Вопросы применения CRC-контроля для повышения помехоустойчивости телекоммуникационных систем

П. Н. Ерлыков

Петербургский государственный университет путей сообщения Императора Александра I

petrerlikov@mail.ru

Н. С. Ерлыков

Петербургский государственный университет путей сообщения Императора Александра I

nikolaysergeevich.yerlikov@mail.ru

Ю. Я. Меремсон

Петербургский государственный университет путей сообщения Императора Александра I

meremson@list.ru

Аннотация. **В статье описано применение CRC-алгоритма по схеме Горнера. Показаны достоинства и недостатки CRC-алгоритма. Сделаны предложения по улучшению работы CRC-алгоритма.**

Ключевые слова: CRC-алгоритм, схема Горнера, полином, остаток, делимое, делитель, займ

I. Постановка задачи

В [1] было показано, что при CRC-контроле с использованием схемы Горнера может возникнуть повторяемость остатков. Естественно, чем чаще повторяются остатки (то есть – контрольные числа, по которым выполняется оценка правильности принятой информации), тем хуже выполняется сам контроль передачи информации.

Применение CRC-контроля с использованием схемы Горнера описано в [2, 3, 4].

Рассмотрим возможности применения алгоритмов CRC-контроля с использованием схемы Горнера.

На передающем пункте можно по алгоритму CRC вычислять остаток передаваемого на приемный пункт сообщения (числа) и передавать остаток на приемный пункт. На приемном пункте по аналогичному алгоритму CRC, выполненному над полученным сообщением (числом) должен быть тоже получен свой остаток.

Если остатки, полученные как на передающем пункте, так и на приемном пункте совпадают, то сообщение можно считать с известной долей вероятности – правильным.

Однако, часто, возможно, для повышения скорости передачи информации, CRC-контроль выполняется по-другому.

На передающей стороне к концу сообщения, предназначенному для передачи, добавляется количество нулей, равное ширине полинома. Это сообщение (число) по мере передачи на приемный пункт обрабатывается по схеме Горнера CRC-алгоритмом с получением определенного остатка. Полученный остаток, разрядность которого равна той же ширине полинома, остается при передаче сообщения в конце младших разрядов передаваемого кодового слова (числа) как раз на месте ранее добавляемых нулей. На приемный пункт по каналу связи поступает уже сообщение (кодовое слово – число) с этим остатком.

На приемном пункте обработка CRC-алгоритмом по схеме Горнера такого видоизмененного сообщения должна давать в остатке ноль.

Равенство остатка нулю является основанием, с определенной долей вероятности считать, что передачи и прием информации выполнены правильно.

По нашему мнению, принимать нулевое состояние того или иного регистра в качестве основания правильности передачи информации не очень хорошо потому, что регистр может обнулиться случайно из-за ошибки в устройствах автоматики, не имеющей ничего общего ни с передачей, ни с контролем передачи информации. Оставим это мнение при себе и будем дальше рассматривать данный вариант CRC-контроля.

На первый взгляд обнуление остатка при выполнении приведенных операций не выглядит слишком очевидным и вот почему.

Если бы при выполнении CRC-контроля выполнялось бы обычное классическое деление по схеме Горнера, то для исключения остатка, передаваемое сообщение нужно было бы увеличить настолько, чтобы частное на приемной стороне выросло на единицу и оказалось бы без остатка.

Не нужно забывать при использовании CRC-алгоритмов используется не классический алгоритм Горнера, а схема Горнера с поразрядным вычитанием с отбрасыванием займов.

С учетом этого рассмотрим такую догадку: чтобы отнять от суммы какое-нибудь число, можно отнять двукратную величину этого числа, а однократную прибавить.

В этом случае автоматическое получение среднего остатка вместо числа нулей, прибавленных с младшей стороны контролируемого числа при передаче числа с передающего пункта, приобретает следующий смысл.

Средний остаток в любом случае содержит если и не все единицы, что может в частном случае, то какую-то комбинацию нулей и единиц.

Образование каждой единицы среднего остатка происходит при вычитании единицы из нуля в соответствующем разряде с образованием отброшенного займа, вдвое превышающего вес этой единицы.

Поэтому при образовании всего среднего остатка за счет поразрядного образования каждой из его единиц с помощью отбрасывания займа возникает определенная дополнительная часть всей суммы отброшенных займов.

Эта дополнительная часть, естественно, вдвое превышает вес образованного среднего остатка.

Таким образом, при образовании среднего остатка фактическое делимое дополнительно увеличилось на удвоенную величину среднего остатка.

Например, если средний остаток равен числу 1101 (13), то фактическое делимое увеличилось при его образовании дополнительно на 26 единиц.

Это значит, что при обработке такого числа на приемном пункте CRC-алгоритмом фактическое делимое должно уменьшиться на эту же величину с тем, чтобы произошло возвращение прежнего остатка, равного четырём нулям.

Именно это и происходит на приемном пункте за счет того, что при вычитании единиц полинома из среднего остатка в соответствующих разрядах не происходит образования отбрасываемых займов.

Эта сумма не возникших отбрасываемых займов как раз и составляет ту величину, которая дополнительно возникала на передающей стороне при образовании среднего остатка.

