McMaster University
Department of Computing and Software
Musa Al-hassy

CompSci 3EA3
May 8, 2018

.

Reference Sheet for "What I'm Currently Learning"

Hello, World!

Pretty PDF Enter `M-x compile` to produce a nice looking PDF of your reference sheet.
- ⋄ I've bound this command to `C-c C-m` in my Emacs setup ;-)

Section Headers A usual Org header, say `* my section`, results in the boxed headers used in this cheat sheet.

Parallel Environments The sequence `<p TAB` produces a 'parallel' environment for producing text side-by-side. The column break is automatic, but as this is sugar for a `minipage` containing a `multicolum` we can force a column separation with `\columnbreak`: This command, in Org, necessities newlines between the items being separated.

To learn more, manipulating this source is the way to go!

The next page contains sample output from a logic-based class.

Propositional Calculus

Metatheorem Any two theorems are equivalent; ‘ true ’ is a theorem.
Equivales is an equivalence relation that is associative — $((p \equiv q) \equiv r) \;\equiv\; (p \equiv (q \equiv r))$ — and has identity true.
Discrepancy ‘ $\not\equiv$ ’ is symmetric, associative, has identity ‘ false ’, mutually associates with equivales — $((p \not\equiv q) \equiv r) \;\equiv\; (p \not\equiv (q \equiv r))$ — and mutually interchanges with it as well — $p \not\equiv q \equiv r \;\equiv\; p \equiv q \not\equiv r$ —.

Implication has the alternative definition $p \Rightarrow q \;\equiv\; \neg p \vee q$, has true as left identity and false as right zero, distributes over $\equiv$ in the second argument, and is self-distributive; and has the properties

Shunting

$$p \wedge q \Rightarrow r \quad\equiv\quad p \Rightarrow (q \Rightarrow r)$$

Contrapositive

$$p \Rightarrow q \quad\equiv\quad \neg q \Rightarrow \neg p$$

Modus Ponens

$$\begin{aligned} p \wedge (p \Rightarrow q) &\quad\equiv\quad p \wedge q \\ p \wedge (q \Rightarrow p) &\quad\equiv\quad p \\ p \wedge (p \Rightarrow q) &\quad\Rightarrow\quad q \end{aligned}$$

Moreover it has the useful property “(3.62)”: $p \Rightarrow (q \equiv r) \quad\equiv\quad p \wedge q \;\equiv\; p \wedge r$.

Conjunction and disjunction distribute over one another, $\vee$ distributes over $\equiv$, $\wedge$ distributes over $\equiv - \equiv$ in that $p \wedge (q \equiv r \equiv s) \quad\equiv\quad p \wedge q \;\equiv\; p \wedge r \;\equiv\; p \wedge s$, and they satisfy,

Excluded Middle

$$p \vee \neg p$$

Contradiction

$$p \wedge \neg p \equiv \mathsf{false}$$

Absorption

$$\begin{aligned} p \wedge (\neg p \vee q) &\equiv p \wedge q \\ p \vee (\neg p \wedge q) &\equiv p \vee q \end{aligned}$$

De Morgan

$$\begin{aligned} \neg(p \wedge q) &\equiv \neg p \vee \neg q \\ \neg(p \vee q) &\equiv \neg p \wedge \neg q \end{aligned}$$

Loops implement finite quantifications

A finite quantification can be defined axiomatically by the empty-range rule and split-off term rules. Together these form a recursive definition which can be phrased as a loop.

```
// For -⊕- : T → T → T,
// fold(A,a,b) ≈ (⊕ x : a..b-1 • A[x])
/*@ axiomatic Fold {
  @
  @ logic T
  @   fold{L}(T *A, integer a, integer b)
  @   reads a,b,A, A[..] ;
  @
  @ axiom foldEmptyRange{L} :
  @   \forall T *A, integer a, b; a >= b
  @   ==>  fold(A,a,b) == identity(⊕);
  @
  @ axiom foldSplitOffTerm{L} :
  @   \forall T *A, integer a, b; a <= b
  @   ==>     fold(A, a, b+1)
  @        == fold(A, a, b  ) ⊕ A[b];
  @ }
  @*/
```

```
/*@ requires \valid(A+(0..N-1));
  @ assigns \nothing;
  @ ensures \result == fold(A,0,N);
  @*/
T fold(int N, T* A) {

    T total = identity(⊕);

    /*@ loop invariant 0 <= n <= N;
      @ loop invariant total == fold(A,0,n);
      @ loop assigns n, total;
      @ loop variant N-n;
    */
    for(int n = 0; n != N; n++)
        total = total ⊕ A[n];
    return total;
}
```

This pseudo-code is reified by giving concrete values for `(T, ⊕, identity)` such as `(int, +, 0)` or `(bool, ||, false)`. Any monoid will do.

