Министерство науки и высшего образования Российской Федерации

Федеральное государственное образовательное учреждение высшего профессионального образования

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

А.М. ГОЛИКОВ

ИССЛЕДОВАНИЕ ЦИКЛИЧЕСКИХ ИЗБЫТОЧНЫХ КОДОВ CRC

Учебно-методическое пособие по лабораторной работе

Томск 2019

Голиков, А. М. Исследование циклических избыточных кодов CRC: Учебно-методическое пособие по лабораторной работе [Электронный ресурс] / А. М. Голиков. — Томск: ТУСУР, 2019. — 13 с.

В лабораторной работе проводится циклических избыточных кодов CRC на основе разработки программы для моделирования такой системы в среде МАТЛАБ. Лабораторная работа предназначен для направления подготовки магистров 11.04.02 "Инфокоммуникационные технологии и системы связи" по магистерским программам подготовки: "Радиоэлектронные системы передачи информации", "Оптические системы связи и обработки информации", "Инфокоммуникационные системы беспроводного широкополосного доступа", "Защищенные системы связи", для направления подготовки магистров 11.04.01 "Радиотехника" по магистерской программе подготовки: "Радиотехнические системы и комплексы", "Радиоэлектронные устройства передачи информации", "Системы и устройства передачи, приема и обработки сигналов", "Видеоинформационные технологии и цифровое телевидение" и специалитета 11.05.01 "Радиоэлектронные системы и комплексы" специализации "Радиолокационные системы и комплексы", "Радиоэлектронные системы передачи информации", "Радиоэлектронные системы космических комплексов", а также бакалавриата направления 11.03.01 "Радиотехника" (Радиотехнические средства передачи, приема и обработки сигналов), бакалавриата 11.03.02 Инфокоммуникационные технологии и системы связи (Системы мобильной связи, Защищенные системы и сети связи, Системы радиосвязи и радиодоступа, Оптические системы и сети связи) и может быть полезна аспирантам.

ОГЛАВЛЕНИЕ

1 Введение

Циклический избыточный код (CRC - Cyclic redundancy check). Наиболее известными из методов обнаружения ошибок передачи данных являются [1]:

- *Посимвольный контроль чётности*, называемый также поперечным, подразумевает передачу с каждым байтом дополнительного бита, принимающего единичное значение по чётному или нечётному количеству единичных бит в контролируемом байте. Посимвольный контроль чётности прост как в программной, так и в аппаратной реализации, но его вряд ли можно назвать эффективным методом обнаружения ошибок, так как искажение более одного бита исходной последовательности резко снижает вероятность обнаружения ошибки передачи. Этот вид контроля обычно реализуется аппаратно в устройствах связи.
- *Поблочный контроль чётности*, называемый продольным. Схема данного контроля подразумевает, что для источника и приёмника информации заранее известно, какое число передаваемых символов будет рассматриваться ими как единый блок данных. В этой схеме контроля для каждой позиции разрядов в символах блока (поперёк блока) рассчитываются свои биты чётности, которые добавляются в виде обычного символа в конце блока. По сравнению с посимвольным контролем чётности, поблочный контроль чётности обладает большими возможностями по обнаружению и даже корректировке ошибок передачи, но всё равно ему не удаётся обнаруживать определённые типы ошибок.
- *Вычисление контрольных сумм*. В отличие от предыдущих методов, для метода контрольных сумм нет чёткого определения алгоритма. Каждый разработчик трактует понятие контрольной суммы по-своему. В простейшем виде контрольная сумма – это арифметическая сумма двоичных значений контролируемого блока символов. Но этот метод обладает практически теми же недостатками, что и предыдущие, самый главный из которых – нечувствительность контрольной суммы к чётному числу ошибок в одной колонке и самому порядку следования символов в блоке.
- *Контроль циклически избыточным кодом* – CRC. Это гораздо более мощный и широко используемый метод обнаружения ошибок передачи информации. Он обеспечивает обнаружение ошибок с высокой вероятностью. Кроме того, этот метод обладает рядом других полезных моментов, которые могут найти своё воплощение в практических задачах.

