УДК _____

№ госрегистрации _____

Инв. №_____

УТВЕРЖДАЮ

_____

головной исполнитель

_____ _____

«_____» _____ 2021 г.

МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ "ТЕОРИЯ ПСЕВДОСЛУЧАЙНЫХ ГЕНЕРАТОРОВ"

Разбор практических задач с теоретическим обоснованием

по теме:

Типовые задачи контрольных работ

(промежуточный)

Преподаватель дисциплины _____ М.И. Рожков

Руководитель создания документа _____ А.Ю. Нестеренко

Москва 2021

СПИСОК ИСПОЛНИТЕЛЕЙ

Выполнил студент _____ Щеглова П.Н.

СОДЕРЖАНИЕ

Определения, обозначения и сокращения 4
Обозначения и сокращения 4
Определения 5
Введение 6
Сборка документа 7
1 Задачи контрольных работ №1,2 8
1.1 Разбор примеров задач общих для двух контрольных 8
1.1.1 Задача 1 8
1.1.2 Задача 2 11
1.1.3 Задача 3 12
1.1.4 Задача 4 16
1.1.5 Задача 5 16
1.1.6 Задача 6 19
1.2 Задачи из контрольной работы №1 21
1.2.1 Задача 7 21
1.2.2 Задача 8 23
1.2.3 Задача 9 27
1.2.4 Задача 10 27
1.3 Задачи из контрольной работы №2 31
1.3.1 Задача 7 31
1.3.2 Задача 8 32
1.3.3 Задача 9 33
1.3.4 Задача 10 35
Список использованных источников 37

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящих методических материалах применят следующие термины с соответствующими определениями и сокращениями (взяты на основе [1])

Обозначения и сокращения

ЛРП	линейная рекуррентная последовательность	нумерованная последовательность элементов поля, таких что, начиная с некоторого элемента последовательности a_m, каждый следующий представим в виде линейной комбинации m предыдущих $(a_0, a_1, ..., a_{m-1})$, причем коэффициенты - константы из данного поля;
х.м.	характеристический многочлен или характеристическая функция	функция, задающая зависимость нового элемента последовательности от предыдущих.

Определения

вектор начального состояния	вектор первых элементов последовательности, независимых друг от друга, на основе которых вырабатываются последующие элементы ЛРП;
минимальный многочлен	многочлен минимальной степени, задающий данную ЛРП;
минимальный период ЛРП	минимальное число первых элементов последовательности, после которых новые элементы полностью повторяются в том же порядке;
примитивный многочлен	неприводимый многочлен степени m с периодом $q^m - 1$;
ЛРП максимального периода	ЛРП, у которой х.м. примитивный.

ВВЕДЕНИЕ

Целью работы является демонстрация навыков подготовки электронных документов в системе компьютерной верстки документов latex. Выполнены требования к подготавливаемому документу:

— титульный лист по ГОСТ 7.32-2001;

— общий объем документа не менее 18 страниц;

— наличие разделов документа, включая ненумерованные (введение, обозначения и т.п.);

— наличие формул (строчные и выключенные);

— наличие ссылок (по документу и внешних);

— наличие таблиц, изображений и т.п.;

— наличие списка литературы и ссылок на него по тексту документа;

— определение собственных команд, упрощающих процесс набора документа,

— отсутствие орфографических ошибок, наличие смысла в подготовленном документе, обоснование, для чего документ подготовлен;

— краткая информация о сборке документа и используемых шрифтах, размерах (шрифтов, полей и т.п.);

— информация о том, какие стилевые пакеты применяли и для какой цели.

Содержательно документ подготовлен для демонстрации студентам, проходящим курс теории псевдослучайных генераторов, хода решения типовых задач из контрольноых работ, для некоторых типов задач приведено решение для всех вариантов входных параметров. Первыми разбираются общие задачи для двух контрольных, затем уникальные для первой контрольной задачи и для второй. Теоретические обоснования даны в виде ссылок на соответствующие утверждения из источников и частично продублированы в виде утверждений.

СБОРКА ДОКУМЕНТА

Шаблон ГОСТ 7.32-2001 найден на просторах сети и частично отредактирован (убраны ненужные файлы и команды, обновлены комментарии к командам, изменены названия на нужные). Для компиляции используются pdflatex и bibtex. На сборочном компьютере установлен texlive-full. Стиль и язык - utf8x, 14pt, прочие настройки взяты из шаблонного файла G7-32.cls. Остальные стандартные настройки убраны в preamble.inc.tex. (шаблонный, но также измененный). Стиль титульного листа и заголовки, как и введение с источниками - отдельные подключаемые файлы.

1 Задачи контрольных работ №1,2

1.1 Разбор примеров задач общих для двух контрольных

1.1.1 Задача 1

Найти минимальный многочлен $m(x)$ для ЛРП с х.м. $f(x) \in \{x^5+x+1, x^5+x^4+1, x^5+x^2+1, x^5+x^3+1\} \in F_2[x]$ и вектором начального состояния:

$$s(0) \in \{(11111), (11011), (11101), (11100), (10110), (00001), (00011), (00111), (01111)\}$$

По утверждению 1.6.2 из [2] любой характеристический многочлен ЛРП кратен минимальному многочлену. Тогда достаточно проверить делители характеристической функции.

а) x^5+x+1

Так как корней нет (0 или 1 не подходят), делители следует искать среди многочленов степени 2,3, причем неприводимых. Таких 2 степени в нашем поле только одно - $1+x+x^2$, проверим делимость простым делением уголком - остаток от деления равен 0, получаем, что $f(x) = (x^2+x+1)(x^3+x^2+1)$. x^3+x^2+1 - в свою очередь не имеет корней и не делится на $1+x+x^2$, а значит неприводим. Так как ЛРП ненулевая (начальный вектор ненулевой), делитель 1 также не является минимальным многочленом по определению. Следовательно минимальный многочлен $m(x) \in \{x^2+x+1, x^3+x^2+1, x^5+x+1\}$.

Проверим многочлен (x^2+x+1): многочлен показывает, что каждое следующее число последовательности получается из двух предыдущих как линейная комбинация с коэффициентами как в многочлене, то есть если первые числа последовательности 1,1, то ЛРП соответствует вектору начального состояния $(1,1,0,1,1)$, если первые числа последовательности 0,1, то $(0,1,1,0,1)$, и по такому же принципу подходит вектор начального состояния (1,0,1,1,0). Таким образом, для полученных векторов $m(x) = (x^2+x+1)$. (P.S. теория говорит нам, что проверять совпадение последовательности необходимо и достаточно лишь в начальном векторе,

далее последовательность будет вычисляться в соответствии с характеристической функцией, минимальный многочлен должен подходить указанным образом и иметь минимальную степень среди претендентов, поэтому оставшиеся многочлены-претенденты не подходят).

Проверим многочлен (x^3+x^2+1): многочлен показывает, что каждое следующее число последовательности получается из трех предыдущих как линейная комбинация с коэффициентами как в многочлене, то есть в нашем случае сумма первого и третьего задает четвертое, тогда если первые числа последовательности 1,1,1, то ЛРП соответствует вектору начального состояния $(1,1,1,0,1)$, если первые числа последовательности 1,1,0, то $(1,1,0,1,0)$, и по такому же принципу подходят вектора начального состояния (1,0,1,0,0), (1,0,0,1,1), (0,1,1,1,0), (0,1,0,0,1), (0,0,1,1,1). Таким образом, для полученных векторов $m(x) = (x^3+x^2+1)$.

Для всех остальных состояний кроме (0,0,0,0,0), минимальный многочлен будет совпадать с характеристической функцией.

б) x^5+x^4+1

Так как корней нет (0 или 1 не подходят), делители следует искать среди многочленов степени 2,3, причем неприводимых. Таких 2 степени в нашем поле только одно - $1+x+x^2$, проверим делимость простым делением уголком - остаток от деления равен 0, получаем, что $f(x) = (x^2+x+1)(x^3+x+1)$. x^3+x+1 - в свою очередь не имеет корней и не делится на $1+x+x^2$, а значит неприводим. Так как ЛРП ненулевая (начальный вектор ненулевой), делитель 1 также не является минимальным многочленом по определению. Следовательно минимальный многочлен $m(x) \in \{x^2+x+1, x^3+x+1, x^5+x^4+1\}$.

Проверим многочлен (x^2+x+1): многочлен показывает, что каждое следующее число последовательности получается из двух предыдущих как линейная комбинация с коэффициентами как в многочлене, то есть если первые числа последовательности 1,1, то ЛРП соответствует вектору начального состояния $(1,1,0,1,1)$, если первые числа последовательности 0,1, то $(0,1,1,0,1)$, и по такому же принципу подходит вектор начального

состояния (1,0,1,1,0). Таким образом, для полученных векторов $m(x) = (x^2 + x + 1)$.

Проверим многочлен $(x^3 + x + 1)$: многочлен показывает, что каждое следующее число последовательности получается из трех предыдущих как линейная комбинация с коэффициентами как в многочлене, то есть в нашем случае сумма первого и второго задает четвертое, тогда если первые числа последовательности 1,1,1, то ЛРП соответствует вектору начального состояния $(1, 1, 1, 0, 0)$, если первые числа последовательности 1,1,0, то $(1, 1, 0, 0, 1)$, и по такому же принципу подходят вектора начального состояния (1,0,1,1,1), (1,0,0,1,0), (0,1,1,1,0), (0,1,0,1,1), (0,0,1,0,1). Таким образом, для полученных векторов $m(x) = (x^3 + x + 1)$.

Для всех остальных состояний кроме (0,0,0,0,0), минимальный многочлен будет совпадать с характеристической функцией.

