Cours *Preuves sur Ordinateur*

Devoir maison à rendre le 20 décembre 2013

Théorème de Ramsey

Ce devoir porte sur la preuve du théorème de Ramsey dans Coq (avec logique classique). Nous vous proposons une formalisation possible en Coq, mais vous êtes libres d'en proposer une autre. L'objectif est donner une preuve Coq du théorème `Ramsey` du fichier `ramsey.v`.

Les questions annotées par « (Coq) » sont à traiter dans le fichier `ramsey.v`. Les autres sont à traiter sur papier (LaTeX n'est pas exigé).

Les questions marquées d'une astérisque (∗) sont facultatives. Toutes les autres questions sont obligatoires, indépendamment d'un éventuel autre choix de formalisation. Quelque soit la formalisation adoptée, l'énoncé du théorème `Ramsey` du fichier `ramsey.v` ne doit pas être modifié.

1 Ramsey's Theorem

Notations and Definitions.

- Given $A \subseteq \mathbb{N}$, we let $[A]^2 \subseteq A \times A$ be the set of all $(n, m) \in A \times A$ such that $n < m$.
- A set $U \subseteq \mathbb{N}$ is **unbounded** if for all $n \in \mathbb{N}$ there is $m \in U$ such that $n \leq m$.
- Given $k \in \mathbb{N}$, a **k-coloring** (of $[\mathbb{N}]^2$) is a function $\mathsf{C} : [\mathbb{N}]^2 \to \{0, \ldots, k\}$.

  A set $A \subseteq \mathbb{N}$ is **homogeneous** for C if there is a color $i \in \{0, \ldots, k\}$ such that for all $(n, m) \in [A]^2$, we have $\mathsf{C}(n, m) = i$.

The Infinite Ramsey's Theorem is the following:

Theorem 1.1 (Ramsey). *For all $k \in \mathbb{N}$ and all k-coloring C, there is an unbounded set which is homogeneous for C.*

The following property is essential to the proof of Theorem 1.1.

Lemma 1.2 (Infinite Pigeonhole Principle). *Let $U \subseteq \mathbb{N}$ be unbounded and $(I_i)_{0 \leq i \leq k}$ be subsets of $\mathbb{N}$ such that $U \subseteq I_0 \cup \cdots \cup I_k$. There is an unbounded $V \subseteq U$ such that $V \subseteq I_i$ for some $i \in \{0, \ldots, k\}$.*

Question 1.3. *Prove Lemma 1.2*

A Proof of Ramsey's Theorem. We propose to formalize the following proof of Theorem 1.1. Fix $k \in \mathbb{N}$ and a k-coloring C of $[\mathbb{N}]^2$.

We define, by induction on $n \in \mathbb{N}$, a sequence $(U_n)_{n\in\mathbb{N}}$ of subsets of $\mathbb{N}$ such that $U_{n+1} \subseteq U_n$ and U_n is unbounded. Let $U_0 := \mathbb{N}$. Let $n \in \mathbb{N}$ and assume that U_n has been defined. Consider, for each color $i \in \{0, \ldots, k\}$, the set $V_n^i \subseteq U_n$ defined as follows:

$$V_n^i \quad := \quad \{p \mid p \in U_n \text{ and } p > m \text{ and } \mathsf{C}(m,p) = i\} \qquad \text{where} \qquad m := \min(U_n)$$

Let $U_{n+1} := V_n^i$ for some $i \in \{0, \ldots, k\}$ such that

(i) V_n^i is unbounded,

(ii) and for all $j \in \{0, \ldots, k\}$, if V_n^j is unbounded then $\min(V_n^i) \leq \min(V_n^j)$.

Question 1.4. *Show that the sequence $(U_n)_{n\in\mathbb{N}}$ is well defined and unique.*

In order to obtain Theorem 1.1, it remains to extract an homogeneous unbounded set from the sequence $(\min(U_n))_{n\in\mathbb{N}}$.

Question 1.5. *Show Theorem 1.1.*

2 Toward a Formalized Proof of Ramsey's Theorem

Fix $k \in \mathbb{N}$ and a k-coloring C of $[\mathbb{N}]^2$. In order to formalize the above proof in Coq (with classical logic), we propose to define the sequence $(\min(U_n))_{n\in\mathbb{N}}$ as a predicate `Seq : nat → Prop`. We shall however not explicitely define the sequence $(U_n)_{n\in\mathbb{N}}$.