2. Теоретическая часть

Циклический избыточный код (англ. Cyclic redundancy code, CRC) – алгоритм вычисления контрольной суммы, предназначенный для проверки целостности передаваемых данных. Алгоритм CRC обнаруживает все одиночные ошибки, двойные ошибки и ошибки в нечётном числе бит. Понятие циклических кодов достаточно широкое, однако на практике его обычно используют

для обозначения только одной разновидности, использующей циклический контроль (проверку) избыточности.

Главная особенность значения CRC состоит в том, что оно однозначно идентифицирует исходную битовую последовательность и поэтому используется в различных протоколах связи, а также для проверки целостности блоков данных, передаваемых различными устройствами. Благодаря относительной простоте алгоритм вычисления CRC часто реализуется на аппаратном уровне.

При передаче пакетов по сетевому каналу могут возникнуть искажения исходной информации вследствие разных внешних воздействий: электрических наводок, плохих погодных условий и многих других. Сущность методики в том, что при хороших характеристиках контрольной суммы в подавляющем числе случаев ошибка в сообщении приведёт к изменению его контрольной суммы. Если исходная и вычисленная суммы не равны между собой, принимается решение о недостоверности принятых данных, и можно запросить повторную передачу пакета.

Основная идея алгоритма CRC состоит в представлении сообщения в виде огромного двоичного числа, делении его на другое фиксированное двоичное число и использовании остатка этого деления в качестве контрольной суммы. Получив сообщение, приёмник может выполнить аналогичное действие и сравнить полученный остаток с «контрольной суммой».

На рисунках 1 и 2 изображено графическое представление кодирования и декодирования CRC-кода:

