МНОГООСНОВНЫЕ АЛГЕБРЫ, АБСТРАКТНЫЕ ТИПЫ ДАННЫХ И ТРАНСФИНИТНАЯ РЕКУРСИЯ

Крывый С.Л.

Аннотация: *Описывается абстрактный тип данных ``натуральное число" как многоосновная алгебраическая система, пополненная операторами рекурсии и индукции. Исследуются пределы, до которых распространяется действие рекурсии и индукции на множества, отличные от множества натуральных чисел.*

Ключевые слова: *многоосновные алгебры, абстрактный тип данных, трансфинитная рекурсия.*

Keywords: MSC, verification, RAD.

ACM Classification Keywords: D.2.4 Software/Program Verification - Formal methods

Введение

Абстрактные типы данных (АТД) активно используются в процессе разработки программного обеспечения, его обосновании и верификации. Этот упрощенный процесс можно схематически изобразить в таком виде [axo-79]:

Математическая модель		Абстрактный тип данных		Структуры данных
----------------------------------	$\Rightarrow$	----------------------------------	$\Rightarrow$	---------------------------
Неформальный алгоритм		Программа на псевдокоде		Программа на языке программирования

С помощью таких технологий строятся системы баз данных, баз знаний, системы компьютерной алгебры и геометрии, графические системы и т. д. Главным требованием при построении таких систем является правильность и эффективность построенных алгоритмов и программ. В процессе построения эффективных алгоритмов и программ важную роль играет успешный выбор структур данных. Неформально описывая алгоритм решения прикладной задачи, исходя из выбранной математической модели, приходится пользоваться такого типа данными, которых нет ни в одном языке программирования, но которые свойственны этой математической модели. Такого типа данные называются *абстрактными типами данных*. Более формально, под абстрактным типом данных понимают некоторую формальную математическую модель вместе с операциями, функциями и предикатами, определёнными на этой модели. Примерами такого типа данных могут служить множества, вместе с операциями объединения, пересечения и разности. В модели АТД операторы могут иметь операндами не только данные, которые определяются этим АТД, но и операнды языка программирования и операнды, которые определены другими АТД. Результатом выполнения оператора тоже может быть тип данных, который не определяется данным АТД. Но в рамках данного АТД считается, что хотя бы один операнд или результат любого оператора имеет тип данных, определённый в данной модели АТД.

АТД определяются, как правило, с помощью аксиоматики и отличаются от структур данных в языках программирования тем, что при использовании АТД абстрагируются от способа их реализации и рассматриваются только их свойства, которые вытекают из аксиоматики. В общем случае определение АТД сводится к определению таких понятий:

- объекты,
- базовые операции,

- конструкторы новых операций, функций и предикатов,
- определения (дефиниции) новых объектов.
- Основными конструкторами, которые используются при определении новых операций, функций и предикатов есть рекурсия и индукция. Неформально под *рекурсией* понимают такой способ определения функции, при котором значение функции для произвольных значений ее аргументов выражаются известным способом через значения этой функции для меньших значений ее аргументов. Простейшим видом рекурсии является *примитивная рекурсия*.
- *Индукцией* называют такой способ определения функции, при котором значения функции для произвольного значения ее аргумента выражаются известным образом через значения этой функции для аргумента, которые непосредственно предшествует данному аргументу.
- Известно, что индукция, как и рекурсия работают на специального типа множествах, которые являются полностью упорядоченными. Основной вопрос, который нас будет интересовать - это пределы до которых можно распространить действие рекурсии и индукции.
- Рассмотрим АТД “натуральное число”, операции и предикаты, определённые на нем, а также определение новых операций и предикатов на этих АТД с помощью индукции и рекурсии. Этот АТД описывается в виде многоосновной алгебраической системы. Заметим, что каждую алгебраическую систему [Мальцев-70] можно рассматривать как многоосновную алгебру. Действительно, если

$$A=(\mathrm{A},\ \Omega=\left\{\omega_1^{k_1},...,\omega_n^{k_n}\right\},\ \Pi=\left\{\pi_1^{m_1},...,\pi_r^{m_r}\right\}),\quad i=1,2,...,n,\ j=1,2,...r,$$

- алгебраическая система, где $w_i^{k_i}: A^{k_i}\to A$, $\pi_j^{m_j}: A^{m_j}\to\{true(1),\ false(0)\}$, а *true* и *false* булевские константы (обычно обозначаемые как 1 и 0), то с этой системой ассоциируется двухосновная алгебра

$$A=(U=(A,\{true,\ false\}),\Omega=\{\omega_1^{k_1},...,\omega_n^{k_n},\pi_1^{m_1},...,\pi_r^{m_r}\}).$$

- В этой многоосновной алгебре каждая операция $w_i^{k_i}$ имеет тип элементов множества *A*, а каждая операция $\pi_j^{m_j}$ имеет тип булевский. Таким образом при рассмотрении АТД как алгебраической системы мы имеем дело с многоосновными алгебрами.

Алгебраическая система «натуральное число»

Аксиоматика. Рассмотрим АТД *N*, элементы которого называются натуральными числами. Как известно этот тип данных определяется аксиоматическим способом:

1. $0\in N$;

2. $s: N\to N$ - унарная операция, называемая “следующее натуральное” и удовлетворяет условию: если $n\in N$, то $s(n)\in N$;

3. $\forall n\in N\ s(n)\neq 0$;

4. если $s(n)=s(m)$, то $m=n$;

5. если *A* - множество такое, что $0\in A$ и из того, что для произвольного $n\in A$ вытекает $s(n)\in A$, то $A=N$.

