Problem Set 5

Due: Start of class on Tuesday, April 1.

Problem 1. A sequence of four bits is called a *nibble*. Let N be the set of all nibbles, and let $\sim$ be a binary relation on N. The relation $x \sim y$ holds if and only if y can be obtained by *rotating* x one or more times. Rotating the nibble $b_1b_2b_3b_4$ gives the nibble $b_4b_1b_2b_3$, where $b_i \in \{0, 1\}$.

(a) Show that $\sim$ is an equivalence relation.

Solution. To show that $\sim$ is an equivalence relation, we must show that it is symmetric, reflexive and transitive.

Let $R : N \to N$ such that $R(b_1b_2b_3b_4) = b_4b_1b_2b_3$. R is simply the rotation operation. We shall denote the n-th iteration of R by R^n. For example, $R^3(x) = R(R(R(x)))$.

- First, we note that for any nibble x, $R^4(x) = x$. Therefore for any nibble x, $x \sim x$, so $\sim$ is reflexive.
- Now suppose that $x \sim y$. That means that there exists $n > 0$ such that $y = R^n(x)$. Let m be any multiple of 4 such that $m > n$. Because $R^4(x) = x$, $R^m(x) = x$ (we could prove this by induction on $m/4$). But $R^m(x) = R^{m-n}(R^n(x)) = R^{m-n}(y)$ where $m - n > 0$. Therefore, $y \sim x$. We have shown that $\sim$ is symmetric.
- Finally, suppose $x \sim y$ and $y \sim z$. Then $y = R^n(x)$ and $z = R^m(y)$ with $n > 0$ and $m > 0$. Thus, $z = R^m(R^n(x)) = R^{m+n}(x)$ and $m + n > 0$, so $x \sim z$. Therefore $\sim$ is transitive.

We conclude that $\sim$ is an equivalence relation as it is reflexive, symmetric and transitive.

(b) Describe the equivalence classes of N under the relation $\sim$.

Solution. The equivalence classes of $\sim$ are produced by taking a nibble for which the equivalence class isn't known, rotating it to get all the nibbles in its class, and then repeating this procedure until all nibbles have been placed in an equivalence class.

The equivalence classes are:

1. 0000
2. 0001, 0010, 0100, 1000
3. 0011, 0110, 1100, 1001

4. 0101, 1010
5. 0111, 1110, 1101, 1011
6. 1111

Problem 2. Let p be a positive integer. Then integers x and y are *congruent modulo* p if $x - y$ is a multiple of p. In symbols, this is written $x \equiv y \pmod{p}$.

(a) Which integers are congruent to 1 mod 4?

Solution. There are infinitely many integers that are congruent to 1 mod 4. From the definition, they are all the integers which can be written $1 + 4k$, where k is any integer. Those integers are: $\ldots, -11, -7, -3, 1, 5, 9, 13, \ldots$.

(b) Show that congruence modulo p is an equivalence relation.

Solution. To show that congruence modulo p is an equivalence relation, we show that it is reflexive, symmetric and transitive.

- For any integer x, $x - x = 0 = p \cdot 0$, so $x \equiv x \pmod{p}$. So congruence modulo p is reflexive.
- For any integers x and y such that $x \equiv y \pmod{p}$, we have $x - y = pk$, where k is an integer. Therefore, $y - x = p \cdot (-k)$, where $-k$ is also an integer, so $y \equiv x \pmod{p}$. So congruence modulo p is symmetric.
- For any integers x, y and z such that $x \equiv y \pmod{p}$ and $y \equiv z \pmod{p}$, there exist integers i and j such that $x - y = pi$ and $y - z = pj$. Therefore $x - z = x - y + y - z = p(i + j)$. Since $i + j$ is also an integer, we conclude that $x \equiv z \pmod{p}$. So congruence modulo p is transitive.

Since it is reflexive, symmetric and transitive, congruence modulo p is an equivalence relation.

Problem 3. Fibonacci numbers are defined as follows:

$$\begin{aligned} F(0) &= 0 \\ F(1) &= 1 \\ F(n) &= F(n-1) + F(n-2) \qquad (\text{for } n \geq 2) \end{aligned}$$

Thus, the first few Fibonacci numbers are 0, 1, 1, 2, 3, 5, 8, 13, and 21. Prove that for all $n \geq 1$, $F(n-1) \cdot F(n+1) - F(n)^2 = (-1)^n$.

