УДК 004.942

Я.В. ОДАРИЧ, Е.Ю. НАЛИВАЙЧУК, Н.В. НАЛИВАЙЧУК

Национальный технический университет Украины «КПИ», Киев

ВЫЧИСЛЕНИЯ В НЕКАНОНИЧЕСКИХ ГИПЕРКОМПЛЕКСНЫХ ЧИСЛОВЫХ СИСТЕМАХ

Показаны основные отличия и примеры неканонических гиперкомплексных числовых систем. Приведены сравнительные характеристики задачи разделения секрета и его восстановления с использованием канонических и неканонических гиперкомплексных числовых систем различного вида.

***Ключевые слова**: гиперкомплексная числовая система, неканоническая гиперкомплексная числовая система, задача разделения секрета.*

Введение

Множество гиперкомплексных числовых систем можно классифицировать по признаку каноничности, определение которого исходит из произведения пар базисных элементов.

Если для гиперкомплексной числовой системы все такие произведения равняются одному из базисных элементов с коэффициентом из множества $\{-1; 0; +1\}$, то такая система является канонической.

Если же хоть одно из произведений базисных элементов является суммой двух или большего количества слагаемых и/или с коэффициентом, который за пределами множества $\{-1; 0; +1\}$, то такая гиперкомплексная числовая система называется неканонической.

Примером неканонической гиперкомплексной числовой системы является система 3-й размерности, известная как триплексные числа или числа Люша, таблица умножения которых имеет вид, как в табл. 1.

Таблица 1

Таблица умножения триплексных чисел

E_1	E_2	E_3
E_2	$(-E_1 + E_3)/2$	$-E_2$
E_3	$-E_2$	E_1

Поскольку неканонических гиперкомплексных числовых систем бесконечно много, их можно перечислить только с учетом некоторых ограничений, таких как размерность числовой системы, выполнение свойств коммутативности, ассоциативности, правила единичного элемента в базисе, различные ограничения на операции сложения и/или умножения и другие [4].

Так, можно привести примеры таблиц умножения неканонических гиперкомплексных числовых систем 2-й и 4-й размерности, для которых выполняется свойство коммутативности, а также выполняется правило единичного элемента в базисе, указанном в табл. 2, 3.

Таблица 2

Пример таблицы умножения неканонической гиперкомплексной числовой системы 2-й размерности

E_1	E_2
E_2	$E_1 + E_2$

Таблица 3

Пример таблицы умножения неканонической гиперкомплексной числовой системы 4-й размерности

E_1	E_2	E_3	E_4
E_2	$-2E_2 + 2E_3 - 4E_4$	$-4E_1 - 2E_2 - 2E_3$	$-E_3$
E_3	$-4E_1 - 2E_2 - 2E_3$	$2E_2 - 2E_3 + 4E_4$	E_2
E_4	$-E_3$	E_2	$-E_1$

1. Постановка задачи

Известен ряд практических задач, в которых неканонические гиперкомплексные числовые системы нашли свое применение.

Одной из таких задач является задача разделения секрета, для решения и усиления которой могут использоваться неканонические гиперкомплексные числовые системы.

2. Анализ последних исследований и публикаций

Задача разделения секрета и ее решение с использованием канонических гиперкомплексных числовых систем была рассмотрена ранее в некоторых работах [1 – 3].

В настоящее время существует возможность улучшить стойкость данного алгоритма при его моделировании в неканонических гиперкомплексных числовых системах.

Напомним, что для восстановления секрета в гиперкомплексных числовых системах необходимо найти аналог функции Эйлера, которая определена только в вещественных числах.

В качестве такого аналога используются изоморфные переходыв область вещественных чисел на основе фундаментальной теоремы Гаусса и ее модификации [2], а также алгоритм Евклида [1, 3].

Процедура восстановления данных, представленных в неканонических гиперкомплексных числовых системах, с помощью алгоритма Евклида практически не отличается от процедуры восстановления данных представленных в канонических гиперкомплексных числовых системах, за исключением некоторых дополнительных проверок, связанных с получением модуля числа и возможным появлением делителей нуля.

