ДИСКРЕТНЕ СТРУКТУРЕ 1

предавање 12 (19.12.2022.)
Тема: **Ојлерова функција. Булове алгебре.**

Александра Костић

Катедра за алгебру и математичку логику
Математички факултет, Београд

Ојлерова функција

Дефиниција

Нека је $n > 1$ природан број. Са $\varphi(n)$ означавамо број природних бројева m тако да $1 \leq m < n$ и нзд$(m, n) = 1$. Функција φ се назива **Ојлерова функција**.

Ојлерова функција

Дефиниција

Нека је $n > 1$ природан број. Са $\varphi(n)$ означавамо број природних бројева m тако да $1 \leq m < n$ и нзд$(m, n) = 1$. Функција φ се назива **Ојлерова функција**.

Тврђење

Нека су $m, n > 1$ природни бројеви такви да је нзд$(m, n) = 1$. Тада је $\varphi(mn) = \varphi(m)\varphi(n)$.

Доказ: на часу.

Ојлерова функција

Дефиниција

Нека је $n > 1$ природан број. Са $\varphi(n)$ означавамо број природних бројева m тако да $1 \leq m < n$ и нзд$(m, n) = 1$. Функција φ се назива **Ојлерова функција**.

Тврђење

Нека су $m, n > 1$ природни бројеви такви да је нзд$(m, n) = 1$. Тада је $\varphi(mn) = \varphi(m)\varphi(n)$.

Доказ: на часу.

Последица: Ако је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, онда је $\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$.

Ојлерова функција

Дефиниција

Нека је $n > 1$ природан број. Са $\varphi(n)$ означавамо број природних бројева m тако да $1 \leq m < n$ и нзд$(m, n) = 1$. Функција φ се назива **Ојлерова функција**.

Тврђење

Нека су $m, n > 1$ природни бројеви такви да је нзд$(m, n) = 1$. Тада је $\varphi(mn) = \varphi(m)\varphi(n)$.

Доказ: на часу.

Последица: Ако је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, онда је $\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$.

Нека је $n > 1$ природни број. Скуп $\{r_1, \ldots, r_n\}$ природних бројева је **потпуни систем остатака по модулу** n ако је сваки цео број конгуентан по модулу n тачно једном од бројева r_i.
Можемо приметити да је r_i није конгруентно по модулу n броју r_j, за $i \neq j$. Један пример за потпуни систем остатака по модулу n је $\{0, 1, 2, \ldots, n-1\}$.

Ојлерова функција

Дефиниција

Нека је $n > 1$ природан број. Са $\varphi(n)$ означавамо број природних бројева m тако да $1 \leq m < n$ и нзд$(m, n) = 1$. Функција φ се назива **Ојлерова функција**.

Тврђење

Нека су $m, n > 1$ природни бројеви такви да је нзд$(m, n) = 1$. Тада је $\varphi(mn) = \varphi(m)\varphi(n)$.

Доказ: на часу.

Последица: Ако је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, онда је $\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$.

Нека је $n > 1$ природни број. Скуп $\{r_1, \ldots, r_n\}$ природних бројева је **потпуни систем остатака по модулу** n ако је сваки цео број конгуентан по модулу n тачно једном од бројева r_i.
Можемо приметити да је r_i није конгруентно по модулу n броју r_j, за $i \neq j$. Један пример за потпуни систем остатака по модулу n је $\{0, 1, 2, \ldots, n-1\}$.

Ојлерова теорема

(Ојлерова теорема) Нека су a и n позитивни природни бројеви, такви да нзд$(a, n) = 1$. Тада важи $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Доказ: на часу.

Булове алгебре

Увео их је Џорџ Бул средином 19. века.

Булове алгебре

Увео их је Џорџ Бул средином 19. века.

Дефиниција

Алгебарска структура $\mathbf{B} = (B, \curlyvee, \curlywedge, ', 0, 1)$, где је $B \neq \emptyset$, $0, 1 \in B$, $\curlyvee$ и $\curlywedge$ су бинарне а $'$ је унарна операција на скупу B, је **Булова алгебра** уколико су задовољене следеће аксиоме:

A1: $x \curlyvee y = y \curlyvee x$,

A2: $x \curlywedge y = y \curlywedge x$,

A3: $x \curlyvee (y \curlywedge z) = (x \curlyvee y) \curlywedge (x \curlyvee z)$,

A4: $x \curlywedge (y \curlyvee z) = (x \curlywedge y) \curlyvee (x \curlywedge z)$,

A5: $x \curlyvee 0 = x$,

A6: $x \curlywedge 1 = x$,

A7: $x \curlyvee x' = 1$,

A8: $x \curlywedge x' = 0$,

A9: $0 \neq 1$.

