Международная конференция
«Современные проблемы математики, информатики и биоинформатики»,

посвященная 100-летию со дня рождения члена-корреспондента АН СССР Алексея Андреевича Ляпунова
11 - 14 октября 2011 г., Академгородок, Новосибирск, Россия

АЛГЕБРАИЧЕСКАЯ СТРУКТУРА И МОДЕЛЬ ВЫЧИСЛЕНИЙ ДЛЯ АРИФМЕТИКИ ОГРАНИЧЕННЫХ ЦЕЛЫХ НЕОТРИЦАТЕЛЬНЫХ ЧИСЕЛ

Ю. Г. Сметанин
Вычислительный центр им. А. А. Дородницына РАН

М. В. Ульянов
Московский государственный университет печати,
Научно-исследовательский университет Высшая школа экономики

ОБЛАСТЬ ИССЛЕДОВАНИЙ

Статья А. А. Ляпунова «К алгебраической трактовке программирования» содержит определение программирования на основе «теоретико-множественной базы» и рассматривает программирование с позиций общей алгебры.

ОСОБЕННОСТИ ЗАДАЧИ

Особенностью основных формализмов теории алгоритмов — машины Поста, машины Тьюринга, нормальных алгорифмов Маркова, равно как и алгебраического подхода к формализации компьютерных вычислений, предложенного Глушковым В. М., Цейтлиным Г. Е. и Ющенко Е. Л. является счётность носителя этих моделей, что противоречит реальным форматам данных и схемным или микропрограммным алгоритмам реализации арифметических операций в реальном компьютере.

Объект: *Алгебраическая структура с частичными операциями как формализм компьютерной целочисленной арифметики*.

Предмет: *Модель вычислений с предусловиями выполнения команд и формализм арифметических выражений.*

Цель: *Устранение особенностей входов с использованием эквивалентных преобразований*.

АЛГЕБРАИЧЕСКАЯ СТРУКТУРА С ЧАСТИЧНЫМИ ОПЕРАЦИЯМИ (I)

Обозначим через I_n множество первых n неотрицательных целых чисел:

$$I_n \subset N_0, \quad I_n = \{0,1,\ldots,n-1\},$$

через $B(I_n \times I_n)$ — множество всех подмножеств декартова произведения $I_n \times I_n$.

Алгебраическая структура с частичными операциями для арифметики ограниченных целых неотрицательных чисел — A_Q, вводится в виде четвёрки

$$A_Q = \langle I_n, S, F, Q \rangle,$$

где I_n — носитель, S — сигнатура алгебраической структуры, F — функция ограничения носителя для операций, Q — множество предикатов ограничения операндов операций.

Сигнатура S структуры A_Q есть множество, включающее следующие пять арифметических операций

$$S = \{s_i \mid i = \overline{1,5}\} = \{s_1 = "+", s_2 = "-", s_3 = "*", s_4 = "\text{div}", s_5 = "\text{mod}"\}$$

АЛГЕБРАИЧЕСКАЯ СТРУКТУРА С ЧАСТИЧНЫМИ ОПЕРАЦИЯМИ (II)

Функция F — функция ограничения носителя

$$F : S \to B(I_n \times I_n), \quad F(s_i) \subset B(I_n \times I_n),$$
$$F(s_i) = \{(k,l) \mid q_i(k,l) = true\}, \quad (k,l) \in I_n \times I_n, \quad q_i \in Q.$$

Множество предикатов $Q = \{q_i \mid i = \overline{1,5}\}$ задаёт условия, ограничивающие операнды из I_n для частичных арифметических операций, а именно:

$$s_1 = "+": \quad q_1(k,l) = (k + l \le n - 1),$$
$$s_2 = "-": \quad q_2(k,l) = (k \ge l),$$
$$s_3 = "*": \quad q_3(k,l) = (k * l \le n - 1),$$
$$s_4 = "/": \quad q_4(k,l) = (l \ne 0),$$
$$s_5 = "/": \quad q_5(k,l) = (l \ne 0).$$

Операция s_i ограничена по операндам и задаётся соответствующим отображением

$$s_i : F(s_i) \to I_n, i = \overline{1,5}.$$

МОДЕЛЬ ВЫЧИСЛЕНИЙ С ПРЕДУСЛОВИЯМИ ВЫПОЛНЕНИЯ ОПЕРАЦИЙ (I)

Модель вычислений M формально задаётся в виде совокупности

$$M = \langle I_A, R \rangle,$$

где I_A — информационная алгебра модели вычислений, а R — механизм реализации

$$R = \langle P, C, \Omega \rangle,$$

где P — абстрактный процессор; C — множество базовых операций модели вычислений, Ω — множество управляющих и операционных ячеек механизма реализации.

