LENDYUK T.V. Knowledge-oriented Information Technology for Design of Adaptive Learning System

Actual task of generation of individual learning path in learning management system using SCORM package is solved. Learning objects metadata enriching in SCORM package with new fields is proposed. It was shown that modern education must adapt to the individual student's characteristics in knowledge control and generation of individual learning path. The generation of individual learning path using the navigation in learning contents with choice of learning objects sequence is proposed.

УДК 581.3

Николайчук Я.Н., Ивасьев С.В., Якименко И.З., Касянчук М.Н.

МЕТОД КОМПАКТНОЙ КОДИРОВКИ ПРОСТЫХ МНОГОРАЗРЯДНЫХ ЧИСЕЛ В ДВОИЧНОЙ СИСТЕМЕ ИСЧИСЛЕНИЯ

Введение. Изучение простых чисел, которые являются ключом к разрешению многих математических проблем и появляются в разных областях математики и ее приложениях, ведется с глубокой древности [1]. Криптография [2], имитационное моделирование, программирование [3], тестирование материнских плат персональных компьютеров – вот далеко неполный перечень современного практического применения простых чисел. Поэтому простые числа интересуют не только математиков, но и некоторые коммерческие организации, а также военных, ввиду их особого использования в области защиты информации [4]. О важности вопроса говорит то, что за поиск больших простых чисел назначены крупные денежные премии.

Криптостойкость большинства асимметричных криптосистем основана на сложности задачи факторизации.Существует отличный от традиционного способ решения этой задачи: не пытаться разложить число на простые сомножители[6], а находить произведения известных простых чисел и сравнивать полученный результат с числом, которое нужно факторизовать [7]. Для такого решения необходимо заранее сгенерировать таблицы простых чисел.

Однако хранение многоразрядных простых чисел, представленных полноразрядными двоичными кодами, является неэффективным в связи с тем, что требует больших объемов памяти.

Обзор литературы. Теорема о распределении простых чисел утверждает, что количество $\pi(n)$ простых чисел на отрезке от 1 к n растет с ростом n, как $\frac{n}{\ln n}$, то есть $\frac{\pi(n)}{n/\ln n} \to 1,\ n \to \infty$ [8, 9]. Оценка объемов памяти, необходимой для хранения простых чисел до 32 разрядов, представляет 4 Гб, до 64 разрядов – 36 Гб, а до 128 – 2^{213} Терабайт. При работе над некоторыми задачами теории чисел разрядность простых чисел может достигать 512 бит, что отвечает чрезвычайно большим объемам необходимой памяти. Например, для хранения объема простых чисел разрядностью до 1024 бит по предварительным оценкам нужно 1048576 байт, так как при сохранении целого числа в двоичной системе используются все байты, которые несут значение числа.

В работе [10] предложен метод компактной кодировки многоразрядных простых чисел (МРПЧ), суть которой заключается в том, что в устройствах памяти запоминается определенное число младших разрядов, а 1 бит используется для идентификации сквозных переносов в старшие разряды. Коды старших разрядов определяются путем подсчета числа переносов, которые идентифицируются битом синхронизации.

Цель работы. Разработка нового метода компактного кодирования и хранения больших массивов МРПЧ и, как следствие, экономия дискового пространства.

Метод компактной кодировки простых многоразрядных чисел. Возможность более компактного хранения МРПЧ может быть реализована за счет избыточности многоразрядных двоичных кодов, поскольку разница между двумя простыми МРПЧ с одинаковыми окончаниями не превышает 10–20 бит. Причем информативная часть простого числа находится в 20–30 битах младших разрядов при идентичности сотен старших битов, начиная с 32–64 бит. Для примера возьмем числа из интервала 2^{20}–2^{64}:

1052629_{10} =10000000111111010101 (2^{20});

2147487701_{10}=10000000000000000000111111010101 (2^{32});

9223372036854779861_{10}=1000000000000000000000000000000000000000000000000000000000111111010101(2^{64}).

В результате проведенного анализа представления простых чисел в двоичной системе исчисления обнаружено, что для чисел с одинаковыми младшими разрядами можно хранить лишь часть битов.

