1-я лекция курса "Теория дискретных функций"

(1-й курс; лектор - проф. А.С.Подколзин)

Появление и развитие вычислительной техники привело к необходимости решать множество задач дискретного характера. Такие задачи возникают как при разработке чипов, так и при создании прикладных программ. Для описания структуры и функционирования вычислительных систем были созданы разнообразные дискретные математические модели. В математике возникли новые направления, связанные с этими моделями - теория дискретных функций, теория автоматов, теория алгоритмов, теория сложности вычислений, теория кодирования и др. Эти направления, хотя и сравнительно молодые, располагают внушительным запасом мощных методов и нетривиальных результатов. Данный курс ориентирован лишь на предварительное ознакомление с миром дискретной математики и математической кибернетики.

Знакомство с теорией дискретных функций естественно начинать с простейшего, хотя и наиболее распространенного случая таких функций, - с алгебры логики. Функции алгебры логики были введены в рассмотрение Дж.Булем еще в середине 19 века. Они представляли собой средство определять истинность или ложность сложного высказывания исходя из истинности или ложности составляющих его элементарных высказываний. Соответственно, как аргументы функции, так и она сама принимали всего два значения - "истина" или "ложь". Впоследствии К.Шеннон "открыл" возможность применения таких функций для описания работы релейно-контактных схем, из которых собирались первые компьютеры. Здесь уже функция имела значения 0 либо 1, соответственно отсутствию или наличию тока в проводнике. В настоящее время работа с функциями алгебры логики - неотъемлемая часть процесса проектирования чипов. Они широко применяются и в программировании. Мы рассмотрим лишь небольшой фрагмент алгебры логики, связанный с задачами полноты и выразимости для множеств функций.

Данный конспект лекций представляет собой переработку материала, содержащегося в учебнике С.В.Яблонского "Введение в дискретную математику", а также в монографии В.Б.Кудрявцева, С.В.Алешина и А.С.Подколзина "Введение в теорию автоматов". Однако, имеется существенное расхождение между изложением материала в курсе и в этих книгах, особенно в первой из них. Главным образом, оно вызвано необходимостью уточнения понятия формулы и понятия равенства функций, без которого доказательства становятся запутанными и теряют математическюу строгость. Многие определения и формулировки из данной книги пришлось скорректировать, и пользоваться ими на экзамене в первоначальном варианте не рекомендуется.

Алгебра логики

Функции и множества вообще

Начнем с напоминания некоторых общих свойств функций и множеств. Понятие множества в математике является базисным. Оно не определяется, а лишь характеризуется посредством аксиом. Рассматриваются отношение $a \in A$ принадлежности элемента a множеству A, а также определяемые через это отношение операции $A \cup B$, $A \cup B$, $A \setminus B$.

Понятие функции, вообще говоря, может быть сведено к понятию множества, через рассмотрение графика этой функции. Однако, проще считать его тоже не определяемым, а лишь характеризуемым с помощью аксиом. Чтобы задать функцию f, нужно задать, во-первых, множество $\mathrm{Dom}(f)$, на котором она задана - область определения функции, а, во-вторых, для каждого элемента x области определения указать значение $f(x)$ этой функции. Таким образом, приходим к следующему определению равенства функций f, g:

$f = g \leftrightarrow \mathrm{Dom}(f) = \mathrm{Dom}(g)\ \&\ \forall_x(x \in \mathrm{Dom}(f) \rightarrow f(x) = g(x))$.

Вся эта преамбула про функции и множества введена лишь для того, чтобы уточнить общепринятое в математике понятие равенства функций. Оно отличается от того, которое имеется в учебнике "Введение в дискретную математику", где равными могут оказаться функции с различными областями определения. На это стоит обратить внимание при чтении данного учебника.

Конечный упорядоченный набор $(a_1 \ldots, a_n)$ - это, по сути, тоже функция, определенная на начальном отрезке $\{1, \ldots, n\}$ натурального ряда и принимающая в точке i значение a_i. Так как мы будем иметь дело только с упорядоченными наборами, слово "упорядоченный" условимся опускать. С помощью таких наборов определяется прямое произведение $A_1 \times \ldots \times A_n$ множеств $A_1, \ldots, A_n$. Оно состоит из всевозможных наборов $(a_1, \ldots, a_n)$, где $a_i \in A_i; i = 1, \ldots, n$. Иногда рассматривается набор длины 0. Он определен на пустом множестве и обозначается Λ.