в) $x^5 + x^2 + 1$

Так как корней нет (0 или 1 не подходят), делители следует искать среди многочленов степени 2,3, причем неприводимых. Таких 2 степени в нашем поле только одно - $1+x+x^2$, проверим делимость простым делением уголком - остаток от деления равен 1, получаем, что $f(x)$ неприводим. Так как ЛРП ненулевая (начальный вектор ненулевой), делитель 1 также не является минимальным многочленом по определению. Следовательно минимальный многочлен $m(x) = x^5 + x^4 + 1$ для любого ненулевого начального вектора.

г) $x^5 + x^3 + 1$

Так как корней нет (0 или 1 не подходят), делители следует искать среди многочленов степени 2,3, причем неприводимых. Таких 2 степени в нашем поле только одно - $1+x+x^2$, проверим делимость простым делением уголком - остаток от деления равен $x+1$, получаем, что $f(x)$ неприводим. Так как ЛРП ненулевая (начальный вектор ненулевой), делитель 1 также не является минимальным многочленом по определению. Следовательно минимальный многочлен $m(x) = x^5 + x^4 + 1$ для любого ненулевого начального вектора.

1.1.2 Задача 2

Для каких $m(x) \in \{m_1(x) = x^2+x+1, m_2(x) = x^3+x+1, m_3(x) = x^3+x^2+1, m_4(x) = x+1\}$ в семействе $S(f)$, $f(x) \in \{x^5+x+1, x^5+x^4+1, x^4+x^2+1, x^4+1, x^3+1\}$, $f \in F_2[x]$, существует ЛРП, минимальный многочлен которой равен $m(x)$?

Если многочлен является неприводимым делителем функции f из семейства $S(f)$, то в этом семействе обязательно найдется ЛРП, для которой данный многочлен является минимальным [2].

а) $f(x) = x^5 + x + 1$

Так как корней нет (0 или 1 не подходят), делители следует искать среди многочленов степени 2,3, причем неприводимых. Таких 2 степени в нашем поле только одно - $1 + x + x^2$, проверим делимость простым делением уголком - остаток от деления равен 0, получаем, что $f(x) = (x^2 + x + 1)(x^3 + x^2 + 1)$. $x^3 + x^2 + 1$ - в свою очередь не имеет корней и не делится на $1 + x + x^2$, а значит неприводим. Тогда для многочленов $m_1(x) = x^2 + x + 1, m_3(x) = x^3 + x^2 + 1$ существуют ЛРП из данного семейства, для которых они являются минимальным. Например, см. а.

б) $f(x) = x^5 + x^4 + 1$

Так как корней нет (0 или 1 не подходят), делители следует искать среди многочленов степени 2,3, причем неприводимых. Таких 2 степени в нашем поле только одно - $1 + x + x^2$, проверим делимость простым делением уголком - остаток от деления равен 0, получаем, что $f(x) = (x^2 + x + 1)(x^3 + x + 1)$. $x^3 + x + 1$ - в свою очередь не имеет корней и не делится на $1 + x + x^2$, а значит неприводим. Тогда для многочленов $m_1(x) = x^2 + x + 1, m_2(x) = x^3 + x + 1$ существуют ЛРП из данного семейства, для которых они являются минимальным. Например, см. б.

в) $f(x) = x^4 + x^2 + 1$ Так как корней нет (0 или 1 не подходят), делители следует искать среди многочленов степени 2, причем неприводимых. Таких 2 степени в нашем поле только одно - $1 + x + x^2$, проверим делимость простым делением уголком - остаток от деления равен 0, по-

лучаем, что $f(x) = x^4 + x^2 + 1 = (x^2 + x + 1)^2$. Тогда для многочлена $m_1(x) = x^2 + x + 1$ существуют ЛРП из данного семейства, для которых он является минимальным. Например, см. а или б.

г) $f(x) = x^4 + 1$ $f(x)$ приводим (корень 1): $(x + 1)^4$. Тогда для многочлена $m_4(x) = x + 1$ существуют ЛРП из данного семейства, для которых он является минимальным.

д) $f(x) = x^3 + 1$ $f(x)$ приводим (корень 1): $(x + 1)(x^2 + x + 1)$. Тогда для многочлена $m_1(x) = x^2 + x + 1, m_4(x) = x + 1$ существуют ЛРП из данного семейства, для которых он является минимальным.

1.1.3 Задача 3

Для каких $r \in \{1,2,3,\ldots,30\}$ в семействе $S(f)$ ЛРП с х.м. $f(x) \in \{(x^2 + x + 1)^8, (x + 1)^{10}, (x^3 + x + 1)^4, (x^2 + x + 1)^2(x + 1)^4, (x + 1)^{12}, (x^3 + x^2 + 1)^3\}, f \in F_2[x]$, существует ЛРП с минимальным периодом, равным r?

Минимальный период ЛРП равен периоду его минимального многочлена [2], следовательно достаточно для каждой х.м. вычислить периоды всех ее делителей:

а) $(x^2 + x + 1)^8$, его делитель, многочлен $x^2 + x + 1$ не имеет корней и неприводим, период делителя находим из Теоремы 2.6 из [2] $r = 2^2 - 1 = 3$, так как делитель этого числа 1 - не подходит, в связи с тем, что период многочлена степени выше 1 должен быть больше 1, то период равен 3. Далее, находим наименьшее такое t, что $2^t \geqslant 8$, $t = 3$. По Случаю 2 из Теоремы 2.6 из [2] период ненулевой последовательности из $S(f)$ будет лежать в множестве $\{3, 6, 12, 24\}$. Тогда, так как для любого делителя х.м. в семействе ЛРП найдется такая, для которой он будет минимальным многочленом (Теорема 2.1 из [2]), тогда для всех представленных в множестве вариантов найдется такая ЛРП, для которой минимальный период принадлежит множеству $r \in \{1,3,6,12,24\}$.

$x^3(\mod x^2 + x + 1) = (x + 1)x = x^2 + x = 1, r = 3$

$x^3(\mod (x^2+x+1)^2) = x^3 \neq 1$

$x^6(\mod (x^2+x+1)^2 = x^4+x^2+1) = (x^2+1)x^2 = x^4+x^2 = 1, r = 6$

$x^3(\mod (x^2+x+1)^3) = x^3 \neq 1$

$x^6(\mod (x^2+x+1)^3 = 1+x+x^3+x^5+x^6) = 1+x+x^3+x^5 \neq 1$, тогда $r = 12$

$x^{12}(\mod (x^2+x+1)^8) = x^{12} \mod 1+x^8+x^{16} = x^{12} \neq 1$

$x^{24} \mod 1+x^8+x^{16} = (1+x^8)x^8 = x^8+x^{16} = 1, r = 24$

б) $(x+1)^{10}$, его делитель - многочлен $x+1$ не имеет корней и неприводим, его период $r = 2^1 - 1 = 1$. Находим наименьшее такое t, что $2^t \geqslant 10$, $t = 4$. В этом случае период ненулевой последовательности из $S(f)$ будет лежать в множестве $\{1, 2, 4, 8, 16\}$. Тогда, так как для любого делителя х.м. в семействе ЛРП найдется такая, для которой он будет минимальным многочленом, тогда для всех представленных в множестве вариантов найдется такая ЛРП, для которой минимальный период принадлежит множеству $r \in \{1, 2, 4, 8, 16\}$.

$x^1 \mod x+1 = 1, r = 1$

$x^2 \mod x^2+1 = 1, r = 2$

$x^4 \mod x^3+x^2+x+1 = (x^2+x+1)x = 1, r = 4$

$x^8 \mod x^4+1 = 1, r = 8$

$x^8 \mod x^{10}+x^8+x^2+1 = x^8 \neq 1$

$x^{16} \mod x^{10}+x^8+x^2+1 = (x^8+x^2+1)x^6 = x^{14}+x^8+x^6 = (x^8+x^2+1)x^4+x^8+x^6 = x^{12}+x^8+x^4 = (x^8+x^2+1)x^2+x^8+x^4 = x^{10}+x^8+x^2 = 1, r = 16$

в) $(x^3+x+1)^4$, его делитель - многочлен x^3+x+1 не имеет корней и неприводим, его период $r = 2^3 - 1 = 7$, так как делитель этого числа 1 - не подходит, в связи с тем, что период многочлена степени выше 1 должен быть больше 1, то период равен 7. Далее находим наименьшее такое t, что $2^t \geqslant 4$, $t = 2$. В этом случае период ненулевой последовательности из $S(f)$ будет лежать в множестве $\{7, 14, 28\}$. Тогда, так как для любого делителя

х.м. в семействе ЛРП найдется такая, для которой он будет минимальным многочленом, тогда для всех представленных в множестве вариантов найдется такая ЛРП, для которой минимальный период принадлежит множеству $r \in \{1, 7, 14, 28\}$.

$$x^7 \mod x^3 + x + 1 = (x+1)(x+1)x = x^3 + x = 1, r = 7$$

$$x^7 \mod (x^3 + x + 1)^2 = x^7 \mod 1 + x^2 + x^6 = x + x^3 \neq 1$$

$$x^{14} \mod 1 + x^2 + x^6 = (1 + x^2)^2 x^2 = x^2 + x^6 = 1, r = 14$$

$x^{14} \mod (x^3 + x + 1)^4 = x^{14} \mod 1 + x^4 + x^{12} = (1 + x^4)x^2 = x^2 + x^6 \neq 1$

$x^{28} \mod (x^3 + x + 1)^4 = x^{28} \mod 1 + x^4 + x^{12} = (1 + x^4)^2 x^4 = (1 + x^8)x^4 = x^4 + x^{12} = 1, r = 28$

г) $(x^2 + x + 1)^2 (x + 1)^4$, его делитель - многочлен $x^2 + x + 1$ не имеет корней и неприводим, его период $r = 2^2 - 1 = 3$, так как делитель этого числа 1 - не подходит, в связи с тем, что период многочлена степени выше 1 должен быть больше 1, то период равен 3; его делитель, многочлен $x+1$ не имеет корней и неприводим, его период $r = 2^1 - 1 = 1$. Далее, наименьшее такое t, что $2^t \geqslant 2$, $t = 1$, наименьшее такое t, что $2^t \geqslant 4$, $t = 2$. В этом случае период ненулевой последовательности из $S(f)$ будет лежать в множестве $\{3, 6; 1, 2, 4; 12\}$. Тогда, так как для любого делителя х.м. в семействе ЛРП найдется такая, для которой он будет минимальным многочленом, тогда для всех представленных в множестве вариантов найдется такая ЛРП, для которой минимальный период принадлежит множеству $r \in \{1,2,3,4,6,12\}$.

