Math 386 2012/12/19 **FINAL EXAM** Name <u>SOLUTIONS</u>

- Start each numbered problem on a *fresh page.*
- Hand in *both* this paper and test booklet.
- Show all your work for each problem; show enough work to fully justify your answer.
- Simplify answers as much as possible.
- All numerical answers may be in terms of actual numbers, factorials, and binomial coefficients *only*: not multinomial coefficients, for instance.

(1) [Points: 1] Did you read the instructions and will you follow them? Ans. ?

(2) [Points: 10] We want to count all the ways to form an *unordered* pair $\{A, B\}$ of disjoint subsets of $[n]$. How many ways are there?

Solution. I am not asking for *complementary subsets.* I am also not asking for elements of $[n]$ or elements of A and B.

Let's begin by counting *ordered* pairs (A, B). (That is, we distinguish A from B.) Each element of $[n]$ has three choices: it can be in A, or B, or neither. Thus, there are 3^n ways to make ordered pairs. Since each unordered pair $\{A, B\}$ can be ordered in two ways, to count unordered pairs we divide by 2, so the answer appears to be $3^n/2$.

This is impossible: the number is a fraction. What is wrong? We'd better check to see whether there really are two ways to order an unordered pair $\{A, B\}$. All we know is that $A \cap B = \varnothing$. The two orderings are (A, B) and (B, A). They are the same ordered pair if $A = B$. By disjointness, that implies $A = B = \varnothing$. Thus, there is one unordered pair, $\{\varnothing, \varnothing\}$, that comes from a single ordered pair. The number of ordered pairs other than $(\varnothing, \varnothing)$ is $3^n - 1$, so the number of unordered pairs other than $\{A, B\}$ is $\frac{1}{2}(3^n - 1)$. Adding to that the one unordered pair $\{\varnothing, \varnothing\}$, we have the answer: $\frac{1}{2}(3^n + 1)$.

But you may object that $\{\varnothing, \varnothing\}$ is not a pair, it is only one set. (You don't like having a multiset in this problem.) That is a perfectly reasonable objection, so your answer would be $\frac{1}{2}(3^n - 1)$.

(-2 points if you overlooked the problem with $\varnothing$.)

(3) [Points: 10] How many ways are there to permute the letters of MISSOURI? (Don't find the actual number; it takes too long.)

Solution. There are 8 letters, counting multiplicity, with two double letters, so the answer is $8!/2!^2$.

(4) [Points: 12] Prove that the number of partitions of n, whose two largest parts differ by at least 2, is equal to $p(n - 2)$. [$p(n)$ is the number of partitions of n.]

Solution. A partition of n has the form $a_1 \geq a_2 \geq \cdots \geq a_k$. Let $\mathcal{P}(n) =$ the set of all partitions of n. Let $\mathcal{P}'(n) =$ the set of partitions of n in which $a_1 \geq a_2 + 2$. We want to prove $|\mathcal{P}'(n)| = |\mathcal{P}(n - 2)$.

Here is a bijection $f : \mathcal{P}'(n) \to \mathcal{P}(n - 2)$. Define $f(a_1, a_2, \ldots, a_k) = (a_1 - 2, a_2, \ldots, a_k)$. Then $f(a_1, a_2, \ldots, a_k) \in \mathcal{P}(n - 2)$ because $a_1 - 2 \geq a_2$. I claim the inverse function $g : \mathcal{P}(n-2) \to \mathcal{P}'(n)$ is defined by $g(b_1, b_2, \ldots, b_k) = (b_1 + 2, b_2, \ldots, b_k)$.

Here $a_1 = b_1 + 2 \geq a_2 = b_2$ so we do have a valid function into $\mathcal{P}'(n)$. Thus, we have a bijection and we deduce that $|\mathcal{P}'(n)| = |\mathcal{P}(n-2)$.

I don't expect the proof to be written out formally with a bijection, but you have to check everything involved, that is, verify that you can go in both directions.

(There is a little flaw, which I don't deduct for. The proof only works for $k = 2$. We ought to consider $k = 1$ separately. That's easy.)

(5) [Points: 12] $S(n, k)$ is the Stirling number of the second kind, for $n, k \geq 0$. Assume $n, k > 1$. Prove the recurrence relation

$$S(n, k) = S(n-1, k-1) + kS(n-1, k).$$

Solution. There are combinatorial and algebraic proofs.