Пусть P_n – числа с одинаковыми младшими разрядами, то есть:

$$P_1 = \sum_{i=1}^{n-1} P_i^1 2^i \text{, где } P_i^1 = 0,1;$$

$$P_2 = \sum_{i=1}^{n-1} P_i^2 2^i \text{, где } P_i^2 = 0,1; \qquad (1)$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$P_n = \sum_{i=1}^{n-1} P_i^n 2^i \text{, где } P_i^n = 0,1.$$

Следовательно, получается разложение чисел в двоичной системе:

$$P_{1(2)}^1 = \left(P_{n-1}^1, P_{n-2}^1, \ldots, P_1^1, P_0^1\right);$$

$$P_{2(2)}^2 = \left(P_{n-1}^2, P_{n-2}^2, \ldots, P_1^2, P_0^2\right); \qquad (2)$$

$$P_{1(2)}^1 = \left(P_{n-1}^1, P_{n-2}^1, \ldots, P_1^1, P_0^1\right).$$

Причем P_3^i; P_2^i; P_1^i; P_0^i, $i = 1,n$ являются одинаковыми. Старшие разряды изменяются очень медленно, в результате чего следует, что их хранить не обязательно, а можно использовать бит синхронизации, который указывает, когда в старшие разряды P_{n-1}^i; P_{n-2}^i; …; P_{n-k}^i, i=1,n надо добавлять 1.

Николайчук Ярослав Николаевич, *д.т.н., профессор, заведующий кафедрой специализированных компьютерных систем Тернопольского национального экономического университета.*

Ивасьев Степан Владимирович, *к.т.н., старший преподаватель кафедры компьютерной инженерии Тернопольского национального экономического университета.*

Якименко Игорь Зиновьевич, *к.т.н., доцент кафедры компьютерной инженерии Тернопольского национального экономического университета.*

Касянчук Михаил Николаевич*, к.ф.-м.н., доцент кафедры компьютерной инженерии Тернопольского национального экономического университета.*

Украина, 46009, г. Тернополь, Тернопольская область, ул. Львовская, 11.

Таблица 1 – Разложение простых чисел с окончанием 0101 в двоичной системе исчисления

Десятичное представление	Двоичное представление			Бит синхронизации
	Верхние разряды числа	7-ми битное окончание числа	Окончание	
142789	1000101	1011100	0101	0
142837	1000101	1011111	0101	0
142949	1000101	1100110	0101	0
142981	1000101	1101000	0101	0
143093	1000101	1101111	0101	0
143141	1000101	1110010	0101	0
143333	1000101	1111110	0101	0
143413	1000110	0000011	0101	1
143461	1000110	0000110	0101	0

Не уменьшая общности, ограничим наши рассуждения анализом 8 бит, то есть от 4-го к n-k-1-му разряду, для которых выполняется условие: $n - k - 5$=8 бит.

В таблице 1 приведен пример разложения кодов простых чисел в двоичной системе исчисленияна группы разрядов и конкатенацию с битом синхронизации.

Разложение МРПЧ происходит согласно такому алгоритму:

1. Вход *P*[0.*j*], Limit;
2. Проверка простоты *P*;
3. Если *P* не простое, то *P*++ шаг 2;
4. *C*[]= *P*[4.11];
5. *P*++;
6. Проверка простоты;
7. Если *Pi*,*j* не простое, то шаг 5;
8. *C*[]= *P*[4.11];
9. *D*[]= *P*[12.*j*];
10. *C*[8]=0;
11. Если *D* ≠ *P*[12.*j*], тогда *C*[8]=1;
12. Запись *C* в файл;
13. Если *P*≠Limit, тогда 7;
14. Выход.

Анализ метода кодировки МРПЧ показывает, что, в сравнении с известными алгоритмами в двоичной системе исчисления, он характеризуется линейно-логарифмической вычислительной сложностью, что позволяет обеспечить экономию дискового пространства. Эффективность разработанного метода сохранения МРПЧ растет с увеличением разрядности чисел, так как используется только один информативный байт для чисел разной разрядности.

Распределение простых чисел не является равномерным, потому проведено исследование распределения простых чисел с одинаковыми окончаниями для выявления сходимости количества простых чисел между битами синхронизации. Таблица 2 иллюстрирует минимальные количества простых чисел между битами синхронизации при растущих разрядностях последовательности простых чисел.

