Math 55: Midterm #1, 25 September 2003

Problem 1: **(a)** Define what it means for a compound proposition to be a tautology.
(b) Use a truth table to determine whether $((p \vee q) \wedge (p \to r)) \to (q \vee r)$ is a tautology by the definition of (a). Explain why your answer is intuitively reasonable.
(c) Verify the result of (b) by applying logical equivalences. State which equivalence you are using at each step.

Solution:
(a) A compound proposition, which depends on propositions p, q, r and so forth, is a tautology when it evaluates to true for any values of the propositions p, q and so forth.
(b) Intuitively, if we know either p or q is true and p implies r when true, then we know that either q or r is true. The truth table reads

p	q	r	$p \vee r$	$p \to q$	$q \vee r$	$(a \wedge b) \to c$
F	F	F	F	T	F	T
F	F	T	F	T	T	T
F	T	F	T	T	T	T
F	T	T	T	T	T	T
T	F	F	T	F	F	T
T	F	T	T	T	T	T
T	T	F	T	F	T	T
T	T	T	T	T	T	T

where we abbreviate $a = p \vee q$, $b = p \to r$ and $c = q \vee r$.
(c) By definition of implication, the given statement is equivalent to

$$\neg((p \vee q) \wedge (\neg p \vee r)) \vee (q \vee r)$$

which by de Morgan is equivalent to

$$\neg(p \vee q) \vee \neg(\neg p \vee r) \vee q \vee r$$

after we apply associativity of $\vee$. Using de Morgan twice more and cancelling double negatives gives

$$(\neg p \wedge \neg q) \vee (p \wedge \neg r) \vee q \vee r.$$

Commutativity gives

$$q \vee (\neg p \wedge \neg q) \vee r \vee (p \wedge \neg r)$$

and distributing each single-variable or over each and gives

$$((q \vee \neg p) \wedge (q \vee \neg q)) \vee ((r \vee p) \wedge (r \vee \neg r)).$$

The increase in complexity is only temporary; excluded middle and domination simplify the expression to

$$(q \vee \neg p) \vee (r \vee p)$$

which reduces to T by associativity, commutativity, excluded middle and domination.

Problem 2: Consider the following pseudocode:

function G(**set** $A = \{a_1, a_2, \ldots, a_n\}$, **set** $B = \{b_1, b_2, \ldots, b_m\}$, **function** $f : A \to B$)
    for $i := 1$ **to** m
        $h := 0$
        for $j := 1$ **to** n
            if $(f(a_j) = b_i)$ **then** $h := h + 1$
        end
        if $(h \neq 1)$ **then return F**
    end
    return T

(a) What function of f, A and B does G return?
(b) What is its worst-case complexity in terms of m and n in big-O notation? Give constants C and k and justify your answer.
(c) Modify the pseudocode to reduce the worst-case complexity to $O(m+n)$.
(d) Let $p > 2$ be a positive integer and $A = B = \{0, 1, 2, \ldots, p-1\}$. For what values of $a \in \mathbf{Z}$ does G return T for the function $f : A \to B$ defined by $f(n) = an \bmod p$?

Solution: **(a)** It returns **T** iff the input function f is a bijection (a one-to-one correspondence) between A and B.

(b) The worst case is when h is always equal to 1 after the inner loop, so the outer loop does not terminate early. Then G requires mn evaluations of f, so the worst-case complexity is $W(m,n) = O(mn)$.
(c) Use a temporary array c of length m, set it to zeroes initially, and increment c_i by 1 whenever $f(a_j) = b_i$. It is easiest if you assume $a_j = j$ and $b_i = i$; otherwise you may need a lookup table of the indices i for each target b_i. Alternatively, throw each b_i out of B as it is hit and see if anything is left over or thrown out twice.
(d) This function is a bijection when a is invertible $\pmod{p}$, which happens when $\gcd(a,p) = 1$.

