Logic for Computer Science

Summer semester
2019-2020

LECTURE 5: INTRODUCTION to FIRST-ORDER LOGIC

Lectures: LORENZO CLEMENTE
Tutorials: DARIA WALUKIEWICZ, JACEK CHRZASZCZ, JĘDRZEJ KOŁODZIEJSKI
Labs: DARIA, JACEK + PIOTR HOFMAN

MOTIVATING EXAMPLE

This is the equality that we all know (no cheating here)

$$1 + 1 = 2 \;?$$

Answer: It depends on the interpretation of symbols $1, 2, +$!

(semantics)

YES in the structure $(\mathbb{N}, 1, 2, +, =)$

$$[\![1+1]\!] = 2$$

Domain (universe)

NO in the structure $(\underset{\text{domain}}{\mathbb{N}}, 1, 2, \oplus, =)$

$$[\![1+1]\!] = 0$$

addition modulo 2

arity

Signature (syntax) $\Sigma = \{ 1 : 0,\ 2 : 0,\ + : 2,\ = : 2 \}$

function symbols

relation symbol

OTHER EXAMPLES of STRUCTURES

Signature $\Sigma = \{\underbrace{0:0,\ 1:\overset{\text{arity}}{0}}_{\text{constants (arity 0)}},\ \underbrace{+:2,\ \cdot:2}_{\text{functions (arity > 0)}}\}$

(equality "$=$" is always included)

Arithmetic $(\mathbb{N}, 0, 1, +, \cdot)$. Domain $\mathbb{N} = \{0, 1, 2, \ldots\}$.

Standard interpretation of $0, 1, +, \cdot$.

Signature $\Sigma = \{\top:0, \bot:0, \wedge:2, \vee:2, \neg:1\}$ function symbols

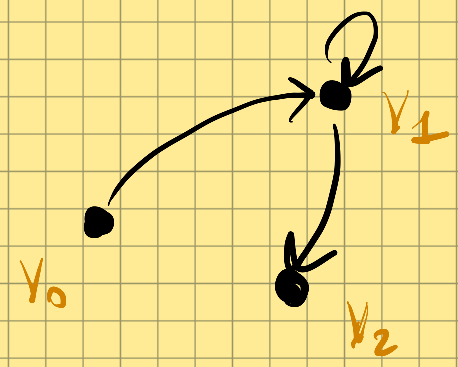
Propositional logic $(\mathbb{B}, \top, \bot, \wedge, \vee, \neg)$

Domain $\mathbb{B} = \{0, 1\}$. Interpretation (truth tables) $\neg = \begin{cases} 0 \mapsto 1 \\ 1 \mapsto 0 \end{cases}$

RELATIONAL STRUCTURES (GRAPHS & DATABASES)

↳ no function symbols (except constants)

Signature $\Sigma = \{E:2\}$. Graph $G = (V, E)$.



Domain : set of vertices $V = \{v_0, v_1, v_2\}$.

The interpretation of $E:2$ is the set of edges $E = \{(v_0,v_1), (v_1,v_1), (v_1,v_2)\}$

Relational database $(D, \text{Courses}, \text{Groups})$

relational signature $\Sigma = \{\underbrace{\text{Courses}:3, \text{Groups}:2}_{\text{relations}}, \text{grześ}:0, \underbrace{\text{LDI}:0, 3:0}_{\text{Constants}}, \dots\}$

Courses $= \{(\text{grześ}, \text{LDI}, 3), (\text{janusz}, \text{LDI}, 4), \dots\}$

Groups $= \{(3, \text{lorenzo}), (4, \text{jacek}), \dots\}$

$D = \{\text{grześ}, \text{LDI}, 4, \dots\}$

SIGNATURE (syntax)

STRUCTURE over Σ (semantics)

$$\Sigma = \Sigma^F \cup \Sigma^R$$

$$\mathcal{A} = (A, \underbrace{\dots}_{\text{interpretation}})$$

$$\Sigma^F = \Sigma^F_0 \cup \Sigma^F_1 \cup \dots,$$

CONSTANTS $\quad \Sigma^F_0 = \{c:0, d:0, \dots\} \xrightarrow{\text{interpretation}} c:0 \in \Sigma^F_0, \quad c \in A$

