

# Programowanie Funkcyjne 2023

## Lista zadań nr 3

Na zajęcia 25 i 27 października 2023

**Zadanie 1 (4p).** Zapoznaj się z modułami Set oraz Map z biblioteki standardowej. Następnie zaimplementuj moduł Perm implementujący skończone permutacje (bijekcje  $\sigma$ , takie że jest tylko skończenie wiele elementów  $x$  takich, że  $\sigma(x) \neq x$ ). Powinieneś utworzyć plik perm.ml, dla którego plik perm.mli ma następującą zawartość.

```
module type OrderedType = sig
  type t
  val compare : t -> t -> int
end

module type S = sig
  type key
  type t
  (** permutacja jako funkcja *)
  val apply : t -> key -> key
  (** permutacja identycznościowa *)
  val id : t
  (** permutacja odwrotna *)
  val invert : t -> t
  (** permutacja która tylko zamienia dwa elementy miejscami *)
  val swap : key -> key -> t
  (** złożenie permutacji (jako złożenie funkcji) *)
  val compose : t -> t -> t
  (** porównywanie permutacji *)
  val compare : t -> t -> int
end

module Make(Key : OrderedType) : S with type key = Key.t
```

Wygodnie będzie reprezentować permutacje jako pary map skończonych (moduł Map), reprezentujące odpowiednio funkcję i funkcję do niej odwrotną. Jeśli danemu kluczowi nie jest przypisana żadna wartość w mapie, to funkcja na tym kluczu działa jako identyczność. Warto utrzymywać niezmiennik, że kluczowi  $k$  przypisujemy wartość  $v$  tylko wtedy gdy  $k \neq v$ . Ułatwi to implementację funkcji compare (zobacz specyfikację funkcji compare z modułu Map). Do implementacji funkcji compose przyda się funkcja merge z modułu Map. Dlaczego nasza reprezentacja permutacji powinna być typem abstrakcyjnym?

**Zadanie 2 (4p).** Napisz funkcję is\_generated, która sprawdza czy dana permutacja należy do podgrupy permutacji generowanej przez zadaną listę generatorów. Innymi słowy, funkcja dla danej permutacji  $p$  oraz listy permutacji  $g$  rozstrzyga, czy permutację  $p$  można utworzyć za pomocą identyczności, odwracania i składania permutacji znajdujących się na liście  $g$ . W tym celu użyj techniki *nasycania zbioru*, która polega na konstruowaniu kolejnych zbiorów permutacji z ciągu opisanego rekurencyjnie

$$\begin{aligned} X_0 &= \{\sigma \mid \sigma \in g\} \cup \{\text{id}\} \\ X_{n+1} &= X_n \cup \{\sigma^{-1} \mid \sigma \in X_n\} \cup \{\sigma_1 \circ \sigma_2 \mid \sigma_1, \sigma_2 \in X_n\} \end{aligned}$$

tak długo aż znajdziemy  $p$  w jednym ze zbiorów lub podany ciąg się *nasyci*, tzn. aż znajdziemy takie  $n$ , że  $X_n = X_{n+1}$ . Do obliczania kolejnych elementów tego ciągu przyda się funkcja fold z modułu Set.

Dodatkowym problemem jaki pojawia się w tym zadaniu jest to, że nasze rozwiązanie powinno działać dla permutacji elementów dowolnego typu. Możesz wybrać jeden z dwóch wariantów rozwiązania tego problemu.

- Zaprogramuj funktor który dla dowolnej implementacji permutacji utworzy moduł zawierający funkcję `is_generated`.
- Zapoznaj się z modułami pierwszej kategorii (*first-class modules*), których opis znajdziesz w rozdziale 10.5 dokumentacji języka OCaml zamieszczonej w SKOSie. Następnie zaprogramuj funkcję o następującej sygnaturze.

```
val is_generated :
  (module Perm.S with type t = 'a) -> 'a -> 'a list -> bool
```

W tym celu mogą (ale nie muszą) okazać się przydatne typy lokalnie abstrakcyjne (*locally abstract types*) opisane w rozdziale 10.4.

