

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.**

УСКОРЕНИЕ ВЫЧИСЛЕНИЯ КОНТРОЛЬНОЙ КОМБИНАЦИИ

Аннотация. Основная идея параллельного алгоритма заключается в полном использовании современных процессоров с точки зрения параллелизма как на уровне команд, так и на уровне потоков. Эти ресурсы используются в алгоритмах для ускорения циклической проверки избыточности (CRC). В данной статье сравниваются между собой некоторые методы расчета контрольной комбинации, а именно сравнивается быстродействие последовательных методов расчета CRC и параллельных алгоритмов.

Ключевые слова: параллельное вычисление, многоядерные системы, многопоточность, контрольная сумма, достоверность информации, алгоритм вычисления CRC

Golovyashkin¹ A.N., Sukhov² I.V., Bannov³ V.Ya., Kozin⁴ A.S.

^{1,2,3,4} Penza State University, Penza, Russia

¹ angpenza@yandex.ru

² suhoviwan2012@mail.ru

⁴ kozinlesha123@yandex.ru

SPEEDING UP THE CALCULATION OF THE CONTROL COMBINATION

Annotation. The main idea of the parallel algorithm is to make full use of modern processors in terms of parallelism at both the command and thread levels. These resources are used in algorithms to speed up cyclic redundancy check (CRC). This article compares some methods of calculating the control combination, namely sequential methods of calculating CRC with a parallel algorithm, and compares their performance.

Keywords: parallel computing, multicore systems, multithreading, checksum, information reliability, CRC calculation algorithm

Современные процессоры расширили возможности параллелизма на уровне команд (ILP) и параллелизма на уровне потоков (TLP). Эти ресурсы используются в алгоритмах для ускорения циклической проверки избыточности (CRC). В данной статье сравниваются между собой некоторые методы расчета контрольной комбинации, а именно последовательные методы расчета CRC с параллельным алгоритмом, сравниваются их быстродействие. Для получения информации о времени подсчета контрольной комбинации быстродействия алгоритмы были реализованы на языке программирования C.

CRC (cyclic redundancy code) – циклический избыточный код, иногда называемый также контрольной суммой. По своей сути – это просто вычисленное на основе исходного передаваемого сообщения число (или можно сказать код), которое передается вместе с самим сообщением (дописывается в конец информационной части) и служит для контроля его без-ошибочной передачи.

Коды циклической проверки избыточности широко используются в цифровых сетях и системах хранения для обнаружения случайных изменений данных во время их передачи или хранения. Например, CRC-32 используется сетевым стандартом IEEE 802.3 (Ethernet) [2] и программами сжатия, такими как Bzip2 и Gzip, для проверки целостности данных. Кроме того, в протоколе передачи управления потоком (SCTP) и интерфейсе интернет-малых компьютерных систем (iSCSI) используется CRC-32C для обнаружения ошибок. Из-за гауссовского шума при передаче, неисправностей жесткого диска и некоторых других причин данные могут быть случайно изменены. CRC демонстрирует хорошее расстояние Хэмминга и обладает хорошей производительностью обнаружения ошибок, что делает его подходящим для обнаружения ошибок. Разрядность CRC может быть различной, как правило, степень двойки.

Расчет CRC можно осуществлять последовательно (побитно, таблично, матрично и т.д) и параллельно. Рассмотрим табличный метод последовательного расчета CRC применяемого для сравнения.

Данный алгоритм позволяет вычислять контрольную сумму побайтно, в отличие от «классического» [3] побитового алгоритма. Суть алгоритма заключается в том, что при последовательном сдвиге данных по байту за итерацию, изменения, которые должны были происходить в течение 8 сдвигов при классическом алгоритме, заносятся в таблицу, на основе которой вычисляется контрольная сумма. При последовательном сдвиге регистра, выдвинутый байт является индексом элемента в рассчитанной таблице, с которым будет складываться по модулю два байт из сообщения (рис. 1). Представленный выше табличный метод побайтного расчета, можно использовать для сдвига 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. Метод параллельного расчета CRC:

Метод параллельного расчета заключается в одновременном чтении нескольких байтов. Однако размер справочной таблицы увеличивается экспоненциально с одновременным считыванием битов, что может привести к тому, что справочная таблица не сможет поместиться в кэш L1. Записи требуются для достижения ускорения за счет чтения 16 бит за раз. Алгоритм с разделением на 4 [4] считывает 32 бита за раз, при этом требования к памяти

оптимизированы для того, чтобы занимать разумные объемы кэша. На каждой итерации, 32-битный фрагмент считывается из буфера данных и разбивается на четыре фрагмента. Затем выполняются четыре поиска в таблице, которые используют эти четыре фрагмента в качестве индексов. Этот алгоритм параллельного вычисления может выполнять поиск по четырем таблицам одновременно. Также этот метод может быть улучшен и осуществлять поиск по 8, по 16 таблицам одновременно.

