Дискретна математика

проф. д-р Тодорка Глушкова,
Катедра „Компютърни технологии", ФМИ

6

Булева алгебра

Съдържание

- Булева алгебра
- Предикатна логика
- Приложения

Булева алгебра

- Булевата алгебра (или алгебра на съжденията) е специална алгебрична структура, която съдържа логическите оператори И, ИЛИ, НЕ, както и множествените функции сечение, обединение, допълнение.
- Тя е дефинирана за първи път от британския математик Джордж Бул, с цел да се използват алгебрични методи в логиката. Булевата алгебра и булевите операции стоят в основата на информатиката, програмирането и функционирането на компютърните системи, тъй като компютрите са програмирани да извършват точно тези логически операции.

Булева алгебра

- Константите, с които се оперира в тази алгебра са 0 и 1
- Операторите се срещат често написани по различен начин, напр. И, ИЛИ, НЕ (англ. AND, OR, NOT); ∧, ∨, ¬;
- математиците често използват + за ИЛИ, · за И и черта над символа за НЕ.

Булева алгебра и съждителна логика

- Съждителната логика формално можем да представим в две стъпки:
  - **Синтаксис** – правила за изграждане на логически изрази (формули)
    - Формула – последователност от символи, които могат да се комбинират по определен начин
  - **Семантика** – снабдява изразите със значение
    - Определя как да бъдат интерпретирани символите в една логическа формула

Синтаксис

Дефиниция:

Множеството на логическите формули върху множеството на променливите $V = \{ A_1, A_2, \ldots \}$ се дефинира рекурсивно както следва:

- Булевите стойности 0 и 1 са формули
- Всяка променлива $A_1 \in V$ е формула
- Ако F и G са формули, тогава $(\neg F)$, $(F \wedge G)$, $(F \vee G)$, $(F \rightarrow G)$, $(F \leftrightarrow G)$, $(F \not\leftrightarrow G)$ също са формули

Синтаксис

Оператори:

- “¬": отрицание
- “∧ ": конюнкция (И-оператор)
- “∨ ": дизюнкциянюнкция (ИЛИ-оператор)
- “→ ": импликация
- “↔ ": еквивалентност
- “↮ ": антивалентност (XOR-оператор)

Формули

Атомарна формула F: Формула, която не може да бъде разлагана
В съждителната логика това е множеството на атомарните формули е идентично с множеството $V \cup \{ 0, 1 \}$

Съставна формула: Формула, която може да се разрага.
Съставните ѝ части означаваме като подформули
Използваме означението: $F \in G$, съответно $F \notin G$

Обобщения за формули:

$$\bigwedge_{i=1}^{n} F_i = F_1 \wedge \ldots \wedge F_n \qquad \bigvee_{i=1}^{n} F_i = F_1 \vee \ldots \vee F_n$$

Интерпретации

- Семантиката на формулите се определя посредством моделиращата релация $\models$
- За да можем да я дефинираме формално първо трябва да въведем понятието за интерпретация

Дефиниция:

Нека са дадени:
- F е логическа формула
- $A_1, \ldots, A_n$ променливи, съдържащи се във F

Всяка $I: \{ A_1, A_2, \ldots \} \rightarrow \{ 0, 1 \}$ се нарича интерпретация на F

Пример

$(\neg A \to \neg B) \wedge ((B \to A) \vee (A \to B))$

$A \to 0$
$B \to 0$

1

$(\neg 0 \to \neg 0) \wedge ((0 \to 0) \vee (0 \to 0))$ интерпретация

Пример

$(\neg A \to \neg B) \wedge ((B \to A) \vee (A \to B))$

$A \to 1$
$B \to 0$

2

$(\neg 1 \to \neg 0) \wedge ((0 \to 1) \vee (1 \to 0))$

интерпретация

Пример

$(\neg A \to \neg B) \wedge ((B \to A) \vee (A \to B))$

$A \to 0$
$B \to 1$

3

$(\neg 0 \to \neg 1) \wedge ((1 \to 0) \vee (0 \to 1))$

интерпретация

Пример

$(\neg A \to \neg B) \wedge ((B \to A) \vee (A \to B))$

4

$A \to 1$

$B \to 1$

$(\neg 1 \to \neg 1) \wedge ((1 \to 1) \vee (1 \to 1))$

интерпретация

Въпрос

Ако имаме формула с n на брой променливи, колко е броят на възможните интерпретации?

