Множества, Сетоиды, Теорема Диаконеску

Set — не множество

Аксиома (выбора)

Пусть задано семейство непустых множеств A $(\forall a \in A. \exists y \in a)$. Тогда найдётся функция, возвращающая по элементу из каждого множества $(\exists f : A \to \cup A. f(a) \in a)$.

Закодируем семейство с помощью отношения R: $R(a, b)$, если $b \in a$.

```
Theorem choice :
 forall (A B : Type) (R : A->B->Prop),
   (forall x : A, exists y : B, R x y) ->
    exists f : A->B, (forall x : A, R x (f x)).
```

К сожалению, `choice` доказуем (f определяется как значения, которые возвращает конструктивный квантор существования).

Сетоид

Определение

Сетоид — сет с отношением эквивалентности

Такое определение делает равенство невычислимым.
Почему аксиома выбора перестаёт быть доказуемой? Пусть $x \in A, y \in A, R(x, y)$.
Но тогда должно быть $f(x) = f(y)$, хотя квантор может подсказывать разные значения ($\exists p.R(x, p)$ и $\exists q.R(y, q)$ и $p \neq q$).

```
Reflx: {A : Type} -> (R: A -> A -> Type) -> Type
Reflx {A} R = (x : A) -> R x x

Symm: {A : Type} -> (R: A -> A -> Type) -> Type
Symm {A} R = (x : A) -> (y : A) -> R x y -> R y x

Trans: {A : Type} -> (R: A -> A -> Type) -> Type
Trans {A} R = (x : A) -> (y : A) -> (z : A) -> R x y -> R y z -> R x z

data IsEquivalence: {A : Type} -> (R: A -> A -> Type) -> Type where
    EqProof: {A: Type} -> (R: A -> A -> Type) ->
       Reflx {A} R -> Symm {A} R -> Trans {A} R -> IsEquivalence {A} R

record Setoid where
    constructor MkSetoid
    Carrier: Type
    Equiv: Carrier -> Carrier -> Type
    EquivProof: IsEquivalence Equiv
```

```
data Map: (A:Setoid) -> (B:Setoid) -> Type where
  MkMap: {A:Setoid} -> {B:Setoid} -> (f: (Carrier A) -> (Carrier B)) ->
     ({x:Carrier A} -> {y:Carrier A} ->
     ((Equiv A) x y) -> ((Equiv B) (f x) (f y))) -> Map A B

MapF: {A:Setoid} -> {B:Setoid} -> Map A B -> (Carrier A -> Carrier B)
MapF (MkMap {A} {B} f ext) = f

MapExt: {A:Setoid} -> {B:Setoid} -> (p: Map A B) ->
     ({x:Carrier A} -> {y:Carrier A} -> ((Equiv A) x y) -> ((Equiv B) (MapF p x) (MapF p y
MapExt (MkMap {A} {B} f ext) = ext

Rel: Type -> Type -> Type
Rel a b = a -> b -> Type

postulate ext_ac: {I: Setoid} -> {S: Setoid} ->
  (A: Rel (Carrier I) (Carrier S)) ->
  ((x: Carrier I) -> (g : Carrier S ** A x g)) ->
  (chs: (Map I S) ** ((w: Carrier I) -> A w ((MapF chs) w)))

excluded_middle: (P: Type) -> Or P (Not P)
```

Теорема Диаконеску

Теорема

Если рассмотреть ИИП с ZFC, то для любого P выполнено $\vdash P \vee \neg P$.

Доказательство.

Рассмотрим $\mathcal{B} = \{0, 1\}$, $A_0 = \{x \in \mathcal{B} | x = 0 \vee P\}$ и $A_1 = \{x \in \mathcal{B} | x = 1 \vee P\}$. $\{A_0, A_1\}$ — семейство непустых множеств, и по акс. выбора существует $f : \{A_0, A_1\} \to \cup A_i$, что $f(A_i) \in A_i$. (Если P, то $A_0 = A_1$ и $\{A_0, A_1\} = \{\mathcal{B}\}$).

$\vdash f(A_0) \in A_0 \mathbin{\&} f(A_1) \in A_1$	а.выбора: $f(A_i) \in A_i$
$\vdash f(A_0) \in \mathcal{B} \mathbin{\&} (f(A_0) = 0 \vee P) \mathbin{\&} f(A_1) \in \mathcal{B} \mathbin{\&} (f(A_1) = 1 \vee P)$	а.выделения
$\vdash (f(A_0) = 0 \mathbin{\&} f(A_1) = 1) \vee P$	Удал. (&) + дистр.
$\vdash P \vee f(A_0) \neq f(A_1)$	$0 \neq 1$ и транз.

Теорема Диаконеску

Теорема

Если рассмотреть ИИП с ZFC, то для любого P выполнено $\vdash P \vee \neg P$.

Доказательство.

Рассмотрим $\mathcal{B} = \{0, 1\}$, $A_0 = \{x \in \mathcal{B} | x = 0 \vee P\}$ и $A_1 = \{x \in \mathcal{B} | x = 1 \vee P\}$. $\{A_0, A_1\}$ — семейство непустых множеств, и по акс. выбора существует $f : \{A_0, A_1\} \to \cup A_i$, что $f(A_i) \in A_i$. (Если P, то $A_0 = A_1$ и $\{A_0, A_1\} = \{\mathcal{B}\}$).

$\vdash f(A_0) \in A_0 \ \& \ f(A_1) \in A_1$	а.выбора: $f(A_i) \in A_i$
$\vdash f(A_0) \in \mathcal{B} \ \& \ (f(A_0) = 0 \vee P) \ \& \ f(A_1) \in \mathcal{B} \ \& \ (f(A_1) = 1 \vee P)$	а.выделения
$\vdash (f(A_0) = 0 \ \& \ f(A_1) = 1) \vee P$	Удал. (&) + дистр.
$\vdash P \vee f(A_0) \neq f(A_1)$	$0 \neq 1$ и транз.
$\vdash P \to A_0 = A_1$	Определение A_i
$\vdash A_0 = A_1 \to f(A_0) = f(A_1)$	Конгруэнтность
$\vdash f(A_0) \neq f(A_1) \to \neg P$	Контрапозиция
$\vdash P \vee \neg P$	Подставили

$\square$

Аксиома выбора в HoTT

Определение

Обозначим пропозициональное усечение типа T как $\|T\|$

Рассмотрим $B : E \to \texttt{Set}$ — некоторое семейство множеств. Заметим, что выражение $\Pi x^E . \|Bx\|$ означает непустоту каждого элемента семейства. Тогда следующее выражение задаёт аксиому выбора:

$$\Pi x^E . \|Bx\| \to \|\Pi x^E . Bx\|$$

```
\class Choice \extends BaseSet {
  | choice {B : E -> \Set} :
      (\Pi (x : E) -> TruncP (B x)) -> TruncP (\Pi (x : E) -> B x)
}
```

Теорема Диаконеску в Аренде

Вспомогательные определения:

```
\truncated \data Quotient {A : \Type} (R : A -> A -> \Type) : \Set
```

Вспомним A из теоремы Диаконеску:
$A_0 := \{x \in \mathcal{B} | x = 0 \vee P\}$, $A_1 := \{x \in \mathcal{B} | x = 1 \vee P\}$. $A := \{A_0, A_1\}$

$$R(x, y) := \begin{cases} \text{И}, & x = y \\ P, & x \neq y \end{cases}$$

Иными словами, $A := \mathcal{B}/_R$, то есть `Quotient {Bool} R`