Введение в математическую логику и теорию алгоритмов

Лекция 15. Аксима выбора

Вполне упорядоченные множества

Пусть A – множество, а $R \subset A \times A$ – двуместное отношение, являющееся элементом нашей модели и задающее линейный порядок на A, т.е. для отношения R выполнены утверждения:

(1) $\forall u(\neg R(u,u))$ (антисимметричность)

(2) $\forall u,v,w(u<v \wedge v<w \to v<w)$ (транзитивеность)

(3) $\forall u,v(u=v \vee u<v \vee v<u)$ (линейность)

В дальнейшем вместо $R(x,y)$ мы будем писать $x<y$.

Порядок называется *фундированным*, если в любом непустом подмножестве множества A есть минимальный элемент, то есть выполнено утверждение

(4) $\forall u(u \subset A \wedge u \neq \varnothing \to \exists v(v \in u \wedge \forall w(w<v \to w \notin u)))$

Фундированный линейный порядок на множестве A называется *полным*, а само множество — *вполне упорядоченным*.

Примеры вполне упорядоченных множеств: конечный класс с любым линейным порядком, любой элемент множества ω, само множество ω.

Несколько простых свойств полных порядков:

(1) Во вполне упорядоченном множестве A существует наименьший элемент, мы будем обозначать его символом 0.

(2) Любое непустое подмножество вполне упорядоченного множества вполне упорядочено.

(3) Для каждого элемента x, кроме наибольшего, существует единственный непосредственно следующий за ним, то есть такой элемент y, что $x<y$ но не существует такого z, что $x<z<y$. Нужно в качестве y взять наименьший элемент из больших x (такие существуют). Такой элемент мы будем обозначать $x+1$, следующий за ним (если такой существует) $x+2$ и т.д. Рекурсивно определим для любого $n \in \omega$ элемент $a+n$ так, что $a+n$ – следующий за $a+(n-1)$ (если такой элемент существует).

Определение. Элемент x, не являющийся наименьшим и не имеющий непосредственно предшествующего (т.е. $x \neq y+1$ для всех y) называется *предельным*.

(4) Всякий элемент вполне упорядоченного множества имеет вид $a+n$ для некоторого $n \in \omega$ и предельного a. Действительно, если x — не предельный, то рассмотрим множество $x_0 > x_1 > \cdots > x_n > \ldots$ таких элементов, что $x_n + n = x$. В этом множестве должен быть наименьший элемен, он является предельным.

(5) Если A и B — вполне упорядоченные множества, то множества $A+B$ и $A\times B$ вполне упорядочены.

Напомним, что если A и B — два упорядоченных множества, то через $A\times B$ мы обозначаем множество пар, порядок на котором задан так: $<a_0,b_0> < <a_1,b_1>$ если $b_0<b_1$ или $b_0=b_1$ и $a_0<a_1$. Если A и B — два непересекающихся упорядоченных множества, то через $A+B$ мы обозначаем множество $A\cup B$, порядок на котором задан так: если $a\in A, b\in B$, то $a<b$ если $a,b\in A (a,b\in B)$ то порядок определяется порядком на $A(B)$.

Действительно, если $C\subset A+B$ содержит элементы из A, то нужно взять наименьший в $C\cap A$ если это множество непусто, в противном случае — в $C\cap B$. Если $C\subset A\times B$, то сначала найдем наименьший элемент $b_0\in B$, такой, что $<a,b_0>\in C$ для некоторого $a\in A$. Далее возьмем (непустое) подмножество $\{a|a\in A, <a,b_0>\in C\}$ и найдем в нем наименьший элемент a_0. Ясно, что $<a_0,b_0>$ будет наименьшим в C.

(6) Множества $\omega+k, \omega+\omega=\omega\times 2, k\times\omega, \omega\times k, \omega\times\omega$ вполне упорядочены. Здесь $k\in\omega$, а запись $\omega+\omega$ подразумевает, что мы берем две непересекающиеся копии множества ω (впрочем, можно просто вместо $\omega+\omega$ взять $\omega\times 2$). В множестве $\omega\times 2$ есть предельный элемент: $<0,1>$.

Начальные отрезки

Определение. Подмножество B вполне упорядоченного множества A называется *начальным отрезком* множества A, если вместе с каждым элементом множество B содержит и все меньшие, то есть $a\in B, b<a\Rightarrow b\in B$.