Введём носитель информационной алгебры

$$Y = \{ y_i \mid i = \overline{1,m} \}, \quad Y \subset A \times I_n, \quad y_i = (a, z),\ a \in A,\ z \in I_n,$$

где компонент a является адресным компонентом ячейки, а компонент z — информационным.

На этой основе мы вводим информационную алгебру модели вычислений в виде

$$I_A = \langle Y, C_I \rangle,$$

где Y — носитель, а C_I — множество операций механизма реализации над объектами из Y, состоящее из операций чтения содержимого ячейки и записи в ячейку.

МОДЕЛЬ ВЫЧИСЛЕНИЙ С ПРЕДУСЛОВИЯМИ ВЫПОЛНЕНИЯ ОПЕРАЦИЙ (II)

В состав механизма реализации включены его собственные ячейки, составляющие множество Ω. Результат формируется в специальной ячейке θ механизма реализации и, в случае его допустимости, возвращается в носитель. Для идентификации отсутствия результата операции введём в рассмотрение специальный элемент "$undef$", который помещается в ячейку результата θ, но не возвращается в носитель. Символические имена составляют множество A_Ω:

$$A_\Omega = \{\alpha, \beta, \gamma, \theta, f, t, r, nul, u, g\},$$

при этом сами элементы множества Ω определяются следующим образом:

$$\Omega = \{y_\alpha = (\alpha, z),\ y_\beta = (\beta, z),\ y_\gamma = (\gamma, z),\ y_\theta = (\theta, x),$$
$$y_f = (f, 0),\ y_t = (t, 1),\ y_r = (r, b),\ y_{nul} = (nul, z = 0),$$
$$y_u = (u, n-1),\ y_g = (g, "undef")\},$$
$$z \in I_{n^2}, \quad x \in I_n \cup "undef", \quad b \in \{0,1\}.$$

Отметим, что ячейка с именем g хранит специальное значение "$undef$" для идентификации некорректного результата арифметической операции.

МОДЕЛЬ ВЫЧИСЛЕНИЙ С ПРЕДУСЛОВИЯМИ ВЫПОЛНЕНИЯ ОПЕРАЦИЙ (III)

Приведём пример алгоритма в элементарных операциях предложенной модели вычислений с предусловиями выполнения команд, который вычисляет арифметическое выражение:

$$c \leftarrow (a+b)*d\,.$$

```
´θ ← ´g
´α ← ´a
´β ← ´b
´γ ← ´α + ´β
´r ← [´γ ≤ ´u]
 Q1: [´r = ´t]{
                ´α ← ´d
                ´β ← ´α * ´γ
                ´r ← [´β ≤ ´u]
                 Q2: [´r = ´t]{
                                ´θ ← ´β
                                ´c ← ´θ
                              }
              }
stop.
```

Отметим, что фрагмент, вычисляющий произведение, вложен в предусловие допустимости результата сложения, таким образом, результат возвращается в носитель, при допустимости всех промежуточных результатов.

ПОЛИНОМИАЛЬНЫЕ АРИФМЕТИЧЕСКИЕ ВЫРАЖЕНИЯ

Рассматриваемый нами частный случай ограничивается алгебраической структурой и соответствующей моделью вычислений, поддерживающей только следующие три арифметические операции:

$$\widetilde{S} = \{s_i \mid i = \overline{1,3}\} = \{s_1 = "+", s_2 = "-", s_3 = "*"\}.$$

Будем называть далее ***арифметическим выражением*** полиномиальную функцию $g(X)$, где X есть m-компонентный кортеж — $(x_1, x_2, \ldots, x_m)$. Область определения аргументов ограничена множеством I_n, а область допустимых значений функции g есть множество I_n, объединённое с элементом "*undef*":

$$g : I_n^m \to I_n \cup "undef", \quad g(X) = g(x_1, x_2, \ldots, x_m) = \sum c \cdot \prod_{j,k \in 1,\ldots,m} x_j \cdot \ldots \cdot x_k,$$

где c — некоторые константы из I_n. Такую запись будем ***называть обобщённой полиномиальной формой арифметического выражения***.

Рассматриваемая совокупность многочленов g является, очевидно, подмножеством арифметических выражений, для которого разрешёнными операциями являются умножение, сложение и вычитание.