д) $(x + 1)^{12}$, его делитель, многочлен $x + 1$ не имеет корней и неприводим, его период $r = 2^1 - 1 = 1$. Далее, наименьшее такое t, что $2^t \geqslant 12$, $t = 4$. В этом случае период ненулевой последовательности из $S(f)$ будет лежать в множестве $\{1, 2, 4, 8, 16\}$ (По Случаю 3 из Теоремы 2.6 из [2]). Тогда, так как для любого делителя х.м. в семействе ЛРП найдется такая, для которой он будет минимальным многочленом, то найдется такая ЛРП, для которой минимальный период принадлежит множеству $r \in \{1, 2, 4, 8, 16\}$.

$x^1 \mod x+1 = 1, r = 1$

$x^2 \mod x^2+1 = 1, r = 2$

$x^4 \mod x^3+x^2+x+1 = (x^2+x+1)x = 1, r = 4$

$x^8 \mod x^4+1 = 1, r = 8$

$x^8 \mod x^12+x^8+x^4+1 = x^8 \neq 1$

$x^{16} \mod x^{12}+x^8+x^4+1 = (x^8+x^4+1)x^4 = x^{12}+x^8+x^4 = 1, r = 16$

е) $(x^3+x^2+1)^3$, его делитель - многочлен x^3+x^2+1 не имеет корней и неприводим, его период $r = 2^3-1 = 7$, так как делитель этого числа 1 - не подходит, в связи с тем, что период многочлена степени выше 1 должен быть больше 1, то период равен 7. Далее находим наименьшее такое t, что $2^t \geqslant 3$, $t = 2$. В этом случае (По Случаю 2 из Теоремы 2.6 из [2]) период ненулевой последовательности из $S(f)$ будет лежать в множестве $\{7, 14, 28\}$. Тогда, так как для любого делителя х.м. в семействе ЛРП найдется такая, для которой он будет минимальным многочленом, тогда найдется такая ЛРП, для которой минимальный период принадлежит множеству $r \in \{1, 7, 14, 28\}$.

$x^7 \mod x^3+x^2+1 = (x^2+1)(x^2+1)x = x^5+x = (x^2+1)x^2+x = x^4+x^2+x = x^3+x^2 = 1, r = 7$

$x^7 \mod (x^3+x^2+1)^2 = x^7 \mod 1+x^4+x^6 = x+x^5 \neq 1$

$x^{14} \mod 1+x^4+x^6 = (1+x^4)^2x^2 = x^2+x^10 = (1+x^4)x^4+x^2 = (1+x^4)x^2+x^4+x^2 = 1, r = 14$

$x^{14} \mod (x^3+x^2+1)^3 = x^{14} \mod 1+x^2+x^3+x^4+x^7+x^8+x^9 = (1+x^2+x^3+x^4+x^7+x^8)x^5 = x^5+x^7+x^8+x^9+x^{12}+x^{13} = 1+x^2+x^3+x^4+x^5+(1+x)(x^3+x^5+x^6+x^7+x^10+x^11)... = 1+x+x^5+x^7 \neq 1$

$x^{28} \mod (x^3+x^2+1)^3 = x^{28} \mod 1+x^2+x^3+x^4+x^7+x^8+x^9 = ... = 1, r = 28$ Без вариантов.

1.1.4 Задача 4

Найти первые три бита (нумерация координат слева направо) вектора 57–го состояния ЛРП с х.м. $f(x) = (x^3 + x^2 + 1)^4 \in F_2[x]$ и вектором начального (ненулевого) состояния $s(0) \in (F2)^{12}, s(0) \in \{(101100\ldots0), (110100\ldots0), (111100\ldots0), (011000\ldots0), (1000\ldots0), (0100\ldots0), (101000\ldots0), (100100\ldots0)\}$.

Делитель характеристической функции, многочлен $x^3 + x^2 + 1$ не имеет корней и неприводим, его период $r = 2^3 - 1 = 7$, так как делитель этого числа 1 - не подходит, в связи с тем, что период многочлена степени выше 1 должен быть больше 1, то период равен 7. Далее, наименьшее такое t, что $2^t \geqslant 4$, $t = 2$. По Случаю 2 из Теоремы 2.6 из [2] период ненулевой последовательности из $S(f)$ будет лежать в множестве $\{7, 14, 28\}$.

$x^{14} \mod (x^3 + x^2 + 1)^4 = x^{14} \mod 1 + x^8 + x^{12} = (1 + x^8)x^2 = x^2 + x^10 \neq 1$

$x^{28} \mod (x^3 + x^2 + 1)^4 = x^{28} \mod 1 + x^8 + x^{12} = (1 + x^8)^2x^4 = (1 + x^{16})x^4 = x^4 + x^{20} =$

$(1 + x^8)x^8 + x^4 = (1 + x^8)x^4 + x^8 + x^4 = 1, r = 28$

Тогда 57 состояние ЛРП $s(57) = s(28 * 2 + 1) = s(1)$. Тогда достаточно выработать одну новую координату и сдвинуть начало вектора, по виду х.м. видно, что каждый следующий бит получается из 12 предыдущих как сумма первого бита (x^{12}) и пятого (x^8). Тогда $s(57) = s(1) \in \{(01100\ldots01), (10100\ldots01), (11100\ldots01), (11000\ldots01), (000\ldots01), (100\ldots01), (01000\ldots01), (00100\ldots01)\}$. Тогда ответ - первые три бита получившейся последовательности.

1.1.5 Задача 5

Найти минимальный период суммы двух ЛРП с х.м. $f_1(x) \in \{x^3 + x^2 + 1, x^3 + x + 1\}, f_1 \in F_2[x]$, и $f_2(x) \in \{x^2 + x + 1, x^2 + 1\}, f_2 \in F_2[x]$, при условии, что начальный вектор первой ЛРП ра-

вен $s_1 \in \{(010), (110), (111), (101), (011), (001), (100)\}$, а второй равен $s_2 \in \{(11), (10), (01)\}$.

а) $f_1(x) = x^3 + x^2 + 1, f_1 \in F_2[x]$, $f_2(x) = x^2 + x + 1, f_2 \in F_2[x]$

Многочлены $x^3 + x^2 + 1$ и $x^2 + x + 1$ не имеют корней, а значит неприводимы. Характеристический многочлен суммы двух ЛРП $f(x) = (x^3 + x^2 + 1)(x^2 + x + 1)$ 5 степени, следовательно вектор начального состояния для данной ЛРП имеет длину 5. Для установленного варианта начальных векторов выработаем последовательность до 5 знаков и просуммируем, чтобы получить начальный вектор суммы ЛРП: $v_1 \in \{(01001), (11010), (11101), (10100), (01110), (00111), (10011)\}$, $v_2 \in \{(11011), (10110), (01101)\}$, следовательно, если $s_2 = (11)$, то $s \in \{(10010), (00001), (00110), (01111), (10101), (11100), (01000)\}$, если $s_2 = (10)$, то $s \in \{(11111), (01100), (01011), (00010), (01000), (10001), (00101)\}$, если $s_2 = (01)$, то $s \in \{(00100), (10111), (10000), (11001), (00011), (01010), (11110)\}$.

В зависимости от начального вектора минимальным многочленом может быть $m(x) \in \{x^2 + x + 1, x^3 + x^2 + 1, (x^3 + x^2 + 1)(x^2 + x + 1)\}$, 1 не подходит, так как начальный вектор ненулевой. Определяем для полученного начального состояния, начиная с многочлена-претендента меньшей степени, может ли он вырабатывать данную последовательность и получаем, что минимальный период может быть равен $r \in \{3, 7, 21\}$, будучи периодом найденного минимального многочлена.

б) $f_1(x) = x^3 + x^2 + 1, f_1 \in F_2[x]$, $f_2(x) = x^2 + 1, f_2 \in F_2[x]$

Многочлен $x^3 + x^2 + 1$ не имеет корней, а значит неприводим, $x^2+1 = (x+1)^2$. Характеристический многочлен суммы двух ЛРП $f(x) = (x^3+x^2+1)(x^2+1)$ 5 степени, следовательно вектор начального состояния для данной ЛРП имеет длину 5. Для установленного варианта начальных векторов выработаем последовательность до 5 знаков и просуммируем, чтобы получить начальный вектор суммы ЛРП: считаем аналогично предудыщему варианту.

