CS201

Mathematics for Computer Science I

Lecture 6

Axiom of Choice $\Rightarrow$ Zorn's Lemma

- W is also an initial segment of both G and H:
  - Consider $a \in W$ and $b \in G$ such that bRa.
  - Element a belongs to a set X that is an initial segment of both G and H, therefore $b \in X$.
  - Since W is union of all such initial segments, $b \in W$.
  - Same argument for H.
- Clearly, W is the largest initial segment of G and H.

Axiom of Choice ⇒ Zorn's Lemma

- Suppose W is a proper subset of both G and H.
  - Let $c \in G \backslash W$ and $d \in H \backslash W$ be minimal elements. They exist since both G and H are well-ordered.
  - Also, since both G and H are g-sets,

$$c = g(W) = d.$$

  - Hence, $W \cup \{g(W)\}$ is an initial segment of both G and H.
  - This contradicts the fact that W is the largest initial segment of both G and H.
- Therefore, either $W = G$ or $W = H$ implying that either G is an initial segment of H or vice versa.

Axiom of Choice $\Rightarrow$ Zorn's Lemma

- Let U be the union of all g-sets.
- U is well-ordered:
  - Consider any subset V of U.
  - V intersects one of the g-sets G making up U.
  - Since G is well-ordered, $G \cap V$ has a minimal element, say m_G.
  - Suppose there is $m \in V$ such that mRm_G.
  - If $m \in G$ then $m_G Rm$ showing $m = m_G$.
  - If $m \notin G$, there exists a g-set H such that $m \in H$.
  - Since $m \in H \backslash G$, G is an initial segment of H implying that $m_G Rm$.
  - Therefore, $m = m_G$ and so minimal element of V is m_G.

Axiom of Choice $\Rightarrow$ Zorn's Lemma

- U is a g-set:
  - Consider $a \in U$.
  - Then $a \in G$ for some g-set making up U.
  - For any $c \in U$ such that cRa, $c \in H$ where H is another g-set making up U.
  - Since H is an initial segment of G or vice versa, $c \in G$ also.
  - Hence,

$$\begin{aligned} g(\{c \mid cRa \;\&\; c \in U \;\&\; c \neq a\}) &= g(\{c \mid cRa \;\&\; c \in G \;\&\; c \neq a\}) \\ &= a. \end{aligned}$$

Axiom of Choice $\Rightarrow$ Zorn's Lemma

- Since U is the union of all g-sets, it is the largest g-set.
- However, $g(U) \notin U$ and $U \cup \{g(U)\}$ is a larger g-set.
- A contradiction of the initial assumption that there is no maximal element of A.
- This proves Zorn's Lemma.

Zorn's Lemma $\Rightarrow$ Well-Ordering Principle

- We want to show that every set is well-ordered by defining an appropriate well-ordering on it.
- Let A be a set and consider partial orders R_B and subsets B of A such that R_B is a well-order on B.
- In other words, define $\mathcal{Z}$ to be the set

$$\{(B, R_B) \mid B \subseteq A \,\&\, (A, R_B) \text{ a partial order } \& \, (B, R_B) \text{ a well-ordering}\}.$$

- Set $\mathcal{Z}$ is non-empty since for finite subsets of A, it is straightforward to find well-ordering on them.

Zorn's Lemma $\Rightarrow$ Well-Ordering Principle

- Element (B, R_B) of $\mathcal{Z}$ is an initial segment of element (C, R_C) if $B \subseteq C$, R_C agrees with R_B on B, and $bR_C c$ for every $b \in B$ and $c \in C \backslash B$.
- Define a relation $\mathcal{R}$ on $\mathcal{Z}$ with $(B, R_B)\mathcal{R}(C, R_C)$ iff (B, R_B) is an initial segment of (C, R_C).
- Relation $\mathcal{R}$ is partial order on $\mathcal{Z}$.
- Let $\mathcal{C}$ be a chain of $(\mathcal{Z}, \mathcal{R})$.

ZORN'S LEMMA $\Rightarrow$ WELL-ORDERING PRINCIPLE

- Define U to be the union of all sets in the chain $\mathcal{C}$.
- Define a relation R_U on U as:
  - aR_Ub iff aR_Cb for (C, R_C) in the chain $\mathcal{C}$ such that $a, b \in C$.
  - If $a, b \in D$ for (D, R_D) in $\mathcal{C}$ then either (C, R_C) is an initial segment of (D, R_D) or vice versa.
  - In either case, aR_Db too since R_C and R_D agree on $C \cap D$.

Zorn's Lemma ⇒ Well-Ordering Principle

- R_U is a well-ordering on U:
  - Let $V \subseteq U$.
  - Then $V \cap C \neq \emptyset$ for some (C, R_C) in the chain $\mathcal{C}$.
  - Since R_C is a well-ordering on C, $V \cap C$ has a minimal element, say m_C.
  - Consider an $m \in V$ with $mR_U m_C$.
  - Since $m \in U$, there exists D in the chain $\mathcal{C}$ such that $m \in D$.
  - Suppose (C, R_C) is an initial segment of (D, R_D). Then, $m_C R_D m$ showing $m_C R_U m$.
  - Hence, $m = m_C$.

Zorn's Lemma $\Rightarrow$ Well-Ordering Principle

- Hence, $(U, R_U) \in \mathcal{Z}$ and (U, R_U) is an upper bound of the chain $\mathcal{C}$.
- By Zorn's Lemma, $(\mathcal{Z}, \mathcal{R})$ has a maximal element (M, R_M).
- If there is an element $a \in A \backslash M$, then define $(M', R_{M'})$ as:
  - $M' = M \cup \{a\}$.
  - $R_{M'}$ agrees with R_M on M, and $b R_{M'} a$ for every $b \in M$.
- We have $(M', R_{M'}) \in \mathcal{Z}$ contradicting the maximality of (M, R_M).
- Therefore, $M = A$.
- And then R_M is a well-ordering on A.

Well-Ordering Principle $\Rightarrow$ Axiom of Choice

- Let A be a set with its elements being nonempty subsets of set U.
- Use the Well-Ordering Principle to define a well-order R on U.
- Define function f, $f : A \mapsto U$ as:

$$f(X) = \text{ minimal element of } (X, R).$$

- Since $X \subseteq U$, and R is a well-ordering of U, f is well-defined.

Proofs

- A proof is a sequence of statements such that any statement in the sequence following from the previous statements from the sequence.
- Some of the statements in a proof are axioms.
- The last statement in a proof is the one that is proven.
- We have seen several proofs of different types: proof by construction, proof by contradiction, proof by diagonalization.
- Later, we will see other types of proofs: proof by induction, proof by contrapositive, ...