Это известная *аксиоматическая система Пеано* и ее алгебраическая система принимает вид:

$$A=(N,\Omega=\{0,s\},\Pi=\{=\}),$$

где *N* - носитель алгебраической системы, *0, s* – нульарная и унарная операции на *N* (причём, операция *s(x) = x + 1*), а = - бинарный предикат равенства, определённый на *N*.

Наличие непустых множеств операций и предикатов, определённых на множестве *N*, позволяет ввести в рассмотрение множества термов (алгебраических выражений) и формул, пользуясь традиционными булевыми связками.

Сначала заметим, что каждое натуральное число можно получить с помощью операций *0* и *s*. Действительно, пусть $m \in N$ - любое натуральное число, тогда

$$m = \underbrace{s(...s(s}_{m \text{ раз}}(0)))...),$$

где операция *s* применяется *m* раз к числу *0.*

Аксиома 4 использует кроме операции *s(n)* также операцию *pr(n)*, которая называется “предшественник” числа *n*, причем *pr(0)=0*. Эти операции связаны между собой очевидными соотношениями *pr(s(n)) = n* и *s(pr(n)) = n*, если $n \neq 0$.

Множество термов T_N определяется индуктивно.

Определение 1. Термами называются выражения, построенные по таким правилам:

а) *0* - терм,

б) если *n* терм, то *s(n)* и *pr(n)* - термы,

в) термами есть те и только те выражения, которые построены по правилам а) - б).

Множество формул F_N определяется индуктивно аналогичным образом.

Определение 2. Формулами называются выражения, построенные по таким правилам:

а) *true, false* - формулы,

б) если *m, n* - термы, то *m = n* - формула,

в) если *A* и *B* - формулы, то $A \wedge B, A \vee B, A \to B$ - формулы,

г) формулами являются те и только те выражения, которые построены по правилам а) - в).

Пользуясь этими множествами, вышеприведенную алгебраическую систему можно расширить таким образом:

$$\mathrm{A} = (U = (T_N, F_N), \Omega = \{0, s, pr, \neg, \vee, \wedge, \to\}, \Pi = \{true,\ false, =\}),$$

где $s, pr : T_N \to T_N$, $=: T_N \times T_N \to F_N,$

$\vee, \wedge, \to: F_N \times F_N \to F_N$, $\neg : F_N \to F_N$.

Следовательно, полученная таким способом АС, является двухосновной и ее называют ***моделью Пеано***. Используя индуктивное определение множества натуральных чисел *N*, можно ввести операцию декартового произведения $N \times N.$

Элементами множества $N \times N$ являются те и только те элементы, которые построены по правилам:

а) $(0,0) \in N \times N,$

б) если $(m, n) \in N \times N,$ то *(s(m),n)* и *(m,s(n))* $\in N \times N.$

Это определение очевидным образом обобщается на произвольные множества *A, B,…,C* и функцию *f*, которые имеют индуктивные определения.

Определение традиционных операций и предикатов

Операции. Напомним сначала схему операции примитивной рекурсии, с помощью которой определяются функции. Будем говорить, что *(n+1)*-арная функция *f* получена из *n*-арной функции *g* и *(n+2)*-арной функции *h* с помощью ***операции примитивной рекурсии***, если

$$f(x_1, x_2, ..., x_{n-1}, x_n, 0) = g(x_1, x_2, ..., x_n);$$

$$f(x_1, x_2, ..., x_{n-1}, x_n, s(y)) = h(x_1, x_2, ..., x_n, y, f(x_1, x_2, ..., x_n, y)).$$

Частным случаем примитивной рекурсии является ***итерация***, схема которой имеет вид [Гудст-70]:

$$f(x_1, x_2, ..., x_{n-1}, x_n, 0) = g(x_1, x_2, ..., x_n);$$

$$f(x_1, x_2, ..., x_{n-1}, x_n, s(y)) = h(x_1, x_2, ..., x_n, f(x_1, x_2, ..., x_n, y)).$$

Введем операцию сложения натуральных чисел “*plus*”, пользуясь операциями полученной АС и рекурсии. Это определение имеет вид:

plus(0,y) = y;

plus(s(x),y) = s(plus(x,y)).

Можно ввести операцию сложения и другим способом:

plus(0,y) = y;

plus(s(x),y) = plus(x,s(y))).

С помощью операции *plus*, вводится операция умножения *mult (x,y)* натуральных чисел *x* и *y:*

mult(0,y) = 0;

mult(s(x),y) = plus(mult(x,y),y)).

Используя операции *s* и *pr*, введенные выше операции *plus* и *mult* принимают вид:

plus(x,y) = if x = 0 then y else s(plus(pr(x),y)),

mult(x,y) = if x = 0 then 0 else plus(mult(pr(x),y),y).

Из этих определений вытекает, что в обоих операциях присутствует унарный предикат *x = 0*. Расширим сигнатуру предикатов АС этим предикатом, который обозначим *isz : N* $\to$ *{true, false}* (is zero). Теперь ***алгебраическая система N*** принимает вид:

$$A = (U = (T_N, F_N), \Omega = \{0, s, pr, \neg, \vee, \wedge, \to\}, \ \Pi = \{true, \ false, =, isz\}),$$

с *множеством аксиом* для введенных операций *pr(x)* и предиката *isz(x):*

$$\neg(true) = false, \qquad \neg(false) = true,$$

$$isz(0) = true; \qquad isz(s(x)) = false;$$

$$pr(0) = 0; \ \ pr(s(x)) = x; \qquad \neg(isz(x)) \to (s(pr(x)) = x).$$

В новой системе аксиомы 3 и 4 принимают вид: *isz(s(x)) = false* и *pr(s(x)) = x* соответственно. Действительно, из того что *s(x) = s(y)* вытекает *pr(s(x)) = x = pr(s(y)) = y*. Введем ещё некоторые функции и предикаты, пользуясь возможностями этой АС:

$$sg(m) = \begin{cases} 0, если\ m = 0, \\ 1, если\ m > 0, \end{cases} \quad \overline{sg}(m) = \begin{cases} 1, если\ m = 0, \\ 0, если\ m > 0, \end{cases} \quad monus(m,n) = \begin{cases} m - n, если\ m \geq n, \\ 0, если\ m < n. \end{cases}$$

Хорошо известно, что эти функции можно получить операцией примитивной рекурсии [Мальцев-70]. Заметим также, что операция *pr(m)* - примитивно рекурсивная функция, поскольку

pr(0) = 0, pr(s(m)) = m.