В зависимости от начального вектора минимальным многочленом может быть $m(x) \in \{x+1, x^2+1, x^3+x^2+1, (x^3+x^2+1)(x+1), (x^3+x^2+1)(x^2+1)\}$, 1 не подходит, так как начальный вектор ненулевой. Определяем для полученного начального состояния, начиная с многочлена-претендента меньшей степени, может ли он вырабатывать данную последовательность и получаем, что минимальный период может быть равен $r \in \{1, 2, 7, 7, 14\}$, будучи периодом найденного минимального многочлена.

в) $f_1(x) = x^3 + x + 1, f_1 \in F_2[x],\ f_2(x) = x^2 + x + 1, f_2 \in F_2[x]$

Многочлен $x^3 + x + 1$ и $x^2 + x + 1$ не имеют корней, а значит неприводимы. Характеристический многочлен суммы двух ЛРП $f(x) = (x^3+x+1)(x^2+x+1)$ 5 степени, следовательно вектор начального состояния для данной ЛРП имеет длину 5. Для установленного варианта начальных векторов выработаем последовательность до 5 знаков и просуммируем, чтобы получить начальный вектор суммы ЛРП: считаем аналогично предудыщему варианту.

В зависимости от начального вектора минимальным многочленом может быть $m(x) \in \{x^2+x+1, x^3+x+1, (x^3+x+1)(x^2+x+1)\}$, 1 не подходит, так как начальный вектор ненулевой. Определяем для полученного начального состояния, начиная с многочлена-претендента меньшей степени, может ли он вырабатывать данную последовательность и получаем, что минимальный период может быть равен $r \in \{3, 7, 21\}$, будучи периодом найденного минимального многочлена.

г) $f_1(x) = x^3 + x + 1, f_1 \in F_2[x],\ f_2(x) = x^2 + 1, f_2 \in F_2[x]$

Многочлен $x^3 + x + 1$ не имеет корней, а значит неприводим, $x^2+1 = (x+1)^2$. Характеристический многочлен суммы двух ЛРП $f(x) = (x^3+x+1)(x^2+1)$ 5 степени, следовательно вектор начального состояния для данной ЛРП имеет длину 5. Для установленного варианта начальных векторов выработаем последовательность до 5 знаков и просуммируем, чтобы получить начальный вектор суммы ЛРП: считаем аналогично предудыщему варианту.

В зависимости от начального вектора минимальным многочленом может быть $m(x) \in \{x+1, x^2+1, x^3+x+1, (x^3+x+1)(x+1), (x^3+x+1)(x^2+1)\}$, 1 не подходит, так как начальный вектор ненулевой. Определяем для полученного начального состояния, начиная с многочлена-претендента меньшей степени, может ли он вырабатывать данную последовательность и получаем, что минимальный период может быть равен $r \in \{1, 2, 7, 7, 14\}$, будучи периодом найденного минимального многочлена.

1.1.6 Задача 6

Найти минимальный многочлен суммы двух ЛРП с х.м. $f_1(x) \in \{x^3 + x^2 + 1, x^3 + x + 1\}, f_1 \in F_2[x]$, и $f_2(x) \in \{x^3 + x + 1, x^3 + 1\}, f_2 \in F_2[x]$, при условии, что начальный вектор первой ЛРП равен $s_1 \in \{(010), (111), (110), (001), (100), (101), (011)\}$, а второй равен $s_2 \in \{(101), (111), (010), (001), (011), (100), (110)\}$

а) $f_1(x) = x^3 + x^2 + 1, f_1 \in F_2[x]$, $f_2(x) = x^3 + x + 1, f_2 \in F_2[x]$

Многочлены $x^3 + x^2 + 1$ и $x^3 + x + 1$ не имеют корней, а значит неприводимы. Характеристический многочлен суммы двух ЛРП $f(x) = (x^3 + x^2 + 1)(x^3 + x + 1)$ 6 степени, следовательно вектор начального состояния для данной ЛРП имеет длину 6. Для установленного варианта начальных векторов выработаем последовательность до 6 знаков и просуммируем, чтобы получить начальный вектор суммы ЛРП: вычисляем аналогично 1.1.5.

В зависимости от начального вектора минимальным многочленом может быть $m(x) \in \{x^3 + x + 1, x^3 + x^2 + 1, (x^3 + x^2 + 1)(x^3 + x + 1)\}$, 1 не подходит, так как начальный вектор ненулевой. Определяем для полученного начального состояния, начиная с многочлена-претендента меньшей степени, может ли он вырабатывать данную последовательность и получаем минимальный многочлен.

б) $f_1(x) = x^3 + x^2 + 1, f_1 \in F_2[x]$, $f_2(x) = x^3 + 1, f_2 \in F_2[x]$

Многочлены $x^3 + x^2 + 1$ не имеет корней, а значит неприводим, $x^3 + 1 = (x + 1)(x^2 + x + 1)$. Характеристический многочлен суммы

двух ЛРП $f(x) = (x^3 + x^2 + 1)(x^3 + 1)$ 6 степени, следовательно вектор начального состояния для данной ЛРП имеет длину 6. Для установленного варианта начальных векторов выработаем последовательность до 6 знаков и просуммируем, чтобы получить начальный вектор суммы ЛРП: вычисляем аналогично 1.1.5.

В зависимости от начального вектора минимальным многочленом может быть $m(x) \in \{x+1, x^2+x+1, x^3+1, x^3+x^2+1, (x^3+x^2+1)(x+1), (x^3+x^2+1)(x^2+x+1), (x^3+x^2+1)(x^3+1)\}$, 1 не подходит, так как начальный вектор ненулевой. Определяем для полученного начального состояния, начиная с многочлена-претендента меньшей степени, может ли он вырабатывать данную последовательность и получаем минимальный многочлен.

в) $f_1(x) = x^3 + x + 1, f_1 \in F_2[x],\ f_2(x) = x^3 + x + 1, f_2 \in F_2[x]$

Многочлен $x^3 + x + 1$ не имеет корней, а значит неприводим. Характеристический многочлен суммы двух ЛРП $f(x) = (x^3 + x + 1)^2$ 6 степени, следовательно вектор начального состояния для данной ЛРП имеет длину 6. Для установленного варианта начальных векторов выработаем последовательность до 6 знаков и просуммируем, чтобы получить начальный вектор суммы ЛРП: вычисляем аналогично 1.1.5.

В зависимости от начального вектора минимальным многочленом может быть $m(x) \in \{x^3 + x + 1, (x^3 + x + 1)^2\}$, 1 не подходит, так как начальный вектор ненулевой. Определяем для полученного начального состояния, начиная с многочлена-претендента меньшей степени, может ли он вырабатывать данную последовательность и получаем минимальный многочлен.

г) $f_1(x) = x^3 + x + 1, f_1 \in F_2[x],\ f_2(x) = x^3 + 1, f_2 \in F_2[x]$

Многочлены $x^3 + x + 1$ не имеет корней, а значит неприводим, $x^3 + 1 = (x + 1)(x^2 + x + 1)$. Характеристический многочлен суммы двух ЛРП $f(x) = (x^3 + x + 1)(x^3 + 1)$ 6 степени, следовательно вектор начального состояния для данной ЛРП имеет длину 6. Для установленного варианта начальных векторов выработаем последовательность до 6

знаков и просуммируем, чтобы получить начальный вектор суммы ЛРП: вычисляем аналогично 1.1.5.

В зависимости от начального вектора минимальным многочленом может быть $m(x) \in \{x+1, x^2+x+1, x^3+1, x^3+x+1, (x^3+x+1)(x+1), (x^3+x+1)(x^2+x+1), (x^3+x+1)(x^3+1)\}$, 1 не подходит, так как начальный вектор ненулевой. Определяем для полученного начального состояния, начиная с многочлена-претендента меньшей степени, может ли он вырабатывать данную последовательность и получаем минимальный многочлен.

1.2 Задачи из контрольной работы №1

1.2.1 Задача 7

Найти период многочлена:

а) $f(x) = x^4 + x^3 + x^2 + x + 1; F_2[x]$

Корней у многочлена нет (1,0 не подходят), поэтому необходимо рассмотреть неприводимые многочлены 2 степени. Таких в нашем поле только одно - $1 + x + x^2$, проверим делимость простым делением уголком - остаток от деления равен $x + 1$. Таким образом, многочлен $f(x)$ неприводим, тогда в соответствии с Следствием 1.6.5 (из [2]) период должен быть делителем числа $q^m - 1 = 2^4 - 1 = 15$. Рассмотрим числа $\{3, 5, 15\}$. $x^3 \mod x^4 + x^3 + x^2 + x + 1 = x^3 \neq 1$, $x^5 \mod x^4 + x^3 + x^2 + x + 1 = x(x^3 + x^2 + x + 1) = 1$, следовательно $r = 5$.

б) $f(x) = 2x + 1; Z_3[x]$

Многочлен первой степени, поэтому он неприводим, но тогда период многочлена может быть равен 1 или $3^1 - 1 = 2$. $x - 1(\mod 2x + 1) = 2\frac{x+2}{2}(\mod 2x+1) = 2(2x+1)(\mod 2x+1) = 0$, следовательно период $r = 1$.

в) $f(x) = x + 1; Z_3[x]$

Многочлен первой степени, поэтому он неприводим, но тогда период многочлена может быть равен 1 или $3^1 - 1 = 2$. $x - 1(\mod x + 1) = (x + 2)(\mod x + 1) = 1 \neq 0$, следовательно период $r \neq 1$. Таким образом, период многочлена $r = q^m - 1 = 3^1 - 1 = 2$.