The algebraic proof is hard to get right, but if you tried, I gave partial credit for knowing the formula.

If you defined $S(n, k)$ as the number of ways to put n distinguishable objects into k indistinguishable boxes, you missed something: no box can be empty. This is important in the combinatorial proof. (A small deduction.)

The combinatorial proof (see Theorem 5.8) has to be well stated for full credit, but if you get the idea across pretty well, you get most of the credit.

(6) [Points: 10] Prove that the number of permutations of $[n]$ with k cycles equals the number of permutations of $[n]$ with k left-to-right maxima.

Solution. We set up a bijection f from the set of permutations with k cycles to the set of permutations in one-line form with k left-to-right maxima.

Suppose we have a permutation p with k cycles. Put it in canonical cycle form and erase the parentheses. In the resulting one-line form, each leading number in a cycle is larger than all the preceding leading numbers, and those leading numbers are larger than all other numbers in their cycles, so the first number of each cycle becomes a left-to-right maximum. A number that is not first in its cycle is less than the first number of its cycle, so it is not a left-to-right maximum. Thus, the left-to-right maxima of the one-line form are exactly the leading numbers of the cycles. It follows that $f(p)$ does have k left-to-right maxima.

Now we define an inverse function g. Let q be a permutation in one-line notation with k left-to-right maxima. Split q into cycles by starting a new cycle with every left-to-right maximum. Then $g(q)$ is in canonical cycle form and $f(g(q)) = q$ (obviously). Also, $g(f(p) = p$ (obviously). Thus, $g = f^{-1}$, which proves f has an inverse.

That proves f is a bijection, so the number of permutations with k cycles equals the number of permutations with k left-to-right maxima.

In the proof, I expect to see a clear definition of f, a proof that the left-to-right maxima are at the leading numbers of cycles and *nowhere else*, and the definition of the inverse function.

(7) [Points: 10] Find the product pq of the permutations $p = 412356$ and $q = (412)(356)$.

Solution. There are three methods.

(a) Convert q to one-line notation: $q = 245163$. Then multiply, performing p first: $1 \to 4 \to 1$, $2 \to 1 \to 2$, $3 \to 2 \to 4$, $4 \to 3 \to 5$, $5 \to 5 \to 6$, $6 \to 6 \to 3$, giving $pq = 124563$. (But, since it's hard to remember which permutation is performed first, I accepted the answer 135462, which is really qp.)

(b) Convert p to cycle form: $p = (1432)(5)(6)$. Then multiply from left to right: $pq = (1432)(5)(6) \cdot (412)(356) = (1)(2)(3456)$. (However, since some people think we should multiply from right to left, I accepted $(1)(2356)(4)$ if you explained how you got it.)

(c) Combine both methods of reading a permutation, without converting either p or q.

(8) [Points: 15] How many integers in [3000] are not divisible by any of 2, 3, or 7?

Solution. This requires the P.I.E. I expect a complete setup.
The universe is $U = [3000]$ so $|U| = 3000$.
The properties to avoid are divisibility by 2, 3, or 7, so we need sets

$$A_1 = \{\text{all numbers in } U \text{ that are divisible by } 2\},$$
$$A_2 = \{\text{all numbers in } U \text{ that are divisible by } 3\},$$
$$A_3 = \{\text{all numbers in } U \text{ that are divisible by } 7\}.$$

Thus,

$$|A_1| = 3000/2 = 1500, \quad |A_2| = 3000/3 = 1000, \quad |A_3| = \lfloor 3000/7 \rfloor = 428.$$

(Note that $|A_3| \neq 3000/7 \neq 428$; please only write correct statements!) Also,

$$A_1 \cap A_2 = \{\text{all numbers in } U \text{ that are divisible by } 6\},$$
$$A_1 \cap A_3 = \{\text{all numbers in } U \text{ that are divisible by } 14\},$$
$$A_2 \cap A_3 = \{\text{all numbers in } U \text{ that are divisible by } 21\},$$

so

$$|A_1 \cap A_2| = 3000/6 = 500, \quad |A_1 \cap A_3| = \lfloor 3000/14 \rfloor = 214,$$
$$|A_2 \cap A_3| = \lfloor 3000/21 \rfloor = 142.$$

