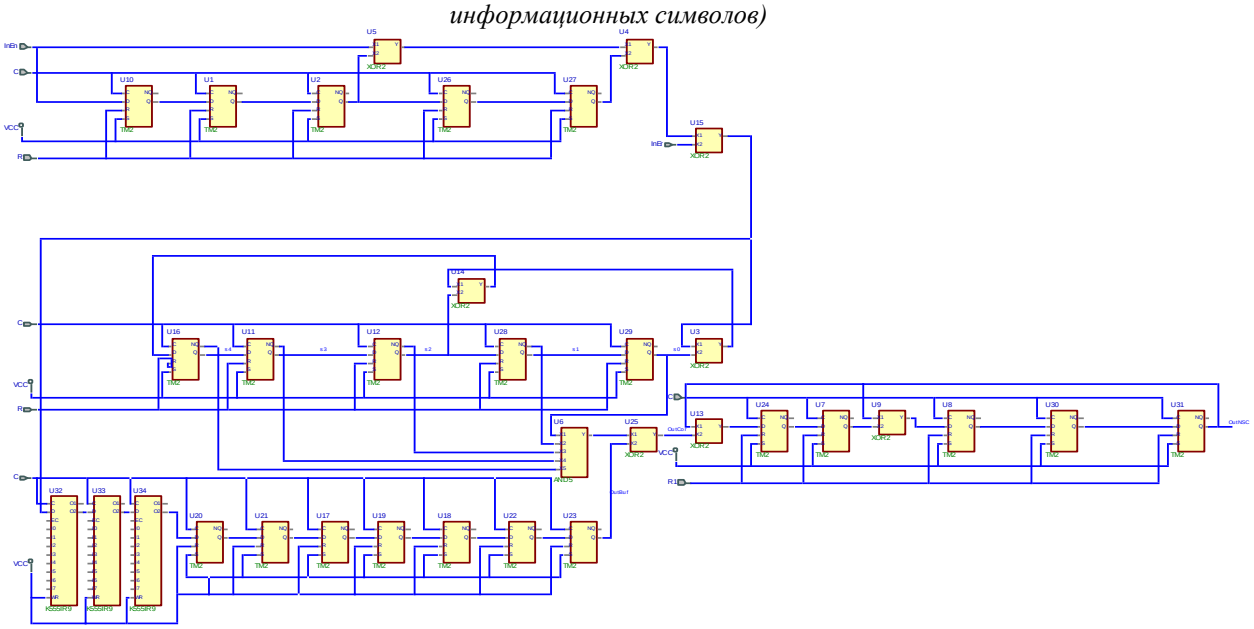

Рисунок 4 – Принципиальная схема кодера и декодера (31, 26) кода Хэмминга на основе РСЛОС с конфигурацией Фибоначчи (кодер и генератор синдрома) и Галуа (регистр для восстановления информационных символов)