Если функция f определена на прямом произведении $A_1 \times \ldots \times A_n$, то ее называют функцией от n переменных и обозначают $f(x_1, \ldots x_n)$. Заметим, что на самом деле никаких "переменных" у нас пока нет. Они появятся позднее, когда речь пойдет о формулах. Для функции "число переменных" - это просто число сомножителей в прямом произведении, являющемся ее областью определения.

Функции алгебры логики

Обозначим посредством E_2 множество $\{0, 1\}$. Прямое произведение $E_2 \times \ldots \times E_2$, где число сомножителей равно n, обозначаем B_n. Оно представляет собой множество координат вершин n-мерного куба с длиной стороны 1. В алгебре логики данное множество называется n-мерным булевым кубом. Допускается случай $n = 0$, и тогда булев куб состоит из единственного пустого набора Λ.

Функцией алгебры логики называется функция $f : B_n \rightarrow E_2$. Здесь n - любое целое неотрицательное. Иными словами, функция алгебры логики $f(x_1, \ldots, x_n)$ определена на наборах нулей и единиц, имеющих длину n, и в качестве своего значения принимает 0 либо 1. При $n = 0$ получаем константные функции 0,1. Наборы из нулей и единиц будем называть двоичными наборами.

Множество всех функций алгебры логики обозначается P_2.

Функцию алгебры логики $f(x_1, \ldots, x_n)$ можно задать таблицей, имеющей $n+1$ столбец. В первых n столбцах, соответствующих переменным $x_1, \ldots, x_n$, перечисляются все 2^n возможных наборов их значений. В последнем столбце указываются соответствующие значения функции f. Так как высота такого столбца равна 2^n, то количество возможных способов их заполнения равно 2^{2^n}. Это - число функций алгебры логики, зависящих от n переменных.

Функцию алгебры логики $f(x_1, \ldots, x_n)$ назовем существенно зависящей от переменной x_i, $i \in \{1, \ldots, n\}$, если существуют такие значения $\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n$ из E_2, что

$f(\alpha_1, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n) \neq f(\alpha_1, \ldots, \alpha_{i-1}, 1, \alpha_{i+1}, \ldots, \alpha_n)$.

В этом случае x_i называется существенной переменной функции f. Переменная, не являющаяся существенной, называется несущественной или фиктивной. Уточним, что фактически здесь подразумевается лишь номер переменной i.

Пусть x_i - несущественная переменная функции $f(x_1, \ldots, x_n)$. Тогда функция

$g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)$

называется полученной из f удалением i - й несущественной переменной. Обратно, говорим, что f получена из g добавлением i-й несущественной переменной.

Если функции f, g получены друг из друга цепочкой переходов ввода или удаления несущественной переменной, то назовем их эквивалентными. Заметим, что в учебнике эти функции названы равными, что не соответствует общепринятому пониманию равенства функций.

Функция алгебры логики $f(x_1, \ldots, x_n)$ называется симметрической относительно переменных $x_{i_1}, \ldots, x_{i_k}$, если любая перестановка значений этих переменных не изменяет значения функции. В частном случае, когда функция симметрическая относительно всех своих переменных, она называется симметрической. Такую функцию можно задавать таблицей, существенно более короткой, чем в общем случае. Она имеет всего два столбца. В первом из них указывается количество переменных, равных 1. Во втором - соответствующее значение функции. Таблица имеет всего $n + 1$ строку.

Обычно функции алгебры логики задаются не таблицами, а формулами. Для этого, прежде всего, выделяются некоторые функции алгебры логики, которые считаются "элементарными". Выбор таких функций в достаточной степени произвольный, однако чаще всего рассматриваются следующие элементарные функции:

1. Константы 0,1 (нуль-местные функции).
2. Тождественная функция x (одноместная).
3. Функция "отрицание", которая обозначается $\bar{x}$ (иногда - $\neg(x)$), и равна $1 - x$.
4. Функция "конъюнкция", или "и". Она обозначается $x_1 \& x_2$ либо $x_1 \cdot x_2$ и равна минимуму (или, что в данном случае то же самое, произведению) значений x_1, x_2.
5. Функция "дизъюнкция", или "или". Она обозначается $x_1 \vee x_2$ и равна максимуму значений x_1, x_2.
6. Функция "импликация" (логическая связка "если-то"). Она обозначается $x_1 \to x_2$. Эта функция принимает значение 0 в единственном случае: если $x_1 = 1$, а $x_2 = 0$. Иначе она равна 1.
7. Функция "сумма по модулю 2". Она обозначается $x_1 + x_2$ или $x_1 \oplus x_2$. Обычно будем использовать первое обозначение. Она принимает значение, равное сумме по модулю 2 значений x_1, x_2. Иными словами, она равна 1, если данные значения различаются.

