Уменьшение числа остатков при CRC-контроле

Н. С. Ерлыков[1], П. Н. Ерлыков[2]
Петербургский государственный университет Императора Александра I
[1]nikolaysergeevich.yerlykov@mail.ru, [2]petrerlikov@mail.ru

***Аннотация*. В статье описаны виды CRC-алгоритмов. Авторы рассмотрели передаваемые по линии связи сообщения в виде кодовых слов, рассматриваемых при CRC-контроле, в виде двоичных чисел.**

Ключевые слова: CRC-алгоритмы; полиномы; двоичные числа; фактические делимые; займы; остатки; ширина полинома

I. Введение

CRC-коды (Cyclic Redundancy Check – Контроль циклической избыточности) широко применяется для проверки целостности данных, в том числе в беспроводных и проводных линиях связи.

В работе рассмотрен способ «выровненного» сообщения, по которому к концу сообщения в виде «специального» остатка вносится число нулей, равное ширине полинома. Это сообщение обрабатывается при передаче алгоритмом CRC с получением определённого «среднего» остатка и с этим остатком посылается и обрабатывается алгоритмом CRC при приёме с возвратом остатка в виде заданного числа нулей. Авторами показана возможность задавать на передающем пункте и возвращать в пункте приёма не только остаток в виде числа нулей, равного ширине полинома, но и любые «специальные» остатки, разрядность которых равна ширине полинома. При рассмотрении задачи возврата «специальных» остатков авторами использовано в качестве замены любых контролируемых чисел максимально возможное число «нормальных» остатков, то есть таких, которые получались бы при обработке алгоритмом CRC чисел без добавления «специальных» остатков. Такой подход к анализу алгоритмов CRC открывает для разработчика дополнительные возможности CRC-контроля.

I. Постановка задачи

При применении CRC-алгоритмов уменьшается количество различных возможных остатков по сравнению с обычным делением того же числа на тот же полином. Это происходит из-за того, что остаток при CRC-делении должен иметь разрядность на единицу меньшую разрядности полинома, так как числа одинаковой разрядности при применяемой XOR-арифметике не подлежат сравнению по величине.

Для сравнения применения CRC-алгоритмов деления с обычным делением можно, в частности, сравнивать количества возможных вариантов остатка в том и другом случаях. Чем больше это количество, при одном и том же делителе, тем меньше вероятность повторения одинакового остатка.

Можно заметить, что при применении обычного деления, число остатков (с учетом нуля при делении без остатка) равно делителю. Например, при применении в качестве делителя числа 19, число остатков равно 19-ти, начиная с остатка, равного 18-ти, до остатка, равного нулю.

В данном примере число остатков при CRC-делении с учётом остатка, равного нулю, равно 16-ти. Это значит, что вероятность повторений этих остатков при алгоритме CRC деления больше, чем при обычном делении.

На основании сказанного оценку делений можно выполнять, используя сравнение количеств возможных вариантов остатков при CRC-делении и при обычном делении при одинаковом делителе, равном полиному.

Одинаковыми эти остатки могут быть лишь в тех случаях, когда в качестве порождающего полинома взяты только степени числа два, например, 4, 8, 16, 32, 64. В этих случаях применение CRC-деления не отличается от обычного деления. Однако реальные порождающие полиномы никогда не выражают единицей только в одном самом старшем разряде.

Это означает, что проверка ошибочности переданной информации при применении CRC-алгоритмов несколько ниже, чем при применении обычного деления.

II. Примеры решения задачи

В качестве примеров выберем ряд используемых в разных стандартах CRC-полиномов. Для каждого из примеров приведены следующие данные.

- Обозначение алгоритма CRC. Алгоритм всегда обозначается максимальной степенью числа 2 полинома. Часто после этого значения следует название стандарта, в котором применяется данный алгоритм.
- Дальше приведено разложение полинома по степеням «X».
- В следующих скобках приведено двоичное число полинома.
- Далее приведено более подробное обозначение стандарта передачи информации, в котором используется CRC-алгоритм.

В каждом из примеров приведены два максимально возможных числа остатков от деления проверяемой информации. Первое число остатков соответствует обычному делению на число, равное полиному. Второе

число остатков соответствует использованию CRC-деления.

Пример 1. CRC-4 (1 0011). ITU G.704. Порождающий полином равен десятичному числу 19. При обычном делении возможное число остатков равно числу 19. При CRC-алгоритме при максимальном остатке, равном числу 1111 в двоичной форме, возможное число остатков равно 16-ти. Данный полином используется для контроля целостности данных, передаваемых через поток E1 в соответствии со стандартом ITU G.704. Данные имеют размер 2048 бит. Алгоритм позволяет рассчитать коэффициент ошибок потока E1.

Пример 2. CRC-5-EPC (10 1001) Gen 2 RFID. Порождающий полином равен десятичному числу 41. При обычном делении возможное число остатков равно числу 41. При CRC-алгоритме при максимальном остатке, равном числу 1 1111 в двоичной форме, возможное число остатков равно 32-м.