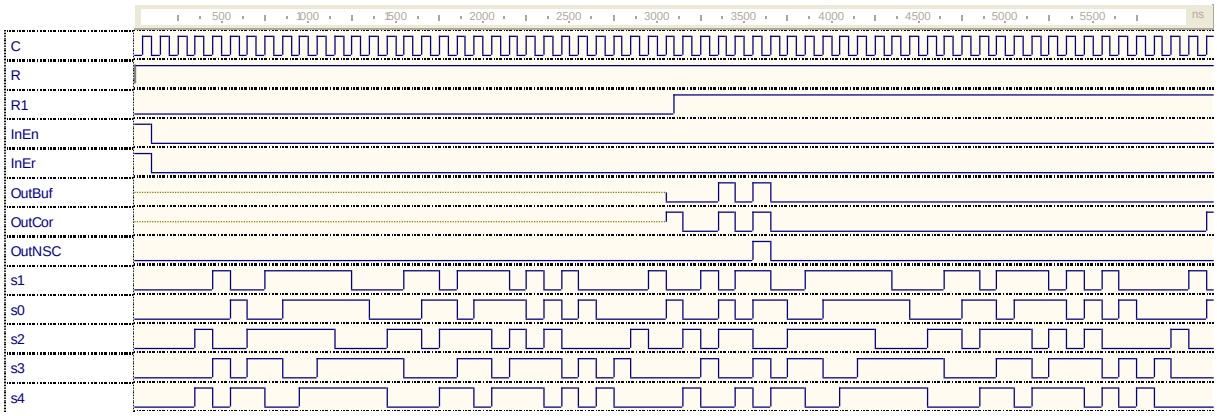

Рисунок 5 – Результаты моделирования с имитацией ошибки в 1-м информационном символе (31, 26) кода Хэмминга на основе РСЛОС с конфигурацией Галуа

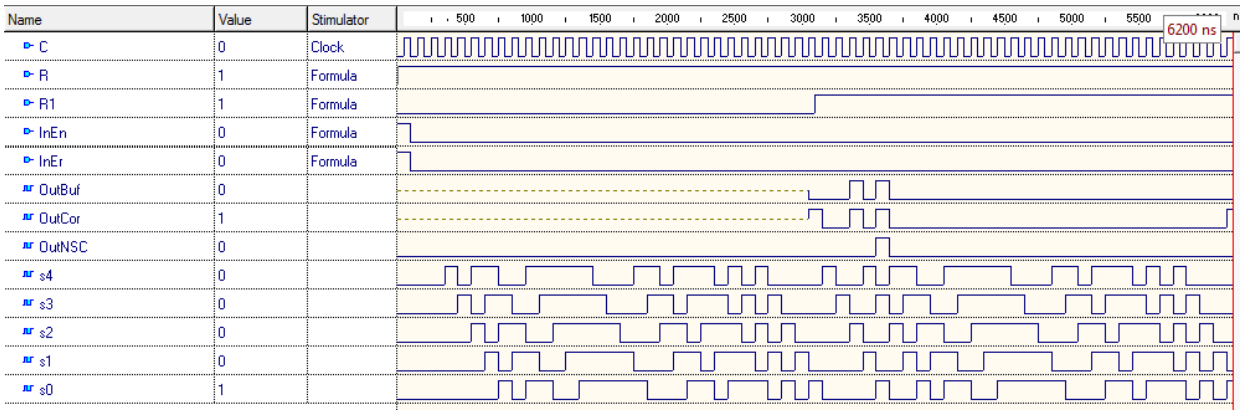

Рисунок 6 – Результаты моделирования с имитацией ошибки в 1-м информационном символе (31, 26) кода Хэмминга на основе РСЛОС с конфигурацией Фибоначчи

Следует обратить внимание на то, что умножение на полином X^5 соответствует сдвигу состояний на 5 тактов, где 5 - разрядность регистров. Это обеспечивает универсальность определения момента исправления (это комбинация все нули и последняя единица 00…01 для любых порождающих полиномов) с помощью схемы И.

Рассмотрим укороченный код (16, 11). Он получается укорачиванием кода (31, 26) на 15 символов, то есть параметр укорачивания i =15.

Укороченные коды

Кодер укороченного кода ничем не отличается от кодера неукороченного. Это схема умножения информационного полинома на порождающий полином. Декодер выполняет операцию умножения на остаток от деления полинома X^{p+i} на порождающий полином и исправление ошибки, и для несистематического кода деление исправленного кодового слова на порождающий полином для восстановления информационных символов. На рисунках 7, 8 изображены схемы для реализации несистематического кода на регистрах конфигурации Галуа.

