Combinatorics and Graph Theory II (Math 689). Spring 2000. Problems and Solutions.

July 19, 2000

PREFACE

These are the problems suggested as homework in a graduate course Combinatorics and Graph Theory II (Math 689) taught at the University of Delaware in Spring, 2000.

Each student was responsible for two or three problems which were assigned randomly. Sometimes the same problem was assigned to several people. The solutions had to be submitted in a form of a Latex file. I read them and returned to the authors with comments. Sometimes it took several iterations to produce the final document.

I would like to thank David Chandler, Carl Devore, Vasyl Dmytrenko, Frank Fiedler, David Kravitz, Sukhendu Mehrotra, Sven Reichard and Jason Williford – the students from this class who submitted solutions. Often their work was very original and many solutions differed completely from those I had in mind. And there were several problems on which I never worked myself.

Hopefully all solutions included in this document are correct, but the whole set is by no means polished. Special thanks go to David Kravitz who helped me to prepare this version. I will appreciate all comments. Please send them to `lazebnik@math.udel.edu`.

– Felix Lazebnik

. . .
If you can hear the music
Why don't you help me sing?

– *Leonard Cohen*

. . .
but when I could not sleep
I learned to write
I learned to write
what might be read
on nights like this
by one like me.

– *Leonard Cohen*

Problem 1. *Let G be a graph of order $n \geq 1$. Find a lower and an upper bounds on $e = e(G)$ if G*

(i) is connected; is not connected;

(ii) has exactly c, $1 \leq c \leq n$, connected components;

(iii) is Hamiltonian; is not Hamiltonian;

(iv) contains no P_k – a path with $k \geq 1$ edges.

Proof. (by Vasyl Dmytrenko)

(i) G is connected iff there is a spanning tree T of G with $e(T) = n - 1$. Hence, $n - 1 \leq e(G) \leq \binom{n}{2}$, and both bounds are exact.

Suppose G is not connected. Let $G = G_1 \sqcup G_2$ (disjoint union), $v(G_1) = k$, $v(G_2) = n - k$. Then $e \leq \binom{k}{2} + \binom{n-k}{2} = k^2 - nk + \frac{n^2-n}{2}$. Since the function $f(x) = x^2 - nx + \frac{n^2-n}{2}$ decreases on $[1, n/2]$ and increases on $[n/2, n-1]$, the upper bound is $f(1) = f(n-1) = \binom{n-1}{2} = \frac{(n-1)(n-2)}{2}$. Thus, $0 \leq e \leq \frac{1}{2}(n-1)(n-2)$. Again, both bounds are evidently exact. The upper bound is attained by $K_{n-1} \sqcup K_1$ only.

(ii) Let $G_1, G_2, \ldots, G_c$ be the components of G, $v(G_i) = k_i$, $i = 1, \ldots, c$. Since each G_i is connected, by (i) $e(G_i) \geq k_i - 1$, and $e \geq e(G_1) + \cdots + e(G_c) = (k_1 - 1) + \cdots + (k_c - 1) = k_1 + \cdots + k_c - c = n - c$.

Now suppose that G has maximal possible number of edges e. Take any two components G_i and G_j. Then by (i) one of k_i or k_j is 1 (otherwise, we could replace the pair G_i, G_j by $K_1, K_{k_i+k_j-1}$ and increase $e(G_i) + e(G_j)$ and, therefore, e). Hence, $G_i = K_1$ for all i except one, say, $i = c$, and $G_c = K_{n-c+1}$ if G is an extremal graph, and $n - c \leq e \leq \binom{n-c+1}{2}$.

(iii) If G is Hamiltonian, then G contains an n-cycle. Therefore, $n \leq e \leq \binom{n}{2}$, and C_n and K_n are examples of extremal graphs for these bounds.

If G is not Hamiltonian, then $0 \leq e \leq \binom{n-1}{2} + 1$. The lower bound is obvious. Let us prove the upper bound. We present two proofs of this fact (by Felix Lazebnik).

Proof 1 (without Ore's Theorem).

We show that every graph of order $n \geq 3$ with *at least* $\binom{n-1}{2} + 2$ edges is Hamiltonian. Notice that the upper bound cannot be lowered, since a graph obtained from a copy of K_{n-1} by adding one new vertex and joining this vertex to one of the vertices of K_{n-1} is not Hamiltonian (contains a vertex of degree 1).

The statement is correct for $n = 3$, since the only graph of order 3 and size ≥ 3 is C_3 which is Hamiltonian. Therefore we assume that the statement is correct for $n = k \geq 3$

Let G be a graph of order $k+1$ with $\geq \binom{k}{2}+2$ edges. If $G = K_{k+1}$, then G is Hamiltonian. If $G \neq K_{k+1}$, then we show that G has a vertex u such that $k/2 < d_G(u) \leq k-1$. Suppose the contrary. Then all vertices of G have degrees either less than $k/2$, or at least k. Since G is of order $k+1$, there are no vertices with degrees greater than k. Let G have a vertices of degree k and b vertices of degree less than $k/2$. Then $a+b = v(G) = k+1$ and

$$k^2 - k + 4 \leq 2e(G) \leq ak + bk/2 = ((a+b)k + ak)/2 = ((k+1)k + ak)/2.$$

Therefore $k^2 - k + 4 \leq ((k+1)k + ak)/2 \iff k - 3 + 8/k \leq a \iff a \geq k-2$. So G has at least $k-2$ vertices joined to all other vertices (i.e., of degree k). Therefore every vertex of G is joined to at least $k-2$ others, so $d_G(x) \geq k-2$ for all $x \in V(G)$. Since $k-2 \geq k/2$ for $k \geq 4$, $b = 0$. But then $a = k+1$ and $G = K_{k+1}$ – a contradiction. Therefore the desired vertex u exists.

Then graph $G-u$ is of order k and size at least $\binom{k}{2}+2$. By inductive hypothesis it is Hamiltonian.

Let $v_1 v_2 \dots v_k$ be a Hamiltonian cycle in $G-u$. Since u is connected to more than half vertices of the cycle, it is connected to at least two *consecutive* vertices of the cycle, say v_i and v_{i+1} (indices are taken modulo n). Then $xv_i v_{i-1} \dots v_1 v_n \dots v_{i+1} x$ is a Hamiltonian cycle in the obtained graph. □

Proof 2 (with Ore's Theorem).

Let G be of order $n \geq 3$ and size at least $\binom{n-1}{2}+2$. We prove that for any non-edge xy of G, $d_G(x) + d_G(y) \geq n$. Then by Ore's Theorem, G is Hamiltonian. Let G^c be the complement of G. Then $d_G(x) + d_G(y) \geq n \iff d_{G^c}(x) + d_{G^c}(y) \leq n-2$. But $e(G^c) = \binom{n}{2} - e(G) \leq n-3$. Since $v(G^c) = n$ and xy is an edge of G^c, then $e(G^c) \leq n-3$ implies $d_{G^c}(x) + d_{G^c}(y) \leq n-2$. □

(iv) Now suppose that G contains no P_k for some k, $1 \leq k < n$. We show that $0 \leq e \leq \frac{1}{2}(k-1)n$. The lower bound is obvious, and we will prove the upper bound. We use the same idea as in the proof of Ore's Theorem on the existence of a Hamiltonian cycle in a graph.

Lemma 1. *If C is a connected component of G and $|V(G)| \geq 3$, then there exist two non-adjacent vertices x and y such that $d(x) + d(y) < k$.*

Proof. Suppose that for any two non-adjacent vertices x and y of C, $d(x) + d(y) \geq k$. Let $P = x_1 \dots x_l$ be a longest path in C, and let $S = \{x_1, \dots x_l\}$.

First, show that $x_1 x_l \notin E(G)$. Indeed, if $x_1 \dots x_l$ is a cycle, then for any i the neighborhood $N(x_i) \subseteq S$. Otherwise, $y \in N(x_i) \setminus S$ implies $yx_i x_{i+1} \dots x_l x_1 \dots x_{i-1}$ is a path of length $l+1$. Hence, $S = V(G)$, and P is Hamiltonian. Note also that $N(x_1) \subseteq S$ and $N(x_l) \subseteq S$.

Let $M := \{x_i | x_{i-1}x_l \in E(C)\}$. Then $N(x_1) \cap M = \emptyset$. Indeed, if $x_i \in N(x_1) \cap M$, then $x_1x_i, x_{i-1}x_l \in E(G)$, and $x_1x_2 \dots x_{i-1}x_l x_{l-1} \dots x_i$ is a cycle of length l, that is impossible by the above. Therefore, $N(x_1) \sqcup M \subseteq S \setminus \{x_1\}$, and $k \leq d(x_1) + d(x_l) \leq l-1$ imply $l \geq k+1$, a contradiction. □

Now we prove that $e \leq \frac{1}{2}(k-1)n$ by induction on n. For $n \leq 2$ the statement is evident. Let $n > 2$, and let k be a fixed number. If $n \leq k$, then $e \leq \binom{n}{2} \leq \frac{1}{2}(k-1)n$. Suppose that the statement holds for all graphs of order $< n$. Let $|V(G)| = n$. If G is disconnected, the inequality follows from the induction hypothesis. If G is connected, by the lemma $\exists x, y \in V(G)$ such that $d(x) + d(y) < k$. Therefore, for one of them, say, x, $d(x) \leq \frac{k-1}{2}$. Then $e \leq d(x) + e(G-x) \leq \frac{k-1}{2} + \frac{k-1}{2}(n-1) = \frac{k-1}{2}n$.

□

Remark 1. It was conjectured by P. Erdős and V. Sós (1963) that if $e(G) > \frac{k-1}{2}n$, then G contains <u>every</u> tree with k edges.

Problem 2. *Look carefully through the derivation of the lower bound for $c_3(v, e)$ that we did in class. Analyze when "=" occurs. Use it to prove that the only extremal graph on v vertices with $e = \left\lfloor \frac{v^2}{4} \right\rfloor$ edges is $K_{n,n}$, if $v = 2n$, and $K_{n,n+1}$, if $v = 2n+1$.*

Proof. (by Felix Lazebnik)

Recall the proof of the inequality $c_3(v, e) \geq \frac{4e}{3v}\left(e - \frac{v^2}{4}\right)$. It contains the following "steps":

$$c_3(v, e) \geq c_3(G) = \frac{1}{3} \sum_{\{x,y\} \in E(G)} (d(x) + d(y) - |Nbh(x) \cup Nbh(y)|) \geq$$

$$\frac{1}{3} \sum_{\{x,y\} \in E(G)} (d(x) + d(y) - v) \geq \dots \geq \frac{4e}{3v}\left(e - \frac{v^2}{4}\right)$$

<u>Case 1: $v = 2n$</u>. For our graph, both $c_3(G)$ and $\frac{4e}{3v}\left(e - \frac{v^2}{4}\right)$ are $= 0$. Therefore, for any edge $\{x, y\}$ of G, $Nbh(x) \cup Nbh(y) = V(G)$. Therefore G is bipartite with partitions $Nbh(x)$ and $Nbh(y)$, since an edge between vertices from $Nbh(x)$ or between vertices from $Nbh(y)$ would produce a triangle in G. Let $|Nbh(x)| = a$, $|Nbh(y)| = b$. Then G is a <u>subgraph</u> in $K_{a,b}$, and $a + b = v$. Then $e(G) \leq e(K_{a,b}) = a \cdot b \leq \left(\frac{a+b}{2}\right)^2 = \left(\frac{v}{2}\right)^2$. But $e(G) = \left\lfloor \frac{v^2}{4} \right\rfloor$, so $\left\lfloor \frac{v^2}{4} \right\rfloor \leq ab \leq \frac{v^2}{4}$. Since ab is an integer, then $ab = \left\lfloor \frac{v^2}{4} \right\rfloor$, and since G is a subgraph of $K_{a,b}$, then $G \cong K_{a,b}$. On the other hand it is easy to see that $a + b = v$ and

$ab = \left\lfloor \frac{v^2}{4} \right\rfloor$ implies that integers $a, b, a \leq b$, are $(a,b) = \left(\frac{v}{2}, \frac{v}{2}\right)$ if v is even and $(a,b) = \left(\left\lfloor \frac{v}{2} \right\rfloor, \left\lfloor \frac{v}{2} \right\rfloor + 1\right)$ if v is odd. □

Case 2: $v = 2n+1$. In this case $v(G) = 2n+1, e(G) = n(n+1)$ and G has no triangles. The average degree of G is $\frac{2n(n+1)}{2n+1} = n + \frac{n}{2n+1}$. So there exists a vertex x such that $d_G(x) \leq n$. Let $G' = G \setminus \{x\}$. Then $v(G') = 2n, e(G') \geq n^2$ and G' has no triangles.

According to Case 1 above, $G' \cong K_{n,n}$ and $e(G') = n^2$. So $d(x) = n$. Since G' is triangle–free, then $Nbh_G(x)$ is one of the two maximal independent sets of $K_{n,n}$. This implies that $G \cong K_{n+1,n}$. □

Problem 3. *Let $v(G) = 2n$, $e(G) n^2$, but $G \ncong K_{n,n}$, $n \geq 2$. Prove that G contains at least $n-1$ triangles.*

Proof. (by David Chandler)

The proof is by induction. With one exception, there are only two graphs with $|V(G)| = 2n$, $|E(G)| = n^2$, but $G \ncong K_{n,n}$, and no more than $n-1$ triangles. One is $K_{n+1,n-1}$, with one additional edge between vertices of the $n+1$ partition. The other is $K_{n,n}$, with one vertex disconnected from one of its neighbors and reconnected to a vertex in the same partition.

The exception, or $n = 3$, is a 3–regular graph with two disjoint triangles, and three more edges connecting them. The statement is clear for $n = 2$ and $n = 3$. We assume the statement for n and show that it is true for $n+1$. We are given a graph with $2n+2$ vertices and $n^2 + 2n + 1$ edges. Since it is not the $(n+1)$–regular bipartite graph, it must contain a triangle. We choose a vertex of a triangle which has minimal degree. If the minimal degree is greater than $n+1$, then there must be two other vertices with degree no more than n, because the average degree is $n+1$. Also, two vertices from a triangle must have at least two common neighbors, not just one, because the sum of their degrees is at least $2n+4$ and there are only $2n$ other vertices. We delete 2 vertices from the graph with no more than $2n$ edges, and one more edge from a triangle, reducing the number of triangles by at least two. By the induction hypothesis, if we started with no more than n triangles, we must be down to the complete regular bipartite graph with no triangles.

