Компьютерная алгебра
(курс лекций)

Игорь Алексеевич Малышев
Computer.Algebra@yandex.ru

Лекция 7

Математические объекты компьютерной алгебры

Содержание лекции

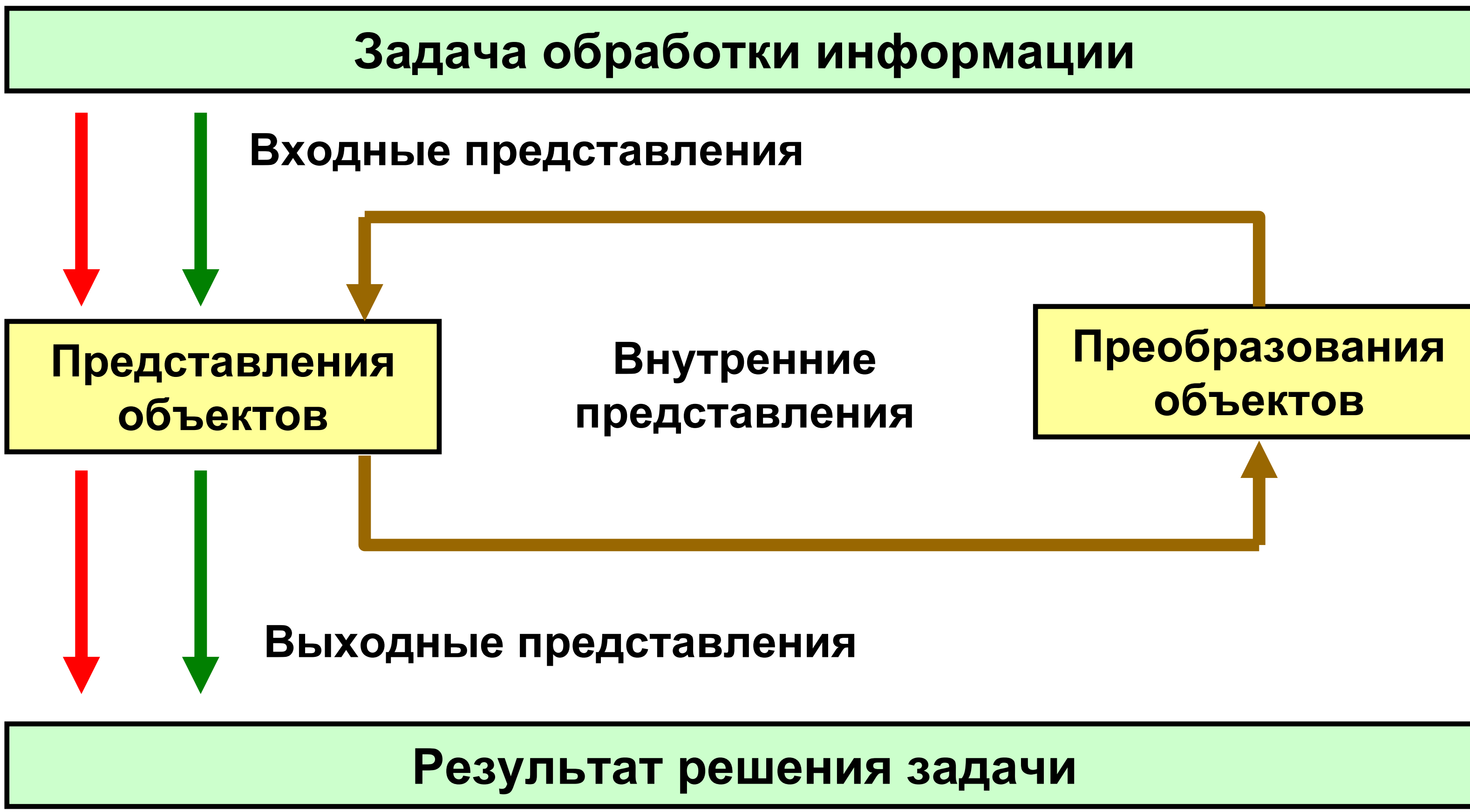
- Свойства представлений математических объектов (МО)
- Символьные представления МО
- Характеристика задач построения эквивалентных представлений
- Представление базовых объектов компьютерной алгебры
- Представление алгебраических функций
- Представление трансцендентных функций
- Представление матриц

План лекции: тема подраздела

- **Свойства представлений математических объектов (МО)**
- Символьные представления МО
- Характеристика задач построения эквивалентных представлений
- Представление базовых объектов компьютерной алгебры
- Представление алгебраических функций
- Представление трансцендентных функций
- Представление матриц