$\boxed{2^n}$

Семантика

Нека F и G са логически формули, а I - интерпретация.
Семантиката се задава посредством релацията c , дефинирана индуктивно върху изграждането на формулите както следва:

- I c 1
- I $\not\models$ 0
- I c A_i :$\Leftrightarrow$ I(A_i) = 1
- I c ($\neg$F) :$\Leftrightarrow$ I $\not\models$ F
- I c (F $\wedge$ G) :$\Leftrightarrow$ I c F и I c G
- I c (F $\vee$ G) :$\Leftrightarrow$ I c F или I c G
- I c (F $\rightarrow$ G) :$\Leftrightarrow$ I$\not\models$ F или I c G
- I c (F $\leftrightarrow$ G) :$\Leftrightarrow$ I c F тогава и само тогава, когато I c G
- I c (F $\not\leftrightarrow$ G) :$\Leftrightarrow$ I$\not\models$ (F $\leftrightarrow$ G)

Една интерпретация I за която I c F се нарича **модел** на F

Булеви функции

Всяка съждителна формула F с n променливи можем да разглеждаме като булева функция

$f^F: \{0,1\}^n \rightarrow \{0,1\}$, която за една интерпретация I приема стойност 1, само тогава, когато I е модел за F

Ако I присвоява на променливите $A_1, \ldots, A_n$ логическите стойности $b_1, \ldots, b_n$, тогава стойността на функцията

$$f^F(b_1, \ldots, b_n) = \begin{cases} 1, \text{ ако } I \models F \\ 0, \text{ ако } I \not\models F \end{cases}$$

Понеже дефиниционната област е дискретна, булевите функции могат да се представят като таблици

Таблици

Отрицание:

	A	¬A
0	0	1
1	1	0

Конюнкция:

	A	B	A ∧ B
0	0	0	0
1	0	1	0
2	1	0	0
3	1	1	1

Дизюнкция:

	A	B	A ∨ B
0	0	0	0
1	0	1	1
2	1	0	1
3	1	1	1

Импликация:

	A	B	A→B
0	0	0	1
1	0	1	1
2	1	0	0
3	1	1	1

Еквивалентност:

	A	B	A↔B
0	0	0	1
1	0	1	0
2	1	0	0
3	1	1	1

Антивалентност:

	A	B	A↮B
0	0	0	0
1	0	1	1
2	1	0	1
3	1	1	0

Пример 1

изпълнима

$$\underbrace{F_1 = \underbrace{\underbrace{(\neg A \lor B)}_{G_1} \land \underbrace{(\neg B \lor C)}_{G_2}}_{G_4} \land \underbrace{(\neg C \lor A)}_{G_3}}_{F_1}$$

1 Колко модела?

A	B	C	G_1	G_2	G_3	G_4	F_1
0	0	0	1	1	1	1	1
0	0	1	1	1	0	1	0
0	1	0	1	0	1	0	0
0	1	1	1	1	0	1	0
1	0	0	0	1	1	0	0
1	0	1	0	1	1	0	0
1	1	0	1	0	1	0	0
1	1	1	1	1	1	1	1

Пример 2

общовалидна

$$\underbrace{F_2 = (\underbrace{(\underbrace{(A\to B)}_{G_1} \wedge \underbrace{(B\to C)}_{G_2})}_{G_4} \to \underbrace{(A\to C)}_{G_3})}_{F_2}$$

1 Колко модела?

A	B	C	G_1	G_2	G_3	G_4	F_2
0	0	0	1	1	1	1	1
0	0	1	1	1	1	1	1
0	1	0	1	0	1	0	1
0	1	1	1	1	1	1	1
1	0	0	0	1	0	0	1
1	0	1	0	1	1	0	1
1	1	0	1	0	0	0	1
1	1	1	1	1	1	1	1

Пример 3

неизпълнима

$$F_3 = \underbrace{\underbrace{\underbrace{(A \nleftrightarrow B)}_{G_1} \land \underbrace{(A \nleftrightarrow C)}_{G_2}}_{G_4} \land \underbrace{(B \nleftrightarrow C)}_{G_3}}_{F_3}$$

1 Колко модела?