In the second case, if there is a triangle with a vertex of degree $n+1$ or less, we delete that vertex. If we deleted $n+1$ edges, the average degree is now less than $n+1$ and we can delete a vertex of degree no more than n. If we deleted fewer than $n+1$ edges first, then the average degree is still less than $n+2$ and we can delete a vertex of degree no more than $n+1$. By the induction hypothesis, we again have either $K_{n,n}$, $K_{n,n}$ with one end of one edge moved, $K_{n+1,n-1}$ with the extra edge, or the exception for $n = 3$.

Note that in each case we have deleted $2n+1$ edges, not fewer, because we got an extremal graph.

We now ask what graph we could get if we add back the two vertices and $2n+1$ edges. In the exceptional case, the largest independent set has only two vertices, so we cannot add a vertex of degree 4 or two vertices of degree 3 without forming at least 2 more triangles.

In case one, we first add back one edge to $K_{n,n}$ to produce n triangles. The only way to add back to two degree n vertices without making more triangles is to connect them to the remaining n partition, forming $K_{n+2,n}$ plus one edge, as claimed. Note that the minimum degree of a vertex in a triangle is not really greater than $n+1$.

In case two, if we start with $K_{n,n}$ and add back a vertex of degree greater than $n+1$, we get more than n triangles. If we add back a vertex of degree $n+1$ we get at least n triangles, and that only by connecting to every vertex in one partition and to one vertex in the other partition. To avoid additional triangles, the second vertex must also be connected to all the vertices in the first partition, or to the vertices of the second partition, avoiding one of the two that are connected. We again form one of the extremal graphs.

If we start with $K_{n+1,n-1}$, plus one edge, we are allowed only one additional triangle. The only way to add a degree $n+1$ vertex without creating two triangles is to connect it to every vertex of the $n+1$ partition. Any greater degree would create more triangles. The other vertex has to be connected to n independent vertices, either the n–partition, forming $K_{n+2,n}$ plus one edge, or to the $(n+1)$–partition, skipping one of the joined vertices, forming the other extremal graph.

If we start with $K_{n,n}$ with one end of one edge moved, adding a vertex of degree $n+1$ adds at least $n-1$ triangles, and the case $n=2$ reverts to $K_{3,1}$ plus one edge.

The other final possibility is that the two deleted vertices were connected to each other and both have degree n to the reduced graph. If we have $K_{n,n}$, we do not want to get $K_{n+1,n+1}$, so at least one of the vertices must be connected to both partitions, or they must both be connected to all the points of the same partition, one of our graphs. If it were connected to two or more points from each partition, we would get more than n triangles already unless $n=4$, in which case adding the second vertex adds triangles. So we have $K_{n+1,n}$ with one edge moved to $n+1$ forming $n-1$ triangles. By symmetry, the second vertex cannot be joined to all the vertices not connected to the first without forming a second set of $n-1$ triangles. If $n=2$ we get the exceptional case. Otherwise the second vertex is connected to the first plus an independent set, only one vertex of which is a neighbor of the first. We have $K_{n+1,n+1}$ with one edge moved.

If we have $K_{n+1,n-1}$ plus one edge, or $K_{n,n}$ with one edge moved, we can add only one triangle. We add back the two connected vertices so that they can have at most one common neighbor. In the case of $K_{n+1,n-1}$ plus one edge, one vertex must be connected to both partitions of $K_{n+1,n-1}$, forming at least $n-1$ triangles. Therefore $n=2$ but we can treat $K_{3,1}$ plus an edge as $K_{2,2}$ with an edge moved.

In the case of $K_{n,n}$ with one edge moved, we could connect one of the vertices

to every vertex of one partition and the other vertex to the other partition of vertices. We now have the same graph with n increased by one. Still with no common neighbors suppose each point is connected to $n-1$ vertices of one partition and one vertex of the other. Then we have added $n-1$ and $n-2$ triangles respectively and again $n=2$. The graph is the same as the previous one for $n=2$ with the vertices relabeled. Since if each of the added vertices is connected to at least two vertices in each partition of $K_{n,n}$ minus an edge, we definitely have more than one extra triangle, the only other possibility is to have two independent sets of n vertices intersecting in one point. There is only one candidate for such a point, and only if $n=2$. We get the exceptional case.

The proof is complete.

□

Proof. (by Sukhendu Mehrotra)

The proof is by induction. Assume the result is true for all $m \leq n-1$. Let G be a graph of order $2n$ and size n^2, not isomorphic to $K_{n,n}$. We may assume G has an edge xy which is not a side of a triangle in G, for if no such edge exits, assuming all triangles to be edge-disjoint, we get a lower bound of $\lfloor \frac{n^2}{3} \rfloor \geq (n-1)$ triangles. Consider the graph $G' = G - x - y$. Since x and y have no common neighbour, G' has at least $n^2 - (2n-1) = (n-1)^2$ edges.

First consider the case when G' has exactly $(n-1)^2$ edges. If G' is isomorphic to $K_{n-1,n-1}$ then one of x and y, say x, must be a common neighbour of two vertices a and b lying in opposite sets of the bipartition of G', for if not, x and the neighbours of y in G', and y and neighbours of x in G' give a bipartition of G, implying that G was isomorphic with $K_{n,n}$ to start with. Since y has $n-1$ neighbours in G', this implies, y must also be a common neighbour of two vertices lying in opposite sets of the bipartition of G'. It is then clear that both x and y are vertices of at least $n-2$ triangles in G.

If G' is not isomorphic with $K_{n-1,n-1}$, by the induction hypothesis, it has at least $n-2$ triangles. As above, the neighbours of x and y cannot both be independent sets of vertices in G' and so there must be at least one other triangle in G with either x or y as a vertex.

Let us now assume that G' has more than $(n-1)^2$ edges. Then, clearly, by the induction hypothesis, G' has at least $n-2$ triangles. Let ab be an edge of a triangle in G'. $H = G' - ab$ is either isomorphic with $K_{n-1,n-1}$ or it is not. If it is, clearly $H \cup ab$ has $n-1$ triangles. If it is not, then it must contain at least $n-2$ triangles by the induction hypothesis, and so, counting the triangle that ab is an edge of, G' must have at least $n-1$ triangles. This completes the proof. □

Problem 4. *Let n, p be positive integers and $3 \leq p \leq n$. Let $T(n, p-1)$ denote the Turan graph, i.e., the complete $(p-1)$-partite graph of order n with partition*

sizes as equal as possible, i.e., the number of vertices in every two partitions are equal or differ by 1.

(i) Prove that Turan's graph is unique

(ii) Prove that for every $(p-1)$-partite graph G of order n, $e(G) \leq e(T(n,p-1))$. Then show that $e(G) = e(T(n,p-1))$ if and only if $G \cong T(n,p-1)$.

(iii) Prove that $\binom{p-1}{2} + e(T(n-p+1,p-1)) + (p-2)(n-p+1) = e(T(n,p-1))$.

Proof. (by David Kravitz)

(i) Suppose we have two different Turan graphs, one having x partitions with $a-1$ vertices (and $p-1-x$ having a vertices), the other having y partitions with $b-1$ vertices (and $p-1-y$ with b vertices).

$$x(a-1) + (p-1-x)a = n = y(b-1) + (p-1-y)b$$

$$\Rightarrow (p-1)a - x = (p-1)b - y$$

$$\Rightarrow (p-1)(a-b) = x - y$$

Since $0 \leq |x-y| < p-1$, we know that $(a-b) = 0$ and thus $a = b$. But then $x - y = 0 \Rightarrow x = y$. Therefore, Turan's graph is unique, as both graphs are the same.

(ii.) Suppose we have a complete $(p-1)$-partite graph $G \ncong T(n,p-1)$, so we know by previous part that while one partition P has x vertices, another partition Q has $x-2$ or less vertices. Let us move a vertex v from P to Q, changing edges as is appropriate. While every other edge in G remains unchanged, v will lose $x-2$ or less neighbors in Q, then gain $x-1$, the number of vertices left in P. Therefore, we have constructed a $(p-1)$-partite graph with more edges than G. Thus, any complete $(p-1)$-partite graph $G \ncong T(n,p-1)$ of order n with one partition having 2 or more vertices than another has fewer edges than another $(p-1)$-partite graph. Since any non-complete graph will only have fewer edges than G, we have proven that for any $(p-1)$-partite graph G with n vertices $e(G) < e(T(n,p-1))$ whenever $G \ncong T(n,p-1)$.

Since a maximum number of edges over all $(p-1)$-partite graphs must exist, and an extremal graph cannot be anything other than $T(n,p-1)$, we know that this is the only extremal graph.

(iii.) First suppose that every partition has only one vertex. The new graph would have 0 vertices and edges. This also means that $p-1$ equals n, so

$$\binom{p-1}{2} + e(T(n-p+1,p-1)) + (p-2)(n-p+1) =$$

$$\binom{p-1}{2} + 0 + (p-2)(n-n) = \binom{p-1}{2}$$

This is clearly the number of edges we started with. Therefore, we are done if no partition of the graph has more than one vertex. Thus, suppose that some partition has more than one. We delete $p-1$ vertices, one from each partition. Clearly, the resulting graph is $T(n-p+1, p-1)$, as we have $n-p+1$ vertices in $p-1$ partitions (some may be empty if the partition started with one vertex) and any two partitions have numbers of vertices either equal or differing by 1. Therefore the number of edges we removed in deletion of these vertices is equal to $e(T(n,p-1)) - e(T(n-p+1,p-1))$. Let us now count how many edges were removed.

There are two ways an edge could have been removed. Either (1) the edge was incident with two of the $p-1$ vertices we removed, or (2) it was incident with one of those and another vertex.

(1) Since every one of the $p-1$ vertices was adjacent to every other one, there were a total of $\binom{p-1}{2}$ edges of this type.

(2) Now, every one of the $n-p+1$ vertices not removed was adjacent to all but one of the vertices we removed (the one in its own partition was not a neighbor, all others were). This means that we removed $(p-1)-1 = p-2$ edges for each of the $n-p+1$ vertices, and thus we removed a total of $(n-p+1)(p-2)$ edges of the second type. Hence

$$e(T(n,p-1)) - e(T(n-p+1,p-1)) = \binom{p-1}{2} + (n-p+1)(p-2)$$

$$\Rightarrow \binom{p-1}{2} + e(T(n-p+1,p-1)) + (p-2)(n-p+1) = e(T(n,p-1))$$

□

Problem 5. *Let G be a graph with average degree $\bar{d} > 0$, $|V(G)| = n$.*

i. Show that there always exist $x, y \in V(G)$ such that xy is an edge of G and $\frac{1}{2}[d(x) + d(y)] \geq \bar{d}$.

ii. Is there always a non-edge with the same property?

iii. Is there always an edge $xy \in E(G)$ such that $\frac{1}{2}[d(x) + d(y)] \leq \bar{d}$?

iv. Is there always a non-edge xy such that $\frac{1}{2}[d(x) + d(y)] \leq \bar{d}$?

Proof. (by Jason Williford)

i. Assume the contrary, i.e. that $\forall xy \in E(G)$, $\frac{1}{2}[d(x) + d(y)] < \bar{d}$. Then

$$\sum_{xy \in E(G)} \frac{1}{2}[d(x) + d(y)] < |E(G)|\bar{d}$$

In the summation above $d(x)$ will appear for every edge with x as an endpoint, i.e. $d(x)$ times. Thus we obtain $\sum_{x \in V(G)} (d(x))^2 < n(\bar{d})^2$, a contradiction as

$$\sum_{x \in V(G)} ((d(x))^2 \geq n\bar{d}^2$$

by Jensen's Inequality for the function $f(t) = t^2$.

One verification of this (suggested by Dr. Bellamy) is to consider a random variable X which takes on each of the values $d(x)$ for $x \in V(G)$ with probability $\frac{1}{n}$. $\mathrm{Var}(X) = \sum_{x \in V(G)} \frac{1}{n}(d(x))^2 - \bar{d}^2$, and $\mathrm{Var}(X) \geq 0$.

Therefore such an edge exists in any graph G.

ii. Consider a graph H with vertex set $V = \{1, 2, 3\}$ and edge set $E(G) = \{\{1, 2\}\}$. The average degree of H is $\bar{d} = \frac{2}{3}$, but for the only non-edges $\{1, 3\}$ and $\{2, 3\}$, $\frac{1}{2}(d(1) + d(3)) = \frac{1}{2}(d(3) + d(2)) \leq \frac{2}{3}$. Therefore no such non-edge exists in general for all graphs with non-edges. (Note: to make it more interesting for this part and the last part only I assumed we were only working with graphs that have non-edges, otherwise if G is allowed to be complete this is trivially false as G would have no non-edges).

iii. Let H be defined as before. For the only edge $\{1, 2\}$ of H, $\frac{1}{2}(d(1) + d(2)) = 1 \geq \frac{2}{3}$. Therefore no such edge exists in general for all G.

iv. Let G have at least one non-edge. Consider the complement of G denoted here by G', with average degree $\bar{d}'$, and vertex degrees denoted by $d'(x)$. By our previous result, there exists an edge xy of G' such that $\frac{1}{2}[d'(x) + d'(y)] \geq \bar{d}'$. This implies that there is a non-edge of G such that

$$\frac{1}{2}[2n - 2 - d(x) - d(y)] \geq \ n - 1 - \bar{d}.$$

This implies $\frac{1}{2}[d(x) + d(y)] \leq \bar{d}$.

(Again, this result assumes G has non-edges. If G is allowed to be complete, the statement is actually false).

□

Problem 6. *Let $v = |V(G)|$, $e = |E(G)|$, $m \geq 2$, and G does not contain a subgraph isomorphic to $K_{2,m}$.*

(i) Prove that $\displaystyle\sum_{x \in V(G)} \binom{d(x)}{2} \leq (m-1)\binom{v}{2}$.

(ii) Deduce from that $e \leq \dfrac{\sqrt{m-1}}{2} v^{\frac{3}{2}} + \dfrac{v}{4}$.