Solution. The proof is by induction on n. Let $P(n)$ be the proposition that $F(n-1) \cdot F(n+1) - F(n)^2 = (-1)^n$.

First, we must show that $P(1)$ holds. In that case, we have:

$$\begin{aligned} F(1-1)\cdot F(1+1) - F(1)^2 &= 0\cdot 1 - 1^2 \\ &= -1^1 \end{aligned}$$

Therefore, $P(1)$ is true.

Next, we must show for all $n \geq 1$ that $P(n+1)$ is true, assuming that $P(n)$ is true. We transform the left side of the equation in proposition $P(n+1)$ into the right side as follows.

$$\begin{aligned} & F((n+1)-1)\cdot F((n+1)+1) - F(n+1)^2 \\ = \;& F(n)\cdot F(n+2) - F(n+1)^2 \\ = \;& F(n)\cdot (F(n+1)+F(n)) - F(n+1)\cdot (F(n)+F(n-1)) \\ = \;& F(n)\cdot F(n+1) + F(n)\cdot F(n) - F(n+1)\cdot F(n) - F(n+1)\cdot F(n-1) \\ = \;& F(n)\cdot F(n) - F(n+1)\cdot F(n-1) \\ = \;& -(-1)^n \\ = \;& (-1)^{n+1} \end{aligned}$$

We begin by simplifying. Then we use the definitions of $F(n+2)$ and $F(n+1)$. In the next two steps, we multiply out and cancel terms. In the fifth step, we use the induction hypothesis. In the last step, rewriting the expression gives the right side of the equation in $P(n+1)$.

Since we have proved $P(1)$ and showed that $P(n)$ implies $P(n+1)$ for all $n \geq 1$, the proposition $P(n)$ is true for all $n \geq 1$ and the claim is proved.

Problem 4. Recall that a *permutation* is a bijective function mapping a finite set to itself. Use induction to prove that there are $n! = n\cdot(n-1)\cdot(n-2)\cdots 3\cdot 2\cdot 1$ different permutations on a set of n elements.

Solution. Let $F(S)$ be the set of permutations of S.

Let $P(n)$ be the predicate "if S is a n element set then $|F(S)| = n!$". We shall prove by induction on n that $P(n)$ holds for all positive integers.

Base case: There is exactly one function from the empty set to the empty set, it is bijective, and $0! = 1$. So $P(0)$ is true.

Inductive step: Suppose that for some integer $n \geq 0$ that $P(n)$ is true.

Let S be a $n+1$ element set. $S = A \cup \{e\}$ where A is a n element set and e is some element of S.

For $m \in S$, let $P_m = \{f \in F(S) : f(e) = m\}$. Each element of $F(S)$ is in exactly one of the sets P_m, so $|F(S)| = \sum_{m\in S} |P_m|$. We shall show that there are bijections between $F(A)$ and

P_e, as well as between P_m and P_e. From this we can conclude that $|F(S)| = (n+1)|F(A)| = (n+1)!$ which shows that $P_(n+1)$ is true. We must now simply show that the bijections we announced exist.

Let $G : F(A) \to P_e$ such that for $i \in A$, $(G(f))(i) = f(i)$ and $(G(f))(e) = e$. G is injective because if $G(f) = G(g)$ then $\forall i \in A, f(i) = g(i)$, which means that $f = g$. G is surjective because for $f \in P_e$, we can consider f', the restriction of f to A. f' is in $F(A)$ and $G(f') = f$, so each element in P_e has a preimage in $F(A)$. Thus G is a bijection. Therefore, as announced, we find that there is a bijection between $F(A)$ and P_e.

Let $t_m \in F(S)$ be the bijection that exchanges e and m, and leaves all other elements unchanged (t_e is simply the identity function). Note that $t_m(t_m(i)) = i$.