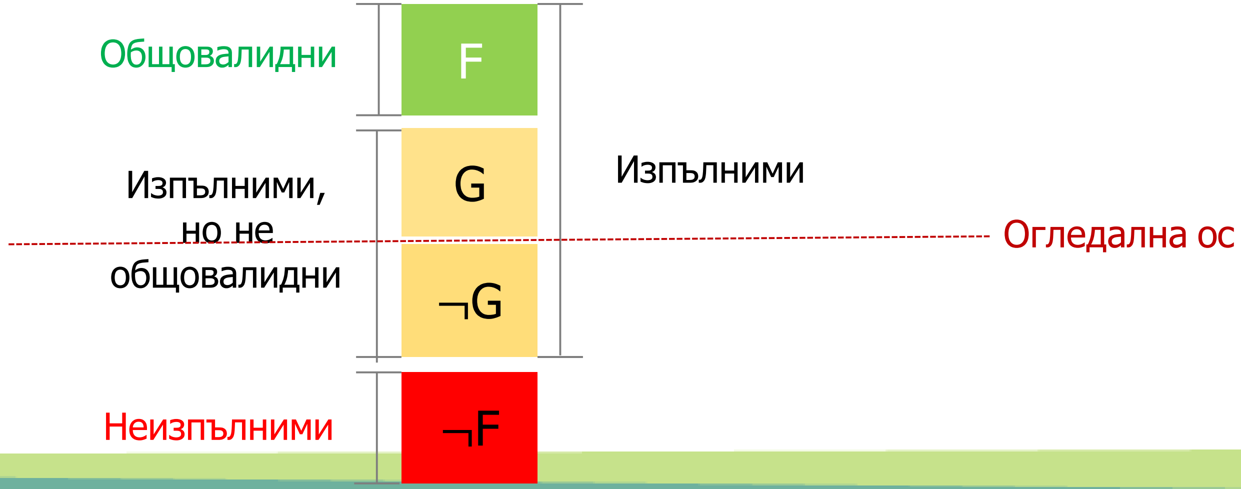
A	B	C	G_1	G_2	G_3	G_4	F_3
0	0	0	0	0	0	0	0
0	0	1	0	1	1	0	0
0	1	0	1	0	1	0	0
0	1	1	1	1	0	1	0
1	0	0	1	1	0	1	0
1	0	1	1	0	1	0	0
1	1	0	0	1	1	0	0
1	1	1	0	0	0	0	0

Видове формули

Една логическа формула F се нарича:

- Изпълнима – ако F притежава поне един модел
- Неизпълнима – ако F не притежава модел
- Общовалидна – ако ¬F е неизпълнима

Всяка общовалидна формула означаваме също като тавтология



За множества от формули

Дефиниции:

Тези три дефиниции могат да бъдат обобщени за множества от формули:

- Изпълнимо – когато съществува интерпретация I, която е модел за всяка $F_i \in M$.
  - Внимание: моделът за всички формули трябва да бъде еднакъв. Не е достатъчно всяка формула сама за себе си да бъде изпълнима.
- Неизпълнимо– когато F1, …,Fn нямат общ модел
- Общовалидно – обратното, ако всяка интерпретация е модел за елементите от M

Логически следствия

Дефиниции:

Нека M ≔ { F_1, …, F_n } е множество от логически формули.
Записваме, M c G („от M следва G“), когато всеки модел на M е също модел на G.

Означаваме:

- c G, за ∅ c G
- F c G, за { F } c G

Освен това:

- c G е в сила, когато G е общовалидна
- F c G е в сила, когато F → G е общовалидна
- { F_1, …, F_n } c G е еквивалентна на { F_2, …, F_n } c F_1 → G

Еквивалентност

Нека F и G са логически формули.
Релацията $\equiv$ е дефинирана както следва:

- $F \equiv G :\Leftrightarrow F$ c G и G c F

Две формули F и G с $F \equiv G$ се наричат еквивалентни

Еквивалентност

Две формули F и G са еквивалентни, когато имат едни и същи модели. От математическа гледна точка “$\equiv$” е релация на еквивалентност върху множеството на съждителните формули, като притежава следните свойства:

- Рефлексивност: за всички формули F е в сила $F \equiv F$
- Симетричност: от $F \equiv G$ следва $G \equiv F$
- Транзитивност: от $F \equiv G$ и $G \equiv H$ следва $F \equiv H$

Освен това:

- F е само тогава общовалидна, когато $F \equiv 1$
- F е само тогава неизпълнима, когато $F \equiv 0$