Lattices

The distributive lattice interface $(L, \sqsubseteq, \sqcap, \sqcup, \bot, \top)$ has the following implementations:

- Booleans: $(\mathbb{B}, \Rightarrow, \wedge, \vee, \mathsf{false}, \mathsf{true})$ —Our ambient logic!
- Extended Number Line: $(\mathbb{R}, \leq, \min, \max, -\infty, +\infty)$
- Naturals under division: $(\mathbb{N}, |, \gcd, \mathsf{lcm}, 1, 0)$
- Substructures of a given *datatype* with the substructure ordering.
  E.g., sets, lists, and graphs with subset, subsequence, and subgraph ordering.

An *order* is a relation $\text{-}\sqsubseteq\text{-} : L \to L \to \mathbb{B}$ satisfying the following three properties:

Reflexivity

$$a \sqsubseteq a$$

Transitivity

$$a \sqsubseteq b \wedge b \sqsubseteq c \Rightarrow a \sqsubseteq c$$

Antisymmetry

$$a \sqsubseteq b \wedge b \sqsubseteq a \Rightarrow a = b$$

An order is *bounded* if there are elements $\top, \bot : L$ being the lower and upper bounds of all other elements:

Top Element

$$a \sqsubseteq \top$$

Bottom Element

$$\bot \sqsubseteq a$$

A *lattice* is a pair of operations $\text{-}\sqcap\text{-}, \text{-}\sqcup\text{-} : L \to L \to L$ specified by the properties:

$\sqcup$-Characterisation

$$a \sqsubseteq c \wedge b \sqsubseteq c \quad\equiv\quad a \sqcup b \sqsubseteq c$$

$\sqcap$-Characterisation

$$c \sqsubseteq a \wedge c \sqsubseteq b \quad\equiv\quad c \sqsubseteq a \sqcap b$$

Let $\Box$ be one of $\sqcap$ or $\sqcup$, then:

Symmetry of $\Box$

$$a \Box b \;=\; b \Box a$$

Associativity of $\Box$

$$(a \Box b) \Box c \;=\; a \Box (b \Box c)$$

Idempotency of $\Box$

$$a \Box a \;=\; a$$

Zero of $\Box$

$$\begin{aligned} a \sqcup \top &= \top \\ a \sqcap \bot &= \bot \end{aligned}$$

Identity of $\Box$

$$\begin{aligned} a \sqcup \bot &= a \\ a \sqcap \top &= a \end{aligned}$$

Absorption

$$\begin{aligned} a \sqcap (a \sqcup b) &= a \\ a \sqcup (a \sqcap b) &= a \end{aligned}$$

Self-Distributivity of $\Box$

$$a \Box (b \Box c) \quad=\quad (a \Box b) \Box (a \Box c)$$

Weakening / Strengthening

$$\begin{aligned} a &\sqsubseteq a \sqcup b \\ a \sqcap b &\sqsubseteq a \\ a \sqcap b &\sqsubseteq a \sqcup b \\ a \sqcup (b \sqcap c) &\sqsubseteq a \sqcup b \\ a \sqcap b &\sqsubseteq a \sqcap (b \sqcup c) \end{aligned}$$

Induced Defs. of Inclusion

$$\begin{aligned} a \sqsubseteq b &\quad\equiv\quad a \sqcup b = b \\ a \sqsubseteq b &\quad\equiv\quad a \sqcap b = a \end{aligned}$$

Monotonicity of $\Box$

$$a \sqsubseteq b \wedge c \sqsubseteq d \Rightarrow a \Box c \sqsubseteq b \Box d$$

Golden Rule

$$\begin{aligned} a \sqcap b = a &\equiv b = a \sqcup b \\ a \sqcap b = a \sqcup b &\equiv a = b \\ a \sqcup b \sqsubseteq a \sqcap b &\equiv a = b \end{aligned}$$

Duality Principle:
If a statement S is a theorem, then so is $S[(\sqsubseteq, \sqcap, \sqcup, \top, \bot) := (\sqsupseteq, \sqcup, \sqcap, \bot, \top)]$.