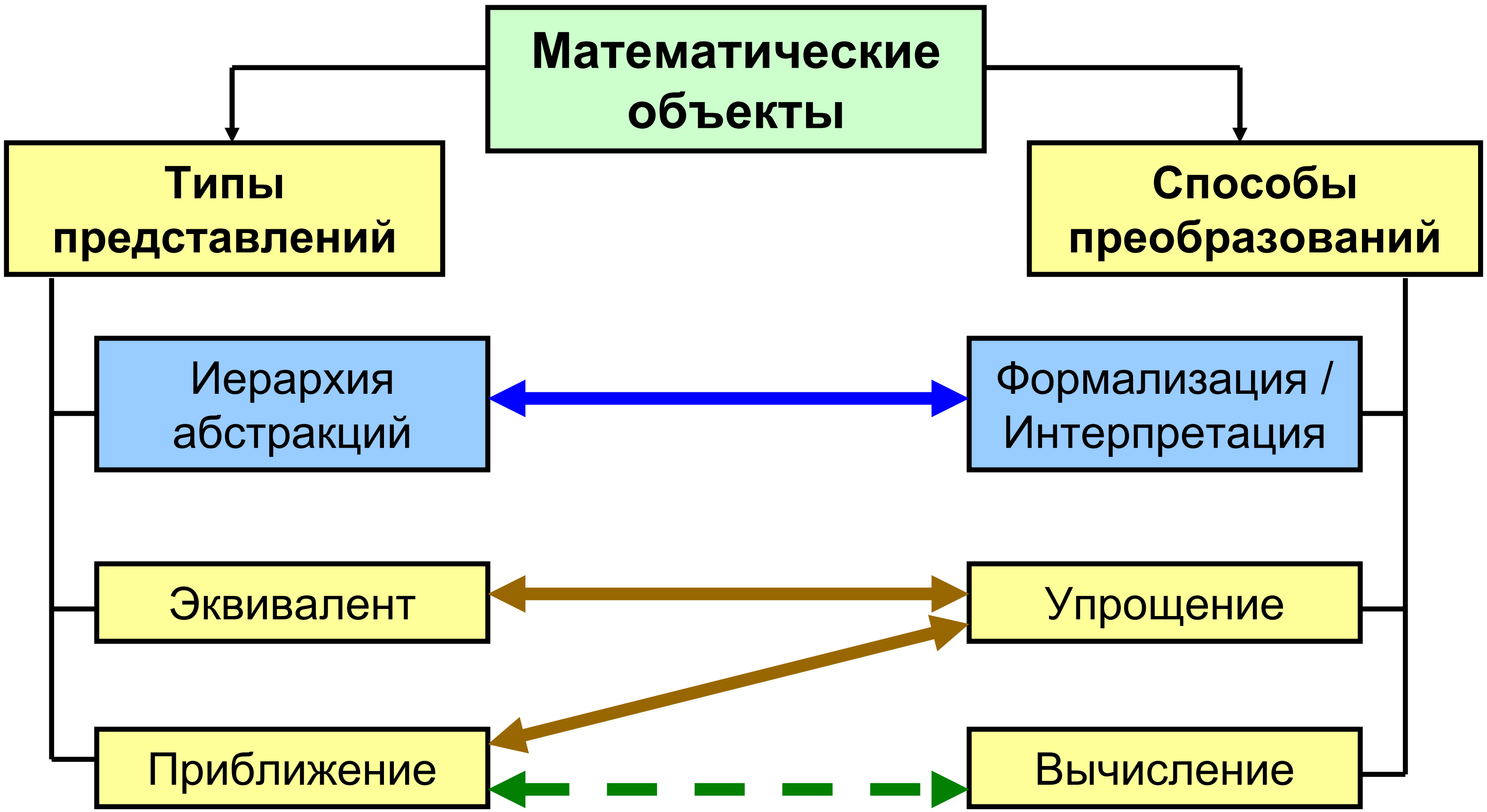
Свойства представлений МО

Жизненный цикл обработки информации



Свойства представлений МО

Представления и преобразования



Свойства представлений МО

Иерархия абстракций представлений

Математические объекты

Предметное представление	Символьное представление	Машинное представление
на языке предметной области	на языке символов алфавита	на языке структур данных
Примеры.	**Примеры.**	**Примеры.**
Иррациональные числа.	2.718 281 828 459 045	+ 2 → 718 → 281
Алгебраические уравнения.	$2 x^{2} + 3 y^{3} = 5$	
Интегральное исчисление.		

Свойства представлений МО

Виды эффективных представлений

Эффективные представления

- по полноте моделируемых свойств математических объектов
  - Канонические представления
  - Нормальные представления
- по способу моделирования особых математических объектов
  - Плотные представления
  - Разреженные представления

Свойства представлений МО

Канонические и нормальные представления

Пусть задано множество объектов M и множество представлений R, между которыми установлено соответствие.

Тогда представление называется **каноническим**, если соответствие является взаимно однозначным, т.е. каждому объекту $m \in M$ соответствует один и только один элемент $r \in R$.

Представление множества объектов M называется **нормальным**, если только для одного (особого) элемента множества объектов, так называемого **нулевого элемента**, существует единственное представление в множестве представлений R.

Чтобы распознать, являются ли два объекта m_1 и m_2 одним и тем же объектом, в случае канонического представления достаточно сравнить их представления r_1 и r_2 .

Чтобы узнать, являются ли два разных представления r_1 и r_2 , представлением одного и того же объекта в случае нормального представления необходимо произвести алгебраическую операцию получения нулевого объекта и, если полученное представление ($r_1 - r_2$) есть представление нулевого объекта, то тогда r_1 и r_2 соответствуют одному объекту из множества M.

Свойства представлений МО

Проблема идентичности объектов

Пример.
X + Y и Y + X – два разных представления одного и того же объекта – полинома.

Важность проблемы идентичности объектов в системах компьютерной алгебры
обусловлена с одной стороны, существованием у объектов
(всюду определённых) алгебраических свойств,
а с другой – невозможностью выполнения операции деления,
если второй операнд равен нулю
(обнаруживаемой и автоматически нейтрализуемой компьютером).

Проблема идентичности
наиболее легко разрешается для канонических представлений,
разрешима (но с бо́льшими трудностями) для нормальных представлений,
не разрешима для всех остальных представлений.

Если мы не можем установить, представляют ли r_1 и r_2 один и тот же объект,
то как корректность выполненных вычислений,
так и результат этих вычислений сомнительны.

Свойства представлений МО

Плотные и разреженные представления

Особую роль в представлениях математических объектов играют нулевые и иные особые элементы алгебраических структур (в частности, бесконечности, пустые множества или соотношения неопределённостей).

Различают два способа моделирования особых элементов :
1) Представлять и хранить особые элементы в структурах данных;
2) Представлять и хранить не сами особые элементы,
   а соглашения о работе с такими элементами.

При втором способе возникает возможность получения более компактного представления данных и более эффективных преобразований над данными.

В **плотных представлениях** хранятся все особые элементы,
а в **разреженных представлениях** – особые элементы не хранятся.

Замечание 1. Плотность и разреженность представлений первоначально рассматривались исключительно по отношению к нулевым элементам.
В настоящее время эти понятия можно обобщить для всех особых элементов.
Замечание 2. Различие эффективности плотных и разреженных представлений наиболее заметно при представлениях полиномов и матриц – математических объектов, при обработке которых очень важен динамический баланс между временной и емкостной сложностями алгоритмов.

План лекции: тема подраздела

- Свойства представлений математических объектов (МО)
- **Символьные представления МО**
- Характеристика задач построения эквивалентных представлений
- Представление базовых объектов компьютерной алгебры
- Представление алгебраических функций
- Представление трансцендентных функций
- Представление матриц

Символьные представления МО

Язык термов

Произвольная совокупность попарно разных символов (букв) $X = \{ x_1, x_2, \dots , x_n, \dots \}$ называется алфавитом. Конечная последовательность букв составляет слово в алфавите X. С помощью пустого слова $e \in X$ и операции конкатенации слов p и q (т.е. приписывании слова q непосредственно после последнего символа слова p) получим **язык слов** F(X).

Язык термов определяется индуктивно.

Алфавит языка термов состоит из трёх типов символов:
1) Предметные символы – T_0 (буквы a, b, x, y, … без индексов и с индексами)
2) Функциональные символы – F (буквы f, g, … с верхними, обозначающими арность, и нижними индексами. Если арность равна нулю, то можно не указывать
3) Символы-разделители – левая и правая круглые скобки, а также запятая.

Термами называют слова, построенные по следующим правилам:
1. Все символы из T_0 – термы.
2. Если $t_1, \dots , t_n$ – термы, то $f^{\,n} (t_1, \dots , t_n)$ – терм ($f^{\,n} \in F, n \geq 1$)
3. Термами являются только те слова, которые определены правилами 1. и 2.