8. Функция "эквивалентность". Она обозначается $x_1 \leftrightarrow x_2$. Равна 1, если значения x_1, x_2 совпадают, и равна 0 в противном случае.

9. Функция "штрих Шеффера". Она обозначается $x_1|x_2$. Ее значение определяется как $\overline{x_1 \ \& \ x_2}$. Иными словами, оно равно 0 только в случае $x_1 = x_2 = 1$.

10. Функция "стрелка Пирса". Она обозначается $x_1 \downarrow x_2$. Ее значение определяется как $\overline{x_1 \ \vee \ x_2}$. Иными словами, оно равно 1 только в случае $x_1 = x_2 = 0$.

Две последние функции играют особую роль. Во-первых, каждая из них является "полной" - через нее можно выразить любую другую функцию алгебы логики. Во-вторых, оказалось, что физическая реализация этих функций "дешевле", чем реализация дизъюнкций и конъюнкций, из-за чего в чипах они и встречаются гораздо чаще.

Используя элементарные функции, с помощью формул можно определять другие функции. В математике понятию формулы редко дают точное определение. Исключение составляют лишь курсы математической логики. Там дается точное определение не только того, что такое формула, но даже того, что такое математическая теория.

Различие между формулой и функцией состоит в том, что функция - абстрактный математический объект, а формула - лишь способ его задания. В традиционных разделах математики изучаются функции, а не формулы; поэтому и потребности в точном определении формулы не возникает. В теории дискретных функций и математической кибернетике рассматриваются различные способы задания функций - формулы, схемы, программы и др. Зачастую ставится задача оптимизации таких способов - уменьшение числа элементов схемы, уменьшение времени ее работы и т.п. Таким образом, основным объектом исследования становится уже не функция, а способ ее задания, в частности, формула. Разумеется, чтобы доказывать какие-то утверждения о таком способе, необходимо иметь точное его определение.

К сожалению, автор учебника "Введение в дискретную математику", чтобы сделать определение формулы "интуитивно более понятным", вместо традиционного индуктивного определения из математической логики, привел такую версию, в которой понятия формулы и функции отождествляются уже в базисе индукции: "Каждая функция $f(x_1 \dots x_n)$ из B называется формулой над B". Такое "смазанное" определение, по-видимому, оказалось не очень хорошей идеей, и лектору было поручено использовать в данном курсе обычное определение формулы. Это определение, взятое из математической логики, было упрощено до той степени, в которой оно будет необходимо для работы с дискретными функциями. Следует заметить, что использование точного определения ничуть не усложнило доказательств, а некоторые из них даже упростило.

Под формулой в математической логике понимается слово в некотором алфавите A. Алфавитом может служить произвольное конечное либо бесконечное множество, а словом в этом алфавите называется произвольная функция, определенная на начальном отрезке натурального ряда и принимающая значения из A. По существу, это синоним термина "упорядоченный набор элементов A". Таким образом, слово $a_1 \dots a_n$ - функция α, определенная на $\{1, \dots, n\}$ и принимающая в точке i значение a_i. Обычно вместо записи $a_1 \dots a_n$ мы будем пользоваться записью $\alpha(1) \dots \alpha(n)$. Как

и в случае наборов, пустое слово (слово с пустой областью определения) обозначаем Λ.

Чтобы строить формулы из некоторого множества F функций алгебры логики, которые мы захотим считать "элементарными", нужно как-то обозначить эти функции. Пусть S - множество символов (на самом деле - объектов произвольной природы), которые будут использоваться для обозначения функций из F. Отображение Σ множества S на множество F, сопоставляющее каждому символу из S обозначаемую этим символом функцию, назовем сигнатурой для F. Вообще говоря, различным символам из S может сопоставляться одна и та же функция.

Для построения формул нам понадобятся также переменные. Выберем для всех последующих рассмотрений фиксированный счетный список $X = \{x_1, x_2, \ldots\}$ объектов, которые будем называть символами переменных.

Формулы в сигнатуре Σ определяются индуктивно:

1. Если x_i - символ переменной, то однобуквенное слово, образованное символом x_i - формула в Σ.

2. Если $s \in S$, функция $f = \Sigma(s)$ зависит от n переменных, причем $\Phi_1, \ldots, \Phi_n$ - формулы в сигнатуре Σ, то слово $s(\Phi_1, \ldots, \Phi_n)$ - формула в сигнатуре Σ.