г) $f(x) = x^2 + x + 1; Z_3[x]$

$f(x) = x^2 + x + 1 = x^2 - 2x + 1 = (x - 1)^2$. По Случаю 2 из Теоремы 2.6 из [2], так как $x - 1(\mod x - 1) = 0$, $e = r(x - 1) = 1$, $p = 3$, t – наименьшее натуральное число, при котором $p^t \geqslant n$, тогда $t = 1$. Тогда период многочлена может быть $1, 3$. Период многочлена степени выше 1 должен быть больше 1, поэтому в данном примере $r = 3$.

д) $f(x) = x^2 + x + 2; Z_3[x]$

Так как корней у многочлена нет (0,1,2 не подходят), он неприводим. Период многочлена степени выше 1 должен быть больше 1, тогда в соответствии с Следствием 1.6.5 (из [2]) период многочлена должен быть делителем числа $q^m - 1 = 3^2 - 1 = 8$. Рассмотрим числа $\{2, 4, 8\}$. $x^2 \mod x^2 + x + 2 = -x - 2 \neq 1$, $x^4 \mod x^2 + x + 2 = (2x + 1)^2 = x^2 + x + 1 = -1 \neq 1$. Следовательно, $r = 8$.

е) $f(x) = x^2 + 2x + 2; Z_3[x]$

Так как корней у многочлена нет (0,1,2 не подходят), он неприводим. Период многочлена степени выше 1 должен быть больше 1, тогда в соответствии с Следствием 1.6.5 (из [2]) период многочлена должен быть делителем числа $q^m - 1 = 3^2 - 1 = 8$. Рассмотрим числа $\{2, 4, 8\}$. $x^2 \mod x^2 + 2x + 2 = x + 1 \neq 1$, $x^4 \mod x^2 + 2x + 2 = (x + 1)^2 = x^2 + 2x + 1 = -1 \neq 1$. Следовательно, $r = 8$.

ж) $f(x) = x^2 + 1; Z_3[x]$

Так как корней у многочлена нет (0,1,2 не подходят), он неприводим. Период многочлена степени выше 1 должен быть больше 1, тогда в соответствии с Следствием 1.6.5 (из [2]) период многочлена должен быть делителем числа $q^m - 1 = 3^2 - 1 = 8$. Рассмотрим числа $\{2, 4, 8\}$. $x^2 \mod x^2 + 1 = -1 \neq 1$, $x^4 \mod x^2 + 1 = (-1)^2 = 1$. Следовательно, $r = 4$.

и) $f(x) = x^3 + 1; Z_3[x]$

Так как у многочлена есть корень 2, делим уголком на $x-2 = x+1$ и получаем $f(x) = (x+1)(x^2+2x+1) = (x+1)^3$. По Случаю 2 из Теоремы 2.6 из [2], так как $x - 1(\mod x+1) = 1 \neq 0$, $e = r(x-1) = 3^1 - 1 = 2$, $p = 3$, t – наименьшее натуральное число, при котором $p^t \geqslant n$, тогда $t = 1$. Тогда период многочлена может быть $2, 6$. Проверим для $r = 2 : x^2(\mod x^3 + 1) = x^2 \neq 1$, тогда в данном примере $r = 6$.

к) $f(x) = x^3 + x + 1; Z_3[x]$

Так как у многочлена есть корень 1, делим уголком на $x - 1$ и получаем $f(x) = (x-1)(x^2+x+2)$. Из примера д видим, что (x^2+x+2) неприводим и его период $r(x^2 + x + 2) = 8$. Период $x - 1$, так как $x - 1(\mod x - 1) = 0$, равен 1. По Случаю 3 из Теоремы 2.6 из [2]: $r = \text{НОК}(r(x-1), r(x^2+x+2)) = \text{НОК}(1, 8) = 8$.

л) $f(x) = x^3 + x + 2; Z_3[x]$ Так как у многочлена есть корень 2, делим уголком на $x-2 = x+1$ и получаем $f(x) = (x+1)(x^2+x+2)$. Из примера д видим, что $(x^2 + x + 2)$ неприводим и его период $r(x^2 + x + 2) = 8$. Период $x + 1$, из примера в, равен 2. По Случаю 3 из Теоремы 2.6 из [2]: $r = \text{НОК}(r(x+1), r(x^2+x+2)) = \text{НОК}(2, 8) = 8$.

1.2.2 Задача 8

Укажите все примитивные многочлены из множества:

а) $f(x) \in \{x + 1, x^2 + 1, x^2 + x + 1, x^3 + 1\}, (f(x) \in F_2[x])$

$x \mod x + 1 = 1$, следовательно $r = q^m - 1 = 2^1 - 1 = 1$, тогда многочлен имеет максимальный период и неприводим, так как имеет степень 1. Примитивен.

$x^2 + 1 = (x + 1)^2$, приводим. Не примитивен.

$x^2 + x + 1$ непримводим, так как не имеет корней. Так как период многочлена степени выше 1 должен быть больше 1, $r = q^m - 1 = 2^2 - 1 = 3$ в соответствии с Следствием 1.6.5 (из [2]). Примитивен.

$x^3+1=(x+1)(x^2-x+1)$ приводим. Не примитивен.

б) $f(x) \in \{x^2+1, x^3+1, x^3+x+1\}, (f(x) \in F_2[x])$

$x^2+1=(x+1)^2$, приводим. Не примитивен.

$x^3+1=(x+1)(x^2-x+1)$ приводим. Не примитивен.

x^3+x+1 неприводим, так как не имеет корней. Так как период многочлена степени выше 1 должен быть больше 1, $r=q^m-1=2^3-1=7$ в соответствии с Следствием 1.6.5 (из [2]). Примитивен.

в) $f(x) \in \{x^3+1, x^3+x^2+1, x^4+x^2+1\}, (f(x) \in F_2[x])$

$x^3+1=(x+1)(x^2-x+1)$ приводим. Не примитивен.

x^3+x^2+1 не имеет корней, неприводим. Так как период многочлена степени выше 1 должен быть больше 1, $r=q^m-1=2^3-1=7$ в соответствии с Следствием 1.6.5 (из [2]). Примитивен.

x^4+x^2+1 не имеет корней, но приводим: $x^4+x^2+1=(x^2+x+1)^2$. Не примитивен.

г) $f(x) \in \{x^5+1, x^5+x+1, x^4+x^2+x+1\}, (f(x) \in F_2[x])$

x^5+1 имеет корень 1, приводим. Не примитивен.

x^5+x+1 не имеет корней, неприводим (не делится на x^2+x+1). Так как период многочлена степени выше 1 должен быть больше 1, $r=q^m-1=2^5-1=31$в соответствии с Следствием 1.6.5 (из [2]). Примитивен.

x^4+x^2+x+1 имеет корень 1, приводим. Не примитивен.

д) $f(x) \in \{x^5+x^2+1, x^3+x^2+x+1, x^4+x^3+x^2+x+1\}, (f(x) \in F_2[x])$

x^5+x^2+1 корней нет (0 и 1 не подходят), делители следует искать среди многочленов степени 2,3, причем неприводимых. Таких 2 степени в нашем поле только одно - $1+x+x^2$, проверим делимость простым делением уголком - остаток от деления равен 1, получаем, что $f(x)$ неприводим. Так как период многочлена степени выше 1 должен

быть больше 1, $r = q^m - 1 = 2^5 - 1 = 31$ в соответствии с Следствием 1.6.5 (из [2]). Примитивен.

$x^3 + x^2 + x + 1$ имеет корень 1, приводим. Не примитивен.

$x^4+x^3+x^2+x+1$ корней нет (0 или 1 не подходят), делители следует искать среди многочленов степени 2, причем неприводимых. Таких 2 степени в нашем поле только одно - $1 + x + x^2$, проверим делимость простым делением уголком - остаток от деления равен $x + 1$, получаем, что $f(x)$ неприводим. Так как период многочлена степени выше 1 должен быть больше 1, период должен быть делителем числа $q^m - 1 = 2^4 - 1 = 15$ в соответствии с Следствием 1.6.5 (из [2]). Рассмотрим числа $\{3, 5, 15\}$. $x^3 \mod x^4 + x^3 + x^2 + x + 1 = x^3 \neq 1$, $x^5 \mod x^4 + x^3 + x^2 + x + 1 = x(x^3 + x^2 + x + 1) = 1$, следовательно $r = 5$. Не примитивен.

е) $f(x) \in \{x - 2, x - 1, x^2 + 1\}, (f(x) \in Z_3[x])$

Многочлен $x - 2$ первой степени, поэтому он неприводим, но тогда период многочлена может быть равен 1. $x - 1(\mod x - 2) = 1 \neq 0$, следовательно период $r \neq 1$. Таким образом, тогда в соответствии с Следствием 1.6.5 (из [2]) период многочлена $r = q^m - 1 = 3^1 - 1 = 2$. Примитивен.

Многочлен $x - 1$ первой степени, поэтому он неприводим, но тогда период многочлена может быть равен 1. $x - 1(\mod x - 1) = 0$, следовательно период $r = 1 \neq q^m - 1 = 3^1 - 1 = 2$. Не примитивен.

Так как корней у многочлена $x^2 + 1$ нет (0,1,2 не подходят), он неприводим. Период многочлена степени выше 1 должен быть больше 1, тогда в соответствии с Следствием 1.6.5 (из [2]) период многочлена должен быть делителем числа $q^m - 1 = 3^2 - 1 = 8$. Рассмотрим числа $\{2, 4, 8\}$. $x^2 \mod x^2 + 1 = -1 \neq 1$, $x^4 \mod x^2 + 1 = (-1)^2 = 1$. Следовательно, $r = 4 \neq q^m - 1 = 3^2 - 1 = 8$. Не примитивен.

