

Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК _____

Дворникова
Татьяна Николаевна

Быстрое преобразование корректирующих кодов, применяемых в микро- и
наноэлектронных устройствах

АВТОРЕФЕРАТ

на соискание степени магистра технических наук
по специальности 1-41 80 03 «Нанотехнологии и наноматериалы (в
электронике)»

(подпись магистранта)

Научный руководитель
Будько Анатолий Антонович

(фамилия, имя, отчество)

кандидат технических наук, доцент

(ученая степень, ученое звание)

(подпись научного руководителя)

Минск 2017

Библиотека БГУИР

Нормоконтроль

(фамилия, имя, отчество)

(дата, подпись)

ВВЕДЕНИЕ

В настоящее время идет бурное развитие средств обработки информации, основанных на широком применении микро- и наноэлектроники.

Разработчики сложных информационных систем стремятся увеличить надежность и помехоустойчивость отдельных элементов систем (средств обработки информации, устройств памяти, ввода-вывода, модуляции-демодуляции и др.), причем даже при очень высокой надежности элементов необходимо использовать общесистемные средства повышения помехоустойчивости [5].

Помехоустойчивым (корректирующим) кодированием называется кодирование, при котором осуществляется обнаружение либо обнаружение и исправление ошибок в принятых кодовых комбинациях [1,4].

Теория кодирования возникла в конце 1940-х годов с появлением работ Голея, Хэмминга и Шеннона.

Хэмминг первым предложил конструктивный метод построения кодов с избыточностью и простым декодированием.

В результате широких исследований в области теории кодирования разработан ряд конструктивных методов синтеза корректирующих кодов.

Целью магистерской работы является разработка метода быстрого декодирования низкоскоростных корректирующих кодов, используемых в микро- и наноэлектронных устройствах. Метод быстрого декодирования низкоскоростных корректирующих кодов будет разработан на основе использования быстрых алгоритмов спектральных преобразований в различных системах упорядочений функций Уолша.

С развитием новых методов передачи цифровой информации внимание исследователей привлекли функции Уолша. Появилось множество работ, посвященных теории и практическому применению функций Уолша в устройствах, разрабатываемых в области микро- и наноэлектроники [7, 8, 11].

Преобразование Уолша осуществляется с помощью быстрых алгоритмов. К настоящему времени имеется определенное количество таких алгоритмов, которые получены в основном используя факторизации матриц Уолша в различных упорядочениях. Существует четыре системы упорядочений: Уолша-Адамара, Уолша-Пэли, Уолша Качмажа и Уолша-Трахтмана. Однако свойства, а также вопросы генерирования и преобразования в различных системах упорядочения изучены не в одинаковой степени [24, 27].

При рассмотрении алгоритмов быстрого преобразования Уолша выделяются так называемые «замечательные» алгоритмы быстрого преобразования Уолша.

Все алгоритмы быстрого преобразования Уолша требуют одинаковое количество арифметических операций, однако решение об использовании для конкретного применения того или иного алгоритма принимается на основе сравнения. «Замечательные» алгоритмы быстрого преобразования Уолша обладают свойствами симметрии, их граф для любой размерности может быть легко получен. Применяются замечательные графы, имеющие симметрию, одинаковые итерации, позволяют осуществить вычисления на местах. Известно, что алгоритмы Кули-Туки и Сэнди не требуют дополнительной памяти, поскольку вычисления осуществляются на местах. В то время алгоритм Кроузера-Радера-Рошфора не позволяет осуществить вычисления на местах и требует дополнительной памяти. Однако граф быстрого преобразования Уолша (алгоритм Гротера-Рейдера) имеет все одинаковые итерации, что дает определенное преимущество при осуществлении вычислений мгновенного спектра по Уолшу [6, 19].

В магистерской работе рассматриваются в различных системах упорядочения получение замечательных алгоритмов быстрого преобразования Уолша, основанные на представлении элементов матриц Уолша в экспоненциальной или показательной форме. На основе алгоритмов быстрых преобразований строятся процессоры БПУ.

При практическом использовании помехоустойчивых кодов осуществляются две операции: кодирование и декодирование. Основной проблемой при использовании корректирующих кодов в микро- и нанoeлектронных устройствах является декодирование [4]. Поэтому быстрое декодирование, заключающееся в сокращении числа операций, необходимых для декодирования, является актуальной задачей. Использование БПУ позволяет решать проблемы декодирования помехоустойчивых кодов.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Функции Уолша находят применение в различных областях передачи и обработки цифровой информации. Преобразование Уолша осуществляется с помощью быстрых алгоритмов.

Целью магистерской работы является разработка метода быстрого декодирования низкоскоростных корректирующих кодов, используемых в микро- и нанoeлектронных устройствах, на основе использования быстрых алгоритмов спектральных преобразований в различных системах упорядочений функций Уолша.

Задачи исследования – разработка быстрых алгоритмов спектральных преобразований Уолша в различных упорядочениях. Определение взаимосвязи матриц корректирующих кодов в матрицы Уолша.

В главе 1 рассмотрена структурная схема процесса передачи информации, применение кодов, исправляющих ошибки и методы декодирования низкоскоростных кодов.

В главе 2 приведены функции Уолша, их свойства, связь между номерами функций Уолша в различных системах упорядочения, разработан метод извлечения алгоритмов быстрых спектральных преобразований в базисе Уолша для различных систем упорядочений и на основе этого метода получены два варианта алгоритмов быстрого преобразования Уолша в системе упорядочений Уолша-Пэли, которые относятся к «замечательным» алгоритмам.

В главе 3 установлены основные принципы преобразования M–последовательности в последовательность Уолша в различных системах упорядочения функций Уолша с помощью определенных перестановок и определены эти перестановки.

По результатам работы сделано заключение.

Практическое применение полученных результатов заключается в синтезе перестановочных генераторов во всех системах упорядочения функций Уолша. Это позволяет использовать дополнительную гибкость при реализации быстрых декодеров. Данная задача является актуальной для современных систем передачи и обработки информации, реализуемых на микро- и нанoeлектронных устройствах.

Результаты работы были опубликованы в сборнике тезисов докладов XIV Белорусско-российской научно-технической конференции «Технические средства защиты информации» БГУИР, 2016.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В большинстве современных систем связи используется передача сообщений в цифровом виде. Из-за наличия помех и замираний в каналах связи сбой при приеме любого одиночного элемента вызывает искажение цифровых данных всей группы, что может привести к неблагоприятным последствиям.

Эффективным средством борьбы с помехами в цифровых системах связи является применение помехоустойчивого кодирования, основанного на введении искусственной избыточности в передаваемое сообщение, что приводит к уменьшению информационной скорости передачи. При этом возможно достижение требуемых значений к показателям достоверности принимаемой информации [12].

Избыточные символы используются для того, чтобы подчеркнуть индивидуальность каждого сообщения. Их всегда выбирают так, чтобы сделать маловероятной потерю сообщением его индивидуальности из-за искажения при воздействии помех. Кроме того, в процессе кодирования применяется эффект усреднения шума, который достигается за счет того, что избыточные символы зависят от нескольких информационных символов.

При обработке символов блоками, а не одного за другим уменьшается общее количество ошибок. При увеличении длины блока доля ошибочных символов в блоке стремится к средней частоте ошибок в канале, а доля блоков, число ошибок в которых существенно отличается от среднего значения, становится очень малой. Кроме того необходимо, чтобы существовала схема «кодирования», нечувствительная к ошибкам в некоторой доле символов блока и не приводящая при этом к потере сообщением своей «индивидуальности», т.е. не приводящая к ошибочному блоку. При усреднении шума возрастают резервы улучшения характеристик при увеличении длины блока. Таким образом, длинные блоковые коды эффективнее коротких [13]. При исправлении ошибок в сообщении, представляемом последовательностью из n двоичных символов, необходимо, чтобы не все 2^n возможных последовательностей представляли сообщения. Когда каждая из возможных принятых последовательностей n символов представляет некоторое сообщение, нет никаких оснований считать, что одна последовательность является более правильной, чем любая другая. Для исправления всех наборов из t или менее ошибок необходимо и достаточно, чтобы каждая последовательность, представляющая сообщение, отличалась от последовательности, представляющей любое другое сообщение, не менее чем в $2t + 1$ местах. Число позиций, в которых две последовательности отличаются друг от друга называется расстоянием Хемминга d между этими двумя последовательностями. Наименьшее значение d для всех пар кодовых

последовательностей называется кодовым расстоянием d_{\min} . Так как d_{\min} всегда должно быть на единицу больше удвоенного числа исправляемых ошибок, то

$$t \geq (d_{\min} - 1)/2$$

Параметр t указывает, что все комбинации из t или менее ошибок в любой принятой последовательности могут быть исправлены [21].