Из анализа таблицы 2 следует, что при обработке всех 32-разрядных простых чисел количество повторений их окончаний не менее 2 (рисунок 1).

Для более детальной оценки эффективности метода на рисунке 2 приведен график, который иллюстрирует количество простых чисел, что находятся между единичными битами синхронизации.

Таблица 2 – Количество минимальных повторений старших битов в зависимости от разрядности простого числа с известным окончанием

Минимальное количество повторений	Разрядность
31	13
24	14
20	16
21	14
19	16
14	17
12	18
11	19
10	20
9	20
7	21
6	23
5	25
4	26
2	26

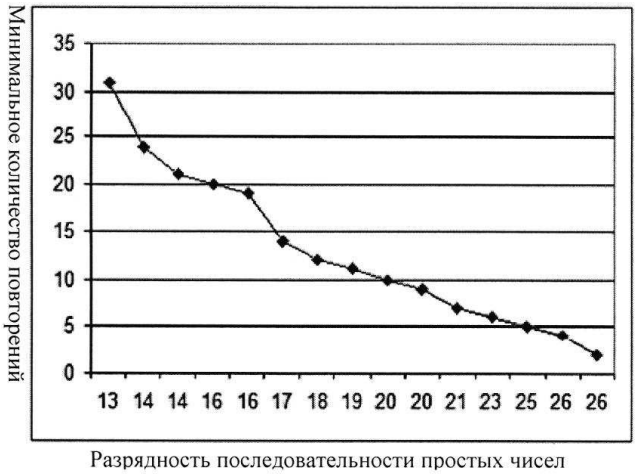

Рисунок 1 – Сходимость последовательности простых чисел между битами синхронизации

Исследования эффективности проведены для схемы, при которой происходит разделение на 4 нижних разряда последовательности простых чисел с одинаковыми окончаниями, следующие 7 бит и

бита синхронизации, количество которых выражает значение верхних разрядов такого разделения.

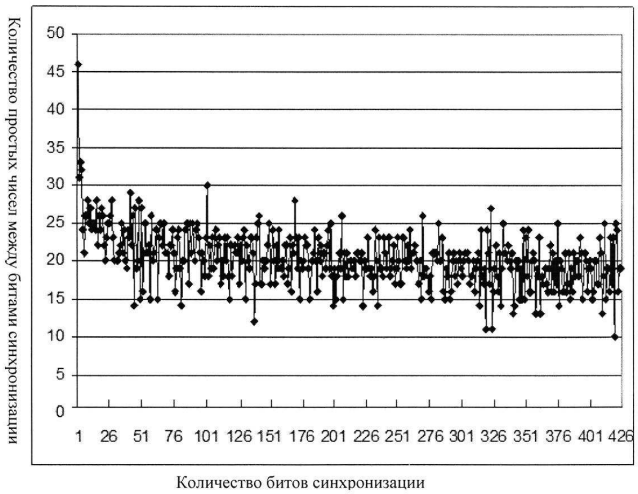

Рисунок 2 – Количество простых чисел между единичными битами синхронизации

Исследования на сходимость количества простых чисел с одинаковыми окончаниями между битами синхронизации показывают, что для эффективного сохранения последовательности МРПЧ, которые больше 64 бит, целесообразно немного изменить схему кодировки, использовав 15 бит младших разрядов из последовательности и бит синхронизации, который будет сопровождать нарастание битов в старших 15 разрядах.

Следовательно, для сохранения последовательности МРПЧ до 1024 битов для каждого простого числа отмеченной разрядности необходимо 128 байт, а при использовании разработанного метода – лишь 2 байта.

Заключение. В работе разработан метод компактного кодирования многоразрядных простых чисел в двоичной системе исчисления, который позволяет существенно увеличить эффективнось сохранения информации, поскольку для записи 32-битного числа используются лишь семибитное окончание и бит синхронизации, что, в свою очередь, приводит к значительной экономии ресурсов памяти.