FUNCTIONS of arity i $\quad \Sigma^F_i = \{f:i, g:i, \dots\} \xrightarrow{\text{interpretation}} f:i \in \Sigma^F_i, \quad f : A^i \to A$

$\vdots$

$$\Sigma^R = \Sigma^R_1 \cup \Sigma^R_2 \cup \dots,$$

RELATIONS of arity i $\quad \Sigma^R_i = \{R:i, S:i, \dots\} \xrightarrow{\text{interpretation}} R:i \in \Sigma^R_i, \quad R \subseteq A^i$

TERMS (syntax) denote VALUES (semantics)

constant function

$$[\![1 + x]\!]_{\underbrace{x \mapsto 5}_{\text{valuation}}} = 6$$

free variable

valuation
(assigns values to variables)

Fix a structure $\mathcal{A} = (A, \cdots)$ and a valuation $\rho : Var \to A$.

first-order variables $\quad [\![x]\!]\rho = \rho(x)$

constants $\quad [\![c]\!]\rho = c$

functions $\quad [\![f(t_1, \ldots, t_k)]\!]\rho = f([\![t_1]\!]\rho, \ldots, [\![t_k]\!]\rho)$

FORMULAS denote T/F PROPERTIES

(syntax) (semantics)

Examples:

$$\mathbb{R}, y \mapsto 2 \models \exists x \cdot x * x = y$$

$$\mathbb{Q}, y \mapsto 2 \not\models \exists x \cdot x * x = y$$

$$\mathbb{A}, \rho \models t_0 = t_1 \iff [\![t_0]\!]\rho = [\![t_1]\!]\rho$$

$$\mathbb{A}, \rho \models R(t_1, \ldots, t_k) \iff ([\![t_1]\!]_\rho, \ldots, [\![t_k]\!]_\rho) \in R$$

$$\mathbb{A}, \rho \models \varphi_0 \wedge \varphi_1 \iff \mathbb{A}, \rho \models \varphi_0 \text{ and } \mathbb{A}, \rho \models \varphi_1$$

$$\mathbb{A}, \rho \models \exists x \cdot \varphi \iff \text{There is } a \in A : \mathbb{A}, \rho[x \mapsto a] \models \varphi$$

$$\mathbb{A}, \rho \models \forall x \cdot \varphi \iff \text{for all } a \in A : \mathbb{A}, \rho[x \mapsto a] \models \varphi$$

VALIDITY

$\models \varphi$ iff for every model $\mathcal{A}$ and valuation ρ, $\mathcal{A}, \rho \models \varphi$

$\models 1 + 1 = 2$? ✗

$\mathbb{N} \models 1 + 1 = 2$ ✓

SATISFIABILITY

$SAT(\varphi)$ iff there is a model $\mathcal{A}$ and a valuation ρ, $\mathcal{A}, \rho \models \varphi$

PROPERTIES DEFINABLE in FIRST-ORDER LOGIC

Signature $\Sigma = \{+, *, f:1\}$, $\mathbb{A} = (\mathbb{R}, +, *, f : \mathbb{R} \to \mathbb{R})$

unary function

Properties of structures: (closed formula: no free variables)

f is periodic $\iff \mathbb{A} \models \exists p \cdot \forall x \cdot f(x+p) = f(x)$

BOUND variable

Properties of elements in structures — free variables

$a \in \mathbb{R}$ is zero $\iff \mathbb{A}, x \mapsto a \models \varphi(\underline{x})$, where $\varphi(x) \equiv \underline{x} + x = x$