ж) $f(x) \in \{x + 2, x^2 + 2, x^3 + 2\}, (f(x) \in Z_3[x])$

Многочлен $x+2=x-1$ первой степени, поэтому он неприводим, но тогда период многочлена может быть равен 1. $x-1(\mod x-1)=0$, следовательно период $r=1\neq q^m-1=3^1-1=2$. Не примитивен.

Многочлен x^2+2 имеет корень 1, приводим. Не примитивен.

Многочлен x^3+2 имеет корень 1, приводим. Не примитивен.

и) $f(x)\in\{x^2+x+1, x^2-x+1, x^2+x+2\}, (f(x)\in Z_3[x])$

Многочлен x^2+x+1 имеет корень 1, приводим. Не примитивен.

Многочлен x^2-x+1 имеет корень 2, приводим. Не примитивен.

Так как корней у многочлена x^2+x+2 нет (0,1,2 не подходят), он неприводим. Период многочлена степени выше 1 должен быть больше 1, тогда в соответствии с Следствием 1.6.5 (из [2]) период многочлена должен быть делителем числа $q^m-1=3^2-1=8$. Рассмотрим числа $\{2,4,8\}$. $x^2 \mod x^2+x+2=-x-2\neq 1$, $x^4 \mod x^2+x+2=(2x+1)^2=x^2+x+1=-1\neq 1$. Следовательно, $r=8$. Примитивен.

к) $f(x)\in\{x^2+1, x^2+2, x^2+2x+2\}, (f(x)\in Z_3[x])$

Так как корней у многочлена x^2+1 нет (0,1,2 не подходят), он неприводим. Период многочлена степени выше 1 должен быть больше 1, тогда в соответствии с Следствием 1.6.5 (из [2]) период многочлена должен быть делителем числа $q^m-1=3^2-1=8$. Рассмотрим числа $\{2,4,8\}$. $x^2 \mod x^2+1=-1\neq 1$, $x^4 \mod x^2+1=(-1)^2=1$. Следовательно, $r=4\neq q^m-1=3^2-1=8$. Не примитивен.

Многочлен x^2+2 имеет корень 1, приводим. Не примитивен.

Так как корней у многочлена x^2+2x+2 нет (0,1,2 не подходят), он неприводим. Период многочлена степени выше 1 должен быть больше 1, тогда в соответствии с Следствием 1.6.5 (из [2]) период многочлена должен быть делителем числа $q^m-1=3^2-1=8$. Рассмотрим числа $\{2,4,8\}$. $x^2 \mod x^2+2x+2=x+1\neq 1$, $x^4 \mod x^2+2x+2=(x+1)^2=x^2+2x+1=-1\neq 1$. Следовательно, $r=8$. Примитивен.

л) $f(x)\in\{x^2+2x+1, x^2+1, x^2-1\}, (f(x)\in Z_3[x])$

Многочлен $x^2 + 2x + 1$ имеет корень 2, приводим. Не примитивен.

Так как корней у многочлена $x^2 + 1$ нет (0,1,2 не подходят), он неприводим. Период многочлена степени выше 1 должен быть больше 1, тогда в соответствии с Следствием 1.6.5 (из [2]) период многочлена должен быть делителем числа $q^m - 1 = 3^2 - 1 = 8$. Рассмотрим числа $\{2, 4, 8\}$. $x^2 \mod x^2 + 1 = -1 \neq 1$, $x^4 \mod x^2 + 1 = (-1)^2 = 1$. Следовательно, $r = 4 \neq q^m - 1 = 3^2 - 1 = 8$. Не примитивен.

Многочлен $x^2 - 1$ имеет корень 1, приводим. Не примитивен.

1.2.3 Задача 9

Последовательность $c(1)$,$c(2)$,$c(3)$,$c(4)$,$c(5)$,... = 1,2,3,0,4,... является суммой двух чисто периодических последовательностей над полем Z_5, периоды которых равны 8 и 12. Найти $c(51), c(52), c(53), c(50), c(49), c(29), c(28), c(27), c(26), c(25)$.

Одним из периодов суммы двух чисто периодических последовательностей является наименьшее общее кратное периодов двух этих последовательностей, но может быть и меньше. Для решения данной задачи нам достаточно найти какой-либо период r =НОК$(8, 12) = 24$. Тогда $c(51) = c(3) = 3, c(52) = c(4) = 0, c(53) = c(5) = 4, c(50) = c(2) = 2, c(49) = c(1) = 1, c(29) = c(5) = 4, c(28) = c(4) = 0, c(27) = c(3) = 3, c(26) = c(2) = 2, c(25) = c(1) = 1$

1.2.4 Задача 10

Укажите все двоичные характеристические многочлены $f \in \{f_1, f_2, f_3\}$, для которых в семействе $S(f)$ существует ЛРП с минимальным периодом w.

а) $w = 2, f \in \{x + 1, x^2 + 1, x^3 + 1\}$ Семейство ЛРП строится на основании характеристической функции f_i, минимальный период ЛРП является периодом ее минимального многочена. Минимальный многочлен - некоторый делитель характеристической функции. f_1 - неприводимый

многочлен, его делители $1, x+1$, тогда возможный период только $w=1$, следовательно f_1 - не включаем в ответ. f_2 раскладывется как $(x+1)^2$, его делители $1, x+1, x^2+1$, тогда возможные периоды $1, 2$, следовательно f_2 - включаем в ответ. f_3 раскладывется как $(x+1)(x^2+x+1)$, его делители $1, x+1, x^2+x+1, x^3+1$, тогда возможные периоды $1, 3$, следовательно f_3 - не включаем в ответ.

б) $w=3, f \in \{(x+1)^2, x^3+1, x^3+x+1\}$ Семейство ЛРП строится на основании характеристической функции f_i, минимальный период ЛРП является периодом ее минимального многочена. Минимальный многочлен - некоторый делитель характеристической функции. f_1 раскладывется как $(x+1)^2$, его делители $1, x+1, x^2+1$, тогда возможные периоды $1, 2$, следовательно f_1 - не включаем в ответ. f_2 раскладывется как $(x+1)(x^2+x+1)$, его делители $1, x+1, x^2+x+1, x^3+1$, тогда возможные периоды $1, 3$, следовательно f_2 - включаем в ответ. f_3 - неприводимый многочлен, его делители $1, x^3+x+1$, тогда возможные периоды $1, 2^3-1=7$, следовательно f_3 - не включаем в ответ.

в) $w=4, f \in \{(x+1)^2, (x+1)^3, x^3+x^2+1\}$ Семейство ЛРП строится на основании характеристической функции f_i, минимальный период ЛРП является периодом ее минимального многочена. Минимальный многочлен - некоторый делитель характеристической функции. f_1 раскладывется как $(x+1)^2$, его делители $1, x+1, x^2+1$, тогда возможные периоды $1, 2$, следовательно f_1 - не включаем в ответ. f_2 раскладывется как $(x+1)^3$, его делители $1, x+1, x^2+1, x^3+x^2+x+1$, тогда возможные периоды $1, 2, 4$, следовательно f_2 - включаем в ответ. f_3 - неприводимый многочлен, его делители $1, x^3+x^2+1$, тогда возможные периоды $1, 2^3-1=7$, следовательно f_3 - не включаем в ответ.

г) $w=6, f \in \{(x+1)^2, (x+1), x^4+x^2+1\}$ Семейство ЛРП строится на основании характеристической функции f_i, минимальный период ЛРП является периодом ее минимального многочена. Минимальный многочлен - некоторый делитель характеристической функции. f_1 раскладывется как $(x+1)^2$, его делители $1, x+1, x^2+1$, тогда возможные периоды $1, 2$, следовательно f_1 - не включаем в ответ. f_2 - неприводимый многочлен, его

делители $1, x+1$, тогда возможный период только $w=1$, следовательно f_2 - не включаем в ответ. f_3 раскладывется как $(x^2+x+1)^2$, его делители $1, x^2+x+1, x^4+x^2+1$, тогда возможные периоды $1, 2^2-1=3, 2^4-1=15$,, следовательно f_3 - не включаем в ответ.

д) $w=4, f \in \{(x+1)^4, x^3+1, x^2+x+1\}$ Семейство ЛРП строится на основании характеристической функции f_i, минимальный период ЛРП является периодом ее минимального многочена. Минимальный многочлен - некоторый делитель характеристической функции. f_1 раскладывется как $(x+1)^4$, его делители $1, x+1, x^2+1, x^3+x^2+x+1, x^4+1$, тогда возможные периоды $1, 2, 4$, следовательно f_1 - включаем в ответ. f_2 раскладывется как $(x+1)(x^2+x+1)$, его делители $1, x+1, x^2+x+1, x^3+1$, тогда возможные периоды $1, 3$, следовательно f_2 - не включаем в ответ. f_3 - неприводимый многочлен, его делители $1, x^2+x+1$, тогда возможные периоды $1, 2^2-1=3$, следовательно f_3 - не включаем в ответ.

е) $w=3, f \in \{(x+1)^3, x^3+1, x^2+x+1\}$ Семейство ЛРП строится на основании характеристической функции f_i, минимальный период ЛРП является периодом ее минимального многочена. Минимальный многочлен - некоторый делитель характеристической функции. f_1 раскладывется как $(x+1)^3$, его делители $1, x+1, x^2+1, x^3+x^2+x+1$, тогда возможные периоды $1, 2, 4$, следовательно f_1 - не включаем в ответ. f_2 раскладывется как $(x+1)(x^2+x+1)$, его делители $1, x+1, x^2+x+1, x^3+1$, тогда возможные периоды $1, 3$, следовательно f_2 - включаем в ответ. f_3 - неприводимый многочлен, его делители $1, x^2+x+1$, тогда возможные периоды $1, 2^2-1=3$, следовательно f_3 - включаем в ответ.