Символьные представления МО

Алгебра термов

Множество всех термов в алфавите X сигнатуры Ω обозначим T (X, Ω).

Определим на множестве T (X, Ω) универсальную алгебру.
Пусть $X = \{ x_1, x_2, \ldots , x_n, \ldots \}$ – некоторый алфавит, а Ω - множество операций.
Представим множество Ω в следующем виде:
$\Omega = \Omega' \cup \Omega_0$, где Ω_0 обозначает множество нульарных операций
(заметим, что арность $f \in F$ в языке термов удовлетворяла условию $n \geq 1$)
Обозначим T (X, Ω') множество термов, в котором $T_0 = X \cup \Omega_0$, а $F = \Omega'$.
Таким образом, получили универсальную алгебру T (X, Ω'),
которую далее будем обозначать T (X, Ω) (имея в виду описанный выше переход)
и называть **алгеброй термов**.

Пусть имеем произвольную алгебру G = (A, Ω) и алгебру термов T (X, Ω).
Заметим, что алгебра G в общем случае может совпадать с T (X, Ω).
Если $\Omega_0 \neq \varnothing$, то пусть a (f) обозначает элемент из A,
который соответствует нульарной операции f из Ω_0.
Рассмотрим отображение $h : T_0 \rightarrow A$ такое, что h (f) = a (f) для $f \in \Omega_0$.
Отображение h можно продлить на всю алгебру T (X, Ω),
если для $p_1, p_2, \ldots , p_n \in T (X, \Omega)$ и $f^{\,n} \in \Omega$ $(n \geq 1)$
положить $h (f \ (p_1, p_2, \ldots , p_n)) = f \ (h (p_1), \ h (p_2), \ \ldots , h (p_n))$.
Отображение h называется **интерпретацией** T (X, Ω) на G.

Символьные представления МО

Задача унификации термов

По определению, множество всех термов $T(X, \Omega)$ содержит множество переменных X.
Подстановкой называется отображение $v: X \to T(X, \Omega)$ такое,
что для всех $x \in X$, за исключением элементов некоторого конечного подмножества из X,
имеет место $v(x) = x$.
Расширим подстановку v до некоторой функции $v' : T(X, \Omega) \to T(X, \Omega)$:
1) если $t \in X$, то $v'(t) = v(t)$;
2) если t – символ константы, то $v'(t) = t$;
3) если $t = f(t1, \dots, t_n)$ для некоторой n-арной операции f и термов $t_1, \dots, t_n \in T(X, \Omega)$,
   то $v'(t) = f(v'(t_1), \dots, v'(t_n))$.
Терм $v'(t)$ называется результатом применения подстановки v к терму t.

Пусть заданы два терма s и t. Задача определения подстановки,
делающей эти термы равными называется **задачей унификации термов**.

Подстановка v называется унификатором термов s и t, если $v'(s) = v'(t)$.
Унификатор v называется **наибольшим общим унификатором** термов s и t и обозначается
НОУ.(s, t) = v, если для любого другого унификатора w термов s и t
существует такая подстановка *a*, что $a' \circ v' = w'$.
Если для термов s и t существует хотя бы один унификатор,
то среди унификаторов существует наибольший общий.

Символьные представления МО

Алгоритм унификации термов (с помощью стека)

Вход: термы s, t.

Выход: подстановка *h*, записанная как список пар $x_i = t_i$,
если t и s обладают наибольшим общим унификатором.
Процедура возвращает отказ, если унификаторов нет.

Алгоритм:
h = ( ); /* ( ) – это обозначение пустого списка */
Запомнить пару (s = t) в стек;
Пока стек не пуст, выполнять следующий цикл :

Извлечь из стека пару термов (s = t) и произвести одно из следующих действий,
в зависимости от выполнения одного из условий :

1. Если s – переменная, t – терм, не содержащий вхождений s ,
   то все вхождения переменной s в стеке заменяются на t и все вхождения s в h заменяются на t,
   затем подстановка s = t добавляется к списку подстановок в h;
2. Если t – переменная, а s – терм, то произвести действия, как в п.1. , поменяв ролями s и t
   (к h добавляется пара t = s);
3. Если s и t – составные термы, $s = f(s_1, s_2, ..., s_n)$ и $t = f(t_1, t_2, ..., t_n)$,
   то все пары $s_i = t_i$, $1 < i < n$, запоминаются в стек;
4. Если s и t – одинаковые символы констант или переменных, то ничего не делать;
5. Во всех остальных случаях производится выход из цикла и возвращается отказ.

Если выход из цикла произошёл не после выполнения условия 5,
то *h* содержит элементы $x_i = t_i$ искомой подстановки.

Символьные представления МО

Группа подстановок

Множество S (U) всех биекций вида $s : U \to U$
с бинарной операцией произведения (композиции) отображений
$g \circ f$ для $f, g \in S(U)$,
обладающее следующими свойствами (для всех $f, g, h \in S(U)$):
1) Операция произведения отображений ассоциативна : $h \circ (g \circ f) = (h \circ g) \circ f$
2) Операция произведения отображений имеет нейтральный элемент
   (тождественное отображение) 1_U : $1_U \circ f = f = f \circ 1_U$
3) Для всякой биекции $f : U \to U$ существует обратный (симметричный) элемент – биекция $g = f^{-1}$: $g \circ f = 1_U = f \circ g$

является алгебраической группой
относительно операции произведения отображений
и называется **группой подстановок**.
Замечание. В конечных группах, определённых на множестве из n элементов
$N = \{ 1, 2, \dots, n \}$ подстановки называются (симметрическими) перестановками
и обозначаются S_n.
Теорема Артура Кэли. Любая конечная группа $(G, \circ)$ изоморфна некоторой подгруппе группы перестановок множества элементов этой группы.

Теорема Кэли (доказательство)

Пусть * — бинарная операция в группе G.
Рассмотрим некоторый элемент $g \in G$ и функцию $f_g : G \to G$, $f_g(x) = g * x$. f_g — перестановка, т.к.:
1. Для любых x, y таких, что $x \neq y$ верно, что $g * x \neq g * y$. Следовательно f_g — инъекция.
2. Мощность G — конечна, следовательно f_g — биективно и является перестановкой.

Пусть $\circ$ — композиция двух перестановок.
Если f_g — перестановка, то $f_{g^{-1}}$ — обратная перестановка, где g^{-1} — обратный элемент g,
так как $(f_{g^{-1}} \circ f_g)(x) = f_{g^{-1}}(f_g(x)) = g^{-1} * g * x = x$.