Предикаты. Пользуясь этими функциями, получаем выражения для функции |m - n| и предикатов m = n (eq(m,n)), m $\leq$ n (leg(m,n)), m < n (less(m,n)):

|m - n| = monus(m,n) + monus(n,m), eq(m,n) = $\overline{sg}$ (|m-n|) = $\overline{sg}$ (monus(m,n) + monus(n,m)),

leq(m,n) =monus(1,monus(m,n)), less(m,n) = $\overline{sg}$ ($\overline{sg}$ (monus(n,m))).

Нетрудно показать, что эти функции и предикаты удовлетворяют таким соотношениям:

monus(0,m) = 0, |m - 0| = |0 - m| = m,

eq(0,s(n)) = eq(s(m),0) = false, eq(0,0) = true,

leq(0,s(n)) = true, leq(s(m),0) = false, leq(0,0) = true,

less(0,s(n)) = true, less(s(m),0) = false, less(0,0) = false

и если *m >0, n> 0*, то

monus(m,n) = monus(pr(m),pr(n)),

|m - n| = |pr(m) - pr(n)|,

eq(m,n) = eq(pr(m),pr(n)),

leq(m,n) = leq(pr(m),pr(n)),

less(m,n) = less(pr(m),pr(n)).

Эти соотношения стают полезными при вычислении значений этих функций и предикатов.

Заметим, что в этой АС предикат eq (предикат =) становится производным, т .е. выражается через предикат *isz*. Исходя из этого, АС *N* принимает более лаконичный вид:

$$A = (U = (T_N, F_N), \Omega = \{0, s, pr, \neg, \vee, \wedge, \rightarrow\}, \Pi = \{true, false, isz\}).$$

Операции *plus* и *mult* в этой АС принимают вид:

plus(m,n) = if isz(m) then n else s(plus(pr(m),n)).

mult(m,n) = if isz(m) then 0 else plus(mult(pr(m),n),n).

Из определения *leq* ($\leq$) вытекают такие свойства:

а) (рефлексивность *leq*). Действительно, *leq(m,m) = true*, и в силу свойств этого предиката получаем *leq(m,m) = leq(0,0) = true*.

б) (антисимметричность *leq*). Если *leq(m,n) = true* и *leq(n,m) = true*, то в силу свойств этого предиката получаем: *leq(m,n) = true* и *leq(n,m) = true* тогда и только тогда, когда *leq(0,n') = true* и *leq(n',0) = true*, но это возможно только в том случае, когда *n' = 0*, а это значит что *m = n.*

в) (транзитивность leq). Если leq(m,n) = true и leq(n,k) = true, то leq(m,n) = true тогда и только тогда, когда leq(0,n') = true, где n' $= \underbrace{pr(...pr(pr}_{m\ \text{раз}}(n))...)),$ и leq(n,k) = true $\Leftrightarrow$ leq(0,k') = true, где k'

$= \underbrace{pr(...pr(pr}_{n\ \text{раз}}(k))...)).$ Тогда leq(m,k) = true $\Leftrightarrow$ leq(0,k'') = true, где

k'' $= \underbrace{pr(...pr(pr}_{m\ \text{раз}}(k))...)),$ и *leq(n',k'') = true* в силу *leq(n,k) = true*.

г) Из вышеприведённых свойств предиката вытекает, что любые два элемента множества *N* сравнимы. Следовательно, отношение *leq* является отношением линейного порядка. Более того, из аксиомы 5 вытекает, что множество *N* является полностью упорядоченным, т. е. произвольное непустое его подмножество имеет минимальный элемент. Действительно, предположим что существует подмножество *B* множества *N*, в котором нет минимального элемента. Рассмотрим множество *C = N \ B*. Та как $0 \in C$ (в противном случае 0 был бы минимальным в *B*), то *s(0)* $\in$ *C* на том же основании. Но тогда в множестве *C* нет ни одного элемента, поскольку *C = N* в силу аксиомы 5. А отсюда следует, что *B* = $\varnothing$.

С помощью операции *mult* вводится отношение *делимости* натуральных чисел.

Определение 3. Натуральное число m называется кратным натуральному числу x, если существует такое натуральное число y, что m = mult(x,y). Число x в этом случае называется делителем числа m (обозначение m|x).

Далее, с помощью введённых выше предикатов вводятся бинарные функции *floor(m,n)* - наибольшее целое число, не превосходящее частного от деления *m* на *n*), *ceil(m,n)* - наименьшее целое число, не меньшее частного от деления *m* на *n*), а также операция mod*(m,n)* - частное от деления *m* на *n* (*n > 0*):

$$floor(m,n)=\begin{cases}0,\ if\ \ m=0,\\ \sum_{i=1}^{m}\overline{sg}\ (\ mult\ (i,n),\ m),\ in\ other\ case.\end{cases}$$

$$ceil(m,n)=\begin{cases}0,\ \ if\ \ m=0,\\ s(\sum_{i=1}^{m}\overline{sg}\ (\ mult\ (i,n),\ m)),\ \ in\ other\ case.\end{cases}$$

$$\mathrm{mod}(m,n)=\begin{cases}m,\ if\ \ less(m,n)=true,\\ \mathrm{mod}\ (\ monus\ (m,n),\ n),\ in\ other\ case.\end{cases}$$

Из этих определений вытекают такие простейшие свойства введённых функций:

floor(0,n) = 0, ceil(0,n) = 0,

floor(m,n) = ceil(m,n) тогда и только тогда, когда *m*|*n*,

ceil(m,n) - floor(m,n) = 1, если m $\neq$ 0,

mod(0,n) = 0, m = mult(n,floor(m,n)) + mod(m,n),

mod(m,n) = m/n – mult(n,floor(m,n)), если n $\neq$ 0.