Let $g_m : F(S) \to F(S)$ such that $(g_m(f))(i) = t_m(f(i))$. The range of g_m is included in $F(S)$ because $g_m(f)$ is simply f composed with t_m, and the composition of two permutations of a set S is still a permutation of S. Note that $(g_m(g_m(f)))(i) = t_m(t_m(f(i))) = f(i)$, so $g_m(g_m(f)) = f$. So g_m is a bijection, and is its own inverse.

For $f \in P_m$, $(g_m(f))(e) = t_m(f(e)) = t_m(m) = e$. So $g_m(P_m) \subseteq P_e$. Moreover, for $f \in P_e$, $(g_m(f))(e) = t_m(f(e)) = t_m(e) = m$. So $g_m(P_e) \subseteq P_m$. Since $g_m(g_m(f)) = f$, each element $f \in P_e$ is the image by g_m of $g_m(f)$, which is an element of P_m. Therefore, g_m defines a surjection from P_m to P_e. Since g_m is also globally injective, g_m defines a bijection between P_m and P_e. Therefore, the second type of bijection we had announced exists. Which allows us to conclude that $P(n+1)$ is true.

Thus by induction on n we have shown that $P(n)$ is true for all n. That is, there are $n!$ permutations of a n element set.

Problem 5. Let A, B, and C be finite sets, and let $f : B \to C$ and $g : A \to B$ be functions. Let h be the function with domain A and range C that maps $x \in A$ to $f(g(x))$. Prove or disprove the following claims:

(a) If h is surjective, then f must be surjective.

Solution. True.

For all x in C: Since h is surjective, there exists y in A such that $h(y) = x$. Therefore, by definition of h, $f(g(y)) = x$, so x is in the image of f.

Therefore, all of C is in the image of f, so f is surjective.

(b) If h is surjective, then g must be surjective.

Solution. False.

Suppose $A = C = \{1\}$ and $B = \{1, 2\}$. Let f be such that $f(1) = f(2) = 1$, and g such that $g(1) = 1$. In this case h is indeed surjective, as $h(1) = 1$, but g is not surjective as it doesn't map anything to 2.

(c) If h is injective, then f must be injective.

Solution. False.

Taking the same example as in the previous case. h is injective, because only 1 maps to 1. However, f is not injective as $f(1) = f(2)$.

(d) If h is injective, then g must be injective.

Solution. True.

For all x and y: If $g(x) = g(y)$ then $h(x) = f(g(x)) = f(g(y)) = h(y)$ so $x = y$ because h is injective.

Therefore, g is injective.

Problem 6. Xena the Warrior Princess and Conan the Barbarian are playing poker. Xena is the dealer. Conan insists that she first deal him one card, then one to herself, then one to him, and so forth, until they each have five cards. He admits that this gives him a slight edge, since he gets the first chance to draw a good card. But he thoughtfully agrees to give her the first card when he is dealer. Xena argues that Conan's "brainless barbarian" dealing method is pointless. She might as well deal five cards to him and then five cards to herself.

Conan challenges Xena to try her "prissy princess" dealing method. However, after Xena deals five cards to Conan, he asks her what her odds are of getting a pair of aces. She guesses maybe 1 in 20 or so. Conan says, "Ha! So much for your math! Your odds are ZERO, because I already have three aces! This proves my point: by dealing to me first, you gave me first shot at the good cards!"

Prove that Xena's method of dealing is more favorable to Conan or prove the opposite. Your argument should make use of a bijection.

Solution. Let the sample space S be the set of sequences of 52 distinct cards. We shall consider that each outcome is equally likely because the deck is well shuffled.

The functions X_C and C_C map outcomes to the set of cards that Xena and Conan get using Conan's method of dealing, and X_X and C_X do the same for Xena's method of dealing.

Let P be the permutation of elements of S that maps any sequence $(c_1, c_2, c_3, \dots)$ to $(c_1, c_3, c_5, c_7, c_9, c_2, c_4, c_6, c_8, c_{10}, c_{11}, c_{12}, c_{13}, \dots)$. P is indeed a permutation of S because it can be inverted by mapping $(c_1, c_2, c_3, \dots)$ to $(c_1, c_6, c_2, c_7, c_3, c_8, c_4, c_9, c_5, c_{10}, c_{11}, c_{12}, c_{13})$. It is easily verified that $X_X(P(s)) = X_C(s)$ and $C_X(P(s)) = C_C(s)$.