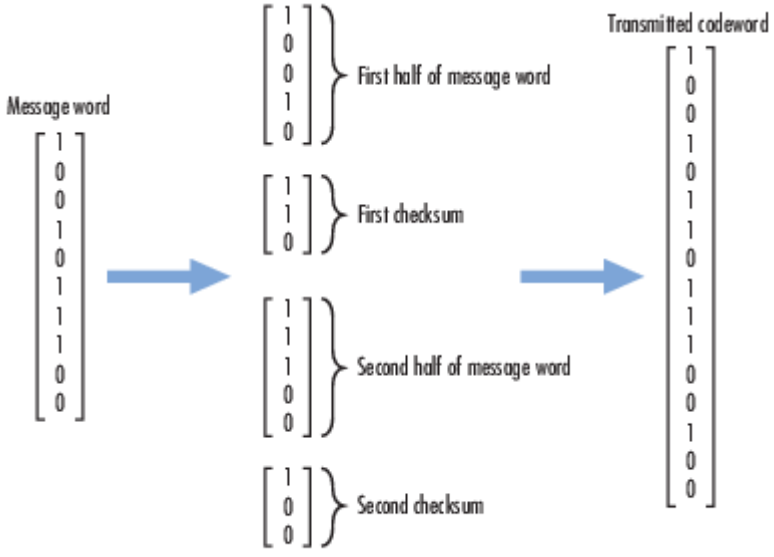

Рис. 1 - Принцип работы кодера CRC

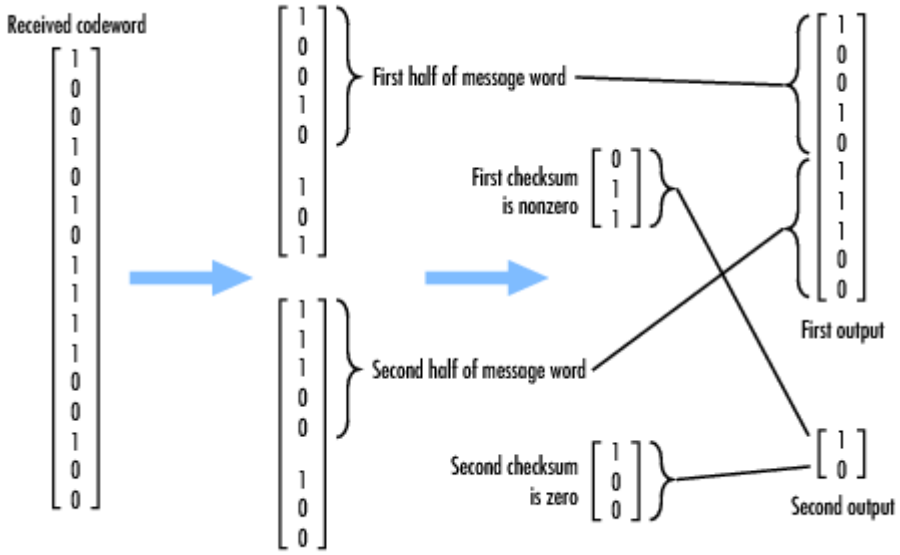

Рис. 2 - Принцип работы декодера CRC

Степенью CRC-полинома *W* называют позицию самого старшего единичного бита. Например, степень полинома 10011_2 равна 4.

Для вычисления CRC используют полиномиальную арифметику. Вместо представления делителя, делимого (сообщения), частного и остатка в виде положительных целых чисел, можно представить их в виде полиномов с двоичными коэффициентами или в виде строки бит, каждый из которых является коэффициентом полинома.

Например, десятичное число 23 в 16-ричной и 2-ичной системах будет иметь вид $23_{10}=17_{16}=10111_2$, что совпадает с полиномом: $1\cdot x^4+0\cdot x^3+1\cdot x^2+1\cdot x^1+1\cdot x^0$ или упрощённо: $x^4+x^2+x^1+1$.

И сообщение, и делитель могут быть представлены в виде полиномов, с которыми можно выполнять любые арифметические действия без переносов.

Как правило, контрольная сумма добавляется к исходному сообщению и полученное расширенное сообщение передаётся через канал связи.

На другом конце канала приёмник может сделать одно из возможных действий (оба варианта совершенно равноправны):

1. Выделить текст полученного сообщения, вычислить для него контрольную сумму и сравнить её с переданной.

2. Вычислить контрольную сумму для всего переданного сообщения, и посмотреть, получится ли в результате нулевой остаток.

Поскольку исходное сообщение может быть очень большим (до нескольких Мбайтов) и так же из-за того, что для получения CRC используется CRC-арифметика, использовать обычную компьютерную операцию деления нельзя.

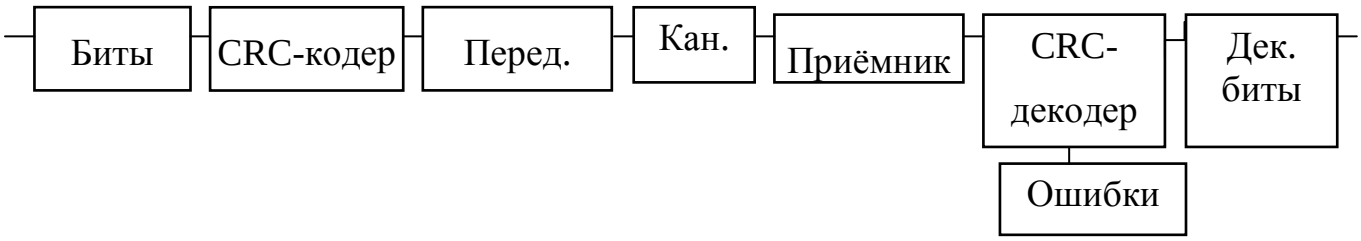

Рис. 3 - Обобщенная структурная схема исследования CRC кодов

Самый популярный и рекомендуемый IEEE полином для CRC-32 используется в Ethernet, FDDI; также этот многочлен является генератором кода Хемминга. Использование другого полинома — CRC-32C — позволяет достичь такой же производительности при длине исходного сообщения от 58 бит до 131 кбит, а в некоторых диапазонах длины входного сообщения может быть даже выше — поэтому в наши дни он тоже пользуется популярностью. К примеру, стандарт ITU-T использует CRC-32C с целью обнаружения ошибок в полезной нагрузке.