ж) $w=4, f \in \{(x+1)^2, (x+1)^3, (x+1)^4\}$ Семейство ЛРП строится на основании характеристической функции f_i, минимальный период ЛРП является периодом ее минимального многочена. Минимальный многочлен - некоторый делитель характеристической функции. f_1 раскладывется как $(x+1)^2$, его делители $1, x+1, x^2+1$, тогда возможные периоды $1, 2$, следовательно f_1 - не включаем в ответ. f_2 раскладывется как $(x+1)^3$, его делители $1, x+1, x^2+1, x^3+x^2+x+1$, тогда возможные периоды $1, 2, 4$, следовательно f_2 - включаем в ответ. f_3 раскладывется как $(x+1)^4$,

его делители $1, x+1, x^2+1, x^3+x^2+x+1, x^4+1$, тогда возможные периоды $1, 2, 4$, следовательно f_3 - включаем в ответ.

и) $w = 6, f \in \{(x^3+1)(x+1)^2, (x^3+1)(x+1)\}$ Семейство ЛРП строится на основании характеристической функции f_i, минимальный период ЛРП является периодом ее минимального многочена. Минимальный многочлен - некоторый делитель характеристической функции. f_1 раскладывется как $(x^2+x+1)(x+1)^3$, его делители $1, x+1, x^2+1, x^2+x+1, (x+1)^3, (x^2+x+1)(x+1)^3$, тогда возможные периоды $1, 2, 3, 4$,НОК$(3,4) = 12$, следовательно f_1 - не включаем в ответ. f_2 раскладывется как $(x^2+x+1)(x+1)^2$, его делители $1, x+1, x^2+1, x^2+x+1, (x^2+x+1)(x+1)^2$, тогда возможные периоды $1, 2, 3$,НОК$(2,3) = 6$, следовательно f_2 - включаем в ответ.

к) $w = 8, f \in \{(x+1)^8, (x+1)^7, (x+1)^6\}$ Семейство ЛРП строится на основании характеристической функции f_i, минимальный период ЛРП является периодом ее минимального многочена. Минимальный многочлен - некоторый делитель характеристической функции. f_1 раскладывется как $(x+1)^8$, его делители $1, x+1, x^2+1, x^3+x^2+x+1, x^4+1, x^5+x^4+x+1, x^6+x^4+x^2+1, x^7+x^6+x^5+x^4+x^3+x^2+x+1, x^8+1$, тогда возможные периоды $1, 2, 4, 8$, следовательно f_1 - включаем в ответ. f_2 раскладывется как $(x+1)^7$, его делители $1, x+1, x^2+1, x^3+x^2+x+1, x^4+1, x^5+x^4+x+1, x^6+x^4+x^2+1, x^7+x^6+x^5+x^4+x^3+x^2+x+1$, тогда возможные периоды $1, 2, 4, 8$, следовательно f_2 - включаем в ответ. f_3 раскладывется как $(x+1)^6$, его делители $1, x+1, x^2+1, x^3+x^2+x+1, x^4+1, x^5+x^4+x+1, x^6+x^4+x^2+1$, тогда возможные периоды $1, 2, 4, 8$, следовательно f_3 - включаем в ответ.

л) $w = 8, f \in \{(x+1)^5, (x+1)^6, (x+1)^7\}$ Семейство ЛРП строится на основании характеристической функции f_i, минимальный период ЛРП является периодом ее минимального многочена. Минимальный многочлен - некоторый делитель характеристической функции. f_1 раскладывется как $(x+1)^5$, его делители $1, x+1, x^2+1, x^3+x^2+x+1, x^4+1, x^5+x^4+x+1$, тогда возможные периоды $1, 2, 4, 8$, следовательно f_1 - включаем в ответ. f_2 раскладывется как $(x+1)^6$, его делители $1, x+1, x^2+1, x^3+x^2+x+1, x^4+1, x^5+x^4+x+1, x^6+x^4+x^2+1$, тогда возможные периоды $1, 2, 4, 8$,

следовательно f_2 - включаем в ответ. f_3 раскладывется как $(x+1)^6$, его делители $1, x+1, x^2+1, x^3+x^2+x+1, x^4+1, x^5+x^4+x+1, x^6+x^4+x^2+1, x^7+x^6+x^5+x^4+x^3+x^2+x+1$, тогда возможные периоды $1, 2, 4, 8$, следовательно f_3 - включаем в ответ.

1.3 Задачи из контрольной работы №2

1.3.1 Задача 7

Заданы две ЛРП с х.м. $f_1(x) = x^2+x+1 \in F_2[x], f_2(x) = x^2+1 \in F_2[x]$. Начальные состояния указанных ЛРП равны соответственно $(11,11), (11,10), (11,01), (10,11), (01,11), (01,01), (01,10), (10,10), (10,01)$. Найти минимальный период их произведения.

Первый характеристический многочлен $f_1(x) = x^2+x+1$ неприводим, тогда он совпадает с минимальным многочленом и его период - минимальный период первой ЛРП $\omega_1 = 2^{deg(f_1(x))=2} - 1 = 3$. Второй характеристический многочлен приводим $f_2(x) = x^2+1 = (x+1)^2$, тогда в зависимости от начального состояния период данной ЛРП равен $\omega_2 = 1$ (для вектора (11)) или $\omega_2 = 2$. Произведение ЛРП - также ЛРП, и ее период (не обязательно минимальный) равен ω =НОК(ω_1,ω_2) = 3 или НОК(ω_1,ω_2) = 6.

Рассмотрим оба принципиальных варианта:

а) (11, 11) ω =НОК(ω_1,ω_2) = 3; $x^w + 1$ - х.м.

Выработаем 3 знак - (110, 111), тогда начальный вектор произведения ЛРП (110). $x^3+1 = (x+1)(x^2+x+1)$, и как видно из начального вектора (x^2+x+1) - минимальный многочлен, тогда минимальный период ЛРП равен 3.

б) (11,10) ω =НОК(ω_1,ω_2) = 6; $x^w + 1$ - х.м.

Выработаем до 6 знака - (110110, 101010), тогда начальный вектор произведения ЛРП (100010). $x^6+1 = (x+1)^2(x^2+x+1)^2$, и как видно из начального вектора $(x+1)^2(x^2+x+1)$ - минимальный многочлен, тогда минимальный период ЛРП равен 6.

1.3.2 Задача 8

Укажите функциональную связь между выходным знаком с номером $m = \{5,6,7,8,9,10\}$ и координатами начального состояния $x = (x_1,x_2,x_3)$ фильтрующего генератора, вырабатывающего выходную последовательность по закону:

$\gamma_1 = f(x)$

$\gamma_2 = f(\delta_L(x))$

...

$\gamma_j = f(\delta_{L^{j-1}}(x))$

...

$f(x) = f(x_1,x_2,x_3) \in \{x_1x_3 + x_2, x_1x_2 + x_3\}$;

$\delta_L(x) = \delta_L(x_1,x_2,x_3) = (x_2,x_3,L(x)), L(x) = L(x_1,x_2,x_3) = x_1 + x_2$

а) $f(x) = x_1x_3 + x_2$

$\gamma_1 = x_1x_3 + x_2$

$\gamma_2 = x_2(x_1 + x_2) + x_3 = x_1x_2 + x_2 + x_3$

$\gamma_3 = x_2x_3 + x_3 + x_1 + x_2$

$\gamma_4 = x_3(x_1 + x_2) + x_1 + x_2 + x_2 + x_3 = x_1x_3 + x_2x_3 + x_1 + x_3$

$\gamma_5 = x_2(x_1+x_2)+x_3(x_1+x_2)+x_2+x_1+x_2 = x_1x_2+x_1x_3+x_2x_3+x_2+x_1$

$\gamma_6 = x_2x_3 + x_2(x_1 + x_2) + x_3(x_1 + x_2) + x_2 + x_3 = x_1x_2 + x_1x_3 + x_3$

$\gamma_7 = x_2x_3 + x_2(x_1 + x_2) + x_1 + x_2 = x_1x_2 + x_2x_3 + x_1$

$\gamma_8 = x_2x_3 + x_3(x_1 + x_2) + x_2 = x_1x_3 + x_2$

Зациклилось.

б) $f(x) = x_1x_2 + x_3$

$\gamma_1 = x_1x_2 + x_3$

$\gamma_2 = x_2x_3 + x_1 + x_2$

$\gamma_3 = x_3(x_1 + x_2) + x_2 + x_3 = x_1x_3 + x_2x_3 + x_2 + x_3$

$\gamma_4 = x_2(x_1+x_2)+x_3(x_1+x_2)+x_3+x_1+x_2 = x_1x_2+x_1x_3+x_2x_3+x_1+x_3$

$\gamma_5 = x_2x_3+x_2(x_1+x_2)+x_3(x_1+x_2)+x_2+x_1+x_2 = x_1x_2+x_1x_3+x_1+x_2$

$\gamma_6 = x_2x_3 + x_2(x_1 + x_2) + x_2 + x_3 = x_1x_2 + x_2x_3 + x_3$

$\gamma_7 = x_2x_3 + x_3(x_1 + x_2) + x_1 + x_2 = x_1x_3 + x_1 + x_2$

$\gamma_8 = x_2(x_1 + x_2) + x_2 + x_3 = x_1x_2 + x_3$

Зациклилось.