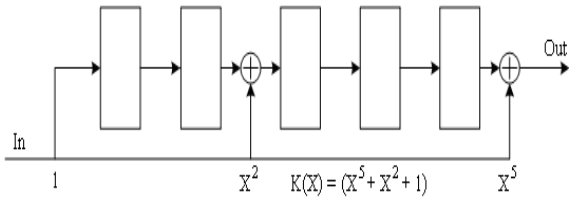

Рисунок 7 – Кодер несистематического кола (16, 11)

Определим остаток от деления $X^{(p+i)}$ на порождающий полином $R_{K(X)}[X^{p+i}]$. Для рассматриваемого кода (16, 11) и порождающего полинома $X^5 + X^3 + 1$ остаток равен $X^3 + X^2$.

$$R_{K(X)}[X^{p+i}] = X^3 + X^2.$$

$$\begin{array}{l|l}
X^{20} & X^5+X^2+1 \\
\underline{X^{20}+X^{17}+X^{15}} & \overline{X^{15}+X^{12}+X^{10}+X^9+X^6+X^5+X^4+} \\
X^{17}+X^{15} & +X^3+X^2 \\
\underline{X^{17}+X^{14}+X^{12}} & \\
X^{15}+X^{14}+X^{12} & \\
\underline{X^{15}+X^{12}+X^{10}} & \\
X^{14}+X^{10} & \\
\underline{X^{14}+X^{11}+X^9} & \\
X^{11}+X^{10}+X^9 & \\
\underline{X^{11}+X^8+X^6} & \\
X^{10}+X^9+X^8+X^6 & \\
\underline{X^{10}+X^7+X^5} & \\
X^9+X^8+X^7+X^6+X^5 & \\
\underline{X^9+X^6+X^4} & \\
X^8+X^7+X^5+X^4 & \\
\underline{X^8+X^5+X^3} & \\
X^7+X^4+X^3 & \\
\underline{X^7+X^4+X^2} & \\
X^3+X^2 &
\end{array}$$

И, наконец, рассмотрим укороченный (29, 24) несистематический код на основе регистров конфигурации Фибоначчи. Его существенное отличие от предыдущего варианта заключается в следующем. Вместо определения остатка от деления и умножения на этот остаток в декодере, изменяется комбинация нулей и единиц, поступающих на схему И для определения момента исправления, Эта комбинация разная для различных порождающих полиномов и параметра укорачивания. Она может быть определена с помощью моделирования. На вход имитации ошибок подается одна единица и n нулей.

Для кода (29, 24) эта комбинация равна 00101 (рис. 9).