(7) Классы $[0,a)$ (совокупность элементов меньших a) и $[0,a]$ (совокупность элементов не больших a) являются начальными отрезками.

(8) Любой начальный отрезок множества A, отличный от A, имеет вид $[0,a)$. Достаточно взять наименьший элемент, не принадлежащий отрезку.

(9) Объединение любого семейства начальных отрезков является начальным отрезком.

Определение. Подмножество B упорядоченного множества A *кофинально* множеству A, если для любого $a\in A$ найдется $b\in B, a\leqslant b$.

Вполне упорядоченные множества представляют особый интерес, поскольку для них можно проводить доказательство по индукции и давать индуктивные определения примерно так же, как и для натуральных чисел. Индуктивное доказательство основывается на том, что если во вполне упорядоченном множестве есть элементы, удовлетворяющие некоторому условию, то найдется наименьший элемент, удовлетворяющий данному условию. Индуктивное определение основано на том, что если значение функции f на вполне упорядоченном множестве A определено на элементе 0 и значение $f(a)$ однозначно определяется набором значений $f(a')$ при $a'<a$, то, используя индукцию нетрудно показать, что такая функция определена на всем множестве A и единственна. Такая индукция называется *трансфинитной* индукцией. Достаточно часто трансфинитное индуктивное определение дается отдельно для предельных и непредельных элементов: значение отображения на непредельном элементе определяется значением на предыдущем элементе, значение на предельном

– набором значений на всех меньших. Мы не будем давать формальное определение трансфинитной индукции, ограничившись несколькими примерами.

Пусть A — вполне упорядоченное множество, $f\colon A \to A$ — монотонно возрастающая функция, то есть $a < b \Rightarrow f(a) < f(b)$. Тогда $f(a) \geqslant a$ для всех $a \in A$. Следовательно образ $f(A)$ кофинален A.

Доказательство. Пусть a' — наименьший элемент в множестве $s = \{a \in A | a > f(a)\}$. Тогда $a' > f(a') \Rightarrow f(a') > f(f(a'))$ (монотонность), т.е. $f(a')$ меньше $a', f(a') \in s$, противоречие. □

Два вполне упорядоченных множества A и B с порядками $<_A$ и $<_B$ называются *изоморфными*, если существует взаимнооднозначная функция отображающая A на B, сохраняющая порядок, то есть выполнено утверждение
$\exists f(Func(f) \wedge Dom(f) = A \wedge Ra(f) = B \wedge \forall u, v(u <_A v \equiv f(u) <_B f(v)))$

Следующий результат важен не только как иллюстрация понятий трансфинитная индукция и рекурсия, но и сам по себе.

Теорема об отображении полных порядков.
Пусть A и B — два вполне упорядоченных множества. Тогда или A изоморфно некоторому начальному отрезку B, или B изоморфно некоторому начальному отрезку A, причем этот изоморфизм единственен.

Доказательство. Назовем начальный отрезок I множества A *корректным*, если он изоморфен некоторому начальному отрезку множества B. Пусть I — корректный отрезок, а f_I — соответствующий изоморфизм на I. Нетрудно заметить, что для любого $a \in I$ образ $f_I([0, a))$ является начальным отрезком множества B. Таким образом f_I удовлетворяет (трансфинитному) рекурсивному соотношению $f_I(a) =$ *наименьший элемент* $\{b | b \in B, b \neq f_I(a')$ *для всех* $a' < a\}$. Таким образом, значение $f_I(a)$ полностью определяется значениями $f_I(a')$ при $a' < a$ и $f(0) = 0$. Отсюда, по трансфинитной индукции, следует, что такой изоморфизм единственен. Кроме того, если J такой начальный отрезок множества A, что $J \subset I$, то J тоже корректный и (из единственности) $f_I = f_J$ на J.