В то же время, используя неканонические гиперкомплексные числовые системы, можно существенно улучшить стойкость схемы разделения секрета.

3. Анализ полученных результатов

3.1 Анализ вычислительной сложности задачи разделения секрета для канонических и неканонических гиперкомплексных числовых систем

Рассмотрим вычислительную сложность задачи разделения секрета для канонических гиперкомплексных числовых систем размерностей n и $n+1$, а также неканонических гиперкомплексных числовых систем размерности n с одной составной и, соответственно, $(n-1)^2$ составными ячейками табл. 4). При этом предполагается, что у данных числовых систем единичный элемент в базисе.

Таблица 4

Вычислительные сложности задачи разделения секрета и его восстановления в различных системах

	Разделение секрета (вычисление вычета)	Восстановление секрета с помощью алгоритма Евклида
Каноническая гиперкомплексная числовая система размерности n	$O(4n^2 + n * n!)$	$O(7n^2 + n + n * n! + Ln(m * (4n^2 + 4n + n * n!)))$
Каноническая гиперкомплексная числовая система размерности $n+1$	$O(4n^2 + 4n + 4 + (n+1)(n+1)!)$	$O(7n^2 + 15n + 8 + (n+1)(n+1)! + Ln(m * (4n^2 + 12n + 8 + (n+1) * (n+1)!)))$
Неканоническая гиперкомплексная числовая система размерности n с одной составной ячейкой	$O(4n^2 + 4n - 4 + n * n!)$	$O(7n^2 + 8n - 7 + n * n! + Ln(m * (5n^2 + 9n - 5 + n * n!)))$
Неканоническая гиперкомплексная числовая система размерности n с $(n-1)^2$ составных ячеек	$O(4n^3 - 8n^2 + 8n - 2 + n * n!)$	$O(7n^3 - 14n^2 + 18n - 5 + n * n! + Ln(m * (5n^3 - 10n^2 + 15n - 3 + n * n!)))$

Очевидно, что вычислительная процедура разделения секрета в неканонической гиперкомплексной числовой системе размерности n с $(n-1)^2$ составных ячеек, сложнее, чем аналогичная процедура в канонической гиперкомплексной числовой системе размерности $n+1$.

При этом очевидно, что сложность разделения секрета возрастает с усложнением таблицы умножения выбранной неканонической гиперкомплексной числовой системы.

Тоже самое можно сказать и про процедуру восстановления секрета.

С другой стороны, для усиления задачи разделения секрета при работе с каноническими гиперкомплексными числами необходимо повышать размерность гиперкомплексной числовой системы.

Но, учитывая вышесказанное, можно сделать вывод, что для данной цели можно использовать представление данных в неканонических гиперкомплексных числовых системах той же размерности, с более сложной структурой таблицы умножения.

3.2. Анализ вычислительной сложности восстановления секрета для канонических и неканонических гиперкомплексных числовых систем

Сложность взлома схемы разделения секрета злоумышленником уже была рассмотрена в [2].

Покажем вычислительные сложности подбора гиперкомплексной числовой системы злоумышленником, – а фактически, процедуры перебора канонических и неканонических гиперкомплексных числовых систем, для которой примем как ограничение наличие единичного элемента в базисе (табл. 5).

Заключение

Можно утверждать, что хотя и сложность разделения и восстановления секрета в неканонических гиперкомплексных числовых системах превышает сложность этой задачи в канонических гиперкомплексных числовых системах, сложность взлома секрета значительно выше при использовании неканонических гиперкомплексных числовых систем.