Используя избыточность, содержащуюся в двоичной последовательности на выходе демодулятора, декодер обнаруживает и исправляет возникшие ошибки. Двоичная последовательность символов на выходе декодера уже не является избыточной. Если воздействие шума в канале не слишком сильное и декодер может исправить все возникшие ошибки, то двоичная последовательность на выходе декодера будет совпадать с двоичной последовательностью на выходе преобразователя «источник информации — двоичная последовательность».

Одной из разновидностей блочных кодов являются низкоскоростные коды, обладающие рядом особенностей, которые обуславливают их применение в современных системах связи с высокой помехозащищенностью.

Низкоскоростными являются коды, у которых скорость передачи $R=k/n$ мала (это выполнимо при $k \ll n$, где k – количество информационных символов, n – количество избыточных символов) и кодовое расстояние $d \approx n/2$. Благодаря этому коды могут корректировать примерно четверть ошибок на длине кодовой комбинации n и занимают особое положение в теории и практике помехоустойчивого кодирования. Для них разрабатываются новые эффективные алгоритмы формирования и декодирования. С точки зрения теории кодирования они являются классическими кодами, с другой стороны, свойства кодов позволяют использовать их в качестве основы для формирования так называемых сложных сигналов, используемых в микро- и нанoeлектронных устройствах. [7, 8]. При этом используются чисто кодовые методы, основанные на теории векторных пространств и конечных полей, а также алгоритмы и методы теории цифровой обработки сигналов.

Практический интерес представляет исследование различных семейств низкоскоростных кодов, способов их формирования и декодирования, параметров и корреляционных свойств, размеров ансамблей (мощности кодов), сложности структуры и вычислительной сложности обработки. Современные технические средства способны генерировать любой ансамбль кодовых последовательностей с заданными свойствами [5].

Существует три основных метода декодирования: синдромное декодирование, мажоритарное декодирование, декодирование по максимуму правдоподобия. Лучший способ декодирования случайных ошибок заключается в сравнении полученной последовательности с каждой возможной кодовой последовательностью. Такой метод называется декодирование по

максимуму правдоподобия. Минимальная вероятность ошибки получается при использовании декодера, если все входные последовательности сообщений равновероятны. Декодер сравнивает условные вероятности и выбирает максимальную вероятность [9].

Для декодирования кодовых последовательностей, сформированных на основе низкоскоростных кодов могут также использоваться процедуры декодирования, основанные на посимвольном приеме.

Функции Уолша находят применение в различных областях передачи и обработки информации. Однако, несмотря на многочисленные работы математиков и работы, в которых рассматриваются вопросы об инженерном использовании функций Уолша, для более широкого их применения необходимы дополнительные исследования, направленные на изучение свойств этих функций [1].

Функции Уолша являются кусочнопостоянными функциями с нормированным интервалом определения $[0,1)$ или $[-0.5, +0.5)$ и интервалом изменения аргумента, который зависит от порядка системы функций Уолша и равен $\frac{1}{2^n}$, где $n = 1, 2, \dots$. Известны определения функций Уолша через разностное уравнение [14], функции Радемахера [6], тригонометрические функции [22] и в виде матриц [2, 19].

Как разностное уравнение функции Уолша определяются следующим выражением

$$W(j+p, \theta) = (-1)^{j/2} \left\{ W\left[j, 2\left(\theta + \frac{1}{4}\right)\right] + (-1)^{j+p} W\left[n, 2\left(\theta - \frac{1}{4}\right)\right] \right\}, \quad (1)$$

где j – обозначает целую часть числа

$p = 0$ или 1 ;

$j = 0, 1, 2, \dots$;

$W(0, \theta) = 1$ для $0 \leq \theta < 1$;

$W(0, \theta) = 0$ для $\theta < 0$ или $\theta \geq 1$.

$W[0, 2(\theta + 1/4)]$ и $W[0, 2(\theta - 1/4)]$ переносят $W(0, 2\theta)$ влево и вправо на $1/4$. После того как $W(1, \theta)$ найдена, функция $W(1, 0)$ может быть сгенерирована, установив $j=1, P=0$. $W(3, 0) \dots$ и т.д.

Упорядочение функций Уолша может проводиться различными способами. Упорядочения Пэли, Адамара, Качмажа и Трахтмана являются особыми, так как их матрицы являются симметричными, и поэтому они рассматриваются и используются в быстрых преобразованиях Уолша [22, 26, 27].

Между номерами функций Уолша в различных системах упорядочения существует связь. Связь между номерами функций Уолша в различных системах упорядочения приведена на рисунке 1

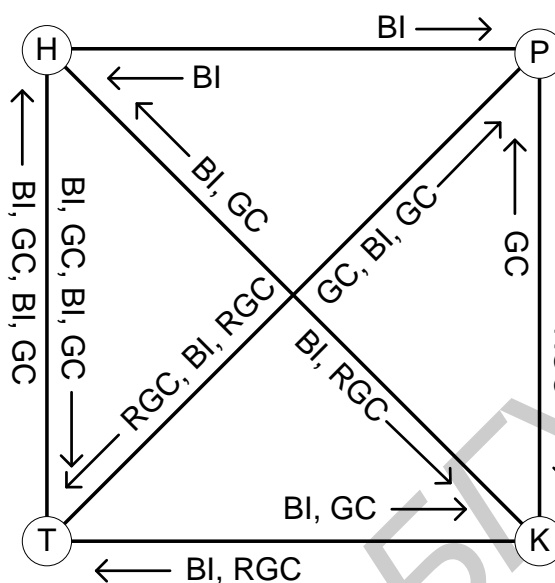


Рисунок 1 – Связь между номерами функций Уолша в различных системах упорядочения

BI – бинарная операция инверсии

CG – преобразование в код Грея

RGC – преобразование в обратный код Грея

Если необходимо сравнить порядковые номера функций Уолша в различных системах, следует провести несколько операций с бинарными порядковыми номерами в соответствии со схемой на рисунке 1 [22].

Для сравнения номеров функций Уолша в различных системах, необходимо выполнить одну или несколько операций с двоичными представлениями номеров функций в соответствии с приведенной схемой. Схема может быть проиллюстрирована на примере в таблице 1

Данные таблицы показывают, что для перехода от одной системы упорядочения к другой производится перестановка столбцов матрицы Уолша. Она может быть использована для преобразования псевдослучайной последовательности в Уолш-последовательность

Таблица 1 – Номера функции в системы упорядочения Трахтмана и Пэли

Номер функции в системе T	Двоичный номер в системе T	Двоичный код после GC операции	Двоичный код после VI операции	Двоичный номер в системе P	Номер в системе P
0	000	000	000	000	0
1	001	001	100	110	6
2	010	011	110	101	5
3	011	010	010	011	3
4	100	110	011	010	2
5	101	111	111	100	4
6	110	101	101	111	7
7	111	100	001	001	1

Быстрое преобразование Уолша (БПУ). Для функции $f(x)$ в интервале определения $[0, 1)$ прямое преобразование по Уолшу имеет вид:

и обратное

Дискретные функции Уолша образуются равномерной выборкой непрерывных функций. Для них справедливы рассмотренные свойства и дискретные преобразования дискретной функции определяются следующим образом:

и обратное преобразование

—

В матричном виде пара преобразований Уолша

—

где — векторы-столбцы

Функции Уолша находят применение в различных областях передачи и обработки информации. Преобразование Уолша осуществляется с помощью быстрых алгоритмов [1].

