Math 778B Homework

Austin Mohr

November 26, 2011

Problem 1

Proposition 1. *If $\mathbf{v}_1, \ldots, \mathbf{v}_m$ is a collection of points in $\mathbb{R}^n$ such that the distance between any two of them is a fixed value $\alpha \neq 0$, then $m \leq n + 1$.*

Proof. We proceed by induction on n. For the case $n = 1$, there are clearly at most 2 points that are pairwise distance α apart. For general n, begin by choosing a set X containing n points that are pairwise distance α apart (by induction, this can always be done). Let H be the hyperplane containing X. We show that there are precisely two points in $\mathbb{R}^n$ that are distance α from all points of X. Denote such a point by p. Since H is $(n-1)$-dimensional, it cannot be that p lies in H, as this would violate the inductive hypothesis. We also know that the projection of p onto H must be equidisant from all points of X (else p is not equidistant from all points of X). Thus, there is a unique line orthogonal to H on which p must lie. Now, p together with any two points of X form an equilateral triangle. Hence, p must lie on L at distance $\frac{\sqrt{3}\alpha}{2}$ from H, giving two possible choices for p. We may add either choice to X and maintain the property of all points having pairwise distance α, but not both (the two choices are at distance $\sqrt{3}\alpha$). Therefore, there are at most $n+1$ points in $\mathbb{R}^n$ that are all pairwise distance α apart, as desired. □

Problem 2

A vector $\mathbf{x} \in \mathbb{R}^8$ belongs to point set of the 6-dimensional Gosset polytope provided it satisfies one of the following:

- The first two coordinates are a permutation of $\{1, 1\}$ and the last six coordinates are a permutation of $\{1, 1, 1, 1, -3, -3\}$ (call these *type 1 points*).
- The first two coordinates are a permutation of $\{-1, 3\}$ and the last six coordinates are a permutation of $\{-1, -1, -1, -1, -1, 3\}$ (call these *type 2 points*).

Let V denote the collection of points that can be defined in this way.

Proposition 2. *The point set V is a two-distance set on 27 points contained in a 6-dimensional subspace of $\mathbb{R}^8$.*

Proof. There are $1 \cdot \binom{6}{2} = 15$ type 1 points and $2 \cdot \binom{6}{1} = 12$ type 2 points, and so there are indeed a total of 27 points in V.

The points as specified are naturally elements of $\mathbb{R}^8$. In addition, they satisfy two linear equations. Namely, for all $\mathbf{x} \in V$,

- $\sum_{i=1}^{8} \mathbf{x}_i = 0$, and
- $\sum_{i=1}^{2} \mathbf{x}_i = 2$.

Since neither of these dependencies can be deduced from the other, it follows that each reduces the dimension of the space by one. Hence, the points of V exist in a 6-dimensional subspace of $\mathbb{R}^8$.

Finally, we show that V is a two-distance set. To that end, let $\mathbf{x}, \mathbf{y} \in V$. We proceed by analyzing cases on the types of $\mathbf{x}$ and $\mathbf{y}$.

Case $\mathbf{x}$ and $\mathbf{y}$ both type 1: The points $\mathbf{x}$ and $\mathbf{y}$ must either differ in two coordinates or four. In the former, their distance will be $\sqrt{2 \cdot 4^2} = 4\sqrt{2}$. In the latter, their distance will be $\sqrt{4 \cdot 4^2} = 8$.

Case $\mathbf{x}$ and $\mathbf{y}$ both type 2: As in the previous case, the points $\mathbf{x}$ and $\mathbf{y}$ can differ in two coordinates or four, yielding the same two possible distances.

Case $\mathbf{x}$ and $\mathbf{y}$ are of different types: Without loss of generality, let $\mathbf{x}$ be type 1 and $\mathbf{y}$ be type 2. Let $\mathbf{y}_k = 3$. Among all the possible permutations of coordinates for $\mathbf{x}$ and $\mathbf{y}$, the only factor affecting the distance is whether $x_k = 1$ or $x_k = -3$. In the former case, their distance is $\sqrt{7 \cdot 2^2 + 6^2} = 8$. In the latter, their distance is $\sqrt{8 \cdot 2^2} = 4\sqrt{2}$. □

Problem 3

A vector $\mathbf{x} \in \mathbb{R}^5$ belongs to point set of the 5-dimensional halfcube provided it satisfies both of the following:

- All coordinates of $\mathbf{x}$ are either 0 or 1.
- The sum of the coordinates of $\mathbf{x}$ is even.

