Math 55: Sample Final Exam, 9 December 2009

3: **(a)** B is countable: in fact, a 1-1 correspondence between B and the natural numbers is provided by the function $f(b_0 b_1 b_2 \ldots b_n) = b_0 + 2^1 b_1 + \ldots + 2^n b_n$. In other words, B *is* the set of binary representations of the natural numbers.
(b) F is uncountable, by the diagonal process. Suppose F were countable or finite, and arrange the elements of F into a sequence $f_0, f_1, f_2, \ldots$. Define $g : \mathbf{N} \to \{0, 1\}$ by $g(n) = 1 - f_n(n)$. Then $g(n) \neq f_n(n)$ for any n, so $g \notin F$. This contradicts the assumption that we have listed all the elements of F, so F cannot be countable or finite.
(c) Since a program is a finite bit string, the number of C programs is countable by (a). But functions are uncountable by (b), so C programs cannot evaluate all of them.

4: **(a)** Subtracting the number of edges of C_n from the number of edges of the complete graph K_n gives $|\bar{E}| = n(n-1)/2 - n = n(n-3)/2$.
(b) Since $n(n-3)/2 \neq n$ for $n \neq 5$, C_n and $\bar{C}_n$ have different numbers of edges and hence cannot be isomorphic. For $n = 5$, they are isomorphic: the map $1 \to 1$, $2 \to 4$, $3 \to 2$, $4 \to 5$, $5 \to 3$ preserves edges.
(c) By symmetry and the handshaking theorem, all vertices of $\bar{C}_n$ have the same degree $\deg(v) = 2 \cdot n(n-3)/2n = (n-3)$, which is even iff n is odd. By Euler's theorem, $\bar{C}_n$ has an Euler circuit iff n is odd.

5: **(a)** A partial order is a relation which is reflexive, antisymmetric and transitive. R is a partial order because for any a, b and $c \in \mathbf{Z}_n$, $a|a$, $a|b \wedge b|a \to a = b$ and $a|b \wedge b|c \to a|c$.
(b) The matrix M has $M_{ij} = 1$ whenever $i|j$, so summing the entries in column j counts exactly $d(j)$ divisors i of $j \in \mathbf{Z}_n$.
(c) A prime p has only two divisors, 1 and p, so $d(p) = 2$. There are $k+1$ powers of two dividing 2^k, namely $1 = 2^0, 2^1, 2^2, \ldots, 2^k$, so $d(2^k) = k+1$.
(d) Plugging **(b)** into the definition of expectation and swapping sums gives

$$E(d) = \frac{1}{n}\sum_{j=1}^{n} d(j) = \frac{1}{n}\sum_{j=1}^{n}\sum_{i=1}^{n} M_{ij} = \frac{1}{n}\sum_{i=1}^{n}\sum_{j=1}^{n} M_{ij} = \frac{1}{n}\sum_{i=1}^{n}\lfloor n/i \rfloor \leq \frac{1}{n}\sum_{i=1}^{n} n/i \leq \sum_{i=1}^{n} 1/i.$$

since row i of M contains $\lfloor n/i \rfloor$ 1s.

6: (a) Following through the steps, $S(38, 14)$ returns 2.
(b) S computes $\gcd(a, b)$: First, we observe that S terminates because two passes through the while loop reduce the integer ab by at least a factor of two. Furthermore, $\gcd(ac, bc)$ is a loop invariant. It is clearly preserved by the first three cases of the if-test. The case when a and b are both odd works because

$$\gcd(ac, bc) = \gcd(|a - b|c, \min(a, b)c) = \gcd(ac - bc, bc)$$

if $a \geq b$, and similarly for $a < b$. Since $ac = a$ and $bc = b$ initially, $\gcd(a, b) = \gcd(ac, bc) = ac$ finally.
(c) Since ab is reduced by at least a factor of 2 every two steps, the worst-case complexity of $S(a, b)$ is $O(\log ab) = O(\log a + \log b) = O(\log \max(a, b))$.