Если e — нейтральный элемент в группе, то f_e — тождественная перестановка.
Таким образом множество всех функций $K = \{ f_g \mid g \in G \}$ — подгруппа симметрической группы,
так как композиция двух функций из K не выводит из K,
потому что $(f_a \circ f_b)(x) = f_a(f_b)(x) = a * b * x = f_{a*b}(x) = f_c(x)$, где $c = a * b$, значит $f_a \circ f_b \in K$

Рассмотрим множество K. По доказанному выше, оно является подгруппой симметрической группы.
Осталось доказать, что G и K изоморфны. Для этого рассмотрим функцию $T : G \to K$, $T(x) = f_x$.
Заметим, что для всех $x \in G$ $(f_g \circ f_h)(x) = f_{g*h}(x)$, то есть $T(g) \circ T(h) = T(g * h)$.
Значит T — гомоморфизм.
1. T — инъекция, потому что $f_g(x) = f_{g'}(x)$. Следовательно, $g = f_g(x) * x^{-1} = f_{g'}(x) * x^{-1} = g'$.
2. Сюрьективность T очевидна из определения K.
То есть T — гомоморфизм и биекция, а значит изоморфизм G и K установлен.

Символьные представления МО

Примеры применения теоремы Кэли - 1

Пример 1.

Пусть $\mathbf{Z}_4$ – группа вычетов по модулю 4 с операцией сложения.

Найдём подгруппу симметрической группы $\mathbf{S}_4$, изоморфную $\mathbf{Z}_4$

Определим отображение $\alpha : \mathbf{Z}_4 \to \mathbf{S}_4$ следующим образом:

$$\alpha(0) = \begin{vmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \end{vmatrix}$$

$$\alpha(1) = \begin{vmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \end{vmatrix}$$

$$\alpha(2) = \begin{vmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{vmatrix}$$

$$\alpha(3) = \begin{vmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \end{vmatrix}$$

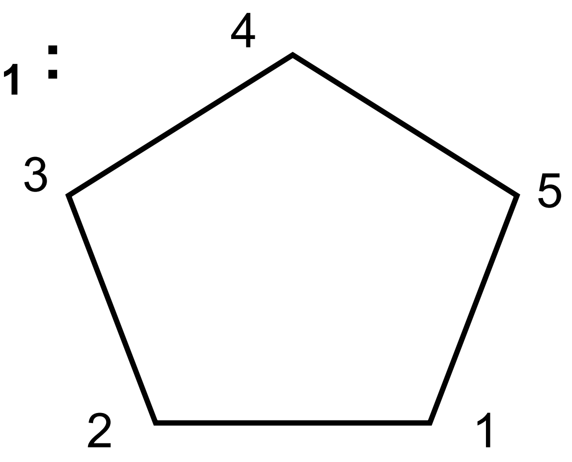
где перестановка $\alpha(0)$ задаёт тождественное отображение или «таблицу сложения» с числом 0. Аналогично, перестановки $\alpha(1)$, $\alpha(2)$, $\alpha(3)$ задают «таблицы сложения» с числами 1, 2 и 3 соответственно.

Символьные представления МО

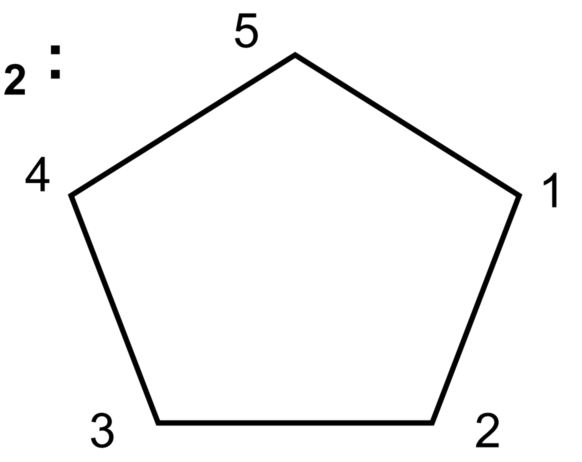
Примеры применения теоремы Кэли - 2

Пример 2.
Пусть H – группа перестановок вершин правильного пятиугольника при его вращениях в плоскости, переводящих самого в себя.
Если вращение производится против часовой стрелки, то имеем перестановки :
h_0 : (1) (2) (3) (4) (5) – поворот на угол 0,
h_1 : (2 3 4 5 1) – поворот на угол (π / 5),
h_2 : (3 4 5 1 2) – поворот на угол (2π / 5) и т.д.
H = ({ h_0 , …, h_4 }, $\circ$) является подгруппой симметрической группы перестановок.

h_1 :



h_2 :



Символьные представления МО

Алгебра списковых структур

Пусть F (X) – полугруппа (с бинарной операцией конкатенации - conc) с единицей (в виде нульарной операции – пустого слова – e) над некоторым конечным алфавитом $X = \{ x_1, x_2, \dots , x_n, \dots \}$.
Произвольное слово $p = y_1 y_2 \dots y_m$ из F (X) будем называть **списком** элементов $y_1, y_2, \dots , y_m$, а сами элементы $y_i \in X$, $i = 1, \dots , m$ – составляющими этого списка.

Теорема. Все функции и операции над списками представимы в виде термов с помощью следующих операций: e, conc, head, tail, где
$head (p) = y_1$ ($head : F (x) \to F (x)$) – первый символ слова p.
$tail (p) = y_2 \dots y_m$ ($tail : F (x) \to F (x)$) – слово без первого символа.

Определение. Универсальная алгебра G = (F (X) , W = {e, conc, head, tail}) называется **алгеброй списковых структур (АСС)**.

Два списка p и q равны, если равны их длины (т.е. число составляющих списка: $l (p) = l (q)$), а также равны символы ($p_i = q_i$), имеющие одинаковые номера позиций в списках.
Расширив АСС предикатом равенства списков, получим **алгебраическую систему списковых структур (АССС)**.

Теорема. АССС является алгоритмически полной системой, иными словами, в ней можно вычислить произвольную частично рекурсивную функцию.

План лекции: тема подраздела

- Свойства представлений математических объектов (МО)
- Символьные представления МО
- **Характеристика задач построения эквивалентных представлений**
- Представление базовых объектов компьютерной алгебры
- Представление алгебраических функций
- Представление трансцендентных функций
- Представление матриц

Синтез эквивалентных представлений

Постановка задач упрощения выражений

Пусть T – это класс (лингвистических) объектов (выражений).
Пусть ~ обозначает некоторое отношение эквивалентности на классе T.

Тогда постановка задачи
построения эквивалентного представления
для данного математического объекта имеет две формы:

(1) Построение эквивалентного данному более простого объекта.
(2) Построение единственного представления
для эквивалентных объектов.

Обе вышеуказанные задачи
являются в компьютерной алгебре **задачами упрощения выражений**.

Замечание. Результат упрощения – это эквивалент или аппроксимация.

Синтез эквивалентных представлений

Типы эквивалентности выражений

(1) Лингвистическая эквивалентность

Тождество символьных строк.

