

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
АКАДЕМИЯ ПРОБЛЕМ КАЧЕСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
РОССИЙСКАЯ АКАДЕМИЯ КОСМОНАВТИКИ имени К. Э. ЦИОЛКОВСКОГО
ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР «ИНФОРМАТИКА И УПРАВЛЕНИЕ» РАН
(ВЫЧИСЛИТЕЛЬНЫЙ ЦЕНТР РАН имени А. А. ДОРОДНИЦЫНА)
АО «УПКБ "ДЕТАЛЬ"», АО «РАДИОЗАВОД»,
АО «ФНПЦ «ПО "СТАРТ" имени М. В. ПРОЦЕНКО», АО «НИИЭМП»
АО «ПНИЭИ», АО «НИИФИ», АО «НПП "РУБИН"»
ЕВРАЗИЙСКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ имени Л. Н. ГУМИЛЕВА
ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ



ТРУДЫ
МЕЖДУНАРОДНОГО СИМПОЗИУМА
НАДЕЖНОСТЬ И КАЧЕСТВО

Посвящается 300-летию Российской академии наук

Том 1

ПЕНЗА 2024

**Труды Международного симпозиума НАДЕЖНОСТЬ И КАЧЕСТВО. –
2024. – Т 1. – 498 с.**

Представлены доклады XXIX Международного симпозиума «Надежность и качество», посвященного 300-летию Российской академии наук, проходившего с 27 мая по 1 июня 2024 г. в г. Пензе.

Рассмотрены актуальные проблемы теории и практики повышения надежности и качества; эффективности внедрения инновационных и информационных технологий в фундаментальные научные и прикладные исследования, образовательные и коммуникативные системы и среды, экономику и юриспруденцию; методов и средств анализа и прогнозирования показателей надежности и качества приборов, устройств и систем, а также анализа непараметрических моделей и оценки остаточного ресурса изделий двойного назначения; ресурсосбережения; проектирования интеллектуальных экспертных и диагностических систем, систем управления и связи, интерактивных, телекоммуникационных сетей и сервисных систем; экологического мониторинга и контроля состояния окружающей среды и биологических объектов; исследования физико-технологических процессов в науке, технике и технологиях для повышения качества выпускаемых изделий радиопромышленности, приборостроения, аэрокосмического и топливно-энергетического комплексов, электроники и вычислительной техники и др.

Издание предназначено для студентов, аспирантов, ученых и научных сотрудников, заинтересованных в исследовании надежности и качества эффективных комплексных систем.

УДК 621.396.6:621.315.616.97:658:562

Оргкомитет благодарит за поддержку в организации и проведении Международного симпозиума и издании настоящих трудов Министерство науки и высшего образования РФ, Правительство Пензенской области, Академию проблем качества РФ, Российскую академию космонавтики имени К. Э. Циолковского, Российскую инженерную академию, ФИЦ ИУ РАН (Вычислительный центр РАН имени А. А. Дородницына), АО «УПКБ “ДЕТАЛЬ”», АО «НИИФИ», АО «ПНИЭИ», АО «НПП “РУБИН”», АО «РАДИОЗАВОД», АО «ППО “ЭЛЕКТРОПРИБОР”», АО «ФНПЦ «ПО “СТАРТ” имени М. В. Проценко», АО «НИКИРЭТ», ООО «Экспериментальная мастерская “НаукаСофт”», Евразийский национальный университет имени Л. Н. Гумилева, Пензенский государственный университет.

Издание зарегистрировано в Российском индексе научного цитирования (РИНЦ) с 2005 г.

Редакционная коллегия:

Юрков Н. К. – главный редактор;

Трусов В. А. – ответственный секретарь;

**Гуляков А. Д., Майстер В. А., Северцев Н. А., Сыдыков Е. Б., Абрамов О. В.,
Артамонов Д. В., Безродный Б. Ф., Бецков А. В., Васин С. М., Дивеев А. И., Иофин А. А.,
Каиштанов В. А., Кемалов Б. К., Острейковский В. А., Пиганов М. Н.,
Роберт И. В., Романенко Ю. А., Савченко В. П., Садыхов Г. С., Увайсов С. У.,
Халютин С. П., Шайко-Шайковский А. Г., Шахнов В. А., Якимов А. Н.**

АЛГОРИТМЫ ВЫЧИСЛЕНИЯ ЦИКЛИЧЕСКОГО ИЗБЫТОЧНОГО КОДА

Аннотация. Контрольная сумма в настоящее время используется для выявления ошибок в сообщении, что приводит к увеличению достоверности передаваемой информации. В данной статье рассмотрены некоторые методы расчета контрольной комбинации, сравнение их быстродействия, для чего было написано программное обеспечение на языке программирования C, позволяющее получить информацию о времени подсчета контрольной комбинации.

Ключевые слова: контрольная сумма, достоверность информации, программное обеспечение, язык программирования C

Golovyashkin¹ A.N., Kozin² A.S., Sukhov³ I.V.^{1,2,3} Penza State University, Penza, Russia¹ angpenza@yandex.ru² kozinlesha123@yandex.ru³ suhoviwan2012@mail.ru

CALCULATION ALGORITHMS CYCLIC REDUNDANCY CODE

Annotation. The checksum is currently used to identify errors in the message, which leads to an increase in the reliability of the transmitted information. This article discusses some methods for calculating the control combination, comparing their performance, for which software was written in the C language, which allows you to get information about the time of counting the control combination.