Let

$$\mathsf{SU} \quad := \quad \{\min(U_n) \mid n \in \mathbb{N}\}$$

Given $S \subseteq \mathbb{N}$ and $a \in \mathbb{N}$, let $W(S,a)$ be the set of all $t \in \mathbb{N}$ such that for all $b < a$ with $b \in S$,

(i) $\mathsf{C}(b,a) = \mathsf{C}(b,t)$,

(ii) and $\mathsf{C}(b,a) = \mathsf{C}(b,c)$ for all $c \in S$ such that $b < c < a$.

Question 2.1. *Show that for all $n \in \mathbb{N}$, we have $U_n \subseteq W(\mathsf{SU}, \min(U_n))$.*

Question 2.2. *Let $a \in \mathbb{N}$ and consider $S, T \subseteq \mathbb{N}$ such that*

$$\forall b < a \ (b \in S \iff b \in T)$$

Show that $W(S,a) = W(T,a)$.

Question 2.3. *Show that there is a unique $\mathsf{Seq} \subseteq \mathbb{N}$ such that*

$$\forall a \in \mathbb{N} \ (a \in \mathsf{Seq} \iff W(\mathsf{Seq}, a) \text{ is unbounded}) \tag{1}$$

The Coq predicate `Seq : nat → Prop` will formalize the set Seq. The interest of Seq is that it is actually equal to SU, but makes no reference to the sequence $(U_n)_{n\in\mathbb{N}}$.

Theorem 2.4. *For all $a \in \mathbb{N}$, we have*

$$a \in \mathsf{SU} \iff a \in \mathsf{Seq}$$

Theorem 2.4 can be shown by well-founded induction.

Question 2.5. *Let $a \in \mathsf{SU}$ and assume that*

$$\forall b < a \ (b \in \mathsf{SU} \iff b \in \mathsf{Seq}) \tag{IH}$$

Show that $a \in \mathsf{Seq}$.

For the converse, it may be useful to use the following property.

Question 2.6. *Let $a \in \mathsf{Seq}$ and assume (IH). Show that for all $p \in \mathbb{N}$ such that $\min(U_p) < a$ and $a \in U_p$, we have $a \in U_{p+1}$.*

Question 2.7. *Show Theorem 2.4.*

3 Coq Formalization

The formalization of the above proof of Ramsey's theorem will be done in two step:

(1) To show Theorem 1.1 assuming a Coq predicate `Seq : nat -> Prop` which formalizes Seq.

(2) To define such a Coq predicate `Seq` using well-founded induction on natural numbers and the accessibility predicate of Coq.

Step (2) is defered until Section 3.2 below. For step (1), we use classical logic. In particular, we will need the Minimum Principle and the Infinite Pigeonhole Principle. The Minimum Principle also uses well-founded induction on `lt : nat -> nat -> Prop` (most often used with the Coq notation `<`), which does not require classical logic.

Question 3.1 (Coq). *Prove* `Theorem LtInd` *of* `Section WF_Induction`.

Question 3.2 (Coq). *Prove* `Theorem MinP` *of* `Section Minimum_Principle`.

Question 3.3 (Coq). *Prove* `Theorem IPP` *of* `Section IPP`.

3.1 Formalization of the Proof Assuming Seq

The Coq variable `Seq : nat -> Prop` of `Section Ramsey`, together with the hypothesis `DefSeq`, formalises a set Seq satisfying condition (1) of Section 2.

We propose to first formally prove that `Seq` is unbounded and then derive a formal proof of Ramsey's Theorem.

An alternative proof that Seq is unbounded. Theorem 2.4 already implies that Seq is unbounded. However, we shall not formalize this proof since we do not formalise the sequence $(U_n)_{n\in\mathbb{N}}$. In order to show from scratch that Seq is unbounded, we propose the following proof plan.

Given $n \in \mathbb{N}$, let $\mathsf{CumHom}_n \subseteq \mathbb{N}$ be such that for all $a \in \mathbb{N}$, $a \in \mathsf{CumHom}_n$ if and only if the following set $W'(n,a)$ is unbounded. Given $n, a \in \mathbb{N}$, the set $W'(n,a)$ is the set of all $t \in \mathbb{N}$ such that for all $b < n$ with $b \in \mathsf{Seq}$,

(i) $\mathsf{C}(b,a) = \mathsf{C}(b,t)$,

(ii) and $\mathsf{C}(b,a) = \mathsf{C}(b,c)$ for all $c \in \mathsf{Seq}$ such that $b < c < n$.