Быстрое преобразование Уолша позволяет существенно сократить число операций до $N \cdot \log_2 N = n \cdot N$.

В микроэлектронных устройствах широко применяются различные алгоритмы быстрых преобразований, самым известным из которых пожалуй является быстрое преобразование Фурье (БПФ). Известно множество вариантов построения алгоритмов БПФ, многие из которых широко описаны в литературе. Учитывая некоторую похожесть функций Уолша и тригонометрических функций можно достаточно просто построить алгоритмы быстрого преобразования Уолша.

К настоящему времени имеется определенное количество таких алгоритмов, которые получены в основном используя факторизации матриц Уолша в различных упорядочений. Возможное количество алгоритмов быстрого преобразования Уолша очень велико. Однако они не равноценны. При рассмотрении алгоритмов быстрого преобразования Уолша выделяются так называемые «замечательные» алгоритмы быстрого преобразования Уолша [1].

Основная идея получения алгоритмов БПУ заключается в разложении матриц Уолша W_{2^n} ранга 2^n в произведение n матриц таким образом, что каждая матрица содержит только два ненулевых элемента в каждой строке:

(6)

При умножении на матрицу размерностью N необходимо затратить $(N - 1)N$ операций, а при умножении на факторизованную матрицу потребуется nN операций. Факторизация матриц Уолша-Адамара основана на представлении таких матриц, как:

$$, \tag{7}$$

где \otimes - оператор произведения Кронекера.

Лучший метод извлечения алгоритмов БПУ может быть получен в системе упорядочения Уолша-Адамара [1].

Этот метод основан на представлении любого элемента матрицы Уолша в экспоненциальной форме. Рассмотрим использование этого метода и его улучшения для получения алгоритма БПУ в системе упорядочения Уолша-Пэли. Уравнение для преобразования Уолша-Пэли могут быть выражены в виде итерации, используя выражение для любого элемента функции Уолша [19].

$$\tag{8}$$

Расчет уравнения может быть выполнен в виде набора итераций. На первой итерации составляющие вектора \bar{y}_1 могут быть рассчитаны как:

На второй итерации составляющие вектора \bar{y}_2 могут быть рассчитаны как:

Расчет преобразований Уолша будет закончен после n итераций.

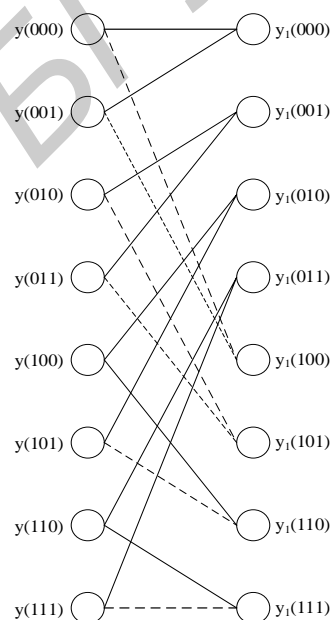
Теперь рассмотрим вывод алгоритма БПУ для случая где, $n=3$. Уравнение для преобразования Уолша:

Составляющие вектора \bar{y}_2 для второй итерации могут быть рассчитаны как:

$$\bar{y}_1(u_3, v_3, v_2) = \sum_{v_1=0}^1 (-1)^{u_3 v_1} \bar{y}(v_3, v_2, v_1) \quad (2.41)$$

Составляющие вектора \bar{y}_1 могут быть рассчитаны как:

$$\begin{aligned}
 & u_3 v_3 v_2 \\
 & y_1(000) = (-1)^{0.0} y(000) + (-1)^{0.1} y(001); \\
 & y_1(001) = (-1)^{0.0} y(010) + (-1)^{0.1} y(011); \\
 & y_1(010) = (-1)^{0.0} y(100) + (-1)^{0.1} y(101); \\
 & y_1(011) = (-1)^{0.0} y(110) + (-1)^{0.1} y(111); \\
 & y_1(100) = (-1)^{1.0} y(000) + (-1)^{1.1} y(001); \\
 & y_1(101) = (-1)^{1.0} y(010) + (-1)^{1.1} y(011); \\
 & y_1(110) = (-1)^{1.0} y(100) + (-1)^{1.1} y(101); \\
 & y_1(111) = (-1)^{1.0} y(110) + (-1)^{1.1} y(111);
 \end{aligned}$$



$$\bar{y}_2(u_3, u_2, v_3) = \sum_{v_2=0}^1 (-1)^{u_2 v_2} \bar{y}_1(u_3, v_3, v_2) \quad (12)$$

$$u_3 u_2 v_3$$

$$y_2(000) = (-1)^{0.0} y_1(000) + (-1)^{0.1} y_1(001);$$

$$y_2(001) = (-1)^{0.0} y_1(010) + (-1)^{0.1} y_1(011);$$

$$y_2(010) = (-1)^{1.0} y_1(000) + (-1)^{1.1} y_1(001);$$

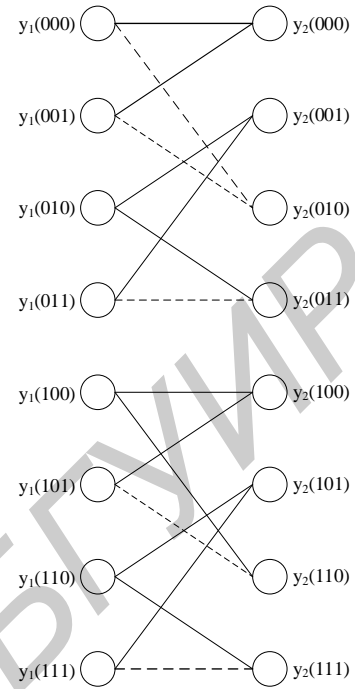
$$y_2(011) = (-1)^{1.0} y_1(010) + (-1)^{1.1} y_1(011);$$

$$y_2(100) = (-1)^{0.0} y_1(100) + (-1)^{1.1} y_1(101);$$

$$y_2(101) = (-1)^{0.0} y_1(110) + (-1)^{0.1} y_1(111);$$

$$y_2(110) = (-1)^{1.0} y_1(100) + (-1)^{0.1} y_1(101);$$

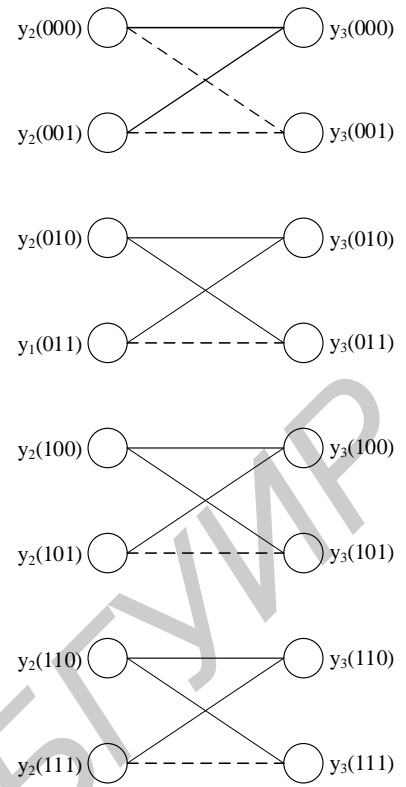
$$y_2(111) = (-1)^{1.0} y_1(110) + (-1)^{1.1} y_1(111);$$



Составляющие вектора $\bar{y}_3 = \bar{Y}$ для третьей итерации могут быть рассчитаны как:

$$\bar{y}_3(u_3, u_2, u_1) = \sum_{v_3=0}^1 (-1)^{u_1 v_3} \bar{y}_2(u_3, u_2, v_3); \bar{Y} = \bar{y}_3 \quad (13)$$

$$\begin{aligned}
y_3(000) &= (-1)^{0.0} y_2(000) + (-1)^{0.1} f_1(001); \\
y_3(001) &= (-1)^{1.0} y_2(000) + (-1)^{1.1} f_1(001); \\
y_3(010) &= (-1)^{0.0} y_2(010) + (-1)^{0.1} f_1(011); \\
y_3(011) &= (-1)^{1.0} y_2(010) + (-1)^{1.1} f_1(011); \\
y_3(100) &= (-1)^{0.0} y_2(100) + (-1)^{0.1} f_1(101); \\
y_3(101) &= (-1)^{1.0} y_2(100) + (-1)^{1.1} f_1(101); \\
y_3(110) &= (-1)^{0.0} y_2(110) + (-1)^{0.1} f_1(111); \\
y_3(111) &= (-1)^{1.0} y_2(110) + (-1)^{1.1} f_1(111);
\end{aligned}$$



Полученный граф быстрого преобразования Уолша-Пэли показан на рисунке 2.

