УДК 511.1, 512.542, 530.145

А.К. БЕЛЯЕВ, В.П. КЛИМЕНКО

О ПРЕДСТАВЛЕНИИ АРИФМЕТИЧЕСКИХ ФУНКЦИЙ В СИСТЕМЕ ОБРАТИМЫХ ПРЕОБРАЗОВАНИЙ АБСТРАКТНОГО РЕГИСТРА

Анотація. *Розглядається підхід до побудови довизначень частково визначених арифметичних функцій у системі обернених перетворень та їх класів на абстрактному регістрі. Визначаються умови замикання класів і можливість їх представлення в системі квантових обчислень.*
Ключові слова: *абстрактний реєстр, композиція арифметичних функцій, квантова модель обчислень.*

Аннотация. *Рассматривается подход к построению доопределений частично определенных арифметических функций в системе обратимых преобразований и их классов на абстрактном регистре. Определяются условия замыкания классов и возможность их представления в системе квантовых вычислений.*
Ключевые слова: *абстрактный регистр, композиция арифметических функций, квантовая модель вычислений.*

Abstract. *The article studies approach to building extensions of partially defined arithmetic functions within the system of reversible transformations and their classes on the abstract register. The conditions for class closures and possibilities of their representation in the system of quantum calculations are defined.*
Key words: *abstract register, the composition of arithmetic functions, quantum computation model.*

1. Введение

Развитие современных технологий в области создания вычислительных средств, например, нанотехнологий, квантовых вычислений, приводит к появлению новых требований к организации вычислений, а также к представлению преобразований, описывающих возможности таких технологий.

Так, один из основных вопросов в описании и моделировании квантовых вычислений [1] проявляется в необходимости представления вычислений в системе обратимых преобразований, в том числе представления арифметических функций, лежащих в основе вычислений.

Для описания арифметических преобразований и функций в области дискретных преобразований в [2] предложена система периодически определенных преобразований, абстрактного бесконечного регистра.

Абстрактный регистр представляется некоторой универсальной моделью для описания вычислений [2, 3]. Представление арифметических функций в системе периодически определенных преобразований дает возможность их структурного описания для реализации арифметических функций и служит основой постановки и решения задач оптимизации вычислений [2].

Практическая реализация описанной системы преобразований связана с областью приложений, а также с возможностью введения необходимых ограничений в представление преобразований на конечных множествах состояний ввиду ограничений разрядности абстрактного регистра.

ISSN 1028-9763. Математичні машини і системи, 2011, № 1

Ограничение разрядности, как правило, ведет к нарушению регулярности в описании арифметических функций из-за их частичного определения на конечных множествах состояний.

С задачей доопределения частично определенных арифметических функций связывается построение системы обратимых арифметических вычислений на конечных множествах состояний и для описания квантовых вычислений.

Поэтому построение классов обратимых арифметических функций и их представление в системе преобразований n-разрядного абстрактного регистра представляется актуальным.

В работе разрабатывается подход для построения таких доопределений.

2. Постановка задачи

Для обоснования подхода к построению описанных классов и проведения анализа доопределений частично определенных арифметических функций на конечном множестве состояний будем рассматривать некоторый набор известных элементарных арифметических функций. Эти функции могут быть представлены в классе периодически определенных преобразований бесконечного абстрактного двоичного регистра и иметь структурные описания на конечном абстрактном регистре. Обозначим функции набора через a, b, c, d,

где a – перечисление состояний абстрактного регистра;

b – циклический сдвиг (влево) кодов состояний абстрактного регистра;

c – арифметическое умножение кодов состояний на число три;

d – вычисление суммы натурального ряда чисел $\sum_{i=1}^{x} i$, где x – текущее состояние абстрактного регистра.

Описание функций a, b в классе периодически определенных преобразований рассматривается в [2].

Функции c, d описываются в составе технических устройств [4, 5]. В этих устройствах исходные состояния n-разрядных двоичных регистров преобразуются в значения результатов вычисления заданных функций. Регулярность структурного описания арифметических функций соответствует определению класса периодически определенных преобразований и образуется в результате периодического повторения логических функций переключения состояний разрядов регистров. Логические функции определяются базовыми уравнениями периодически определенных преобразований [2].