Свойства операций, предикатов и отношений

Операции, предикаты и отношения, определённые на данной АС, имеют хорошо известные свойства. Прежде всего это предикат равенства, который является рефлексивным, симметричным, транзитивным и удовлетворяет свойству подстановки, т. е. $\forall x, y, z \in N$

(PE) x = x, (CE) x = y $\rightarrow$ y = x, (TE) (x = y $\wedge$ y = z) $\rightarrow$ x = z,

(SE) (t = t' $\wedge$ f(...t...)) $\rightarrow$ f(...t'...).

Операции *plus* и *mult* удовлетворяют законам коммутативности, ассоциативности и дистрибутивности. Т. е. имеет место

Теорема 1. а) plus(x,y) = plus(y,x), б) plus(x,plus(y,z)) = plus(plus(x,y),z),

в) mult(x,y) = mult(y,x), г) mult(x,mult(y,z)) = mult(mult(x,y),z),

д) mult(x,plus(y,z)) = plus(mult(x,y),mult(x,z)).

Доказательство оставляем читателю.

На основе коммутативности операции *mult,* получаем, что когда число *x* является делителем числа *m*, т. е. существует такое число *y*, что *m = mult(x,y)*, то и число *y* тоже является делителем числа *m*. В частности, отсюда вытекает, что 1 и *m* являются делителями *m*.

Отношение делимости рефлексивное, транзитивное и антисимметричное:

а) m |m (рефлексивность),

б) m|n $\wedge$ n|k $\rightarrow$ m |k (транзитивность),

в) m|n $\wedge$ n|m $\rightarrow$ m = n (антисимметричность).

В самом деле, в случае а) имеем:

mult(1,m) = plus(mult(pr(1),m),m) = plus(mult(0,m),m) = plus(0,m) = m.

В случае б) на основе теоремы 1.в) и 1.г) получаем:

m = mult(n,x) $\wedge$ n = mult(k,y) $\rightarrow$ mult(mult(k,y),x) = mult(k,mult(y,x)).

Отсюда следует, что *m*|*k*. В случае в) имеем *m = mult(n,k)* $\wedge$ *n = mult(m,s)*. Отсюда получаем:

m = mult(mult(m,s),k) = mult(mult(s,m),k) = mult(s,mult(m,k)) = plus(mult(pr(s),mult(m,k)),mult(m,k)).

Это равенство выполняется только в том случае, когда pr(s) = 0 и k = 1, т. е. s = k = 1. Но тогда n = mult(m,1) = mult(1,m) = plus(mult(0,m),m) = plus(0,m) = m.

На основе рефлексивности отношения делимости вводятся понятия простого числа и общего делителя. Число *m* называется *простым*, если оно имеет всего два делителя 1 и *m*. Пусть *m, n* $\in N$ и существует *x* $\in N$ такое, что *m*|*x* и *n*|*x*. В этом случае число *x* называется *общим делителем* чисел m и n. Наибольшее среди общих делителей число *k* называется *наибольшим общим делителем* чисел *m* и *n* (*НОД(m,n)*) Из полученных свойств отношения делимости вытекают следующие свойства НОД:

НОД(m,m) = m,

НОД(m,n) = НОД(m-n,n), если m > n и

НОД(m,n) = НОД(m,n-m), если m < n.

Отсюда, как правило, начинаются курсы по теории чисел и формальной арифметике.

Трансфинитная индукция и рекурсия

Рассмотренная алгебраическая система имеет носителем полностью упорядоченное множество (пум) натуральных чисел *N*. Возникает вопрос: на каждое ли полностью упорядоченное множество (пум) распространяется принцип математической индукции и рекурсии?

Полностью упорядоченные множества. Прежде чем давать ответ на этот вопрос, рассмотрим структуру пум. Непосредственно из определения пум вытекает, что пум имеет наименьший элемент. Кроме того,

- для каждого элемента *x*, кроме максимального, в пум существует элемент *y*, который является непосредственно следующим для *x*, т. е. если *y* непосредственно следует за *x*, то не существует элемента *z*, для которого выполняются неравенства *y > z > x* (отношение доминирования в пум); элемент, который непосредственно следует за элементом *x* обозначается *x + 1*, за ним *x + 2* и т. д. (аналог операции *s(x)* на множестве *N*);

- некоторые элементы в пум могут не иметь непосредственного предшественника (например, если $N \times N$ есть множеством, элементы которого упорядочены отношением лексикографического порядка $(m,n) \leq (m',n') \Leftrightarrow (m < m') \vee ((m = m') \wedge (n \leq n'))$, то элементы *(n,0)* не будут иметь предшественника и такие элементы называются *предельными*;

- произвольный элемент пум имеет вид *x + n*, где *x* - предельный элемент, а *n* - натуральное число (обозначение *x + n* следует понимать в смысле первого из этих пунктов). Действительно, если *x* не предельный элемент, то возьмём его непосредственного предшественника *pr(x),* и если он не предельный, то возьмём его непосредственного предшественника *pr(pr(x))* и т. д. Бесконечно этот процесс длится не может в силу полной упорядоченности множества. Понятно также, что такое представление элементов пум однозначно, поскольку в каждого элемента может быть не более одного предшественника. Имеет место такое очевидное утверждение.