Let V denote the collection of points that can be defined in this way.

Proposition 3. *The point set V is a two-distance set on 16 points.*

Proof. There are $2^5 = 32$ binary strings of length five, and precisely half of these have an even number of 1's. Thus, $|V| = 16$.

Let $\mathbf{x}, \mathbf{y} \in V$. Notice that they cannot differ in an odd number of coordinates, as this would entail that one of $\mathbf{x}$ or $\mathbf{y}$ had an odd number of 1's. Thus, they must differ in either two coordinates or four. In the former case, their distance will be $\sqrt{2 \cdot 1^2} = \sqrt{2}$. In the latter, their distance will be $\sqrt{4 \cdot 1^2} = 2$. □

Problem 4

Proposition 4. *Let I be a linearly independent subset of a vector space. There is a linearly independent set containing I that is maximal with this property.*

Proof. Let V be the ambient vector space. Define

$$\mathcal{I} = \{A \subset V \mid A \text{ is linearly independent and } I \subset A\}.$$

The collection $\mathcal{I}$ is partially ordered by inclusion. The conclusion of the proposition is precisely to show that $\mathcal{I}$ has a maximal element, which we accomplish by Zorn's lemma.

Choose a chain $\mathcal{C}$ of elements of $\mathcal{I}$ and let $C = \bigcup \mathcal{C}$. Certainly, C is an upper bound for $\mathcal{C}$ and contains I. It remains to show that C is linearly independent. To that end, consider any finite collection $v_1, \ldots, v_m$ of vectors in C. Since $\mathcal{C}$ is a chain, there is some set $A_0 \in \mathcal{C}$ containing all v_i. By the linear independence of A_0, no non-trivial linear combination of the v_i is equal to zero. As the v_i were arbitrary, it follows that C is linearly independent. Therefore, every chain has an upper bound in $\mathcal{I}$, and the conclusion follows from Zorn's lemma. □

Problem 5

A *degenerate plane* is a set of n points and n lines configured such that exactly $n-1$ points lie on a common line L (so exactly 1 point, call it p, lies off the line) and, for each point q on L, there is a unique line passing through p and q.

Proposition 5. *A set of n points and n lines is a degenerate plane if and only if*

1. *any two lines intersect in exactly one point,*
2. *there is exactly one line through any two points, and*
3. *given any four points, some line contains at least three of them.*

Proof. By inspection, one can see that a degenerate plane satisfies the three listed properties.

For the reverse direction, consider the case where every line contains exactly two points. It follows that there are $\binom{n}{2}$ lines, which is equal to n precisely when $n = 3$. One can check that the only configuration satisfying the desired properties when $n = 3$ is the degenerate plane.

Consider now the case where there is some line L containing at least 3 points. It cannot be that L contains all n points, as no further lines could be included without violating condition 2. If L contains exactly $n-1$ points (and so exactly 1 point lies off of L), there must be a unique line through each point of L and the remaining point lying off L. Such a configuration is precisely a degenerate plane. In particular, this must be the case for $n = 4$.

Finally, suppose for contradiction that $n \geq 5$ and L contains at least 3 points (and so at least 2 points lie off of L). Let x and y be two of the points lying off of L and let p, q, and r be three of the points lying on L. By property 3, there must be a line containing three of the points in the set $\{x, y, p, q\}$. Since L already contains p and q, there can be no other line containing them (by condition 2). Thus, without loss of generality, there is a line M containing x, y, and p. Similarly, there must be a line containing three of the points in the set $\{x, y, p, r\}$. By condition 2, such a line can neither contain both of p and r (because L already contains them) nor can it contain both of x and y (because M already contains them). Since no such line exists, there can be no configuration satisfying the desired properties when $n \geq 5$ and L contains at least 3 points, which exhausts the remaining cases. □

Problem 6

Proposition 6. *The chromatic number of the unit-distance graph of $\mathbb{R}^n$ is finite.*

Proof. We tile $\mathbb{R}^n$ with a certain multi-colored cube, which is itself composed of many single-colored cubes.