Важни еквивалентности

идемпотентност	неутралност	Де Морган
$F \wedge F \equiv F$ $F \vee F \equiv F$	$F \wedge 1 \equiv F$ $F \vee 0 \equiv F$	$\neg(F \wedge G) \equiv \neg F \vee \neg G$ $\neg(F \vee G) \equiv \neg F \wedge \neg G$

комутативност	елиминация	Двойно отрицание
$F \wedge G \equiv G \wedge F$ $F \vee G \equiv G \vee F$	$F \wedge 0 \equiv 0$ $F \vee 1 \equiv 1$	$\neg\neg F \equiv F$

дистрибутивност	абсорбация
$F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$ $F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$	$F \vee (F \wedge G) \equiv F$ $F \wedge (F \vee G) \equiv F$

Пълна система от логически оператори

- Може би предизвиква учудване, че в таблицата се съдържат само съждителните елементарни оператори ¬, ∧ и ∨
- Не става въпрос за ограничение

?

Всички останали могат да се свеждат до тези три.
Множеството на тези три оператора се нарича пълна система от оператори

Примери

$$x \to y \equiv \neg x \lor y$$

$$x \leftrightarrow y \equiv (\neg x \land \neg y) \lor (x \land y)$$

$$\equiv (\neg x \lor y) \land (x \lor \neg y)$$

$$x \nleftrightarrow y \equiv (\neg x \land y) \lor (x \land \neg y)$$

$$\equiv (\neg x \lor \neg y) \land (x \lor y)$$

Предикатна логика

- Съществуват някои недостатъци на съждителното смятане, свързани с това, че:
  - съждителната логика изразява само логическата структура на сентенциите.
  - С нея не могат да се изразят твърдения като: "Релацията < е транзитивна" или "Всяко естествено число е равно на сумата от квадратите на 4 естествени числа."

Предикатна логика

- Логически изводи, при които такива структури имат значение, не могат да се изразят със съждителната логика. Затова се налага да разгледаме предикатната логика.

Пример:

Всички гълъби са птици: $\forall x\,(Sx \rightarrow Mx)$

Всички птици са животни: $\forall x(Mx \rightarrow Fx)$

$\Rightarrow$ Всички гълъби са животни: $\forall x\,(Sx \rightarrow Fx)$

Пример

1. Сократ е човек
2. Всички хора са смъртни
3. Тогава Сократ също е смъртен

- Свойството да бъде човек е параметризирано съждение: Човек(x)
- Което в зависимост от аргумента е вярно или грешно: за индивида „x = Сократ“ съждението е вярно
- Едно атомарно съждение, стойността на което се определя от един или повече участващи индивиди, се нарича предикат
- Второто съждение дава квантитативно твърдение за индивиди
- В терминологията на логиката може да се представи: „за всички x е в сила: ако Човек(x) е вярно съждение, тогава Смъртен(x) е също вярно съждение“

Предикатна логика

- Предикатната логика е разширение на съждителната логика със следното:
  - Многоместни предикати
  - Възможности за формулиране на квантифицирани съждения
- Нарича се предикатна логика от първа степен

1. Човек(Сократ)
2. ∀x (Човек(x) → Смъртен(x))
3. c Смъртен(Сократ)

Предикатна логика

- ***Логически квантори:*** За да изразим съждение като предходното, въвеждаме **квантовите променливи.**
- Ясно е, че едно твърдение със свободни променливи не е нито вярно, нито невярно, докато свободните променливи не получат стойности.
- ***Например:*** "Ако x $\neq$0, то x.y =1".

Ако x=2; y=1/2, твърдението е вярно.

Ако x=2;y=3, твърдението не е вярно.

- **Заб.** Когато правим тези замествания, винаги имаме предвид конкретна област на стойностите. Например: x,y – реални числа; а не x-марсианец, а y – Мики Маус.

Предикатна логика

- ***Квантор за съществуване***

  Как да изразим в математиката съществуването на нещо?

- Нека P е твърдение и нека съществуването на x означим с $\exists x$. Тогава

  $\exists x$:P е твърдението:

  ”Съществува една x, такава че P”. Променливата x е квантова променлива.

Предикатна логика

- Твърдението $\exists x$:P е вярно, ако P е вярно за поне една стойност на x, избрана от нейната област (домейн).
- Символът $\exists$ е квантор за съществуване.

