NOTES ON DOWEK'S "PROOFS AND ALGORITHMS"

WILLIAM DEMEO AND HYEYOUNG SHIN

Abstract. This document contains notes on the book [Dow11], *Proofs and Algorithms*, by by Gilles Dowek. We exerpt the main definitions and theorems, attempt to solve some exercises, and fix any typos or problems with the original text that we may find.

Part 1. Proofs

1. 1 Predicate Logic

First let's recall an elementary definition that plays a central role in this section. Let E be a set. A *binary relation* on E is a subset of $E \times E$. If $\leq$ is a binary relation on E that satisfies properties (1)–(3) below, then we call $\leq$ a *partial order* and we call the pair $\langle E, \leq\rangle$ a *partially ordered set*.

(1) $(\forall x)\,(x \in E \longrightarrow x \leq x)$;
(2) $(\forall x, y)\,(x \in E \bigwedge y \in E \bigwedge x \leq y \bigwedge y \leq x \longrightarrow x = y)$
(3) $(\forall x, y, z)\,(x \in E \bigwedge y \in E \bigwedge z \in E \bigwedge x \leq y \bigwedge y \leq z \longrightarrow x \leq z)$

When (1) holds we say "$\leq$ is reflexive"; when (2) holds we say "$\leq$ is antisymmetric"; when (3) holds we say "$\leq$ is transitive".

1.1. Inductive Definitions.

1.1.1. *The Fixed Point Theorem.*

Definition 1.2 (Weakly complete ordering) An partial order relation $\leq$ is said to be weakly complete if each increasing sequence has a limit.[1]

Definition 1.3 (Increasing function) Let $\leq$ be an ordering relation over a set E and f a function from E to E. The function f is increasing if $x \leq y \Rightarrow fx \leq fy$.

Definition 1.4 (Continuous function) Let $\leq$ be a weakly complete ordering relation over the set E, and f an increasing function from E to E. The function f is continuous if for every increasing sequence $(u_i)_i$ we have $\lim_i(fu_i) = f(\lim_i u_i)$.

Proposition 1.1 (First fixed point theorem) Let $\leq$ be a weakly complete ordering relation over a set E that has a least element m. Let f be a function from E to E. If f is continuous then $p = \lim_i(f^i m)$ is the least fixed point of f.

Definition 1.5 (Strongly complete ordering) An ordering relation $\leq$ over a set E is strongly

Date: February 16, 2017.

[1]A *sequence* is a function whose domain is the set $\mathbb{N} = \{0, 1, \dots\}$ of natural numbers, so Definition 1.3 can be used to infer what we mean by "increasing sequence" in Definition 1.2, although, the domain of a sequence need not be $\mathbb{N}$. So, more precisely, an *increasing sequence* is an *poset homomorphism* $u : \langle \mathbb{N}, \leq\rangle \to \langle E, \leq\rangle$; that is, if $n \leq m$ in $\mathbb{N}$, then $u_n \leq u_m$ in E.

complete if every subset A of E has a least upper bound, denoted by $\sup A$.[2]

Exercise 1.1 Show that any strongly complete ordering is also weakly complete. (done)

Is the ordering shown below weakly complete? Is it strongly complete?

```
b       c
 \     /
  \   /
   \ /
    a
```

(Answers: yes; no.)

Proposition 1.2 If the ordering $\leq$ over the set E is strongly complete, then any nonempty subset A of E has a greatest lower bound, $\inf A$.[3]

Proof. If A is a nonempty subset of E, then A has a least upper bound $\sup A$, since $\leq$ is strongly complete. The subset $B = \{y \in E \mid (\forall x \in A)\, y \leq x\}$ of E is nonempty since $\sup A \in B$. Therefore, B has a least upper bound, say, l. Note

- $(\forall y \in B)\, y \leq l$
- $\big((\forall y \in B)\, y \leq l'\big) \;\Rightarrow\; l \leq l'$.

Then l is th greatest lower bound of A. Why?

- l is a lower bound of A since if $x \in A$, then x is an upper bound of B and $l \leq x$.
- l is the greatest lower bound since if y is a lower bound of A, y is in B and $y \leq l$.

Proposition 1.3 (Second fixed point theorem) Let $\langle E, \leq \rangle$ be a strongly complete partially ordered set. Let f be a function from E to E. If f is increasing then $p = \inf\{c \mid fc \leq c\}$ is the least fixed point of f.

Proof. Let C be the set $\{c \mid fc \leq c\}$ and c be an element of C. Then $p \leq c$ since p is $\inf C$. Since f is increasing $fp \leq fc$. Note $fc \leq c$ because c is an element of C.

1.1.2. *Inductive Definitions.*

1.1.3. *Structural Induction.*

1.1.4. *Derivations.*

1.1.5. *The Reflexive-Transitive Closure of a Relation.*

1.2. **Languages.**

1.2.1. *Languages Without Variables.*

1.2.2. *Variables.*

1.2.3. *Many-Sorted Languages.*

1.2.4. *Substitution.*

1.2.5. *Articulation.*

---

[2] Notice that this definition does not require E have a least element and also does not require A be nonempty. This is not a problem. In fact, it is implicit in this definition that E contain a least element—namely, $\sup \emptyset$—as well as a greatest element—namely, $\sup E$.

[3] Dowek does not assume A is empty and this causes a problem in the original proof of Prop 1.2.

1.3. **The Languages of Predicate Logic.**

1.4. **Proofs.**

1.5. **Examples of Theories.**

1.6. **Variations on the Principle of the Excluded Middle.**

1.6.1. *Double Negation.*

1.6.2. *Multi-conclusion Sequents.*

References

[Dow11] Gilles Dowek. *Proofs and algorithms*. Undergraduate Topics in Computer Science. Springer, London, 2011. An introduction to logic and computability, Translated from the French by Maribel Fernandez. URL: `http://dx.doi.org/10.1007/978-0-85729-121-9`, `doi:10.1007/978-0-85729-121-9`.

University of Hawaii
E-mail address: `williamdemeo@gmail.com`
E-mail address: `hyeyoungshinw@gmail.com`