Ниже в таблице перечислены наиболее распространённые многочлены — генераторы CRC:

Таблица 1. Распространённые полиномы CRC кодов

Название	**Полином**
CRC-1	$x+1$ (используется в аппаратном контроле ошибок, также известен как бит чётности)
CRC-4-ITU	x^4+x+1
CRC-5-ITU	$x^5+x^4+x^2+1$
CRC-5-USB	x^5+x^2+1
CRC-6-ITU	x^6+x+1
CRC-7	x^7+x^3+1 (системы телекоммуникации, ITU-T G.707, ITU-T G.832, MMC, SD)
CRC-8	$x^8 + x^7 +x^6+ x^4+x^2+1$
CRC-16-IBM	$x^{16}+x^{15}+x^2+1$ (Bisync, Modbus, USB, ANSI X3.28)
CRC-16-CCITT	$x^{16}+x^{12}+x^5+1$ (X.25, HDLC, XMODEM, Bluetooth, SD)
CRC-30(CDMA)	$x^{30}+x^{29}+x^{21}+x^{20}+x^{15}+x^{13}+ x^{12}+ x^{11}+ x^8+ x^7+ x^6+ x^2+ x+1$

3 Практическая часть.

Виртуальная модель передачи данных с обнаружением ошибок при помощи CRC-кода была реализована в среде Simulink Matlab. Модель демонстрирует работу CRC-кодера и декодера, позволяет исследовать обнаруживающую способность кода для разных генераторных полиномов.

На рисунке 4 приведена разработанная модель:

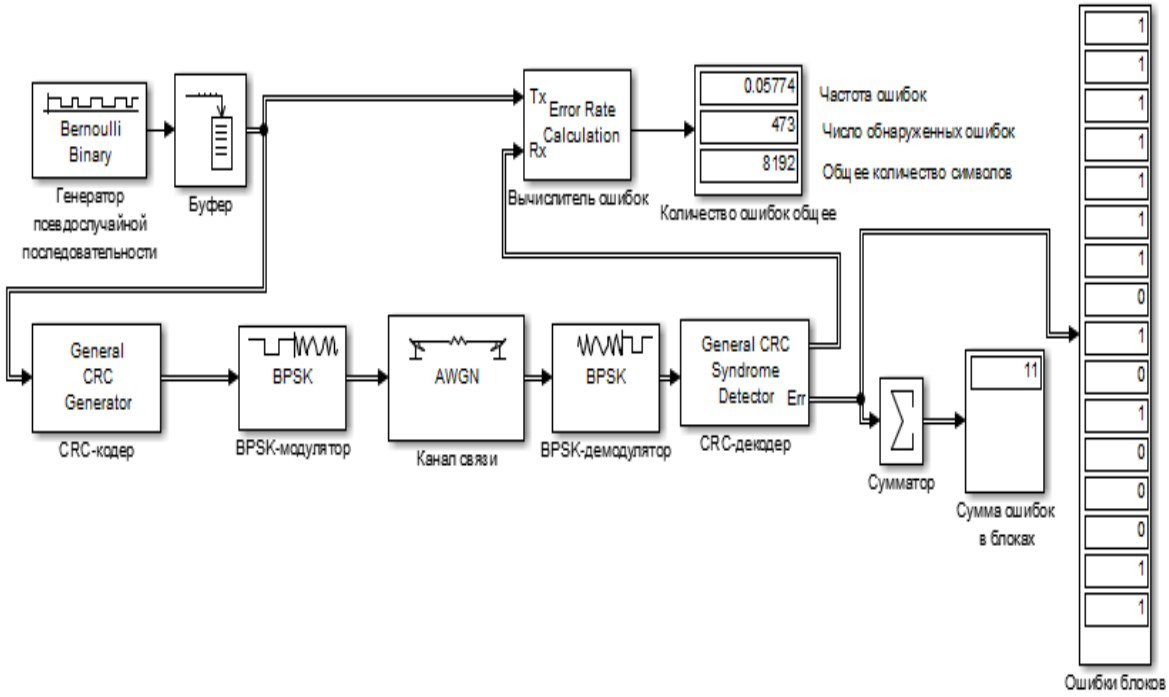

Рис. 4 - Разработанная модель исследования CRC-кодов

В её основу положены следующие элементы, встроенные в библиотеку Simulink:

- Bernoulli Binary Generator;
- General CRC Generator;
- BPSK Modulator Baseband;
- AWGN Channel;
- BPSK Demodulator Baseband;
- General CRC Syndrome Detector;
- Error Rate Calculation;
- Buffer;
- Add;
- Display (Дисплей, отражающий ошибки).