Теорема 2. Произвольное ограниченное сверху пум имеет наибольший элемент.

Доказательство. Множество *A* называется ограниченным сверху, если существует элемент $a \in A$ такой, что для всех $x \in A$ выполняется неравенство $x \leq a$. Поскольку любой элемент пум имеет вид *x + n*, то когда этот элемент имеет непосредственно следующего, то выбираем этот следующий и т. д. Этот выбор не может быть бесконечным, поскольку множество *A* ограничено сверху. Последний из выбранных элементов, для которого в множестве *A* не существует следующего за ним элемента и будет искомым элементом. □

Одним из способов построения пум является операция декартового произведения. Рассмотрим декартово произведение $N \times N$. На этом множестве можно определить разные порядки. Чаще всего встречаются покоординатный порядок и лексикографический порядок, о котором говорилось выше. Определение покоординатного порядка имеет вид:

(m,n) $\leq$(m',n') $\Leftrightarrow$ (m $\leq$ m') $\wedge$ (n $\leq$ n'),

а определение лексикографического выглядит так:

(m,n) $\leq$ (m',n') $\Leftrightarrow$ (m < m') $\vee$ (m = m') $\wedge$ (n $\leq$n').

Первый из этих порядков частичный, а второй линейный и, даже, полный. Он имеет вид *(0,0)* < *(0,1)* < *(0,2)* < … < *(1,0)* < *(1,1)* < … < *(2,0)* > *(2,1)* < … . Как отмечалось, у элементов вида (*n,0*) нет предшественников и они являются предельными. Общий случай построения пум вытекает из такого утверждения.

Теорема 3. Если множество A полностью упорядочено, то декартово произведение A$\times$A тоже полностью упорядоченное множество относительно лексикографического порядка.

Доказательство. Пусть *B* $\subseteq$*A*$\times$*A, (a,b)* $\in$ *B* = $A_1 \times A_2$, где $A_1, A_2 \subseteq$*A* и a_0, b_0 - наименьшие элементы в множествах A_1, A_2 соответственно. Если $a \neq a_0$ и $b \neq b_0$ (иначе *(a,b)* - наименьший элемент в множестве *B*), то рассмотрим последовательность элементов

(a,b), (pr(a),b), (pr(pr(a)),b),…,(a_0*',b), (* a_0*',pr(b)), (* a_0*',pr(pr(b))),…,* (a_0, b_0).

Эта последовательность не может быть бесконечной в силу полной упорядоченности множеств *A*. Тогда элемент (a_0, b_0) - наименьший элемент в множестве *B*. □

Примером такого типа пум может служить множество всех слов *F(X)* конечной длины в некотором конечном алфавите *X*, при условии, что символы алфавита *X* линейно упорядочены. Свойства этого множества детально исследовались в работе [Крывый-10].

Следующая теорема даёт ответ на поставленный выше вопрос.

Теорема 4 [Принцип трансфинитной индукции]. Пусть a_0 - наименьший элемент в пум A и P(x) – некоторое свойство элемента x $\in$A. Тогда, если из истинности P(a_0) и P(x) для всех x < a вытекает истинность P(a), то P(x) истинно для всех x из A.

Доказательство. Допустим противное, т. е. что существует такое непустое подмножество *A'* элементов из *A*, что *P(a*) ложно на элементах этого множества при выполнении условий теоремы. Пусть *a* - минимальный элемент в *A'*. Поскольку *P(* a_0*)* истинно, то *a* $\neq$ a_0 и *a* > a_0. Из условий теоремы вытекает, что *P(x)* истинно для всех *x* < *a*, но тогда из этих же условий должна следовать истинность и *P(a),* а это противоречит нашему предположению. □

Перейдём к рассмотрению рекурсии. Сначала введём понятие начального отрезка линейно упорядоченного множества. Если линейно упорядоченное множество *A* разбито на два непересекающиеся подмножества *B* и *C* так, что любой элемент множества *B* меньше произвольного элемента множества *C*, то множество *B* называют *начальным отрезком множества A*.

Пусть *A* - произвольное пум. Поскольку пум является линейно упорядоченным множеством, которое имеет минимальный элемент, то будем обозначать этот элемент 0, а произвольный его начальный отрезок - *[0,x)* или *[0,x].* Мы хотим дать рекурсивное определение функции *f : A* $\rightarrow$*B*, где *B* - некоторое множество. Такое определение должно связывать значения функции *f(x)* на некотором элементе *x* $\in$*A* со значениями *f(y)* для всех *y* < *x*. Это значит, что рекурсивное определение определяет функцию *f(x)* в предположении, что известно ограничение функции *f* на начальный отрезок *[0,x)* множества *A*. Обозначим $f|_{[0,x)}$ сужение функции *f* на начальный отрезок *[0,x).*

Теорема 5. Пусть A - пум, B - произвольное множество и задано некоторое рекурсивное правило, т.е. функция F, которая ставит в соответствие элементу $x \in A$ и функции g: [0,x) $\to$ B некоторый элемент множества B. Тогда существует единственная функция f:A$\to$B, для которой f(x)=F(x, $f|_{[0,x)}$) для всех $x \in A$.

Доказательство теоремы вытекает из такого утверждения: существует единственное отображение *f* отрезка *[0,a]* в множество *B*, для которого рекурсивное определение *f(x) = F(x,* $f|_{[0,x)}$)) выполняется для всех $x \in [0,a]$. Такое отображение будем называть *корректным*. Следовательно, необходимо доказать, что для каждого $a \in A$ существует единственное корректное отображение *f* отрезка *[0,a]* в множество *B*.