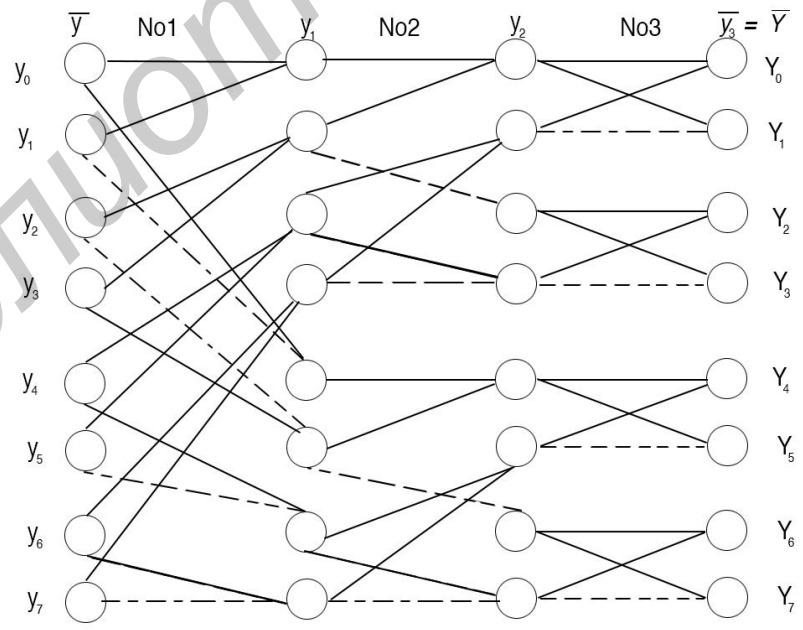


Рисунок 2 - Граф быстрого преобразования Уолша-Пэли.

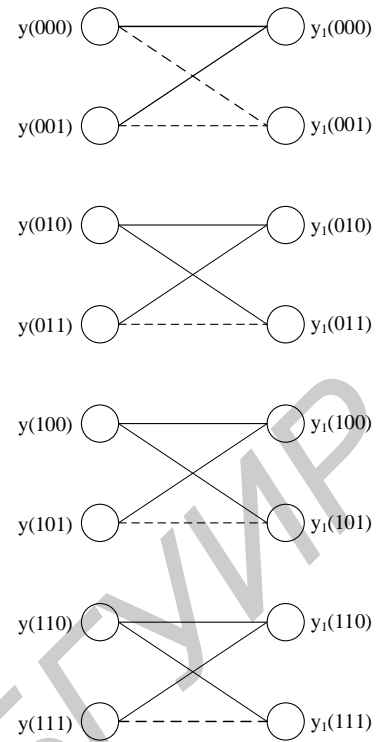
Факторизация матрицы Уолша-Пэли для рассматриваемого случая:

$$W_S^{(p)} = \begin{bmatrix} 1 & & & 1 \\ 1 & & & -1 \\ & 1 & & 1 \\ & 1 & & -1 \\ & & 1 & 1 \\ & & 1 & -1 \\ & & & 1 \\ & & & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \\ & 1 & 1 \\ & 1 & -1 \\ & & 1 & 1 \\ & & 1 & -1 \\ & & & 1 & 1 \\ & & & 1 & -1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 1 & -1 \\ & 1 & 1 \\ & 1 & -1 \\ & & 1 & 1 \\ & & 1 & -1 \\ & & & 1 & 1 \\ & & & 1 & -1 \end{bmatrix} \times$$

Составляющие вектора \bar{y}_1 рассчитаны $\bar{y}_1(u_3, v_3, v_2)$, но их можно рассчитать, как $\bar{y}_1(v_3, v_2, u_3)$.

$$\bar{y}_1(v_3, v_2, u_3) = \sum_{v_1=0}^1 (-1)^{u_3 v_1} y(v_3, v_2, v_1) \quad (14)$$

$$\begin{aligned}
& v_3 v_2 u_3 \\
& y_1(000) = (-1)^{0.0} y(000) + (-1)^{0.1} y(001); \\
& y_1(001) = (-1)^{1.0} y(000) + (-1)^{1.1} y(001); \\
& y_1(010) = (-1)^{0.0} y(010) + (-1)^{0.1} y(011); \\
& y_1(011) = (-1)^{1.0} y(010) + (-1)^{1.1} y(011); \\
& y_1(100) = (-1)^{0.0} y(100) + (-1)^{0.1} y(101); \\
& y_1(101) = (-1)^{1.0} y(100) + (-1)^{1.1} y(101); \\
& y_1(110) = (-1)^{0.0} y(110) + (-1)^{0.1} y(111); \\
& y_1(111) = (-1)^{1.0} y(110) + (-1)^{1.1} y(111);
\end{aligned}$$



Тогда составляющие вектора $\overline{y_2}$ могут быть рассчитаны как:

$$y_2(v_3, u_3, u_2) = \sum_{v_2=0}^1 (-1)^{u_2 v_2} f_1(v_3, v_2, u_3) \quad (15)$$

$$v_3 u_3 u_2$$

$$y_2(000) = (-1)^{0.0} y_1(000) + (-1)^{0.1} y_1(010);$$

$$y_2(001) = (-1)^{1.0} y_1(000) + (-1)^{1.1} y_1(010);$$

$$y_2(010) = (-1)^{0.0} y_1(001) + (-1)^{0.1} y_1(011);$$

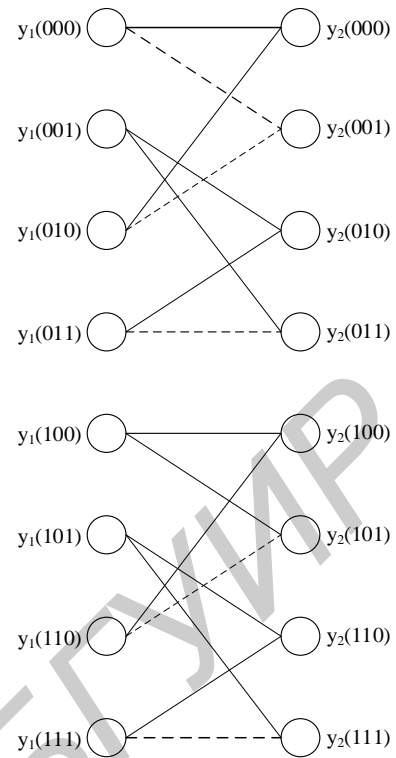
$$y_2(011) = (-1)^{1.0} y_1(001) + (-1)^{1.1} y_1(011);$$

$$y_2(100) = (-1)^{0.0} y_1(100) + (-1)^{0.1} y_1(110);$$

$$y_2(101) = (-1)^{1.0} y_1(100) + (-1)^{1.1} y_1(110);$$

$$y_2(110) = (-1)^{0.0} y_1(101) + (-1)^{0.1} y_1(111);$$

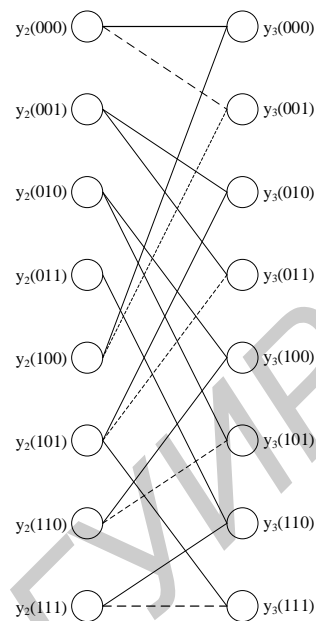
$$y_2(111) = (-1)^{1.0} y_1(101) + (-1)^{1.1} y_1(111);$$