Finally,

$$A_1 \cap A_2 \cap A_3 = \{\text{all numbers in } U \text{ that are divisible by } 42\},$$

so that

$$|A_1 \cap A_2 \cap A_3| = \lfloor 3000/42 \rfloor = 71.$$

The properties are to be avoided, so we want $|U| - |A_1 \cup A_2 \cup A_3|$. By the P.I.E.,

$$\begin{aligned} |U| - |A_1 \cup A_2 \cup A_3| &= |U| - \sum_{i=1}^{3} |A_i| + \sum_{i<j\leq 3} |A_i \cap A_j| - |A_1 \cap A_2 \cap A_3| \\ &= 3000 - (1500 + 1000 + 428) + (500 + 214 + 142) - 71 = 857. \end{aligned}$$

The answer is 857. (I disregarded trivial arithmetic errors.)

(9) [Points: 10] Use generating functions to solve the recurrence relation $a_n = na_{n-1} + 1$ ($n \geq 1$), with $a_0 = 3$.

Solution. First method. Use exponential generating functions. Let $A(x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}$. From the recurrence relation,

$$\sum_{n=1}^{\infty} a_n \frac{x^n}{n!} = \sum_{n=1}^{\infty} a_{n-1} n \frac{x^n}{n!} + \sum_{n=1}^{\infty} 1 \frac{x^n}{n!}.$$

That gives $A(x) - a_0 = xA(x) + e^x - 1$, thus

$$A(x) = \frac{e^x + 2}{1 - x}.$$

This is difficult to solve; I gave 6 points for getting this correct closed form for $A(x)$, and that's what I expect for an A on this problem.

The numerator is the ordinary generating function of the sequence

$$(3, 1/1!, 1/2!, 1/3!, \ldots, 1/n!, \ldots).$$

There was an exercise by which we know that the coefficients of x^n in $A(x)$ (that means we treat $A(x)$ as an ordinary generating function temporarily) are $a_n/n! = 3 + 1/1! + \cdots + 1/n!$. We deduce that

$$a_n = n!(3 + 1/1! + \cdots + 1/n!).$$

That would get full credit.

(This is so similar to the derangement number—except that we have the beginning of the series for e instead of $1/e$ as with derangements—that I wondered if a_n is the nearest integer to $n!(2 + e)$. In fact, that is true, if $n \geq 2$.)

(10) [Points: 10] Find a closed form for the exponential generating function for the number of permutations of n in which all cycles have even length. Simplify your closed form as far as possible, of course. (Do not try to find the coefficients of the generating function.)

Solution. Let e_n be the number. The book proves the value of e_n (for even n) by a complicated bijection. (For odd n the value is 0.) That is not necessary here. Use the exponential formula.

Let $E(x) = \sum_{n=0}^{\infty} e_n \frac{x^n}{n!}$. Let $b_k =$ the number of ways to make an even cycle out of k numbers, so $b_k = (k-1)!$ if $k > 0$, even, and $b_k = 0$ otherwise. Let $B(x) = \sum_{k=1,\text{ even}}^{\infty} b_k \frac{x^k}{k!} = \sum_{k=1,\text{ even}}^{\infty} \frac{x^k}{k}$. According to the exponential formula, $E(x) = e^{B(x)}$. Therefore,

$$E(x) = e^{\sum_{k=1}^{\infty} x^k/k}.$$

This gets 6 points.

Simplifying $A(x)$ better gets the remaining 4 points. We know $\sum_{k=1}^{\infty} \frac{x^k}{k} = -\ln(1-x)$, so $A(x) = \frac{1}{2}\big[-\ln(1-x) + \ln(1+x)\big] = \ln\sqrt{\frac{1+x}{1-x}}$. The simplification of $E(x)$ is

$$E(x) = \sqrt{\frac{1+x}{1-x}}.$$

(It's not very hard to get the exact formula for e_n from this, instead of from the complicated bijection in the textbook, but I didn't expect anyone to do that!)

(11) [Points: 5] Find a pair of orthogonal Latin squares of order 3.

Solution. Here is one example. (You can check orthogonality by eye. For instance, 1 in the first square forms the three pairs 11, 12, 13 in rows 1, 2, 3, respectively.)

1	2	3
2	3	1
3	1	2

1	2	3
3	1	2
2	3	1

(12) [Points: 15] For each of these parameter sets, decide whether it cannot belong to a BIBD, or it definitely does belong to a BIBD, or you can't tell from what we learned in class. Do your best to decide. Of course, you should provide justification.