Далее представлено описание основных блоков:

Bernoulli Binary Generator (генератор псевдослучайной последовательности) – генерирует случайную бинарную последовательность (рисунок 3.59).

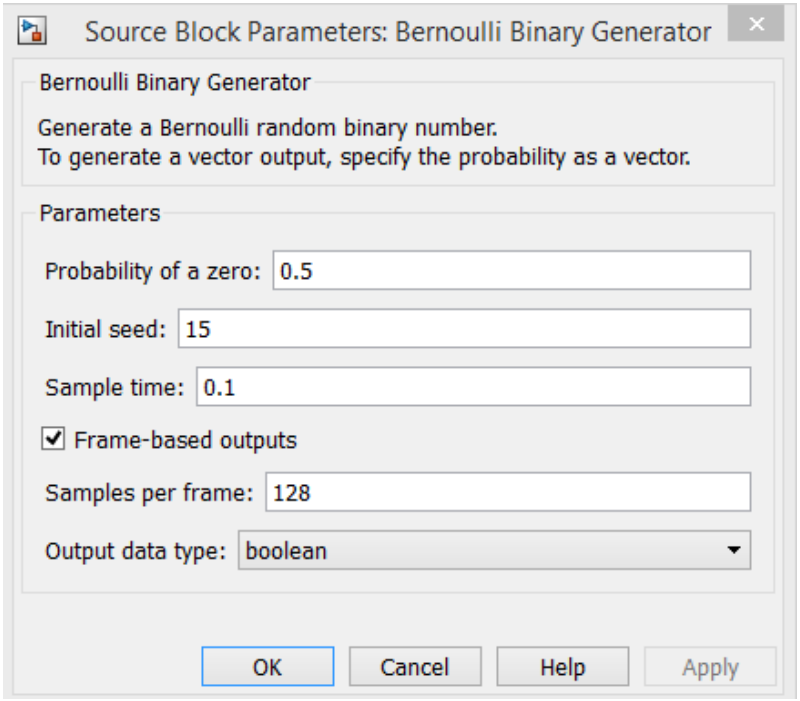

Рис. 5 - Параметры блока «Bernoulli Binary Generator»

«Probability of a zero» - вероятность появления нуля;
«Initial seed» - начальное значение для генерации;
«Sample time» - длительность сэмпла;
«Samples per frame» - размер фрейма.
General CRC Generator (CRC-кодер) – циклический избыточный кодер.
«Generator polynomial» - генераторный полином, может быть задан в 3 формах:
1) В обычной записи, например: x^3 + x^2 + x + 1.
2) в виде матрицы-строки с указанием степеней с ненулевыми коэффициентами, например: [4 1 0] = x^4 + x + 1.
3) в виде матрицы-строки с указанием нулевых и ненулевых коэффициентов, например: [1 1 0 1 1] = x^4 + x^3 + x + 1.