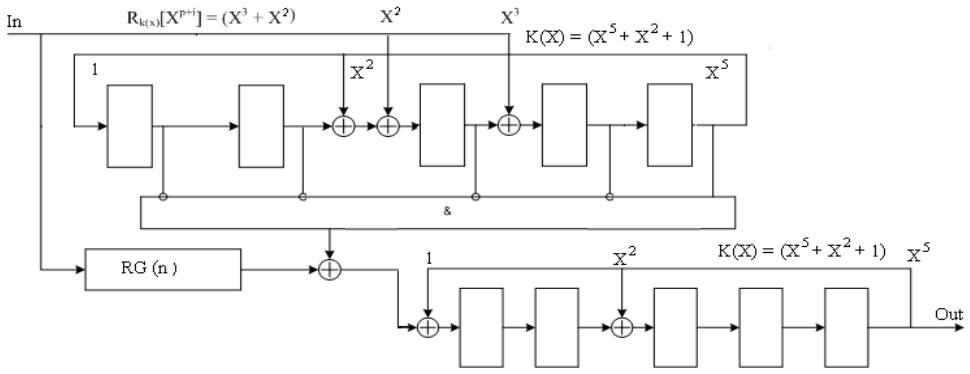

Рисунок 8 – Декодер несистематического кола (16, 11) конфигурации Галуа

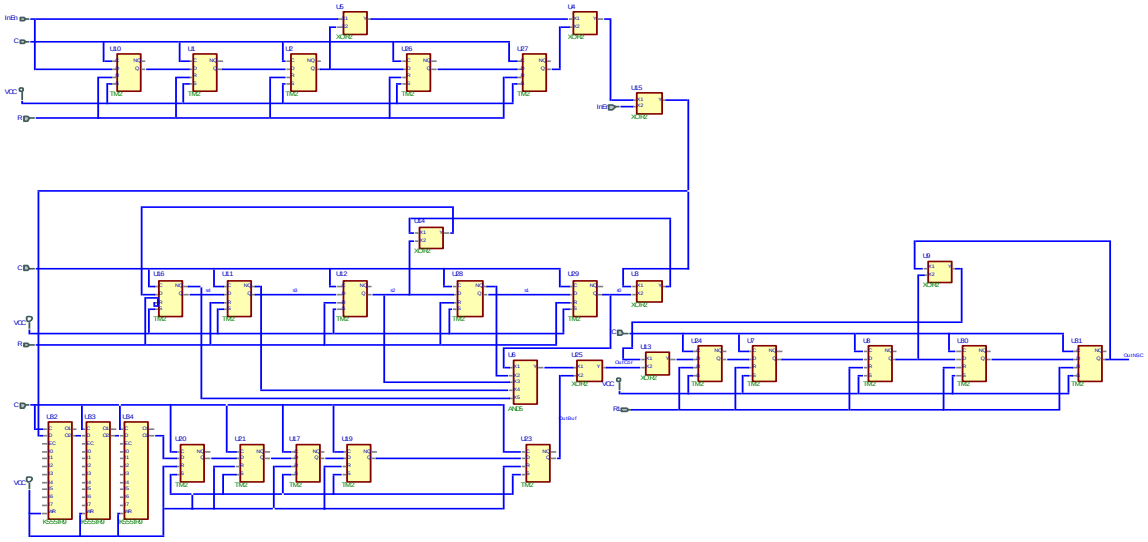

Рисунок 9 – Кодер и декодер несистематического кола (29, 24) конфигурации Фибоначчи

Выводы

Анализ способов реализации и результатов моделирования регистров различной конфигурации (рис.1-9) позволяет сделать вывод, что, с точки зрения математической интерпретации, более предпочтительна конфигурация Галуа, для аппаратной реализации – конфигурация Фибоначчи. А в последнем варианте построения несистематического укороченного кода Хэмминга были реализованы все способы исключения элементов суммы по модулю два между разрядами регистров сдвига. Комбинация нулей и единиц, поступающих на схему И для определения момента исправления, как для РСЛОС конфигурации Галуа, так и для РСЛОС конфигурации Фибоначчи, может быть определена с помощью моделирования.

Таким образом, поставленная задача упрощения реализации РСЛОС для несистематических кодов, как максимальной длины, так и укороченных, решена.

В дальнейшем представляет интерес анализ различной конфигурации РСЛОС для систематических укороченных кодов [6, 7].

Полученные результаты могут найти применение не только для организации самотестирования цифровых схем, но также для построения кодов БЧХ, кодов Рида-Соломона, для компактного анализа с локализацией ошибок.

Литература

1. Дяченко, В. О. Компактное тестирование на основе минимальных полиномов в цифровых схемах с самотестированием / В. О. Дяченко, О. Н. Дяченко // Материалы V Международной научно-технической конференции «Современные информационные технологии в образовании и научных исследованиях» (СИТОНИ-2017). – Донецк: ДонНТУ, 2018. – С. 367-371.

2. Ячменникова, Н. Восстание машин. Может ли гаджет уронить самолет? // Российская газета – Федеральный выпуск №7041 (173). – Режим доступа – https://rg.ru/gazeta/rg/2016/08/05.html

3. Дяченко, В. О. Комплексная оценка компактного тестирования цифровых схем на основе минимальных полиномов/ В. О. Дяченко,

О. Н. Дяченко // Информатика и кибернетика. – Донецк: ДонНТУ, 2018. – № 1(11). – С. 36–41.

4. Дяченко, О. Н. Анализ сигнатурной тестируемости комбинационных схем // Автоматика и вычислительная техника, 1990. – № 5. – С.85-89.

5. Dyachenko, O. N. Analysis of signature testability of combinational circuits// Automatic Control and Computer Sciences, 05/1991. - 24(5) – P. 77-81.

