**Лекция 9**

**Каноническое упрощение
алгебраических выражений**

**Содержание лекции**

* Редукция алгебраических выражений
* Метод локализации
* Метод критических пар
* Метод пополнения

**План лекции: тема подраздела**

* **Редукция алгебраических выражений**
* Метод локализации
* Метод критических пар
* Метод пополнения

**Редукция алгебраических выражений**

**Методы неканонических упрощений**

Разнообразие алгоритмов упрощения алгебраических выражений, реализованных в системах компьютерной алгебры (СКА), обеспечивается существованием и постоянным расширением методов неканонических упрощений.

Неканонические упрощения предназначены для фактического «упрощения» выражений относительно различных интуитивных критериев простоты.

Т.к. интуитивные критерии простоты формируются пользователями СКА, методы неканонических упрощений часто имеют вид набора технических приёмов.

Некоторые специализированные методы неканонических упрощений:

* Подстановка

(подстановка выражения вместо переменной в другое выражение)

* Синтаксическое вхождение

(распознавание равных подвыражений в сложном выражении посредством поиска вхождений)

* Выделение из выражений интересующей информации

(информация об ограниченности, непрерывности, монотонности, выпуклости и т.п.)

**Редукция алгебраических выражений**

**Система переписывания термов**

Основная парадигма вычислений с равенствами - использование их как правил переписывания (подстановки) термов.

Эта парадигма лежит в основе:

* разрешающих процедур, использующих канонические формы;
* построения абстрактных интерпретаторов ориентированных равенств, рассматриваемых как язык программирования.

Системой переписывания термов (над сигнатурой Q) называется такое множество ориентированных равенств:

^ = { X j ^ р j| і є I }

что для любого ориентированного равенства X ^ р из ^ справедливо:

Т(р) с T(X)

**Редукция алгебраических выражений**

**Определение отношения редукции**

Отношением редукции ^ эт, соответствующим

называется наименьшее бинарное отношение над T,

содержащее ^ и замкнутое относительно подстановки (а) и замены (P):

1. M ^я N ^а ( M ) ^яа ( N )
2. M ^ P [ u ^ M ] ^ P [ u ^ N ]

Это равносильно тому, что ^ - это наименьшее отношение,

содержащее все такие пары ( а ( X) , а ( р ) ), что ( X ^ р ) є ^, и замкнутое относительно замены (2).

Пример. Если ^ = { A ^ B , F ( B , x ) ^ G ( x , x ) } , то F ( A , A ) ^ F ( B , A ) ^ G ( A , A )

Замечание. Далее вместо ^ мы будем использовать обозначение ^ .

**Редукция алгебраических выражений**

**Свойства отношения редукции**

Замечание. В классах T алгебраических объектов с отношением эквивалентности ~ отношение редукции

концептуально определяется как «правило перехода за один шаг от объекта s к более простому эквивалентному объекту t».

Итерация отношения редукции представляет собой канонизацию для отношения ~, если выполнены следующие условия:

1. отношение ^ может быть реализовано алгоритмически и рефлексивное, симметричное, транзитивное замыкание отношения редукции совпадает с отношением эквивалентности;
2. отношение ^ является полным, т.е. обладает следующими свойствами: Единственность.

Итерация процесса редукции, которая начинается с одного и того же объекта, всегда завершается получением одного и того же объекта, который далее не редуцируется.

Завершимость.

Итерация процесса редукции всегда завершается после конечного числа шагов объектом, который далее не редуцируется.

**Редукция алгебраических выражений**

**Разнообразие отношений редукции**

Замечание. В общем случае под отношением редукции может пониматься произвольное бинарное отношение следующего вида ^ с T x T

определённое на произвольном множестве алгебраических выражений T (T ф 0).

Далее используются следующие условные обозначения

для различных отношений, порождённых отношением редукции:

|  |  |
| --- | --- |
| ^ +^ \* о \*^0^ (n+1) = ^ . | обратное отношение; транзитивное замыкание; рефлексивно-транзитивное замыкание; рефлексивно-транзитивно-симметричное замыкание; отношение тождества;. ^ (n) |

**Редукция алгебраических выражений**

**Идеи методов построения канонизаций**

Замечание. Основой построения канонизаций для отношения ~ является алгоритмическая процедура проверки свойств полноты (т.е. единственности и завершимости) итерации редукций.

Проверка свойства завершимости для конкретного отношения редукции, как правило, требует специальной техники построения доказательства.

(Поэтому далее не рассматривается).

