Московский физико-технический институт
Факультет инноваций и высоких технологий
Основы комбинаторики и теории чисел, осень 2012
Лекция 2: отображения и соответствия

Аннотация

Понятие соответствия. Понятие отображения. Обозначения. Инъективные и сюръективные соответствия. Инъекции и сюръекции. Биекции. Взаимно однозначные отображения. Понятия образа и прообраза множества при соответствии. Критерий равенства образа пересечения и пересечения образов. Область определения и область значений соответствия. Сужение и продолжение соответствия. Частично определённые функции. Композиция соответствий, её ассоциативность. Тождественное отображение. Обратное соответствие. Возведение соответствия в степень. Возведение множества в степень. Булеан. Свойства возведения множества в степень.

Эта лекция целиком будет состоять из определений и простых утверждений, из них вытекающих. Мы поговорим о соответствиях, отображениях и связанных понятиях. Они немного по-разному определяются в разных источниках, поэтому нужно договориться о терминологии.

1 Основные виды соответствий и отображений

Определение 1. *Соответствием* между множествами A и B называют произвольное подмножество декартова произведения $F \subset A \times B$.

При этом множества A и B понимаются несимметрично: вместо того, чтобы говорить, что элементы $a \in A$ и $b \in B$ соответствуют друг другу, говорят, что элементу a соответствует элемент b (или несколько разных элементов, или ни одного). Эту асимметрию подчёркивают обозначениями: вместо $F \subset A \times B$ пишут $F\colon A \to B$, а вместо $(a, b) \in F$ пишут $b \in F(a)$. В последнем случае $F(a)$ выступает как множество всех элементов B, соответствующих данному a.

Определение 2. *Отображением* из множества A в множество B называется однозначное соответствие между A и B, т.е. такое соответствие, что для любого $a \in A$ найдётся ровно одно $b \in B$, соответствующее a.

Для отображения тоже используют запись $F\colon A \to B$, а про отдельные элементы пишут $b = F(a)$ или $F\colon a \mapsto b$. Отображения также называют *функциями*.

Некоторые авторы произвольное подмножество $A \times B$ называют (бинарным) отношением и пишут aFb. В этом случае априорной асимметрии между A и B нет. В нашем курсе слово «отношение» будет использоваться только для подмножеств $A \times A$. Также иногда на соответствия накладывают требование непустозначности, при которой каждому a должно соответствовать хотя бы одно b, т.е. $F(a)$ должно быть непустым. Мы этого делать не будем. Соответствия также называют *многозначными функциями* и используют обозначение $F\colon A \rightrightarrows B$, чтобы подчеркнуть многозначность.

Определение 3. *Инъективным* соответствием называется соответствие, при котором для любых $a_1 \neq a_2$ множества $F(a_1)$ и $F(a_2)$ не пересекаются. Инъективное отображение называется *инъекцией*.

Требование инъективности отображения можно переформулировать так: при $a_1 \neq a_2$ должо быть выполнено $F(a_1) \neq F(a_2)$. А можно так: каждый элемент B соответствует не более, чем одному элементу A. Иногда для инъекции используют обозначение $F\colon A \hookrightarrow B$.

Определение 4. *Сюръективным* соответствием называется соответствие, при котором любой элемент B соответствует хотя бы одному элементу A, т.е. любой $b \in B$ лежит в $F(a)$ для некоторого $a \in A$. Сюръективное отображение называется *сюръекцией*.

В определении сюръекции можно сказать, что любой элемент b равняется $F(a)$ для некоторого a. Иногда для сюръекции используют обозначение $F\colon A \twoheadrightarrow B$.

Определение 5. *Биекцией* называется отображение, являющееся одновременно инъекцией и сюръекцией.