Пример 3. CRC-5-ITU (11 0101) ITU G.704. Порождающий полином равен десятичному числу 53. При обычном делении возможное число остатков равно числу 53. При CRC-алгоритме при максимальном остатке, равном числу 1 1111 в двоичной форме, возможное число остатков равно 32-м.

Пример 4. CRC-5-USB (10 0101) USB token packets.Порождающий полином равен десятичному числу 37. При обычном делении возможное число остатков равно числу 37. При CRC-алгоритме, при максимальном остатке, равном 11111 в двоичной форме, возможное число остатков равно 32-м.

Пример 5. CRC-6-ITU (100 0011) ITU G.704. Порождающий полином равен десятичному числу 67. При обычном делении возможное число остатков равно числу 67. При CRC-алгоритме при максимальном остатке, равном числу 11 1111 в двоичной форме, возможное число остатков равно 64-м.

Пример 6. CRC-7 (1000 1001) Системы телекоммуникации, ITU-T G.707, ITU-T G.832, MMC, SD. Порождающий полином равен десятичному числу 137. При обычном делении возможное число остатков равно числу 137. При CRC-алгоритме при максимальном остатке, равном числу 111 1111 в двоичной форме, возможное число остатков равно 128-ми.

Пример 7. CRC-8-CCITT (1 0000 0111) (ATM HEC), ISDN Header Error Control and Cell Delineation ITU-T I.432.1 (02/99).Порождающий полином равен десятичному числу 263. При обычном делении возможное число остатков равно числу 263. При CRC-алгоритме при максимальном остатке, равном числу 1111 1111 в двоичной форме, возможное число остатков равно 256-ти.

Пример 8. CRC-8-Dallas/Maxim (1 0011 0001) 1-Wire bus.Порождающий полином равен десятичному числу 305. При обычном делении возможное число остатков равно числу 305. При CRC-алгоритме, при максимальном остатке, равном числу 1111 1111 в двоичной форме, возможное число остатков равно 256-ти.

Пример 9. CRC-8 (1 1101 0101) ETSI EN 302 307, 5.1.4. Порождающий полином равен десятичному числу 469. При обычном делении возможное число остатков равно числу 469. При CRC-алгоритме при максимальном остатке, равном числу 1111 1111 в двоичной форме, возможное число остатков равно числу 256.

Пример 10. CRC-8-SAE J1850 (1 0001 1101). Порождающий полином равен десятичному числу 285. При обычном делении возможное число остатков равно числу 285. При CRC-алгоритме, при максимальном остатке, равном числу 1111 1111 в двоичной форме, возможное число остатков равно 256-ти.

Пример 11. CRC-10 (110 0011 0011) Порождающий полином равен десятичному числу 1 587. При обычном делении возможное число остатков равно числу 1 587. При CRC-алгоритме при максимальном остатке, равном двоичному числу 11 1111 1111, возможное число остатков равно 1 024-м.

Пример 12. CRC-11 (1011 1000 0101) FlexRay. Порождающий полином равен десятичному числу 2 949. При обычном делении возможное число остатков равно числу 2 949. При CRC-алгоритме, при максимальном остатке, равном двоичному числу 111 1111 1111, возможное число остатков равно 2 048-ми.

Пример 13. CRC-12 (1 1000 0000 1111) (Системы телекоммуникации. Порождающий полином равен десятичному числу 6 159. При обычном делении возможное число остатков равно числу 6 159. При CRC-алгоритме, при максимальном остатке, равном двоичному числу 1111 1111 1111, возможное число остатков равно 4 096-ти.

Пример 14. CRC-15-CAN (1100 0101 1001 1001) Порождающий полином равен десятичному числу 50 585. При обычном делении возможное число остатков равно числу 50 585. При CRC-алгоритме, при максимальном остатке, равном двоичному числу 1111 1111 1111 1111, возможное число остатков равно 32 768-ми.

Пример 15. CRC-16-IBM (11000 0000 0000 0101) Bisync, Modbus, USB, ANSI X3.28, многие другие; также известен как *CRC-16* и *CRC-16-ANSI*. Порождающий полином равен десятичному числу 98 309. При обычном делении возможное число остатков равно числу 98 309. При CRC-алгоритме, при максимальном остатке, равном двоичному числу 1 1111 1111 1111 1111, возможное число остатков равно 65 536-ти.

Пример 16. CRC-16-CCITT (1 0001 0000 0010 0001) (X.25, HDLC, XMODEM, Bluetooth, SD и др.Порождающий полином равен десятичному числу 69 665. При обычном делении возможное число остатков равно числу 69 665. При CRC-алгоритме, при максимальном остатке, равном двоичному числу 1 1111 1111 1111 1111, возможное число остатков равно числу 65 536-ти.

Пример 17. CRC-16-T10-DIF (1 1000 1011 1011 0111). SCSI DIF. Порождающий полином равен десятичному числу 101 303. При обычном делении возможное число остатков равно числу 101 303. При CRC-алгоритме при

максимальном остатке, равном двоичному числу 1 1111 1111 1111 1111, возможное число остатков равно 65 536-ти.

