kaspersky.academy

Комбинаторика

Лекция 2. Комбинаторика

Математика в кибербезопасности

Лекция 2. Комбинаторика

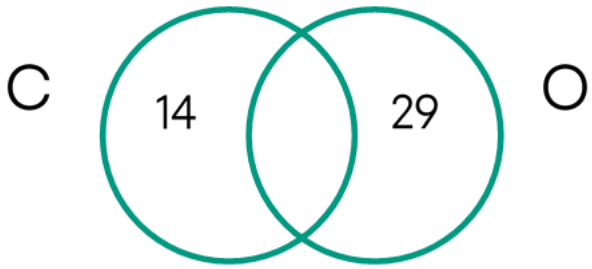
Формула включения-исключения множеств

Видео 1, 0:50

Мы знаем, что существуют разные множества. Одна из важных характеристик множества – его мощность. **Мощность множества –** это количество элементов, входящих в множество.

Кстати, множества могут быть бесконечными!

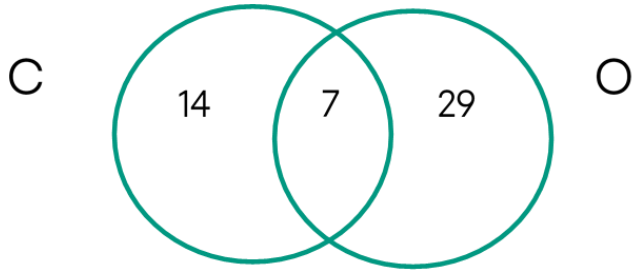
Но нас интересуют вполне конкретные множества – будем считать бравых парней из отряда Джона Сноу и Одичалых, которые по каким-то неведомым причинам присоединились к ним. Пусть в множество C – отряд Сноу – входит 14 человек. А множество O – одичалые – состоит из 29 человек.



C – отряд Сноу, $|C| = 14$
O – одичалые, $|O| = 29$

Некоторые из одичалых входят в множество отряда Сноу – то есть, множества O и C пересекаются, и это пересечение непусто.

$$|C \cap O| = 7$$



А как нам посчитать **общее количество воинов** – и одичалых, и парней Сноу? Просто сложить мощности С и О нельзя – дважды посчитаем тех, кто входит и в первое, и во второе множество. А значит, один раз это «лишнее» пересечение нужно вычесть.

$$|С \cup О| = |С| + |О| - |С \cap О| = 14 + 29 - 7 = 36$$

Вуаля, всего воинов 36!

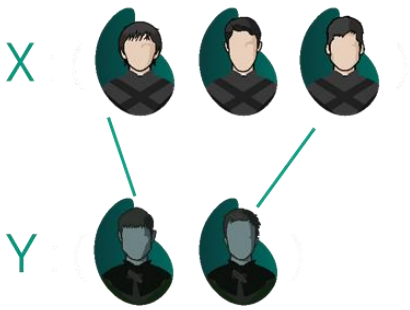
И вот еще одна формула включения-исключения для **трех** множеств:

$$|С \cup Б \cup О| = |С| + |Б| + |О| - |С \cap О| - |С \cap Б| - |О \cap Б| + |С \cap Б \cap О|$$

Множества и отображения

Видео 1, 4:40

Множества можно не только объединять и пересекать, но еще можно отображать элементы одного множества в элементы другого.



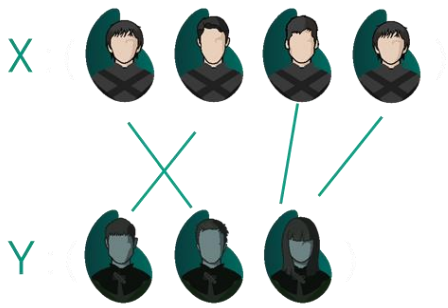
$$\forall x \in X \; \exists! \, y \in Y: y = f(x)$$

Читать: для любого x из множества X найдется такой единственный y из множества Y, что y можно получить из x, применяя функцию f. Эта функция будет являться правилом отображения множества X во множество Y.
Помните: каждый x должен хоть куда-нибудь отобразиться!