(iii) Show that, given a set of n points in the plane, the number of pairs of points at distance exactly 1 is at most $\dfrac{n^{\frac{3}{2}}}{\sqrt{2}} + \dfrac{n}{4}$.

(iv) Given a set A of points in the plane, let $f(A)$ be the number of pairs of points in A that are at distance 1. Let $f(n) = \max\{f(A) \mid |A| = n\}$. The inequality in part (iii) gives an upper bound on $f(n)$. Can you suggest a good lower bound for $f(n)$?

Proof. (by Frank Fiedler)

(i) Let $D_2(G)$ denote the number of different paths of length 2 in G. Every such path yxz determines x uniquely ($x, y, z \in V(G)$). Summing over all vertices $x \in V(G)$, every (unordered) pair $\{y, z\}$ of neighbors of x gives a path of length 2 from y to z via x (cf. Figure 1). Clearly, every path is just counted once. Hence

$$D_2(G) = \sum_{x \in V(G)} \binom{d(x)}{2}.$$

On the other hand, every pair $\{y, z\}$ of vertices determines as many paths

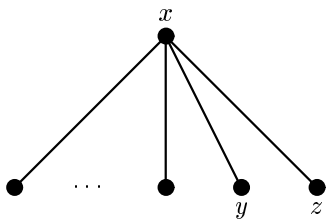

Figure 1: Neighborhood of x

of length 2 as the number of common neighbors of y and z. Since G does not contain a $K_{2,m}$, any two vertices have at most $(m-1)$ neighbors in common (cf. Figure 2). Thus

$$\sum_{x \in V(G)} \binom{d(x)}{2} \leq (m-1)\binom{v}{2}$$

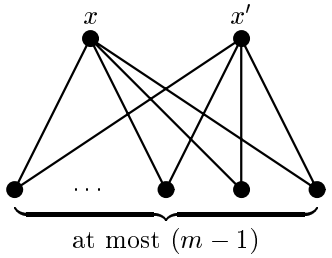

Figure 2: Neighborhood of x

(ii) By Jensen's inequality, for the function $f(t) = \binom{t}{2}$ on $[0, \infty]$.

$$\begin{aligned}
v\binom{\frac{2e}{v}}{2} &\leq \sum_{x \in V(G)} \binom{d(x)}{2} \leq (m-1)\binom{v}{2} \\
\frac{v}{2}\frac{2e}{v}\left(\frac{2e}{v} - 1\right) &\leq (m-1)\frac{v(v-1)}{2} \\
e^2 - \frac{1}{2}ev &\leq (m-1)\frac{v^2(v-1)}{4} \\
\left(e - \frac{v}{4}\right)^2 &\leq (m-1)\frac{v^2(v-1)}{4} + \frac{v^2}{16} \\
&= (m-1)\frac{v^3}{4} - v^2\left(\frac{1}{16} - \frac{m-1}{4}\right)
\end{aligned}$$

Since $m \geq 2$, then $v^2(\frac{1}{16} - \frac{m-1}{4}) < 0$. Hence

$$\left(e - \frac{v}{4}\right)^2 < (m-1)\frac{v^3}{4}$$

and

$$e < \frac{\sqrt{m-1}}{2}v^{\frac{3}{2}} + \frac{v}{4}$$

(iii) Let S be a set of n points $\{P_1, \ldots, P_n\}$ in the plane. Let $H(S)$ be the graph with vertex set $\{v_1, \ldots, v_n\}$ and an edge between v_i and v_j iff the distance from P_i to P_j is 1.

Given three points in the plane, there is at most one point (in the plane) that has distance 1 to all of them. Hence $H(S)$ does not contain a $K_{2,3}$ and therefore

$$\begin{aligned}
|E\left(H(s)\right)| &\leq \frac{\sqrt{3-1}}{2}n^{\frac{3}{2}} + \frac{n}{4} \\
&= \frac{n^{\frac{3}{2}}}{\sqrt{2}} + \frac{n}{4}
\end{aligned}$$

(iv) Using triangles, it is always possible to arrange n points in a way so that we get $2n-3$ points at distance 1. For $n=7$ this can be improved to $12 = 2 \cdot 7 - 2$ (a hexagon and its center).

Remark. David Chandler suggested the following superlinear bound. Let $n = \sum a_i 3^i$, $a_i \in \{0,1,2\}$, be the representation of n in base 3. Then $f(n) \geq \sum_{i>j} a_i a_j 3^j + \sum i a_i 3^i + \sum \frac{a_i^2 - a_i}{2} 3^i$. This bound is a 'little' worse that the best known lower bound of Erdős, which is of the form $n^{1+c/\log\log n}$ (On a set of distances of n points, *Amer. Math. Monthly* **53**, 248–250, 1946).

Here is the argument.

Arrange the points to form a network of equilateral triangles with unit sides. The triangles all have the same orientation, but are shifted in the plane with respect to each other. Specifically, the second triangle is displaced by one unit in a direction not parallel to any existing edge. The third triangle is displaced so that the displacements form another equilateral triangle. The next step is to form 2 more configurations of 9 vertices congruent to the first 9 but displaced in a new direction, so that with $n=27$ vertices, each vertex is in 3 levels of triangles for a total degree of 6. The process can be repeated indefinitely. If we write n in base 3: $n = \sum_{i=0}^{k} a_i 3^i$, $a_i \in \{0,1,2\}$, then the size of the graph obtained will be $|G| = \sum_{i>j} a_i a_j 3^j + \sum i a_i 3^i + \sum_{a_i=2} 3^i$. We can think of the vertex set as the union of configurations of 3^i vertices, with 0, 1, or 2 configurations at each level. Each vertex is connected to one vertex in each higher configuration, accounting for $\sum_{i>j} a_i a_j 3^j$ edges. Within each configuration, each vertex has degree $2i$, accounting for $\sum i a_i 3^i$ edges. Within each level, if $a_i = 2$, the degree of the vertex is raised to $2i+1$, accounting for an additional $\sum_{a_i>2} 3^i$ or $\sum \frac{a_i^2 - a_i}{2} 3^i$ edges.

If $n = 3^k + c$ where $c = 1, 2$, or 4, we can do better by forming the k level configuration and then adding on to one of its triangles, adding 2, 4, or 9 edges instead of 1, 3, or 8. In fact, if $k > 1$ and $c = 2, 4$, or 8, we can add to two triangles, adding 5, 10, or 22 edges instead of 3, 8, or 22, improving the result for $c = 2$ or 4. If $c = 3, 6$, or 12, we can add to 3 triangles, adding 9, 18, or 39 edges, instead of 6, 15, or 36. If we jump to 49 vertices, the triangle configuration produces 160 edges $= 81 + 36 + 3 + 18 + 9 + 4 + 9$, while a double array of wheels of 7 vertices produces $2 \times 7 \times 12 = 168$ edges. In general, if we start with a configuration of x vertices chosen from the tesselation the plane with triangles, where the average degree $d < 6$, if n is a power of x, we can get:

$$f(n) \geq n \frac{d}{2} \log_x n = n \ln(n) \frac{d}{2 \ln x}$$

Clearly, increasing x too much will not help, because d is bounded. In fact, for triangles, $\frac{2}{\ln 3} \cong 1.82$, for 7 wheels, $\frac{24/7}{\ln 7} \cong 1.76$, and for wheels of 19 vertices and 42 edges, $\frac{84/19}{\ln 19} \cong 1.50$. If n is a power of 3, $f(n) \geq n \log_3 n$.

In general $f(n) \geq c_n \lfloor \log_3 n \rfloor n$, where $c_n \geq \frac{3}{4}$ and $c_n \to 1$ as $n \to \infty$.

Proof: For $3^k \le n \le \frac{4}{3} \cdot 3^k$, we have:

$$f(n) \ge k\,3^k = \lfloor \log\, n \rfloor\, 3^k \ge \frac{3}{4}\, \lfloor \log_3\, n \rfloor\, n$$

so the inequality holds. For $\frac{4}{3} \cdot 3^k \le n \le \frac{5}{3} \cdot 3^k$:

$$\begin{aligned} f(n) \ge f(3^k + 3^{k-1}) &\ge k\,3^k + (k-1)\,3^{k-1} + 3^{k-1} \\ &= k(3^k + 3^{k-1}) = \frac{4}{3}\,k(3^k) \\ &\ge \frac{4}{5}\,k \cdot n \ge \frac{3}{4}\,k \cdot n\,. \end{aligned}$$

For $\frac{5}{3} \cdot 3^k \le n < 3^{k+1}$, $\frac{3}{4}\, \lfloor \log_3\, n \rfloor\, n$, continues to increase linearly, while $f(n)$ increases faster in each successive block, so the inequality holds for all n, with $c = \frac{3}{4}$.

Asymptotically, if $\log\, n \ge (3^\ell + 1)(\ell - 1)$, then we can replace $\frac{3}{4}$ by $\frac{3^\ell}{1+3^\ell}$. □

Problem 7. *In class we determined a lower bound on* $c_3(v,e) = \min\{c_3(G) \mid G \text{ is a } (v,e)\text{–graph}\}$. *What can be said about* $C_3(v,e) = \max\{c_3(G) \mid G \text{ is a } (v,e)\text{–graph}\}$*? It turns out that these problems are quite different, and if we could not say much about* $c_3(v,e)$*, that we can determine* $C_3(v,e)$ *explicitly.*

Theorem. *Let* $e = \binom{s}{2} + t$, $0 < t \le s$. *Then* $C_3(v,e) = \binom{s}{3} + \binom{t}{2}$.

The generalization of this theorem for the maximum number of complete subgraphs K_r, $r \ge 3$, *was proven by Erdős and Hanani (1962). Go over the proof in [Bol78]. Find all misprints. Notice that the maximum depends on* e *only!*

Proof. (by Frank Fiedler) There are two types of misprints. The first deals with the inequality

$$\binom{d}{r-1} + \binom{t-d}{r-1} < \binom{t}{r-1}$$

Here equality is possible since $d < r-1$, $t-d < r-1$, and $t < r-1$ implies $0+0=0$. The other misprint (which does not effect the proof either) is

$$\binom{d}{r-1} + \binom{s-1}{r} + \binom{s+t-d}{r-1} < \binom{s}{r} + \binom{t}{r-1}$$

This equation is based on the fact that if $m = \binom{s}{2} + t$ and $t \le d < s$ then $m - d = \binom{s-1}{2} + t'$, $0 < t' \le s-1$ (Note that representations of this form are unique). Hence $t' = s - 1 + t - d$. So above line should read

$$\binom{d}{r-1} + \binom{s-1}{r} + \binom{s-1+t-d}{r-1} < \binom{s}{r} + \binom{t}{r-1}$$

□

Problem 8. *We will consider this a 2 part question since there were multiple number 9's.*

(i) Prove that every graph G contains a spanning bipartite subgraph H such that $d_H(x) \geq \frac{1}{2}d_G(x)$ for every vertex $x \in V(G) = V(H)$. This also implies that $e(H) \geq \frac{1}{2}e(G)$.

(ii) Is it possible to two-color the vertices of any finite graph such that at most half of the neighbors of any vertex v has the same color as v?

Proof. (by David Kravitz)

(i) Since there are finitely many subgraphs of G, there are finitely many bipartite subgraphs of G. Let H be a spanning bipartite subgraph so that no other bipartite subgraph has more edges. Say $V(H) = V(G)$ is partitioned into two sets, A and B. Now, by contradiction suppose that there is a vertex $x \in A$ such that $d_H(x) < \frac{1}{2}d_G(x)$. Since H had a maximum number of edges, there are no vertices $b \in B$ such that $vb \in V(G) - V(H)$, or else we could add an edge while still having a bipartite subgraph of G.

For $S' \subseteq V(G)$, let $N_{S'}(x) = N_G(x) \cap S'$. Then

$$d_H(x) < \frac{1}{2}d_G(x) \Rightarrow 2d_H(x) < d_G(x)$$

$$\Rightarrow 2|N_B(x)| < |N_A(x)| + |N_B(x)|$$

$$\Rightarrow |N_B(x)| < |N_A(x)|$$

Now, if we move vertex x from A to B, remove the $|N_B(x)|$ edges from x to B and add the $|N_A(x)|$ edges from x to A that existed in G, we now have a bipartite subgraph of G with more edges than H, a contradiction. Therefore there is no $x \in H$ such that $d_H(x) < \frac{1}{2}d_G(x)$, and we are done.

(ii) Yes, it is possible. To see this, take any bipartite subgraph H meeting the condition above and give it a 2-coloring. Clearly, this color assignment to $V(H)$ given to $V(G)$ is sufficient.

□

Proof. (by Frank Fiedler)
Every graph G has spanning bipartite graphs, the empty graph being one. Among these, there are graphs that have a maximal number of edges since G is finite. Let H be a spanning bipartite subgraph of G with a maximal number of edges.

Let $v \in V(G) = V(H)$. Since H is bipartite, there exists a natural partition of the vertices of H into two classes. Let $C_{(v)}$ denote the class v belongs to, $C_{(\neg v)}$ be the other one. Consider a bipartite graph H' constructed from H in the

following way: v is put into $C_{(\neg v)}$ and is connected to all vertices $N_G(v) \setminus N_H(v)$, *i.e.*, to all vertices in $C_{(v)} \cap N_G(v)$ (since H has a maximal number of edges, v is connected to all vertices in $C_{(\neg v)} \cap N_G(v)$ in H).

Clearly, H' is a bipartite spanning subgraph of G. The number of edges of H' is

$$E(H') = E(H) - d_H(v) + d_{H'}(v)$$

By construction, we have

$$d_{H'}(v) + d_H(v) = d_G(v).$$

Since H is maximal, this implies

$$d_H(v) \geq \frac{1}{2} d_G(v).$$

Since v was arbitrary, this also implies $e(H) \geq \frac{1}{2} e(G)$. □

Problem 9. *Generalize the statements of Problems 8, 9 to p-partite subgraphs and p colors, respectively.*

Proof. (by Vasyl Dmytrenko)

Show that every finite graph G contains a spanning subgraph H such that $d_H(x) \geq \frac{p-1}{p} d_G(x)$ $\forall x \in V(G) = V(H)$ and $\forall p, 2 \leq p \leq n$.