Проверка свойства единственности алгоритмизируется с помощью трёх методов:

1. Метод локализации (используется в общем случае);
2. Метод критических пар (используется для отношений редукции, которые порождаются конечным числом схем редукций);
3. Метод пополнения (если конечнопорождённые отношения редукции не являются полными, то они могут быть пополнены

путём добавления схем редукции, возникающих при анализе критических пар).

**План лекции: тема подраздела**

* Редукция алгебраических выражений
* **Метод локализации**
* Метод критических пар
* Метод пополнения

**Определения основных понятий**

Отношение ^ называется нётеровым

(названным в честь немецкого математика Амалии Эмми Нётер), если оно удовлетворяет свойству завершимости.

Если отношение ^ понятно из контекста, то через x (символ с нижним подчёркиванием) обозначается нормальная форма элемента x из T относительно ^ , т.е. не существует такого у є T , что x ^ у.

Элемент z є T называется общим потомком элементов x , у є T ,

если x ^ \* z \* ^ у (это обозначается x і у).

**Алгоритм нормальной формы**

Пусть символ ~ означает отношение эквивалентности на T, а символ ^ означает некоторую нётерову редукцию, такую, что о \* = ~ .

Допустим, что задана такая функция «выбора» Sel: T ^ T , что x ^ Sel ( x ) для произвольного x є T , который не находится в нормальной форме.

Рассмотрим вычислимую функцию S , определяемую рекурсивно:

S ( x ) = { x , если x в нормальной форме ;

S ( Sel ( x ) ) , в противном случае }

Назовём S такого типа алгоритмом нормальной формы

для редукции ^.

Ключевая идея метода локализации:

построить алгоритмический тест, проверяющий что S является канонизацией.

**Метод локализации**

**Общая схема построения теста для S**

Этап 1. Проверить, удовлетворяет ли функция (процедура) S

свойствам (аксиомам) канонического упрощения - (SE) и (SC).

Этап 2. Выполнить последовательное сведение исходной задачи тестирования к задаче построения более простых тестов (т.е. в конечном итоге к «локализации» целевого теста).

Этап 3. Преобразовать интуитивно полученную последовательность шагов

к эффективной алгоритмической процедуре (с помощью метода критических пар).

Замечание 1. S удовлетворяет аксиоме (SE), т.е.

S ( x ) ^ \* х.

Замечание 2. Для произвольного х є T справедливо утверждение:

х ^ \* S ( х )

Замечание 3. Аксиома (SC), выполнимость которой для S требуется проверить, имеет следующий вид:

х ^ \* у ^ S ( х ) = S ( у )

**Основные леммы метода локализации**

Пусть ^ - нётерово отношение редукции и S - алгоритм приведения к нормальной форме для ^ .

Тогда справедливы следующие утверждения:

Лемма 1. (сведение каноничности к условию Алонзо Чёрча - Джона Барклея Россера).

Алгоритм S является канонизацией для отношения ^ \* в том и только в том случае,

когда ^ имеет свойство Чёрча - Россера,

т.е. для произвольных x , у є T из x ^ \*у имеем x і y.

Лемма 2. (сведение условия Чёрча - Россера к условию слияния).

Отношение ^ имеет свойство Чёрча - Россера тогда и только тогда, когда оно удовлетворяет условию слияния, т.е. для произвольных x , у , z є T , если x \* ^ z ^ \* у , то x і у.

Лемма 3. (сведение условия слияния к условию локального слияния).

Отношение ^ удовлетворяет условию слияния тогда и только тогда,

когда ^ удовлетворяет условию локального слияния, т.е. для произвольных x , у , z є T ,

если x ^ z ^ у , то x і у.

Из свойства канонизации отношения о- \* очевидным образом следует свойство Чёрча - Россера,

Наоборот, пусть x ^ \* у .

Тогда для некоторого z имеем :

S (x) \* ^ x ^ \* z \* ^ у ^ \* S (у) вследствие свойства Чёрча - Россера.

Повторно применяя свойство Чёрча - Россера к :

S (x) и z S (у) и z

получаем равенство S (x) = z и аналогично равенство z = S (у) что и требовалось доказать.

Из свойство Чёрча - Россера

очевидным образом следует справедливость условия слияния.

Наоборот, поскольку отношение ^ \* представляет собой объединение всех отношений ^ n то можно воспользоваться индукцией по числу n.

Базис индукции для n = 0 выполняется очевидным образом.

Если x ^ n+1 у , то либо x ^ z ^ n у либо x ^ z ^ n у для определённого z .

В обоих случаях из предположения индукции следует справедливость z ^ \* u \* ^ у для некоторого u .