Пример 18. CRC-16-DNP (1 0011 1101 0110 0101) DNP, IEC 870, M-Bus. Порождающий полином равен десятичному числу 81 253. При обычном делении возможное число остатков равное числу 81 253. При CRC-алгоритме при максимальном остатке, равном двоичному числу 1 1111 1111 1111 1111, возможное число остатков равно 65 536-ти.

Можно рассмотреть аналогично следующие значительно большие числа порождающих полиномов, а именно: полиномы CRC-24, CRC-30, CRC-32 и CRC-64. Однако, ограничимся рассмотренными полиномами и сделаем некоторые выводы.

Для предварительной оценки сравнения вероятностей обнаружения ошибок при обычном делении и использовании CRC-деления можно принять отношение количеств возможных контрольных чисел при одном и том же делителе. В числителе указано возможное число различных остатков при использовании обычного деления. В знаменателе указано число различных остатков при применении алгоритма CRC-деления.

Для первого примера это соотношение равно 19/16. Это и остальные отношения представлены ниже.

Пример 1: 19/16 = 1,19.

Пример 2: 41/32 = 1,28.

Пример 3: 53/32 = 1,65.

Пример 4: 37/32 = 1,16.

Пример 5: 67/64 = 1,05.

Пример 6: 137/128 = 1,07.

Пример 7: 263/256 = 1,03.

Пример 8: 305/256 = 1,19.

Пример 9: 469/256 = 1,83.

Пример 10: 285/256 = 1,11.

Пример 11: 1 587/1 024 = 1,56.

Пример 12: 2 949/2 048 = 1,44.

Пример 13: 6 159/4 096 = 1,50.

Пример 14: 50 585/32768 = 1,82.

Пример 15: 98 309/65536 = 1,50.

Пример 16: 69 665/65 536 = 1,06.

Пример 17: 101 303/65 536 = 1,55.

Пример 18: 81 253/65 536 = 1,24.

Можно показать, что теоретически минимально возможная величина приведенного отношения равна единице. Этот случай соответствует порождающему полиному с единицей только в самом старшем разряде. Однако у любого из порождающих полиномов имеется ещё хотя бы одна единица в другом разряде. Поэтому практическое минимальное отношение может быть немногим больше единицы.

Теоретически максимально возможная величина приведённого отношения может приближаться к двум, но не достигать двух. Это тот случай, когда порождающий полином состоит из единиц во всех разрядах.

Однако, у любого из порождающих полиномов имеются ещё хотя бы несколько нулей в разрядах, кроме самого старшего. Поэтому, практическое максимальное отношение может быть немногим меньше двух. В этом случае больше всего снижается вероятность обнаружения ошибок передачи при использовании CRC-деления по сравнению с обычным делением. Однако, это снижение практически не снижает очень высокой вероятности обнаружения ошибок при CRC-делении.

Видно, что отношение близко к единице для примеров: 5, 6, 7 и 16. В остальных случаях разница использования обычного деления и применения алгоритмов CRC больше, но не превосходит величины 1,82 в примере 14.

При более тщательном знакомстве с использованием CRC-алгоритмов можно узнать, что иногда применяют так называемые «зеркальные» алгоритмы обработки поступающей информации, в других случаях применяют «зеркальные», то есть «отражённые» порождающие полиномы.

«Зеркальная» обработка поступающей с передающего на приёмный пункт информации никак не влияет на приведённые расчёты. На результаты наших расчётов никакие параметры контролируемой информации не влияют.

Что касается использования «зеркальных» полиномов то результаты расчётов, естественно, будут иными. Однако, и в этом случае результаты уложатся в те же выше оговорённые границы отношений.

Объясняется это тем, что при «зеркализации» порождающего полинома младший разряд становится старшим, а старший разряд – младшим. А так как младший разряд всегда равен единице, то степень полинома сохраняется. Кроме того, «зеркализация» не меняет ширины полинома.

Возникает вопрос. Раз созданы программы выполнения этих алгоритмов с использованием компьютерной техники, то почему бы не использовать эту же технику для передачи на приёмный пункт одновременно с «остатком» самого «частного» от деления, тем более, что двоичная разрядность «частного» в ряде случаев меньше разрядности контрольных чисел.

Если выполнять передачу на приёмный пункт частного при использовании алгоритма CRC, то вероятность обнаружения ошибок при передаче информации вырастет.

III. Заключение

Из рассмотренного сравнения возможных чисел остатков можно сделать вывод, что, несмотря на небольшое снижение вероятности обнаружения ошибок при применении алгоритмов CRC по сравнению с обычным делением, их применение имеет неоспоримые преимущества из-за простоты использования, больших скоростей проверки и возможности применения в ряде случаев как на передающей стороне, так и на приёмной микропроцессоров, а не процессоров универсальных или специализированных компьютеров.

В пользу применения этих алгоритмов несомненно также относится специальный подбор порождающих полиномов, наиболее подходящих для контроля конкретной передаваемой информации при применении тех или иных стандартов.

Список литературы

[1] Ross N. Williams. Элементарное руководство по CRC-алгоритмам обнаружения ошибок. [Электронный текст].

[2] Глоссарий простых телекоммуникационных терминов. [Электронный текст].

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