Таким образом, каждая формула в сигнатуре Σ представляет собой слово в алфавите $X \cup S$, пополненном двумя скобками и запятой.

Заметим, что пока мы никак не определили связь между формулами и функциями. Мы лишь дали индуктивное определение некоторому классу слов. Перейдем к установлению такой связи.

Пусть Φ - формула в сигнатуре Σ; $\tilde{x} = (x_{i_1}, \ldots, x_{i_n})$ - какой-либо упорядоченный набор переменных, включающий все переменные формулы Φ; $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ - двоичный набор.

Определим значение $\Phi[\tilde{x}, \tilde{\alpha}]$ формулы Φ на наборе $\tilde{\alpha}$ значений переменных $\tilde{x}$ индукцией по построению формулы Φ:

1. Если Φ есть однобуквенное слово x_{i_j}, то $\Phi[\tilde{x}, \tilde{\alpha}] = \alpha_j$.

2. Пусть Φ имеет вид $s(\Phi_1, \ldots, \Phi_n)$, $f = \Sigma(s)$, причем уже определены $\Phi_1[\tilde{x}, \tilde{\alpha}] = \beta_1, \ldots, \Phi_n[\tilde{x}, \tilde{\alpha}] = \beta_n$. Тогда
   $\Phi[\tilde{x}, \tilde{\alpha}] = f(\beta_1, \ldots, \beta_n)$.

Заметим, что функции мы пока не определили. Значение формулы на наборе значений переменных - это лишь промежуточное понятие.

Переменную x_{i_j} формулы Φ назовем существенной, если существуют такие значения $\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n$, что

$\Phi_1[\tilde{x}, \alpha_1, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n] \neq \Phi_1[\tilde{x}, \alpha_1, \ldots, \alpha_{i-1}, 1, \alpha_{i+1}, \ldots, \alpha_n]$.

В противном случае переменная x_{i_j} называется несущественной, или фиктивной. Очевидно, что для однозначного определения значения формулы достаточно указать значения только ее существенных переменных.

Перейдем теперь к определению функции, задаваемой формулой. Сначала рассмотрим следующий вопрос. Пусть имеются две формулы $x \vee y$ и $y \vee z$. Задают ли эти формулы одну и ту же функцию или разные функции ? С одной стороны, каждая из них определяет двуместную дизъюнкцию. Это предполагает ответ "да". С другой стороны, если положить значения x, y равными нулю, а значение z - равным 1, то значения формул, а следовательно, и задаваемых ими функций окажутся различными. Это вызывает желание ответить "нет". Кажущееся противоречие объясняется некорректной постановкой вопроса. В действительности формула сама по себе не задает никакой функции. Чтобы она задавала функцию, следует обязательно добавить к ней список переменных, относительно которых она будет рассматриваться. В приведенном выше примере каждая из формул задавала функцию от двух переменных - дизъюнкцию, если ее рассматривать только относительно ее собственных переменных. Эти функции, разумеется, совпадают. Однако, если рассматривать каждую формулу относительно переменных x, y, z (одна из них будет несущественной), то функции от трех переменных окажутся уже различными.

Теперь можно перейти к определению связи между формулой и функцией. Пусть Ф - формула в сигнатуре Σ; $P = \{x_{i_1}, \ldots, x_{i_n}\}$ - некоторое множество переменных, включающее все существенные переменные формулы Ф. Будем считать, что $i_1 < i_2 < \ldots < i_n$. Обозначим $\tilde{x} = (x_{i_1}, \ldots, x_{i_n})$. Рассмотрим функцию алгебры логики f, определенную на B_n и такую, что для любого $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n) \in B_n$ выполнено $f(\alpha_1, \ldots, \alpha_n) = \Phi[\tilde{x}, \tilde{\alpha}]$. Скажем, что формула Ф определяет функцию f относительно переменных P (или "для переменных P").

Можно не уточнять P (если Ф и f уже имеются) и говорить, что Ф определяет f, если текущий контекст позволяет такое сокращение.

Будем называть формулы в сигнатуре Σ, представляющие собой переменные, вырожденными, а прочие формулы - невырожденными. Если функция f определяется в сигнатуре $\Sigma : S \to F$ невырожденной формулой, то говорим, что она получена суперпозициями из функций системы F (или "получена суперпозициями над F").