To begin, let C be an n-dimensional cube whose antipodal points are at strictly less than unit distance. Thus, no two points of C are at unit distance.

Next, let C' be an n-dimensional cube with side length strictly greater than 2 formed by the union of a sufficient number of almost-disjoint copies of C. Fix some indexing scheme on the copies of C, so that we may write $C' = \bigcup_{i=1}^{m} C_i$. For each i, color all points of the cube C_i color i. If a particular point belongs to multiple cubes, we may assign it any color present among these cubes. Notice that if two points $x, y \in C'$ are at unit distance, then $x \in C_j$ and $y \in C_k$ ($j \neq k$), since there no unit distances within any particular C_i. Thus, the larger cube C' is properly colored by a finite number of colors.

Finally, tile the entirety of $\mathbb{R}^n$ with almost-disjoint copies of C'. As before, if a point would belong to multiple color classes, we may assign it a color arbitrarily from among those classes.

We claim that this tiling is a proper coloring of $\mathbb{R}^n$. Suppose we have two points receiving the same color. Either they belong to the same copy of C', in which case we've already shown that their distance is less than 1, or they belong to two different copies of C'. In the latter case, these points are at greater than unit distance, since the side length of a copy of C' is greater than 2 and the side length of any smaller monochromatic cube comprising it is less than unit distance. Therefore, any two points at unit distance

receive two different colors from among a finite collection of colors, and so the chromatic number of $\mathbb{R}^n$ is finite. $\square$

Problem 7

Proposition 7. *Let A and B be finite sets and let $f : A \to B$ and $g : B \to A$ be independent random variables. If, for some fixed $\epsilon > 0$ and for all $a \in A$, $\Pr(g_{f_a} = a) > \frac{1}{2}$, then $|A| \leq |B|$.*

Proof. We show first that, for any $a \in A$, there is some element $b \in B$ such that $\Pr(g_b = a) > \frac{1}{2}$. Suppose, for contradiction, that this is not the case. It follows that

$$\begin{aligned}
\frac{1}{2} &< \Pr(g_{f_a} = a) \\
&= \sum_{b' \in B} \Pr((f_a = b') \wedge (g_{b'} = a)) \\
&= \sum_{b' \in B} \Pr(f_a = b') \Pr(g_{b'} = a) \\
&\leq \frac{1}{2} \sum_{b' \in B} \Pr(f_a = b') \\
&= \frac{1}{2}.
\end{aligned}$$

Let $h : A \to B$ be the function that sending an element of A to its corresponding element of B as above. We claim that h is an injection. Suppose, for contradiction, that this is not the case. That is, there are distinct elements $a_1, a_2 \in A$ such that $\Pr(g_b = a_1) > \frac{1}{2}$ and $\Pr(g_b = a_2) > \frac{1}{2}$. It follows that

$$\begin{aligned}
1 &= \sum_{a' \in A} \Pr(g_b = a') \\
&\geq \Pr(g_b = a_1) + \Pr(g_b = a_2) \\
&= 1.
\end{aligned}$$

Since h is an injection from A into B, it follows that $|A| \leq |B|$, as desired. $\square$

Problem 8

Proposition 8. *Let V be the poset consisting of all finite subsets of an infinite set ordered by inclusion. Let $f, g : V \to \mathbb{F}$, where $\mathbb{F}$ is any field. For any set X belonging to V, the following inversion holds for f and g:*

$$f(X) = \sum_{Y \subseteq X} g(Y)$$

if and only if

$$g(X) = \sum_{Y \subseteq X} (-1)^{|X-Y|} f(Y).$$

Proof. We proceed by induction. For the base case, suppose that $X = \emptyset$. We see that

$$\begin{aligned}
f(\emptyset) &= \sum_{Y \subseteq \emptyset} g(Y) \\
&= g(\emptyset)
\end{aligned}$$

and

$$\begin{aligned} g(\emptyset) &= \sum_{Y \subseteq \emptyset} (-1)^{|\emptyset - Y|} f(Y) \\ &= (-1)^0 f(\emptyset) \\ &= f(\emptyset). \end{aligned}$$

Thus, the two statements are equivalent in the base case.