СПИСОК ЦИТИРОВАННЫХ ИСТОЧНИКОВ

1. Серовайский, С.Я. Простые числа от Пифагора до криптографии / С.Я. Серовайский. – [Электронный ресурс]. – Режим доступа: //http://www.tphs.info/lib/exe/fetch.php/wiki:autor:serov:2006_11_cryptography.pdf // Математика: Республиканский научно-методический журнал. – 2009. – № 1–3. – С. 12–23.
2. Крэндалл, Р. Простые числа. Криптографические и вычислительные аспекты / Р. Крэндалл, К. Померанс. – М.: УРСС, 2011. – 664 с.
3. Уоррен, Г.С. Алгоритмические трюки для программистов / Г.С. Уоррен. – М.: Вильямс, 2007. – 288 с.
4. Минаев, В.А. Безопасность в сфере конфиденциальной информации и закон формирования простых чисел / В.А. Минаев, В.П. Хренов // Спецтехника и связь. – 2008. – № 3. – С. 45–48.
5. Василенко, О.Н.Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. – М.: МЦНМО, 2003. – 328 с.
6. Николайчук, Я.Н. Метод факторизации многоразрядных чисел на основе свойств квадратичности вычетов в системе остаточных классов / Я.Н. Николайчук, С.В. Ивасьев, И.З. Якименко, М.Н. Касянчук // Вестник Брестского государственного технического университета. – № 5 (95). – 2015. – С. 42–45.
7. Каленикова, Н.А. Ускорение факторизации в методе Ферма / Н.А. Каленикова, В.А. Минаев, В.П. Хренов // Вестник Российского нового университета. – №3. – 2010. – С. 12–16.
8. Ингам, А.Э. Распределение простых чисел / А.Э. Ингам. – М.: УРСС, 2005. – 160 с.
9. Бухштаб, А.А. Теория чисел / А.А. Бухштаб. – М.: Просвещение, 1966. – 384 с.
10. Николайчук, Я.Н. Метод сохранения простых многоразрядных чисел в базисе Радемахера / Я.Н. Николайчук, И.З. Якименко, М.Н. Касянчук, С.В. Ивасьев // Труды международной молодежной математической школы «Вопросы оптимизации вычислений». – Киев: Институт кибернетики имени В.М. Глушкова НАН Украины. – 2015. – С. 159–161.

Материал поступил в редакцию 16.01.2017

NYKOLAYCHUKY A.N., IVASIEV S.V., YAKYMENKO I.Z., KASIANCHUK M.N. The method of compact encoding of the simple multi-digital numbers in the binary numerical system

In present work we proposed the method of compact encoding of the simple multi-digital numbers in the binary numerical system, which is compared with known characterized by linear logarithmic computational complexity and should significantly increases the efficiency of keeping information, provide excess of storage space, because for record 32-bit number somebody use only seven-bit edge and bit synchronization.

УДК 004.9

Дубчак Л.О., Кочан В.В., Василькив Н.М.

СРЕДСТВО УСКОРЕННОЙ ОБРАБОТКИ НЕЧЕТКИХ ДАННЫХ НА ОСНОВЕ МЕХАНИЗМА МАМДАНИ

Введение. Математическая теория нечетких множеств и нечеткая логика являются обобщениями классической теории множеств и классической формальной логики. Данные понятия были впервые предложены американским ученым Лотфи Заде в 1965 году [1]. Основной причиной появления новой теории стало наличие нечетких и приближенных рассуждений при описании человеком процессов, систем, объектов.

Основными преимуществами нечетких систем по сравнению с другими является [1, 2]:

- возможность оперировать входными данными, заданными нечетко, например, значениями, которые постоянно меняются во времени (динамические задачи);
- возможность нечеткой формализации критериев оценки и сравнения;

Дубчак Леся Орестовна, *к.т.н., доцент кафедры компьютерной инженерии, факультет компьютерных информационных технологий Тернопольского национального экономического университета.*

Кочан Владимир Владимирович, *к.т.н., профессор кафедры информационно-вычислительных систем и управления, факультет компьютерных информационных технологий Тернопольского национального экономического университета.*

Василькив Надежда Михайловна, *к.т.н., доцент кафедры информационно-вычислительных систем и управления, факультет компьютерных информационных технологий Тернопольского национального экономического университета.*

Украина, 46009, г. Тернополь, Тернопольская область, ул. Львовская, 11.