Fundamentelele limbajelor de programare
CURS 1

Traian Florin Șerbănuță și Andrei Sipoș

Facultatea de Matematică și Informatică, DL Info, Anul II

Semestrul II, 2023/2024

Preliminarii matematice

Mulțimi

Obiectele matematice despre care vom vorbi la acest curs vor fi formalizate în teoria mulțimilor: așadar, cum se întâmplă în general în acest caz, orice obiect cu care lucrăm va fi o mulțime.

Vom presupune oarecum cunoscut modul uzual de a lucra cu mulțimi și de aceea vom parcurge acum sumar doar eventualele puncte care pot părea mai subtile.

Vom încerca să justificăm cât mai multe fapte, dar, pentru demonstrații complete și riguroase, facem din nou trimitere la cursul „Logică matematică”, disponibil la adresa:

`https://cs.unibuc.ro/~asipos/lm/`

Operații pe mulțimi

Conform axiomelor teoriei mulțimilor, următoarele operații sunt bine definite:

$$x \cap y := \{z \in x \mid z \in y\}$$

$$x \setminus y := \{z \in x \mid z \notin y\}$$

$$\bigcup F := \{z \mid \text{există } y \in F \text{ cu } z \in y\}$$

$$x \cup y := \bigcup \{x, y\}$$

$$F \neq \emptyset \Rightarrow \bigcap F := \left\{z \in \bigcup F \mid \text{pentru orice } x \text{ cu } x \in F, \text{ avem } z \in x\right\}$$

$$\mathcal{P}(x) := \{z \mid z \subseteq x\}$$

Mulțimi Moore

Definiție

Fie X o mulțime. Numim o mulțime $A \subseteq \mathcal{P}(X)$ **mulțime Moore** pe X dacă $X \in A$, iar, pentru orice $B \subseteq A$ nevidă, avem $\bigcap B \in A$.

Teoremă

Fie X o mulțime și A o mulțime Moore pe X. Atunci există și este unic $C \in A$, numit **minimul** lui A, astfel încât pentru orice $D \in A$, avem $C \subseteq D$.

Demonstrație

Unicitatea rezultă imediat: dacă avem C_1, $C_2 \in A$ cu acea proprietate, atunci $C_1 \subseteq C_2$ și $C_2 \subseteq C_1$, deci $C_1 = C_2$. Pentru existență, cum $X \in A$, avem $A \neq \emptyset$, deci $\bigcap A \in A$. Luăm $C := \bigcap A$ și verificăm că are proprietatea căutată.

Perechi ordonate

În matematică, se folosește deseori noțiunea de **pereche ordonată** a lui x și y, notată cu (x, y). Cum am spus, în universul nostru de discurs există doar mulțimi, deci trebuie și ca (x, y) să fie tot o mulțime. Ea trebuie să „codifice" ideea de pereche ordonată, adică pentru orice x, y să existe (x, y), iar aceasta să poată fi distinsă de (y, x), când $x \neq y$, sau în general de vreun (a, b) cu $a \neq x$ sau $b \neq y$. Nu va conta ce definiție alegem, atât timp cât va avea proprietățile dorite și o vom folosi în mod consecvent.

Definiția cea mai frecvent folosită este cea dată de Kazimierz Kuratowski în 1921: $(x, y) := \{\{x\}, \{x, y\}\}$. Putem apoi verifica:

Proprietatea perechilor ordonate

Fie x, y, u, v cu $(x, y) = (u, v)$. Atunci $x = u$ și $y = v$.

Produsul cartezian

Propoziție

Fie x, y, X, Y cu $x \in X$ și $y \in Y$. Atunci $(x, y) \in \mathcal{P}(\mathcal{P}(X \cup Y))$.

Demonstrație

Trebuie să arătăm că pentru orice $z \in (x, y)$, avem $z \in \mathcal{P}(X \cup Y)$. Fie $z \in (x, y)$. Atunci trebuie să arătăm că pentru orice $t \in z$, $t \in X \cup Y$, adică $t \in X$ sau $t \in Y$. Fie $t \in z$. Cum $(x, y) = \{\{x\}, \{x, y\}\}$, avem $z = \{x\}$ sau $z = \{x, y\}$. Cum $t \in z$, avem $t = x$ sau $t = y$. Deci $t \in X$ sau $t \in Y$.