Допустим, что для всех *c<a* утверждение имеет место. Это значит, что существует единственное корректное отображение f_c: *[0,c]* $\to$ *B*, т. е. что для всех $d \le c$ значения f_c совпадают со значениями, которые получены на основе рекурсивного определения.

Рассмотрим отображения f_{c_1} и f_{c_2} для двух разных значений c_1 и c_2. Пусть, например, $c_1 < < c_2$. Отображение f_{c_2} определено на большем отрезке *[0,* c_2*]* и если f_{c_2} ограничить на меньший отрезок, то оно совпадет с f_{c_1}, поскольку ограничение корректного отображения на меньший отрезок будет корректным отображением в силу предположения о единственности отображения на отрезке *[0,* c_1*].*

Таким образом, все отображения f_c согласуются между собой в том смысле, что когда их значения определены, то они одинаковы. Объединяя их, получаем некоторое единственное отображение *h*, которое определено на отрезке *[0,a).* Применяя к *a* и *h* рекурсивное правило, получаем некоторое значение $b \in B$. Доопределим *h* в точке *a*, полагая *h(a) = b*. В результате получаем отображение *h : [0,a]* $\to$ *B*, которое, очевидно, является корректным.

Покажем, что на отрезке *[0,a]* корректное отображение единственно. Действительно, его ограничение на отрезок *[0,c]* при *c < a* должно совпадать с f_c и остаётся показать, что в точке *a* это отображение однозначно. Но последнее гарантируется рекурсивным определением. Этим индуктивное доказательство завершается.

Остаётся заметить, что для разных *a* корректные отображения согласуются между собой и поэтому задают некоторую функцию *f : A* $\to$ *B*, которая удовлетворяет рекурсивному определению.

Таким образом, доказано существование и единственность функции, поскольку ограничение этой функции на произвольный отрезок *[0,a]* корректно и поэтому определено однозначно. □

Аналогичная ситуация возможна и в общем случае, т. е. в случае когда рекурсивное правило не полностью определено. Введём общее понятие согласованности функций (частный случай которого фигурировал в доказательстве предыдущей теоремы), заданных на одних и тех множествах.

Определение 4. Пусть *A* - пум, а *B* - произвольное множество. Частичные функции *f : A*$\to$*B* и *g : A*$\to$*B* называются *согласованными функциями*, если *f(x)* и *g(x)* или одновременно не определены, или определены и *f(x) = g(x),* где $x \in A$.

Имеет место

Теорема 6 [Принцип трансфинитной рекурсии]. Пусть f(x) = F(x, $f|_{[0,x)}$) является частичным отображением, т. е. для некоторых x и g : [0,x) $\to$ B оно может быть не определено. Тогда существует единственная функция f, которая

1) или определена на всем множестве A и согласована с рекурсивным определением, т. е. f(x) = F(x, $f|_{[0,x)}$);

2) или определена на некотором начальном отрезке [0,a) и на нём согласована с рекурсивным определением, причём для точки a и функции f рекурсивное правило неприменимо (отображение F не определено).

Доказательство. Дополним множество *B* специальным элементом $\perp$, который обозначает неопределённость отображения, и модифицируем рекурсивное правило таким образом. Новое правило даёт значение $\perp$ тогда, когда старое правило было не определено, вне зависимости от того, встречалось ли ранее значение $\perp$, или нет.

Применяя к модифицированному правилу теорему 5, получаем некоторую функцию *f′*. Если эта функция не принимает значения $\perp$ на любом из значений своих аргументов, то имеет место случай 1), который приведен в условии теоремы (при *f* = *f′*). Если же функция *f′* принимает значения $\perp$ при некотором значении *a* своего аргумента, то она принимает это же значение и на всех значениях аргументов больших *a*. Заменяя значение $\perp$ на неопределённость, получаем из функции *f′* функцию *f*. Областью определения функции *f* выступает некоторые начальный отрезок *[0,a)* и, следовательно, имеет место случай 2), приведённый в условии теоремы. □

Теперь можно дать ответ на поставленный выше вопрос. Этот ответ вытекает из теоремы Цермело.

Теорема Цермело. Произвольное множество можно полностью упорядочить.

Доказательство этой теоремы строится на аксиоме выбора и вызывает большое количество нареканий своей неконструктивностью. На счётном множестве полный порядок указать нетрудно, поскольку полный порядок с *N* переносится на данное счётное множество (и этого достаточно для некоторых областей науки о вычислениях). Но в случае множества действительных чисел никакого конкретного полного порядка указать нельзя и, доказав с помощью аксиомы выбора его существование, мы так и не можем себе этот порядок представить.

Пусть *A* некоторое заданное множество. Рассмотрим в каком виде используется аксиома выбора. Допустим, что существует функция φ, определённая на всех собственных подмножествах множества *A*, кроме самого множества *A*, которая ставит в соответствие один элемент за пределами этого подмножества:

$$X \subseteq A \Rightarrow \varphi(X) \in A \setminus X.$$

После того, как такая функция зафиксирована, можно строить полный порядок на множестве *A* таким способом. Наименьшим элементом множества *A* объявляем элемент $a_0 = \varphi(\varnothing)$. За ним идет элемент $a_1 = \varphi(\{a_0\})$. По построению он отличается от a_0. Далее идет элемент $a_2 = \varphi(\{a_0, a_1\})$ и т. д. Если множество *A* бесконечно, то такой процесс можно продолжать и получать последовательность $a_0, a_1, a_2, \dots$. Если и после этого остаются нерассмотренные элементы в множестве *A*, то строим элемент $w = \varphi(\{a_0, a_1, a_2, \dots\})$ и так будем продолжать до тех пор, пока не исчерпаем всё множество *A*. Когда этот процесс закончится, то полученный порядок будет полным порядком на множестве *A*. □

Из теоремы Цермело следует, что возможность распространения рекурсивных и индуктивных определений на трансфинитные области было бы конструктивным, если бы была конструктивной аксиома выбора.

