A természetes levezetés

Buday Gergely
Eszterházy Károly Egyetem
Gyöngyösi Károly Róbert Campus

2017. ősz

Bevezetés

A természetes levezetés egy grafikus kalkulus, ami azt akarja ábrázolni, hogy a matematikusok hogyan írnak le bizonyításokat. Matematikai szimbólummal az a kérdés, hogy

$$\Gamma \vdash A$$

igaz-e, vagyis a Γ formulahalmazból levezethető-e A. Ez a szintaktikai igazságfogalom. A másik igazságfogalom a szemantikai:

$$\Gamma \vDash A$$

Ekkor az a kérdés, hogy egy bizonyos modellben, modellek egy csoportjában, vagy minden modellben, ha a Γ formulahalmaz elemei igazak, akkor ugyanezekben a modellekben A kijelentés is igaz-e. Ez a szemantikai igazságfogalom a *modellelmélet* tárgya, míg a szintaktikai igazságfogalom a *bizonyításelmélet* vizsgálatainak a területe.

A szabályokról általában

A természetes levezetés levezetési szabályainak a formája a következő:

$$\frac{A \qquad B}{D}$$

A vízszintes vonal jelentése: levezethető. A vonal felett vannak a feltételek, vagy premisszák, a vonal alatt pedig a következtetés, avagy konklúzió. Felolvasva: ha az összes premissza teljesül, akkor a konklúzió is igaz. A fenti példában: ha A és B is teljesül, akkor D is igaz.

Kétfajta szabály van a természetes levezetésben: a bevezetési és a kivezetési szabályok. Angol *introduction rule* és *elimination rule*. A nevük jelentése: egy bevezetési szabályban egy új logikai szimbólum jelenik meg a konklúzióban, míg egy kivezetési szabályban a premissza fő logikai szimbóluma a konklúzióban már nem szerepel, eltűnik. Elsőnek nézzük az és művelet bevezetési szabályát:

$$\frac{A \qquad B}{A \wedge B}\ \wedge\mathrm{I}$$

A nagy I betű az *introduction* szóra utal, vagyis ez egy bevezetési szabály, a logikai és művelet bevezetési szabálya. A következő szabályban:

$$\frac{A \wedge B}{A}\ \wedge\mathrm{E1}$$

az E betű az *elimination* szóra utal, azaz kivezetési szabály, méghozzá a logikai és művelet kivezetési szabálya. Az 1-es szám arra utal, hogy a logikai és műveletnek *két* kivezetési szabálya van, amiből az elsőt láthatjuk.

Néha használjuk a függőleges pontokat a nem részletezett levezetés jelölésére:

$$\begin{array}{c} \vdots \\ \dfrac{A}{X} \end{array}$$

jelentése: *valahogyan* levezettük A-t, amiből következik X. Ennek a jelölésnek egy másik példája az, amikor egy *feltevést* — angolul *assumption* — használunk:

$$\begin{array}{c} [A] \\ \vdots \\ \dfrac{B}{X} \end{array}$$

Ekkor X-ben kioltjuk a feltevést, angolul ezt *discharging the assumption*-nak nevezzük.

A kijelentéslogika szabályai

Ahogy már feljebb bemutattam, az és művelet bevezetési szabálya:

$$\frac{A \qquad B}{A \land B} \land\mathrm{I}$$

Úgy is mondhatjuk, hogy a vonal feletti premisszák között és kapcsolat van, de ez az és a meta-nyelv és kapcsolata. Mindig van egy meta-nyelv, amiben tárgyalunk egy tárgynyelvet. Az Isabelle tételbizonyító programban a Pure logika egy ilyen metanyelv, amiben csak néhány logikai művelet van, míg a tárgynyelv a Higher Order Logic (HOL), amiben a teljes logikai apparátus fellelhető. A teljes rendszert így Isabelle/HOL-nak nevezik.

