School of Computing and Information Systems
COMP30026 Models of Computation Problem Set 6

30–27 August 2021

Content: resolution for predicate logic, clausal form, skolemization, unification.

P6.1 For each of the following pairs of terms, determine whether the pair is unifiable. If it is, give the most general unifier.

(i) $h(f(x), g(y, f(x)), y)$ and $h(f(u), g(v, v), u)$

(ii) $h(f(g(x, y)), y, g(y, y))$ and $h(f(u), g(a, v), u)$

(iii) $h(g(x, x), g(y, z), g(y, f(z)))$ and $h(g(u, v), g(v, u), v)$

(iv) $h(v, g(v), f(u, a))$ and $h(g(x), y, x)$

(v) $h(f(x, x), y, y, x)$ and $h(v, v, f(a, b), a)$

(Don't forget our agreed convention: for constants we use letters from the beginning of the alphabet, here a and b, whereas for variables we use letters from the end of the alphabet.)

P6.2 Consider these statements:

S_1: "No politician is honest."
S_2: "Some politicians are not honest."

(a) Using the predicate symbols P and H for being a politician and being honest, respectively, express the two statements as first order predicate formulas F_1 and F_2.

(b) Is $F_1 \Rightarrow F_2$ satisfiable?

(c) Is $F_1 \Rightarrow F_2$ valid?

(d) Consider these statements:

S_3: "No Australian politician is honest."
S_4: "All honest politicians are Australian."

Using the predicate symbol A for "is Australian", express S_3 and S_4 in clausal form.

(e) Using resolution, show that S_1 is a logical consequence of S_3 and S_4.

(f) Prove or disprove the statement "S_2 is a logical consequence of S_3 and S_4."

P6.3 Consider the following unsatisfiable set of clauses:

$$\{\{P(x)\}, \{\neg P(x), \neg Q(y)\}, \{Q(x), \neg R(y)\}, \{R(x), S(a)\}, \{R(b), \neg S(x)\}\}$$

What is the simplest refutation proof, if "simplest" means "the refutation tree has minimal depth"? What is the simplest refutation proof, if "simplest" means "the refutation tree has fewest nodes"?

P6.4 Consider the following predicates:

- $E(x, y)$, which stands for "x envies y"
- $F(x, y)$, which stands for "x is more fortunate than y"

(a) Using 'a' for Adam, express, in first-order predicate logic, the sentence "Adam envies everyone more fortunate than him."

(b) Using 'e' for Eve, express, in first-order predicate logic, the sentence "Eve is no more fortunate than any who envy her."

(c) Formalise an argument for the conclusion that "Eve is no more fortunate than Adam." That is, express this statement in first-order predicate logic and show that it is a logical consequence of the other two.

P6.5 Using the unification algorithm, determine whether $Q(f(g(x), y, f(y, z, z)), g(f(a, y, z)))$ and $Q(f(u, g(a), v), u)$ are unifiable. If they are, give a most general unifier. (As usual, we use letters from the end of the alphabet for variables, and letters from the beginning of the alphabet for constants.)

P6.6 Determine whether $P(f(g(x), f(g(x), g(x))), x)$ and $P(f(u, f(v, v)), u)$ are unifiable. If they are, give a most general unifier.

P6.7 Here is an example of a refutation proof where factoring will be needed. Let us try to capture Bertrand Russell's "barber paradox" as a formula in first order predicate logic. Let $B(x)$ mean "x is a barber" and let $S(u, v)$ mean "u shaves v". We want to express that barbers shave people who do not shave themselves, and also, no barber shaves someone who shaves themself. That is:

$$\forall x, y \left(B(x) \Rightarrow (S(y, y) \oplus S(x, y)) \right) \tag{1}$$

Turn this formula into clausal form. Then use resolution (with factoring) to show that there are no barbers! That is, show that $\neg\exists v\ B(v)$ is a logical consequence of the formula (1).

P6.8 Let p_i be the ith prime number and consider this conjecture: $p_1 p_2 \cdots p_k + 1$ is always prime, that is, when we add 1 to the product of the first k prime numbers, we get a new prime number. This statement is really a universally quantified statement; it says "for all k, 1 + the product of the first k primes is prime."

If the conjecture is wrong, we can hope to use Haskell to show this, by finding a counter-example. In general, we may be able to use Haskell to refute "universal" claims, or, equivalently, to *prove* "existential" claims.

(a) Can we program our way out of proving "universal" claims with the same ease?

(b) Does the conjecture hold?

A prime pair is a pair $(p, p+2)$ where both p and $p+2$ are prime.

(c) (Optional.) Use Haskell to find the first 50 prime pairs.