**Wskazówka:** Moduł `Perm` implementuje funkcję `compare`, więc może być parametrem dla funktora `Set.Make` z biblioteki standardowej.

## Mini-Projekt: Asystent Dowodzenia, cz. I

**Zadanie 3 (1p).** W tym oraz następnych zadaniach zajmiemy się fragmentem logiki intuicjonistycznej, w którym formuły składają się tylko ze zmiennych zdaniowych ( $p, q, r, \dots$ ), binarnego spójnika implikacji ( $\rightarrow$ ) oraz 0-arnego spójnika fałszu ( $\perp$ ).<sup>1</sup> Np. poprawnymi formułami są

$$p \quad p \rightarrow q \quad (p \rightarrow \perp) \rightarrow \perp \quad (p \rightarrow q \rightarrow r) \rightarrow (p \rightarrow q) \rightarrow p \rightarrow r.$$

Wypisując formuły przyjmujemy, że implikacja wiąże w prawo, więc ta ostatnia formuła w istocie oznacza

$$(p \rightarrow (q \rightarrow r)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow r)).$$

Na stronie przedmiotu znajdują się szablony rozwiązań. W plikach `logic.mli` oraz `logic.ml` uzupełnij definicję typu `formula` o zaproponowaną przez siebie reprezentację formuł w rozważanej logice.

**Wskazówka:** Zauważ, że formuły to nic innego, jak drzewa binarne, które mają dwa rodzaje liści.

**Zadanie 4 (2p).** Uzupełnij definicję funkcji `string_of_formula` znajdującą się w pliku `logic.ml`. Funkcja powinna przekształcać formułę w napis czytelny dla człowieka, używający jak najmniejszej liczby nawiasów. Funkcja ta jest prywatna dla modułu `Logic` i służy jedynie zaimplementowaniu funkcji `pp_print_formula`, którą można zarejestrować w interpreterze, jako sposób wyświetlania formuł:

```
utop # #install_printer Logic.pp_print_formula ;;
utop # let f = {zależne od Twojej reprezentacji formuł} ;;
val f : Logic.formula = (p → ⊥) → p → q
```

**Uwaga:** Jeśli jesteś odważny, możesz rozwiązać trudniejszy wariant tego zadania, polegający na bezpośrednim zaimplementowaniu funkcji `pp_print_formula`. W tym celu zapoznaj się z modułem `Format` z biblioteki standardowej. Za rozwiązanie które ładnie formatuje bardzo duże formuły, można dostać dodatkowe punkty!

**Zadanie 5 (3p).** Wprowadzimy teraz formalny system dowodzenia do naszej logiki. Będzie to wariant systemu naturalnej dedukcji, znanego Wam z kursu logiki. *Osądem* nazwiemy parę  $\Gamma \vdash \varphi$ , taką że  $\Gamma$  jest skończonym zbiorem formuł (zwanym *założeniami*), a  $\varphi$  jest formułą (zwaną *tezą* albo *konsekwencją*). Znak  $\vdash$  pełni tu tylko rolę przecinka. Dowody są drzewami, zbudowanymi z następujących reguł wnioskowania.

$$\frac{}{\{\varphi\} \vdash \varphi} (\text{Ax}) \quad \frac{\Gamma \vdash \varphi}{\Gamma \setminus \{\psi\} \vdash \psi \rightarrow \varphi} (\rightarrow \text{I}) \quad \frac{\Gamma \vdash \varphi \rightarrow \psi \quad \Delta \vdash \varphi}{\Gamma \cup \Delta \vdash \psi} (\rightarrow \text{E}) \quad \frac{\Gamma \vdash \perp}{\Gamma \vdash \varphi} (\perp \text{E})$$

Innymi słowy, dowody to drzewa, których wszystkie wierzchołki są etykietowane osądami i spełniają jeden z warunków:

<sup>1</sup>Rozszerzenie tego rachunku po pełnej logice intuicjonistycznej z koniunkcją, dysjunkcją i stałą prawdy nie wprowadza istotnych utrudnień — ale dodaje trochę kodu do napisania. Jeśli masz ochotę, rozszerz logikę o dodatkowe konstrukcje!