Problem 3: Define a sequence a_n recursively by $a_0 = 1$ and $a_{n+1} = \sum_{j=0}^{n} a_j$ for $n \geq 0$.
(a) Compute a_0, a_1, ..., a_5.
(b) State a closed formula for the sum S of a geometric series $S = \sum_{j=0}^{n-1} r^j$ with ratio $r \neq 1$.
(c) Use strong induction to prove that $a_n = 2^{n-1}$ for $n \geq 1$.

Solution: **(a)** $a_0 = 1$, $a_1 = a_0 = 1$, $a_2 = a_1 + a_0 = 2$, $a_3 = a_2 + a_1 + a_0 = 4$, $a_4 = 4 + 2 + 1 + 1 = 8$, $a_5 = 16$.
(b) $S = (1 - r^n)/(1 - r)$.
(c) Base: $n = 1$. Clearly $a_1 = 1 = 2^{1-1}$. Induction hypothesis: Assume $a_0 = 1$, $a_1 = 2^0$, $a_2 = 2^1$, ..., $a_n = 2^{n-1}$. Then by definition,

$$a_{n+1} = \sum_{j=0}^{n} a_j = 1 + \sum_{j=1}^{n} 2^{j-1} = 1 + (1 + 2 + 4 + \cdots + 2^{n-1}).$$

By (b), the right-hand side is equal to

$$1 + \frac{1 - 2^n}{1 - 2} = 1 + 2^n - 1 = 2^{n+1-1}$$

so the induction is complete.

Problem 4: **(a)** Compute $61^{61} \bmod 9$ by modular arithmetic.
(b) State Fermat's little Theorem.
(c) Use (b) and modular arithmetic to compute $61^{61} \bmod 11$.
(d) State the Chinese Remainder Theorem for the case when there are two moduli p and q.

(e) Use (a–d) to compute $61^{61} \bmod 99$.

Solution:
(a) Since $61 \equiv -2 \pmod 9$, we have

$$61^{61} \equiv -2^{61} \equiv -2 \cdot 8^{60} \equiv -2 \cdot (-1)^{60} \equiv -2 \equiv 7 \pmod 9.$$

(b) If p is prime then for any integer a, $a^p \equiv a \pmod p$. If $\gcd(a,p) = 1$ then $a^{p-1} \equiv 1 \pmod p$.
(c) Since $p = 11$ is prime and $\gcd(61, 11) = 1$, FlT implies that $61^{10} \equiv 1 \pmod{11}$. Hence $61^{61} \equiv 61 \equiv 6 \pmod{11}$.
(d) If p and q are relatively prime then for any integers a and b, the pair of congruences

$$x \equiv a \pmod p, \qquad x \equiv b \pmod q,$$

have a unique solution x in the range $0 \le x < pq$.
(e) Let $x = 16^{61} \bmod 99$. Then x satisfies the pair of congruences

$$x \equiv 7 \pmod 9$$

$$x \equiv 6 \pmod{11}$$

which can be solved by brute force: The second congruence implies

$$x \in \{6, 17, 28, 39, 50, 61, 72, 83, 94\}$$

but then only $x = 61$ satisfies the first as well. Or, we can apply the CRT: seek

$$x = x_1 \cdot 11 + x_2 \cdot 9$$

whereupon

$$2x_1 \equiv 7 \pmod 9$$

$$9x_2 \equiv 6 \pmod{11}.$$

By inspection, the inverse of 2 mod 9 is 5 and the inverse of $9 \equiv -2 \pmod{11}$ is $-6 \equiv 5 \pmod{11}$. Or we can run the Euclidean algorithm backward and forward to find these inverses. Mulitiplying each congruence by the appropriate inverse then gives

$$x_1 \equiv 35 \equiv 8 \pmod 9$$

$$x_2 \equiv 30 \equiv 8 \pmod{11}$$

so

$$x \equiv 8 \cdot 11 + 8 \cdot 9 \equiv 160 \equiv 61 \pmod{99}.$$