- ***<u>Пример</u>***: Нека P : $x^2 + 3x + 2 = 0$, x-свободна променлива.

Верността на P зависи от стойността на x:

- ако x=2, то P е F;
- ако x=-2, то P е T.

Областта на стойностите на x е Z.

<u>Като запис: $\exists x : x^2 + 3x + 2 = 0$.</u>

Предикатна логика

- ***Универсален квантор.*** -В много математически твърдения като:

“ За всяко $x \neq 0$, съществува y: $x.y=1$” се твърди, че за всяка стойност на свободната променлива x твърдението P е в сила.

- ***Дефиниция:*** Нека P е твърдение със свободна променлива x. Тогава $\forall$ x:P е твърдение, което се чете: “За всяко x – P”

Предикатна логика

- Променливата x е свързана във $\forall$ x:P, като $\forall$ x:P е вярно, ако P е вярно за всяка стойност на x от нейната област.
- **“$\forall$” е универсален квантор.**
- Вече можем да запишем и пълното твърдение:

$\forall$ x:(x $\neq$0 $\rightarrow$ $\exists$y:xy=1)

или $\forall$ x $\neq$0, $\exists$y:xy=1

Предикатна логика

Определяне верностните стойности на квантифицираните твърдения:

1) За да докажем, че ∀ x:P е вярно, трябва да го докажем за всички стойности на x.
2) За да докажем, че ∀ x:P е грешно, е достатъчно да докажем, че поне за една стойност на x е невярно.
3) За да докажем, че ∃x:P е вярно, е достатъчно да намерим само един случай за x, в който твърдението да е вярно.
4) За да докажем, че ∃x:P е грешно, е достатъчно да докажем, че не ∃x, така, че P да е вярно или, че P е грешно за ∀ x.

Предикатна логика

- **Проблем:** Ако е дадено едно квантифицирано съждение, може ли и неговото отрицание да запишем като квантифицирано съждение?

Отговор: Да!

ТЕОРЕМА 1: Нека P е твърдение. Тогава

$\neg(\forall x:P) \Leftrightarrow \exists x:\neg P;$

$\neg(\exists x:P) \Leftrightarrow \forall x:\neg P;$

Използвана литература в курса

- D. W. Hoffmann, Theoretische Informatik, Hansen Verlag, 2009
- H. P. Gumm, M. Sommer, Einfuehrung in die Informatik, Oldenbourg Wissenschaftsverlag, 2004
- J. W. Grossman, Discrete Mathematics, Macmillan Pub. Co., 1990
- К. Манев, Увод в дискретната математика, КЛМН, 2005
- Й. Денев, Р. Павлов, Я. Демирович. Дискретна математика. Наука и изкуство, София, 1984.

Използвана литература в курса

- Д. Байнов, С. Костадинов, Р. Павлов, Л. Луканова. Ръководство за решаване на задачи по дискретна математика. Университетско издателство “Паисий Хилендарски”, Пловдив, 1990.
- В.А. Успенский, Машина Поста, Москва, Наука, 1988, ISBN 5-02-013735-9.
- L. Lovasz, J. Pelikan, K. Vesztergombi, Discrete Mathematics – Elementary and Beyond, Springer Verlag, New York, 2003, ISBN 0-387-95584-4.

Използвана литература в курса

- E. Bender, S. Williamson, A Short Course in Discrete Mathematics, Dover, 2006, ISBN 0-486-43946-1.
- P. Linz, An Introduction to Formal Languages and Automata, Jones and Bartlett Publishers, 6-th edition, Jones & Bartlett Publishers, ISBN-13: 9781284077247, 2016
- Kenneth H. Rosen, Kamala Krithivasan, Discrete mathematics and its application, McGraw-Hill Companies, 7-th edition, ISBN 978-0-07-338309-5, 2012

Използвана литература в курса

- Owen D. Byer, Deirdre L. Smeltzer, Kenneth L. Wantz, Journey into Discrete Mathematics, AMS, MAA Press, Providence Rhode Island, ISBN 9781470446963, 2018
- Christopher Rhoades, Introductory Discrete Mathematics, Willford Press, ISBN 1682854922, 9781682854921, 2018
- David Liben-Nowell, Discrete Mathematics for Computer Science, Wiley, 2017, ISBN 1119397197, 9781119397199, 2017.
- ***http://www.jflap.org/*** - софтуерна среда