I worked with Sydney Wong, Eric Severson, Srivatsav Kunnawalkam, Rachel Mendelson, Helen Hu, and Richard.

1. Recall that the extended Hamming code takes the Hamming code and adds a "parity check" bit; it has dimension 4 and uses 8 bits. The code generator matrix that I like is (which is slightly different from the order I may have given in class):

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

Show how it could be used to correct 1 error and detect 2 errors.

Proof. Let C be the extended Hamming code. Taking pairwise scalar products of the rows shows that the generated code annihilates itself, so $C \subseteq C^\perp$. In general, the dimension of the dual code complements that of the code, so $C^\perp$ has dimension 4. Thus $C = C^\perp$, so the extended Hamming code is self-dual.

Suppose $v \in \mathbb{F}_2^8$. If $v \in C$, clearly $Gv = 0$. We must interpret "v contains one error" to mean that $v = c + e_i$ for some $c \in C$ and some i. Of course, this vector could theoretically result from making more than one error, but this is not something we are able to distinguish. So this must be our interpretation. In this case, $Gv = Gc + Ge_i = 0 + G_i^T = G_i^T$, where G_i^T is the ith column of G. Thus, if v contains a single error, in the ith entry, then Gv is the ith column of G. We can correct this error by inverting the ith bit of v.

Furthermore, if Gv is one of the columns of G, then v must have just one error. This follows from the fact that G is self-dual, i.e. that its nullspace is C: $Gv = G_i^T = Ge_i$ implies $v + e_i \in \text{null}(G) = C$, so v contains one error in the ith entry. So if v were to contatin 2 errors, then Gv could not be a column of G. Also, $Gv \neq 0$, since this would imply $v \in C^\perp = C$. So if v contains 2 errors, then we can detect this situation because Gv will be a nonzero vector that is not a column of G, however we will not be able to correct the error. □

2. A "High low mid" pattern in a permutation $(a_1, \ldots, a_n)$ of length n is 3 terms a_i, a_j, a_k, where $i < j < k$ and $a_i > a_k > a_j$. Count the number of permutations of length n which avoid any "high low mid" patterns.

Proof. Let $(a_1, \ldots, a_{n+1})$ be a permutation that avoids any high low mid patterns, and let s_{n+1} be the number of such permutations. Then there exists some k for which $a_k = 1$. Now, let

$$M = \max\{b : a_i = b \text{ for some } i \leq k\}$$

and let m be such that $a_m = M$. We know that $\{a_1, \ldots, a_k\} \subseteq \{1, \ldots m\}$, and that $(a_1, \ldots, a_{n+1})$ is a permutation, therefore $k = |\{a_1, \ldots, a_k\}| \leq |\{1, \ldots M\}| = M$.

Now, assume for a contradiction that $k > M$. Then there is some number $c \in \{1, \ldots, M\}$ such that c is not represented in the first k items of the permutation. Equivalently, c *is* represented in the final $n - k$ terms, so there exists some $i > k$ such that $a_i = c$. But then $(a_m, a_k, a_i) = (M, 1, j)$ is a high low mid pattern, which is a contradiction. Thus, $M = k$.

This means that $\{a_{k+1}, \ldots, a_{n+1}\} = \{k+1, \ldots, n+1\}$. Therefore, $(a_{k+1}, \ldots, a_{n+1})$ is a permutation of $\{k+1, \ldots, n+1\}$ containing no high low mid patterns, and $(a_1, \ldots, a_{k-1})$ is a permutation of $\{1, \ldots k-1\}$ containing no high low mid patterns. So the number of permutations of $[n+1]$ containing no high low mid patterns, where $a_k = 1$, is $s_{k-1} \cdot s_{n+1-k}$. This gives

$$s_{n+1} = \sum_{k=1}^{n+1} s_{k-1} s_{n+1-k} = \sum_{k=0}^{n} s_k s_{n-k}.$$

Clearly $s_0 = 1$, since the empty cycle contains no high low mid patterns, so s_n is the Catalan numbers. □

3. Find all subsets $F \subset \mathbb{Z}$ such that the equation $a + 2b = n$ with $a, b \in F$ has exactly one solution for every positive integer n.

Proof. I am going to assume that F contains no negative integers. Under this assumption, F must contain 0, since otherwise $a + 2b = 1$ would have no solutions with $a, b \in F$. Let $F(x) = \sum_{a \in F} x^a$. Then $a + 2b = n$ with $a, b \in F$ has exactly one solution for every positive integer n if and only if

$$F(x)F(x^2) = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}.$$

Substituting x^2 for x gives

$$F(x^2)F(x^4) = \frac{1}{1-x^2} = \frac{1}{1-x}\frac{1}{1+x} = F(x)F(x^2)\frac{1}{1+x}$$
$$\implies F(x) = F(x^4)(1+x).$$

Suppose, for some n, that

$$F(x) = F(x^{4^{n+1}}) \prod_{k=0}^{n} (1 + x^{4^k}).$$

Substituting $x^{4^{n+1}}$ for x in the equation $F(x) = F(x^4)(1+x)$ gives

$$F(x^{4^{n+1}}) =,$$

so

$$F(x) = F(x^{4^{n+2}})(1 + x^{4^{n+1}}) \prod_{k=0}^{n} (1 + x^{4^k}) = F(x^{4^{n+2}}) \prod_{k=0}^{n+1} (1 + x^{4^k}).$$