Тут нужно быть аккуратным: соответствие, являющееся одновременно инъективным и сюръективным, вовсе не обязательно будет биекцией. Ведь оно не обязательно будет отображением. В качестве синонима слова «биекция»используют выражение «взаимно однозначное соответствие». Это объясняется следующим утверждением:

Утверждение 6. *Соответствие является биекцией тогда и только тогда, когда каждому элементу A соответствует ровно один элемент B, а также каждый элемент B соответствует ровно одному элементу A.*

Доказательство. Пусть F является биекцией. Тогда, поскольку оно является отображением, каждому элементу A соответствует ровно один элемент B. Поскольку оно является сюръекцией, каждый элемент B соответствует хотя бы одному элементу A, а поскольку оно является инъекцией, то не более чем одному. Значит, каждый элемент B соответствует ровно одному элементу A, т.е. соответствие является взаимно однозначным.

Обратно, взаимно однозначное соответствие является однозначным, т.е. отображением. А поскольку каждый элемент B соответствует ровно одному элементу A, то оно является одновременно инъективным и сюръективным. А значит, это биекция. □

2 Образ и прообраз. Сужение и продолжение

Определение 7. Пусть $F\colon A \to B$ — соответствие, а $S \subset A$. Тогда *образом* множества S называется множество всех элементов B, соответствующих какому-то элементу S. Формально можно записать так: $F(S) = \cup_{s \in S} F(s) \subset B$.

Заметим, что для одноэлементных множеств $F(\{a\}) = F(a)$.

Определение 8. Пусть $F\colon A \to B$ — соответствие, а $T \subset B$. Тогда *прообразом* множества T называется множество элементов A, которым соответствует хотя бы один элемент T. Формально $F^{-1}(T) = \{a\colon F(a) \cap T \neq \varnothing\} \subset A$.

Для отображений определения образа и прообраза можно упростить. Образ можно определить как $F(S) = \{F(s) : s \in S\}$, а прообраз — как $F^{-1}(T) = \{a : F(a) \in T\}$. В терминах образов и прообразов можно определить инъективность и сюръективность: соответствие инъективно, если образы разных элементов не пересекаются, или, эквивалентно, если прообраз каждого элемента не более чем одноэлементен. Соответствие сюръективно, если образ A равен B, или если прообраз любого элемента непуст.

Про связь понятий образа и прообраза можно доказать много различных утверждений. Приведём для примера одно.

Утверждение 9. *Образ пересечения любых двух множеств равняется пересечению образов тех же множеств тогда и только тогда, когда соответствие инъективно.*

Доказательство. Пусть соответствие не инъективно. Тогда найдутся такие a_1 и a_2, что $F(a_1)$ и $F(a_2)$ пересекаются. Тогда $F(\{a_1\} \cap \{a_2\}) = F(\varnothing) = \varnothing$, но $F(\{a_1\}) \cap F(\{a_2\}) = F(a_1) \cap F(a_2)$ не пусто по предположению. Значит, образ пересечения множеств $\{a_1\}$ и $\{a_2\}$ не равен пересечению образов.

Теперь пусть соответствие инъективно. Рассмотрим произвольные подмножества S и Q множества A. Докажем, что $F(S \cap Q) = F(S) \cap F(Q)$. Для этого докажем включение в обе стороны. Вначале пусть $y \in F(S \cap Q)$. Это значит, что $y \in F(x)$ для некоторого $x \in S \cap Q$. Но тогда $x \in S$ и $x \in Q$. А раз $y \in F(x)$, то $y \in F(S)$ и $y \in F(Q)$. Значит, $y \in F(S) \cap F(Q)$.

Теперь пусть $y \in F(S) \cap F(Q)$. Это значит, что $y \in F(S)$ и $y \in F(Q)$. Значит, $y \in F(x_1)$ для некоторого $x_1 \in S$ и $y \in F(x_2)$ для некоторого $x_2 \in Q$. Но при $x_1 \neq x_2$ в силу инъективности множества $F(x_1)$ и $F(x_2)$ не пересекаются. А их пересечение содержит по крайней мере y. Значит, $x_1 = x_2 = x$, и $x \in S \cap Q$. А так как $y \in F(x)$, получаем, что $x \in F(S \cap Q)$. □

Определение 10. *Областью определения* соответствия $F : A \to B$ называется множество $\operatorname{Dom} F = F^{-1}(B)$. Иными словами, область определения — множество тех элементов A, которым соответствует хотя бы один элемент B.