В первом случае имеем : x ^ \* u \* ^ у и, следовательно, x і у .

Во втором случае на основе свойства слияния имеем : x ^ \* v \* ^ u и для некоторого v .

Поэтому x ^ \* v \* ^ u \* ^ у то есть. снова x і у .

Из второго условия (т.е. условия локального слияния) очевидным образом следует первое условие (т.е. условие слияния).

Наоборот, пусть z 0 є T - произвольный фиксированный элемент.

Пользуясь «нётеровой» индукцией, докажем такое индукционное предположение :

Для всех z таких , что z 0 ^ + z и для произвольных x , у если x ^ \* z\* ^ у, то x і у.

Покажем, что для всех x , у , если x ^ \* z0\* ^ у, то x і у.

Случаи, когда x = z 0 и z 0 = у очевидны.

В противном случае имеем : x \* ^ x 1 ^ z 0 ^ у 1 ^ \* у для некоторых x 1 , у 1 .

Тогда согласно условию локального слияния и предположению индукции

существуют термы u , v , w , удовлетворяющие следующим пяти свойствам (см. след. слайд) :

(1) x 1 \* ^ z 0 ^ \*у 1 (2) x \* ^ x 1 ^ \* u (3) u\* ^ у 1 ^ \* у (4) v ^ \* w (5) у ^ \* w, что и требовалось доказать.

**Метод локализации**

**Доказательство Леммы 3**



Z

0

\

У 1



x

П И

u

v



ПИ - предположение индукции

**Метод локализации**

**Локальный критерий каноничности**

Из доказанных выше лемм

следует критерий проверки каноничности отображения S :

**Лемма 4. (локальный критерий каноничности).**

Отображение S является канонизацией для отношения ^ \*

тогда и только тогда,

когда для произвольных x , y , z

из x ^ z ^ у следует S ( x) = S (у ).

**Метод локализации**

**Эффективность метода локализации**

Замечание 1. Локальный критерий каноничности не является эффективным, т.к. для его проверки, в общем случае, необходимо рассмотреть бесконечно много x , у , z .

Замечание 2. Локальный критерий каноничности можно сделать эффективным,

если отношение ^ порождено конечным числом схем редукции посредством операций подстановки и замены.

Замечание 3. Центральная роль свойства Чёрча - Россера
для канонического упрощения

впервые была установлена при разработке ^-исчисления.

**План лекции: тема подраздела**

* Редукция алгебраических выражений
* Метод локализации
* **Метод критических пар**
* Метод пополнения

Метод критических пар используется для нахождения решения задачи упрощения для отношений эквивалентности = E на множествах термов, где E - система равенств алгебры T (X , Q ).

Для точной формулировки метода необходимы дополнительные понятия для описания замены термов в термах.

Замечание. Поясним эти понятия на примере.

Формальное определение можно получить

на основе алгебраических свойств древовидных графов.

Будем изображать термы из T (X , Q ) в виде деревьев.

Введём функцию разметки дерева терма, устанавливающую отношение между множеством мест N \* и множеством подтермов, расположенных на этих местах.

Множество всех мест (адресов) терма t обозначим следующим образом: Oc (t).

Пример.

Имеем терм t = ( g f x y g x y 3 x )

Дерево терма изображено на рисунке - см. следующий слайд.

Будем говорить, что подтерм ( f x y ) входит в t на месте (1), подтерм ( g x y 3) входит в t на месте (2), подтерм ( y ) входит в t на месте (1,2) и т.д.

Обозначим эти соответствия следующим образом: t / (1) = ( f x y )

t / (2) = ( g x y 3 )

t/(1, 2) = ( y )

Кроме того, t / (e) = t , где e - пустая последовательность мест.

Тогда множество всех мест терма t имеет вид:

Oc (t ) = { e , (1) , (2) , (3) , (1, 1) , (1, 2) , (2, 1) , (2, 2) , (2,3) }



Дерево терма t.

**Операция «местной» замены**

Обозначим символом «\_» (подчёркивание) конкатенацию на множестве N \* всех мест.

Префиксное упорядочение < на N \* определим следующим образом: u < v тогда и только тогда, когда u \_ w = v для некоторого w.

Далее положим:

* v / u = w , если u \_w = v
* u | v (скажем в этом случае, что u и v дизъюнктны), если не выполнено ни u < v , ни v < u .

Для термов s , t є T ( X , Q ) и места u обозначим t [ u ^ s ] терм, полученный из t заменой подтерма, который стоит на месте u на подтерм s .

Замечание.