Ca urmare, pentru orice X și Y, mulțimea definită prin

$$X \times Y := \{w \in \mathcal{P}(\mathcal{P}(X \cup Y)) \mid \text{există } x \in X \text{ și } y \in Y \text{ cu } w = (x, y)\}$$

conține toate perechile ordonate de elemente din X cu elemente din Y. O numim **produsul cartezian** al lui X și Y.

Relații binare

Propoziție-Definiție

Fie R o mulțime. Următoarele afirmații sunt echivalente:

- există A și B astfel încât $R \subseteq A \times B$;
- elementele lui R sunt perechi ordonate, adică pentru orice $z \in R$ există x, y cu $z = (x, y)$.

În acest caz, R se numește **relație (binară)**, iar dacă A și B sunt ca mai sus, spunem că R este o relație **între** A și B. Dacă A este astfel încât R este între A și A, spunem că R este o relație **pe** A.

Demonstrație

Implicația „$\Rightarrow$" este evidentă. Pentru implicația „$\Leftarrow$", notăm mulțimea $\bigcup\bigcup R$ atât cu A, cât și cu B. Fie $z \in R$. Atunci există x, y cu $z = \{\{x\}, \{x, y\}\} \in R$. Așadar, $\{x\}$, $\{x, y\} \in \bigcup R$ și deci x, $y \in \bigcup\bigcup R$. Ca urmare, $(x, y) \in \bigcup\bigcup R \times \bigcup\bigcup R = A \times B$.

Observăm și că A și B **nu sunt unice** cu acea proprietate! De exemplu, $\emptyset$ este o relație pe $\emptyset$, dar și pe $\{\emptyset\}$.

Definiție

Dacă A este o mulțime, notăm cu Δ_A și denumim **relația diagonală** pe A acea relație pe A definită prin

$$\{p \in A \times A \mid \text{există } a \text{ cu } p = (a, a)\}.$$

Definiție

Fie A, B mulțimi și R o relație între A și B. Spunem că R este **grafic** între A și B dacă pentru orice $a \in A$ există și este unic $b \in B$ astfel încât $(a, b) \in R$.

Definiție

Fie A, B mulțimi. Spunem că f este **funcție între A și B** (și notăm acest fapt cu $f : A \to B$) dacă există R, un grafic între A și B, astfel încât $f = (A, B, R)$. A se numește **domeniul** lui f, B **codomeniul** lui f, iar R **graficul** lui f. Pentru orice $a \in A$ vom nota cu $f(a)$ acel unic $b \in B$ cu $(a, b) \in R$.

Detalii de codificare

Un grafic și o funcție sunt mulțimi, dar ele nu sunt aceeași mulțime! Avem nevoie de includerea codomeniului în „codificarea” noțiunii de funcție pentru a putea mai târziu formaliza corect surjectivitatea.

Propoziție

Fie R o relație binară. Următoarele afirmații sunt echivalente:

- există A și B astfel încât R este grafic între A și B;
- pentru orice x, y, z cu (x, y), $(x, z) \in R$, avem $y = z$.

Propoziție

Fie R o relație binară și A, B, C, D astfel încât R este grafic atât între A și B, cât și între C și D. Atunci $A = C$.

Aceste două propoziții (lăsate ca exercițiu) ne arată că domeniul unei funcții este complet determinat de grafic (și îl putem numi **domeniul graficului**), ca urmare el ar fi putut să nu fie inclus în modul de definiție. El este inclus, totuși, prin tradiție.

Notații despre funcții

Pentru orice mulțime A, avem că (A, A, Δ_A) este funcție. O numim **funcția identică pe** A sau **funcția identitate pe** A și o notăm cu id_A.

Observăm că dacă A, B sunt mulțimi, iar $f : A \to B$, atunci $f \in (\{A\} \times \{B\}) \times \mathcal{P}(A \times B)$, ca urmare putem defini mulțimea tuturor funcțiilor de la A la B, notată cu B^A, prin

$$\{f \in (\{A\} \times \{B\}) \times \mathcal{P}(A \times B) \mid f \text{ funcție}\}.$$

Imagini

Definiție

Fie A, B și $f : A \to B$. Fie $X \subseteq A$ și $Y \subseteq B$. Atunci:

- notăm cu $f_*(X)$ și numim **imaginea directă** a lui X prin f mulțimea
$$\{y \in B \mid \text{există } x \in X \text{ cu } f(x) = y\};$$
- notăm cu $f^*(Y)$ și numim **imaginea inversă** a lui Y prin f mulțimea
$$\{x \in A \mid f(x) \in Y\};$$
- notăm cu $\mathrm{Im} f$ și numim **imaginea** lui f mulțimea $f_*(A)$.