Составляющие вектора $\bar{y}_3 = \bar{Y}$ для третьей итерации могут быть рассчитаны как:

$$\bar{y}_3(u_3, u_2, u_1) = \sum_{v_3=0}^1 (-1)^{u_1 v_3} y_2(v_3, u_3, u_2); \bar{y}_3 = \bar{Y} \quad (16)$$

$$\begin{aligned}
y_3(000) &= (-1)^{0 \cdot 0} y_2(000) + (-1)^{0 \cdot 1} y_2(100); \\
y_3(001) &= (-1)^{1 \cdot 0} y_2(000) + (-1)^{1 \cdot 1} y_2(100); \\
y_3(010) &= (-1)^{0 \cdot 0} y_2(001) + (-1)^{0 \cdot 1} y_2(101); \\
y_3(011) &= (-1)^{1 \cdot 0} y_2(001) + (-1)^{1 \cdot 1} y_2(101); \\
y_3(100) &= (-1)^{0 \cdot 0} y_2(010) + (-1)^{0 \cdot 1} y_2(110); \\
y_3(101) &= (-1)^{1 \cdot 0} y_2(010) + (-1)^{1 \cdot 1} y_2(110); \\
y_3(110) &= (-1)^{0 \cdot 0} y_2(011) + (-1)^{0 \cdot 1} y_2(111); \\
y_3(111) &= (-1)^{1 \cdot 0} y_2(011) + (-1)^{1 \cdot 1} y_2(111);
\end{aligned}$$



Граф преобразования Уолша-Пэли показана на рисунке 3

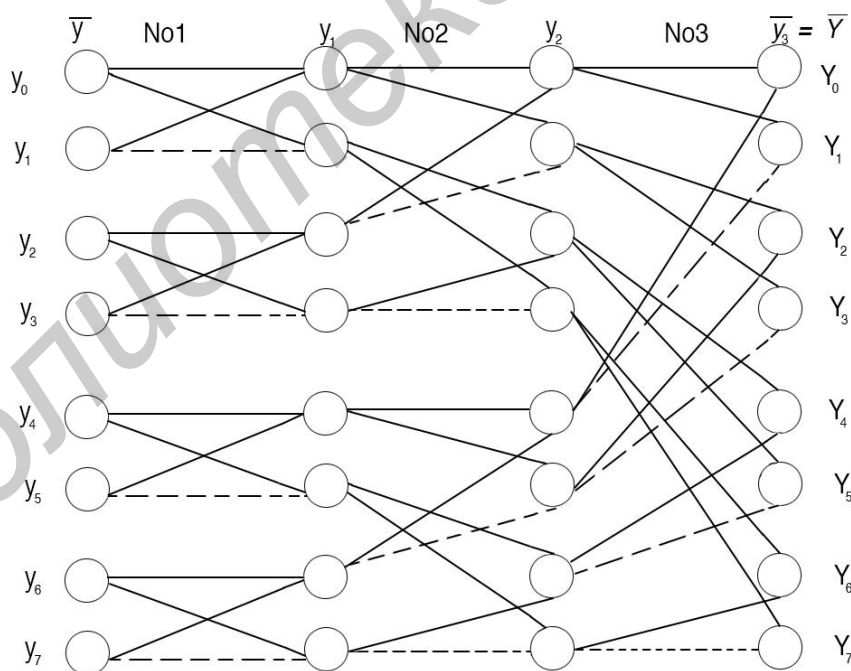


Рисунок 3 Граф преобразования Уолша-Пэли.

Полученные графы алгоритмов БПУ относятся к замечательным, так же как и Кули-Туки, Сэнди, Кроузера-Радера-Рошфора, Эндрю-Кейн-Пратта. Эти графы БПУ обладают некоторыми замечательными свойствами, такими как симметричность и возможность получения графа для любого

количества n . Все алгоритмы быстрого преобразования Уолша требуют одинаковое количество арифметических операций, однако решение об использовании для конкретного применения того или иного алгоритма принимается на основе сравнения. Известно, что алгоритмы Кули-Туки и Сэнди не требуют дополнительной памяти, поскольку вычисление может быть выполнено "на местах", в то время как алгоритм Кроузера-Радера-Рошфора не допускает вычисление на местах и, следовательно, требует дополнительный массив $N = 2^n$ ячеек памяти. Это легко проверить, необходимым и достаточным условием для расчета на местах: что все матрицы разложения матрицы имеют свои ненулевые элементы, расположенные в симметричной структуре. Глядя на рассматриваемое разложение матриц Уолша, мы видим, что только алгоритм Кули-Туки и алгоритм Сэнди удовлетворяют этому условию и, следовательно, позволяют произвести вычисления на местах, в то время как все другие алгоритмы нет [22].

Рассмотренным методом получения алгоритмов быстрого преобразования Уолша можно получить алгоритм вычисления для быстрого преобразования в системе упорядочений Уолша-Трахтмана рисунке 4 и 5.

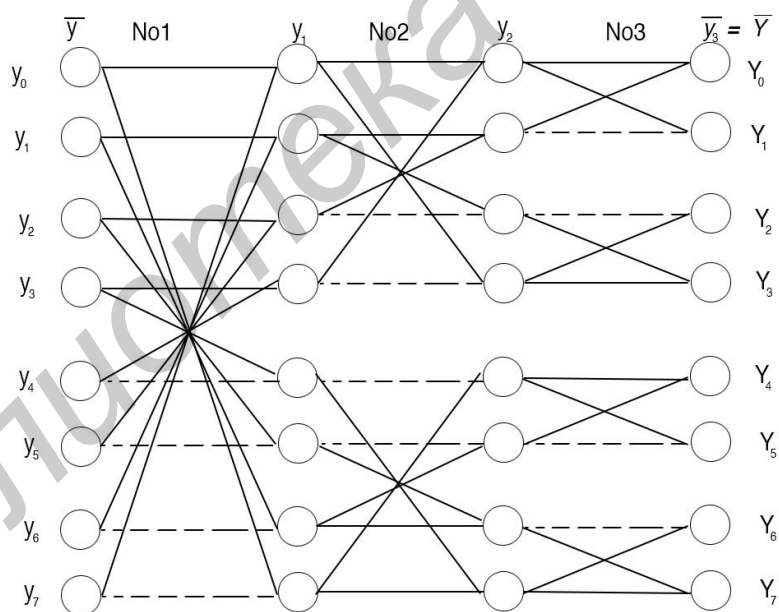


Рисунок 4 - Граф быстрого преобразования Уолша-Трахтмана для вычисления на местах

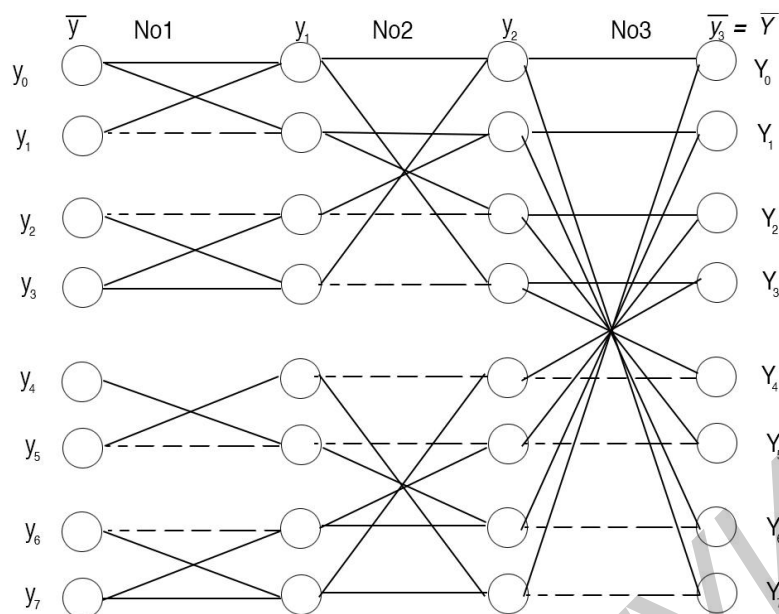


Рисунок 5 - Граф быстрого преобразования Уолша-Трахтмана для вычисления на местах (второй вариант)

Разложение матрицы Уолша-Трахтмана в соответствии с быстрым преобразованием Уолша-Трахтмана будет выглядеть [21]:

$$W' = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$

Легко удостовериться, что все коэффициенты разложения матрицы имеют свои ненулевые элементы, расположенные в симметричной структуре.