Структурные описания функций a, b, c непосредственно определяются базовыми уравнениями абстрактного регистра, тогда как описание функции d представляется композицией преобразований и образует сложное структурное описание преобразований в классе периодически определенных преобразований.

Ограничение разрядности бесконечного абстрактного регистра, а также выполнение условий обратимости преобразований на конечном регистре, переводит рассмотрение описанных выше преобразований из класса частично определенных в некоторый класс (частично) доопределенных преобразований конечного n-разрядного абстрактного двоичного регистра. Этот класс может быть описан в конечной симметрической группе G.

Действительно, пусть P – множество состояний конечного n-разрядного двоичного абстрактного регистра, где $P = \{0, 1, 2, ..., m-1\}$, а $m = 2^n$. В системе обратимых преобразований на множестве P определим систему перестановок элементов симметрической группы G порядка $m!$. Перестановками состояний будем представлять предложенный набор арифметических функций.

Возможным способом частичного доопределения арифметических функций (описанных выше) на конечных множествах состояний является представление функций в системе остаточных классов по $\bmod 2^n$. Тогда наборы функций в виде перестановок степени m для случая $n=3$ представляются в виде

$$a=\begin{pmatrix}0\,1\,2\,3\,4\,5\,6\,7\\1\,2\,3\,4\,5\,6\,7\,0\end{pmatrix},\ b=\begin{pmatrix}0\,1\,2\,3\,4\,5\,6\,7\\0\,2\,4\,6\,1\,3\,5\,7\end{pmatrix},\ c=\begin{pmatrix}0\,1\,2\,3\,4\,5\,6\,7\\0\,3\,6\,1\,4\,7\,2\,5\end{pmatrix},\ d=\begin{pmatrix}0\,1\,2\,3\,4\,5\,6\,7\\0\,1\,3\,6\,2\,7\,5\,4\end{pmatrix}.$$

Функция a – циклическая перестановка степени m.

Функция b может рассматриваться в виде некоторой частично доопределенной функции, хотя эта функция не определяется в системе остаточных классов по $m=2^n$.

Функции c – инволютивное преобразование для $n=3$.

Функция d – представляется циклической перестановкой степени $(m-2)$.

Функциональный анализ представленных функций и их композиций показывает, что пара частично доопределенных функций $\{a,d\}$ является образующими симметрической группы G. Симметрическая группа G, однако, содержит множество произвольных транспозиций.

Преобразования, реализующие множество произвольных транспозиций, не описываются в системе периодически определенных преобразований и не образуют регулярного структурного описания на абстрактном бесконечном регистре в соответствии с определениями [2].

Поэтому система обратимых арифметических функций, определенная на конечных множествах состояний n-разрядного двоичного абстрактного регистра и построенная на основе непосредственного вычисления значений функций в системе остаточных классов, не приводит к сужению класса частично доопределенных арифметических функций, а также не позволяет определить условия логического замыкания классов этих функций.

Аналогичные построения могут быть проведены и для пары частично доопределенных функций $\{a,b\}$, для которых нарушение структурной регулярности в результате композиции функций в этом случае непосредственно связывается с выбором исходной системы образующих функций, определенных на конечном абстрактном регистре. Функция b не образует замыкание класса частично доопределенных арифметических функций.

Для построения класса частично доопределенных арифметических фунций и выяснения условий логического замыкания класса определим ограничения в области частичного доопределения функций и проведем некоторые пребразования функций предложенного набора.

3. Построение класса частично доопределенных арифметических функций

Представим символы состояний области определения частично доопределенных функций в виде соответствия символов двух множеств: $A=\{0,1,...,(\frac{m}{2}-1)\}$ и $B=\{\frac{m}{2},(\frac{m}{2}+1),...,(m-1)\}$ для четных m. Назовем множество B зеркальной частью области определения частично доопределенных функций. Тогда разность соответствующих пар символов, очевидно, равна $\frac{m}{2}$, где $|a_i-b_i|=\frac{m}{2}$, а $a_i\in A$, а $b_i\in B$, и $i=\{0,1,...,\frac{m}{2}\}$. Определим условие соответствия пар символов для значений функций путем вычисления модуля разности соответствующих значений частично доопределенных функций в виде

$$\left| f(a_i) - f(b_i) \right| = \frac{m}{2}. \qquad (1)$$

Условие (1) выделяет некоторый замкнутый подкласс частично доопределенных преобразований симметрической группе G. Обозначим этот класс функций через U. Рассмотрим примеры представления арифметических функций класса U на основе преобразования функций набора a, b, c, d.