за свако $x, y, z \in B$.

Булове алгебре

Увео их је Џорџ Бул средином 19. века.

Дефиниција

Алгебарска структура $\mathbf{B} = (B, \curlyvee, \curlywedge, ', 0, 1)$, где је $B \neq \emptyset$, $0, 1 \in B$, $\curlyvee$ и $\curlywedge$ су бинарне а $'$ је унарна операција на скупу B, је **Булова алгебра** уколико су задовољене следеће аксиоме:

A1: $x \curlyvee y = y \curlyvee x$,

A2: $x \curlywedge y = y \curlywedge x$,

A3: $x \curlyvee (y \curlywedge z) = (x \curlyvee y) \curlywedge (x \curlyvee z)$,

A4: $x \curlywedge (y \curlyvee z) = (x \curlywedge y) \curlyvee (x \curlywedge z)$,

A5: $x \curlyvee 0 = x$,

A6: $x \curlywedge 1 = x$,

A7: $x \curlyvee x' = 1$,

A8: $x \curlywedge x' = 0$,

A9: $0 \neq 1$.

за свако $x, y, z \in B$.

Операције $\curlyvee$, $\curlywedge$ и $'$ редом називамо буловска дисјункција, буловска конјункција и буловски комплемент. Када је у неком контексту јасно да се ради о буловским операцијама тада их краће називамо конјункција, дисјункција и комплемент. Скуп B називамо домен. Уколико је скуп B коначан, тада је кажемо да је Булова алгебра $\mathbb{B}$ коначна, иначе кажемо да је бесконачна.

Булове алгебре

Увео их је Џорџ Бул средином 19. века.

Дефиниција

Алгебарска структура $\mathbf{B} = (B, \curlyvee, \curlywedge, ', 0, 1)$, где је $B \neq \emptyset$, $0, 1 \in B$, $\curlyvee$ и $\curlywedge$ су бинарне а $'$ је унарна операција на скупу B, је **Булова алгебра** уколико су задовољене следеће аксиоме:

A1: $x \curlyvee y = y \curlyvee x$,

A2: $x \curlywedge y = y \curlywedge x$,

A3: $x \curlyvee (y \curlywedge z) = (x \curlyvee y) \curlywedge (x \curlyvee z)$,

A4: $x \curlywedge (y \curlyvee z) = (x \curlywedge y) \curlyvee (x \curlywedge z)$,

A5: $x \curlyvee 0 = x$,

A6: $x \curlywedge 1 = x$,

A7: $x \curlyvee x' = 1$,

A8: $x \curlywedge x' = 0$,

A9: $0 \neq 1$.

за свако $x, y, z \in B$.

Операције $\curlyvee$, $\curlywedge$ и $'$ редом називамо буловска дисјункција, буловска конјункција и буловски комплемент. Када је у неком контексту јасно да се ради о буловским операцијама тада их краће називамо конјункција, дисјункција и комплемент. Скуп B називамо домен. Уколико је скуп B коначан, тада је кажемо да је Булова алгебра $\mathbb{B}$ коначна, иначе кажемо да је бесконачна.

Примери Булових алгебри

Пример 1: (Прекидачка алгебра) Алгебарска структура $\mathbf{2} = (\{0,1\}, \vee, \wedge, \neg, 0, 1)$, где су операције $\vee$, $\wedge$ и $\neg$ дефинисане на следећи начин:

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

$\neg$	
0	1
1	0

је Булова алгебра. Овако дефинисане операције су, у ствари, логичка дисјункција ($\vee$), логичка конјункција ($\wedge$) и негација ($\neg$).

Примери Булових алгебри

Пример 1: (Прекидачка алгебра) Алгебарска структура $\mathbf{2} = (\{0, 1\}, \vee, \wedge, \neg, 0, 1)$, где су операције $\vee$, $\wedge$ и $\neg$ дефинисане на следећи начин:

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

$\neg$	
0	1
1	0

је Булова алгебра. Овако дефинисане операције су, у ствари, логичка дисјункција ($\vee$), логичка конјункција ($\wedge$) и негација ($\neg$).