$a \in \mathbb{R}$ is strictly positive $\iff \mathbb{A}, x \mapsto a \models \exists y \cdot y * y = \underline{x}$

f is continuous at $a \in \mathbb{R}$ $\iff$ $\mathbb{A}, x \mapsto a \models$

$$\underbrace{\forall \varepsilon \cdot \varepsilon > 0 \to}_{\forall \varepsilon > 0 \cdot} \underbrace{\exists \delta \cdot \delta > 0 \wedge}_{\exists \delta > 0 \cdot} \forall y \cdot \underbrace{|y - x| \leq \delta}_{\dots} \to |f(y) - f(x)| \leq \varepsilon$$

syntactic sugaring

MODEL CHECKING FO in finite relational structures

(≈ query evaluation in DB, parsing in CFG, acceptance in NFA)

Solution: GAMES! = alternation

INPUT: closed φ in NNF and $\mathbb{A} = (A, R, S, \ldots)$.

OUTPUT: YES iff $\mathbb{A} \models \varphi$.

$$\left.\begin{array}{ll} \mathbb{A}, \rho \models x = y & \rightsquigarrow \text{check } \rho(x) = \rho(y) \\ \mathbb{A}, \rho \models R(x_1, \ldots, x_n) & \rightsquigarrow \text{check } R([\![x_1]\!]_\rho, \ldots, [\![x_n]\!]_\rho) \end{array}\right\} \text{PTIME}$$

$\mathbb{A}, \rho \models \varphi \lor \psi \rightsquigarrow$ check $\mathbb{A}, \rho \models \varphi$ OR $\mathbb{A}, \rho \models \psi$ — existential choice

$\mathbb{A}, \rho \models \varphi \land \psi \rightsquigarrow$ check $\mathbb{A}, \rho \models \varphi$ AND $\mathbb{A}, \rho \models \psi$ — universal choice

$\mathbb{A}, \rho \models \exists x \cdot \varphi \rightsquigarrow$ check $\mathbb{A}, \rho[x \mapsto a] \models \varphi$ for SOME $a \in \mathbb{A}$ — existential choice

$\mathbb{A}, \rho \models \forall x \cdot \varphi \rightsquigarrow$ check $\mathbb{A}, \rho[x \mapsto a] \models \varphi$ for ALL $a \in \mathbb{A}$ — universal choice

Depth: $|\varphi|$

Complexity: APTIME (Alternating) = PSPACE

MODEL CHECKING FO in <u>finite</u> relational structures

PSPACE-hardness : from QBF (also PSPACE-hard)

$\forall x_1 \exists x_2 \cdots (x_1 \wedge \neg x_2 \cdots) \cdots$ is a QBF tautology

iff

$$\mathbb{B} \models \forall x_1 \exists x_2 \cdots (T(x_1) \wedge \neg T(x_2) \wedge \cdots) \cdots$$

$$\mathbb{B} = (\{0,1\}, T, \wedge, \vee, \neg)$$

where $T = \{1\}$ unary relation (predicate)

PSPACE-hard already for the fixed structure $\mathbb{B}$!

DATA COMPLEXITY of FO MODEL CHECKING

Fix a formula φ of size $K = |\varphi|$.

INPUT: $\mathbb{A} = (A = \{a_1, \dots, a_n\}, R, S, \dots)$. OUTPUT: YES iff $\mathbb{A} \models \varphi$.

$\mathbb{A}, \rho \models x = y$	$\rightsquigarrow$ check $\rho(x) = \rho(y)$		linear time
$\mathbb{A}, \rho \models R(x_1, \dots, x_m)$	$\rightsquigarrow$ check $R([\![x_1]\!]_\rho, \dots, [\![x_m]\!]_\rho)$		
$\mathbb{A}, \rho \models \varphi \vee \psi$	$\rightsquigarrow$ check $\mathbb{A}, \rho \models \varphi$ OR $\mathbb{A}, \rho \models \psi$		existential choice
$\mathbb{A}, \rho \models \varphi \wedge \psi$	$\rightsquigarrow$ check $\mathbb{A}, \rho \models \varphi$ AND $\mathbb{A}, \rho \models \psi$		universal choice
$\mathbb{A}, \rho \models \exists x \cdot \varphi$	$\rightsquigarrow$ check $\mathbb{A}, \rho[x \mapsto a] \models \varphi$ for SOME $a \in A$		existential choice
$\mathbb{A}, \rho \models \forall x \cdot \varphi$	$\rightsquigarrow$ check $\mathbb{A}, \rho[x \mapsto a] \models \varphi$ for ALL $a \in A$		universal choice