Mai definim **imaginea** unui grafic ca fiind imaginea unei funcții care îl are ca grafic. Știm din cele anterioare că există o asemenea funcție și putem arăta că imaginea nu depinde de funcția aleasă.

Definiție

Fie A, B și $f : A \to B$. Spunem că:

- f este **injectivă** sau **injecție** dacă pentru orice $x, y \in A$ cu $x \neq y$, avem $f(x) \neq f(y)$;
- f este **surjectivă** sau **surjecție** dacă $\mathrm{Im} f = B$, mai exact dacă pentru orice $y \in B$ există $x \in A$ cu $f(x) = y$;
- f este **bijectivă** sau **bijecție** dacă este injectivă și surjectivă.

Compunerea și restricția funcțiilor

Definiție

Fie A, B, C și $f : A \to B$, $g : B \to C$. Definim funcția $g \circ f : A \to C$ (citim „g compus cu f"; ea se notează uneori cu $f; g$, caz în care citim „f succedat de g"), pentru orice $x \in A$, prin

$$(g \circ f)(x) := g(f(x)).$$

Proprietăți elementare

Fie A, B, C, D și $f : A \to B$, $g : B \to C$, $h : C \to D$. Atunci:

- $(h \circ g) \circ f = h \circ (g \circ f)$;
- $f \circ \mathrm{id}_A = f$; $\mathrm{id}_B \circ f = f$.

Definiție

Fie A, B, $f : A \to B$ și $X \subseteq A$. Definim funcția $f_{|X} : X \to B$ (citim „f restricționat la X"), pentru orice $x \in X$, prin $f_{|X}(x) := f(x)$.

Funcții inversabile

Definiție

Fie A, B, $f : A \to B$. Dacă $g : B \to A$, $g \circ f = \mathrm{id}_A$ și $f \circ g = \mathrm{id}_B$, spunem că f este **inversabilă** iar g este **inversa** sa.

O inversă, dacă există, este unică. Mai exact, dacă avem A, B, $f : A \to B$, iar g_1, $g_2 : B \to A$ sunt inverse ale lui f, atunci $g_1 = g_2$, iar aceasta se poate demonstra doar folosind proprietățile elementare ale compunerii:

$$g_1 = g_1 \circ \mathrm{id}_B = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = \mathrm{id}_A \circ g_2 = g_2.$$

Următorul rezultat se demonstrează ușor:

Propoziție

O funcție este inversabilă dacă și numai dacă este bijectivă.

Comportamentul mulțimii vide față de funcții

Fie A o mulțime. Se pune întrebarea: există $f : \emptyset \to A$? Dacă da, cum arată? Presupunem că ar exista o asemenea f. Atunci există R cu $f = (\emptyset, A, R)$ și $R \subseteq \emptyset \times A = \emptyset$, deci $R = \emptyset$ și $f = (\emptyset, A, \emptyset)$. Aceasta este într-adevăr o funcție. Ca urmare, există o unică funcție de la $\emptyset$ la A, anume $(\emptyset, A, \emptyset)$, pe care o numim **funcția vidă a lui** A. Așadar, avem că $A^{\emptyset} = A^0$ este un singleton (o mulțime cu un singur element). Spunem că $\emptyset$ este **mulțimea inițială**.

Dar invers? Există o funcție $g : A \to \emptyset$? Dacă A este nevidă, atunci există $a \in A$, și deci $g(a) \in \emptyset$, o contradicție, dat fiind că nu există $b \in \emptyset$. Ca urmare, funcția există doar când $A = \emptyset$, și atunci $g = (\emptyset, \emptyset, \emptyset)$ (caz particular al celui din paragraful precedent).

Comportamentul singleton-urilor față de funcții

Fixăm X un singleton (repetăm, o mulțime cu un singur element) – de exemplu, putem lua $X := 1 = \{\emptyset\}$, dar alegerea precisă a lui X nu va conta.

Fie A o mulțime. Atunci există o unică funcție de la A la X, anume cea care duce orice element din A în unicul element al lui X. De aceea, spunem că orice singleton este **mulțime terminală** (noțiune **duală** celei de mulțime inițială).

Vrem acum, invers, să găsim toate funcțiile de la X la A. Pentru a găsi o asemenea funcție, trebuie doar să selectăm elementul din A în care va fi dus acel unic element al lui X. Așadar, funcțiile de la X la A sunt în corespondență biunivocă cu elementele lui A. Deseori, în acest curs, vom **identifica tacit** A^X cu A (indiferent care este precis singleton-ul X; de pildă, vom identifica A^1 cu A).