Семейство всех корректных начальных отрезков множества A, конечно, является (по аксиме степени и аксиоме подмножеств) множеством. Рассмотрим отрезок I_0 — объединение всех корректных начальных отрезков. Он корректен, поскольку отображение f_0 — объединение всех f_I — будет требуемым изоморфизмом. Если $A = I_0$ или $B = f_0(I_0)$, то все доказано. Пусть $I_0 = [0, a)$ для некоторого $a \in A$ и $f_0(I_0) \neq B$, положим $b' =$ *наименьший элемент* $B \setminus f(I_0)$. Функция $f' = f_0 \cup \{<a, b'>\}$ является изоморфизмом на $[0, a]$, что противоречит тому, что отрезок $[0, a]$ не корректный. □

Следствие. Подмножество B вполне упорядоченного множества A изоморфно начальному отрезку множества A.

Доказательство. Если B не изоморфно начальному отрезку A, то, по теореме об отображении полных порядков, множество A должно быть изоморфно собственному начальному отрезку B. Это невозможно, поскольку такой отрезок не кофинален A. □

Теорема об отображении полных порядков позволяет ввести отношение порядка на вполне упорядоченных множествах. Мы скажем, что множество A меньше множества $B (A < B)$, если A изоморфно собственному начальному отрезку B. Ясно, что для любого A неверно $A < A$, поскольку требуемый изоморфизм единственен (таким образм тождественен). То есть любые два множества A, B или изоморфны, или $A < B$ или $B < A$.

На первый взгляд вполне упорядоченные множества встречаются достаточно редко, однако мы собираемся вскоре показать, что в некотором смысле любое множество можно вполне упорядочить.

Аксиома выбора

Пусть A — некоторое множество, а f — такая функция, что $Dom(f) = P(A) \setminus \{\varnothing\}$, $Ra(f) \subset A$. Мы скажем, что f является *функцией выбора*, если $f(x) \in x$ для любого $x \subset A, x \neq \varnothing$.

Заметим, что если множество может быть вполне упорядочено, то для него есть функция выбора: в качестве f можно взять функцию $f(x) =$ *наименьший элемент множества* x. Следующая важная теорема утверждает, что верно и обратное.

Теорема Цермело. Если для множества существует функция выбора, то оно может быть вполне упорядочено.

Приблизительная схема доказательства. Мы будем использовать не саму функцию выбора f, а функцию дополнительного выбора g, определенную так, что $g(x) = f(A \setminus x)$. Эта функция определена на $P(A) \setminus \{A\}$ и для любого $x \subset A, x \neq A$ выполнено $g(x) \notin x$. Используя эту функцию, начнем определять порядок. Наименьшим элементом будет $a_0 = g(\varnothing)$. Следующим элементом будет $a_1 = g(\{a_0\})$, потом $a_2 = g(\{a_0, a_1\})$ и так далее. Если $\{a_0, a_1, \dots\} = A$ то порядок определен. В противном случае семейство $\{a_0, a_1, \dots\}$ будет начальным отрезком нашего порядка, а в качестве элемента, следующего за этим отрезком, возьмем $b_0 = g(\{a_0, a_1, \dots\})$, потом $b_1 = g(\{a_0, a_1, \dots\} \cup \{b_0\})$ и т.д.

Определяя порядок мы строим все большие начальные отрезки, причем порядок, который мы строим, "согласован" с функцией g: для любого начального отрезка $[0, a)$ выполнено $a = g([0, a))$.

Перейдем теперь к доказательству.

Доказательство. Пусть A — некоторое множество, f — функция выбора для A. Определим функцию дополнительного выбора $g\colon P(A) \setminus \{A\} \to A$ так, что $g(x) = f(A \setminus x)$, то есть $\forall u(u \subset A \wedge u \neq A \to g(u) \in A \setminus u)$.

Пусть B — подмножество A, и $<_B$ — порядок на B. Мы скажем, что пара $<B, <_B>$ корректна, если

(1) порядок $<_B$ полный и

(2) $\forall u(u \in B \to u = g(\{v | v \in B, v <_B u\}))$, то есть порядок $<_B$ "согласован" с функцией g.

Ясно, что $\{<B, r> \mid <B, r>$ — *корректная пара*$\}$ является множеством, обозначим его S.

Лемма. Корректные пары согласованы, то есть если $< B, <_B >$ *и* $< C, <_C >$ *— две корректные пары, то одна из них является начальным отрезком другой.*

Действительно, по теореме об отображении полных порядков существует изоморфизм одного из упорядоченных множеств на начальный отрезок другого. Пусть h — соответствующий изоморфизм, то есть взаимно однозначная монотонно возрастающая функция, отображающая множество B на начальный отрезок C. Покажем, что функция тождественна, то есть $h(x) = x$ трансфинитной индукцией по элементам B.