Определим функцию a для $m = 2^n$ и $n = 3$. Элементам значения функции a на множестве $A = \{1, 2, 3, 4\}$ ставятся в соответствие значения функций на множестве $B = \{5, 6, 7, 0\}$. Модуль разности пар на множестве значений функции равен 4. То есть, функция a – элемент класса U.

Аналогично для функции c при $m = 2^n$ и $n = 3$. Здесь множеству значений функции на множестве $A = \{0, 3, 6, 1\}$ соответствуют значения на множестве $B = \{4, 7, 2, 5\}$. Модуль разности пар на множестве значений функции равен 4. Таким образом, c – элемент класса U.

Рассмотрим функцию d. Анализ значений функции d в области определения B показывает, что функция d может быть представлена в классе U путем зеркального преобразования области значений функции, определенной на B. Это отличительное свойство функции d, определенной в системе остаточных классов по модулю $m = 2^n$.

Назовем эту операцию «погружением» функции d в класс U. Для $m = 2^n$ и $n = 3$ «погружение» может быть образовано путем умножения функции d слева на некоторый элемент $r = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6\,7 \\ 0\,1\,2\,3\,7\,6\,5\,4 \end{pmatrix}$ группы G. Обозначим преобразованную функцию через d'. Тогда для $m = 2^n$ и $n = 3$ значение функции принимает вид $d' = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6\,7 \\ 0\,1\,3\,6\,4\,5\,7\,2 \end{pmatrix}$, соответствующие разности $\{0, 1, 3, 6\}$ и $\{4, 5, 7, 2\}$ равны 4. Функция d' – циклическая перестановка степени $(m-4)$. Это функция класса U.

Функция b также «погружается» в класс U путем преобразования зеркальной части в области значений B. В этом случае операция «погружения» представляется трансформацией значений функции в области B элементом r группы G. Обозначим преобразованную функцию через b'. Тогда для случая $m = 2^n$ и $n = 3$ функция принимает вид $b' = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6\,7 \\ 0\,2\,7\,5\,4\,6\,3\,1 \end{pmatrix}$, соответствующие разности $\{0, 2, 7, 5\}$ и $\{4, 6, 3, 1\}$ равны 4.

В системе образующих $\{a, d'\}$ преобразование b' для случая $m = 2^n$ и $n = 3$ представляется разложением $b' = (ad')^2 a^2 (d'a)^3$, а функция c, соответственно, разложением $c = d'a^2(d')^3 a$. Результаты разложения могут быть получены в соответствии с методикой, рассмотренной в [6].

Нужно отметить, что в системе образующих $\{a, d'\}$ также представляются функции умножения на нечетные числа, представленные в системе остаточных классах по $m = 2^n$.

Анализ условия (1) – образование элементов класса U показывает, что система образующих класса U может также определяться элементами: функцией a и парой транспозиций вида $\{ (m-2,\ m-1),\ (\frac{m}{2}-1,\ \frac{m}{2}-2) \} \in U$, удовлетворяющих условию (1). В этом наборе образуется более широкий класс функций.

В такой системе образующих порядок элементов класса U равен $N = 2^{\frac{m}{2}} \cdot \frac{m}{2}!$ – т.е., произведению четных чисел натурального ряда $N = 2 \cdot 4 \cdot 6 \cdot ... \cdot m$, где m – четная степень элемента группы G. Описанный набор функций образует замыкание класса U.

Назовем образованный таким образом класс функций центрально симметрическим классом (ЦС классом) преобразований группы G.