(2) Эквивалентность предметной интерпретации

Арифметические выражения $(x+2)^5$ и $(x^5 + 10x^4 + 40x^3 + 80x^2 + 80x + 32)$ лингвистически не эквивалентны, но представляют один полином в кольце R [x].

(3) Функциональная эквивалентность

Выражения $(x^6 – 1) = (x – 1)(x + 1)(x^2 – x + 1)(x^2 + x + 1)$ и $(x – 1)$ представляют различные полиномы и в кольце R [x], и в кольце GF(2) [x], но вместе с тем представляют одну функцию в поле GF(2) [x].

(4) Эквивалентность мероморфных функций

Рациональные выражения $(x^6 – 1) / ((x – 3) (x^2 – 1))$ и $(x^4 + x^2 + 1) / (x – 3)$ функционально не эквивалентны в поле Q [x] (достаточно сравнить их значения в точках $x = \pm 1$), но определяют в этом поле один элемент как мероморфные функции (обе имеют особую точку (полюс функции) при $x = 3$).

Синтез эквивалентных представлений

Отношение конгруэнтности

Замечание.
В дополнение к вышерассмотренным типам эквивалентности
следует указать отношение,
обеспечивающее алгебраическую эквивалентность выражений.

Пусть $A = (X, \Omega)$ является некоторой алгеброй
и ~ является отношением эквивалентности в A.

Тогда отношение ~ называется **отношением конгруэнтности** (**конгруэнцией**)
относительно операции $\omega \in \Omega$, если для любых $a_1, b_1, \dots, a_n, b_n \in X$
верно утверждение:

$$a_1 \sim b_1, \dots, a_n \sim b_n \Rightarrow \omega(a_1, \dots, a_n) \sim \omega(b_1, \dots, b_n)$$

Если отношение конгруэнтности определено для всех операций $\omega \in \Omega$ в алгебре A ,
то оно называется отношением конгруэнции в A (или Ω - конгруэнцией).

Синтез эквивалентных представлений

Построение более простого объекта

Задача построения эквивалентного более простого объекта состоит в нахождении эффективной процедуры $S : T \to T$,
такой, что для всякого объекта $t \in T$
выполнены следующие условия:

(SE) $\quad S(t) \sim t$

(SS) $\quad S(t) \leq t$

Здесь $\leq$ обозначает некоторое рассматриваемое **отношение упрощения**.

Примеры отношений упрощения :

1) « $s \leq t$ » означает « s короче t »
2) структура s более понятна, чем структура t

Конечно, для большинства t требуется, чтобы $S(t) < t$

Синтез эквивалентных представлений

Построение единственного представления

Задача построения единственного представления
для эквивалентных объектов (**задача канонического упрощения**)
состоит в нахождении эффективной процедуры $S : T \to T$
для отношения ~ на T, такой,
что для любых объектов s, t $\in$ T справедливы следующие условия:

(SE) $\quad S(t) \sim t$

(SC) $\quad s \sim t \Rightarrow S(s) = S(t)$

Иными словами, S указывает единственного представителя
в каждом классе эквивалентности.
При этом S (t) называется **каноническим видом** объекта t.

Пример канонизации :
преобразование элементарных арифметических выражений
к полиномиальному виду:

$(x^2 - 1)$ является полиномиальным видом выражения $(1/2)(2x + 2)(x-1)$

Синтез эквивалентных представлений

Замечания к задачам упрощения

Замечание 1. Оба вышеуказанных типа задач не являются полностью независимыми.
Случай 1. Взаимная сводимость задач (упрощение равнозначно канонизации).
Последовательное итеративное уменьшение размера выражений относительно некоторой меры «простоты» может иногда привести к канонизации или, по крайней мере, дать идею конструкции канонизации.
Наоборот, канонизация определяет соответствующее понятие упрощения – канонический вид объекта «проще», чем сам объект.
Случай 2. Взаимная противоречивость задач
(упрощение не означает канонизацию, канонизация не означает упрощение).
Практические процедуры, которые в интуитивном смысле «упрощают» выражения, могут приводить к различным (а не к одному, как требуется при канонизации) упрощённым видам для двух эквивалентных выражений.
Наоборот, канонические виды простых выражений могут быть достаточно «сложными»
(в частности, каноническим видом полинома $(x+2)^5$
является полином $x^5 + 10x^4 + 40x^3 + 80x^2 + 80x + 32$)

Замечание 2. Каноническое упрощение термов в языке первого порядка (т.е. алгебраических выражений) имеет фундаментальную роль в компьютерной алгебре.

Замечание 3. Как постановка, так и методы решения задачи канонического упрощения в значительной степени зависят от используемого понятия эквивалентности.

Синтез эквивалентных представлений

Вычислимость и разрешимость

Напомним, что функция называется **вычислимой**, если она частично-рекурсивна (т.е. реализуется машиной Тьюринга, машиной Поста или нормальным алгорифмом Маркова).

Множество называется **перечислимым** (эффективно перечислимым, рекурсивно-перечислимым, частично разрешимым), если все его элементы могут быть получены с помощью некоторого алгоритма.

Математический объект называется **разрешимым**, если существует алгоритм, который определяет принадлежность объекта заданному множеству.
Множество является разрешимым, если его характеристическая функция вычислима.
Замечание 1. Любое разрешимое множество является перечислимым и арифметическим.
Замечание 2. Существуют перечислимы множества, не являющиеся разрешимыми.
Перечислимое множество является разрешимым тогда и только тогда, когда его дополнение также перечислимо.

Синтез эквивалентных представлений

Каноническое упрощение и распознавание эквивалентности - 1

Теорема. Пусть T – разрешимое множество объектов
и ~ обозначает отношение эквивалентности на T.
Отношение ~ разрешимо тогда и только тогда,
когда существует канонизация S для ~.

Доказательство:
Достаточность. В силу свойств (SE) и (SC)
выполнено $s \sim t \Leftrightarrow S(s) = S(t)$
Необходимость. Пусть g – вычислимая функция,
отображающее множество натуральных чисел N на T.
Положим $S(s) = g(n)$, где n – это наименьшее натуральное число,
для которого $g(n) \sim s$.
Функция S вычислима, т.к. функция g вычислима.
Таким образом, справедливость свойств (SE) и (SC) очевидна.

Синтез эквивалентных представлений

Каноническое упрощение и распознавание эквивалентности - 2

Пример.

В коммутативной полугруппе, определённой образующими: a, b, c, f, s
и определяющими соотношениями: $as = c^2s$, $bs = cs$, $s = f$,
множество правил преобразований: $s \to f$, $cf \to bf$, $b^2f \to af$
составляет канонизацию.

