kaspersky.academy

Алгебра логики

Лекция 1. Высказывания и логические операции

Математика в кибербезопасности

Лекция 1. Высказывания и логические операции

Буль и алгебра логики

Видео 1, 1:15

Как формализовать человеческий язык и перевести его в язык математики? Этой задачей занимался Аристотель.

Аристотель пишет фразы:

Все финики есть фрукты.
Этот объект есть финик.
Значит, этот объект есть фрукт.

Аристотель кодирует каждую фразу математической переменной x:

- Объект есть финик = x_1
- Каждый финик есть фрукт = x_2
- Глагол «есть» - это знак равенства «=».

Аристотель пишет для своих предложений математическое выражение:

$$f = x_1 \cdot x_2$$

Значение функции f покажет, является ли данный объект фруктом:

«Этот объект есть фрукт, если:
он есть финик И все финики есть фрукты.»

Высказывания

Видео 1, 1:54

Высказывания – это утверждения, которые могут быть истинными или ложными.

$$B = \{\text{Ложь, Истина}\}$$

Высказываниями могут быть только утвердительные выражения

Примеры:

Высказывания:

- Вода кипит при 100°C – истина
- Земля стоит на 3 китах – ложь

Не высказывания:

- Сегодня отличная погода!

«Высказывания» в логике компьютера:

- 0 – ложь
- 1 – истина

Логические операции и булевы функции

Видео 1, 2:45

наборы
(записаны как
числа в 2-ой с/с)

	x_1	x_2	f
0	0	0	1
1	0	1	0
2	1	0	0
3	1	1	1

$f = 1\,0\,0\,1$

вектор значения
функции

$f = x_1 \circ x_2$

$\circ$ - какая-то операция

x_1, x_2 – булевы операнды

Логические операции над высказываниями

Видео 2, 0:00

Унарные (которые применяются к одному операнду):

- инверсия (отрицание)

Бинарные (применяются к двум операндам):

- дизъюнкция
- конъюнкция
- импликация
- строгая дизъюнкция
- эквиваленция

Инверсия

Видео 2, 0:26

Инверсия = отрицание. Инверсия меняет значение операнда на противоположное. Обозначение: $\overline{x}$

$$\overline{0} = 1$$
$$\overline{1} = 0$$

Дизъюнкция (логическое сложение)

Видео 2, 0:58

Дизъюнкция истинна, если истинен хотя бы один операнд

$f = x_1 + x_2$

x_1, x_2 – операнды (предикаты), f – функция

Обозначения:

$f = x_1 + x_2$

$f = x_1 \vee x_2$

$f = x_1 \| x_2$

$f = x_1 \text{ OR } x_2$

	x_1	x_2	f
0	0	0	0
1	0	1	1
2	1	0	1
3	1	1	1

Конъюнкция (логическое умножение)

Видео 2, 2:23

Конъюнкция истинна, если верны все операнды

$$f = x_1 \cdot x_2$$

	x_1	x_2	f
0	0	0	0
1	0	1	0
2	1	0	0
3	1	1	1

Обозначения:
$f = x_1 \wedge x_2$
$f = x_1 \cdot x_2$
$f = x_1 \,\&\, x_2$
$f = x_1 \text{ AND } x_2$

Импликация

Видео 2, 2:58

Импликация ложна только тогда, когда из истины следует ложь

	x_1	x_2	f
0	0	0	1
1	0	1	1
2	1	0	0
3	1	1	1

Обозначения:
$f = x_1 \rightarrow x_2$

Строгая дизъюнкция (побитовое исключающее ИЛИ)

Видео 2, 3:40

Строгая дизъюнкция истинна, если ровно один операнд истинен

$$f = x_1 \oplus x_2$$

Строгая дизъюнкция – это сложение по mod 2 (остаток от деления на 2)

	x_1	x_2	f
0	0	0	0
1	0	1	1
2	1	0	1
3	1	1	0

Обозначения:

$f = x_1 \oplus x_2$

$f = x_1 \text{ XOR } x_2$

Эквиваленция (логическое равенство)

Видео 2, 4:32

Эквиваленция истинна, если значения операндов совпадают

$$f = x_1 \sim x_2$$

	x_1	x_2	f
0	0	0	1
1	0	1	0
2	1	0	0
3	1	1	1

Обозначения:

$f = x_1 \equiv x_2$

$f = x_1 \sim x_2$

Свойства логических операций

Видео 3, 0:00

1. Коммутативность
   $x \cdot y = y \cdot x$

2. Ассоциативность
   $(z \cdot y) \cdot x = (x \cdot y) \cdot z$

3. Дистрибутивность
   $x \cdot (y + z) = x \cdot y + x \cdot z$
   $x \cdot (y \oplus z) = x \cdot y \oplus x \cdot z$

4. Идемпотентность
   $x + x = x$
   $x \cdot x = x$

Иерархия функций

Видео 3, 0:58

$-$ инверсия
$\wedge$ – конъюнкция
$\vee$, $\oplus$ – дизъюнкция, строгая дизъюнкция
$\rightarrow$ – импликация
$\sim$ – эквиваленция

Построение вектора значений функции

Видео 3, 2:14

$$f = x \wedge y \sim \overline{z \vee y}$$

1. Определим кол-во строк.
   $2^3 = 8$ строк
2. Следуем иерархии операций:
   - сначала $z \vee y$,
   - затем $\overline{z \vee y}$,
   - и, наконец, $x \wedge y$
3. Считаем f

x	y	z	$z \vee y$	$\overline{z \vee y}$	$x \wedge y$	f
0	0	0	0	1	0	0
0	0	1	1	0	0	1
0	1	0	1	0	0	1
0	1	1	1	0	0	1
1	0	0	0	1	0	0
1	0	1	1	0	0	1
1	1	0	1	0	1	0
1	1	1	1	0	1	0