Depth: K constant! Complexity: PTIME $O(n^K)$

Even in $AC_0 \subseteq NC_1 \subseteq LOGSPACE \subseteq PTIME$

MODEL CHECKING in AC_0

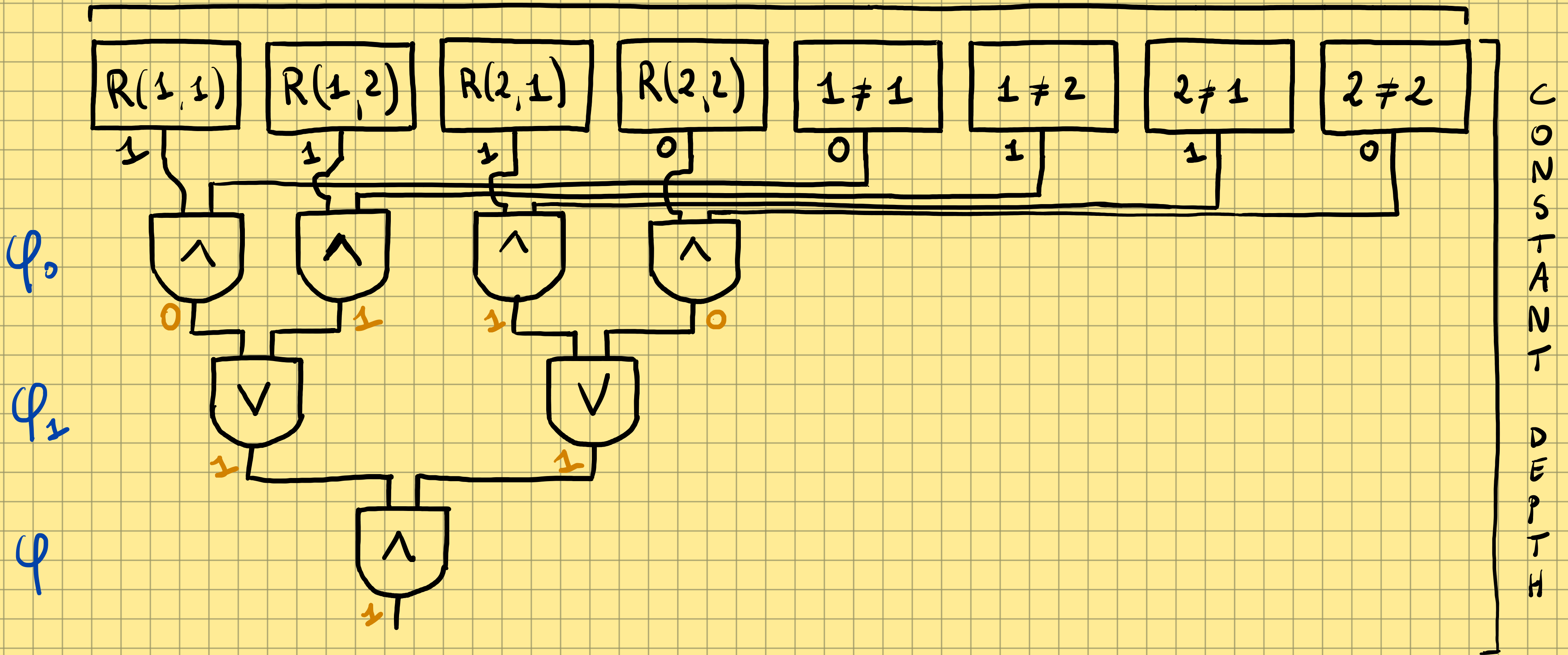
circuits of polynomial size, unbounded fan-in, constant depth

when φ fixed

$$\varphi \equiv \forall x_1 \cdot \overbrace{\exists x_2 \cdot \underbrace{R(x_1, x_2) \wedge x_1 \neq x_2}_{\varphi_0}}^{\varphi_1}$$