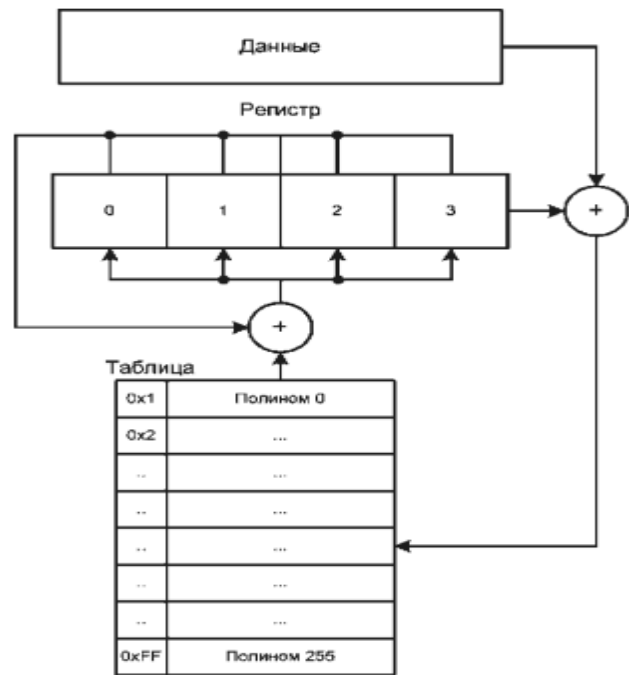


Рисунок 1– Схематичное представление табличного алгоритма

Этот алгоритм делает существующие табличные CRC-алгоритмы пригодными для одновременной обработки нескольких независимых потоков данных, что обеспечивает параллелизм на уровне инструкций. В результате это утраивает и удваивает производительность табличных методов. Этот алгоритм может идеально распараллеливать обычные CRC-алгоритмы, что обеспечивает параллелизм на уровне потоков.

Экспериментальная часть
Код расчета CRC написан на языке C в программе CodeBlocks. Системные параметры компьютера: Процессор AMD fx8320e; Объем оперативной памяти - 16 Гб. Кол-во ядер/потоков: 8 ядер / 8 потоков .

Для сравнения были рассмотрены 3 метода последовательного (табличный со сдвигом на байт, табличный со сдвигом на слово и табличный со сдвигом на 32 бита) и 1 параллельного расчета CRC.

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

Результаты времени расчета CRCТаблица 1

Размер файла	Табличный метод (1 байт), мс	Табличный метод (16 бит), мс	Табличный метод (32 бита), мс	Параллельный метод, мс
0,1 Гб	636	213	161	100
0,2 Гб	1359	508	365	230
0,3 Гб	1568	616	379	270
0,4 Гб	2198	836	569	360
0,5 Гб	2522	888	614	404
1,1 Гб	9170	2337	1400	1150
1,5 Гб	16366	3055	2003	1503

Закключение. Как видно из таблицы 1, параллельный метод вычисляет CRC быстрее последовательных методов, соответственно, нужно меньшее количество тактов для расчета CRC. Таким образом параллельный метод реализованный на многоядерной архитектуре является эффективным алгоритмом расчета CRC. Это приведет к более быстрому реагированию на полученное сообщение, будет увеличиваться производительность, а также понизится энергопотребление. Результаты оценки демонстрируют, что ускорение, достигнутое этим алгоритмом, почти равно количеству используемых потоков.

СПИСОК ЛИТЕРАТУРЫ

- Chi M., He D., Liu J. Exploring various levels of parallelism in high-performance CRC algorithms //IEEE Access. – 2019. – Т. 7. – С. 32315-32326.
- IEEE Standards for Local Area Networks: Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, IEEE Standards 802.3-1985, 1985.
- Chi M., Liu J. VACA: A high-performance variable-length adaptive CRC algorithm //2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). – IEEE, 2017. – С. 1-6.
- Sarwate D. V. Computation of cyclic redundancy checks via table look-up //Communications of the ACM. – 1988. – Т. 31. – №. 8. – С. 1008-1013.