We treat the induction in two stages.

($\Rightarrow$) Let the finite set X be given and let X' be the set obtained by removing a single element from X. We have

$$\begin{aligned} &\sum_{Y \subseteq X} (-1)^{|X-Y|} f(Y) \\ &= \sum_{Y \subseteq X} (-1)^{|X-Y|} \sum_{Z \subseteq Y} g(Z) \\ &= \sum_{Y \subseteq X'} (-1)^{|X-Y|} \sum_{Z \subseteq Y} g(Z) + \sum_{\substack{Y \subseteq X \\ Y \not\subseteq X'}} (-1)^{|X-Y|} \sum_{Z \subseteq Y} g(Z) \\ &= \sum_{Y \subseteq X'} (-1)^{|X-Y|} \sum_{Z \subseteq Y} g(Z) + \sum_{\substack{Y \subseteq X \\ Y \not\subseteq X'}} (-1)^{|X-Y|} \sum_{\substack{Z \subseteq Y \\ Z \subseteq X'}} g(Z) + \sum_{\substack{Y \subseteq X \\ Y \not\subseteq X'}} (-1)^{|X-Y|} \sum_{\substack{Z \subseteq Y \\ Z \not\subseteq X'}} g(Z). \end{aligned}$$

Our aim is to show that the three terms above are (respectively) $g(X')$, $-g(X)$ and $g(X)$, and so conclude that the entire expression is equal to $g(X)$.

The first term can be rewritten as

$$\sum_{Y \subseteq X'} (-1)^{|X-Y|} \sum_{Z \subseteq Y} g(Z) = - \sum_{Y \subseteq X'} (-1)^{|X'-Y|} \sum_{Z \subseteq Y} g(Z).$$

Ignoring the negative sign, we have precisely the statement of the proposition for the set X'. By induction, the above is equal to $-g(X')$.

The second term,

$$\sum_{\substack{Y \subseteq X \\ Y \not\subseteq X'}} (-1)^{|X-Y|} \sum_{\substack{Z \subseteq Y \\ Z \subseteq X'}} g(Z),$$

sums over the subsets of X that are not also subsets of X'. By our choice of X', the aforementioned sets induce a sublattice isomorphic to a lattice of subsets of an $n-1$ element set. Since we further restricted the range of Z to count only those subsets that stay within this smaller sublattice, the resulting sum is precisely the same as the statement of the proposition for the sublattice. By induction, the above is equal to $g(X)$.

Arguing similarly, we have also for the third term that

$$\sum_{\substack{Y \subseteq X \\ Y \not\subseteq X'}} (-1)^{|X-Y|} \sum_{\substack{Z \subseteq Y \\ Z \not\subseteq X'}} g(Z) = g(X').$$

Taken together, we see that the sum of the three terms is $g(Y)$, as desired.

($\Leftarrow$) Let X and X' be as before and write

$$\sum_{Y \subseteq X} g(Y)$$

$$= \sum_{Y \subseteq X} \sum_{Z \subseteq Y} (-1)^{|Y-Z|} f(Z)$$
$$= \sum_{Y \subseteq X'} \sum_{Z \subseteq Y} (-1)^{|Y-Z|} f(Z) + \sum_{\substack{Y \subseteq X \\ Y \not\subseteq X'}} \sum_{Z \subseteq Y} (-1)^{|Y-Z|} f(Z)$$
$$= \sum_{Y \subseteq X'} \sum_{Z \subseteq Y} (-1)^{|Y-Z|} f(Z) + \sum_{\substack{Y \subseteq X \\ Y \not\subseteq X'}} \sum_{\substack{Z \subseteq Y \\ Z \subseteq X'}} (-1)^{|Y-Z|} f(Z) + \sum_{\substack{Y \subseteq X \\ Y \not\subseteq X'}} \sum_{\substack{Z \subseteq Y \\ Z \not\subseteq X'}} (-1)^{|Y-Z|} f(Z).$$

Arguing precisely as before, one can show that the above simplifies to

$$-f(X') + f(X) + f(X').$$

Thus, the entire sum is equal to $f(X)$, as desired.