Ясно, что h переводит наименьший элемент множества B в наименьший элемент множества C, то есть $h(g(\varnothing)) = g(\varnothing)$.

Пусть d — произвольный элемент множества B и отрезки $[0, d)$ и $[0, h(d))$, как и отношения $<_B$ и $<_C$ на них, по индуктивному предположению совпадают. Тогда $d = g(\{x | x <_B d\})$ и $h(d) = g(\{x | x <_C h(d)\})$, значит $d = h(d)$.

Лемма доказана

Поскольку все корректные пары согласованы, то мы можем рассмотреть множество $U = Un\{B | \exists u(< B, u > \in S)\}$ и определить порядок на U так, что $x < y \Leftrightarrow x <_B y$ *для некоторого* $< B, <_B > \in S$. Это полный порядок, поскольку если $x \subset U, x \neq \varnothing$, то $x \cap B \neq \varnothing$ для некоторого B и наименьший (в смысле порядка $<_B$) элемент в этом пересечении будет наименьшим элементом x. Если $U \neq A$, то возьмем $g(U)$ и доопределим порядок на $U \cup \{g(U)\}$ так, что $x < g(U)$ для любого $x \in U$. Легко проверить, что $U \cup \{g(U)\}$ с этим порядком будет корректной парой, что противоречит определению U. □

Утверждение о наличии функции выбора у произвольного множества выглядит достаточно естественно и может быть добавлено в качестве дополнительной аксиомы.

Аксиома выбора.

$$\forall u \exists f(Func(f) \wedge Dom(f) = P(u) \setminus \{\varnothing\} \wedge \forall v(v \in Dom(f) \rightarrow f(v) \in v))$$

для любого множества существует функция выбора.

Эта аксиома обозначается **AC**, а теория, полученная добавлением к **ZF** аксиомы выбора, обозначается **ZFC**.

Аксиома выбора является аксиомой существования, однако, в отличие от прочих аксиом существования, она не дает никакого способа построить множество (функцию выбора), существование которого она гарантирует.

Возникают естественные вопросы:
(1) Действительно ли **ZFC** является расширением теории **ZF**? То есть действительно ли **ZF** $\nvdash$ **AC**?
(2) Не получим ли мы в результате такого расширения противоречивую теорию? То есть верно ли, что **ZF** $\nvdash \neg$**AC**?

Конечно, оба эти вопроса имеют смысл, как мы указывали раньше, лишь в том случае, если мы считаем саму теорию **ZF** непротиворечивой.

Мы уже настолько хорошо знакомы с математической логикой, чтобы понять смысл этих вопросов, но весьма далеки от того, чтобы хоть в общих чертах понять, каким образом были получены ответы. Поэтому ограничимся замечанием о том, что утверждение об (относительной) непротиворечивости теории **ZFC** было получено Гёделем, а (относительная) невыводимость аксиомы **AC** в **ZF** была доказана Коэном.

Аксиома выбора свободно используется в различных математических доказательствах, однако следует заметить, что рассуждения, основанные на аксиме выбора иногда приводят к результатам, выглядищим на первый взгляд парадоксальными. Приведем два таких примера.

Парадокс Банаха – Тарского. Шар можно разбить на пять частей, передвинув которые можно сложить (без пустот и пересечений) два шара такого же радиуса.

Второй пример относится к ***игре Банаха – Мазура***. Игра состоит в следующем: на отрезке $[0, 1]$ выбирается подмножество A. Два игрока поочередно выбирают отрезки $S_0 \supset S_1 \supset S_2 \ldots$. Первый игрок выигрывает, если в пересечении всех отрезков S_i найдется точка из A.

Множество A называется *детерминированным*, если у одного из игроков есть выигрышная стратегия при игре с множеством A. Известно, что многие множества являются детерминированными, например, детерминированно любое счетное множество (докажите это, пожалуйста).

Утверждение о том, что любое множество детерминированно, называется *аксиомой детерминированности*.

Доказано, что из аксиомы выбора следует отрицание аксиомы детерминированности.