Поясним последнее из введённых обозначений на вышеприведённом примере: t [ 2 ^ ( f f x x 2 ) ] = ( g f x y f f x x 2 x )

**Отношение «местной» редукции**

Пусть E - система равенств из T ( X , Q ) .

Отношение редукции ^ E на T ( X , Q ) определим обычным способом: s ^ E t , если t получается из s применением одного из равенств из E как правила преобразования, т.е. слева направо.

Определение. Говорят, что s редуцируется к t с помощью E

(это обозначается s ^ E t), если найдётся такое правило (a, b) є E ,

а также подстановка а и такое u є Oc ( s ) , что s / u = a ( a ) и t = f [ u ^ a ( b ) ] .

Пример. Пусть E - система аксиом для групп:

E = { (1) 1 \* x = x ; (2) x \* x -1 = 1 ; (3) ( x \* y ) \* z = x \* ( y \* z ) } .

Тогда ( x \* x -1) \* z ^ E1 \* z ^ E z

Замечание. В дальнейшем допускаются только такие системы E,

которые имеют следующее свойство:

для произвольных (a, b) є E var (a) з var (b) ,

где var (t) - множество переменных терма t.

**Определение критической пары**

Определение. Говорят, что термы p и q образуют критическую пару в E , если найдутся такие правила (a 1 , b 1 ), ( a 2, b 2 ) є E и такое место u є Oc ( a 1 ), что верно следующее:

* a 1 / u не является переменной;
* a 1/ u и a 2 являются унифицируемыми термами;
* p = а ( a ,) [ u ^ а 2 ( b 2 ) ] q = а , ( b , ) ,

где а 1 и а 2 - подстановки, причём а 1( a1 / u ) = а 2( a2 ) ,

которые представляют собой наибольший общий образ термов a 1 / u и a 2

(обладающий тем свойством,

что никакая переменная из а 1 ( a 1 / u ) не входит в a 1 ,

т.е. p и q получаются путём применения правил (a 1, b 1 ) и ( a 2, b 2 )

к наибольшему общему образу термов a 1 и a 2 ).

Пример.

Рассмотрим правила (3) и (2) и подтерм xy в правиле (3)

(См. предыдущий пример. Знак \* исключаем для простоты выражений).

Пусть a 1 = (xy)z , b 1 = x(yz) , a2 = x-1 x , b 2 = 1 , u = (1)

Тогда x -1 x является наибольшим общим образом термов a1 / u = xy и a2 = x -1 x

( так, что удовлетворено условие на переменные;

возьмём а 1( x ) = x -1 , а 1( y ) = x , а 2 - тождественная подстановка ).

Следовательно, следующие термы:

p = а ,( a,) [ u ^ а 2 ( b 2 ) ] = ( x -1x) z [ (1) ^ 1 ] = 1 \_ z q = а 1 ( b 1 ) = x -1 (xz) образуют критическую пару в E.

**Теорема Кнута - Бендикса**

Теорема (Дональд Кнут, Питер Бендикс, 1967)

(сведение условия локального слияния к условию слияния критических пар).

Отношение редукции ^ E удовлетворяет условиям локального слияния, если для произвольной критической пары ( p , q ) в E справедливо p ^E q .

Если E - конечное множество, то всегда можно построить алгоритм Sel такой, что t ^ E Sel ( t ) , когда t не в нормальной форме.

Если ^ E нётерово, то обозначим S E алгоритм нормальной формы, базирующийся на алгоритме Sel.

**Метод критических пар**

**Алгоритм критической пары**

**Вход**: E (**система равенств**)

**Вопрос**: **Является ли алгоритм** S E **нормальной формы канонизацией для отношения** = E ?

**Положить** C **равным множеству критических пар из** E .

**Цикл**

**Для всех** ( p , q ) є C **выполнить**

( p 0. q о) = S e ( p , s e ( q ) )

**Если** p 0 ф q 0. **то ответ** «S E **не канонично**» **и**

**выход из алгоритма**

**Конец цикла**

**Ответ**: «S E **канонично**»

Замечание. Корректность алгоритма является простым следствием вышеуказанных лемм и теорем.

**Некоторые свойства отношения — E**

Определение. Отношение — E называется стойким,

если для произвольных термов s , t и подстановки а имеет место:

s —— e t а ( s ) —— e а ( t ) .

Определение. Отношение — E называется совместным,

если для произвольных термов s , t 1,t 2 и U є Oc( s ) справедливо:

t і —— e t 2 s [ U —— t і ] —— E s [ U —— t 2 ] .