Familii

Fie I o mulțime. Numim **familie indexată după** I un grafic al cărui domeniu este I. Dacă F este o familie indexată după I, vom nota, pentru orice $i \in I$, acea unică mulțime x pentru care $(i, x) \in F$ cu F_i. De asemenea, vom mai scrie $(F_i)_{i \in I}$ în loc de F.

Definim **reuniunea** și **intersecția**, ca familie, ale lui F – notate cu $\bigcup_{i \in I} F_i$, respectiv cu $\bigcap_{i \in I} F_i$ – ca fiind reuniunea, respectiv intersecția (ultima doar în cazul în care $I \neq \emptyset$) a imaginii ca grafic a lui F.

Mai definim **produsul cartezian** al lui F, notat cu $\prod_{i \in I} F_i$, ca fiind mulțimea tuturor familiilor f indexate după I cu proprietatea că pentru orice $i \in I$, $f_i \in F_i$. Această mulțime există deoarece orice asemenea f este element al lui

$$\mathcal{P}\left(I \times \bigcup_{i \in I} F_i\right).$$

Tipuri de relații binare pe o mulțime

Definiție

Fie A o mulțime și R o relație pe A. Pentru orice x, $y \in A$, vom scrie xRy în loc de $(x, y) \in R$. Spunem că R este:

- **reflexivă** dacă pentru orice $x \in A$, xRx;
- **simetrică** dacă pentru orice x, $y \in A$ cu xRy, avem yRx;
- **tranzitivă** dacă pentru orice x, y, $z \in A$ cu xRy și yRz, avem xRz;
- **de echivalență** dacă este reflexivă, simetrică și tranzitivă;
- **totală** dacă pentru orice x, $y \in A$, avem xRy sau yRx;
- **antisimetrică** dacă pentru orice x, $y \in A$ cu xRy și yRx avem $x = y$;
- **de ordine parțială** (de obicei ele sunt notate cu $\leq$) dacă este reflexivă, antisimetrică și tranzitivă;
- **ireflexivă** dacă pentru orice $x \in A$, nu avem xRx;
- **asimetrică** dacă pentru orice x, $y \in A$ cu xRy, nu avem yRx.

Tipuri de date abstracte, inductive

Până acum s-a mai lucrat cu diverse formalizări ale unor tipuri de date inductive. De exemplu, în Haskell defineam asemenea tipuri cu o sintaxă specifică (cu constructori). De asemenea, la cursul „Logică matematică și computațională" s-au introdus, printre altele, formulele logicii propoziționale într-un mod inductiv, într-un fel care semăna cu următorul:

- orice variabilă este o formulă;
- dacă φ este formulă, atunci $\neg\varphi$ este formulă;
- dacă φ și ψ sunt formule, atunci $\varphi \to \psi$ este formulă;
- doar expresiile obținute prin aplicări ale acestor reguli sunt formule.

Dat fiind că vom lucra cu multe asemenea definiții în cadrul acestui curs, vom explora în continuare cum pot fi făcute riguroase raționamentele cu asemenea tipuri, pentru a nu mai intra în detalii la momentul respectiv.

Formule

Formulele sunt expresii peste mulțimea dată de simboluri (variabile și conectori, toate diferite), iar proprietățile pe care o mulțime A de expresii trebuie să le verifice pentru ca ea să fie mulțime de formule vor fi:

- $V \subseteq A$ (adică variabilele „sunt” formule);
- dacă $\varphi \in A$, atunci $\neg\varphi \in A$;
- dacă φ, $\psi \in A$, atunci $\rightarrow \varphi\psi \in A$.

Submulțimile mulțimii expresiilor care verifică aceste proprietăți formează o mulțime Moore. Așadar, putem lua minimul ei, pe care îl notăm cu $Form$. Numim elementele acestei mulțimi **formule** sau **enunțuri**.

Observăm că am folosit forma **prefixată** a formulelor pentru a le defini – am scris $\rightarrow \varphi\psi$ în loc de $\varphi \rightarrow \psi$ – deoarece ne va fi mai comod la unele demonstrații. În scurt timp, vom oferi un mod prin care vom putea folosi în discursul nostru forma obișnuită, i.e. **infixată**.

Principiul inducției pe formule

Următoarea teoremă reprezintă o formă de inducție **structurală** pe mulțimea formulelor.