Выражения $a^5bc^3f^2s^3$ и $a^5b^2c^2s^5$
представляют один и тот же элемент полугруппы,
т.к. их канонические виды совпадают и равны a^7f^5.

Выражения cs^2 и c^2s
представляют разные элементы,
принимая во внимание, что их канонические виды
соответственно bf^2 и af различны.

Синтез эквивалентных представлений

Каноническое упрощение и вычислимость - 1

Теорема. Пусть T – разрешимое множество объектов,
R – вычислимая бинарная операция на T
и ~ обозначает некоторое отношение эквивалентности,
являющееся отношением конгруэнтности относительно R на T.
Допустим, что задана канонизация S для отношения ~.
Введём множество «канонических представителей» (достаточное множество)
$Rep(T) = \{ t \in T \mid S(t) = t \}$
и определим $R'(s, t) = S(R(s, t))$ для всех $s, t \in Rep(T)$.
Тогда алгебраическая система $(Rep(T), R')$
изоморфна фактор-системе $(T/\sim, R/\sim)$,
кроме того, множество Rep (T) разрешимо и R’ вычислима
(здесь операция $R/\sim(C_s, C_t) = C_{R(s,t)}$,
где C_t обозначает класс эквивалентности, содержащий t, относительно ~)
Доказательство:
При доказательстве используется то обстоятельство, что равенство
$i(t) = C_t$ (т.е. $t \in Rep(T)$) определяет изоморфизм двух алгебраических систем.

Синтез эквивалентных представлений

Каноническое упрощение и вычислимость - 2

Пример.
Правила преобразований: $x^3 \to x^2$, и $x^2y \to x^2$
составляют канонизацию S на множестве T = Q [x, y]
для отношения конгруэнтности по модулю идеала I,
порождённого полиномами $x^3y - x^3$ и $x^3y - x^2$.

Множество Rep (T) совпадает
с семейством тех полиномов f из Q [x, y],
которые не содержат ни одного монома,
делящегося на x^3 или x^2y.
Умножение классов вычетов по модулю I
можно изоморфно представить в множестве Rep (T)
с помощью равенства R' (s, t) = S (st).
Итак, имеем :
$R'(xy + 1, xy - 1) = S((xy + 1)(xy - 1)) = S(x^2y^2 - 1) = x^2 - 1$

Синтез эквивалентных представлений

Неканонические упрощения

Канонизация для отношения эквивалентности на заданном множестве выражений не всегда возможна.

В частности, было доказано (Даниэль Ричардсон, 1968), что для класса выражений, порождённых с помощью следующих элементов:

- переменная x;
- константы: рациональные числа и два трансцендентных числа – π и ln(2);
- операции сложения, умножения и композиции функций;
- функции sin (x), exp (x), abs (x)

задача функциональной эквивалентности алгоритмически неразрешима.

Поэтому требуется иметь более слабые, чем каноническое, но в какой-то мере аппроксимирующие его, типы упрощений.

Наиболее распространены два типа подобных упрощений:

(1) нормальное или 0-эквивалентность (цель: канонизация при сводимости к нулю);
(2) регулярное (цель: алгебраическая независимость нерациональных термов).

Выводы :

Проблема выбора представления математического объекта в компьютерной алгебре объединяет два подхода:
(1) абстрактно-алгебраический и (2) программно-технический.

Абстрактно-алгебраический подход
основан на использовании отношений эквивалентности алгебраических структур.
Программно-технический подход ставит два вопроса:
(1) моделирование объектов компьютерной алгебры
посредством совокупности структур хранения данных,
(2) разработка представлений и преобразований информации
из исходной формы представления во внутреннюю форму и наоборот.

Исходные объекты имеют определенную алгебраическую природу
и при преобразовании их во внутреннюю форму представления
необходимо сохранить их алгебраические свойства
и предусмотреть эффективные способы их преобразований с учетом этих свойств.

Как правило, выбранная форма представления определяет
и способ обработки этой информации,
и набор алгоритмов, используемых в процессе преобразований.

План лекции: тема подраздела

- Свойства представлений математических объектов (МО)
- Символьные представления МО
- Характеристика задач построения эквивалентных представлений
- **Представление базовых объектов компьютерной алгебры**
- Представление алгебраических функций
- Представление трансцендентных функций
- Представление матриц

Представление базовых объектов

Базовые объекты компьютерной алгебры

- Целые числа
- Рациональные числа
- Полиномы от одной переменной
- Полиномы от нескольких переменных
- Рациональные функции

Представление базовых объектов

Представление целых чисел

Возможны различные способы представлений целых чисел:

(1) **ограниченной точности**,

когда количество цифр в целом числе задано.

К таковым относятся все стандартные арифметики

в языках программирования.

(2) **произвольно заданной точности**,

когда количество цифр в заданном числе можно менять,

но только один раз – задавать перед вычислениями.

(3) **неограниченной точности**,

когда количество цифр в числе

не ограничивается никаким наперёд заданным числом,

кроме ограничений, связанных с размером памяти машины.

В системах компьютерной алгебры целые числа неограниченной точности, реализуются программным путем, (этот тип данных считается базовым).

Представление базовых объектов

Представление рациональных чисел

Возможны различные способы представлений рациональных чисел произвольной точности :

(1) отношение числителя и знаменателя (оба - числа произвольной точности)
(более точно, в виде записи, хранящей ссылку на список – числитель
и ссылку на список – знаменатель).
Такое представление является нормальным.
Проблема - для нормального представления необходимо распознавание идентичных чисел.
Пример. Записи вида –2 / 3, 2 / -3, 4 / -6, -10 / 15 и т.п. представляют одно и то же число.

(2) Так же, как в (1), но выполнив дополнительные условия :
(а) числитель и знаменатель числа должны быть сокращены
на наибольший общий делитель (НОД);
(б) знаменатель должен быть положительным числом.
Такое представление является каноническим.
Проблема - требуется вычисление НОД двух целых чисел произвольной точности.
При большом количестве цифр в числах эта процедура является алгоритмически сложной.
Тем более, её надо производить на одном из самых низких уровнях вычислений –
при каждом вычислении чисел.

Замечание. В системах компьютерной алгебры обычно используется
каноническое представление рациональных чисел произвольной точности.

Представление базовых объектов

Представление полиномов от одной переменной

Полином от одной переменной представляет собой сумму мономов,
иными словами – последовательность (или список).
Коэффициенты мономов могут быть числами разных типов,
в том числе целыми числами произвольной точности.
(Степени переменных – короткие целые числа).

Представление полинома является каноническим,
если последовательность мономов упорядочена по возрастанию (или по убыванию)
степени мономов.