While we know that there are infinitely many primes, it is not known whether there are infinitely many prime pairs.

A prime triple is a triple $(p, p+2, p+4)$ with p, $p+2$, and $p+4$ all prime. Here is a Haskell definition of the list of all prime triples, assuming we have already defined `primes`, the list of all primes:

```
primeTriples :: [(Integer,Integer,Integer)]
primeTriples
  = triple primes
    where
      triple (x:y:z:xyzs)
        | x+2 == y && y+2 == z = (x,y,z) : triple (y:z:xyzs)
        | otherwise            =           triple (y:z:xyzs)
```

(d) What happens when you evaluate `primeTriples`?

(e) Prove that there exists one and only one prime triple.

P6.9 (Optional, a bonus exercise for people who love algebra.) Work through the following more substantial resolution example in your own time and make sure that you understand each step. It is optional, but feel free to discuss the problem in a tutorial or the LMS Discussion Forum if there are steps you don't understand.

Dowsing, Rayward-Smith and Walter (see **Readings Online** on the LMS) give the following example of a non-trivial proof using resolution. It is concerned with group theory. A *group* is a set endowed with a binary operation $\circ$. If we use $P(x, y, z)$ to mean $x \circ y = z$ then we can write the so-called *group axioms* as follows:

$$\begin{array}{lr} \forall x \forall y \exists z (P(x,y,z)) & \text{(closure)} \\ \forall x,y,z,u,v,w\,([P(x,y,u) \land P(y,z,v)] \Rightarrow [P(x,v,w) \Leftrightarrow P(u,z,w)]) & \text{(associativity)} \\ \exists x \forall y (P(x,y,y) \land \exists z (P(z,y,x))) & \text{(left identity} \\ & \text{and left inverse)} \end{array}$$

Notice that the associativity axiom says that if $x \circ y = u$ and $y \circ z = v$ then $x \circ v = u \circ z$. In other words, $x \circ (y \circ z) = (x \circ y) \circ z$. The last axiom says that there is some special element x in the set, with the property that $x \circ y = y$ for all y (that is, this element is a *neutral element* for $\circ$). Moreover, for each y there is a z such that $z \circ y$ yields that special element (in other words, each element has a *left inverse*). For an example of a group, consider the set $\mathbb{Z}$ of integers, endowed with the operation $+$.

We can translate the group axioms to clausal form. The first axiom (closure) becomes

$$\{P(x, y, f(x, y))\}$$

The second axiom (associativity) produces two clauses:

$$\{\neg P(x,y,u), \neg P(y,z,v), \neg P(x,v,w), P(u,z,w)\}$$
$$\{\neg P(x,y,u), \neg P(y,z,v), \neg P(u,z,w), P(x,v,w)\}$$

The last axiom (left identity and left inverse) also produces two clauses:

$$\{P(a, y, y)\}$$
$$\{P(g(y), y, a)\}$$

Suppose we want to prove that every element of a group also has a right inverse. That is, we want to prove

$$\exists x \forall y \exists z (P(y, z, x))$$

from the axioms. To do this we first negate our formula, obtaining:

