УСТРОЙСТВО ДЛЯ ВЫЧИСЛЕНИЯ ИНДЕКСА ЭЛЕМЕНТОВ ПОЛЯ ГАЛУА ПО МОДУЛЮ

Калмыков И.А., Кихтенко О.А., Барильская А.В.
Северо-Кавказский государственный технический университет
Ставрополь, Россия

Применение арифметики в кольце полиномов является наиболее целесообразным, когда алгоритмы вычислений отмечаются повышенным содержанием мультипликативных арифметических операций при относительно небольшом количестве аддитивных.

Процедура возведения символа (элемента) конечного поля $GF(p)$ в степень трудоёмка и требует больших затрат на решение уравнения

$$\alpha^{x} \equiv \beta(mod\ \ p), \tag{1}$$

где α, β, x – элементы конечного поля Галуа с характеристикой p.

Для восстановления исходного значения α из получаемого значения β по модулю p используется уравнение:

$$\sqrt[x]{\beta} \equiv \alpha(mod\ \ p). \tag{2}$$

Реализовать выражение (1) можно, используя умножитель по модулю p, однако время данной операции будет равно

$$T_{оп} = (x-1)T_{ум},$$

где $T_{ум}$ - время выполнения модульного умножения.

Сократить время выполнения операции можно, используя индексы.

В работе [1] показана возможность использования теории индексов для эффективной реализации операций мультипликативного типа (умножение, деление, возведение в степень). Число i_A являющееся решением сравнения

$$g^{x} \equiv A\mathrm{mod}p, \tag{3}$$

называется индексом числа A и обозначается $i_A = indA$. Первообразный корень g–основание индекса.

В работе [1] доказана теорема, по которой индекс J произведения простых целых чисел A_1, A_2,…, A_k по модулю p равен сумме индексов сомножителей, взятой по модулю p-1, т.е.

$$J = \sum_{j=1}^{k} i_j \mathrm{mod}(p-1), \tag{4}$$

где i_1, i_2,…, i_k- индексы положительных чисел A_1, A_2,…,A_k по модулю p при первообразном коде g.

Т.о., очевидна возможность сведения операции умножения двух операндов A и B по модулю p к операции суммирования индексов i_A, i_B этих операндов при первообразном корне g по модулю p-1.

Аналогично можно доказать, что операцию возведения в степень (1) можно свести к операции индексов по модулю p-1.

Т.о., для нахождения индекса какого-либо числа A по модулю p надо найти первообразный корень числа p и решение сравнения (1) для данного первообразного корня. Эта операция сравнима по сложности с процедурой вычисления дискретного логарифма в конечном поле.

Аналогичная ситуация возникает и в расширенных полях Галуа $GF(2^{v})$. Т. к. все элементы этого поля получаются с помощью порождающего полинома $p(z)$, то в качестве первообразного корня можно выбрать z. Тогда любой элемент $A(z)$ поля $GF(2^{v})$ можно представить в виде

$$A(z) = z^{i_A}\mathrm{mod}p(z). \tag{5}$$

Следовательно, справедливо

$$A^{\gamma}(z) = \left(z^{i_A}\right)^{\gamma}\mathrm{mod}p(z) = z^{C}\mathrm{mod}p(z). \tag{6}$$

При этом

$$C = i_A\gamma\mathrm{mod}(2^{v}-1). \tag{7}$$

Т. к. значение показателя γ задано, то для реализации выражения (6) необходимо определить значение индекса i_A по модулю $p(z)$ из выражения (5).

Рассмотрим расширенное поле Галуа $GF(2^3)$. В этом поле определен порождающий полином $p(z)=z^3+z+1$, который задает следующие элементы поля (таблица 1).

Таблица 1

Представление элементов поля Галуа *GF(2³)*		
Степенное	Векторное	Полиномиальное
β^0	*001*	*1*
β^1	*010*	*z*
β^2	*100*	z^2
β^3	*011*	*z+1*
β^4	*110*	z^2+z
β^5	*111*	z^2+z+1
β^6	*101*	z^2+1

Видно, что показатели степеней элементов поля $GF(2^3)$ крутятся по модулю $7 = 2^3 - 1$.