□

Problem 9

I will take a previous homework problem as a lemma (I'm still hoping to work out the details).

Lemma 9. *Let $V = \{x_1, \ldots, x_n\}$ be a finite poset ordered by $\leq$ with the greatest common lower bound property, f be a function from V into $\mathbb{R}$, and $g(x) = \sum_{y \leq x} f(y)$ for all $x \in V$. The matrix*

$$M = (g(x_i \wedge x_j))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$$

has determinant equal to $f(x_1) \cdots f(x_n)$.

Lemma 10. *For any positive integer n,*

$$n = \sum_{d|n} \phi(d),$$

where ϕ is Euler's totient function.

Proof. Let a positive integer n be given. For $a, b \in \{1, \ldots, n\}$ say that $a \sim b$ provided $gcd(a, n) = gcd(b, n)$. It is evident that $\sim$ is an equivalence relation and that there is an equivalence class corresponding to each positive integer d dividing n (call such a class A_d).

Since,

$$\sum_{d|n} \phi(d) = \sum_{d|n} \phi\left(\frac{n}{d}\right),$$

it suffices to show that $|A_d| = \phi\left(\frac{n}{d}\right)$ for all divisors d of n. Given $m \in A_d$, the map $m \mapsto \frac{m}{d}$ is injective and $\gcd(m, n) = d$ implies $\gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$. Thus, $|A_d| \leq \phi\left(\frac{m}{d}\right)$. Similarly, for ℓ relatively prime to d, the map $\ell \mapsto \ell d$ is injective and $\gcd\left(\ell, \frac{n}{d}\right) = 1$ implies $\gcd(\ell d, n) = d$. Thus, $\phi\left(\frac{n}{d}\right) \leq |A_d|$, completing the proof. □

Proposition 11. *The matrix*

$$M = (gcd(i, j))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$$

has determinant equal to $\phi(1) \cdots \phi(n)$, where ϕ is Euler's totient function.

Proof. In the language of the first lemma, V is the set of integers $\{1, \ldots, n\}$ ordered by divisibility, which is a finite poset with the greatest common lower bound property (i.e. the greatest common divisor). The function f will be the Euler totient function, and g will be the identity function. The second lemma gives, for all $n \in V$, $g(n) = \sum_{m \leq n} f(m)$. The conclusion follows from the first lemma. □

Problem 10

Let m and n be relatively prime positive integers and let G be the set $\{xm + yn \mid x, y \in \mathbb{Z}^{\geq 0}\}$.

Proposition 12. *The set G does not contain $mn - m - n$.*

Proof. Suppose, for contradiction, that there exists $x, y \in \mathbb{Z}^{\geq 0}$ such that

$$mn - m - n = xm + yn.$$

Some algebra gives

$$(n - x - 1)m = (y + 1)n.$$

From this expression, we see that $(y+1)n$ is a multiple of both m and n. Since m and n are relatively prime, their least common multiple is mn. Thus,

$$(y + 1)n \geq mn,$$

which is a contradiction with the fact that

$$xm + yn < mn,$$

since both xm and yn are positive terms. □

Proposition 13. *The set G contains all integers strictly greater than $mn - m - n$.*

Proof. We are asked to show that the set G contains $mn - m - n + k$ for all $k \geq 1$. We may further assume that $k \leq \min\{m, n\}$. If we can show the claim for these values of k, we can build up to any larger value of k by incrementing x or y, as appropriate, for each additive copy of m or n.

Choose (possibly negative) integers a and b such that

$$am + bn = k.$$

Note that one of $a > 0$ or $b > 0$ must be true, but not both simultaneously. Moreover, we may always choose a and b such that either one of $|a| < n$ or $|b| < m$ holds, since all of the following are equivalent:

- am + bn = k
- (a-n)m + (b+m)n = k
- (a+n)m + (b-m)n = k.

We now consider two cases.

Case 1: $a > 0$

We know immediately that $b \leq 0$, and we may further insist that $|b| < m$. It follows that

$$\begin{aligned} mn - m - n + k &= mn - m - n + am + bn \\ &= (a - 1)m + (m - 1 + b)n. \end{aligned}$$

Since $|b| < m$ and $a > 0$, the representation above is indeed of form $xm + yn$ with $x, y \in \mathbb{Z}^{\geq 0}$.