Since G is finite, there are finitely many p-partite spanning subgraphs of G. Let $H = (A_1, \ldots, A_p, E)$ be such subgraph with maximal possible $e(H)$. Suppose that for some i there is $x \in A_i$ such that $d_H(x) < \frac{p-1}{p} d_G(x)$. If $|A_i| = 1$, then $d_H(x) = d_G(x)$, therefore, we can suppose that $|A_i| \geq 2$. Now by the Pigenhole Principle there exists $A_j, j \neq i$, such that $|\{y \in A_j : yx \in E(G)\}| < \frac{d_G(x)}{p}$ since $|\{y \in A_i : yx \in E(G)\}| > \frac{d_G(x)}{p}$.

Let H' be the p-partite graph $(A'_1, \ldots, A'_p, E)$, where $A'_i = A_i \setminus \{x\}$, $A'_j = A_j \cup \{x\}$, $A'_k = A_k$, if $k \neq i$ and $k \neq j$, and E' is induced by $E(G)$. Then $|E'| = |E| - d_H(x) + d_{H'}(x) > |E|$, a contradiction with maximality of $|E|$.

Similarly to Problem 8,

$$e(H) = \frac{1}{2} \sum_{x \in V(H)} d_H(x) \geq \frac{1}{2} \sum_{x \in V(G)} \frac{p-1}{p} d_G(x) = \frac{p-1}{p} e(G).$$

And similarly to Problem 9, choose color i for $x \in V(G)$ iff $x \in A_i$. Then the number of neighbors colored in a color unlike i is $d_H(x) \geq \frac{p-1}{p} d_G(x)$. Hence, the number of neighbors of x colored in the color i (the same as x) is at most $\frac{d_H(x)}{p}$. □

Problem 10. *Eighteen cellular-phone power stations are to be placed in a circular city of radius four miles. Prove that no matter where in the city they are placed, at least two of them will be able to transmit to at least five other stations.*

Proof. (by Jason Williford)

Let v_i denote the *ith* power station, and $p(x, y)$ the distance between the power stations x and y. Let G be a graph with vertex set $V = \{v_i\}_{i=1,18}$, with edge set $E = \{v_i v_j | p(v_i, v_j) \leq 6, i \neq j\}$.

Claim: the subgraph induced by any four of the vertices of V has at least one edge.

Proof. (based on a proof in Bollobás, *Modern Graph Theory*) Assume the contrary, i.e. that there are four stations which are all distance greater than six from each other. No three points can be colinear as this would imply the distance between the outermost two is twelve or greater. Four points in the plane, no three colinear, can lie in one of two configurations, three points in a triangle with the fourth in its interior, or all four points forming a quadrilateral. In either case, three of these points will form an angle of 90^o or greater. Therefore two of these points will be of distance greater than $6\sqrt{2} > 8$, a contradiction. □

Consider G', the complement of G. It cannot contain K_4 as this would imply there are four vertices of G which induce a subgraph with no edges. Thus by Turan's Theorem, $\mid E' \mid \leq 108$. This implies that $\mid E \mid \geq \binom{18}{2}$ - 108 = 45.

Assume that all vertices of G have degree less than or equal to 4 except for possibly one vertex v_i. Then $90 = \sum_{1 \leq j \leq 18} v_j \leq 4(17) + 17 = 85$, a contradiction. Therefore two vertices of G must have degree greater than or equal to five, and the theorem is proven. □

Problem 11. *Show that there are finitely many finite regular graphs with the property that for each pair of adjacent vertices there is exactly one common neighbor and for each pair of non-adjacent vertices there are exactly two common neighbors. What are possible degrees and orders of these graphs?*

Hint: *Use linear algebra.*

Proof. (by Sven Reichard)

Let Γ be a strongly regular graph of order v and valency k satisfying the above conditions. We will show that there are only finitely many possible values for v and k. This will imply the existence of only finitely many graphs.

First let us observe that v can be expressed in terms of k (see Cameron, p. 331). We fix a vertex x and count edges between neighbors y and non-neighbors z of x.

If we choose z first, we have $v - 1 - k$ choices. Each such z has 2 common neighbors with x, hence the total number is $2(v - 1 - k)$. On the other hand,

each of x's k neighbors has in turn k neighbors, one of which is x, and another one is adjacent to x. Thus we get $k(k-2)$ edges.

Comparing the above, we get

$$\begin{aligned} 2(v-1-k) &= k(k-2) \\ v &= k+1+\frac{k(k-2)}{2} \\ &= 1+\frac{k^2}{2} \end{aligned}$$

Let A be the adjacency matrix of Γ, and let $\bar{A} = J - I - A$ be the adjacency matrix of the complementary graph. (Here, as usual, J denotes the all-one matrix). Then

$$\begin{aligned} A^2 &= kI + A + 2\bar{A} \\ &= (k-2)I - A + \mu J \end{aligned}$$

We know that k is an eigenvalue of A with multiplicity 1. Let x be another eigenvalue of A with eigenvector $\vec{v}$. Then $\vec{v}$ is an eigenvector of J with eigenvalue 0, and

$$\begin{aligned} x^2 &= (k-2) - x \\ \left(x+\frac{1}{2}\right)^2 &= (k-2)+\frac{1}{4} \\ x &= \frac{1}{2}\left(-1 \pm \sqrt{4(k-2)+1}\right) \\ &= \frac{1}{2}\left(-1 \pm \sqrt{4k-7}\right) \\ &= \frac{1}{2}\left(-1 \pm \sqrt{\Delta}\right) \end{aligned}$$

We can express k in terms of the integer Δ:

$$\begin{aligned} k &= \frac{\Delta+7}{4} \\ v &= 1+\frac{(\Delta+7)^2}{32} \end{aligned}$$

Let $r \geq s$ be the eigenvalues with respective multiplicities f and g. Then, since A is symmetric, $1+f+g=v$, and since Γ doesn't have loops,

$$0 = \mathrm{tr}A = k + fr + gs$$

Solving this system of equations we get

$$\begin{aligned} g &= v-1-f \\ 0 &= k+fr+(v-1-f)s \\ &= (r-s)f+k+(v-1)s \\ f &= \frac{k+(v-1)s}{s-r} \\ &= \frac{1}{2}\left(v-1-\frac{2k+1-v}{\sqrt{\Delta}}\right) \\ g &= \frac{k+(v-1)r}{r-s} \\ &= \frac{1}{2}\left(v-1+\frac{2k+1-v}{\sqrt{\Delta}}\right) \end{aligned}$$

Taking the difference we find that

$$\begin{aligned} g-f &= \frac{2k+1-v}{\sqrt{\Delta}} \\ &= \frac{\frac{\Delta+7}{2}-(\frac{\Delta^2+14\Delta+49}{32})}{\sqrt{\Delta}} \\ &= \frac{16\Delta+112-\Delta^2-14\Delta-49}{32\sqrt{\Delta}} \\ &= \frac{-\Delta^2+2\Delta+63}{32\sqrt{\Delta}} \end{aligned}$$

This is an integer, and thus Δ has to be a perfect square; moreover, $\sqrt{\Delta}$ must divide 63. The possible values and corresponding parameters are

$\sqrt{\Delta}$	k	v
1	2	3
3	4	9
7	14	99
9	22	243
21	112	6273
63	994	494019

Since there are only finitely many graphs on a fixed number of vertices, this solves the problem. (The graph on 3 vertices is the triangle, where the condition on μ is vacuous, the graph of order 9 is a lattice graph.) □

Proof. (by Frank Fiedler)

Let G be a strongly regular graph with $\lambda = 1$ and $\mu = 2$. Let A denote its adjacency matrix. Then

$$\begin{aligned} A^2 &= kI + \lambda A + \mu\bar{A} \\ &= (k-2)I - A + 2J \end{aligned} \tag{0.1}$$

Clearly, $\vec{1} = (1, \ldots, 1)^T$ is an eigenvector with eigenvalue k. Applied to (0.1) this gives

$$\begin{aligned} & k^2 = (k-2) - k + 2v \\ \Longrightarrow \qquad & v = \frac{k^2}{2} + 1 \end{aligned} \tag{0.2}$$

In particular, this shows that k must be even and v odd.

A is symmetric and hence diagonalizable. Therefore it has a base of eigenvectors. By the Gram-Schmidt process, w.l.o.g. this is an orthogonal base. Now suppose that $\vec{e} \neq \vec{1}$ is a base element. Let η be its eigenvalue. Then by (0.1)

$$\begin{aligned} & \eta^2 \vec{e} = (k-2)\vec{e} - \eta\vec{e} \\ \Longrightarrow \qquad & \eta_{1,2} = \frac{1}{2}\left(-1 \pm \sqrt{4k-7}\right) \end{aligned} \tag{0.3}$$

Now $\eta = k$ would imply $k^2 + 2 = 0$. Hence $k \neq \eta$. That is, geometrically the eigenvalue k has multiplicity 1. Since A is diagonalizable, geometric and algebraic multiplicity are the same and k has multiplicity 1.

Let $r = \eta_1$ and $s = \eta_2$. f and g be the multiplicities of r, s, respectively. Then

$$\begin{aligned} 1 + f + g &= v \\ k + fr + gs &= \mathsf{Tr}\,(A) \\ &= 0 \end{aligned} \tag{0.4}$$

With (0.3) this becomes

$$0 = 2k - (f+g) + (g-f)\sqrt{4k-7} \tag{0.5}$$

This leaves us with two cases. Either $f = g$ (the so-called half-case) or $f \neq g$.

case 1: If $f = g$ then by (0.4) $f = g = k$. With (0.2) and (0.4) it follows that G is an s.r.g. with parameters $(9, 4, 1, 2)$. This is the (unique) lattice graph $L_2(3)$ (see Figure 3).

case 2: If $f \neq g$ then $\sqrt{4k-7}$ must be an integer. Let $\Delta = \sqrt{4k-7}$. Then with (0.5), (0.2), and (0.4) it follows

$$0 = \frac{\Delta^2 + 7}{2} - \frac{(\Delta^2+7)^2}{32} + (g-f)\Delta$$

Hence

$$0 = \Delta^4 - 2\Delta^2 - 32(g-f)\Delta - 63$$

Therefore Δ divides 63. This leaves Δ with values 1, 3, 7, 9, 21, and 63.

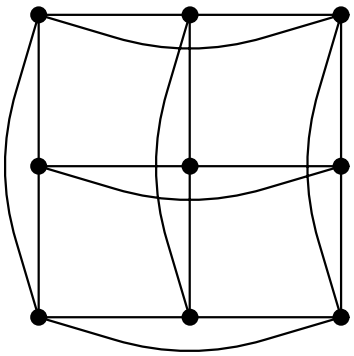

Figure 3: Lattice graph $L_2(3)$

For $\Delta = 1$ we obtain the triangle (see Figure 4). $\Delta = 3$ gives the lattice graph $L_2(3)$ in Figure 3, *i.e.*, although $f = g$ and Δ could be any real number, Δ is an integer. For $\Delta = 7$ the resulting graph was an s.r.g. with parameters $(99, 14, 1, 2)$. To my knowledge, no such graph is known yet. The same holds for graphs with parameters $(243, 22, 1, 2)$, and $(6273, 112, 1, 2)$. For $v = 494019$ the resulting parameters are not strongly feasible (tested with a program by S. Reichard).

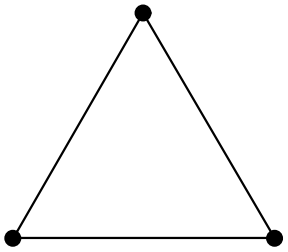

Figure 4: Triangle

□

Problem 12. *(Jensen's inequality) Let f be a function concave up on (a, b), i.e., for any $x_1, x_2 \in (a, b)$, $f(\frac{x_1+x_2}{2}) \leq \frac{f(x_1)+f(x_2)}{2}$. Prove that for all $x_i \in (a, b)$,*

$$f\left(\frac{\sum_{i=1}^{n} x_i}{n}\right) \leq \frac{\sum_{i=1}^{n} f(x_i)}{n},$$

and that the equality is attained if and only if f is linear or all x_i are equal.

For concave down functions, the signs of all inequalities change. What famous inequalities do we get by setting $f(x) = x^2$, or $f(x) = \ln x$ $(x > 0)$, or $f(x) = 1/x$ $(x > 0)$?

Proof. (by David Chandler)

A usual understanding of concavity will imply that $f(tx_1 + (1-t)x_2) \leq tf(x_1) + (1-t)\,f(x_2)$ for all $0 \leq t \leq 1$. The definition above does imply it if x_1, x_2, t are restricted to rationals. Over any larger field we can consider the field as a vector space over the rationals. Choosing a basis, it is then possible to have a separate concave up function corresponding to each basis vector. Each x_i is then the rational linear combination of a finite number of these basis vectors, and we can let f be the sum of the functions applied to the coefficients of their respective basis vectors. The expression $f(tx_1+(1-t)x_2) \leq tf(x_1)+(1-t)f(x_2)$ will then hold for rational t as a consequence of its validity for the functions of which f is a sum. Therefore the proof of Jensen's inequality will hold for such functions, even though they may be highly irregular.

Lemma 2. $f(tx_1 + (1-t)x_2) \leq tf(x_1) + (1-t)f(x_2)$

Proof. We present two proofs of this lemma: one which assumes continuity of f, and another which does not.

First, by induction, the relation holds for t any dyadic rational. If holds for $t = \frac{k}{2^n}$ and for $t = \frac{k+1}{2^n}$, then applying the definition again it holds for $t = \frac{2k+1}{2^{(n+1)}}$. Since the dyadic rationals are dense in the reals, continuity of f implies that the lemma hold for all reals in [0,1].

Proof of lemma assuming t is a rational instead of continuity of f.