For any set of hands H_X and H_C, there is a subset T of S that produces those hands using Conan's method of dealing. Because of the relations we found in the preceding paragraph, Xena's method of dealing produces H_X and H_C for any shuffle in $P(T)$. For any shuffle s that give those hands with Xena's method of dealing, $P^{-1}(s)$ must be in T because of those same relations. Therefore, $P(T)$ is exactly the set of shuffles that produce H_X and H_C with Xena's method of dealing. Since P is a bijection, $|P(T)| = |T|$ so there are the same number of shuffles that produce those hands whether Xena's method or Conan's method of dealing is used. Since shuffles are equally likely, we conclude that the hands have the same probability with both methods.

Since this reasoning applies for any set of hands, we conclude that both methods of shuffling are equivalent. Conan is wrong. His reasoning on the aces is bogus because for each case where he has 3 aces, thus preventing Xena from having two aces, there are even more cases where he has no aces and Xena has slightly better odds of having 2 aces.

Problem 7. Recall that a *tournament* is a directed graph such that for every pair of distinct vertices u and v, there is either an edge from u to v or from v to u, but not both. Furthermore, no vertex has a self-loop.

(a) A *Hamiltonian path* is a directed path that visits every vertex exactly once. Prove that every tournament contains a Hamiltonian path.

Solution. The proof is by strong induction on the number of vertices in the tournament. Let $P(n)$ be the predicate "Every n-vertex tournament graph contains a Hamiltonian path". We shall show by induction that $P(n)$ holds for every positive integer n.

Base case: A tournament graph with a single vertex trivially contains a Hamiltonian path.

Inductive step: Assume that $P(1), \ldots, P(n)$ hold, and consider an $(n+1)$-vertex tournament graph G. Let a be an arbitrary vertex of G. There are three cases to consider.

First, suppose that all of a's edges are outgoing. Then let G' be the n-vertex tournament obtained from G by removing vertex a and all edges connected to a. By induction, G' has a Hamiltonian path. Prepending a to the beginning of this path gives a Hamiltonian path in G.

Second, suppose that all of a's edges are incoming. Then construct G' as before. Again, G' has a Hamiltonian path by induction. Appending a to the end of this path gives a Hamiltonian path in G.

Finally, suppose that a has some incoming edges and some outgoing edges. Let G_1 be the tournament graph on the vertices with edges directed toward a, and let G_2 be the tournament graph on the vertices with edges directed away from a. By induction, both G_1 and G_2 have Hamiltonian path. We can then construct a Hamiltonian path on G by taking the path in G_1, appending a, and then appending the Hamiltonian path in G_2.

In all cases, G contains a Hamiltonian path. Therefore $P(n+1)$ is true. By induction, we conclude that $P(n)$ holds for all $n \geq 1$. Therefore every tournament graph contains a Hamiltonian path.

(If you wish to consider the empty graph as a tournament graph, the theorem still holds; the empty path is a Hamiltonian path of the empty graph.)

(b) A *king* is a vertex u such that for every other vertex v, at least one of the following holds:

1. There is a directed edge from u to v.
2. There is another vertex x such that there is a directed edge from u to x and a directed edge from x to v.

Prove that in every tournament, the verticies with the largest number of outgoing edges must be kings.

Solution. We shall prove this by contradiction. Let a be a node with the largest number k of outgoing edges, and let b be a node that is preventing a from being a king (a can't reach b in two steps or less).

Since a can't reach b in one step, $b \to a$.

Consider any node c other than a and b such that $a \to c$. Since $a \not\twoheadrightarrow b$, there are exactly k such nodes. Because a can't reach b in two steps, we must have $c \not\twoheadrightarrow b$, that is $b \to c$.

Thus b has k outgoing edges to the nodes that a has outgoing edges to, and in addition, b has an extra outgoing edge to a. So b has at least $k + 1$ outgoing edges, which violates the definition of a as a node with the most outgoing edges.

We must conclude that b does not exist, therefore, a can reach any node in at most two steps. Therefore, a is a king.