- wierzchołek nie ma dzieci i jest etykietowany osądem  $\{\varphi\} \vdash \varphi$ , dla pewnej formuły  $\varphi$ ;
- wierzchołek ma tylko jedno dziecko, etykietowane osądem  $\Gamma \vdash \varphi$ , zaś samo jest etykietowane osądem  $\Gamma \setminus \{\psi\} \vdash \psi \rightarrow \varphi$ ;
- wierzchołek ma dwójkę dzieci, których etykiety mają postać odpowiednio  $\Gamma \vdash \varphi \rightarrow \psi$  oraz  $\Delta \vdash \varphi$  (dla pewnych  $\Gamma, \Delta, \varphi$  oraz  $\psi$ ), zaś sam wierzchołek ma etykietę  $\Gamma \cup \Delta \vdash \psi$ ;
- wierzchołek ma etykietę  $\Gamma \vdash \varphi$  oraz tylko jedno dziecko o etykiecie  $\Gamma \vdash \perp$ .

Osąd ma dowód, jeśli istnieje poprawne drzewo dowodu, którego korzeń jest etykietowany tym osądem. Osądy mające dowód nazywamy *twierdzeniami*.

Zaproponuj typ danych reprezentujący twierdzenia w rozważanej logice i uzupełnij jego definicję w pliku `logic.ml`. Czy powinieneś ją wpisać również w pliku `logic.mli`? Przypomnij sobie pojęcie *abstrakcji danych* i zastanów się jak zapewnić, że nie da się skonstruować niepoprawnego dowodu. Czy reprezentacja twierdzeń powinna zawierać informację o całym drzewie dowodu?

Dodatkowo zaimplementuj funkcje `assumptions` oraz `consequence` zwracające odpowiednio założenia i tezę twierdzenia. Pozwolą one na zarejestrowanie funkcji drukującej twierdzenia w interpreterze.

```
utop # #install_printer Logic.pp_print_theorem ;;
```

**Zadanie 6 (4p).** Zaimplementuj funkcje `by_assumption`, `imp_i`, `imp_e` oraz `bot_e` z modułu `Logic` odpowiadające regułom wnioskowania. Ich dokładną specyfikację znajdziesz w pliku `logic.mli`

**Zadanie 7 (2p).** Korzystając z modułu `Logic` zbuduj dowody następujących twierdzeń:

- $\vdash p \rightarrow p$ ,
- $\vdash p \rightarrow q \rightarrow p$ ,
- $\vdash (p \rightarrow q \rightarrow r) \rightarrow (p \rightarrow q) \rightarrow p \rightarrow r$ ,
- $\vdash \perp \rightarrow p$ .

## W następnym odcinku ...

Moduł `Logic` dostarcza metody konstruowania dowodów *w przód*, tzn. takich gdzie z prostych znanych faktów buduje się bardziej skomplikowane. Niestety nie jest to najwygodniejsza metoda przeprowadzania dowodów w logice intuicjonistycznej. Np. skonstruowanie dowodu twierdzenia

$$\vdash (((p \rightarrow \perp) \rightarrow p) \rightarrow p) \rightarrow ((p \rightarrow \perp) \rightarrow \perp) \rightarrow p$$

nie jest łatwe, kiedy się nie wie co się robi (możesz spróbować). Znacznie łatwiej jest konstruować dowody *w tył*, tzn. upraszczać cel do udowodnienia tak długo, aż dojdziemy do rzeczy trywialnych. W terminach drzew dowodów oznacza to konstruowanie drzewa dowodu od korzenia do liści.

Celem drugiej części mini-projektu będzie zbudowanie biblioteki pozwalającej dowodzić *w tył*. Implementacja będzie znacznie bardziej skomplikowana, więc odpowiedni poziom zaufania do udowodnionych twierdzeń uzyskamy innymi środkami: odpowiedzialność za poprawność dowodu zrzucimy na moduł `Logic` z tej listy zadań. Dlatego postaraj się rozwiązać tę listę zadań, choćby już po ćwiczeniach. Jeśli jednak nie uda się Tobie tego osiągnąć, nie przejmuj się — zadania z następnej listy dalej będzie dało się rozwiązać, ale ich dobre przetestowanie może okazać się problematyczne.