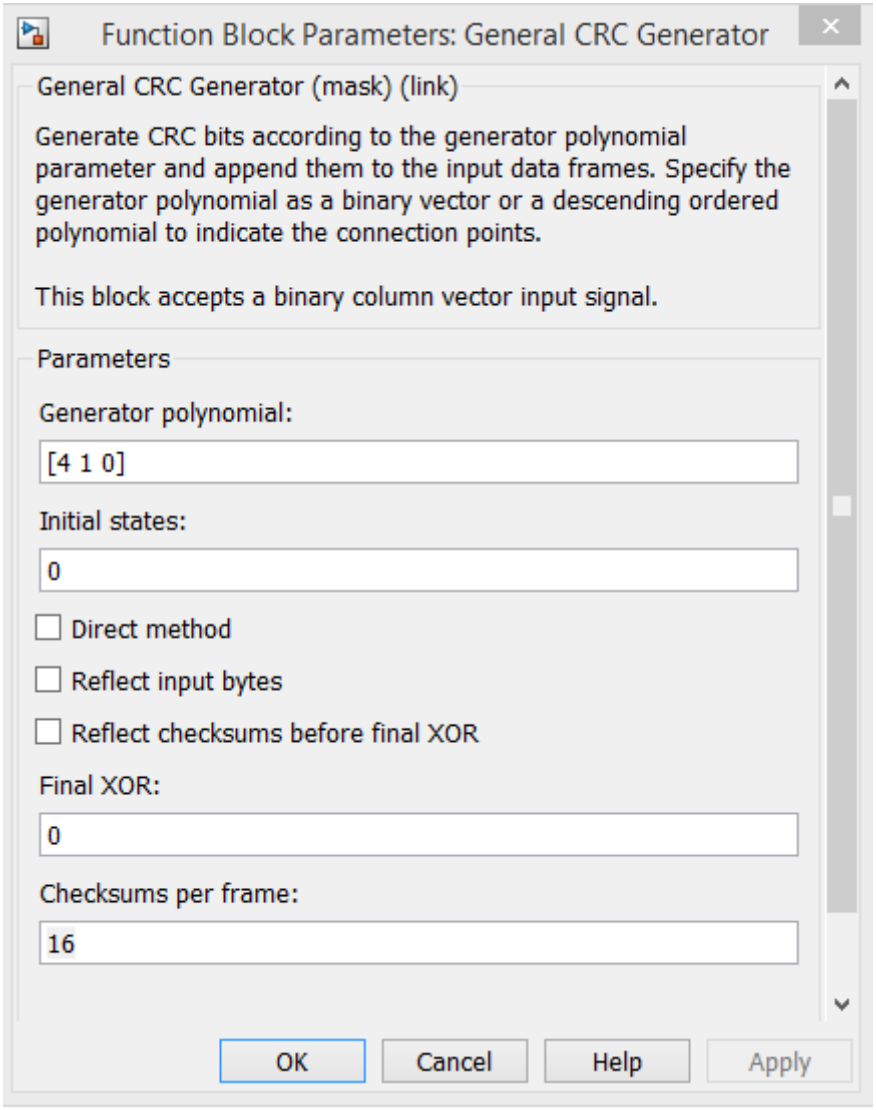

Рис. 6 - Параметры блока «General CRC Generator»

«Initial states» - начальное состояние сдвиговых регистров.

«Direct method» - включение прямого метода вычисления CRC, иначе работает по табличному методу.

«Reflect input bytes» - инвертировать входной поток.

«Reflect checksums before final XOR» - инвертировать контрольные суммы перед конечной операцией XOR.

«Final XOR» - Выполнить операцию XOR в конце кодирования.

«Checksums per frame» - количество контрольных сумм во фрейме.

BPSK Modulator Baseband – BPSK модулятор.

BPSK Demodulator Baseband – BPSK демодулятор.

AWGN Channel (Канал связи) – добавляет «белый» гауссовский шум в канале (рисунок 3.61).

«SNR» - задаёт отношение сигнал/шум в канале.