Таблица 5

Сложность взлома схемы разделения секрета

Каноническая гиперкомплексная числовая система размерности n	$O(2n^3 - 3n^2 + 1)$
Каноническая гиперкомплексная числовая система размерности $n+1$	$O(2n^3 + 3n^2)$
Неканоническая гиперкомплексная числовая система размерности n с одной составной ячейкой	$O(3n + ((n-1)^2 - 1)(2n+1)) =$ $= O(2n^3 - 3n^2 + 3n)$
Неканоническая гиперкомплексная числовая система размерности n с $(n-1)^2$ составных ячеек	$O(3n(n-1)^2) = O(3n^3 - 6n^2 + 3n)$
Неканоническая гиперкомплексная числовая система размерности n с $(n-1)^2$ составных ячеек с целыми коэффициентами при базисных элементах из диапазона $\{-t, 0, t\}$	$O((2t+1)n(n-1)^2) =$ $= O((2t+1)(n^3 - 2n^2 + n))$

При этом, сложность подбора канонической гиперкомплексной числовой системы размерности $n+1$ и неканонической гиперкомплексной числовой системы размерности n практически одинаковы.

Но если учитывать, что коэффициентами при структурных элементах могут быть целые числа из диапазона $\{-t, 0, t\}$, вычислительная сложность возрастает до $O((2t+1)(n^3 - 2n^2 + n))$, что подтверждает вывод о целесообразности и эффективности использования неканононических гиперкомплексных чисел в задаче разделения секрета.

Литература

1. Бояринова Ю.Е. Восстановление информации в задаче разделения секрета для гиперкомплексных числовых систем 2–го порядка с помощью алгоритма Евклида / Ю.Е. Бояринова, Я.В. Одарич // Реєстрація, зберігання і обробка даних. – 2005. – Т. 6 – №1.

2. Бояринова Ю.Е. Разработка алгоритмов восстановления информации в задаче разделения секрета / Ю.Е. Бояринова, Я.В. Одарич, П.В. Трубников // Реєстрація, зберігання і обробка даних. – 2004. – Т. 6. – № 4. – С. 107-112.

3. Бояринова Ю.ЕРеализация алгоритма Евклида для задачи разделения секрета / Ю.Е. Бояринова, Я.В. Одарич, П.В. Трубников // Реєстрація, зберігання і обробка даних. – 2004. – Т. 6 – №3. – С.58-65.

4. Одарич Я.В. Процедура перечисления гиперкомплексных числовых систем методом линейных преобразований / Я.В. Одарич // Реєстрація, зберігання і обробка даних. – 2008. – Т.6. – № 2. – С.107-112.

Поступила в редакцию 18.02.2010

Рецензент: канд. техн. наук, доц. каф. ПМА ФПМ П.П. Маслянко, Национальный технический университет Украины «КПИ», Киев, Украина.

ОБЧИСЛЕННЯ В НЕКАНОНІЧНИХ ГІПЕРКОМПЛЕКСНИХ ЧИСЛОВИХ СИСТЕМАХ

Я.В. Одарич, О.Ю.Наливайчук, М.В.Наливайчук

Вказані головні ознаки і приклади неканонічних гіперкомплексних числових систем. Наведені порівняльні характеристики задачі розділення секрета та його відновлення з використання неканонічних гіперкомплексних числових систем різного виду.

Ключові слова: гіперкомплексна числова система, неканонічна гіперкомплексна числова система, задача розділення секрета.

COMPUTATION IN NONCANONICAL HYPERCOMPLEX NUMBER SYSTEMS

I.V. Odarych, O.J.Nalivaichuk, N.V.Nalivaichuk

Main differences and examples of noncanonical hypercomplex number systems are shown. Comparative characteristics of secret sharing scheme and its recovery using noncanonical hypercomplex number systems are adducted.

Keywords: hypercomplex number system, noncanonical hypercomplex number system, secret sharing scheme.

Одарич Яна Владимировна – младший научный сотрудник кафедры специализированных компьютерных систем Национального Технического Университета Украины «КПИ», Киев, Украина, e-mail: yannuary@yandex.ru.

Наливайчук Елена Юрьевна – младший научный сотрудник кафедры специализированных компьютерных систем Национального Технического Университета Украины «КПИ», Киев, Украина, e-mail: nalivaychuk@scs.ntu-kpi.kiev.ua.

Наливайчук Николай Васильевич – ассистент кафедры специализированных компьютерных систем Национального Технического Университета Украины «КПИ», Киев, Украина, e-mail: coleens@mail.ru.