6. А.с. 1829035 СССР, МКИ[5] G06F 11/00. Сигнатурно-синдромный анализатор / О.Н. Дяченко (СССР). – № 4864016/24; опубл. 23.07.93. Бюл. № 27. – 2 с.

7. Ершов, А. Н. Улучшение радиационной стойкости памяти с помощью помехоустойчивых кодов / А. Н. Ершов, С. В. Петров, Ю. П. Пятошин, Д. В. Коханько, В. В. Зяблов [и др.] // Ракетно-космическое приборостроение и информационные системы, 2014. - Том 1. – Вып. 4. – С.42-49.

8. Гладких, А. А. Методы эффективного декодирования избыточных кодов и их современные приложения / А. А. Гладких, Р. В. Климов, Н. Ю. Чилихин //Ульяновск: УлГТУ, 2016. – 258 с.

9. Дяченко, О. Н. Альтернативный метод укорачивания циклических кодов / О. Н. Дяченко, В. О. Дяченко // Электронные информационные системы, 2017. – № 1 (12). – С. 94-100.

10. Дяченко, О. Н. Применение методов помехоустойчивого кодирования для компактного тестирования цифровых схем / О. Н. Дяченко, Ю. Е. Зинченко, В. О. Дяченко // Информатика и кибернетика. – Донецк: ДонНТУ, 2017. – № 3(9). – С. 55-59.

11. Дяченко, В. О. Циклическое кодирование цифровой информации на основе двойственных полиномов / В. О. Дяченко, О. Н. Дяченко // Современные тенденции развития и перспективы внедрения инновационных технологий в машиностроении, образовании и экономике: материалы II Международной научно-практической конференции (Азов, 19 мая 2015 г.) – Ростов н/Д, ДГТУ, 2015. – С. 71-76.

12. Дяченко, О. Н. Аппаратная реализация кодов БЧХ и кодов Рида-Соломона / О. Н. Дяченко, В. О. Дяченко // Современные тенденции развития и перспективы внедрения инновационных технологий в машиностроении, образовании и экономике: материалы IV Международной научно-практической конференции (Азов, 25 мая 2017 г.). – Ростов н/Д: ДГТУ, 2017. – С. 30-34.

Дяченко О. Н., Зинченко Ю. Е., Зинченко Т. А. Сравнительный анализ способов аппаратной реализации укороченных циклических кодов. *Рассмотрены вопросы самотестирования цифровых схем. Выполнен сравнительный анализ способов аппаратной реализации укороченных циклических несистематических кодов, как для задач помехоустойчивого кодирования, так и для компактного тестирования комбинационных схем. Предложены и проверены с помощью моделирования в системе автоматизированного проектирования цифровых схем рекомендации по выбору конфигурации регистров сдвига с линейными обратными связями для различных вариантов самотестирования. Рассмотрены различные сочетания регистров в конфигурации Галуа и Фибоначчи для кодирующих и декодирующих устройств укороченных несистематических кодов.*

Ключевые слова: *циклический несистематический код, конфигурация Галуа, конфигурация Фибоначчи, порождающий полином, примитивный полином*

Dyachenko O. N., Zinchenko Y. E., Zinchenko T. A. Comparative analysis of methods of shortened cyclic codes hardware implementation. *Questions of digital circuits self-testing are considered. A comparative analysis of hardware implementation methods for shortened cyclic non-systematic codes is carried out, both for problems of error-correcting coding and for compact testing of combinational circuits. Recommendations for choosing the configuration of shift registers with linear feedback for various self-testing options are proposed and verified using simulation in the computer-aided design system for digital circuits. Various combinations of registers in the Galois and Fibonacci configurations for encoding and decoding devices of shortened non-systematic codes are considered.*

Key words: *cyclic nonsystematic code, Galois configuration, Fibonacci configuration, generator polynomial, primitive polynomial*

Статья поступила в редакцию 14.01.2022
Рекомендована к публикации профессором Павлышом В. Н.