Полином можно хранить как в плотном, так и в разреженном представлении.
В плотном представлении хранится: число мономов (определяемое как максимальная
степень старшего монома плюс единица), и все, в том числе, нулевые коэффициенты мономов.
Такое представление эффективно для алгоритмов преобразования полиномов,
в которых (1) число членов рядов для вычислений с повышением точности вычислений растет быстро
и (2) мало число нулевых членов.
В разреженном представлении хранится последовательность (список),
в каждом блоке которой хранится запись об одном ненулевом мономе,
содержащая коэффициент монома и его степень.

Пример. Полином A (x) = x^{1000} - 1 требует существенно различные ресурсы
при хранении в плотном и в разреженном представлениях.

Представление базовых объектов

Представление полиномов от нескольких переменных - 1

Полином от нескольких переменных представляет собой сумму мономов, иными словами – последовательность (или список), а моном – произведение термов (тоже последовательность).

Различают две формы канонического представления полинома от нескольких переменных:

(1) форма с упорядочением последовательности мономов;
(2) рекурсивная форма.

Рекурсивная форма получается с помощью представления полинома от нескольких (N) переменных в виде полинома от одной переменной с коэффициентами – полиномами от других (N-1) переменных.
При таком представлении на заданном порядке переменных полином представляется в виде иерархического списка, где в качестве коэффициентов хранятся ссылки на списки – полиномы меньших степеней.

Представление базовых объектов

Представление полиномов от нескольких переменных - 2

Упорядочение последовательности мономов производится на основе введения некоторого отношения порядка на имена переменных : $x_1 > x_2 > \ldots > x_k$ ($x_r > x_s$ обозначает, что переменная x_r старше переменной x_s)

В результате можно получить следующие канонические представления :
(1) Лексикографическое упорядочение по степени каждой переменной;
(2) Упорядочение по общей степени с прямым (с обратным) лексикографическим порядком на степень каждой переменной.

Замечание 1. Все канонические представления равноправны, но конкретна форма представления влияет на результат алгебраических преобразований.

Пример. Пусть необходимо разделить полином A на полином B :
$A(x, y) = x + 2 * y$ $\quad$ $B(x, y) = x – y$
Если x старше y, то частное = 1, остаток = $3 * y$
Если y старше x, то частное = - 2, остаток = $3 * x$

Замечание 2. Обычно, тип отношения порядка на имена переменных, реализованный в системах компьютерной алгебры, не известен пользователю.

Представление базовых объектов

Представление рациональных функций

Дробно-рациональные функции, представляющие отношение полиномов,
эффективно хранить в виде записи,
содержащей ссылку на полином - числитель и ссылку на полином – знаменатель.
При этом полиномы должны находиться в одной канонической форме.

Представление рациональной функции будет каноническим,
если дополнительно ввести следующие условия :
(1) числитель и знаменатель должны быть сокращены на полином –
наибольший общий делитель (НОД) этих двух полиномов;
(2) числовые коэффициенты числителя и знаменателя должны быть сокращены на общий множитель;
(3) старший коэффициент знаменателя должен быть положительным.

Поиск НОД для двух полиномов от нескольких переменных
является вычислительно трудоемкой операцией.
Кроме того, она должна выполняться на низком уровне вычислений (т.е. очень часто).
Поэтому необходимо предусмотреть две формы представления дробно-рациональных функций:
(1) каноническую и (2) нормальную (без сокращения на НОД).

Замечание. Как правило, в системах компьютерной алгебры
реализуется несколько и канонических, и нормальных форм
представления полиномов от нескольких переменных.

План лекции: тема подраздела

- Свойства представлений математических объектов (МО)
- Символьные представления МО
- Характеристика задач построения эквивалентных представлений
- Представление базовых объектов компьютерной алгебры
- **Представление алгебраических функций**
- Представление трансцендентных функций
- Представление матриц

Представление алгебраических функций

Алгебраические числа
и алгебраические функции

Алгебраическим называется **число**, являющееся решением уравнения:
$P (x) = 0$
где $P (x)$ – полином от одной переменной с целыми коэффициентами.

Пример. Полином $P (x) = x^2 – 2$ порождает алгебраическое число $\sqrt{2}$.

Алгебраической называется **функция**, являющаяся решением уравнения:
$G (x) = 0$
где $G (x)$ – порождающий полином от одной переменной с коэффициентами – полиномами от нескольких переменных с целыми коэффициентами.

Пример. Полином $G (x) = x^2 – 2 + y$ порождает алгебраическую функцию $\sqrt{(2 – y)}$.

Простым радикалом называется положительная дробная степень от полинома с целыми коэффициентами.

Вложенным радикалом называется положительная дробная степень от выражения, содержащего радикалы.

Представление алгебраических функций

Представление простых радикалов - 1

Для представления простых радикалов
необходимо ввести новую квазипеременную – r_1,
обозначающую этот радикал.

С помощью квазипеременной
описывается вхождение степеней простого радикала в другие выражения.

При этом необходимо учитывать,
что порождающий полином удовлетворяет условию: $G(r_1) = 0$.

Для простых радикалов можно построить канонические представления,
однако их редко применяют в системах компьютерной алгебры
по следующим причинам:
(1) алгоритмы получения таких представлений, как правило,
неэффективны и нерациональны;
(2) сами канонические представления не упрощают,
а усложняют вид выражений с радикалами, предъявляемый пользователю.

Представление алгебраических функций

Представление простых радикалов - 2

Для получения канонического представления простого радикала следует (после введения квазипеременной) разрешить следующие проблемы:

(1) Проблема неоднозначности дробно-рациональных отношений радикалов.

Пример. Функции – радикалы (1-y) / (√ (2 - y) - 1) и (√ (2 - y) + 1) – это два представления одного радикала. Их разность равна нулю.

(2) Проблема независимости радикалов друг от друга (в случае работы с несколькими радикалами).

Пример. Радикалы $\alpha = \sqrt{(x+1)}$, $\beta = \sqrt{(x+2)}$ и радикал $\chi = \sqrt{(x^2 + 3*x + 2)}$ взаимозависимы, т.к. разность $(\alpha * \beta - \chi)$ равна нулю.

(3) Проблема приведения дробно-рациональных функций к виду со знаменателями, свободными от радикалов.

Пример. Число – радикал следующего вида: $1 / (\sqrt{2} + \sqrt{3} + \sqrt{5} + \sqrt{7})$ предпочтительнее для пользователя, чем его каноническое представление:

$(22 \sqrt{3} \sqrt{5} \sqrt{7} - 34 \sqrt{2} \sqrt{5} \sqrt{7} - 50 \sqrt{2} \sqrt{3} \sqrt{7} + 135 \sqrt{7} + 62 \sqrt{2} \sqrt{3} \sqrt{5} - 133 \sqrt{5} - 145 \sqrt{3} + 185 \sqrt{2}) / 215$

Представление алгебраических функций

Представление вложенных радикалов

Для вложенных радикалов
выбор канонического представления является еще более сложным,
чем для простых радикалов.