Частично упорядоченные множества. Как следует из доказательства теоремы Цермело, построение полного порядка на множестве *A* желает лучшего. В связи с этим, рассмотрим вопрос распространения принципа математической индукции и рекурсии на частично упорядоченные множества (чум). Ответ на этот вопрос даёт такая

Теорема 7. Следующие свойства чум A эквивалентны:

a) любое непустое подмножество множества A имеет минимальный элемент;

б) в множестве A не существует бесконечной строго убывающей последовательности элементов $a_0 > a_1 > a_2 > \ldots$;

в) на множестве A выполняется принцип математической индукции в таком виде: если для каждого x $\in$ A из истинности свойства P(y) для всех y < x вытекает истинность P(x), то свойство P(x) истинно для всех x из A.

Доказательство. **а)** $\rightarrow$ **б)**. Пусть произвольное непустое подмножество множества *A* имеет минимальный элемент. Если $a_0 > a_1 > a_2 > \ldots$ - бесконечная строго убывающая последовательность, то подмножество *B* = $\{a_0 > a_1 > a_2 > \ldots\}$ не будет иметь минимального элемента, поскольку для любого a_n существует меньший элемент a_{n+1}. Получаем противоречие с существованием в множестве *B* минимального элемента.

б) $\rightarrow$ **а)**. Пусть *B* - непустое подмножество множества *A*, которое не имеет минимального элемента. Тогда бесконечную убывающую последовательность в множестве *B* можно построить таким образом. Возьмём произвольный элемент $b_0 \in B$. Этот элемент не является минимальным в силу предположения. Возьмём $b_1 \in B$ такой, что $b_0 > b_1$. На том же основании элемент b_1 не является минимальным. Далее находим b_2 < b_1 < b_0 и т. д. В результате получаем бесконечную убывающую последовательность, что противоречит условию б).

а) $\rightarrow$ **в)**. Пусть *P(x)* – произвольное свойство элементов из множества *A*. Предположим, что *P(x)* истинное не для всех элементов из *A*. Пусть *B* означает множество элементов, для которых *P(x)* ложно. Свойство *P(* a_0*)* истинное на минимальном элементе $a_0 \in A$ и поэтому $a_0 \notin B$. Для всех *a* < *b*, де *b* - минимальный элемент в множестве *B* свойство *P(a)* выполняется. Но тогда должно выполняться и *P(b)*. Полученное противоречие доказывает утверждение.

в) $\rightarrow$ **а).** Пусть *B* - подмножество множества *A*, в котором отсутствует минимальный элемент. Докажем с помощью индукции, что множество *B* пусто. Пусть *P(x)* означает свойство *x* $\notin$ *B*. Тогда свойство *P(y)* выполняется для всех *y* < *x*, т. е. ни один элемент, меньше *x* не принадлежит к *B*. Если бы *x* принадлежал к *B*, то *x* был бы там минимальным элементом, а это противоречит предположению об отсутствии таких элементов в множестве *B*. □

Доказанная теорема даёт возможность ввести такое определение.

Определение *5.* Чум, для которого выполняется одно из условий выше доказанной теоремы (а, следовательно, и остальные условия), называется *фундированным множеством*.

Примеры фундированных множеств.

1) Множество натуральных чисел N относительно частичного порядка делимости, т. е. *m* < *n* $\Leftrightarrow$ *m* делитель *n*.

2) Множество N $\times$ N относительно частичного порядка (m,n) $\leq$ (m',n') $\Leftrightarrow$ (m < m') $\vee$ (m = m' $\wedge$ $\wedge$ n $\leq$ n'). Для проверки справедливости условия б) выполним такие действия. Пусть

$$(a_0, b_0) \geq \geq (a_1, b_1) \geq (a_2, b_2) \geq \ldots -$$

произвольная последовательность элементов из N $\times$ N. По определению частичного порядка сравниваем первые компоненты пар $a_0 \geq a_1 \geq a_2 \geq \ldots$. В силу фундированности множества N эта последовательность стабилизируется на некотором конечном индексе n. После этого другие компоненты b_i должны убывать и тоже стабилизироваться на некотором конечном индексе m. Поскольку m и n конечны, то это даёт стабилизацию всей последовательности.

3) Рассмотренный случай обобщается на произвольные фундированные множества, что вытекает из следующей теоремы.

Теорема 8. Пусть A и B - два фундированных множества. Тогда их декартово произведение $A \times B$ тоже фундированное множество относительно частичного порядка $(a,b) \leq (a',b') \Leftrightarrow [(a < a') \vee (a = a' \wedge b \leq b')]$.

Доказательство. В последовательности $(a_0, b_0) \geq (a_1, b_1) \geq (a_2, b_2) \geq \dots$ сначала стабилизируются первые компоненты, а потом вторые. □

Из этой теоремы вытекает, что декартово произведение $A_1 \times A_2 \times \dots \times A_n$ конечного числа фундированных множеств $A_1, A_2, \dots, A_n$ является фундированным множеством.

4) Сумой *A+B* двух непересекающихся множеств называется их теоретико-множественное объединение. Имеет место

Теорема 9. Сума A+B двух фундированных множеств является фундированным множеством.