Suppose $t = \frac{k}{\ell}$. For simplicity, take $f(x_1) = 0$, $x_1 = 0$, and $x_2 = 1$. We know the lemma is true for dyadic rationals, so we apply it to 0 and $\frac{k}{\ell}$ with the fraction $\frac{a}{2^n}$ and to $\frac{k}{\ell}$ and 1 with the fraction $\frac{b}{2^n}$ to get $f\left(\frac{ak}{2^n\ell}\right) \leq \frac{af\left(\frac{k}{\ell}\right)}{2^n}$ and

$$f\left(\frac{2^n\ell + bk - b\ell}{2^n\ell}\right) \leq \frac{bf\left(\frac{k}{\ell}\right) + (2^n - b)f(1)}{2^n}.$$

We want the difference

$$2^n\ell + bk - b\ell - ak = (2^n - b)\,\ell + (b-a)\,k$$

of the numerators to be a power of two, so we can take a dyadic fraction of it to get back to $\frac{k}{\ell} = \frac{2^n k}{2^n \ell}$. If $2^n - b = \lambda_1$ and $b - a = \lambda_2$, we need $0 < \lambda_1$ and $-\lambda_2 < \lambda_1$ such that $\lambda_1\ell + \lambda_2 k$ is a power of two. Since k and ℓ are coprime, we can express 1 as a linear combination with $0 < \lambda_1$. Since 2 does not divide both k and ℓ, some power of 2 is congruent to $1 (\mathrm{mod}\, k)$ or $(\mathrm{mod}\, \ell)$. In this way we can increase λ_1 or λ_2 as many times as necessary to guarantee that $0 < \lambda_1 + \lambda_2$. Now pick n so that $\lambda_1 < 2^n$ and $\lambda_1 + \lambda_2 < 2^n$ and solve for a and b. It is clear that

$$f\left(\frac{k}{\ell}\right) \leq \frac{(2^n\ell + bk - b\ell - 2^n k)f\left(\frac{ak}{2^n\ell}\right)}{2^n\ell + bk - b\ell - ak} + \frac{(2^n k - ak)f\left(\frac{2^n\ell + bk - b\ell}{2^n\ell}\right)}{2^n\ell + bk - b\ell - ak}.$$

Substituting and collecting terms we get

$$\frac{\left(2^n\ell - b\ell - a\ell + \frac{ab\ell}{2^n}\right) f\left(\frac{k}{\ell}\right)}{2^n\ell + bk - bl - ak} \leq \frac{\left(2^n k - bk - ak + \frac{abk}{2^n}\right) f(1)}{2^n\ell + bk - bl - ak}$$

which proves the lemma. □

We continue with the proof of the theorem. Let A be the average value of the x's and suppose $x_1 < A$ and $A < x_2$ and that $|A - x_1| < |x_2 - A|$. We use the lemma to get $f(A) \leq \frac{(x_2-A)f(x_1)}{x_2-x_1} + \frac{(A-x_1)f(x_2)}{x_2-x_1}$ and $f(x_1 + x_2 - A) \leq \frac{(A-x_1)f(x_1)}{x_2-x_1} + \frac{(x_2-A)f(x_2)}{x_2-x_1}$. Adding the inequalities we get $f(A)+f(x_1+x_2-A) \leq f(x_1)+f(x_2)$. In this way we can replace the sum of function values with another smaller sum in which the number of x's different from A is reduced by one, but the average of the x's is not changed. By induction on the number of x's different from A, Jensen's inequality is proved.

Equality is attained only if all x_i are equal, or if the function is linear over the interval.

Famous inequalities related to this one:

• $f(x) = x^2$ gives us that variance of a data set is positive, or that the quadratic mean is greater or equal than the arithmetic mean.

• $f(x) = \ln(x),\ x > 0$ gives that the arithmetic mean is greater or equal than the geometric mean.

• $f(x) = \frac{1}{x},\ x > 0$ gives

$$\frac{\sum_{x=1}^{n} x_i}{n} \geq \frac{n}{\sum_{i=1}^{n} \frac{1}{x_i}}.$$

This is an inequality between the arithmetic and harmonic means. If we rewrite it as

$$\left(\sum_{i=1}^{n} x_i\right)^{\left(\frac{1}{2}\right)} \left(\sum_{i=1}^{n} \frac{1}{x_i}\right)^{\left(\frac{1}{2}\right)} \leq n,$$

it can be viewed as a special case of the Cauchy–Schwartz inequality. □

Proof. (by Felix Lazebnik) This proof uses the idea of 'up' and 'down' induction which is credited to Cauchy. This proof also shows that the arguments related to limits are not needed.

First we use induction on k to show that the inequality is satisfied for all $n = 2^k$ (the 'up' part). This follows immediately from the fact that it is correct for $k = 1$ and

$$\frac{x_1 + \ldots + x_{2^{k+1}}}{2^{k+1}} = \frac{1}{2}\left(\frac{x_1 + \ldots + x_{2^k}}{2^k} + \frac{x_{2^k+1} + \ldots + x_{2^{k+1}}}{2^k}\right)$$

for all $k \geq 2$.

Now we suppose that the statement is proven for $n \geq 3$ values of x_i's and show that it implies the statement for $n-1$ values of x (the 'down' part). Let $x_i \in (a,b)$, $i \in [n-1]$, be arbitrary $n-1$ numbers on (a,b). Apply the inequality to the following n numbers: $x_1, x_2, \ldots, x_{n-1}, x_n = \frac{x_1+\ldots+x_{n-1}}{n-1}$. We have

$$f\left(\frac{\sum_{i=1}^{n} x_i}{n}\right) \leq \frac{\sum_{i=1}^{n} f(x_i)}{n} \Leftrightarrow f\left(\frac{\frac{n}{n-1}\sum_{i=1}^{n-1} x_i}{n}\right) \leq \frac{\sum_{i=1}^{n-1} f(x_i) + f\left(\frac{\sum_{i=1}^{n-1} x_i}{n-1}\right)}{n} \Leftrightarrow$$

$$f\left(\frac{\sum_{i=1}^{n-1} x_i}{n-1}\right) \leq \frac{\sum_{i=1}^{n-1} f(x_i) + f\left(\frac{\sum_{i=1}^{n-1} x_i}{n-1}\right)}{n}.$$

Solving the last inequality for $f\left(\frac{\sum_{i=1}^{n-1} x_i}{n-1}\right)$, we obtain

$$f\left(\frac{\sum_{i=1}^{n-1} x_i}{n-1}\right) \leq \frac{\sum_{i=1}^{n-1} f(x_i)}{n-1}.$$

This completes the proof. The assertion about the equality sign should be a part of the inductive hypothesis, and it follows immediately. □

Problem 13. *Let G be a bipartite graph with both colour classes having n vertices and without subgraphs isomorphic to C_4. Prove that*

$$e(G) \leq \frac{1}{2} n \left(1 + \sqrt{4n-3}\right)$$

Prove that the equality above is attained iff the following three conditions hold:

(i) G is $d+1$ regular for some d,

(ii) n is of the form d^2+d+1,

(iii) ever pair of vertices from the same color class, share a unique common neighbour.

Clearly the extremal graphs are the point-line incidence graphs of projective planes of order d.

Proof. (by Sukhendu Mehrotra)

Let A and B be the color classes of G. For any vertex a in G, let $N(a)$ denote the neighborhood of a. Fix a vertex $x \in A$. As G contains no C_4, for any $y, z \in N(x), N(y) \cap N(z) = \{ x \}$. Therefore, since any neighbour of x has neighbours only in A,

$$\sum_{y \in N(x)} deg(y) \leq (n-1) + deg(x).$$

Summing over all vertices x of A we obtain

$$\sum_{x \in A} \sum_{y \in N(x)} deg(y) \leq n(n-1) + e,$$

where e is the size of G. Since each y lies in an $N(x)$ for exactly $deg(y)$ many x's, the inequality above can written as

$$\sum_{y \in B} [deg(y)]^2 \leq n(n-1) + e.$$

Applying Jensen's inequality to the left hand side of the inequality above, using the fact that $\sum_{y \in B} deg(y) = e$, we obtain

$$\frac{e^2}{n} \leq n(n-1) + e.$$

Completing the square, we get

$$\left(e - \frac{n}{2}\right)^2 \leq \frac{n^2}{4}(4n-3),$$

or that,

$$e \leq \frac{n}{2}\left(1 + \sqrt{4n-3}\right).$$

From the above, we see that equality follows iff

(a) $\sum_{y \in N(x)} deg$ y $= (n-1) + deg(x)$, and

(b) $deg(x) = d' = d+1$ for $=$ some d, for all $x \in G$.

Using (b) in (a), we obtain

$$\begin{gathered}(d+1)^2 = (n-1) + (d+1), \\ d^2 + 2d + 1 = n - 1 + d + 1 \\ \text{or, } n = d^2 + d + 1\end{gathered}$$

□

Proof. (by Carl DeVore)

Let V_1 and V_2 denote the sets of vertices of each color class, with $V_1 = \{v_1, v_2, \ldots, v_n\}$. Let $C(x,k)$ denote the continuous extension of $\binom{x}{k}$. Consider any 2-subset S of V_2. Since G contains no C_4, there can be at most 1 element of V_1 adjacent to both elements of S. The number of choices for S is $\binom{n}{2}$. On the other hand, given any $v \in V_1$, there are $\binom{d(v)}{2}$ 2-subsets S of V_2 such that v is adjacent to both elements of S. Therefore, $\sum_{i=1}^{n} C(d(v_i), 2) \leq \binom{n}{2}$. The function $C(x,2)$ is an upward opening parabola, so it is a convex function. By Jensen's inequality, since $e(G) = \sum_{i=1}^{n} d(v_i)$,

$$n\, C\left(\frac{e(G)}{n}, 2\right) \leq \sum_{i=1}^{n} \binom{d(v_i)}{2} \leq \binom{n}{2}.$$

Letting x denote $\frac{e(G)}{n}$ and assuming equality we have a quadratic equation with respect to x, $\frac{1}{2}nx(x-1) = \frac{1}{2}n(n-1)$, whose only positive solution is

$$x = \frac{1}{2}(1 + \sqrt{4n-3}).$$

Hence, $e(G) \leq \frac{1}{2}n(1+\sqrt{4n-3})$.

Equality will be attained iff

(i) equality is attained in Jensen's inequality,

(ii) the right side of the above inequality is an integer,

(iii) for each 2-subset S of V_2 in the above proof, there is exactly 1 element of V_1 adjacent to both elements of S.

Condition (i) will hold iff $d(v_i)$ is constant. For condition (ii) to hold, $4n-3 = m^2$ for some integer m. That implies m is odd, hence $m = 2d+1$ for some integer d. Solving for n gives $n = d^2 + d + 1$. Conversely, if $n = d^2 + d + 1$, then the right side of the above inequality is an integer. Condition (iii) will hold iff each pair of vertices in V_2 has a unique common neighbor. Since $|V_1| = |V_2|$, and the conclusion makes no distinction between the two, their roles can be interchanged in conditions (i) and (iii). If the degree of each element of V_2 is also constant, it must be the same constant as for V_1. So G is regular. Thus we have the three conditions stated at the beginning of the problem.

Reference: *Modern Graph Theory*, Béla Bollobás (Springer, New York, 1998), section IV.2, "Extremal Problems: Complete Subgraphs". □

Problem 14. *The largest eigenvalue of the adjacency matrix A of a connected k–regular graph G is k and its multiplicity is 1.*

Proof. (by Carl DeVore)

Let $\rho(A)$ denote the spectral radius of $A \in \mathbb{C}^{n\times n}$, that is, the maximum of the moduli of the eigenvalues of A. The sum of the entries in each row of A is k. Let j be an n-vector all of whose components are 1. $Aj = kj$, so k is an eigenvalue. Let $|A|_\infty$ denote the maximum-row-sum matrix norm. Theorem 5.6.9 in H&J says that $\rho(A) \leq |A|$ for any matrix norm. A is a real symmetric matrix, so all of its eigenvalues are real, and hence the concept of "largest" eigenvalue is meaningful. We have $\rho(A) \leq |A|_\infty = k \leq \rho(A)$, so k is the largest eigenvalue. Perron's theorem (8.2.11 in H&J) says that if A is a matrix all of whose entries are positive, then $\rho(A)$ is an eigenvalue of multiplicity 1. As G is connected, some power of A, say A^i, has all positive entries. Since $\rho(A^i) = \rho(A)^i$, k^i is an eigenvalue of A^i of multiplicity 1, and hence k is an eigenvalue of A multiplicity 1.

Reference: [H&J] *Matrix Analysis*, Roger A. Horn and Charles R. Johnson (Cambridge University Press, Cambridge, 1985).

□

Problem 15. *The vectors $e_{ij} = e_i + e_j, 0 \leq i < j \leq n$ form a two-distance set of cardinality $\binom{n+1}{2}$ in $\mathbb{R}^{n+1}$. They lie in a hyperplane. Express the e_{ij} as vectors in $\mathbb{R}^n$.*

Proof. (by Sven Reichard) Let $\alpha = \frac{1}{\sqrt{n+1}}$, and $j = \alpha(1,\ldots,1)^T \in \mathbb{R}^{n+1}$. Then $||j|| = 1$, and $e_{ij} \cdot j = 2\alpha$. Thus if we translate the vectors by $e'_{ij} = e_{ij} - 2\alpha j$, the new vectors lie in a n-subspace W with normal vector j.

It remains to exhibit an orthonormal basis for this subspace. If we use Gram-Schmidt's method, things get very quickly very messy. So we take a different approach, depending on Hadamard matrices.

Let us assume that $n+1 = 2^m$ is a power of 2. Then there exists a Hadamard matrix $H_{n+1}$of order $n+1$, and the normed rows of this matrix form an ordered orthonormal basis of $\mathbb{R}^{n+1}$ containing j as its first element. E.g., $n+1 = 4$, and

$$H_n = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

(If H_n is a Hadamard matrix, then so is $H_{2n} = H_n \otimes H_2$, where $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $H_1 = (1)$ satisfies the conditions vacuously.)

If $n+1$ is not a power of 2, we construct our orthogonal basis inductively. We can write $n+1 = 2^{m_1} + 2^{m_2} + \cdots + 2^{m_k}$, where $m_1 > m_2 > \ldots m_k$. We start with $H_{2^{m_1}}$ Suppose the principal l-minor has been constructed, where

$l = 2^{m_1} + \cdots + 2^{m_{i-1}}$. The first row is padded with 1's on the right, the other rows, with 0's. We add 2^{m_i} rows, containing $H_{2^{m_i}}$ on the diagonal and 0's everywhere else. Then we replace the first of the added rows by setting the first l entries to 2^{m_i}, and the next 2^{m_i}, to $-l$.