Однако характер возникающих при этом задач сохраняется.

Во-первых, необходимо ввести новые квазипеременные.

Во-вторых, необходимо решить те же проблемы (1) (2) (3),
которые относятся к простым радикалам – см. предыдущий слайд.

Приведем примеры, которые иллюстрируют проблему (2) –
проблему взаимной независимости вложенных радикалов.

Пример 1. Числа – вложенные радикалы. Имеем взаимозависимость:

$$\sqrt{5 + 2\sqrt{6}} + \sqrt{5 - 2\sqrt{6}} = 2\sqrt{3}$$

Пример 2. Функции – вложенные радикалы. Имеем взаимозависимость:

$$\sqrt{x + \sqrt{x^2 - 1}} = \sqrt{(x + 1) / 2} + \sqrt{(x - 1) / 2}$$

Представление алгебраических функций общего вида - 1

Ключевая проблема построения канонического представления для алгебраических функций общего вида – это проблема определения их взаимозависимости.

Существует два способа решения указанной проблемы:
(1) Факторизация порождающего полинома алгебраической функции и анализ её результатов
(2) Построение примитивных элементов поля алгебраических функций.

Оба способа разрешения взаимозависимости рациональных функций вычислительно трудоёмки, поэтому в системах компьютерной алгебры канонические представления для алгебраических функций не применяются.

Замечание - Вывод. Существование теоретических алгоритмов разрешения проблем представления алгебраических функций не означает их практическую реализацию.

Представление алгебраических функций

Представление алгебраических функций общего вида - 2

1-й способ решения проблемы взаимозависимости

Если порождающий алгебраическую функцию полином неприводим,
т.е. не разложим на множители (полиномы с целыми коэффициентами),
то корни уравнения P (x) = 0 (алгебраические функции) независимы.
Таким образом, для поиска независимых алгебраических функций
необходимо решить задачу факторизации полинома от нескольких переменных.
Более того, если у нас есть несколько порождающих полиномов,
возникает задача разложения полиномов на множители
над алгебраическими полями, что довольно сложно.
Т.е., если есть два неприводимых полинома P_1 и P_2, это еще не значит,
что корни второго полинома не являются независимыми
в терминах корней первого полинома.

Пример. Пусть заданы два порождающих уравнения,
неприводимых над полиномами с целыми коэффициентами: $P_1(\alpha) = 0$ и $P_2(\beta) = 0$.
Если $P_2(\beta) = (\beta + \alpha - 1) * h(\beta, \alpha)$, где h – полином,
то алгебраические функции линейно зависимы.

Представление алгебраических функций общего вида - 3

2-й способ решения проблемы взаимозависимости

Примитивным элементом поля алгебраических функций (алгебраических чисел) называется алгебраическая функция (алгебраическое число), с помощью которой можно выразить все остальные элементы такого поля.

Пример. Пусть число α – это корень полинома ($\alpha^4 - 10 * \alpha^2 + 1$), который равен ($\sqrt{2} + \sqrt{3}$).

Тогда следующие числа:

$\sqrt{2} = (\alpha^3 - 9 * \alpha) / 2$

$\sqrt{3} = (11 * \alpha - \alpha^3) / 2$

можно выразить через него.

План лекции: тема подраздела

- Свойства представлений математических объектов (МО)
- Символьные представления МО
- Характеристика задач построения эквивалентных представлений
- Представление базовых объектов компьютерной алгебры
- Представление алгебраических функций
- **Представление трансцендентных функций**
- Представление матриц

Представление трансцендентных функций

Канонические и нормальные представления

Для трансцендентных функций не существует
ни канонического, ни нормального представлений.

Это обусловлено одной основной причиной:

для произвольной трансцендентной функции,
содержащей хотя бы одну буквенную переменную,
алгебраические операции, круглые скобки,
логарифмическую и экспоненциальную функции
(ln, exp, либо тригонометрические функции),
константы **e, i,** π и вещественные числа,
теоретически не существует приемлемого алгоритма
распознавания идентичности функции и нуля.

Представление трансцендентных функций

Иерархические представления

Представления трансцендентных функций имеют иерархическую структуру.

На каждом уровне иерархии используется развитая система переобозначений промежуточных представлений – выражений различных типов:

(1) Каждое алгебраическое выражение представляется в виде полинома или дробно-рациональной функции от буквенных переменных или вновь введённых квазипеременных;

(2) Новой квазипеременной может быть известная функция от базового (на текущем уровне иерархии) выражения, степень известной функции, степень полинома и т.п.

Замечание. Отсутствие для трансцендентных функций канонических (или нормальных) представлений не позволяет полностью автоматизировать (в среде систем компьютерной алгебры) процесс получения результатов преобразований таких функций.
Поэтому необходимы средства организации диалогов с (квалифицированным) пользователем, интерактивно определяющим следующие аспекты вычислений:
(1) правила преобразований,
(2) свойства функций,
(3) правила применения тождеств,
(4) желаемый вид результата.

План лекции: тема подраздела

- Свойства представлений математических объектов (МО)
- Символьные представления МО
- Характеристика задач построения эквивалентных представлений
- Представление базовых объектов компьютерной алгебры
- Представление алгебраических функций
- Представление трансцендентных функций
- **Представление матриц**

Представление матриц

Формы представления матриц

Различают две формы представления матриц :

Двумерный массив :

$$\begin{pmatrix} a_{11}, a_{12}, \dots, a_{1n} \\ a_{21}, a_{22}, \dots, a_{2n} \\ \dots \quad \dots \quad \dots \\ a_{m1}, a_{m2}, \dots, a_{mn} \end{pmatrix}$$

a_{ij} – это ссылки на представление элементов матриц (формул)

Список списков :

$$((a_{11}, a_{12}, \dots, a_{1n}), (a_{21}, a_{22}, \dots, a_{2n}), \dots, (a_{m1}, a_{m2}, \dots, a_{mn}))$$

Представление матриц

Плотные и разреженные представления

Для представления матриц
обычно используется плотное представление
(т.е. хранятся все элементы матриц, включая нулевые).

В некоторых особых случаях для матриц специального вида
(диагональных, ленточных и т.п.)
применяется разреженное представление.

Замечание. В случае использования разреженного представления
требуются специальные алгоритмы преобразований матриц.

Выводы :

1. При работе с любым видом информации необходимо выбрать её представление.
2. Проблема представления математического объекта имеет два аспекта решения: абстрактный и физический (технический).
3. Выбранная форма представления, как правило, определяет способ обработки и набор алгоритмов, используемый в процессе преобразований.
4. Вид и достоверность результатов преобразований математических объектов в одинаковой степени зависят от используемых представлений и порядка применения преобразований.

Спасибо за внимание !

Вопросы ?