В нашем примере эта сумма составляет 26 единиц. На эту величину происходит уменьшение фактического делимого, и деление выполняется без остатка с возвращением в виде остатка прибавленных на передающей стороне четырех нулей.

И кстати частное при этом останется прежней величиной.

Именно такая операция и происходит на приемной стороне при обработке числа с полученным на передающей стороне средним остатком при обработке числа с добавленными нулями CRC-алгоритмом.

А происходит это следующим образом.

Веса отброшенных займов превышают вдвое веса тех разрядов, за счет которых они возникали на передающей стороне.

Значит, суммарный вес исчезнувших займов вдвое превысит величину среднего остатка.

А это, в свою очередь, на двойную величину среднего остатка уменьшит величину фактического делимого.

Значит, с одной стороны делимое, пришедшее в пункт приема, увеличено на двойную величину среднего остатка, а с другой стороны уменьшено за счет уменьшения суммы отброшенных займов на двойную величину этого среднего остатка.

Поясним сказанное примером.

Допустим, что ширина полинома, равна четырём. Допустим, что на месте четырёх нулей появился новый остаток, равный двоичному числу 1101, то есть равный десятичному числу 13.

Повторим, что это число остатка появляется на месте добавленных со стороны младших разрядов четырёх нулей, то есть оно появляется вместо числа 0000. Но ведь единица в любом из четырёх разрядов могла бы появиться лишь в результате поразрядного вычитания единицы полинома из одного из этих четырёх нулей. А это значит, что при каждом из таких поразрядных вычитаний единицы из нуля образовывался и отбрасывался займ с весом в два раза большим, чем вес того разряда, в котором появилась единица.

Значит, в нашем примере возникнут следующие отброшенные займы: с весом 16 (от единицы остатка с весом 8), с весом 8 (от единицы остатка с весом 4) и с весом 2 (от единицы остатка с весом 1). Сумма этих отброшенных займов составляет число: (16+8+2), равное 26-ти, что, естественно, в два раза больше появившегося остатка, равного 13-ти.

Получается, что делимое уже на передающей стороне из-за отбрасывания этих трёх займов увеличилось на двукратную величину полученного и посланного вместе с сообщением остатка.

На приемном пункте при обработке CRC-алгоритмом этого сообщения со средним остатком за счет наличия единиц среднего остатка на месте нулей сумма отброшенных займов уменьшится как раз на величину 26, вдвое превышающую величину среднего остатка, что эквивалентно уменьшению фактического делимого как раз до той величины, которую оно составляло на передающей стороне при добавленном нулевом остатке.

Поэтому деление будет выполнено без остатка.

II. Выводы

Первым недостатком применения CRC-алгоритма является увеличение кратности остатка (так называемой результирующей контрольной суммы) из-за отбрасывания займов по сравнению с обычным делением того же числа на тот же порождающий полином.

Однако очевидно, что увеличение кратности контрольной суммы снижает вероятность обнаружения других возможных ошибок.

В защиту применения CRC-алгоритма авторы выдвигают простоту реализуемых программ.

Однако ясно, что для реализации этих программ нужно наличие хотя бы микропроцессоров как на передающей, так и на приемной сторонах. А само применение микропроцессоров уже снижает надежность по сравнению с использованием, например, дублирования без применения компьютерной техники.

Однако в этих случаях настолько возрастают сложности применения CRC-алгоритмов и количество избыточной информации, что тем более напрашивается применение дублирования переданных слов с различным кодированием прямых и идентичным им дублирующих слов, без использования компьютерной техники, как на передающей, так и на приемной сторонах.

Дополнительно заметим, что можно, несколько увеличив время передачи сообщения, применять вместо CRC-алгоритма обычное деление.

Для этого достаточно передавать сообщение кадрами, содержащими по два байта сообщения с контрольной суммой (остатком от обычного деления переданного двухбайтового числа на выбранный делитель), при этом проверке на наличие ошибок будут подвергаться каждый раз два байта переданной информации.

Предполагаем, что такой алгоритм проверки при передаче информации не слишком увеличит время передачи, но повысит вероятность обнаружения ошибок при достаточной разрядности делителя. Разрядность делителя можно принимать не большей байта, чтобы не слишком увеличивать время передачи. Очевидно, что при такой проверке не требуется составления специальных программных алгоритмов, которые необходимы при использовании CRC-алгоритмов проверки переданной информации.

И можно передавать на приемный пункт не только остатки от деления, но и частные от деления, что повысит уровень проверки переданной информации.

Список литературы

[1] Ерлыков П.Н, Ерлыков Н.С. Уменьшение числа остатков при CRC-контроле // СПбНТОРЭС, труды ежегодной НТК. 2023. С.187-190.

[2] Горелов Г.В., Фомин А.Ф., Волков А.А., Котов В.К. Теория передачи сигналов. М.: Транспорт, 1999. 415 с.

[3] Ross N. Williams. Элементарное руководство по CRC-алгоритмам обнаружения ошибок. Текст электронный.

[4] Выгодский М.Я. Справочник по элементарной математике. Издание двадцать второе. Москва: Издательство «Наука». Главная редакция физико-математической литературы. 1972 г.