CS109B Notes for Lecture 5/15/95

Tautologies

Logical expressions that evaluate to `TRUE` for any truth-assignment.

- Embody reasoning principles.
- Compare with design of expressions, where interesting functions are true for only *some* truth-assignments.

Example: `NOT` $p\bar{p}$ (a statement cannot be true and false at the same time).

Laws

Tautologies with $\equiv$ as the outermost operator, i.e., $E \equiv F$.

- Important for applying algebraic transformations to logical expressions; optimizing expressions is the goal.

Example: Commutative laws for `AND` and `OR`: $pq \equiv qp$; $p + q \equiv q + p$.

Deriving Tautologies

- Building the truth table always works, but it is exponential in the number of variables.
- *Substitution Principle*: We may make any substitution of an expression for (all occurrences of) a variable in a tautology, and we still have a tautology.

Example: We know $pq \equiv qp$ is a tautology.

- Make the substitution $p \Rightarrow r + s\bar{t}$ and $q \Rightarrow su\bar{v}$. That gives us the tautology $(r+s\bar{t})su\bar{v} \equiv su\bar{v}(r + s\bar{t})$ without having to check a 32-row truth table.
- Make the substitution $p \Rightarrow x$, $q \Rightarrow y$ to get $xy \equiv yx$.
  - □ In general, tautologies stated with one set of variables may have their variables renamed uniformly.

Substitution of Equals for Equals

If we have law $E \equiv F$ and another tautology G, we may substitute F for any or all occurrences of E in G, and the result remains a tautology.

Example: Let us derive an interesting law, the *law of the contrapositive*: $(p \rightarrow q) \equiv (\bar{q} \rightarrow \bar{p})$.

- Abbreviate SEE = "substitution of equals for equals."

1. Starting with the *law of commutativity* of `OR`: $(x+y) \equiv (y+x)$, substitute $x \Rightarrow \bar{p}$ and $y \Rightarrow q$ to get $(\bar{p}+q) \equiv (q+\bar{p})$.
2. Use another easily proved tautology, the *law of double negation*: $q \equiv \bar{\bar{q}}$.
3. SEE in (1) to get: $(\bar{p}+q) \equiv (\bar{\bar{q}}+\bar{p})$.
4. Use the law *definition of implies*: $(\bar{x}+y) \equiv (x \rightarrow y)$.
5. Two different substitutions into this law give us $(\bar{p}+q) \equiv (p \rightarrow q)$ and $(\bar{\bar{q}}+\bar{p}) \equiv (\bar{q} \rightarrow \bar{p})$.
6. SEE twice in (3) to get $(p \rightarrow q) \equiv (\bar{q} \rightarrow \bar{p})$.

Tautology Catalog

It's in the book, Section 12.8.

- Please read these.

Notice:

- `AND` and `OR` behave like union and intersection.
- In fact, if there were a "universal set" U and "complement of a set S" were defined to be $U - S$, then `AND`, `OR`, and `NOT` would behave exactly like union, intersection, and complement.
    - □ $\emptyset$ and U would be 0 and 1, respectively.
    - □ Venn Diagrams would look exactly like graphical representations of truth tables; the 2^n regions of an n-set diagram are the 2^n rows of a truth table.

DeMorgan's Laws

Used to push `NOT` below `AND` and `OR`.

- $\mathtt{NOT}(pq) \equiv (\bar{p} + \bar{q})$
- $\mathtt{NOT}(p + q) \equiv (\bar{p}\bar{q})$
- Consequence: any logical expression can be written so `NOT` applies only to variables, not to higher-level expressions.
- Explains *duality principle*: any tautology involving `AND`, `OR`, `NOT` can have (`AND` and `OR`), (`TRUE` and `FALSE`) interchanged and remain a tautology.
  - ☐ Read pp. 678–9 for proof.

Example: Consider the tautology $p + \bar{p}$.

- By "double negation," $\mathtt{NOT}\big(\mathtt{NOT}(p+\bar{p})\big)$ is also a tautology.
- By DeMorgan, and substitution of equals for equals, $\mathtt{NOT}(\bar{p}\bar{\bar{p}})$ is a tautology.
- Another use of double negation: $\mathtt{NOT}(\bar{p}p)$ is a tautology.

Tautologies as Reasoning Rules

Example: Contrapositive law: $(p \rightarrow q) \equiv (\bar{q} \rightarrow \bar{p})$.

- We saw in class how to prove $p \rightarrow q$ it was easier to prove $\bar{q} \rightarrow \bar{p}$, where
  - ☐ $p =$ "T is a MWST."
  - ☐ $q =$ "T has no cycle."
- Prove "if T has a cycle, then T is not a MWST"; conclude "if T is a MWST, then T has no cycle."

Example: Case analysis: $(p \rightarrow q)(\bar{p} \rightarrow q) \rightarrow q$.

- Consider the following statements:
  - ☐ $p =$ "n is even."
  - ☐ $q =$ "$n^2 \bmod 4 = 0$ or 1."

- Prove "if n is even then $n^2 \bmod 4 = 0$ or 1 (0, in particular)" and "if n is odd, then $n \bmod 4 = 0$ or 1 (1 in particular).

Example: Proof by contradiction: $(\bar{p} \to 0) \equiv p$.

- For instance, p might be "$L(D) \neq L$," where D is a particular DFA and L is a particular language.
- A fooling argument works by starting with $\bar{p}$ (i.e., "$L(D) = L$") and deriving `FALSE`.
  - ☐ More precisely, we show that $L(D)$ is not really L, so we have both $\bar{p}$ and p.
  - ☐ From these, we may use $\bar{p}p \equiv 0$ so we have started with $\bar{p}$ and proved 0, or `FALSE`.
- We may conclude p is true; i.e., $L(D) \neq L$.