Question* 3.4. *Let $n \in \mathbb{N}$.*

(i) Show that for all $a \geq n$, if $a \in \mathsf{Seq}$ then $a \in \mathsf{CumHom}_n$.

(ii) Show that $a \in \mathsf{Seq}$ *if* a *is the least element of* CumHom_n *which is* $\geq n$.

Hence, we get that Seq is unbounded as soon as we prove that for all $n \in \mathbb{N}$, CumHom_n contains some $a \geq n$. This can be shown using a third sequence of sets $(\mathsf{Hom}_n)_{n\in\mathbb{N}}$, where Hom_n is the set of all $a \in \mathbb{N}$ such that for all $b, c \in \mathsf{Seq}$ such that $b < c < n$, we have $\mathsf{C}(b, c) = \mathsf{C}(b, a)$.

Question* 3.5. *Let* $n \in \mathbb{N}$.

(i) Show that Hom_n *is unbounded.*

(ii) Show that there is an $a \geq n$ *such that*

$$\{t \mid t \in \mathsf{Hom}_n \text{ and } \forall b \in \mathsf{Seq}(b < n \Longrightarrow \mathsf{C}(b, t) = \mathsf{C}(b, a)\} \quad \text{is unbounded}$$

(iii) Show that there is an $a \geq n$ *such that* $a \in \mathsf{CumHom}_n$.

The Coq predicate `Seq` is unbounded. We begin by proving in Coq that for all $n \in \mathbb{N}$, there is an $a \in \mathsf{CumHom}_n$ such that $a \geq n$. The sequences of sets $(\mathsf{CumHom}_n)_{n\in\mathbb{N}}$ and $(\mathsf{Hom}_n)_{n\in\mathbb{N}}$ are formalized by the predicates

```
CumHom : nat -> nat -> Prop    and    Hom : nat -> nat -> Prop
```

Question* 3.6 (Coq). *Prove* `Lemma Hom_UB`.

Question* 3.7 (Coq). *Prove* `Lemma CumHom_Hom`.

Question* 3.8 (Coq). *Prove* `Lemma CumHom_UB`.

From this, reasoning as above one can prove that `Seq : nat -> Prop` is unbounded.

Question* 3.9 (Coq). *Prove* `Lemma Seq_UB`.

Proof of Ramsey's Theorem. We can now adapt the reasoning of Question 1.5 and derive a formal proof of Ramsey's Theorem.

Question* 3.10 (Coq). *Prove* `Theorem Ramsey_MinP_IPP_EM`.

3.2 Definition of `Seq` by Well-Founded Induction

Consider a type `A : Type` and a relation `R : A -> A -> Prop`. The well-founded part of `R` is called in Coq its **accessible** part. The Coq inductive predicate `Acc A R : A -> Prop` provides a structural induction principle to reason by well-founded induction in the accessible part of `R`.

In particular, if `R` is (provably in Coq) well-founded, then every `x : A` is accessible. In this case, `Acc A R : A -> Prop` allows to reason by well-founded induction on `R`.

Question 3.11 (Coq). *Prove* `Lemma acc`.

We define `Seq : nat -> Prop` by well-founded induction on the strict ordering `<` of `nat` (recall that `<` is a notation for `lt : nat -> nat -> Prop`).

Question 3.12 (Coq). *Complete the definition of*

```
Fixpoint seq (x : nat) (a : Acc lt x) {struct a} : Prop
```

Given `x : nat`, the predicate `seq x` formally depends on a proof `a` of `Acc lt x`. The definition of `seq` makes sense because it is provably independent from the choice of a particular `a : Acc lt x`.

Question 3.13 (Coq). *Prove* `Lemma seq_invariant`.

Since we have

```
Lemma acc : forall x, Acc lt x
```

it is natural to define `Seq` as

```
Definition Seq x := seq x (acc x)
```

It remains to prove that the Coq predicate `Seq` actually formalizes the set Seq.

Question 3.14 (Coq). *Prove* `Theorem Seq_Correct`.

3.3 Putting Everything Together

Question 3.15 (Coq). *Prove* `Theorem Ramsey`.