The transition from order 4 to order 6 is carried out in detail below.

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 0 & 0 \\ 1 & 1 & -1 & -1 & 0 & 0 \\ 1 & -1 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 0 & 0 \\ 1 & 1 & -1 & -1 & 0 & 0 \\ 1 & -1 & -1 & 1 & 0 & 0 \\ 2 & 2 & 2 & 2 & -4 & -4 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}$$

It is easy to check that the rows of the resulting matrix are mutually orthogonal. Normalizing the rows gives us an orthogonal matrix M which represents a transformation moving the subspace W to the subspace $\{x_0 = 0\}$. Thus deleting the first row we obtain the required transformation from $\mathbb{R}^{n+1}$ to $\mathbb{R}^n$. The matrix for $n = 5$ is thus

$$\begin{pmatrix} 1/2 & -1/2 & 1/2 & -1/2 & 0 & 0 \\ 1/2 & 1/2 & -1/2 & -1/2 & 0 & 0 \\ 1/2 & -1/2 & -1/2 & 1/2 & 0 & 0 \\ \sqrt{3}/6 & \sqrt{3}/6 & \sqrt{3}/6 & \sqrt{3}/6 & -\sqrt{3}/3 & -\sqrt{3}/3 \\ 0 & 0 & 0 & 0 & \sqrt{2}/2 & -\sqrt{2}/2 \end{pmatrix}$$

Multiplying the vectors e'_{ij} by this matrix from the left gives the desired representation in $\mathbb{R}^n$. Note that $Mj = 0$, so we can also use the original vectors e_{ij} instead, i.e., the vectors we're looking for are sums of two distinct columns of M.

It is probably possible to give the components of e'_{ij} explicitly, but I don't think that this would make things clearer. □

Proof. (by David Chandler) A simple way is to transform $\mathbb{R}^{n+1}$ so that basis is $\frac{\mathbf{u}}{\sqrt{n+1}}$, (where $\mathbf{u}$ is the all-ones vector), and vectors of the form $(b, \ldots, b, a, b, \ldots, b, c)$, to form an orthonormal basis for the hyperplane through $\vec{0}$ parallel to H. We want unit vectors:

$$a^2 + (n-1)b^2 + c^2 = 1$$

We want them orthogonal:

$$2ab + (n-2)b^2 + c^2 = 0$$

We also want them orthogonal to $\mathbf{u}$:

$$a + (n-1)b + c = 0$$

Note that a can go in any one of n positions. Subtract the second equation from the first:

$$a^2 - 2ab + b^2 = 1$$

$$a = b + 1$$

Substitute into the third equation:

$$1 + nb + c = 0$$

$$c = -1 - nb$$

Substitute into the first equation:

$$b^2 + 2b + 1 + (n-1)b^2 + 1 + 2nb + n^2b^2 = 1$$

$$\left(n^2 + n\right) b^2 + (2n+2)b + 1 = 0$$

$$\begin{aligned} b &= -\frac{1}{n} - \frac{1}{n\sqrt{n+1}} \\ a &= 1 - \frac{1}{n} - \frac{1}{n\sqrt{n+1}} \\ c &= \frac{1}{\sqrt{n+1}} \end{aligned}$$

So the transformation matrix is:

$$\begin{bmatrix} \frac{1}{\sqrt{n+1}} & \frac{1}{\sqrt{n+1}} & \cdots & \cdots \\ \frac{1}{\sqrt{n+1}} & 1 - \frac{1}{n} - \frac{1}{n\sqrt{n+1}} & -\frac{1}{n} - \frac{1}{n\sqrt{n+1}} & \cdots \\ \vdots & -\frac{1}{n} - \frac{1}{n\sqrt{n+1}} & \ddots & \ddots \\ \vdots & \vdots & \ddots & \ddots \end{bmatrix}$$

We add any two such vectors and ignore the first component. The general form is:

$$(2b, \ldots, 2b, a+b, 2b, \ldots, 2b, a+b, 2b, \ldots, 2b)$$

or

$$(b+c, \ldots, b+c, a+c, b+c, \ldots, b+c)$$

□

Problem 16. *Let $A_1, \ldots, A_m$ be subsets of a set of n elements. Assume that their pairwise intersections have only two sizes. Prove that $m \leq 1 + n(n+1)/2$.*

Proof. (by David Chandler) The conclusion is the "Nonuniform RW (Ray-Chaudhuri-Wilson) Theorem #5.34 on page 117, *Linear Alg. Methods in Comb. with Appl. to Geom. and Comp. Sci.*, L. Babai and Peter Frankl (Frankl-Wilson, 1981). (The proof is Babai: 1988). Here $s = 2$, the number of intersection sizes, and the conclusion is that $m \leq \sum_{i=0}^{s} \binom{n}{i}$. The bound can always be achieved by taking all subsets of $[n]$ no larger than s. I doubt there is any other way to achieve the bound for $s \geq 2$, but I don't have a proof. It is easy to verify uniqueness for intersection sizes 0 and 1.

Let $L = \{\ell_1, \ldots, \ell_s\}$ be the set of intersection sizes and $\mathcal{F} = \{A_1, \ldots, A_m\}$ be the family of subsets arranged in order of increasing size, $|A_1| \leq \cdots \leq |A_m|$. With each set A_i associate the incidence vector $\mathbf{v}_i \in \mathbb{R}^n$ having 1 in the j^{th} position if $j \in A_i$ and 0 otherwise. The Euclidean inner product gives intersection size: $\mathbf{v}_i \cdot \mathbf{v}_j = |A_i \cap A_j|$. For each A_i, define a polynomial in n variables:

$$f_i(x) = \prod_{\substack{k=1 \\ \ell_k < |A_i|}}^{s} (\mathbf{v}_i \cdot \mathbf{x} - \ell_k) \quad (\mathbf{x} \in \mathbb{R}^n)$$

and note that $f_i(V_0) = \begin{cases} \neq 0 & \text{if } j = i \\ = 0 & \text{if } j = i\,. \end{cases}$

Proposition 5.16 states that the polynomial obtained by reducing each monomial in f_i to the monomial which is no more than degree one in any x_i is the unique such polynomial having the same value on $\mathbf{x} \in \{0,1\}^n$ (using the substitution $x_i = x_i^2$).

Suppose the f_i's were linearly dependent. The polynomials still would be linearly dependent with $\mathbf{x}$ restricted to $\{0,1\}^n$. Since the triangular matrix $f_i(\mathbf{v}_j)$ has a non–zero diagonal, we get a contradiction. $|\mathcal{F}| \leq$ the size of a basis for the multilinearized polynomials, whose monomials have total degree no more than $s = |L|$. We get a total of $\sum_{i=0}^{s} \binom{n}{s}$ basis monomials. □

Proof. (by Vasyl Dmytrenko) Here is the proof with the additional condition: we suppose that $A_1, \ldots, A_m$ are k-subsets of a set of n elements. This exercise can be found in [BF], ex.1.2.16 (see also exercises 1.2.14, 1.2.13 and 1.2.8).

If for any i $|A_i| = k$, then for any $i \neq j$ the symmetric difference $A_i \triangle A_j$ has size $|A_i| + |A_j| - |A_i \cap A_j| = 2k - |A_i \cap A_j|$. Thus, pairwise symmetric differences have only two sizes, say, a and b. Now show that if $A_1, \ldots, A_m$ are any subsets of the set $S = \{s_1, \ldots, s_n\}$ with pairwise symmetric differences of sizes a or b, then $m \leq 1 + n(n+1)/2$. (This is exercise 1.2.14 in [BF]).

Let a_i be the $(-1,1)$-incidence vector of A_i, i.e. the k-th coordinate of a_i is 1 if $s_k \in A_i$ and -1 otherwise. Consider the function

$$F(x,y) := (\|x-y\|^2 - 4a)(\|x-y\|^2 - 4b),\ x, y \in \mathbb{R}^n.$$

For $i \neq j$ $\|a_i - a_j\|^2 = 4|A_i \triangle A_j|$ since the k-th coordinate of $a_i - a_j$ has the absolute value 2 iff $s_k \in A_i \triangle A_j$. Therefore, $F(a_i, a_j) = \begin{cases} 16ab \neq 0 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$. It implies that the functions $f_i(x) := F(x, a_i)$, $i = 1, \ldots, n$, are linearly independent. Indeed, $\lambda_1 f_1(x) + \cdots + \lambda_m f_m(x) = 0$ yields $\lambda_i f_i(a_i) = 0$, i.e. $\lambda_i = 0$ for any $i = 1, \ldots, n$. On the other hand, $f_i(x)$ is a linear combination of $(\sum_{k=1}^n x_k^2)^2$, $(\sum_{k=1}^n x_k^2)x_j$, $x_i x_j$, x_i and 1. Since $x_k^2 = 1$ for all k, f_i is a linear combination of $x_i x_j$, $1 \leq i < j \leq n$, x_i, $1 \leq i \leq n$, and 1. The number of these monomials is $\frac{n(n-1)}{2} + n + 1 = \frac{n(n+1)}{2} + 1$. Hence, all f_i belong to a linear space of dimension $d = \frac{n(n+1)}{2} + 1$, and they are linearly independent, therefore, $m = \frac{n(n+1)}{2} + 1$. □

Problem 17. *Let $A_1, \ldots, A_m$ be subsets of a set of n elements. Assume that all $|A_i|$ are even and all $|A_i \cap A_j|$, $(i \neq j)$, are odd. Find good estimates for m.*

Proof. (by Jason Williford) This is the "Reverse Oddtown Problem". We have already shown that $m \leq n$. We shall prove that the maximum value for m is n if n is odd, and $n - 1$ if n is even.

If n is odd, let $A_i = [n] \backslash \{i\}$ for $i \in [n]$. The cardinality of each A_i is $n - 1$ which is even, and if $i \neq j$ then $|A_i \cap A_j| = |[n] \backslash \{i, j\}| = n - 2$ which is odd. Therefore we have n sets satisfying our criteria, thus the maximum value of m is exactly n if n is odd.

If n is even, let $A_i = [n-1] \backslash \{i\}$ for $i \in [n-1]$. $|A_i| = n - 2$ which is even, and if $i \neq j$ then $|A_i \cap A_j| = |[n-1] \backslash \{i, j\}| = n - 1 - 2$ which is odd. Therefore the maximum possible m is $(n - 1)$ or n.

We show by contradiction that it cannot be n. In the handout "A correction of 'Another Solution For Reverse Oddtown Problem'" it is shown that if $m-1$ is odd (hence m is even) then the incidence vectors of the corresponding sets are all linearly independent over F_2. Assume there is a family $F = \{A_i\}_{i=1}^n$ satisfying the above criteria. As $|F| = n$ is even, then the corresponding incidence vectors (denoted v_i) are linearly independent over F_2. Also, using the usual dot product modulo 2, $v_i \cdot v_i = 1$ and $v_i \cdot v_j = 0$ for $i \neq j, \forall i, j \in [n]$.

Consider $\sum_{i \in [n]} v_i = v$. We know $v \neq v_i$ for any i as this would violate the linear independence of the vectors v_i. We have $v \cdot v_j = \sum_{i \in [n]} v_i \cdot v_j = 1$ $\forall j \in [n]$. This implies that the set A corresponding to v is such that $|A \cap A_i|$ is odd $\forall i \in [n]$.

Also $v \cdot v = \sum_{i \in [n]} v_i \cdot v = n \bmod(2) = 0$. This implies that $|A|$ is even. Consider $F' = F \cup A$. This is a family satisfying the Reverse Oddtown conditions, but $|F'| = n + 1$, a contradiction as $|F'| \leq n$. Therefore the maximum value m can attain is $n - 1$ if n is even. □

Problem 18. *Let $A_1, \ldots, A_m$ be subsets of a set of n elements. Assume that all $|A_i|$ are odd and all $|A_i \cap A_j|$, $(i \neq j)$, are odd. Find good estimates for the largest value of m.*

Proof. (by F. Fiedler) Suppose n is odd. Consider $[n] = \{1\} \cup C_1 \cup C_2 \cup \ldots \cup C_{\frac{n-1}{2}}$ where $C_i = \{2i, 2i+1\}$. Let $C = C_1 \cup C_2 \cup \ldots \cup C_{\frac{n-1}{2}}$. Build a new family $\mathcal{F}'$ of sets $D_S = \{1\} \cup \left(\bigcup_{C_i \in S} C_i\right)$, $S \subseteq C$. Then all D_S are of odd cardinality and intersect each other in an odd number of elements. Clearly, $\mathcal{F}' = 2^{\lfloor \frac{n-1}{2} \rfloor}$.

On the other hand, let $\mathcal{F} = \{B_1, \ldots, B_k\} \subseteq 2^{[n]}$ be a family of sets of odd cardinality such that two sets intersect in an odd number of elements. Add a new point x to $[n]$ and let $\mathcal{F}' = \{B_i \cup \{x\} \mid B_i \in \mathcal{F}\} \cup \{B_i^c \mid B_i \in \mathcal{F}\}$ where B_i^c denotes the complement of B_i in $[n]$. All sets in $\mathcal{F}'$ are of even cardinality. Clearly, $|(B_i \cup \{x\}) \cap (B_j \cup \{x\})|$ is even, $i \neq j$. Since n is odd, $|B_i^c \cap B_j^c|$ is even as well as $|B_i^c \cap (B_j \cup \{x\})|$, $i \neq j$. Finally, $(B_i \cup \{x\}) \cap B_i^c = \emptyset$ is of even cardinality. Hence $\mathcal{F}'$ is a family of subsets of $n+1$ elements, each set is of even cardinality and two sets intersect in an even number of points. Thus $|\mathcal{F}'| \leq 2^{\lfloor \frac{n+1}{2} \rfloor}$ and $|\mathcal{F}| = \frac{1}{2}|\mathcal{F}'| \leq 2^{\lfloor \frac{n-1}{2} \rfloor}$.