Therefore, $F(x) = F(x^{4^{n+1}}) \prod_{k=0}^{n} (1 + x^{4^k})$ holds for all n. $F(x)$ must then converge to $\prod_{k=0}^{n} (1 + x^{4^k})$. This product, when expanded, becomes the sum of all terms x^n where

$$n = \sum_{k \in S} k$$

for some $S \subset \{0\} \cup \{x : x = 4^k \text{ for some } k \geq 0\}$. Therefore, F is all such n. In other words, the elements of F all finite sums of powers of 4, where terms are not repeated, together with 0. By "terms are not repeated," I mean that $4 + 16 \in F$, but $4 + 4 \notin F$. Clearly, we could shift all of F down by some constant and obtain a set that also gives unique representations for each positive integer (though also for some negative integers). I do not know if F could be a set that gives unique representations for all positive integers, but not for some negative integers. □

4. There are $2n$ people at a party. Each person has an even number of friends. Prove (using 2 different methods) that there are 2 people with an even number of common friends.

Proof. Let A be the matrix whose ijth component is 1 if the ith and jth people are friends and 0 otherwise. Now, the ijth component of AA^T is 1 if i and j are friends and 0 otherwise (no one can be their own friend, unfortunately).

If we assume that there are not 2 people with an even number of common friends, then everyone must have an odd number of common friends, thus all off-diagonal entries of AA^T are 1. Since this matrix is now the $2n \times 2n$ matrix $J - I$, it has full rank (we argued this last homework). Thus A must also have full rank. But any sum of rows from A will have to have an even number of ones, since all rows of A have an even number of ones (if u and v have an even number of ones, then u and v differ in an even number of entries; thus their sum has an even number of ones). Therefore, any vector with an odd number of ones is not in the rowspan of A, contradicting that it has full rank.

Another way to view this solution is to see A as the mod 2 adjacency matrix of the friendship graph (vertices i and j are joined if and only if people i and j are friends). $A^2 = AA^T$ (since A is symmetric) gives the parity of the number of length 2 paths from i to j, which is equivalent to the number of common friends of i and j; the diagonal entries are 0 because length two paths from a vertex to itself are in correspondence with friends of that vertex - just walk to a neighbor then return. The solution is the same from this point.

Here is a completely separate solution. Assume again, for a contradiction, that everyone has an odd number of common friends. Consider a single person, Alfred. Let A be the set of Alfred's friends, which has even size. Let B be the set of people he is not friends with, excluding himself. Since there are an even number of people, $|A| + |B| + 1$ is even, thus B has odd size.

Now, consider an arbitrary person, Bob, in set B. Bob has a odd number of friends in set A, thus he must have an odd number of friends in set B as well (since he has an even number of total friends, but he is not friends with Alfred, because Alfred is an asshole).

Since Bob was arbitrary, everyone in set B has an odd number of friends in set B. Therefore, if we count all directed friendships in B, by summing over all the friends of everyone in B, then we will be summing an odd number of odd terms, thus the sum will be odd. But this sum is simply 2 times the number of friendships within B, which must be even - a contradiction. □

5. A couple of problems to practice with the *absorption identity*

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1},$$

which is really helpful for moving things in and out of binomial coefficients (such as cancelling out terms you don't want). You must use the identity somewhere for both of these.

(a) Simplify $\sum_{k=0}^{n} k\binom{n}{k}$.

Proof.

$$\sum_{k=0}^{n} k\binom{n}{k} = \sum_{k=1}^{n} k \cdot \frac{n}{k}\binom{n-1}{k-1} = n\sum_{k=0}^{n-1}\binom{n-1}{k} = n \cdot 2^{n-1}.$$

□

(b) An (actual!!) paper has its final answer "simplified" to

$$\sum_{k=0}^{n} k \frac{\binom{m-k-1}{m-n-1}}{\binom{m}{n}}.$$

Simplify it further.

Proof.

$$\begin{aligned}
\sum_{k=0}^{n} k \frac{\binom{m-k-1}{m-n-1}}{\binom{m}{n}} &= \frac{1}{\binom{m}{n}} \sum_{k=0}^{n} \left(m - (m-n)\frac{m-k}{m-n} \right) \binom{m-k-1}{m-n-1} \\
&= \frac{m}{\binom{m}{n}} \sum_{k=0}^{n} \binom{m-k-1}{m-n-1} - \frac{m-n}{\binom{m}{n}} \sum_{k=0}^{n} \binom{m-k}{m-n} \\
&= \frac{m}{\binom{m}{n}} \binom{m}{n} - (m-n)\frac{\binom{m+1}{n}}{\binom{m}{n}} \\
&= m - (m-n)\frac{m+1}{m-n+1} \\
&= \frac{m(m-n) + m - m(m-n) - (m-n)}{m-n+1} \\
&= \frac{n}{m-n+1}.
\end{aligned}$$

□

6. Let l be a product of n (distinct) primes. Count the number of ways to write l as a product of m positive integers, none of which are 1.

Proof. This is simply the number of ways to partition n distinguishable objects (since the primes are distinguishable, by assumption) into m nonempty distinguishable subsets (since no factor can be 1). This is just $S(n, m)m!$. □

7. How much time did you spend on this problem set? What comments do you have of the problems? (difficulty, type, enjoyment, fairness, etc.)

I spent about 8-10 hours on this problem set. The only really easy problem was 6. Obviously, #3 was difficult. I would say more about the problems, but I am very tired from doing them. So I'll just stop here.