Вырожденные формулы отбрасываются просто потому, что они задают тождественную функцию, и если нас интересует, какие функции можно получать при помощи "элементарных" функций из F, то нет никаких оснований сразу добавлять тождественную функцию - ведь она может и не выражаться через функции системы F. Однако, для упрощения индуктивного определения формулы использование в базисе индукции переменных вполне оправдано.

Суперпозиции можно определять и без понятия формулы, используя следующие три операции, позволяющие выражать новые функции через ранее полученные:

1. Операция подстановки переменных.

   Пусть $f(x_1, \ldots, x_n) \in P_2$. Рассмотрим упорядоченный набор $(i_1, \ldots, i_n)$ элементов множества $\{1, \ldots, n\}$. В этом наборе допускаются повторения элементов. Например, все они могут совпадать. Пусть $g(x_1, \ldots, x_n)$ - функция, определенная на B_n, а значения ее задаются равенством:

   $g(x_1, \ldots, x_n) = f(x_{i_1}, \ldots, x_{i_n})$.

   Тогда скажем, что g получена из f операцией подстановки переменных. Здесь термин "подстановка" берет свои истоки в математической логике, где определяется операция подстановки в формулу вместо некоторых ее переменных

каких-то других формул. Он никак не связан с термином "подстановка" из алгебры. В частности, еще раз повторим это, в наборе $(i_1, \ldots, i_n)$ допускаются произвольные совпадения разрядов. Заметим также, что в данном пункте мы вообще не рассматриваем формул и работаем только с функциями f, g.

2. Операция подстановки одной функции в другую.

   Пусть имеются функции алгебры логики $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_m)$. Рассмотрим функцию h, определенную на B_{m+n-1}, значения которой задаются следующим равенством:

   $h(x_1, \ldots, x_{n+m-1}) = f(x_1, \ldots, x_{n-1}, g(x_n, \ldots, x_{n+m-1}))$.

   Скажем, что эта функция получена из функций f, g операцией подстановки одной функции в другую.

3. Операция добавления либо удаления фиктивной переменной.

   Эта операция уже была определена в начале лекции.

Можно доказать, что функция тогда и только тогда получается суперпозициями над F, когда она может быть получена из функций системы F конечной последовательностью применений указанных трех операций. По сути, это еще одно определение суперпозиции. Доказательсто этого утверждения выходит за рамки данного курса, так как относится скорее к математической логике, нежели к теории дискретных функций. Хотя оно и несложно (все делается по индукции), но потребовало бы точного определения операции подстановки в формулу набора формул вместо набора переменных, а также понятий вхождения в формулу и операции замены заданного вхождения в формулу на другую формулу. Пришлось бы доказывать также лемму о подстановке и лемму о замене - утверождения о том, что указанные операции над формулами приводят к аналогичным операциям над функциями. Все это далеко увело бы в сторону от рассмотрения функций алгебры логики.

Однако, краткий набросок доказательства все же следует дать. Чтобы показать, что каждая функция, определяемая невырожденной формулой, может быть получена указнными тремя операциями суперпозициями, можно провести индукцию по определению формулы. Базис индукции очевиден. Если вводится новая формула $s(\Phi_1, \ldots, \Phi_n)$, $f = \Sigma(s)$ то для получения операциями суперпозиции определяемой ею функции $f(g_1, \ldots, g_n)$ можно последовательно перемещать операцией подстановки переменных аргументы x_i функции f в конец списка переменных, а затем подставлять вместо них соответствующую функцию g_i операцией подстановки одной функции в другую. Например, рассмотреть функцию $g(x_2, \ldots, x_{n-1}, x_1) = f(x_1, \ldots, x_n)$ и затем подставить в g функцию g_1 вместо x_1. Таким образом получится $f(g_1, x_2, \ldots, x_n)$, и т.д.

Обратно, чтобы показать, что каждая функция, получаемая операциями суперпозиции, может быть задана формулой, используется индукция по длине цепочки применений этих операций. В случае операции подстановки переменных нужно применить к формуле соответствующую подстановку переменных. В случае операции подстановки одной формулы в другую - предпринять подстановку для формул. Добавление и удаление несущественных переменных изменения формулы не требует.

Еще раз повторим, доказательство указанных двух определений суперпозиции, и даже набросок его, в программу данного курса не входят, так как относятся, по

существу, к курсу математической логики. На экзамене этот вопрос задаваться не будет.

Второе определение суперпозиции будет обычно использоваться в различного рода индуктивных доказательствах. Здесь оно удобнее первого. Однако, в нескольких случаях первое определение окажется трудно заменимым. Собственно, для этих случаев и пришлось вводить точное определение формулы.