Case 2: $b > 0$

We know immediately that $a \leq 0$, and we may further insist that $|a| < n$. It follows that

$$\begin{aligned} mn - m - n + k &= mn - m - n + am + bn \\ &= (n - 1 + a)m + (b - 1)n \end{aligned}$$

Since $|a| < n$ and $b > 0$, the representation above is indeed of form $xm + yn$ with $x, y \in \mathbb{Z}^{\geq 0}$. □

Problem 11

Denote by $K_{2m+r,r}$ the Kneser graph whose vertices are all m-element subsets of a $2m+r$-element set.

Proposition 14. *For all integers* $0 \leq k < n$,

$$\chi(K_{2m+r,r}) \leq r+2.$$

Proof. Let our $2m+r$ element set be the set of integers $\{1, 2, \ldots, 2m+r\}$. Define the following sets of vertices:

$$\begin{aligned}
C_1 &= \{x \in V \mid 1 \in x\} \\
C_2 &= \{x \in V \setminus C_1 \mid 2 \in x\} \\
C_3 &= \{x \in V \setminus (C_1 \cup C_2) \mid 3 \in x\} \\
&\vdots \\
C_{r+1} &= \{x \in V \setminus (C_1 \cup \cdots \cup C_r) \mid r+1 \in x\} \\
C_{r+2} &= V \setminus (C_1 \cup \cdots \cup C_{r+1}).
\end{aligned}$$

We claim that the sets above induce a proper coloring of $K_{2m+r,r}$. For $1 \leq i \leq r+1$, any two vertices within C_i represent sets whose intersection contains at least the element i, and so there is no edge between them. Finally, observe that C_{r+2} is the collection of all m-element subsets of the set $\{r+2, r+3, \ldots, 2m+r\}$. Since the size of this set is $2m-1$, any two m-element subsets must intersect, and so there are no edges lying within C_{r+2}. □

Problem 12

Proposition 15. *In general, s^*-independence does* not *imply s-independence.*

Proof. For a counterexample, let $s = 1$ and consider the family $\mathcal{F} = \{\{x\}, \{y\}, \{x, y\}\}$. We have the 1^*-inclusion matrix

$$I^*(\mathcal{F}, 1) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

The rows are indexed by $\{x, y\}$, $\{x\}$, and $\{y\}$, respectively. The columns are indexed by $\{x\}$, $\{y\}$, and $\emptyset$, respectively. Some algebra shows that $I^*(\mathcal{F}, 1)$ can be put into upper triangular form, and so is linearly independent over any field of characteristic 0.

On the other hand, we have the 1-inclusion matrix

$$I(\mathcal{F}, 1) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix},$$

where the rows and columns are indexed as before (with the exception that the column corresponding to $\emptyset$ is removed). We see that the third row can be represented by the sum of the first and second rows, and so the matrix is not linearly independent. □

Problem 13

Consider the group $(\mathbb{Q}, +_1)$, where addition is carried out modulo 1.

Lemma 16. *Let G be a finite subgroup of $(\mathbb{Q}, +_1)$ and let p and q be relatively prime positive integers. If $\frac{p}{q} \in G$, then $\frac{r}{q} \in G$ for all $0 \leq r < q$.*

Proof. Let $\left(\frac{p}{q}\right)^m$ denote the result of combining m copies of $\frac{p}{q}$ under $+_1$. Since p and q are relatively prime, $\operatorname{lcm}(p, q) = pq$, and so the collection $\left\{\left(\frac{p}{q}\right)^n \mid n \in \mathbb{N}\right\}$ contains q elements. Thus, the aforementioned set is equal to $\left\{\frac{r}{q} \mid 0 \leq r < q\right\}$. □

Proposition 17. *Every finite subgroup of $(\mathbb{Q}, +_1)$ is cyclic.*

Proof. Let G be a finite subgroup of $(\mathbb{Q}, +_1)$ and suppose that the nonzero elements of G are $\frac{p_i}{q_i}$ for $1 \leq i \leq n$, where each pair p_i and q_i are relatively prime positive integers. Let m be the least common multiple of all the q_i. Certainly, every element of G can be represented as $\left(\frac{1}{m}\right)^s$ for some $s \geq 0$. It remains to show that $\frac{1}{m}$ is indeed an element of G.