Из таблицы 1 видно, при векторном представлении элементов $GF(2^3)$, соответствующих нулевому, 3-ему, 5-ому и 6-ому индексу, в нулевом разряде присутствует единица $a_0 = 1$, а в элементах поля с индексами 1, 2, 4 – в данном разряде записан нуль $a_0 = 0$.

Единица в 1-ом разряде $a_1 = 1$ векторного представления соответствует индексам – 1, 3, 4, 5, в противном случае, при $a_1 = 0$ индексам 0, 2, 6.

Единица во 2-ом разряде $a_2 = 1$ векторного представления соответствует индексам – 2, 4, 5, 6, в противном случае, при $a_2 = 0$ - индексам 0, 1, 3.

Используя логические функции, можно записать следующие соответствие, приведенные в таблице 2.

Следовательно, для реализации устройства вычисления индекса могут быть использованы базовые логические функции. Структура устройства для вычисления индекса элемента поля Галуа по модулю приведена на рисунке 1.

Таблица 2

Индексное представление	Векторное представление		
0	$\overline{a}_2$	$\overline{a}_1$	a_0
1	$\overline{a}_2$	a_1	$\overline{a}_0$
2	a_2	$\overline{a}_1$	$\overline{a}_0$
3	$\overline{a}_2$	a_1	a_0
4	a_2	a_1	$\overline{a}_0$
5	a_2	a_1	a_0
6	a_2	$\overline{a}_1$	a_0

Устройство состоит из регистра 1, предназначенного для хранения элементов поля Галуа GF(2^3), представленного а двоичном коде, блока 2 элементов НЕ, блока 3, состоявшего из 7 трехвходовых элементов И, шифратора 4 и выхода устройства 5. Выходы регистра 1 подключены к входу соответствующего элемента НЕ, входящего в состав блока 2.

Входы 1-го элемента И блока 3 подключены к выходам 2-ого и 3-его элементов НЕ блока 2 и к 1-ому выходу регистра 1. Входы 2-ого элемента И блока 3 подключены к выходам 1-ого и 3-его элементов НЕ блока 2 и ко 2-ому выходу регистра 1. Входы 3 элемента И блока 3 подключены к выходам 1-ого и 2-ого элементов НЕ блока 2 и к 3-ему выходу регистра 1. Входы 4 элемента И блока 3 подключены к выходу 3-его элемента НЕ блока 2 и к 1-ому и 2-ому выходам регистра 1. Входы 5 элемента И блока 3 подключены к выходу 1-ого элемента НЕ блока 2 и ко 2-ому и 3-ему выходам регистра 1. Входы 6 элемента И блока 3 подключены к 1-ому, 2-ому и 3-ему выходам регистра 1. Входы 7 элемента И блока 3 подключены к выходу 2-ого элемента НЕ блока 2 и к 1-ому и 3-ему выходу регистра 1.