КЛАССИФИКАЦИЯ ВХОДОВ АРИФМЕТИЧЕСКИХ ВЫРАЖЕНИЙ

Обозначим через $X^{(0)} = \left(x_1^{(0)}, \ldots, x_m^{(0)}\right) \in I_n^m$ — кортеж из m элементов множества I_n, — ***конкретный вход*** арифметического выражения. При этом аргумент x_i функции g получает значение $x_i^{(0)}, i = \overline{1,m}$. Определим функцию $\tilde{g}$ как функцию, совпадающую с g, но обладающую другой областью значений промежуточных и окончательных результатов — множеством целых чисел Z: $\tilde{g} : I_n^m \to Z$. При вычислении значения $g\left(X^{(0)}\right)$ могут возникнуть три возможные ситуации, при этом будем называть вход $X^{(0)}$:

— ***допустимым входом***, если $g\left(X^{(0)}\right) \in I_n$, — арифметическое выражение вычислимо для $X^{(0)}$;
— ***входом с потенциально устранимой особенностью***, если $\tilde{g}\left(X^{(0)}\right) \in I_n$, $g\left(X^{(0)}\right) = "undef"$. Содержательно это означает, что промежуточные результаты лежат вне носителя I_n. Возможно, что путём некоторых эквивалентных преобразований такое выражение приводится к виду, для которого вход $X^{(0)}$ является допустимым. В этом случае будем говорить о том, что этот вход является ***входом с эквивалентно устранимой особенностью***;
— ***входом с неустранимой особенностью***, если $\tilde{g}\left(X^{(0)}\right) \in Z / I_n$, $g\left(X^{(0)}\right) = "undef"$. Окончательное значение выражения g для входа X_0 лежит вне носителя I_n. Очевидно, что в этой ситуации никакие эквивалентные преобразования g не приведут к допустимости входа.

ЭКВИВАЛЕНТНЫЕ ПРЕОБРАЗОВАНИЯ АРИФМЕТИЧЕСКИХ ВЫРАЖЕНИЙ (I)

Нашей следующей целью является введение понятия эквивалентных арифметических выражений и описание методики эквивалентных преобразований.

Два арифметических выражения, заданных полиномиальными функциями $g(X)$ и $h(X)$ ***будем называть эквивалентными***, если $\forall X^{(0)} \in I_n^m$ имеет место одна и только одна из следующих ситуаций:

1) $g\left(X^{(0)}\right) = h\left(X^{(0)}\right), \quad g\left(X^{(0)}\right) \in I_n, \quad h\left(X^{(0)}\right) \in I_n,$

2) $\tilde{g}\left(X^{(0)}\right) = \tilde{h}\left(X^{(0)}\right), \quad g\left(X^{(0)}\right) \in I_n, \quad h\left(X^{(0)}\right) = "undef",$

3) $\tilde{g}\left(X^{(0)}\right) = \tilde{h}(X_0), \quad g\left(X^{(0)}\right) = h\left(X^{(0)}\right) = "undef".$

Заметим, что функция $g(x_1, x_2, \ldots, x_m)$ в общем случае представима в виде композиции функций $s_1(\cdot), s_2(\cdot)$ либо $t_1(\cdot), t_2(\cdot), t_3(\cdot)$, объединённых операциями из $\tilde{S}$, аргументы которых представляют собой подмножества множества аргументов функции g.

ЭКВИВАЛЕНТНЫЕ ПРЕОБРАЗОВАНИЯ АРИФМЕТИЧЕСКИХ ВЫРАЖЕНИЙ (II)

Преобразование

$$L : g_1(X) \to g_2(X),$$

задаваемое оператором L, ***будем называть эквивалентным преобразованием***, если L есть произвольная суперпозиция операторов L_c, L_a, L_d:

$$L_c : \begin{cases} s_1(\cdot) \pm s_2(\cdot) \to s_2(\cdot) \pm s_1(\cdot) \\ s_1(\cdot) * s_2(\cdot) \to s_2(\cdot) * s_1(\cdot) \end{cases}$$

$$L_a : \begin{cases} (t_1(\cdot) \pm t_2(\cdot)) \pm t_3(\cdot) \to t_1(\cdot) \pm (t_2(\cdot) \pm t_3(\cdot)) \\ (t_1(\cdot) * t_2(\cdot)) * t_3(\cdot) \to t_1(\cdot) * (t_2(\cdot) * t_3(\cdot)) \end{cases}$$

$$L_d : (t_1(\cdot) \pm t_2(\cdot)) * t_3(\cdot) \Leftrightarrow t_1(\cdot) * t_3(\cdot) \pm t_2(\cdot) * t_3(\cdot)$$

Конкретную суперпозицию операторов L_c, L_a, L_d будем обозначать через $L^{(0)}$. На основании свойств кольца Z, полиномиальные арифметические выражения, заданные функциями $g_1(X)$ и $g_2(X) = L(g_1(X))$, эквивалентны.

УСТРАНЕНИЕ ОСОБЕННОСЕЙ ВХОДОВ ЭКВИВАЛЕНТНЫМИ ПРЕОБРАЗОВАНИЯМИ (I)

Лемма 1. Если разность многочленов $g_1(X)$ и $g_2(X)$, приведённых к обобщённой полиномиальной форме, есть многочлен с нулевыми коэффициентами, то $g_2(X)$ может быть получен из $g_1(X)$ с помощью преобразования L.