Keywords: checksum, reliability of information, software, C programming language

Введение

Циклический избыточный код *CRC* (*cyclic redundancy code*) или контрольная комбинация – число, вычисленное на основе передаваемого сообщения, которое передается, как правило, в конце этого сообщения. Он нужен для контроля безошибочности (детектирование ошибки) передачи. В большинстве случаев полезной нагрузки оно в себе не несет и с точки зрения передаваемой информации является избыточным. Нахождение *CRC* заключается в делении с остатком информационного полинома – передаваемого сообщения. Остаток и есть *CRC* [1].

Разрядность контрольной комбинации может быть различной, как правило, в степени двойки. Рассчитывать можно различными способами: побитно, таблично, матрично и так далее.

Теоретическая часть

Метод побитового сдвига. В общем виде деление числа на многочлен выполняется по такому алгоритму.

Алгоритм вычисления методом побитового сдвига.

Создается массив (регистр), заполненный нулями, равный по длине разрядности (степени) полинома.

Исходное сообщение дополняется, как правило, нулями в младших разрядах, в количестве, равном числу разрядов полинома.

В младший разряд регистра заносится один старший бит сообщения, а из старшего разряда регистра выдвигается один бит.

Если выдвинутый бит равен "1", то производится инверсия битов (операция *XOR* – исключающее ИЛИ) в тех разрядах регистра, которые соответствуют единицам в полиноме.

Если в сообщении ещё есть биты, переходим к шагу 3.

Когда все биты сообщения поступили в регистр и были обработаны этим алгоритмом, в регистре остаётся остаток от деления, который и является контрольной суммой *CRC*.

Сообщение можно разделить на любое число. Существует ряд стандартных полиномов, которые используются при вычислении *CRC*. Они выбираются экспериментально, таким образом, если сообщение отличается всего несколькими соседними битами, это вызывает большое различие *CRC*. Например, для *CRC16* это может быть 0x8005.

Также при расчётах непосредственно перед выдачей финальную контрольную сумму *CRC* можно поделить на какое-то другое число.

Байты сообщения при записи в регистр могут помещаться как старшим битом «вперёд», так и наоборот, младшим. И результирующая *CRC* также может выдаваться, начиная со старшего бита или с младшего [2].

Табличный метод. Для ускорения расчёта *CRC* используется табличный алгоритм. Его суть состоит в следующем: при выполнении операции *XOR* содержимого регистра с постоянной величиной при различных её сдвигах всегда будет существовать некоторое значение, которое при применении операции *XOR* с исходным содержимым регистра даст тот же самый результат. А значит, можно составить таблицу таких величин, где индексом является исходное содержимое регистра. Эта таблица позволяет значительно ускорить расчёт *CRC* заменой восьми операций сдвига одной операцией поиска по таблице.

Алгоритм вычисления табличным методом.

1. Сдвиг регистра на 1 байт влево с чтением нового байта сообщения.
2. *XOR* старшего байта, только что выдвинутого из регистра с новым байтом сообщения, что даёт индекс в таблице.
3. *XOR* табличного значения с содержимым регистра.
4. Если ещё есть байты данных, перейти к шагу 1.

Есть заранее подготовленные таблицы для определенного образующего полинома.

Выше представленный табличный метод побайтного расчета можно усовершенствовать, сдвигая регистр не на байт, а на слово, на 32 бита, на 64 бита и так далее. Увеличение сдвига ускоряет время расчета, но можно увеличивать не до бесконечности, в какой-то момент шина данных не будет успевать считывать большое количество информации, и дальнейшего ускорения не будет [3].

Экспериментальная часть

Код расчета *CRC* написан на языке *C* в программе *CodeBlocks*. Системные параметры компьютера:

Процессор *AMD fx8320e*;

Объем оперативной памяти – 16 Гб.

Были рассмотрены 4 метода расчета: побитный, табличный со сдвигом на байт, табличный со сдвигом на слово и табличный со сдвигом на 32 бита.

Для примера были выбраны несколько файлов разными объемами. Результаты времени расчета для каждого файла представлены в таблице 1.

Результаты времени расчета *CRC*

Таблица 1

Размер файла	Побитовый метод, мс	Табличный метод (1 байт), мс	Табличный метод (2 байта), мс	Табличный метод (4 байта), мс
0,1 Гб	6344	636	213	161
0,2 Гб	16358	1359	508	365
0,3 Гб	29099	1568	616	379
0,4 Гб	42047	2198	836	569
0,5 Гб	52692	2522	888	614
1,1 Гб	136427	9170	2337	1400
1,5 Гб	157212	16366	3055	2003

Обсуждение результатов

Как видно из таблицы 1, с оптимизацией табличного метода время расчета уменьшается, а процессору, соответственно, нужно меньшее количество тактов для расчета *CRC*. Это приведет к более быстрому реагированию на полученное сообщение, будет увеличиваться производительность, а также понизится энергопотребление. Установлено, что ускорение расчета происходит нелинейно, согласно закону Амдала.

СПИСОК ЛИТЕРАТУРЫ

1. Halsall F. Fifth edition, computer networks and the Internet. Addison-Wesley: Pearson Education, 2005, 803 p.
2. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы. СПб.: Питер, 2008, 958 с.
3. Ромашенко А., Румянцев А., Шень А. Заметки по теории кодирования. 2-е изд., испр. и доп. М.: МЦНМО, 2017, 88 с.