На основе этого метода получены два варианта алгоритма быстрого преобразования Уолша в системе упорядочений Уолша-Пэли, которые относятся к «замечательным» алгоритмам. Эти алгоритмы быстрого преобразования Уолша обладают свойствами симметрии, их граф для любой размерности может быть легко получен. Используя этот метод можно получить и другие замечательные алгоритмы быстрых преобразований Уолша.

Кодовые последовательности максимальной длины определяются как M-последовательности.

Двоичные M-последовательности играли и играют особо важную роль в радиотехнических системах, их свойства были изучены достаточно глубоко, в том числе и характеристические многочлены. В литературе [20], приведены таблицы содержащие не нулевые коэффициенты c_n неприводимых многочленов.

Число M-последовательностей Q определяется формулой:

$$Q = \varphi(N)/k, \quad (17)$$

где $\varphi(N)$ – функция Эйлера (число чисел в ряду $1, 2, \dots, N - 1$ взаимно простых с числом N),

$N = p^k - 1$, k – число разрядов в сдвигающем регистре. Если N – простое число, то $\varphi(N) = N - 1$.

M-последовательность является циклическим кодом PM-1. Между собой они связаны перестановкой символов. Для выявления этой связи рассматриваются процессы формирования обоих кодов при помощи порождающей матрицы G. Основное отличие состоит в том, что для порождающей матрицы кода PM-1 используются все элементы поля и они расположены в порядке возрастания.

В качестве порождающей матрицы циклического кода PM-1 используется циклическая группа поля Галуа.

Для перехода от одной системы упорядочения к другой производится перестановка столбцов матрицы Уолша. Она может быть использована для преобразования псевдослучайной последовательности в Уолш-последовательность. В общем случае, если выбрать n диадных линейно независимых значений $y(j)$ ($1, 2, \dots, 2^n - 1$), $j = 1, 2, \dots, n$ на определенных позициях, тогда любая перестановка типа $2^n - 1$ будет сформирована [29].

Теорема 1: Существует $\left(\binom{2^n - 1}{1} \binom{2^n - 2}{2} \dots \binom{2^n - 2^{n-1}}{n-1} \right)$ перестановок $t \rightarrow g$ ($g = 1, 2, \dots, 2^n - 1$) таких, что каждая последовательность Уолша (длинной равной 2^n) может быть преобразована в другую последовательно Уолша [27].

Следует следующий метод построения $\left(\binom{2^n \times 2^n}{1} \right)$ матрицы Уолша.

Пусть ее элементы:

$$w_{st} = (-1)^{\sum_{j=0}^{n-1} s_j g(t)_j} ; 0 \leq s, t \leq 2n-1 \quad (18)$$

$$s = s_{n-1} s_{n-2} \dots s_1 s_0, t = t_{n-1} t_{n-2} \dots t_1 t_0$$

Набор $g(t) = g(t_{n-1} t_{n-2} \dots t_1 t_0) = g(t_{n-1} 00 \dots 0) + g(0 t_{n-2} \dots 00) + \dots + g(00 \dots 0 t_0)$

Для данного ключевого числа

$g(t_{n-1} 00 \dots 0), g(0 t_{n-2} \dots 00), \dots, g(00 \dots 0 t_0) \in \{1, 2, \dots, 2^n - 1\}$ должен быть

двухэлементен и линейно независим.

Это перестановка, $t \rightarrow g(\leftarrow)$, также называется Уолш-сдвигом. Все различные упорядоченные матрицы Уолша являются лишь результатом перестановки $t \rightarrow g(\leftarrow)$.

Если $g(t_{n-1} 00 \dots 0), g(0 t_{n-2} \dots 00), \dots, g(00 \dots 0 t_0) = 00 \dots 0 t_0$,

тогда $g(t) = g(t_{n-1} t_{n-2} \dots t_0)$

$$w_{st} = (-1)^{\sum_{j=0}^{n-1} s_j t_j}$$

Это стандартная форма последовательности Адамара.

Если $g(\leftarrow_{n-1} 00 \dots 0) = t_{n-1} 00 \dots 0, g(\leftarrow_{n-2} 0 \dots 0) = 0 t_{n-2} 0 \dots 0, \dots, g(\leftarrow_0 00 \dots 0 t_0) = 00 \dots 0 t_0$,

тогда $g(\leftarrow) = t_{n-1} t_{n-2} \dots t_0 = t$ и $w_{st} = (-1)^{\sum_{j=0}^{n-1} s_j t_j}$ представляет собой упорядочение Адамара.

В соответствии со схемой рассмотренной ранее, $x \xrightarrow{\text{Операция}} y$ обозначает что, после некоторой операции t -ая строка из X будет $g(\leftarrow)$ -ой строкой Y , это эквивалентно генерированию X через перестановку строк Y , $t \rightarrow g(\leftarrow)$. Тогда для симметричного Уолш-сдвига (что и есть специальная перестановка) операция в той схеме также эффективна только для инвертированных строк.

Например (для $n = 3$) $H \xrightarrow{GC, BI, GI, BI} T$

H -система (Адамара) $g(\leftarrow_2 00) = t_2 00, g(\leftarrow_1 0) = 0 t_1 0, g(\leftarrow_0 0 t_0) = 00 t_0$. В

соответствии с этим для T -системы

К примеру ($n=3$) $H \xrightarrow{GC, BI, GC, BI} T$

$$t_2 00 \xrightarrow{GC} t_2 t_2 0 \xrightarrow{BI} 0 t_2 t_2 \xrightarrow{GC} 0 t_2 0 \xrightarrow{BI} 0 t_2 0 = g^*(t_2 00)$$

$$0 t_1 0 \xrightarrow{GC} 0 t_1 t_1 \xrightarrow{BI} t_1 t_1 0 \xrightarrow{GC} t_1 0 t_1 \xrightarrow{BI} t_1 0 t_1 = g^*(0 t_1 0)$$

$$00 t_0 \xrightarrow{GC} 00 t_0 \xrightarrow{BI} t_0 00 \xrightarrow{GC} t_0 t_0 0 \xrightarrow{BI} 0 t_0 t_0 = g^*(00 t_0)$$

Тогда получим :

$$g^*(000) = 000, g^*(001) = 011, g^*(010) = 101, g^*(011) = 110, g^*(100) = 010,$$

$$g^*(101) = 001, g^*(110) = 111, g^*(111) = 100$$

T-система может быть получена из N системы этой перестановкой столбцов.

Существует $(2^n - 1) \times (2^n - 1)$ перестановок $t \rightarrow y$ ($n = 1, 2, \dots, 2^n - 1$), таких что каждая последовательность Уолша с удаленным первым символом (длина = $2^n - 1$) может быть преобразована в псевдослучайную последовательность [3].

Метод построения $(2^n - 1) \times (2^n - 1)$ матрицы H' .