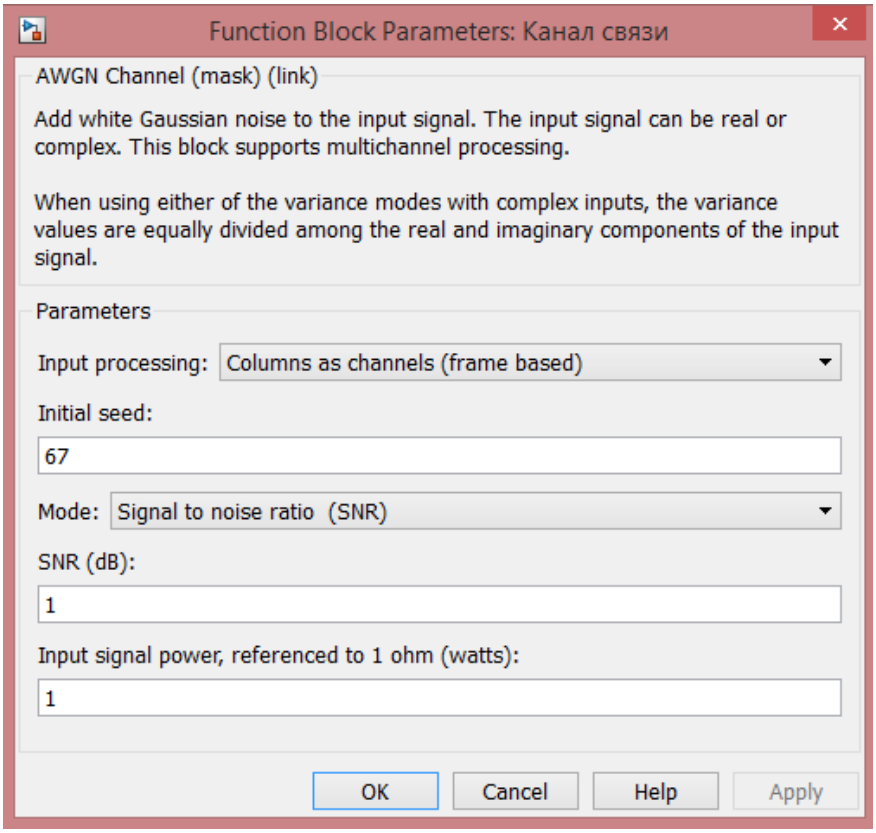

Рис. 7 - Параметры блока «AWGN»

General CRC Syndrome Detector - циклический избыточный декодер. Все параметры декодера задаются аналогично параметрам блока «General CRC Generator» (рисунок 3.3).

Error Rate Calculation – вычислитель ошибок между переданной и принятой последовательностью.

Buffer – буфер. Переводит последовательность бит в один блок.

Add (сумматор) – суммирует ошибки от CRC-декодера.

Display - дисплей, отражающий ошибки.

Результаты моделирования

Исследование циклического избыточного кода

Модель циклического избыточного кода (crc), разработанная представленная на рисунке 4, позволяет исследовать обнаруживающую способность CRC кодов с различными полиномами.

Задаём одинаковый генераторный полином в блоки CRC-кодер и CRC-декодер:

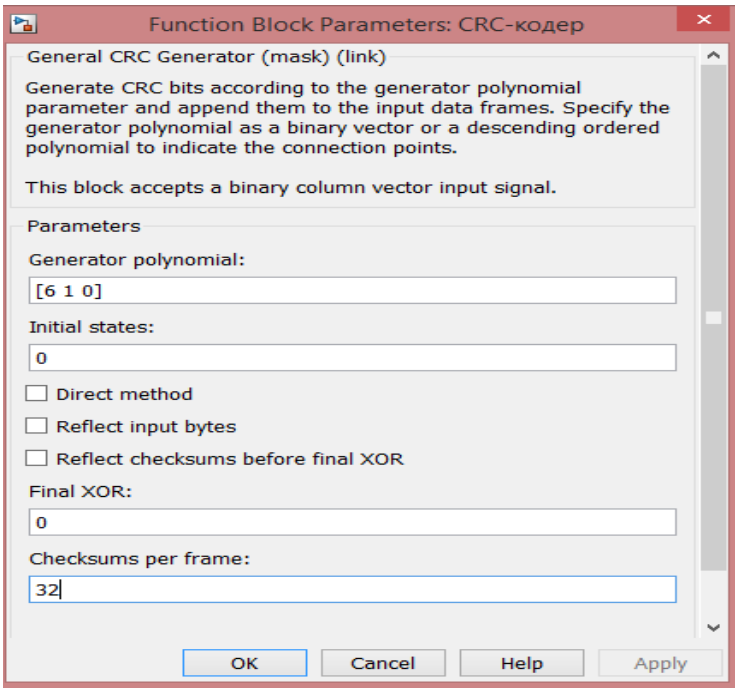

Рис. 8 - Параметры блока CRC-кодер

Общее число передаваемых символов составляет 8192. Количество контрольных сумм изменяется от 2 до 8192, с увеличением каждого предыдущего значения в 2 раза (2, 4, 8, 16…8192).