9: (a) These graphs are not isomorphic because the left contains a simple circuit of length 3 and the right does not.

(b) These graphs are not isomorphic because the right contains a simple circuit of length 3 and the left does not.

(c) These graphs are isomorphic: Take the interior vertices 5 and 6 of the right graph and move them out to the top and bottom. Thus the isomorphism takes $1 \rightarrow 6$, $2 \rightarrow 1$, $3 \rightarrow 2$, $4 \rightarrow 4$, $5 \rightarrow 5$ and $6 \rightarrow 3$.

10: (a)

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

(b) There are two paths of length 3 from 1 to 2: one is $(1, 1, 1, 2)$, where the path loops twice at 1 then goes from 1 to 2. The other is $(1, 2, 1, 2)$, where the path goes from 1 to 2, back again, and then from 1 to 2 again..
(c) Calculating the first few powers of A gives

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix}, \begin{bmatrix} 8 & 5 \\ 5 & 3 \end{bmatrix}, \ldots, A^n = \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix}.$$

Hence the number of paths of length n from 1 to 2 is f_n.

12: (a) Since $2 \equiv 0 \pmod 2$, so is 2^{326}.
(b) Since $2^4 = 16 \equiv 1 \pmod 5$, we can drop all multiples of 4 from the exponent, leaving just 2. Thus $2^{326} \equiv 2^2 \equiv 4 \pmod 5$.

(c) By Fermat's Little Theorem, $2^{46} \equiv 1 \pmod{47}$. Since $326 = 7 \cdot 46 + 4$, we find $2^{326} \equiv 2^4 \equiv 16 \pmod{47}$.
(d) By the Chinese Remainder Theorem, there is a unique solution x of the congruences

$$\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv 4 \pmod{5} \\ x &\equiv 16 \pmod{47} \end{aligned}$$

in the range $0 \le x < 470$. From parts (a-c) above, we also know that $x = 2^{326} \bmod 470$ satisfies these congruences. The solution is $x = 204$ by inspection, so $2^{326} \equiv 204 \pmod{470}$.

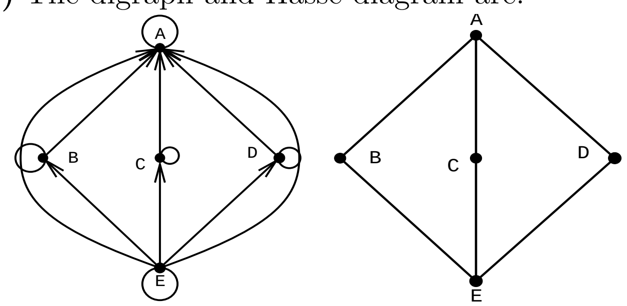
15: (a) The easy way to list equivalence relations is to list partitions into equivalence classes:

$a = \{\{1,2,3\}\}, b = \{\{1,2\},\{3\}\}, c = \{\{1,3\},\{2\}\}, d = \{\{2,3\},\{1\}\}, e = \{\{1\},\{2\},\{3\}\}$.

The corresponding relations are

$$\begin{aligned} &\{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3)\}, \\ &\{(1,1),(1,2),(2,1),(2,2),(3,3)\}, \\ &\{(1,1),(1,3),(2,2),(3,1),(3,3)\}, \\ &\{(1,1),(2,2),(2,3),(3,2),(3,3)\}, \\ &\{(1,1),(2,2),(3,3)\}. \end{aligned}$$

(b) The digraph and Hasse diagram are:



(c) A topologically sorted order for E is e, b, c, d, a.

16: (a) A partial order is a relation which is reflexive, antisymmetric and transitive. R is a partial order because for any a, b and $c \in \mathbf{Z}_n$, $a|a$, $a|b \wedge b|a \rightarrow a = b$ and $a|b \wedge b|c \rightarrow a|c$.