Исходный набор преобразованных функций a, b', c, d' представляется в классе ЦС. Система образующих элементов $\{a, d'\}$ образует группу преобразований порядка $N' = N/2$, т.е. является подгруппой класса ЦС.

Особенностью элементов класса ЦС является наличие центральных элементов, представленных множеством одиночных транспозиций вида $\{(m-1, \frac{m}{2}-1), (m-2, \frac{m}{2}-2), ..., (0, \frac{m}{2})\}$. Центральные элементы коммутативны и образуют коммутативную подгруппу класса ЦС. Симметрия центральных элементов позволяет рассматривать эти элементы в качестве элементов класса арифметических функций в системе частично доопределенных функций.

Частично доопределенные функции умножения на числа два и три могут рассматриваться в качестве системы образующих циклических подгрупп (порядков $m-2$, $m-4$) произведений четных и нечетных чисел на элементы натурального ряда чисел. Так, для случая $n = 4$ образующие могут быть представлены в виде

$$e = \begin{pmatrix} 0123456789ABCDEF \\ 024613578ACE9BDF \end{pmatrix}, \quad f = \begin{pmatrix} 0123456789ABCDEF \\ 03695CA78BE1D42F \end{pmatrix},$$

где функции e, f – элементы класса U. Порядок подгруппы произведений чисел – 12.

В компактном виде образующие представляются таблицей разложений в циклах, соответственно – длины 4 для умножения на три (по горизонтали) и длины 3 для умножения на два (по вертикали). Таблица разложений имеет вид

$$\begin{pmatrix} 1 & 3 & 9 & B \\ 2 & 6 & A & E \\ 4 & 5 & C & D \end{pmatrix}.$$

В таблице отмечена область доопределения функций умножения на числа два и три, а также представлены результаты умножений.

Предлагаемый в работе подход представления частично доопределенных арифметических функций в системе обратимых преобразований абстрактного регистра дает возможность построения преобразований, локализованных в разрядах [6] абстрактного регистра для определения базовых уравнений арифметических преобразований и дальнейшей оптимизации вычислений [7].

В системе квантовых вычислений арифметические функции могут представляться частично доопределенными обратимыми преобразованиями состояний p-позиционного абстрактного регистра на основе микроопераций квантовой системы вычислений [3].

4. Выводы

1. Частично доопределенные обратимые арифметические функции представляются в классе центрально симметрических преобразований симметрической группы G.

2. Система центрально симметрических преобразований образует замыкание класса частично доопределенных обратимых арифметических функций.

СПИСОК ЛИТЕРАТУРЫ

1. Нильсен М. Квантовые вычисления и квантовая информация / М. Нильсен. – М.: Мир, 2006. – 823 с.
2. Глушков В.М. Кибернетика, вычислительная техника, информатика: избр. труды в 3-х т. / Глушков В.М. – Киев: Наукова думка, 1990. – Т. 1. – С. 179 – 191.
3. Беляев А.К. Анализ модели квантовых вычислений / А.К. Беляев, В.П. Клименко // Математичні машини і системи. – 2009. – № 2. – С. 45 – 52.
4. А. с. 744570 СССР, МКИ G06F7/52. Устройство умножения на три / А.К. Беляев, Г.И. Корниенко, В.В. Ткаченко. – Опубл. 30.06.80, Бюл. № 4.
5. А.с. 947855 СССР, МКИ G06F7/552. Устройство для вычисления функции $\sum_{i=1}^{x} i$ / А.К. Беляев, Г.И. Корниенко, В.В. Ткаченко. – Опубл. 30.07.82, Бюл. № 28.
6. Беляев А.К. Базовая система микроопераций и ее применение / А.К. Беляев // Кибернетика. – 1972. – № 2. – С. 71 – 76.
7. Бєляєв А.К. Критерії оптимізації обчислень на абстрактному регістрі / А.К. Бєляєв, І.А. Клименко // Вісник Національного технічного університету України «КПІ». Інформатика управління та обчислювальна техніка. – 2004. – № 41. – С. 61 – 66.
8. Холл М. Теория групп / Холл М. – М.: Иностр. лит., 1962. – 468 с.

Стаття надійшла до редакції 19.01.2011