**Метод критических пар в теории групп**

Пример. Приведённая ниже система аксиом E’ для теории групп является нётеровой и находится по системе E (см. предыдущий пример) путём её пополнения следующими тождествами:

1. 1 -1 = 1
2. x -1 \* ( x \* y ) = y
3. x \* 1 = x
4. ( x -1) -1 = x
5. x \* x -1 = 1
6. x \* ( x -1 \* y ) = y
7. ( x \* y ) -1 = y -1 \* x -1

С помощью конечного числа проверок можно установить справедливость равенств S E. ( p ) = S E. ( q ) для всех критических пар из E’.

Таким образом, по теореме Кнута-Бендикса отношение ^ E, удовлетворяет условию (локального) слияния,

и S E, представляет канонизацию для отношения ^ \* E, = ^ \*E = =E

Иными словами, проверка тождеств в теории групп может быть полностью автоматизирована.

**План лекции: тема подраздела**

* Редукция алгебраических выражений
* Метод локализации
* Метод критических пар
* **Метод пополнения**

**Ключевые идеи метода пополнения**

Если редукция критической пары ( p , q ),

выполненная по алгоритму Кнута-Бендикса в системе равенств E, приводит к неравенству S (p) **ф** S **(q),** то следует попробовать добавить к E правило S (p) = S (q) или правило S (q) = S (p) для достижения полноты.

После такого добавления рефлексивно-симметрично-транзитивное замыкание отношения ^ E не изменяется, а само отношение ^ E расширяется.

Указанный процесс можно итерировать до тех пор, пока не будет достигнуто «насыщение»

(т.е. критическая пара будет иметь единственную нормальную форму).

Построенная таким образом система равенств снова порождает то же самое отношение эквивалентности = E, что и исходная система, но соответствующее ей отношение редукции ^ E единственное, т.е. ассоциированный алгоритм нормальной формы представляет собой канонизацию для отношения = E.

**Метод пополнения**

**Проблемы применения метода пополнения**

Перед расширением E необходимо проверить, сохранится ли после расширения нётеровость отношения ^ E

Для того, чтобы обеспечить свойство нётеровости

в расширенной системе равенств,

следует выбрать одну из двух возможных пар:

( S (p) = S (q)) или ( S (q) = S (p) )

Замечание.

Может оказаться, что сохранение свойства завершимости невозможно доказать ни для одной из указанных пар.

Тогда процесс пополнения не может быть разумно продлён.

**Алгоритм пополнения**

Ниже приведён возможный вариант алгоритма пополнения.

**Дано: E - конечная система равенств, такая, что о**> **E нётерово**

**Найти: F - конечную систему равенств, такую, что ^ \*E = о**- **\*F и ^ F**

**удовлетворяет условию (локального) слияния ( т.е. S F - канонизация )**

**F = E**

**C = множество критических пар из F Пока C** ф0 **выполнять цикл Взять ( p , q ) из C**

**( Р** о**, q** о**) = ( S** f **( p ) , S** f **( q ) )**

**Если p** о **\* q** о**, то**

**Анализировать ( p** о **, q** о **)**

**Добавить к C множество новых критических пар (( p** 0**, q** 0**) , F ) Добавить к F пару ( p** о **, q** о **)**

**Конец Если**

**Извлечь из C пару ( p , q )**

**Конец цикла Пока Остановиться в случае успеха**

**Неочевидные процедуры алгоритма**

Поясним сущность отдельных процедур, вошедших в алгоритм пополнения.

Процедура построения «множества критических пар»

находит критические пары,

полученные из нового правила ( p 0, q 0) и правил из F.

Процедура «анализировать» определяет, остаётся ли отношение ^ E нётеровым, когда ( p 0, q 0) или ( q 0, p 0) добавляются к E.

В первом случае пара ( p 0, q 0) не изменяется, во втором случае p 0 и q 0 меняются местами.

Если не выполняется ни одна из альтернатив,

то процедура «анализировать» останавливается с ответом «неуспех».

**Метод пополнения**

**Результативность алгоритма пополнения**Возможны три варианта результата выполнения алгоритма пополнения:
Алгоритм останавливается с положительным ответом.Тогда полученная в конце работы алгоритма система F удовлетворяет целевым условиям.
Алгоритм останавливается с ответом «неуспех».В этом случае нельзя сказать ничего определённого.
Алгоритм не останавливается.В этом случае алгоритм представляет собой перечисляющую процедуру для отношения = Е.Отношение s = Е t может быть перечислено посредством редукции s и t по отношению к увеличивающейся системе равенств, которая строится в процессе работы агоритма.