Определение 11. *Областью значений* соответствия $F : A \to B$ называется множество $\operatorname{Ran} F = F(A)$. Иными словами, область определения — множество тех элементов B, которые соответствуют хотя бы одному элементу A.

Заметим, что соответствие сюръективно, если его область значений совпадает с B.

Определение 12. Пусть $F : A \to B$ — соответствие, а $S \subset A$. Тогда *сужением* соответствия F на C называется соответствие $F\big|_S : S \to B$, принимающее те же значения, что и F, т.е. $b \in F\big|_S(a) \Leftrightarrow b \in F(a)$ для $a \in S$. Само соответствие F по отношению к $F\big|_S$ называют *продолжением.*

Определение 13. Соответствие $F : A \to B$ называют частично определённой функцией, если $F\big|_{\operatorname{Dom} F}$ — отображение.

Иными словами, образ каждому элементу A либо вообще не соответствует элементов B, либо соответствует ровно один. В теории алгоритмов под функцией мы будем понимать именно частично определённую функцию.

Для частично определённых функций сужение и продолжение могут определять иначе: отображение $F\colon A \to B$ называют сужением отображения $G\colon A \to B$, если $\operatorname{Dom} F \subset \operatorname{Dom} G$ и $F(x) = G(x)$ при $x \in \operatorname{Dom} F$. Соответственно, G в этом случае называется продолжением F. Мы будем использовать такое определение в теории вычислимых функций.

3 Композиция соответствий

Определение 14. Пусть $F\colon A \to B$ и $G\colon B \to C$ — соответствия. Тогда их композицией $G \circ F$ называется соответствие $H\colon A \to C$, определённое правилом: $c \in H(a)$ тогда и только тогда, когда найдётся b, такое что одновременно $c \in G(b)$ и $b \in F(a)$.

Для отображений можно написать проще: $(G \circ F)(a) = G(F(a))$. Именно этой формулой объясняется порядок функций в записи: в композиции $G \circ F$ сначала применяется F, а потом G.

Композиция соответствий ассоциативна, т.е. для любых трёх соответствий $F\colon A \to B$, $G\colon B \to C$ и $K\colon C \to D$ выполнено $(K \circ G) \circ F = K \circ (G \circ F)$. (Равенство на соответствиях определяется как равенство подмножеств декартова произведения). Проверка этого проста, но занудна, и потому остаётся в качестве упражнения.

Композиция соответствий не обязательно коммутативна. Если $C \neq A$, то композиция $F \circ G$ попросту не определена. Если $C = A \neq B$, то композиция $F \circ G$ отображает B в B, а $G \circ F$ — A в A. И даже если $A = B = C$, то композиции в двух порядках всё равно могут не совпадать: например, если $F(x) = 2x$, а $G(x) = x^2$, то $G \circ F(x) = 4x^2$, а $F \circ G(x) = 2x^2$.

Определение 15. *Тождественным отображением* на множестве A называется отображение $\mathrm{id}_A\colon A \to A$, заданное формулой $\mathrm{id}_A(x) = x$.

Композиция ведёт себя похоже на умножение, а тождественное отображение исполняет роль единицы: для любого соответствия F выполнены равенства $F \circ \mathrm{id}_A = F$ и $\mathrm{id}_B \circ F = F$. Эти равенства также несложно проверить. Что касается операции, обратной к умножению, то тут всё несколько сложнее.

Определение 16. Пусть $F\colon A \to B$ — соответствие. *Обратным соответствием* называется соответствие $F^{-1}\colon B \to A$, определяемое правилом $a \in F^{-1}(b) \Leftrightarrow b \in F(a)$.