Hence $m \leq 2^{\lfloor \frac{n-1}{2} \rfloor}$. □

Problem 19. *Here we list several ways of obtaining new designs from existing ones.*

(i) Let $(X, \mathcal{B})$ be a $2-(b, v, r, k, \lambda)$ BIBD. Replacing every block by its complement in X, we obtain the complementary *design $(X', \mathcal{B}')$. Hence the incidence matrix of the complementary design is obtained from the one of the original design by replacing 0's by 1's and 1's by 0's. Show that $(X', \mathcal{B}')$ is a $2-(b', v', r', k', \lambda')$ BIBD and express its parameters in terms of $9b, v, r, k, \lambda)$.*

(ii) Let $(X, \mathcal{B})$ be a $2-(v, k, \lambda)$ SBIBD and let B be a block of $(X, \mathcal{B})$. Let $X' = X \setminus B$, and

$$\mathcal{B}' = \{B_i \setminus B : B_i \in \mathcal{B}, \mathcal{B}_\setminus \neq \mathcal{B}\}$$

Show that $(X', \mathcal{B}')$ is a $2-(b', v', r', k', lambda')$ BIBD. It is called the residual *design of $(X, \mathcal{B})$ with respect to block B. Express parameters of $(X', \mathcal{B}')$ in terms of $v, k,$ and λ.*

(iii) Let $(X, \mathcal{B})$ be a $2-(v, k, \lambda)$ SBIBD and let B be a block of $(X, \mathcal{B})$. Let $X' = B$, and

$$\mathcal{B}' = \{B_i \cap B : B_i \in \mathcal{B}, B_i \neq B\}$$

Show that $X', \mathcal{B}')$ is a $2-(b', v', r', k', \lambda')$ BIBD. It is called the derived design of $(X, \mathcal{B})$ with respect to block B. Express parameters of $(X', \mathcal{B}')$ in terms of $v, k,$ and λ.

(iv) Let $(X, \mathcal{B})$ be a $2-(v,k,\lambda)$ SBIBD. The dual design for $(X, \mathcal{B})$ is obtained in the following way. Its points $\{b'\}$ correspond bijectively to blocks $\{B\}$ of the original SBIBD, its blocks $\{X'\}$ correspond bijectively to the points $\{x\}$ of the original SBIBD, and $b' \in X'$ if and only if $x \in B$. Hence the incidence matrix for the dual design is the transpose of the one of the original. A SBIBD is not necessarily isomorphic with its dual.

(v) Let $(X, \mathcal{B})$ be a $t-(v,k,\lambda)$ design. Given $s < t$, let S be an s-subset of X. Let $X' = X \setminus S$, and

$$\mathcal{B}' = \{B \setminus S : S \subseteq B, B \in \mathcal{B}\}$$

(i.e., take all blocks containing S, and remove S from them). Then $(X', \mathcal{B}')$ is a $(t-s)-(v-s,k-s,\lambda)$ design.

Proof. (by Sven Reichard) For each of the above constructions we will express the new parameters in terms of the old ones. The fact that these parameters exist will prove that we get BIBDs in each case.

(i) **v'** Since the point set of the complementary design is the same as that of the original design, we have $v' = v$.

b' Taking complements is a bijection on the power set of X, so $b' = b$.

r' Given a point $P \in X$, it is contained in a block B if and only if it is not contained in the complement of B. Since there are b blocks altogether, $r' = b - r$.

k' Each original block contains k points, and a new block is the complement in X of an old block. Hence $k' = v - k$.

λ' Given two points P_1, P_2 in X, λ' is the number of (original) blocks containing neither P_1 nor P_2. Inclusion and exclusion gives $\lambda' = v - 2r + \lambda$.

(ii) **v'** Since $X' = X \setminus B$, $v' = v - k$.

b' All block other than B are kept, so $b' = b - 1$.

r' If $P \neq B$ and $P \in B_i$, then $P \in B_i \setminus B$. Thus P occurs in the same number of blocks as before, so $r' = r$.

k' Since $(X, \mathcal{B})$ is symmetric, any two blocks intersect in λ points. Thus, $k' = |B_i \setminus B| = k - \lambda$.

λ' As seen for r', the set of blocks containing a given point doesn't change. Hence, $\lambda' = \lambda$.

(iii) **v'** Since $X' = B$, $v' = k$.

b' Since we keep all blocks but B, $b' = b - 1$.

r' If $P \in B$, we keep all blocks through P except for B itself. Hence $r' = r - 1$.

k' If $B_i \neq B$, then $B_i' = B_i \cap B$. Hence $k' = \lambda$.

λ' Given two points in B, there are $\lambda - 1$ other blocks containing both of them. Hence, $\lambda' = \lambda - 1$.

(iv) It follows from the definition that $v' = v, k' = k$.

(v) **v'** Since the new point set is $X \setminus S$, $v' = v - s$.

b' The design we start with is a t-design, so in particular, it is an $s - (v, k, \lambda_s)$ design, since $s < t$. Hence there are λ_s blocks containing S, and $b' = \lambda_s$.

r' Given a point $x \in X'$, there are λ_{s+1} blocks containing both x and S. Note that $s + 1 \leq t$. Thus each point appears in $r' = \lambda_{s+1}$ new blocks.

k' Since S is taken out from each block, $k' = k - s$.

λ' Let T be a $t - s$ subset of X'. Then every new block containing T is obtained from an old block containing $S \cup T$, and each such old block gives a new one containing T. Since $|S \cup T| = t$, there are $\lambda (= \lambda_t)$ such blocks, and hence $\lambda' (= \lambda'_{t-s}) = \lambda$.

□

Problem 20. *Consider a projective plane π of order n as a SBIBD with parameters $(n^2 + n + 1, n + 1, 1)$. Remove a line B (block) from the sets of lines (blocks) of π and all points B from the set of points of π and other lines of π. Call the blocks of this BIBD "lines" and the points "points". Call the new BIBD π'. Prove that:*

(A1) For any two distinct points in π' there is a unique line passing through them.

(A2) For any point x and line L not passing through x, there exists a unique line L' passing through x which has no points in common with L (i.e. parallel to L)

(A3) There are 3 non-colinear points

Proof. (by David Kravitz) First of all, let us look to see what kind of 2-design we have. Clearly we lose $n + 1$ points, the number of points in B, and we lose one block, B. The number of blocks each point belongs to does not change, so r stays equal to $n + 1$, this and $vr = bk$ gives us $k' = n$. Certainly the number of blocks a pair belongs to does not increase or decrease, so we still have $\lambda = 1$. Thus, we have a $2-(v', b', k', r', \lambda') = 2-(n^2, n^2+n, n, n+1, 1)$ BIBD π'.

(A1) $\lambda' = 1$ means that each pair is in one and only one block, so for any two distinct points there is a unique line passing through them.

(A2) x is on $n+1$ different lines and L is a line with n points on it. If all $n+1$ lines passing through x share a point with L, then at least two, say X and Y, must share the same point $y \neq x$, since $|L|$ is only n. This would imply that both X and Y contain both x and y, a contradiction since $\lambda' = 1$. Therefore, there is at least one L' passing through x with no points in common with L.

Now, by contradiction suppose that there exist two lines X and Y passing through x with no points in common with L. L is a block L_0 from π minus one element $b \in B$. X and Y are also blocks X_0 and Y_0 from π minus one element each from B, but they must intersect L_0 in exactly one place. This element from B must be b for both of them, anything else would cause them to have nothing in common with L_0. But this means that $X_0 \cap Y_0 = \{b, x\}$, a contradiction since this is more than one element. Thus there is only one line passing through x with no points in common with L.

(A3) We do need to require $n > 2$ for this to be true, because if $n = 2$ then π' consists of 4 elements and 6 blocks, so we can represent it by K_4, which does not have two points not colinear. So, suppose $n > 2$.

Take any point x, and any line L which does not pass through x, there are $(n^2 + n) - (n + 1) = n^2 - 1 > 0$ such lines. Now, from part $(A2)$ we may find a line L' with no points in common with L. Take any point other than x on L', say y, and take a point z on the line L. There must be a line M containing y and z since $\lambda' \geq 1$. $k = n > 2$ so there is a point on M other than y, z, say m. This point cannot be on L or L' because then the intersection of L/L' and M would have both y/z and m, a contradiction since $\lambda' = 1$. Therefore, m, y, z are all non-colinear, so we have three non co-linear points whenever $n > 2$.

□

Problem 21. *Prove the Papus Theorem in the usual Euclidean plane E^2: Let A_1, B_1, C_1 be three distinct points of a line l_1 and A_2, B_2, C_2 be three distinct points of a line l_2. Let point F be the intersection of the lines A_1B_2 and B_1A_2, point E be the intersection of the lines C_1A_2 and A_1C_2, point G be the intersection of the lines B_1C_2 and C_1B_2. Prove that points E, F, G are colinear. You may use any method you wish in your proof.*

(i) What if two out of the three points F, E, G do not exist, i.e. the corresponding pairs of lines are parallel?

(ii) State the analog of the Papus Theorem for a circle. Describe a method you would choose to prove it.

Proof. (by Vasyl Dmytrenko) First, simplify a little bit the problem. Let π be the plane defined by the lines l_1 and l_2. Consider the projection of π on the plane π' such that the image of l_2 is "the line on infinity", i.e. there is no point of π' with preimage on l_2. Such projection Pr exists (see, for example, [Ya]). For any two points X and Y denote by (XY) the line defined by X and Y. Let
$k_1 = Pr(A_1B_2), k_2 = Pr(C_1B_2)$,
$m_1 = Pr(B_1A_2), m_2 = Pr(C_1A_2)$,
$n_1 = Pr(A_1C_2), n_2 = Pr(B_1C_2)$, and let
$A = Pr(A_1), B = Pr(B_1), C = Pr(C_1)$, $F' = Pr(F), E' = Pr(E), G' = Pr(G)$.
Then $k_1 \| k_2$, $m_1 \| m_2$, $n_1 \| n_2$, and E, F, G are colinear iff $(F'E') \| (F'G')$.

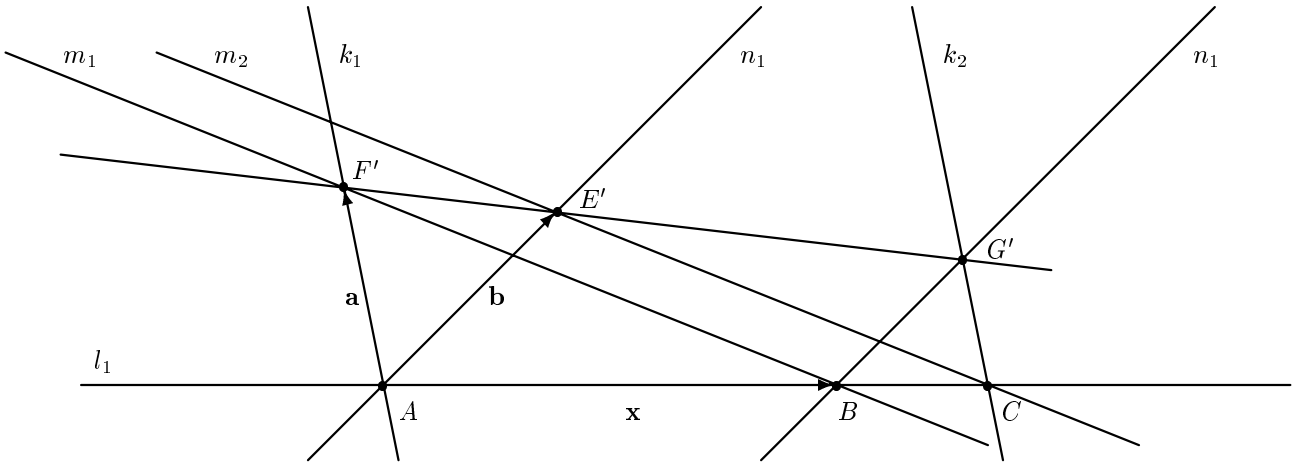

Figure 5:

Now let $\mathbf{a} = \vec{AF'}, \mathbf{b} = \vec{AE'}$, and $\mathbf{x} = \vec{AB} = \alpha\mathbf{a} + \beta\mathbf{b}$ since $\mathbf{a}$ and $\mathbf{b}$ are not colinear. Then $\vec{AC} = \gamma\mathbf{x}$ for some γ, and $\mathbf{a} - \mathbf{x} = \delta(\mathbf{b} - \gamma\mathbf{x})$ for some δ, i.e. $\mathbf{a} - \alpha\mathbf{a} - \beta\mathbf{b} = \delta\mathbf{b} - \gamma\delta\mathbf{a} - \gamma\delta\beta\mathbf{b}$. It yields $\gamma\delta = (\alpha - 1)/\alpha$, and $\alpha = 1 - \beta\gamma$.

Similarly, $\vec{BG'} = \eta\mathbf{b}$ and $\vec{CG'} = \zeta\mathbf{a}$ for some η and ζ. Therefore, $(\gamma - 1)\mathbf{x} + \zeta\mathbf{a} = \eta\mathbf{b}$, that yields $(\gamma - 1)\beta = \eta$ and $\zeta = (\beta\gamma - 1)(\gamma - 1)$.

Finally, $\vec{F'G'} = \gamma\mathbf{x} + \zeta\mathbf{a} - \mathbf{a} = (\gamma - \beta\gamma^2 - 1 + \beta\gamma^2 - \beta\gamma - \gamma + 1)\mathbf{a} + \beta\gamma\mathbf{b} = \beta\gamma(\mathbf{b} - \mathbf{a})$. Thus, $\vec{F'G'} \| \vec{F'E'} = \mathbf{b} - \mathbf{a}$, and E', F', G' (and, therefore, E, F and G) are colinear. □

(i) Suppose that the points F and G do not exist, i.e. $(A_1B_2)\|(B_1A_2)$ and $(B_1C_2)\|(C_1B_2)$.