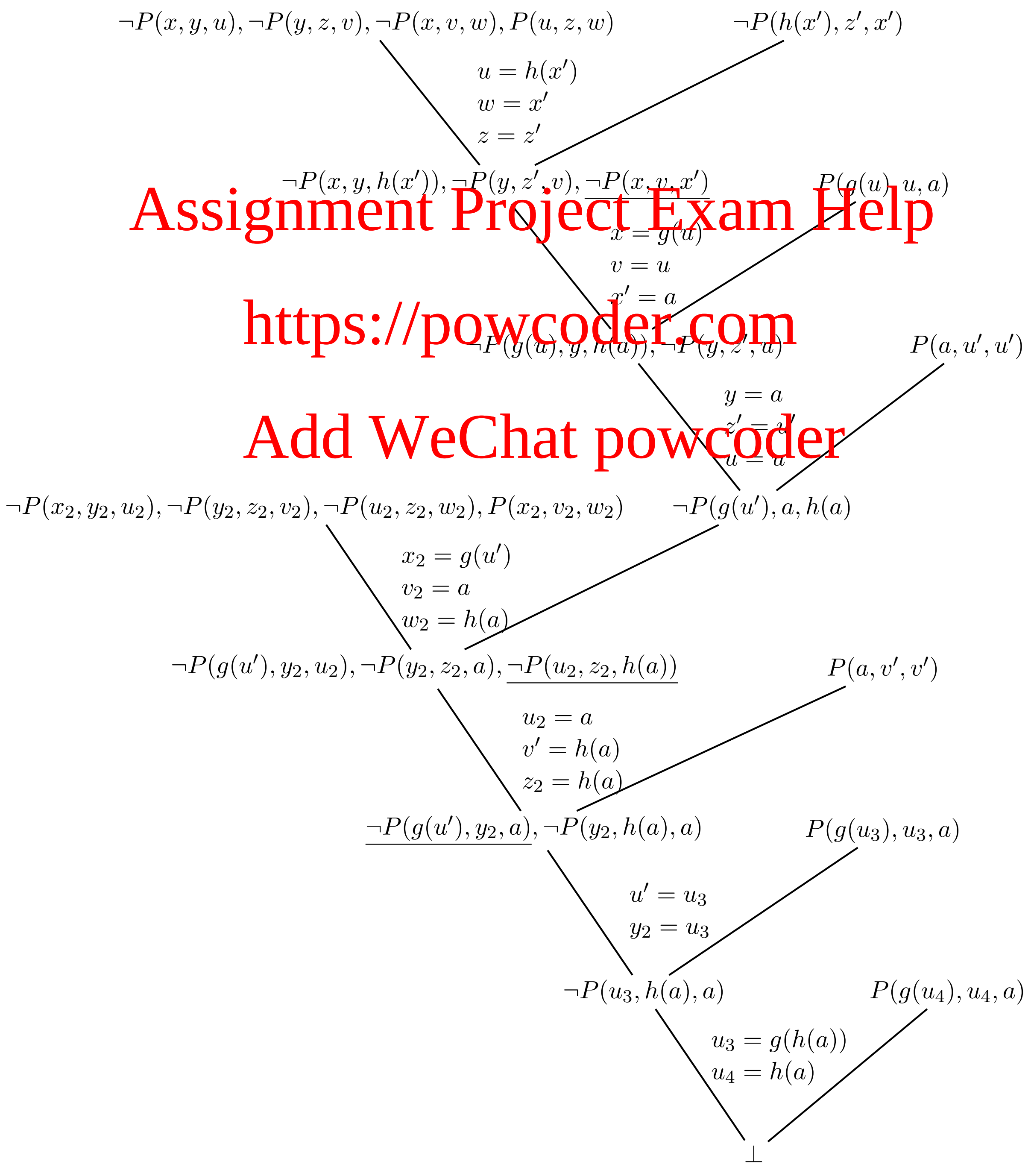
$$\forall x \exists y \forall z (\neg P(y, z, x))$$

In clausal form this becomes $\{\neg P(h(x), z, x)\}$.

Below is the proof by resolution. It is a mechanical proof of a non-trivial theorem. When there is ambiguity, I have used underlining to show which atom takes part in the resolution step.

Make sure you understand each resolution step. Did the refutation make use of all the axioms? If you try to do the proof on your own without looking at the proof above, you will find that there are many blind alleys (most of them will end in failure due to the occur check). So you will most likely take a long time, and do lots of back-tracking. With a computer of course we find the refutation in a flash.

Notice how clauses have had their variables renamed to avoid name clashes. Try to track how the variables x' and z' from the original query get bound during this proof.


$\neg P(x, y, u), \neg P(y, z, v), \neg P(x, v, w), P(u, z, w)$
$\neg P(h(x'), z', x')$
$u = h(x')$
$w = x'$
$z = z'$
$\neg P(x, y, h(x')), \neg P(y, z', v), \underline{\neg P(x, v, x')}$
$P(g(u), u, a)$
$x = g(a)$
$v = u$
$x' = a$
$\neg P(g(a), y, h(a)), \neg P(y, z', a)$
$P(a, u', u')$
$y = a$
$z' = a$
$u' = a$
$\neg P(x_2, y_2, u_2), \neg P(y_2, z_2, v_2), \neg P(u_2, z_2, w_2), P(x_2, v_2, w_2)$
$\neg P(g(u'), a, h(a))$
$x_2 = g(u')$
$v_2 = a$
$w_2 = h(a)$
$\neg P(g(u'), y_2, u_2), \neg P(y_2, z_2, a), \underline{\neg P(u_2, z_2, h(a))}$
$P(a, v', v')$
$u_2 = a$
$v' = h(a)$
$z_2 = h(a)$
$\underline{\neg P(g(u'), y_2, a)}, \neg P(y_2, h(a), a)$
$P(g(u_3), u_3, a)$
$u' = u_3$
$y_2 = u_3$
$\neg P(u_3, h(a), a)$
$P(g(u_4), u_4, a)$
$u_3 = g(h(a))$
$u_4 = h(a)$
$\perp$