(a) $(v, k, \lambda) = (13, 4, 1)$

Solution. The parameters satisfy the basic equations, $bk = vr$ and $r(k-1) = \lambda(v-1)$, with integral values $r = 4$ and $b = 13$. You may or may not remember that a design with these parameters is the projective plane of order 3 (with coordinates in the field $\mathbb{Z}_3$). It also was presented at the beginning of Ch. 17.

(b) $(v, k, \lambda) = (10, 3, 9)$

Solution. The parameters fail to satisfy the basic equations because we get $r = 81/2$, so there is no such BIBD.

(c) $(v, k, \lambda) = (v, 4, \binom{v-2}{2})$

Solution. The parameters satisfy the basic equations with $r = \binom{v-1}{3}$ and $b = \binom{v}{4}$. Thinking about what design might exist, you might notice that if we take all 4-element subsets of $S = [v]$, we get the right parameters. Thus, a BIBD does exist.

(13) [Points: 10] Which of the following designs are symmetric?

(a) $(v, k, \lambda) = (7, 3, 1)$

Solution. We easily calculate that $r = 3$, or that $b = 7$, so the design is symmetric.

(b) $(v, k, \lambda) = (16, 6, 2)$

Solution. Here $r = 6$ and $b = 16$, either of which is sufficient reason to declare the design is symmetric.

(c) $(v, k, \lambda) = (v, k, \binom{v-2}{k-2})$. Consider $v \geq 3$ and all values $2 \leq k \leq v-1$ for each v.

Solution. Calculation shows that $r = \binom{v-1}{k-1}$ and $b = \binom{v}{k}$. The only way $b = v$ is if $k = 1$ or $k = v-1$. The answer is therefore that the design is symmetric if $k = 1$ or $v-1$ and not if $1 < k < v-1$. (N.B. I excluded $k = 1$ so if you omit that the answer is still correct.)

N.B. I didn't ask about existence, but all the designs do exist. (a) is the Fano projective plane. (b) is something I looked up in a book. (c) is the design whose blocks are all k-element subsets of $S = [v]$ (see Example 17.6).

(14) [Points: 10] Remember that $\mathbb{Z}_3$ is the 3-element field.

(a) In the affine plane $\mathrm{AP}(\mathbb{Z}_3)$ over $\mathbb{Z}_3$, what are all the points on the line through $(0,1)$ and $(1,0)$?

Solution. The equation of the line is $x+y=1$, so the points on the line are $(0,1),(1,0),(2,2)$.

(b) The same in the projective plane $\mathrm{PP}(\mathbb{Z}_3)$.

Solution. The projective points are the affine points and the one additional point ∞_m, where m is the slope of the line.

Writing the equation in point-slope form, $y=1-x=1+2x$, so the slope is 2. So the additional point is ∞_2.

(15) [Points: 10]

(a) What is the relationship between the minimum distance d of a binary code C with words of length n, and the number of errors it can detect or correct?

Solution. (6 points) If d is odd, $d=2k+1$, then the code corrects (up to) k errors. If d is even, $d=2k$, then we say the code detects (up to) k errors and corrects (up to) $k-1$ errors. (It detects the presence of an error if $d>k$, so that's another valid answer.)
Another way to say this: If there are e errors, they can be corrected if $d>2e$ and detected if $d\geq 2e$ (and the presence of an error is detected if $d>e$; for some reason this is neglected in coding theory).

(b) Prove your statement.

Solution. (4 points) A word that is received, say w, is a codeword if and only if its distance to the nearest codeword is 0.
If there are e errors and $d>2e$, then there is one codeword at distance e from w (that's the correct word, w_0), but no other codeword can be closer than distance $d-e$ by the triangle inequality. Then $d-e>e$, so taking the closest codeword to w gives the correct word. That is, we can correct w if $d>2e$.
If $d>e$, then w cannot be a codeword unless $e=0$, because the distance to any other codeword besides the correct word w_0 is at least $d-e>0$. So we can detect that there was an error.
In coding theory we like to detect the number of errors. If $d\geq 2e$, then the distance to w_0 is $2e$, and the distance to any other codeword is at least $d-e\geq e$. So the closest codeword has distance e, and that is how we know there were e errors (at least).