Пусть ее элементы будут

$$h'_{st} = (-1)^{\sum_{j=0}^{n-1} s_j y(t)_j} ; 1 \leq s, t \leq 2^n - 1 \quad (19)$$

$$s = s_{n-1} s_{n-2} \dots s_0,$$

$$y(t) = y(t)_{n-1} y(t)_{n-2} \dots y(t)_0; s_j, y(t)_j \in \{0, 1\}$$

В которой:

$$y(t) = \sum_{j=1}^n \oplus y(t - jc_j)$$

« c_j » - коэффициент неприводимого полинома

$$q(x) = \sum_{j=0}^n c_j x^j = 1 + \sum_{j=1}^n c_j x^j$$

Начальные значение в этом уравнении $y_0, y_1, \dots, y_n \in \{0, 1, \dots, 2^n - 1\}$ должны быть диадными линейно независимыми. Понятно, что для каждого s, h'_{st} будет псевдослучайной последовательностью ($n = 1, 2, \dots, 2^n - 1$) генерированные примитивным полиномом $q(x)$ степени n .

Для Уолш-последовательности с удаленным первым символом

$$w'_{st} = (-1)^{\sum_{j=0}^{n-1} s_j t_j}, \quad 1 \leq s, t \leq 2^n - 1.$$

В соответствии с уравнениями получаем перестановку $t \rightarrow y$, которая может осуществлять преобразование Уолш-последовательности в псевдослучайную последовательность. Обычно, обратная перестановка $x \rightarrow y^{-1}$ преобразуемая псевдослучайную последовательность имеет практическое применение.

$$s = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

$$P_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \end{pmatrix}$$

Перестановки

t	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
y(t)	1	2	4	8	3	6	12	11	5	10	7	14	15	13	9

Рисунок 3.1 – M-последовательность в последовательность Уолша в системе упорядочений Уолша-Пэли

$$s = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

$$H_s = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \end{pmatrix}$$

Перестановки

t	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
y(t)	8	1	2	1	12	6	3	13	10	5	14	7	15	11	9

Рисунок 3.2 – M-последовательность в последовательность Уолшав системе упорядочений Уолша-Адамара

$$s = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

$$H_+ = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \end{pmatrix}$$

Перестановки

t	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
y(t)	1	3	7	15	2	4	8	13	6	12	5	11	10	9	14

Рисунок 3.4 – M-последовательность в последовательность Уолшав системе упорядочений Уолша-Качмажа

$$s = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} \quad A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 \end{pmatrix}$$

Перестановки

t	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
y(t)	15	8	11	10	7	3	1	13	4	2	12	9	6	14	5

Рисунок 3.5 – M-последовательности в последовательность Уолша в системе упорядочений Уолша-Трахтмана

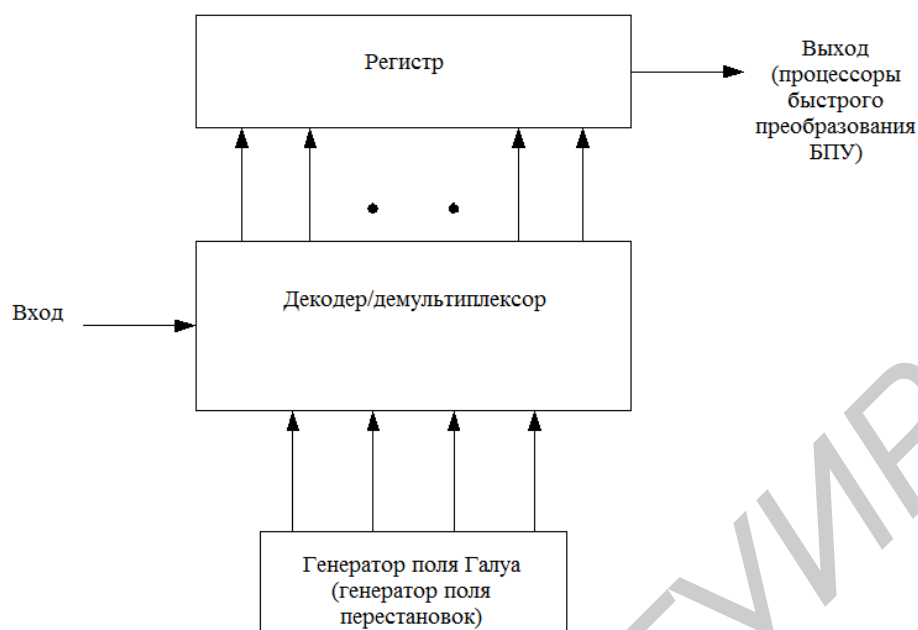


Рисунок 3 - Блок схема преобразования М-последовательности в функции Уолша.

Генератор поля Галуа определяет через декодер/демультиплексор, в какую ячейку памяти (регистр) должен быть записан каждый бит полученного сообщения (вектора).

Для реализация двух полученных алгоритмов перестановок символов исходной последовательности в схеме на рисунке 3 необходимо заменить генератор поля Галуа конечным дискретным автоматом, выполняющим генерацию последовательности заданного вида.

М-последовательность используется для синхронизации и помехоустойчивого кодирования информации [20]. В приемном устройстве при синхронизации решается задача обнаружения и распознавания сигнала, а при декодировании – задача распознавания. В основе обработки сигнала при решении этих двух задач лежит базовый алгоритм вычисления корреляционного вектора принятого сигнала и опорной М-последовательности. Для синхронизации необходимо найти величину временного сдвига принятого сигнала относительно опорного сигнала. Поэтому принятый сигнал умножается на матрицу циклических сдвигов М-последовательности S и по положению максимального значения корреляционного вектора находится величина сдвига. При декодировании принятый сигнал умножается на матрицу всех возможных кодовых слов A . От матрицы S она отличается иным расположением строк и наличием дополнительной строки, состоящей из одних единиц. В матрице A строками являются М-последовательности, расположенные в порядке возрастания двоичного числа, образованного информационными символами.

При декодировании М-последовательности достаточно выполнить

перестановку ее символов, дополнить первым нулевым символом, а результат умножить на матрицу Уолша. Далее в корреляционном векторе находится максимум, номер которого в двоичном виде представляет собой информационные символы.

Для синтеза требуемых генераторов поля перестановок в зависимости от используемого упорядочения функций Уолша представим в табличном виде выходные сигналы автомата в зависимости от входного потока, в качестве которого будем использовать последовательность синхронизирующих импульсов. В качестве базиса выберем JK-триггеры, как наиболее универсальные элементы, что позволит получить более простую комбинационную схему.

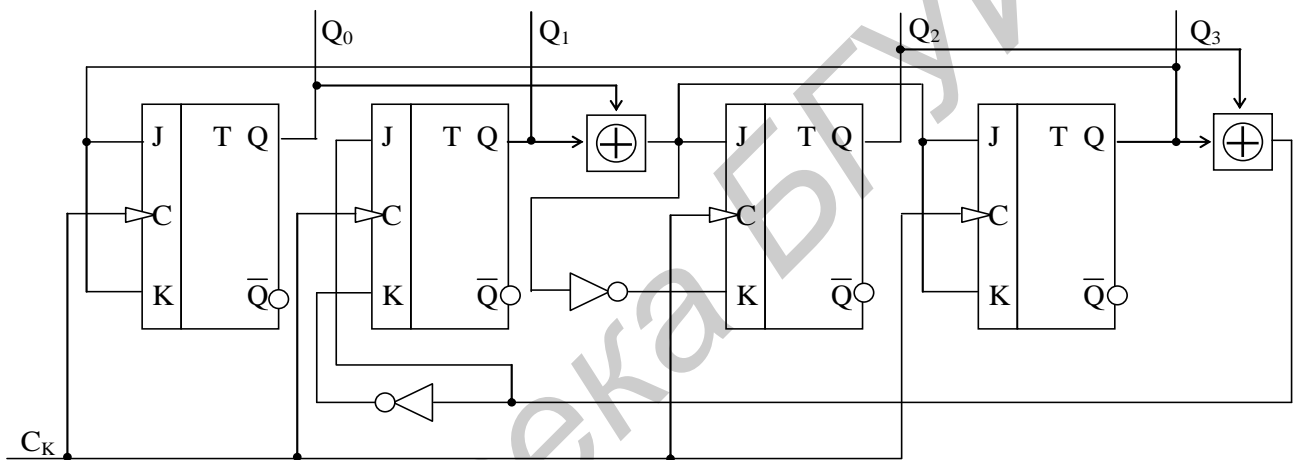


Рисунок 4 – Схема генератора поля перестановок элементов M-последовательности для использования упорядочения функций Уолша по Трахтману