Let $\{q_i' \mid 1 \leq i \leq n'\}$ be the set distinct denominators appearing in G. By the lemma, $\frac{1}{q_i'}$ is an element of G for all $1 \leq i \leq n'$, and so $\sum_{i=1}^{n'} \frac{1}{q_i'}$ is an element of G. The result of the preceding sum is of the form $\frac{p}{m}$ for some positive integer p relatively prime to m. Applying the lemma again, we see that $\frac{1}{m}$ is an element of G, as desired. □

Problem 14

Proposition 18. *Let L be the lattice of finite subgroups of $(\mathbb{Q}, +_1)$ ordered by the subgroup relation. If elements U, V, X, and Y of the lattice satisfy $|V/U| = |Y/X|$, then the segment $[U, V]$ and $[X, Y]$ are poset isomorphic.*

Proof. By the previous problem, each of U, V, X, and Y are isomorphic to, respectively, the cyclic group $\mathbb{Z}_{m_U}, \mathbb{Z}_{m_V}, \mathbb{Z}_{m_X}, \mathbb{Z}_{m_Y}$, where the m's are each integers. Now, $V/U \cong \mathbb{Z}_{\frac{m_V}{m_U}}$ and $Y/X \cong \mathbb{Z}_{\frac{m_Y}{m_X}}$, and so $|V/U| = |Y/X|$ means that $\frac{m_V}{m_U} = \frac{m_Y}{m_X}$. This fact implies that, in the divisibility lattice, $[m_U, m_V] \cong [m_X, m_Y]$. Since the groups in question are cyclic, we have $[m_U, m_V] \cong [U, V]$, as witnessed by the correspondence associating $m \in [m_U, m_V]$ with $\mathbb{Z}_m \in [U, V]$. Similarly, $[m_X, m_Y] \cong [X, Y]$. Therefore,

$$[U, V] \cong [m_U, m_V] \cong [m_X, m_Y] \cong [X, Y],$$

as desired. □

Problem 15

Proposition 19. *For the lattice L and equivalence relation as in the previous problem, we have the indicence coefficient*

$$\begin{bmatrix} n \\ p, q \end{bmatrix} = \begin{cases} 1 & \text{if } pq = n \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $[U, V]$ be a segment of L with $|V/U| = n$. Let $U \cong \mathbb{Z}_{m_U}$ and $V \cong \mathbb{Z}_{m_V}$. Suppose we are given p and q with $pq = n$. Since the groups in question are all cyclic, the unique group $G \in [U, V]$ such that $|V/G| = p$ and $|G/U| = q$ is $\mathbb{Z}_{\frac{m_V}{p}}$. Observe that, indeed

$$|V/G| = \frac{m_V}{\frac{m_V}{p}} = p,$$

$$|G/U| = \frac{\frac{m_V}{p}}{m_U} = \frac{m_V}{p \cdot m_U} = \frac{n}{p} = q.$$

Using similar observations, we see that there is no such group whenever $pq \neq n$. □

Problem 16

Lemma 20. *(Radon's Lemma) For any $d+2$ points in $\mathbb{R}^d$, there exists a partition of the points into two sets A and B such that the convex hull of A intersects the convex hull of B.*

Proof. Let X be a collection $\{x_1, \ldots, x_{d+2}\}$ of $d+2$ points in $\mathbb{R}^d$. Since these points are affinely independent, we can choose a nontrivial affine combination. That is, we can find real numbers a_i (not all zero) such that

$$\sum_{i=1}^{d+2} a_i = 0$$

and

$$\sum_{i=1}^{d+2} a_i x_i = 0.$$

Let now $A = \{x_i \mid a_i > 0\}$ and $B = \{x_i \mid a_i < 0\}$. Note that both sets are nonempty. We construct a point belonging to both the convex hull of A and the convex hull of B. To that end, define

$$a = \sum_{\{i|x_i \in A\}} a_i$$

and consider the point

$$x = \sum_{\{i|x_i \in A\}} \frac{a_i}{a} x_i.$$

The coefficients $\frac{a_i}{a}$ are all positive and sum to 1, and so x is indeed in the convex hull of A.