1.3.3 Задача 9

Найти вероятность выходной 3-гаммы $\gamma = (\gamma_1,\gamma_2,\gamma_3) \in \{(000), (001), (010), (100), (110), (011), (101), (111)\}$ при условии равновероятного входа для фильтрующей схемы, задаваемой функцией $f = f(x_1,x_2,x_3) \in \{f_1 = x_1x_3+x_2, f_2 = x_1x_3+x_1+x_2+x_3, f_3 = x_1x_3+x_2+1\}$, $\gamma_j = f(x_j, x_{j+1}, x_{j+2}), j = 1,2,3.$

$$(\gamma_1,\gamma_2,\gamma_3)(f_1) = (x_1x_3 + x_2, x_2x_4 + x_3, x_3x_5 + x_4),$$

$$(\gamma_1,\gamma_2,\gamma_3)(f_2) = (x_1x_3+x_1+x_2+x_3, x_2x_4+x_2+x_3+x_4, x_3x_5+x_3+x_4+x_5),$$

$$(\gamma_1,\gamma_2,\gamma_3)(f_3) = (x_1x_3 + x_2 + 1, x_2x_4 + x_3 + 1, x_3x_5 + x_4 + 1)$$

x_1	x_2	x_3	x_4	x_5	$\gamma(f_1)$	$\gamma(f_2)$	$\gamma(f_3)$
0	0	0	0	0	(0,0,0)	(0,0,0)	(1,1,1)
0	0	0	0	1	(0,0,0)	(0,0,1)	(1,1,1)
0	0	0	1	0	(0,0,1)	(0,1,1)	(1,1,0)
0	0	0	1	1	(0,0,1)	(0,1,0)	(1,1,0)
0	0	1	0	0	(0,1,0)	(1,1,1)	(1,0,1)
0	0	1	0	1	(0,1,1)	(1,1,1)	(1,0,0)
0	0	1	1	0	(0,1,1)	(1,0,0)	(1,0,0)
0	0	1	1	1	(0,1,0)	(1,0,0)	(1,0,1)
0	1	0	0	0	(1,0,0)	(1,1,0)	(0,1,1)
0	1	0	0	1	(1,0,0)	(1,1,1)	(0,1,1)
0	1	0	1	0	(1,1,1)	(1,1,1)	(0,0,0)
0	1	0	1	1	(1,1,1)	(1,1,0)	(0,0,0)
0	1	1	0	0	(1,1,0)	(0,0,1)	(0,0,1)
0	1	1	0	1	(1,1,1)	(0,0,1)	(0,0,0)
0	1	1	1	0	(1,0,1)	(0,0,0)	(0,1,0)
0	1	1	1	1	(1,0,0)	(0,0,0)	(0,1,1)
1	0	0	0	0	(0,0,0)	(1,0,0)	(1,1,1)
1	0	0	0	1	(0,0,0)	(1,0,1)	(1,1,1)
1	0	0	1	0	(0,0,1)	(1,1,1)	(1,1,0)
1	0	0	1	1	(0,0,1)	(1,1,0)	(1,1,0)
1	0	1	0	0	(1,1,0)	(1,1,1)	(0,0,1)
1	0	1	0	1	(1,1,1)	(1,1,1)	(0,0,0)
1	0	1	1	0	(1,1,1)	(1,0,0)	(0,0,0)
1	0	1	1	1	(1,1,0)	(1,0,0)	(0,0,1)
1	1	0	0	0	(1,0,0)	(0,1,0)	(0,1,1)
1	1	0	0	1	(1,0,0)	(0,1,1)	(0,1,1)
1	1	0	1	0	(1,1,1)	(0,1,1)	(0,0,0)
1	1	0	1	1	(1,1,1)	(0,1,0)	(0,0,0)
1	1	1	0	0	(0,1,0)	(0,0,1)	(1,0,1)
1	1	1	0	1	(0,1,1)	(0,0,1)	(1,0,0)
1	1	1	1	0	(0,0,1)	(0,0,0)	(1,1,0)
1	1	1	1	1	(0,0,0)	(0,0,0)	(1,1,1)

Тогда вероятности комбинаций гаммы следующие:

γ_1	γ_2	γ_3	$P(\gamma(f_1))$	$P(\gamma(f_2))$	$P(\gamma(f_3))$
0	0	0	$\frac{5}{2^5}$	$\frac{5}{2^5}$	$\frac{7}{2^5}$
0	0	1	$\frac{5}{2^5}$	$\frac{5}{2^5}$	$\frac{3}{2^5}$
0	1	0	$\frac{3}{2^5}$	$\frac{3}{2^5}$	$\frac{1}{2^5}$
0	1	1	$\frac{3}{2^5}$	$\frac{3}{2^5}$	$\frac{5}{2^5}$
1	0	0	$\frac{5}{2^5}$	$\frac{5}{2^5}$	$\frac{3}{2^5}$
1	0	1	$\frac{1}{2^5}$	$\frac{1}{2^5}$	$\frac{3}{2^5}$
1	1	0	$\frac{3}{2^5}$	$\frac{3}{2^5}$	$\frac{5}{2^5}$
1	1	1	$\frac{7}{2^5}$	$\frac{7}{2^5}$	$\frac{5}{2^5}$

1.3.4 Задача 10

Найти период нелинейной рекурренты x_1,x_2,..., вырабатываемой из начального вектора-состояния $(x_1,x_2,...,x_n) = (x_1,x_2,x_3,x_4) = (1010)$, $f = x_1 + L(x_2,...,x_n) + (x_2+1)(x_3+1)\cdots(x_n+1) = x_1 + L(x_2,x_3,x_4) + (x_2+1)(x_3+1)(x_4+1)$, $L(x_2,x_3,x_4) \in \{x_2,x_3,x_4,x_2+x_3,x_2+x_4,x_3+x_4,x_2+x_3+x_4\}$.

а) $L(x_2,x_3,x_4) = x_2$

$f(x) = x_1 + x_2 + \overline{x_2} \cdot \overline{x_3} \cdot \overline{x_4}$

$x_5 = x_1 + x_2 + \overline{x_2} \cdot \overline{x_3} \cdot \overline{x_4} = 1 + 0 + 1 \cdot 0 \cdot 1 = 1$

$x_6 = x_2 + x_3 + \overline{x_3} \cdot \overline{x_4} \cdot \overline{x_5} = 0 + 1 + 0 \cdot 1 \cdot 0 = 1$

$x_7 = x_3 + x_4 + \overline{x_4} \cdot \overline{x_5} \cdot \overline{x_6} = 1 + 0 + 1 \cdot 0 \cdot 0 = 1$

$x_8 = x_4 + x_5 + \overline{x_5} \cdot \overline{x_6} \cdot \overline{x_7} = 0 + 1 + 0 \cdot 0 \cdot 0 = 1$

$x_9 = x_5 + x_6 + \overline{x_6} \cdot \overline{x_7} \cdot \overline{x_8} = 1 + 1 + 0 \cdot 0 \cdot 0 = 0$

$x_{10} = x_6 + x_7 + \overline{x_7} \cdot \overline{x_8} \cdot \overline{x_9} = 1 + 1 + 0 \cdot 0 \cdot 1 = 0$

$x_{11} = x_7 + x_8 + \overline{x_8} \cdot \overline{x_9} \cdot \overline{x_{10}} = 1 + 1 + 0 \cdot 1 \cdot 1 = 0$

$x_{12} = x_8 + x_9 + \overline{x_9} \cdot \overline{x_{10}} \cdot \overline{x_{11}} = 1 + 0 + 1 \cdot 1 \cdot 1 = 0$

$x_{13} = x_9 + x_{10} + \overline{x_{10}} \cdot \overline{x_{11}} \cdot \overline{x_{12}} = 0 + 0 + 1 \cdot 1 \cdot 1 = 1$

$x_{14} = x_{10} + x_{11} + \overline{x_{11}} \cdot \overline{x_{12}} \cdot \overline{x_{13}} = 0 + 0 + 1 \cdot 1 \cdot 0 = 0$

$x_{15} = x_{11} + x_{12} + \overline{x_{12}} \cdot \overline{x_{13}} \cdot \overline{x_{14}} = 0 + 0 + 1 \cdot 0 \cdot 1 = 0$

$x_{16} = x_{12} + x_{13} + \overline{x_{13}} \cdot \overline{x_{14}} \cdot \overline{x_{15}} = 0 + 1 + 0 \cdot 1 \cdot 1 = 1$

$x_{17} = x_{13} + x_{14} + \overline{x_{14}} \cdot \overline{x_{15}} \cdot \overline{x_{16}} = 1 + 0 + 1 \cdot 1 \cdot 0 = 1$

$x_{18} = x_{14} + x_{15} + \overline{x_{15}} \cdot \overline{x_{16}} \cdot \overline{x_{17}} = 0 + 0 + 1 \cdot 0 \cdot 0 = 0$

$x_{19} = x_{15} + x_{16} + \overline{x_{16}} \cdot \overline{x_{17}} \cdot \overline{x_{18}} = 0 + 1 + 0 \cdot 0 \cdot 1 = 1$

$x_{20} = x_{16} + x_{17} + \overline{x_{17}} \cdot \overline{x_{18}} \cdot \overline{x_{19}} = 1 + 1 + 0 \cdot 1 \cdot 0 = 0$

Таким образом, $(x_1, x_2, x_3, x_4) = (x_{17}, x_{18}, x_{19}, x_{20}) \Rightarrow r = 16$

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Лось А.Б., Нестеренко Ф.Ю., Рожков М.И. Криптографические методы защиты информации. — М., Юрайт, 2016. — 473 с.

2. Рожков М.И. Теория линейных рекуррентных последовательностей. — 2021. — Режим доступа: https://github.com/jerrydie/tex/blob/main/Teoria_Gener_Rozh.docx.pdf (дата обращения: 03.12.2021).