Доказательство. Любая последовательность $x_1 > x_2 > \dots$ либо полностью принадлежит множеству *B*, либо включает элемент $a \in A$ и тогда все последующие элементы принадлежат к множеству *A*. В первом случае справедливость теоремы следует из фундированности множества *B*, а в другому - из фундированности множества *A*. □

Рассмотренные утверждения и примеры фундированных множеств часто стают полезными при доказательстве терминальности циклов в программах. Например, если необходимо доказать, что данный цикл в программе заканчивается, то вводим (если в этом есть необходимость) некоторый натуральный параметр и убеждаемся в том, что он при каждом повторении цикла уменьшается. Тогда, на основе фундированности множества *N*, этот цикл заканчивается через конечное число повторений.

Лемма Цорна и рекурсия. Часто трансфинитную индукцию или рекурсию заменяют ссылкой на лемму Цорна. Рассмотрим лемму Цорна и причини таких ссылок. Для этого напомним некоторые понятия. *Цепью в чум A* называется произвольное линейно упорядоченное его подмножество *B*. Произвольный элемент $a \in A$ (не обязательно должен быть элементом множества *B*), который удовлетворяет условию $(\forall x \in B)\, x \leq a$, называется *верхней гранью* подмножества *B* в множестве *A*.

Теорема 10 [Лемма Цорна]. Пусть A - чум, в котором каждая цепь имеет верхнюю грань. Тогда в множестве A существует максимальный элемент. Более того, для любого $a \in A$ существует элемент $a \leq b$, который является максимальным в A.

Доказательство. Заметим, что поскольку множество *A* чум, то необходимо различать максимальный и наименьший элементы.

Пусть $a \in A$ – произвольный элемент. Возьмём некоторое пум *I* достаточно большой мощности (большей чем мощность *A*). Построим строго возрастающую функцию $f : I \to A$ при помощи трансфинитной рекурсии. Её значение на минимальном элементе множества *I* положим равным *a*. Допустим, что нам уже известны её значения на всех элементах, меньших некоторого $i \in I$. На основе монотонности *f* эти значения попарно сравнимы между собой. А поэтому существует верхняя грань *s*, которая, в частности, больше или равна *a*. Возьмём некоторый элемент $t > s$ и положим $f(i) = t$. По построению монотонность функции *f* сохраняется. Таким образом, множество *I* равномощно части множества *A*, что противоречит выбору множества *I*. □

Уточним некоторые тонкие моменты этого доказательства, поскольку мы одновременно определяли функцию при помощи трансфинитной рекурсии и доказывали её монотонность при помощи трансфинитной индукции. Наше рекурсивное определение имеет смысл только в тому случае, когда уже построенная часть функции монотонна. Здесь нужно воспользоваться теоремой 6, считая, что следующее значение функции не определено, если уже построенная часть функции не является монотонной, и получить функцию, которая определена на всём множестве *I* или на начальном отрезке. Если функция определена на некотором начальном отрезке, то она монотонна по построению, а поэтому следующее значение тоже определено. А это противоречит частичности функции *f*. □

Ещё одно обстоятельство в доказательстве этой теоремы требует пояснения: можно ли выбрать множество *I*, мощность которого больше мощности *A*? Ответ положительный и вытекает из обобщенной теоремы Кантора.

Теорема 11 [Обобщённая теорема Кантора]. Никакое множество A не может быть равномощно своему булеану B(A). Множество A равномощно некоторому собственному подмножеству множества B(A).

Доказательство. Предположим, что существует взаимно однозначное отображение φ между элементами множества *A* и элементами её булеана *B(A)*. Рассмотрим те элементы $a \in A$, которые не принадлежат соответствующему им подмножеству, и пусть *B* - множество, которое состоит из таких элементов, т. е. $B = \{a \in A : a \notin \varphi(a)\}$.

Покажем, что множество *B* не соответствует ни одному элементу в множестве *B(A)*. Предположим, что это не так и $\varphi(a) = B$ для некоторого элемента $a \in A$. Тогда

$$a \in B \Leftrightarrow a \notin \varphi(a) \Leftrightarrow a \notin B,$$

на основе построения и предположения, что $\varphi(a) = B$. Полученное противоречие показывает, что множество B не соответствует ни одному элементу. Следовательно, отображение φ не является взаимно однозначным.

Равномощность множества *A* и собственного подмножества *B(A)* очевидна, поскольку соответствие есть таким: элементу $a \in A$ соответствует одноэлементное подмножество *{a}* из *B(A)*. □

Заключение

Проведенный анализ показывает, что рекурсия и индукция распространяется на многие частично упорядоченные и полностью упорядоченные множества. С помощью этих операторов описываются такие абстрактные типы данных как списки, строки, стэки, очереди, очереди с приоритетами, бинарные деревья и т. д. (см. [Крывый-10, Hein-95]. Из приведенного анализа также следует, что рекурсию и индукцию можно было бы распространить на произвольные множества, если бы аксиома выбора была конструктивной. А точнее было известно как вычислять функцию, фигурирующую в этой аксиоме.

Библиография

[Ахо-79] Ахо А., Хопкрофт Дж., Ульман Дж. Структуры данных и алгоритмы. –М.: Издат. Дом «Вильямс». - 2000. - 382 с.

[Гудст-70] Гудстейн Р.Л. Рекурсивный математический анализ. – М.: Наука. - 1970. - 472 с.

[Крывый-10] Крывый С.Л. Астрактные типы данных как многоосновные алгебраические системы. – К.: ж. «Инженерия программного обеспечения». – 2010. - № 3. – С. 3 -18.

[Hein-95] Hein J.L. Discrete Mathematics. – Sudbury, Massachusetts: Jones and Bartlett Publishers. -1995.-656 p.

[Мальцев-70] Мальцев А.И. Алгебраические системы . – М.: Наука. - 1970. - 392 с.

Сведения об авторе

***Крывый Сергей** – Киевский национальный университет им. Тараса Шевченка, Украина, Киев, 03680, просп. Глушкова, 4д, Факультет кибернетики. e-mail: krivoi@i.com.ua*