$\mathbb{A} = (A = \{1,2\}, R = \{(1,1),(1,2),(2,1)\})$

POLYNOMIAL SIZE $O(n^k)$, $n = |A|$, k = max arity



NORMAL FORMS for FIRST-ORDER LOGIC

NEGATION NORMAL FORM (NNF)

$\forall x \cdot R(x,y) \vee \neg \forall y \cdot P(y)$ ✗ $\iff$ $\forall x \cdot R(x,y) \vee \exists y \cdot \neg P(y)$ ✓

equivalent

PRENEX NORMAL FORM (PNF) – all quantifiers in front

$(\forall x \cdot P(x)) \vee (\exists x \cdot Q(x))$ ✗ $\iff$ $\forall x \cdot \exists y \cdot P(x) \vee Q(y)$ ✓

equivalent

SKOLEM NORMAL FORM (SNF) – closed universal PNF

$\forall x \cdot \exists y \cdot P(x) \vee Q(y)$ ✗ $\iff$ $\forall x \cdot P(x) \vee Q(\underbrace{f}_{\text{fresh function symbol}}(x))$ ✓

equisatisfiable

(The "CNF" of first-order logic)

SKOLEMISATION

HERBRAND MODELS

$\Sigma = \{ c:0,\ f:2,\ g:1,\ R:2 \}$

$\mathbb{H} = (U, c, f, g, R)$

$U = \{ c, g(c), f(c,c), f(g(c),c), \dots \}$ all constructible terms

$c = c$, $g = \{ (t, g(t)) \mid t \in U \}$, $f = \{ ((u,v), f(u,v)) \mid u, v \in U \}$

$$\boxed{\mathrm{SAT}(\underbrace{\forall \bar{x} . \varphi}_{\mathrm{SNF}}) \text{ iff } \exists \text{ Herbrand model } \mathbb{H} \models \forall \bar{x} . \varphi}$$

PROOF of HERBRAND'S THEOREM

$$\boxed{\mathrm{SAT}(\underbrace{\forall \bar{x}\cdot\varphi}_{\mathrm{SNF}}) \text{ iff } \exists \text{ Herbrand model } \mathbb{H} \models \forall \bar{x}\cdot\varphi}$$

Proof ($\Rightarrow$) Let $\mathbb{A} = (A, c, f, g, R)$. Take $R = \{(\overset{\text{ground terms}}{u, v}) \in U \times U \mid (\underbrace{[\![u]\!]}_{\in A}, \underbrace{[\![v]\!]}_{\in A}) \in R\}$

$$\boxed{\forall n : \mathbb{A} \models \forall x_n, \dots, x_1 \cdot \varphi \Rightarrow \mathbb{H} \models \forall x_n, \dots, x_1 \cdot \varphi}$$

$n = 0$: ✓. $n > 0$: Let r be an arbitrary term.

$$\mathbb{A}, x_n \mapsto [\![r]\!] \models \forall x_{n-1}, \dots, x_1 \cdot \varphi \Rightarrow \mathbb{A} \models \forall x_{n-1}, \dots, x_1 \cdot \varphi[x_n \mapsto r]$$

$$\overset{(\mathrm{HYP})}{\Longrightarrow} \mathbb{H} \models \forall x_{n-1}, \dots, x_1 \cdot \varphi[x_n \mapsto r]$$

$$\Rightarrow \mathbb{H}, x_n \mapsto r \models \forall x_{n-1}, \dots, x_1 \cdot \varphi .$$

r arbitrary & no other element in $U \Rightarrow \mathbb{H} \models \forall x_n, \dots, x_1 \cdot \varphi$ ✓

VALIDITY is SEMIDECIDABLE

$\models \varphi$ iff not $\mathrm{SAT}(\neg\varphi)$

iff not $\mathrm{SAT}(\forall \bar{x} \cdot \psi)$ ← SNF

ground formula (no variables)