Хотя обратное соответствие можно определить для любого соответствия, условие $F^{-1} \circ F = \mathrm{id}_A$ выполнено только для инъективного и непустозначного соответствия. А условия $F^{-1} \circ F = \mathrm{id}_A$ и $F \circ F^{-1} = \mathrm{id}_B$ одновременно выполнены только для биекций. Зато для любых соответствий выполнено равенство $(G \circ F)^{-1} = F^{-1} \circ G^{-1}$.

Наконец, соответствия можно возводить в степень.

Определение 17. Пусть $F\colon A \to A$ — соответствие. Тогда возведение в степень определяется так: $F^0 = \mathrm{id}_A$, а для бо́льших n верно $F^{n+1} = F \circ F^n$.

Возведение соответствий в степень удовлетворяет равенствам: $F^n \circ F^k = F^{n+k}$ и $(F^n)^k = F^{nk}$. Однако из-за некоммутативности равенство $(F \circ G)^n = F^n \circ G^n$ в общем случае неверно.

4 Возведение множества в степень

Если множество A состоит из n элементов, а множество B — из k элементов, то существует всего k^n различных отображений из A в B: действительно, есть по k вариантов значения для каждого из n элементов A. Это мотивирует следующее определение:

Определение 18. Пусть A и B — два множества. Тогда множеством B^A называется множество всех отображений из A в B.

Если B состоит всего из двух элементов (обозначим их b_1 и b_2), то отображение из A в B задаёт разбиение A на два множества: прообраз b_1 и прообраз b_2. Ясно, что для определения отображения достаточно задать прообраз b_1, ведь тогда прообраз b_2 определится автоматически. Таким образом, отображения из A в двухэлементное множество и подмножества A находятся в естественном взаимно однозначном соответствии между собой. Это мотивирует обозначение в следующем определении:

Определение 19. *Булеаном* множества A называется множество всех подмножеств множества A. Обозначение: $\mathcal{P}(A)$ или 2^A.

При помощи булеана можно сформулировать ешё одну естественную эквивалентность: каждому соответствию A и B соответствует отображение из A в 2^B. Действительно, каждому элементу можно однозначно сопоставить его образ при соответствии.

Закончим лекцию свойствами возведения в степень:

Утверждение 20. *При всех A, B и C выполнены следующие свойства:*

a) $(A \times B)^C \sim A^C \times B^C$;

b) $A^{B \cup C} \sim A^B \times A^C$ *(если B и C не пересекаются);*

c) $(A^B)^C \sim A^{B \times C}$,

где знак $\sim$ понимается как «элементы двух множеств могут быть естественным образом отождествлены».

Доказательство. Слова «естественным образом» определены нечётко. Формально нужно построить взаимно однозначное соответствие, которое будет в некотором смысле «естественным».

Первая эквивалентность неформально означает, что пара функций это то же самое, что одна функция, принимающая значение среди пар. Формально пусть $F \in (A \times B)^C$. Это значит, что $F\colon C \to A \times B$. То есть каждому элементу $c \in C$ сопоставлена некоторая пара $(a, b) \in A \times B$. Вместо этого ему можно сопоставить отдельно элементы $a \in A$ и $b \in B$. Получится два отображения, первое отображает c в a, а второе — c в b, то есть пара отображений $(F_1, F_2) \in A^C \times B^C$. Легко понять, что разные F переводятся в разные пары (F_1, F_2), и каждая пара получается из некоторой функции. Таким образом, первая эквивалентность установлена.

Вторая эквивалентность означает, что определить функцию на несвязном объединении двух множеств это то же самое, что определить её на каждом из этих множеств по отдельности.

Третья эквивалентность означает, что функция двух аргументов есть то же самое, что отображение первого аргумента в функцию, зависящую от второго аргумента.

Формальное доказательство этих эквивалентностей остаётся в качестве упражнения.

$\square$