(b) The matrix M has $M_{ij} = 1$ whenever $i|j$, so summing the entries in column j counts exactly $d(j)$ divisors i of $j \in \mathbf{Z}_n$.
(c) A prime p has only two divisors, 1 and p, so $d(p) = 2$. There are $k+1$ powers of two dividing 2^k, namely $1 = 2^0, 2^1, 2^2, \ldots, 2^k$, so $d(2^k) = k+1$.
(d) Plugging **(b)** into the definition of expectation and swapping sums gives

$$E(d) = \frac{1}{n}\sum_{j=1}^{n} d(j) = \frac{1}{n}\sum_{j=1}^{n}\sum_{i=1}^{n} M_{ij} = \frac{1}{n}\sum_{i=1}^{n}\sum_{j=1}^{n} M_{ij} = \frac{1}{n}\sum_{i=1}^{n}\lfloor n/i \rfloor \le \frac{1}{n}\sum_{i=1}^{n} n/i \le \sum_{i=1}^{n} 1/i.$$

since row i of M contains $\lfloor n/i \rfloor$ 1s.

18: (a) B is countable: in fact, a 1-1 correspondence between B and the natural numbers is provided by the function $f(b_0 b_1 b_2 \ldots b_n) = b_0 + 2^1 b_1 + \ldots + 2^n b_n$. In other words, B *is* the set of binary representations of the natural numbers.
(b) F is uncountable, by the diagonal process. Suppose F were countable or finite, and arrange the elements of F into a sequence $f_0, f_1, f_2, \ldots$. Define $g : \mathbf{N} \to \{0, 1\}$ by $g(n) = 1 - f_n(n)$. Then $g(n) \neq f_n(n)$ for any n, so $g \notin F$. This contradicts the assumption that we have listed all the elements of F, so F cannot be countable or finite.
(c) Since a program is a finite bit string, the number of C programs is countable by (a). But functions are uncountable by (b), so C programs cannot evaluate all of them.

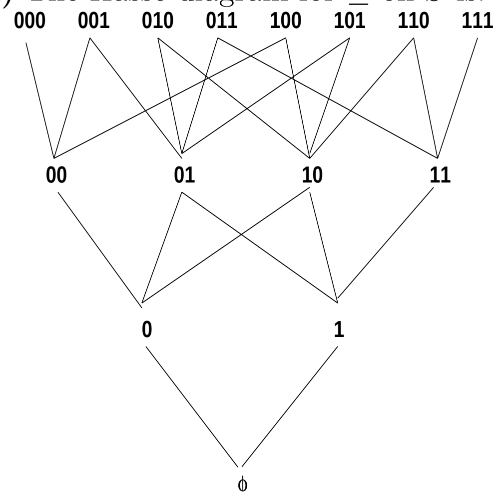
19: (a)
Reflexive: Clearly a and a have the same number of 1's.
Symmetric: The definition is clearly symmetric.
Transitive: Suppose aRb and bRc. Then a has the same number k of 1's as b, and c has the same number of 1's as b, so c has k 1's as well. Hence aRc.
(b) The relation partitions S as follows:

$$\{\{\phi, 0, 00, 000\}, \{1, 01, 10, 001, 010, 100\}, \{11, 011, 101, 110\}, \{111\}\}$$

(c)
Reflexive: Obvious since a is a substring of a.
Antisymmetric: Suppose $a \preceq b$ and $b \preceq a$. Then by definition each is obtained from the other by prefixing and postfixing, so they must be equal.

Transitive: Suppose $a \preceq b$ and $b \preceq c$. Then by definition a is a substring of b which is a substring of c, so a is a substring of c. Hence $a \preceq c$.

(d) The Hasse diagram for $\preceq$ on S is:



A topologically sorted order on S is found by pulling off a minimal element at each step; for example, one such order is

$$\phi, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, 110, 111.$$