($\Rightarrow$)

Semi algorithm $\left\{\begin{array}{l}\text{iff not } \mathrm{SAT}(\psi[\bar{x} \mapsto \bar{u}_1] \wedge \cdots \wedge \psi[\bar{x} \mapsto \bar{u}_m]) \\ \text{for some } n\text{-tuples of ground terms } \bar{u}_1, \ldots, \bar{u}_m \in \mathbb{U}^n.\end{array}\right.$

Proof of ($\Leftarrow$): if $\mathrm{SAT}(\forall \bar{x} \cdot \psi)$, by Herbrand's theorem $\mathbb{H} \models \forall \bar{x} \cdot \psi$.

Proof of ($\Rightarrow$): Assume not $\mathrm{SAT}(\forall \bar{x} \cdot \psi)$. Consider $\Gamma = \{\psi[\bar{x} \mapsto \bar{u}] \mid \bar{u} \in \mathbb{U}^n\}$.

By contradiction, assume $\forall \Delta \subseteq_{fin} \Gamma \cdot \mathrm{SAT}(\Delta)$.

By compactness for <u>PROPOSITIONAL LOGIC</u>, $\mathrm{SAT}(\Gamma)$: $\mathbb{A} \models \Gamma$.

By Herbrand's theorem, $\mathbb{H} \models \Gamma$ ← Herbrand's model! $\Rightarrow$ $\mathbb{H} \models \forall \bar{x} \cdot \psi$ ↯

FIRST-ORDER LOGIC = SQL without aggregation

on relational structures (no functions)

≈ relational DB

$\underbrace{\text{SQL without aggregation}}$

RELATIONAL ALGEBRA

$$\underset{\text{tuple of DB elements}}{E, F ::= (a_1, \dots, a_m)} \mid \underset{\text{relation (table)}}{R} \mid \underset{\text{union}}{E+F} \mid \underset{\text{difference}}{E-F} \mid \underset{\text{product}}{E \times F} \mid \underset{\text{selection}}{\sigma_{i=j}(E)} \mid \underset{\text{projection}}{\Pi_{i_1, \dots, i_k}(E)}$$

from RA to FO (by example)

$(\text{janusz}, \text{LD1}, 5) \longrightarrow x_1 = \text{janusz} \wedge x_2 = \text{LD1}, x_3 = 4$

$\text{Courses} \longrightarrow \text{Courses}(x_1, x_2, x_3)$

$E + F \longrightarrow \varphi_E(\bar{x}) \vee \varphi_F(\bar{x})$

$E \times F \longrightarrow \varphi_E(x_1, \dots, x_m) \wedge \varphi_F(x_{m+1}, \dots, x_{m+n})$

$\sigma_{2=3}(E) \longrightarrow x_2 = x_3 \wedge \varphi_E(x_1, x_2, x_3)$

$\Pi_{3,2}(E) \longrightarrow \exists y_1, y_2, y_3 \cdot \varphi_E(y_1, y_2, y_3) \wedge x_1 = y_3 \wedge x_2 = y_2$

FIRST-ORDER LOGIC = RELATIONAL ALGEBRA

from FO over $x_1, \dots, x_n$ to RA (by example)

Active domain $D = \pi_1(\text{Courses}) + \pi_2(\text{Courses}) + \dots$

$$= \sum_R \sum_i \pi_i(R)$$

$\pi_{3,2}(\sigma_{2=3}(R))$

$x_1 = x_3 \longrightarrow \sigma_{1=3}(\underbrace{D \times \dots \times D}_{n})$

$R(x_3, x_2, x_2) \longrightarrow$

$\varphi(\bar{x}) \vee \psi(\bar{x}) \longrightarrow E_\varphi + E_\psi$

$\neg \varphi(\bar{x}) \longrightarrow D^n - E_\varphi$

$\exists x_2 . \varphi(x_1, \dots, x_n) \longrightarrow \pi_{1,3,4,\dots,n} E_\varphi$