A meta-nyelv tehát egy szinttel feljebb van, abban tárgyaljuk a tárgynyelvet. Ez hasonlít ahhoz, amikor idegen, vagy akár magyar nyelvet tanulva leíró nyelvtant tanulunk, hogyan képezzük a mondatokat, és ez is egy meta-nyelv, ami a leíró nyelvtan kifejezéseit és ábráit tartalmazza.

Az és műveletnek két kivezetési szabálya van:

$$\frac{A \land B}{A} \land\mathrm{E1} \qquad \frac{A \land B}{B} \land\mathrm{E2}$$

Erre mondhatnánk, hogy felesleges, hiszen az és művelet kommutatív, felcserélhető, de a bizonyításelmélet szigorú tudomány, csak azokat a lépéseket engedi meg, amire egyértelmű felhatalmazást adtunk. Vagyis ha nincs felcserélés, mint szabály, akkor nem cserélhetjük fel az és művelet operandusait. Később persze levezethetjük a felcserélhetőséget, de így ez a szabály nem axióma, hanem tétel.

A vagy műveletnél bevezetési szabályból van kettő:

$$\frac{A}{A \lor B} \lor\mathrm{I1} \qquad \frac{B}{A \lor B} \lor\mathrm{I2}$$

Az eddigi szabályok triviálisak, általános logikai ismeretekkel megérthetők. A vagy művelet kivezetési szabálya viszont nem ilyen, és első látásra meghökkentő, talán nem is meggyőző:

$$\dfrac{A \vee B \qquad \begin{array}{c} A \\ \vdots \\ C \end{array} \qquad \begin{array}{c} B \\ \vdots \\ C \end{array}}{C} \vee\mathrm{E}$$

Miről is van itt szó? Az $A \vee B$ diszjunkcióból (ez a vagy művelet latin neve) akkor vezethetünk le egy C állítást, ha akár A-ból, akár B-ből le tudjuk vezetni ezt a C állítást. Természetes nyelvi példával:

- $A =$ esik a hó
- $B =$ esik az eső
- $C =$ felveszem a kabátom

Ekkor ha igaz, hogy

- $A \;\cdots\; C =$ ha esik a hó, akkor felveszem a kabátom

és

- $B \;\cdots\; C =$ ha esik az eső, akkor felveszem a kabátom

akkor le tudom vezetni, hogy

- $A \vee B \;\cdots\; C$ ha esik a hó, vagy esik az eső, akkor felveszem a kabátom

Miért szükséges ez a bonyolultnak tűnő szabály? A diszjunkció, $A \vee B$ azt fejezi ki, hogy *valamelyik* kijelentés igaz, esik a hó, vagy esik az eső, de nem tudom, melyik igaz — akár mindkettő is igaz lehet, azaz havaseső esik. De, mivel a diszjunkció bármelyik tagjából le tudom vezetni a kabát felvételét, magából a diszjunkcióból is le tudom vezetni azt.

Az implikációnak két egyszerű szabálya van: a bevezetés és a kivezetés, ez utóbbinak a neve *modus ponens* a szakirodalomban. Az implikációt akkor tudjuk bevezetni, ha a premisszából le tudjuk vezetni a konklúziót:

$$\frac{\begin{array}{c}[A]\\ \vdots \\ B\end{array}}{A \to B}\ {\to}\mathrm{I}$$

Ennek megértéséhez fontos, hogy a *levezethetőség* ($\cdots$) a meta-logika fogalma, míg az *implikáció* ($\to$) a tárgy-logikáé. A kivezetési szabályt a hétköznapi életben is gyakran használjuk, csak persze nem írásban:

$$\frac{A \qquad A \to B}{B}\ {\to}\mathrm{E}$$

Ez a klasszikus irodalomban tehát a *modus ponens*.