Principiul inducției pe formule

Fie $B \subseteq Form$ astfel încât:

- $V \subseteq B$;
- dacă $\varphi \in B$, atunci $\neg\varphi \in B$;
- dacă $\varphi, \psi \in B$, atunci $\rightarrow \varphi\psi \in B$.

Atunci $B = Form$.

Enunțul rezultă imediat din faptul că B este una din mulțimile ce participă la intersecția prin care a fost definit $Form$.

Citirea formulelor

Proprietatea de citire

Fie $\chi \in Form$. Atunci se întâmplă exact una dintre următoarele alternative:

- $\chi \in V$;
- există $\varphi \in Form$ cu $\chi = \neg\varphi$;
- există φ, $\psi \in Form$ cu $\chi = \rightarrow \varphi\psi$.

Demonstrație

Notăm cu B mulțimea formulelor ce se pot scrie sub acele forme. Atunci, clar, B verifică condițiile Principiului de inducție și, deci, $B = Form$. Faptul că se întâmplă cel mult una dintre alternative rezultă din faptul că am fixat simbolurile ca fiind diferite.

Despre segmente inițiale

Lemă

Fie $\chi \in Form$. Atunci nu există $\alpha \in Form$ care să fie segment inițial strict al lui χ.

Demonstrație

Demonstrăm prin inducție, dar nu structurală, ci inducție completă pe numere după lungimea lui χ. Presupunem că există α ca în enunț. Din proprietatea de citire, distingem trei cazuri. Tratăm doar cazul când există φ, ψ cu $\chi = \rightarrow \varphi\psi$. Atunci, fie α este vid, ceea ce nu se poate, fie există φ', ψ' cu $\alpha = \rightarrow \varphi'\psi'$. Dacă φ și φ' ar avea lungimi diferite, atunci unul ar fi segment inițial strict al celuilalt, contradicție cu ipoteza de inducție. Așadar, $\varphi = \varphi'$ și deci ψ și ψ' au lungimi diferite, de unde rezultă din nou o contradicție cu ipoteza de inducție.

Citirea unică a formulelor

Proprietatea de citire unică

Fie φ, ψ, φ', $\psi' \in$ *Form* cu $\rightarrow \varphi\psi = \rightarrow \varphi'\psi'$. Atunci $\varphi = \varphi'$ și $\psi = \psi'$.

Demonstrație

Dacă φ și φ' ar avea lungimi diferite, atunci unul ar fi segment inițial strict al celuilalt, contradicție. Rezultă că φ și φ' au aceeași lungime. Dar de aici rezultă imediat concluzia dorită.

Scrierea infixată

Pentru a putea folosi, după cum am anunțat, o notație infixată, definim pe *Form* operația $\rightarrow$: *Form*$^2 \rightarrow$ *Form*, pentru orice φ, $\psi \in$ *Form*, prin

$$\varphi \rightarrow \psi := \rightarrow \varphi\psi.$$

Atenție: $\rightarrow$ reprezintă obiecte complet diferite în stânga și în dreapta respectivei ecuații – anume, în stânga este vorba de operația pe care o definim acum, iar în dreapta este vorba de simbolul fixat mai devreme. Ele sunt, însă, utilizate în contexte destul de asemănătoare cât să folosim același semn grafic.

Principiul recursiei pe formule

Principiul recursiei pe formule

Fie A o mulțime și $G_0 : V \to A$, $G_\neg : A \to A$, $G_\to : A^2 \to A$.
Atunci există și este unică $F : Form \to A$ astfel încât:

- pentru orice $v \in V$, $F(v) = G_0(v)$;
- pentru orice $\varphi \in Form$, $F(\neg\varphi) = G_\neg(F(\varphi))$;
- pentru orice $\varphi, \psi \in Form$, $F(\varphi \to \psi) = G_\to(F(\varphi), F(\psi))$.

Principiul recursiei pe formule

Demonstrație

Unicitatea rezultă imediat prin inducție structurală (exercițiu!). Pentru existență, vom construi $S \subseteq \mathit{Form} \times A$ astfel încât să verifice:

- pentru orice $v \in V$, $(v, G_0(v)) \in S$;
- pentru orice $\varphi \in \mathit{Form}$ și $a \in A$ cu $(\varphi, a) \in S$, avem $(\neg\varphi, G_\neg(a)) \in S$;
- pentru orice $\varphi, \psi \in \mathit{Form}$ și $a, b \in A$ cu $(\varphi, a) \in S$ și $(\psi, b) \in S$, avem $(\varphi \to \psi, G_\to(a, b)) \in S$,

și să fie cea mai mică cu aceste proprietăți – ca mai înainte, o construim luând intersecția, la care participă $\mathit{Form} \times A$, a tuturor submulțimilor ce verifică proprietățile.