Значение SNR в блоке «Канал связи» установлено в 1 дБ. Таким образом, битовая вероятность ошибки (BER) составит 0,05786.

На рисунке 9 представлен график зависимости числа обнаруженных ошибок от числа контрольных сумм для различных полиномов CRC-кода.

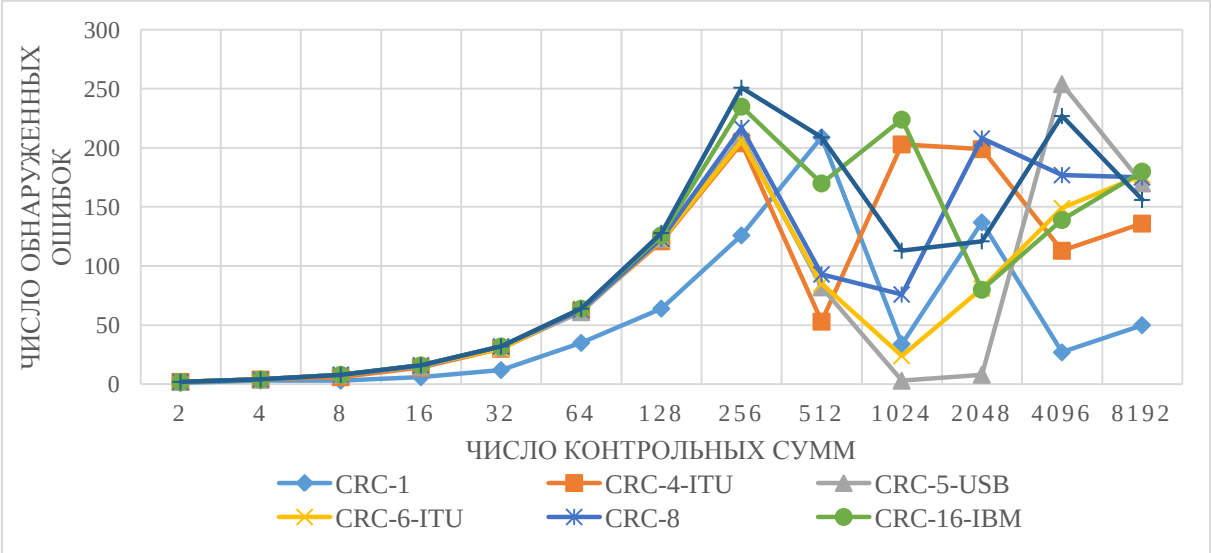

Рис. 9 - График зависимости числа обнаруженных ошибок от числа контрольных сумм для различных полиномов CRC-кода

В данном разделе проведено исследование модели циклического избыточного кода (CRC).

Модель позволяет исследовать CRC-коды с возможностью задания любого генераторного полинома и изменении количества контрольных сумм во фрейме.

Получены следующие результаты и сделаны следующие выводы:

1) чем выше степень полинома, тем лучше его обнаруживающая способность;

2) для каждого полинома есть такое число контрольных сумм в блоке, при котором его обнаруживающая способность максимальна, причём у всех полиномов эти точки различны.

Однако, при выборе полинома CRC-кода также необходимо учитывать и другие факторы:

1) увеличение степени полинома приводит к усложнению реализации кодера и декодера;

2) чем выше частота вычисления контрольных сумм, т.е. чем больше контрольных сумм добавляется в блок данных, тем меньше пропускная способность канала;

3) CRC-коды используют для обнаружения ошибок, что означает наличие канала переспроса. При выборе между кодом CRC/каналом переспроса и помехоустойчивым кодированием, необходимо учитывать характеристики канала связи. При большом числе ошибок передача данных будет невозможна.

4) Выбор полинома зависит от размера передаваемого блока данных, чем больше блок – тем выше степень полинома необходимо подбирать. Таким образом, существует ограничение на размер блока данных, иначе в любом блоке на приёмном конце будет обнаруживаться ошибка.

ЛИТЕРАТУРА

1. Голиков А.М. Модуляция, кодирование и моделирование в телекоммуникационных системах. Теория и практика: Учебное пособие / А.М. Голиков. - СПб.: Издательство «Лань», 2018. – 452с.