Feladatok

A megoldásokban általában két módszert követünk: a *forward* és a *backward*, azaz az *előre* és a *hátra* bizonyítás módszerét. Előbbiben a premisszákból indulunk ki, ezekből próbálunk előre, a levezetendő felé haladni, míg az utóbbiban a levezetendőből próbálunk visszafelé, a premisszákig eljutni.

Legyen ez az első feladat: $P \vee Q \vdash Q \vee P$. A $\vdash$ szimbólum a levezethetőséget jelenti, ahogy azt a bevezetésben is jeleztem. Ha a premisszából indulunk ki és előre akarunk haladni, a vagy művelet kivezetési szabályára van szükségünk:

$$\dfrac{A \vee B \qquad \begin{array}{c} A \\ \vdots \\ C \end{array} \qquad \begin{array}{c} B \\ \vdots \\ C \end{array}}{C} \vee\mathrm{E}$$

Nyilvánvaló, hogy ezt a szabályt akkor tudjuk használni, ha a $A \leftarrow P$ és $B \leftarrow Q$ helyettesítéseket elvégezzük. Kérdés, mit írjunk a C helyébe. Kis gondolkodás után láthatjuk, hogy a levezetendő $Q \vee P$-t írhatjuk oda, tehát a $C \leftarrow Q \vee P$ helyettesítést kell még elvégezni. Ekkor ezt az ábrát kapjuk:

$$\dfrac{P \vee Q \qquad \begin{array}{c} P \\ \vdots \\ Q \vee P \end{array} \qquad \begin{array}{c} Q \\ \vdots \\ Q \vee P \end{array}}{Q \vee P} \vee\mathrm{E}$$

Ebben kellene a kipontozott részt kitölteni a természetes levezetés szabályai szerint. De itt láthatjuk, hogy a kipontozott részek egy-egy szabállyal megoldhatók: a vagy művelet bevezetési szabályait kell használni:

$$\dfrac{A}{A \vee B} \vee\mathrm{I1} \qquad\qquad \dfrac{B}{A \vee B} \vee\mathrm{I2}$$

P-ből $\vee$I2-vel tudjuk levezetni $Q \vee P$-t, Q-ból pedig $\vee$I1-gyel ugyanezt. Így megkapjuk a teljes levezetést, és ezzel a feladatot megoldottuk:

$$\dfrac{P \vee Q \qquad \dfrac{P}{Q \vee P} \vee\mathrm{I2} \qquad \dfrac{Q}{Q \vee P} \vee\mathrm{I1}}{Q \vee P} \vee\mathrm{E}$$

Felolvasva: mivel tudjuk, hogy $P \vee Q$, és mind P-ből, mind Q-ból le tudjuk vezetni, hogy $Q \vee P$, levezethetjük, hogy $Q \vee P$. A vagy kivezetési szabályának leírását idézve: nem tudjuk, hogy P vagy Q igaz, de azt tudjuk, hogy legalább az egyik igaz, ezért ha bármelyikből le tudok vezetni egy állítást, akkor ez az állítás mindenképpen igaz lesz.

A következő feladat: $P \wedge Q \to R,\ Q \to P,\ Q \vdash R$. Próbálkozzunk először a visszirányú bizonyítással: Mivel R-t kell levezetni, észrevesszük, hogy van pont egy premissza, aminek R a konklúziója: $P \wedge Q \to R$. Azt reméljük, hogy ezt használhatjuk a levezetés végén. Hogy ezt megtehessük, $P \wedge Q$-t kell használnunk, és a modus ponenst, avagy $\to$E-t:

$$\frac{A \qquad A \to B}{B} \to\mathrm{E}$$

milyen helyettesítés kell itt? $A \leftarrow P \wedge Q$ illetve $B \leftarrow R$:

$$\frac{\begin{matrix}\vdots \\ P \wedge Q\end{matrix} \qquad P \wedge Q \to R}{R} \to\mathrm{E}$$

a pontozott részt kell kitöltenünk: a $\wedge$I szabályt kell használnunk:

$$\frac{A \qquad B}{A \wedge B} \wedge\mathrm{I}$$

ebből a triviális $A \leftarrow P$ és $B \leftarrow Q$ helyettesítést alkalmazva kapjuk, hogy:

$$\frac{P \qquad Q}{P \wedge Q} \wedge\mathrm{I}$$

ehhez P-t és Q-t kell levezetnünk a premisszákból. Q az egyik premissza, ez tehát megvan. P-t a $Q \to P$ premisszából tudjuk levezetni, ismét az implikáció kivezetési szabályával, $\to$E-vel. Hogy ezt megtehessük, Q-ra is szükségünk lesz, de az ismét rendelkezésünkre áll, mint premissza:

$$\frac{Q \qquad Q \to P}{P} \to\mathrm{E}$$

ezt összedolgozva az első visszirányú lépéssel kapjuk a teljes levezetést:

$$\frac{\dfrac{\dfrac{Q \qquad Q \to P}{P} \to\mathrm{E} \qquad Q}{P \wedge Q} \wedge\mathrm{I} \qquad P \wedge Q \to R}{R} \to\mathrm{E}$$

és ezen a levezetésfán minden felülről nyitott kifejezés premissza, tehát jogosan használtuk. Megjegyzés: a Q premisszát kétszer használtuk, az általánosan használt logikákban ez megengedett, a lineáris logikában azonban nem, ezt erőforrások modellezésére szokták használni.

A $P \to (Q \to R) \vdash Q \to (P \to R)$ feladat megoldásához csak az implikáció bevezetési és kivezetési szabályára van szükségünk:

$$\dfrac{\begin{array}{c}[A]\\ \vdots\\ B\end{array}}{A \to B}\to\mathrm{I} \qquad\qquad \dfrac{A \qquad A \to B}{B}\to\mathrm{E}$$

induljunk el ismét visszafelé, a levezetni kívánt kifejezésből. A $\to$I bevezetési szabályt használhatjuk $A \leftarrow Q$ és $B \leftarrow (P \to R)$ helyettesítéseket alkalmazva. A két nyíl mást jelent: a balra mutató nyíl a helyettesítést, a jobbra mutató nyíl pedig a tárgylogika implikáció szimbóluma. A próbálkozásunk végpontja tehát:

$$\dfrac{\begin{array}{c}[Q]\\ \vdots\\ P \to R\end{array}}{Q \to (P \to R)}\to\mathrm{I}$$

ezt a lépést a $P \to R$ kifejezésre alkalmazva kapjuk, hogy

$$\dfrac{\dfrac{\begin{array}{c}[Q][P]\\ \vdots\\ R\end{array}}{P \to R}\to\mathrm{I}}{Q \to (P \to R)}\to\mathrm{I}$$

most váltsunk stratégiát, és induljunk ki a premisszából. Mivel van egy feltételezésünk, miszerint $[P]$, ezt a $P \to (Q \to R)$ premisszával kombinálva kapjuk, hogy

$$\begin{array}{c}\dfrac{\begin{array}{c}[Q]\\ \vdots\\ [P]\end{array} \qquad P \to (Q \to R)}{Q \to R}\to\mathrm{E}\\ \vdots\\ \dfrac{\dfrac{R}{P \to R}\to\mathrm{I}}{Q \to (P \to R)}\to\mathrm{I}\end{array}$$

a teljes levezetéshez már csak a $Q \to R$ implikációból kell eljutni R-ig, ehhez pedig egy implikáció kivezetésre van szükségünk:

$$\dfrac{\dfrac{\dfrac{[Q] \qquad \dfrac{[P] \qquad P \to (Q \to R)}{Q \to R}\to\mathrm{E}}{R}\to\mathrm{E}}{P \to R}\to\mathrm{I}\ \text{felhasználva: } [P]}{Q \to (P \to R)}\to\mathrm{I}\ \text{felhasználva: } [Q]$$