Синтез генератора поля перестановок для функций Уолша, в системе упорядочений по Пэли и Адамару

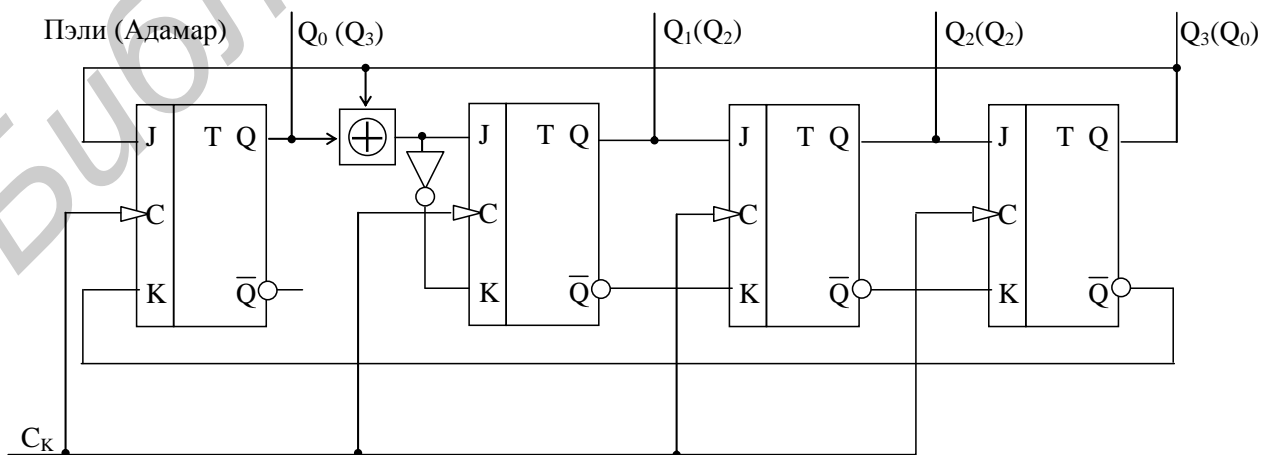


Рисунок 5 – Схема генератора поля перестановок элементов M-последовательности для использования упорядочения функций Уолша по Пэли и Адамару

ЗАКЛЮЧЕНИЕ

В ходе выполнения магистерской работы рассмотрены все системы упорядочения, показана взаимосвязь между М-кодами и функциями Уолша в различных системах упорядочения.

В результате выполнения работы был разработан метод извлечения алгоритмов быстрых спектральных преобразований в базисе Уолша для различных систем упорядочений, основанный на представлении элементов матриц Уолша в экспоненциальной или показательной форме. На основе этого метода получены два варианта алгоритмов быстрого преобразования Уолша в системе упорядочений Уолша-Пэли, которые относятся к «замечательным» алгоритмам. Эти алгоритмы быстрого преобразования Уолша обладают свойствами симметрии, их граф для любой размерности может быть легко получен. Граф быстрого преобразования Уолша имеет все одинаковые итерации, что дает определенное преимущество при осуществлении вычислений мгновенного спектра по Уолшу.

Рассмотренный метод получения алгоритмов быстрого преобразования Уолша может быть использован в различных системах упорядочений.

Используя этот метод можно получить и другие замечательные алгоритмы быстрых преобразований Уолша. В магистерской работе установлены основные принципы преобразования М–последовательности в последовательность Уолша в различных системах упорядочения функций Уолша. Такими системами упорядочения являются системы Адамара, Пэли, Качмажа и Трахтмана. Преобразование М–последовательности в последовательность Уолша осуществляется с помощью определенных перестановок и в работе определены эти перестановки.

Быстрое преобразование дает возможность использовать быстрое декодирование корректирующих кодов. Практической частью данной работы является синтез перестановочных генераторов во всех системах упорядочения функций Уолша. Это позволяет использовать дополнительную гибкость при реализации быстрых декодеров. Данная задача является актуальной для современных систем передачи и обработки информации, реализуемых на микро- и наноэлектронных устройствах.

СПИСОК СОБСТВЕННЫХ ПУБЛИКАЦИЙ

1. Дворникова Т.Н., Новиков Е.В. Использование программных средств в учебном процессе / НТК, Новые информационные технологии в телекоммуникациях и почтовой связи, ВГКС, 2006.
2. Дворникова Т.Н. Методы защиты информации / НТК, Новые информационные технологии в телекоммуникациях и почтовой связи, ВГКС, 2008.
3. Дворникова Т.Н. Защита информации в системах обработки данных / Международная НТК, Современные средства связи, ВГКС, 2006.
4. Дворникова Т.Н. СОРМ в сетях NGN / Международная НТК, Современные средства связи, ВГКС, 2010.
5. Дворникова Т.Н. Стандарт DMR / Международная НТК, Современные средства связи, ВГКС, 2011.
6. Дворникова Т.Н. BLADE-Серверы / Международная НТК, Современные средства связи, ВГКС, 2011.
7. Дворникова Т.Н. Выбор решения для технологической профессиональной радиосвязи / Международная НТК, Современные средства связи, ВГКС, 2012.
8. Дворникова Т.Н. Применение платформы ADL-800 в учебном процессе / Международная НТК, Высшее техническое образование: проблемы и пути развития, БГУИР, 2013.
9. Схемотехника аналоговых и цифровых устройств: учеб.-метод. пособие / Дворникова Т.Н., Будько А.А. – Минск, БГУИР, 2013. – 156 с.: ил.
10. Цифровые и микропроцессорные устройства. Лабораторный практикум на базе пакета программ «Electronics Workbench»/ Дворникова Т.Н. – Минск: УО ВГКС, 2010 – 60 с.
11. Информатика и информационные технологии. Сборник практических заданий для студентов ССО / Дворникова Т.Н. Минск: УО ВГКС, 2010 – 58 с.
12. Введение в радиоэлектроник. Лабораторный практикум : учеб.-метод. пособие / Дворникова Т.Н. – Минск, БГУИР, 2016. – 84 с.: ил.
13. Дворникова Т.Н., Гарасюк В.С. Цифровое ТВ / НТК, Радиотехнические системы, БГУИР, 2013.
14. Дворникова Т.Н., Соловьев Ю.М. Node.JS – Серверный Javascript / НТК, Радиотехнические системы, БГУИР, 2013.
15. Дворникова Т.Н. OFDM модуляция в системах передачи данных / Международная НТК, Современные средства связи, ВГКС, 2014.
16. Дворникова Т.Н., Будько А.А. ЭУМКД «СА и ЦУ», БГУИР, 2014.
17. Дворникова Т.Н., Мурашкина З.И. О целесообразности выполнения

курсовой работы на первом курсе при переходе на систему образования 4+2/ XIX Международная научно-методическая конференции, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. Ульянова (Ленина), 2015.

18. Дворникова Т.Н., И.С. Болотник, О.М. Сильченко Нейронные компьютеры и сети/ Международная НТК, Современные средства связи, ВГКС, 2015.

19. Дворникова Т.Н., Гриб Н.В., Журок Е.В. Моделирование вычислителя веса двоичного кода/ Международная НТК, Современные средства связи, ВГКС, 2015

20. Дворникова Т.Н. Моделирование вычислителя веса двоичного кода/ Международная НТК, Современные средства связи, ВГКС, 2015.

21. Дворникова Т.Н., Будько А.А Алгоритмы быстрого преобразования Уолша/ Белорусско-Российская НТК, Технические средства защиты информации, БГУИР, 2016.