Пример 2: (Алгебра партитивног скупа) Нека је X произвољан непразан скуп и $\mathscr{P}(X)$ партитивни скуп скупа X. Скуп $\mathscr{P}(X)$ заједно са операцијама уније, пресека и скуповног комплементирања (у односу на скуп X) и истакнутим елементима $\emptyset$ и X чини Булову алгебру $\boldsymbol{\mathscr{P}(X)} = (\mathscr{P}(X), \cup, \cap, ^c, \emptyset, X)$. Ако $A, B, C \in \mathscr{P}(X)$, једнакости Булове алгебре

A1: $A \cup B = B \cup A$,

A2: $A \cap B = B \cap A$,

A3: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$,

A4: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,

A5: $A \cup \emptyset = A$,

A6: $A \cap X = A$,

A7: $A \cup A^c = X$,

A8: $A \cap A^c = \emptyset$,

A9: $X \neq \emptyset$.

су познати скуповни идентитети.

Принцип дуалности

Идентитети F_1 и F_2 су **дуални** ако се идентитет F_2 може добити од идентитета F_1 тако што се свако појављивање операције $\curlyvee$ замени са $\curlywedge$, свако појављивање операције $\curlywedge$ замени са $\curlyvee$, свако појављивање 0 замени са 1 и свако појављивање 1 замени са 0.

Пример: Идентитети $(x \curlyvee y) \curlywedge y' = x$ и $(x \curlywedge y) \curlyvee y' = x$ су дуални идентитети, као и идентитети $(x \curlywedge 0) \curlywedge (1 \curlyvee x) = x' \curlyvee 0$ и $(x \curlyvee 1) \curlyvee (0 \curlywedge x) = x' \curlywedge 1$.

Принцип дуалности

Идентитети F_1 и F_2 су **дуални** ако се идентитет F_2 може добити од идентитета F_1 тако што се свако појављивање операције $\curlyvee$ замени са $\curlywedge$, свако појављивање операције $\curlywedge$ замени са $\curlyvee$, свако појављивање 0 замени са 1 и свако појављивање 1 замени са 0.

Пример: Идентитети $(x \curlyvee y) \curlywedge y' = x$ и $(x \curlywedge y) \curlyvee y' = x$ су дуални идентитети, као и идентитети $(x \curlywedge 0) \curlywedge (1 \curlyvee x) = x' \curlyvee 0$ и $(x \curlyvee 1) \curlyvee (0 \curlywedge x) = x' \curlywedge 1$.

Нека је $\phi(\curlyvee, \curlywedge, ', 0, 1)$ произвољан Булов исказ. Тада је $\phi(\curlyvee, \curlywedge, ', 0, 1)$ теорема акко је $\phi(\curlywedge, \curlyvee, ', 1, 0)$ теорема. Аксиоме су дуалне и принцип дуалности је директна последица тога.

Принцип дуалности

Идентитети F_1 и F_2 су **дуални** ако се идентитет F_2 може добити од идентитета F_1 тако што се свако појављивање операције $\curlyvee$ замени са $\curlywedge$, свако појављивање операције $\curlywedge$ замени са $\curlyvee$, свако појављивање 0 замени са 1 и свако појављивање 1 замени са 0.

Пример: Идентитети $(x \curlyvee y) \curlywedge y' = x$ и $(x \curlywedge y) \curlyvee y' = x$ су дуални идентитети, као и идентитети $(x \curlywedge 0) \curlywedge (1 \curlyvee x) = x' \curlyvee 0$ и $(x \curlyvee 1) \curlyvee (0 \curlywedge x) = x' \curlywedge 1$.

Нека је $\phi(\curlyvee, \curlywedge, ', 0, 1)$ произвољан Булов исказ. Тада је $\phi(\curlyvee, \curlywedge, ', 0, 1)$ теорема акко је $\phi(\curlywedge, \curlyvee, ', 1, 0)$ теорема. Аксиоме су дуалне и принцип дуалности је директна последица тога.

Тврђење (основни закони Булових алгебри)

У произвољној Буловој алгебри $\mathbf{B} = (B, \curlyvee, \curlywedge, ', 0, 1)$ за све $x, y, z \in B$ важе следећи идентитети:

1. $0' = 1$, $1' = 0$;
2. $x \curlyvee x = x$, $x \curlywedge x = x$ (*закон идемпотеције*);
3. $x \curlyvee (x \curlywedge y) = x$, $x \curlywedge (x \curlyvee y) = x$ (*закон апсорпције*);
4. Ако је $x \curlyvee y = 1$ и $x \curlywedge y = 0$, тада је $x = y'$. (*јединственост комплемента*)
5. $(x')' = x$ (закон инволуције);
6. $x \curlyvee (y \curlyvee z) = (x \curlyvee y) \curlyvee z$, $x \curlywedge (y \curlywedge z) = (x \curlywedge y) \curlywedge z$ (*закон асоцијативности*);
7. $(x \curlywedge y)' = x' \curlyvee y'$, $(x \curlyvee y)' = x' \curlywedge y'$ (*Де Морганови закони*).