Рассмотрим применение входа $X^{(0)}$ к многочлену $g(X)$. Последовательно подставляя в $g(X)$ значения $x_m^{(0)},\ldots,x_2^{(0)}$, мы придём к представлению $g(X)$ в виде многочлена от x_1:

$$\hat{g}(x_1) = a_r x_1^{\,r} + a_{r-1} x_1^{\,r-1} + \ldots + a_0,$$

где коэффициенты a_i есть результаты подстановки $x_m^{(0)},\ldots,x_2^{(0)}$ в $g(X)$. Мы предполагаем далее, что вход $X^{(0)}$ допустим для $g(X)$ в I_n, и, следовательно $a_i \in I_n$.

Лемма 2. Если арифметические выражения, заданные многочленами от x_1— $\hat{g}_1(x_1)$ и $\hat{g}_2(x_1)$, эквиваленты, и степень каждого из них меньше n, то $g_1(X)$ может быть получен из $g_2(X)$ с помощью преобразования L.

УСТРАНЕНИЕ ОСОБЕННОСЕЙ ВХОДОВ ЭКВИВАЛЕНТНЫМИ ПРЕОБРАЗОВАНИЯМИ (II)

Лемма 2 не применима, если степень многочлена $\hat{g}_1(x_1)$ больше n, т. к. такой многочлен может иметь n корней в I_n, однако справедлива следующая

Лемма 3. Для арифметического выражения, заданного многочленом $g(X)$, преобразованная форма которого $\hat{g}(x_1)$, имеет степень большую или равную n, можно построить эквивалентный в Z многочлен меньшей степени.

Доказательство

Пусть $\hat{g}(x_1) = a_{n+p} x_1^{n+p} + a_{n+p-1} x_1^{n+p-1} + \ldots + a_0$ и $p \geq 0$. Рассмотрим многочлен $h(x_1)$, представляющий собой убывающую факториальную степень $n+p$ по x_1:

$$h(x_1) = x_1^{\underline{n+p}} = x_1(x_1-1)(x_1-2)\ldots(x_1-(n+p-1)) = \sum_{k=1}^{n+p} \begin{bmatrix} n+p \\ k \end{bmatrix} (-1)^{n+p-k} x_1^{k},$$

где квадратные скобки являются обозначением чисел Стирлинга первого рода.

УСТРАНЕНИЕ ОСОБЕННОСЕЙ ВХОДОВ ЭКВИВАЛЕНТНЫМИ ПРЕОБРАЗОВАНИЯМИ (III)

Заметим, что $h(x_1) \equiv 0$ в I_{n+p}, и заведомо обращается в ноль $\forall x_1 \in I_n$. В силу этого следует, что $\forall x_1 \in I_n$ имеет место эквивалентное преобразование (***преобразование понижения степени***) с коэффициентами из Z:

$$x_1^{n+p} = (-1)^{\sum_{k=1}^{n+p-1}} \begin{bmatrix} n+p \\ k \end{bmatrix} (-1)^{n+p-k} x_1^{k}.$$

Применяя предложенное преобразование к $\hat{g}(x_1)$ мы получаем многочлен $\hat{g}_1(x_1)$, имеющий степень не более чем $n+p-1$. Последовательно, а именно $p+1$ раз, применяя аналогичное преобразование, можно получить многочлен $\hat{g}_p(x_1)$, имеющий степень меньше, чем n, с коэффициентами в Z.

Конец доказательства.

Из лемм 1-3 непосредственно следует:

УСТРАНЕНИЕ ОСОБЕННОСЕЙ ВХОДОВ ЭКВИВАЛЕНТНЫМИ ПРЕОБРАЗОВАНИЯМИ (IV)

Теорема: Если вход $X^{(0)}$ является входом с потенциально устранимой особенностью для арифметического выражения, заданного полиномом $g(X)$, то задача построения эквивалентного арифметического выражения, возможно допускающего вход $X^{(0)}$, требует выполнения только двух видов преобразований — преобразования понижения степени и эквивалентных преобразований.

Если при этом, после преобразования понижения степени, все коэффициенты $\hat{g}_p(x_1)$ лежат в I_n, то арифметическое выражение, заданное многочленом $\hat{g}_p(x_1)$ может допускать вход $X^{(0)}$. Если многочлен $\hat{g}_p(x_1)$ не допускает вход $X^{(0)}$ в смысле введённой классификации входов, то на основе лемм 1 и 2 возможно существует эквивалентное преобразование $L(\hat{g}_p(x_1))$ арифметического выражения $g(X)$, допускающего вход $X^{(0)}$.

Конец теоремы.