Rămâne de arătat că S este grafic între Form și A – atunci, clar, $F := (\mathit{Form}, A, S)$ va fi funcția căutată.

Principiul recursiei pe formule

Demonstrație (cont.)

Trebuie să arătăm că, pentru orice $\varphi \in Form$, există și este unic $a \in A$ cu $(\varphi, a) \in S$. Existența rezultă prin inducție structurală (exercițiu!), astfel că vom demonstra în continuare unicitatea.

Fie B mulțimea acelor $\varphi \in Form$ cu proprietatea că există și este unic $a \in A$ cu $(\varphi, a) \in S$. Presupunem prin absurd că $B \neq Form$. Atunci, din contrapusa principiului de inducție pe formule, avem că fie $V \not\subseteq B$, fie există $\varphi_0 \in B$ cu $\neg\varphi_0 \notin B$, fie există φ_0, $\psi_0 \in B$ cu $\varphi_0 \to \psi_0 \notin B$. Ultimul caz este cel mai complex și de aceea îl vom demonstra doar pe acela, primele două rămânând ca exercițiu.

Presupunem, deci, că avem φ_0, $\psi_0 \in B$ cu $\varphi_0 \to \psi_0 \notin B$. Cum φ_0, $\psi_0 \in B$, există și sunt unice a_0, b_0 cu $(\varphi_0, a_0) \in S$ și $(\psi_0, b_0) \in S$, deci avem $(\varphi_0 \to \psi_0, G_\to(a_0, b_0)) \in S$. Cum $\varphi_0 \to \psi_0 \notin B$, există $q \neq G_\to(a_0, b_0)$ cu $(\varphi_0 \to \psi_0, q) \in S$.

Principiul recursiei pe formule

Demonstrație (cont.)

Iau $T := S \setminus \{(\varphi_0 \to \psi_0, q)\}$. Vom arăta că T verifică cele trei proprietăți, ceea ce va contrazice faptul că S este cea mai mică asemenea mulțime.

Fie $v \in V$. Atunci $(v, G_0(v)) \in S$, iar cum $(v, G_0(v)) \neq (\varphi_0 \to \psi_0, q)$, avem $(v, G_0(v)) \in T$. Cea de-a doua proprietate se arată analog.

Pentru a treia, fie $\varphi, \psi \in Form$ și $a, b \in A$ cu $(\varphi, a) \in T$ și $(\psi, b) \in T$. Vrem $(\varphi \to \psi, G_\to(a, b)) \in T$.

Cum $(\varphi, a) \in S$ și $(\psi, b) \in S$, avem $(\varphi \to \psi, G_\to(a, b)) \in S$. Dacă $(\varphi \to \psi, G_\to(a, b)) \notin T$, înseamnă că $(\varphi \to \psi, G_\to(a, b)) = (\varphi_0 \to \psi_0, q)$, deci $\varphi \to \psi = \varphi_0 \to \psi_0$ și $G_\to(a, b) = q$.

Demonstrație (cont.)

Cum $\varphi \to \psi = \varphi_0 \to \psi_0$, din Proprietatea de citire unică avem $\varphi = \varphi_0$ și $\psi = \psi_0$. Cum $\varphi = \varphi_0$, $(\varphi_0, a) = (\varphi, a) \in S$. Dar cum $(\varphi_0, a_0) \in S$ și $\varphi_0 \in B$, avem $a = a_0$. Analog, $b = b_0$. Deci $q = G_\to(a, b) = G_\to(a_0, b_0)$, contradicție cu presupunerea inițială $q \neq G_\to(a_0, b_0)$.

Demonstrația este acum încheiată.

Aplicație: mulțimea variabilelor

Corolar

Există și este unică $Var : Form \to \mathcal{P}(V)$ astfel încât:

- pentru orice $v \in V$, $Var(v) = \{v\}$;
- pentru orice $\varphi \in Form$, $Var(\neg\varphi) = Var(\varphi)$;
- pentru orice $\varphi, \psi \in Form$, $Var(\varphi \to \psi) = Var(\varphi) \cup Var(\psi)$.

De exemplu,
$Var(\neg v_0 \to v_1) = Var(\neg v_0) \cup Var(v_1) =$
$Var(v_0) \cup Var(v_1) = \{v_0\} \cup \{v_1\} = \{v_0, v_1\}$.