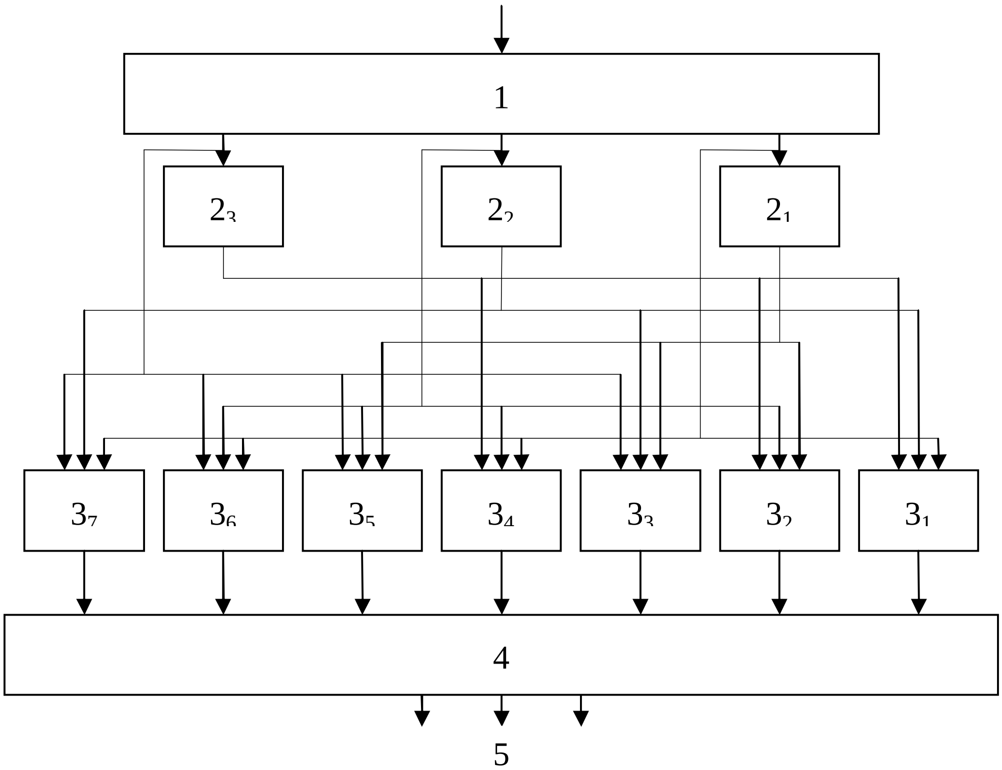

Рис. 1. Структура устройства

Выходы элементов И блока 3 подключены к входам шифратора 4, который преобразует семиразрядный унитарный код в двоичный трёхразрядный позиционный код. Выход шифратора 4 является выходом устройства 5.

СПИСОК ЛИТЕРАТУРЫ:

1. Акушский И.Я., Юдицкий Д.М. Машинная арифметика в остаточных классах. - М.: Сов. радио, 1968. – 440 с.

АВТОМАТИЗАЦИЯ РАЗРАБОТКИ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ В СОЦИАЛЬНО-ЭКОНОМИЧЕСКИХ СИСТЕМАХ НА ОСНОВЕ ПРИМЕНЕНИЯ НЕЧЕТКИХ КОГНИТИВНЫХ МОДЕЛЕЙ

Лагерев Д.Г.
Брянский государственный технический университет
Брянск, Россия

Принятие решений в социально-экономических системах осложняется нестабильностью и неопределенностью внешней среды, а также большим числом факторов, влияние которых нужно учитывать. К тому же для большинства социально-экономических систем затруднено применение традиционного эконометрического подхода к анализу и принятию решений, так как они относятся к классу слабоструктурированных систем. Перечисленные причины свидетельствуют об актуальности автоматизации процесса разработки управленческих решений с помощью систем поддержки принятия решений.

Следует особо отметить задачи, возникающие в ходе реализации процесса принятия управленческих решений, которые решаются в основном на приближенном, качественном уровне, с помощью интуиции и нестрогих рассуждений, например, задача анализа факторов, характеризующих ситуацию, задача разработки прогноза развития ситуации, задача генерации альтернативных вариантов решения. Для повышения эффективности решения указанных задач и обоснованности получаемых результатов предлагается использовать методику когнитивного моделирования. Данная методика основана на представлении моделируемого объекта или процесса в виде когнитивной карты представляющей собой совокупность целевых, управляемых, способствующих, препятствующих и неуправляемых параметров, между которыми задается набор причинно-следственных связей различного знака и веса.

Для автоматизации когнитивного моделирования при разработке управленческих решений была разработана программная система «Игла». В ней реализованы статические (расчет системных показателей) и динамические (импульсный процесс) методы анализа нечетких когнитивных карт. С помощью разработанной программной системы были проведены анализ и моделирование задачи управления инновациями на предприятии, а также обследование рынка труда Брянской области на предмет востребованности выпускников учреждений начального профессионального образования. Применение разработанной программной системы «Игла» при разработке