Now,

$$\begin{aligned} 0 &= \sum_{i=1}^{d+2} \frac{a_i}{a} x_i \\ &= \sum_{\{i|x_i \in A\}} \frac{a_i}{a} x_i + \sum_{\{i|x_i \in B\}} \frac{a_i}{a} x_i \\ &= x + \sum_{\{i|x_i \in B\}} \frac{a_i}{a} x_i, \end{aligned}$$

and so

$$x = -\sum_{\{i|x_i \in B\}} \frac{a_i}{a} x_i.$$

The coefficients $-\frac{a_i}{a}$ are all positive. They will be a convex combinations of points in B provided their sum is 1. This follows from the observation that

$$\begin{aligned} 0 &= \sum_{i=1}^{d+2} a_i \\ &= \sum_{\{i|x_i \in A\}} a_i + \sum_{\{i|x_i \in B\}} a_i \\ &= a + \sum_{\{i|x_i \in B\}} a_i, \end{aligned}$$

and so

$$a = -\sum_{\{i|x_i \in B\}} a_i.$$

□

Problem 17

Let $(P, \leq_P)$ be a poset and let G be the group of poset automorphisms on P. Define the quotient poset P/G whose vertices are the orbits of P. For vertices U and V in P/G, we say $U \leq_{P/G} V$ provided there exists $u \in U$ and $v \in V$ such that $u \leq_P v$.

Proposition 21. *The order $\leq_{P/G}$ defined above is indeed a partial order.*

Proof. We show that $\leq_{P/G}$ is reflexive, antisymmetric, and transitive.

Reflexive: Let U be a vertex of P. We want that $U \leq_{P/G} U$. That is, we want to find $u \in U$ and $u' \in U$ such that $u \leq_P u'$. As P itself is reflexive, we may take $u = u'$.

Antisymmetric: Let U and V be vertices of P and assume both $U \leq_{P/G} V$ and $V \leq_{P/G} U$. That is, there exists $u \in U$ and $v \in V$ such that $u \leq_P v$ and also there exists $v' \in V$ and $u' \in U$ such that $v' \leq_P u'$.

We desire to show $U = V$. To that end, let f be an automorphism of P satisfying $u \leftrightarrow u'$ and $v \leftrightarrow v'$. We see that $v' \leq_P u'$ if and only if $f(v') \leq_P f(u')$ if and only if $v \leq_P u$. Since P is antisymmetric, we have $u = v$. Since orbits of a poset are equivalence classes, it follows that $U = V$.

Transitive: Let U, V, and W be vertices of P and assume both $U \leq_{P/G} V$ and $V \leq_{P/G} W$. That is, there exists $u \in U$ and $v \in V$ such that $u \leq_P v$ and also there exists $v' \in V$ and $w \in W$ such that $v' \leq_P w$.

We desire to show that $U \leq W$. To that end, let f be an automorphism interchanging v and v' and fixing w (if one of v or v' is w, then there is nothing to show). We see that $v' \leq_P w$ if and only if $f(v') \leq_P f(w)$ if and only if $v \leq_P w$. Since P is transitive, we have $u \leq_P w$, which means that $U \leq_{P/G} W$. □

Problem 18

Proposition 22. *For a finite family $\mathcal{F}$ of finite sets,*

$$\mathrm{VCdim}(\mathcal{F}) \leq \log_2 |\mathcal{F}|.$$

Proof. Let S be a set that is shattered by $\mathcal{F}$. We show that $|S| \leq \log_2 |\mathcal{F}|$.

Since S is shattered by $\mathcal{F}$, we know that $\mathcal{P}(S) = T_{\mathcal{F}}(S)$. We know also that $|T_{\mathcal{F}}(S)| \leq |\mathcal{F}|$, as each set of $\mathcal{F}$ contributes at most one new element to the trace. It follows that

$$2^{|S|} = |\mathcal{P}(S)| \leq |T_{\mathcal{F}}(S)| \leq |\mathcal{F}|,$$

and so

$$|S| \leq \log_2 |\mathcal{F}|.$$

□