Есть три вида отображений. Мы начнем с сюръективного.

Сюръективное отображение

Видео 1, 5:25
Если множество X – бравые парни из отряда Сноу, а Y – злобные вихты, которые непрошенно пришли в Черный Замок, то нам нужно построить отображение так, чтобы каждый вихт был пойман кем-то из воинов.



Одного вихта можно ловить вдвоем, но каждый вихт должен быть пойман!

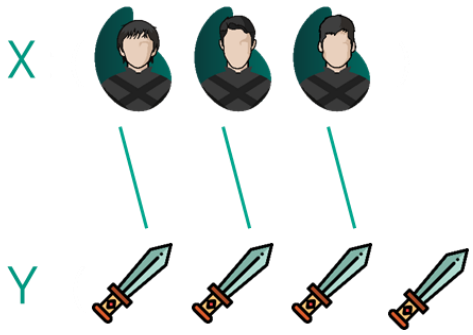
$$\forall y \in Y \; \exists \, x \in X : y = f(x)$$

Читать: для любого y из множества Y найдется хотя бы один x из X и этот y можно получить из x, применяя функцию f.

Инъективное отображение

Видео 2, 0:00

Множество X – воины Черного Замка, а Y – мечи. Все воины должны быть вооружены.



Но если воин берет меч, то только один.

$$\forall x_1, x_2 \in X : x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

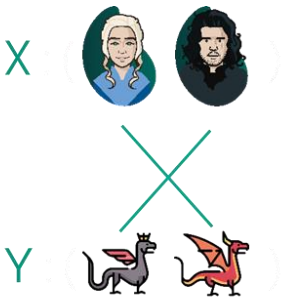
Читать: любые два разные элемента x_1, x_2 из множества X функция f будет переводить в разные элементы из множества Y.

Другими словами, если в y отображается какой-то x, то этот x единственный.

Биективное отображение

Видео 2, 1:00

Джон Сноу и Дейнерис решили полетать на драконах. Их двое, и драконов – тоже двое.



Тогда множество людей будет отображаться в множество драконов однозначно, или биективно.

Когда отображение может быть биективным:

1. $|X| = |Y|$

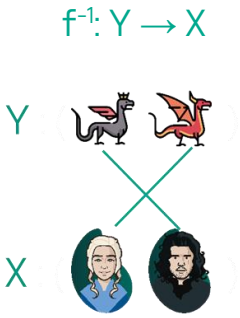
2. Отображение сюръективное и инъективное (в каждый элемент из множества Y отображается какой-то x, и этот x – единственный).

Обратное отображение

Видео 2, 2:00

А можно по известным y из Y восстановить неизвестные x из X? Можно! Но только если отображение было биективным ☺

Отображение множества Y в множество X называется обратным.



kaspersky.academy

Односторонние функции

Видео 2, 3:12

Что нужно знать про отображения и обратные отображения:

- $f(x)$ вычисляется легко
- $f^{-1}(x)$ вычисляется сложно

В алхимической лаборатории стояли две пробирки. Кто-то решил поэкспериментировать и смешать их содержимое. Этот человек отобразил жидкости из бутылок в колбу – это было прямое отображение. Но когда он спохватился и захотел вернуть жидкости в их пробирки, он понял, что это трудная – а может, и невыполнимая – задача!

Смешать зелья легко, разделить обратно – сложно.

А вот пример из математики.

- f – перемножение чисел
- f^{-1} – разложение на множители

Перемножать числа легко, а для разложения на множители нет эффективных алгоритмов. Самое лучшее, что придумало человечество, - это переборные алгоритмы. Не верите? А попробуйте разложить на множители число 6 938 077.

...и наш мир не настолько к вам жесток, поэтому мы покажем вам правильный ответ:
6 938 077 = 2801 * 2477

Как-то так и работают односторонние функции!