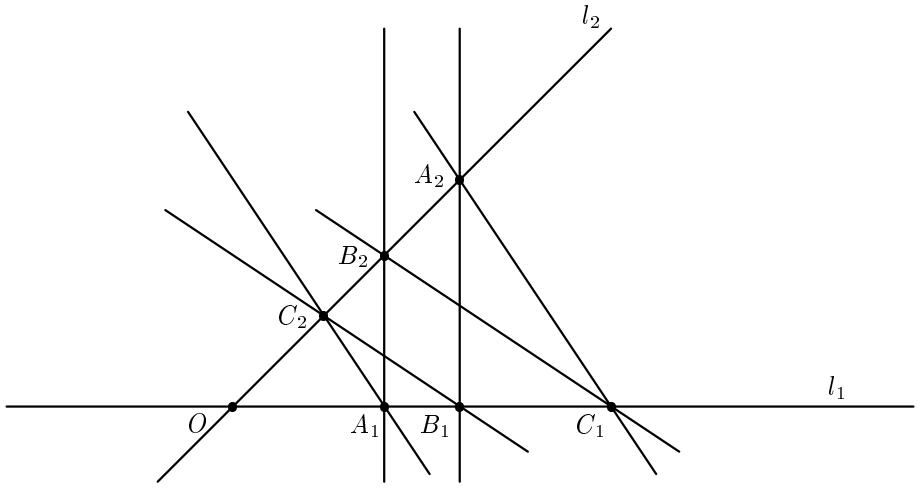

Figure 6:

Let $O = l_1 \cap l_2$. The triangles OA_1B_2 and OB_1A_2 are similar. therefore, $\frac{OA_1}{OB_1} = \frac{OB_2}{OA_2}$. Similarly $\frac{OC_1}{OB_1} = \frac{OB_2}{OC_2}$. It gives

$$\frac{OA_2}{OC_2} = \frac{OA_2/OB_2}{OC_2/OB_2} = \frac{OB_1/OA_1}{OB_1/OC_1} = \frac{OC_1}{OA_1}.$$

Hence, the triangles OA_1B_2 and OB_1A_2 are similar, and $A_1C_2\|C_1A_2$. □

Proof. (by Carl Devore) This output was created by Maple.

Binary Cyclic Self-Orthogonal Codes

Carl Devore <devore@math.udel.edu>

28 June 2000

This program finds the generating polynomials of all binary cyclic self-orthogonal codes of length n for any odd $n > 1$.

Reference: *Introduction to the Theory of Error-Correcting Codes* by Vera Pless (3rd ed., Wiley, 1998), chap. 5, "Cyclic Codes"

```
> restart;
```

n must be odd in this version of the program.

```
> n:= 7:
```

Since n is odd, the factors are distinct. We know that $1 + x$ is a factor, so we only factor $\frac{x^n+1}{1+x} = \sum_{i=0}^{n-1} x^i$.

```
> F:= Factor(add(x^i, i= 0..n-1)) mod 2;
```

$$F := (x^3 + x^2 + 1)\,(x^3 + x + 1)$$

A quirk of Maple requires us to treat the case of a single factor a little differently (only on the next line)..

```
> Fs:= `if`(type(F,`*`), convert(F,set), {F}):
```

Define the reciprocal polynomial.

```
> Recip:=
> p -> expand(x^degree(p)*subs(x= x^(-1), p));
```

$$Recip := p \rightarrow \mathrm{expand}(x^{\mathrm{degree}(p)}\,\mathrm{subs}(x = \frac{1}{x},\, p))$$

Initialize the list of self-orthogonal generators.

```
> SOG:= NULL;
```

$$SOG :=$$

Generate a function that iterates overs all subsets of factors other than $1 + x$.

```
> P:= combinat[subsets](Fs):
```

For each divisor g(x) of $x^n + 1$ containing $1 + x$, check whether the reciprocal of h(x) $= \frac{x^n+1}{\mathrm{g}(x)}$ divides g(x).

```
> while not P[finished] do
> F:= P[nextvalue]();
> g:= (1+x)*convert(F,`*`);
> # h(x) is the product of all factors not used in g
> if Divide(g, Recip(convert(Fs minus F,`*`))) mod 2 then
> SOG:= SOG, g;
> fi;
> od:
```

Print the list of self-orthogonal generators.

```
> linalg[transpose](matrix([[SOG]]));
```

$$\begin{bmatrix} (1+x)\,(x^3+x^2+1) \\ (1+x)\,(x^3+x+1) \\ (1+x)\,(x^3+x^2+1)\,(x^3+x+1) \end{bmatrix}$$

Get the number of self-orthogonal generators.

```
> nops([SOG]);
```

3

□

(ii) *Let γ be a circle, and let $\gamma_1 = \smile A_1C_1$ and $\gamma_2 = \smile A_2C_2$ be arcs of γ_1 such that $\gamma_1 \cap \gamma_2 = \emptyset$. Suppose B_1 and B_2 are points of γ_1 and γ_2 such that $A_1 \neq B_1 \neq C_1$ and $A_2 \neq B_2 \neq C_2$. Let point F be the intersection of the lines A_1B_2* and *B_1A_2, point E be the intersection of the lines C_1A_2* and *A_1C_2, point G be the intersection of the lines B_1C_2* and *C_1B_2. Then the points E, F* and *G are colinear.*

Remark 2. (by Felix Lazebnik) Solving this problem using analytical geometry is a technical challenge.

A more interesting solution can be constructed. It is based on the following idea: since any circle is projectively equivalent to any hyperbola, and a pair of lines is a limiting case of a hyperbola, the problem can be reduced to this case only. Of course, this calls for many justifications.

The problem can be greatly simplified by using one of the facts discussed in class and present in the handout from Yaglom's book. Namely: any circle with a point in its interior can be centrally projected into another circle such that the point is mapped to the center of the image; or, given any circle and a line in its plane which does not cross it, there exists a central projection which carries the circle into another circle and the image of the line becomes the line at infinity. Analytical proofs of these facts can be facilitated by using a symbolic algebra package. Using these ideas, one reduce the problem to a much simpler problem of Euclidean geometry.

Problem 22. *Let C be a circle in the Euclidean plane π, and let O be a point not in the plane. Consider the cone over C with vertex O. Then there is another plane π' that intersects that cone in a circle. If the cone is not right, then π' can be chosen to be not parallel to π.*

Proof. (by Carl Devore) See the corresponding Maple document.
maple document goes here □

Problem 23. *The purpose of this problem is to construct an example of an infinite non-Desarguesian projective plane. The method can be used to build infinite projective planes with other 'defects'. A configuration is a set of elements, called points, and a family of its subsets, called lines, which satisfy the only one axiom:*

(C) two distinct points belong to at most one line.

Examples of configurations are any affine or projective plane, any set of "points" with no lines, set of 10 points and 10 lines of a Desarguesian Theorem.
Let π_0 be a configuration. We are going to define a free projective plane Π, generated by π_0.
Let π_1 be a new configuration, defined in the following way. Points of π_1 are points of π_0. Lines of π_1 are all lines of π_0 and all two element sets of points of π_0 which do not belong to a line of π_0.

(i) Prove that any two points of π_1 lie on one line of π_1. Starting with π_1 we build another configuration π_2 in the following way. Points of π_2 are all points of π_1 and new points which correspond to all two element sets of lines l_1, l_2 of π_1 which do not intersect in π_1. The lines of π_2 are the lines of π_1 extended by new points in the obvious way: if a new point A corresponds to a pair of non-intersecting lines l_1, l_2 of π_1 then A is joined to the set of points of both l_1 and l_2.

(ii) Prove that any two lines of π_2 intersect at one point. But π_2 may loose the property (i). So we continue the construction. For even n we construct π_{n+1} by adding new lines to the set of lines of π_n; for odd n we construct π_{n+1} out of π_n by adding new points and extending some lines of π_n. Let

$$\Pi = \bigcup_{n=0}^{\infty} \pi_n$$

We define points of Π as the union of all points of all π_n. We define lines of Π as those subsets of points L of the set of points of Π such that the intersection of L with the set of points of π_n is a line in π_n for all sufficiently large n (i.e. starting from some $n = n(L)$).

(iii) Prove that if π_0 contains at least four points such that no three of them are colinear, then Π is a projective plane. We call a configuration restricted if every its point belongs to at least three lines, and every its line contains at least three points. It is clear that the Desarquesian configuration is restricted.

(iv) Prove that every restricted configuration from Π is contained in π_0.

(v) Let π_0 be a configuration consisting of four points and no lines, and let Π be the free projective plane generated by π_0. Prove that the Desarquesian Theorem does not hold in Π.

Problem 24. *This problem provides a wide variety of examples of BIBD's.*

Let $V = (F_q)^{n+1}$ be an $(n+1)$–dimensional vector space over the finite field F_q, $n \geq 2$. For a given integer s, $2 \leq s \leq n$, consider the design whose points are the 1–dimensional subspaces of V and whose blocks are the s–dimensional subspaces of V. A point p and a block B are incident if and only if p is a subspace of B.

(i) Prove that the points, blocks, and the incidence define a (b, v, r, k, λ)–BIBD. Compute b, v, r, k, λ in terms of n, q, s.

(ii) Check the result of (i) with what we got before for $n = s = 2$.

(iii) For what values of s the BIBD is symmetric ?
(Hint: It may be helpful first to count the number of all nonsingular $m \times m$ matrices A with the entries from F_q. A way to do this is the following: there are $q^m - 1$ choices for the first row of A. After it is chosen, there are $q^m - q$ ways to choose the second row of A. After the first two rows are chosen, there are ..... ways to choose the third row of A, and so on).

Proof. (by David B. Chandler)

(i) Points are all 1–dimensional subspaces, each of which contains $q-1$ nonzero vectors, and each nonzero vector is in exactly one 1–dimensional subspace. Thus

$$v = \frac{q^{n+1} - 1}{q - 1} = \sum_{i=0}^{n} q^i$$

If we pick any s linearly independent vectors out of $(F_q)^{n+1}$ we determine an s–dimensional subspace. There are

$$\frac{\prod_{i=1}^{s}(q^{n+1} - q^{i-1})}{s!}$$

ways to pick those vectors, because each successive vector is picked from all the vectors of $(F_q)^{n+1}$ which do not lie in the subspace determined by the previously picked vectors. Each subspace is determined by each set of s independent vectors inside it. There are

$$\frac{\prod_{i=1}^{s}(q^{s} - q^{i-1})}{s!}$$

such sets, so the total number of blocks or s–dimensional subspaces is

$$b = \frac{\prod_{i=1}^{s}(q^{n+1} - q^{i-1})}{\prod_{i=1}^{s}(q^{s} - q^{i-1})} = \prod_{i=1}^{s} \frac{(q^{n+2-i} - 1)}{(q^i - 1)}$$

The $q^s - 1$ nonzero vectors of an s–dimensional subspace are partitioned into the $q - 1$ nonzero vectors in each 1–dimensional subspace inside, so

$$k = \frac{q^s - 1}{q - 1}$$

Each 1–dimensional subspace is incident with the same number of s–dimensional subspaces, because we can require the first vector to be picked from that subspace. The number of ways to pick the remaining $s - 1$ vectors does not depend on what was picked first. We have

$$r = \frac{bk}{v} = \prod_{i=1}^{s} \frac{(q^{n+2-i} - 1)}{(q^i - 1)} \times \frac{(q^s - 1)}{(q - 1)} \div \frac{(q^{n+1} - 1)}{(q - 1)} = \prod_{i=1}^{s-1} \frac{(q^{n+i-s+1} - 1)}{(q^i - 1)}$$

Again, having picked two 1–dimensional subspaces, the number of ways to complete to an s–dimensional space does not depend on which two vectors we started with, so we have a 2 design, and

$$\lambda = \frac{(k-1)r}{v-1}$$

$$= (\frac{q^s - 1}{q - 1} - 1) \times \prod_{i=1}^{s-1} \frac{(q^{n+i-s+1} - 1)}{(q^i - 1)} \div (\frac{q^{n+1} - 1}{q - 1} - 1)$$

$$= \frac{(q^{s-1} - 1)}{(q^n - 1)} \prod_{i=1}^{s-1} \frac{(q^{n+i-s+1} - 1)}{(q^i - 1)}$$

$$= \prod_{i=1}^{s-2} \frac{(q^{n+i-s+1} - 1)}{(q^i - 1)}$$

(ii) If we let $n = s = 2$ we get

$$v = \sum_{i=0}^{2} q^i = q^2 + q + 1$$

$$b = \prod_{i=1}^{2} \frac{(q^{4-i} - 1)}{(q^{3-i} - 1)} = \frac{(q^3 - 1)(q^2 - 1)}{(q^2 - 1)(q - 1)} = q^2 + q + 1$$

$$k = \frac{q^2 - 1}{q - 1} = q + 1$$

$$r = \frac{q^{2+1-2+1} - 1}{q - 1} = q + 1$$

and λ is a nil product or $\lambda = 1$.

(iii) The BIBD is symmetric only if $n = s$. If $n > 2$ and $s = 2$, notice that from the formulae, $b > v$. As s increases, v remains fixed while b increase until $s > n + 2 - s$ or $s > n/2 + 1$. Then b decreases until $s = n$. □

Problem 25. *Two designs $(X, \mathcal{B})$ and $(X', \mathcal{B}')$ are called isomorphic if there exist two bijection $f : X \to X'$ and $g : \mathcal{B} \to \mathcal{B}'$ such that $x \in B \iff f(x) \in g(B)$ for each $x \in X$ and each $B \in \mathcal{B}$. Equivalently, the incidence matrices of isomorphic designs are obtained one from another by permutations or rows and columns. Prove that there exists a SBIBD design not isomorphic to its dual.*

Proof. (by Jason Williford)

Listed below is a design $(X, \mathcal{B})$ and its dual with the parameters $v = b = 15, r = k = 7, \lambda = 3$.

B_0 :	0	1	2	3	4	5	6
B_1 :	0	1	2	7	8	9	10
B_2 :	0	1	2	11	12	13	14
B_3 :	0	3	4	7	8	11	12
B_4 :	0	3	4	9	10	13	14
B_5 :	0	5	6	7	8	13	14
B_6 :	0	5	6	9	10	11	12
B_7 :	1	3	5	7	9	11	13
B_8 :	1	3	6	7	10	12	14
B_9 :	1	4	5	8	10	11	14
B_{10} :	1	4	6	8	9	12	13
B_{11} :	2	3	5	8	10	12	13
B_{12} :	2	3	6	8	9	11	14
B_{13} :	2	4	5	7	9	12	14
B_{14} :	2	4	6	7	10	11	13

The next table is the dual, which we denote $(X', \mathcal{B}')$

B'_0 :	0	1	2	3	4	5	6
B'_1 :	0	1	2	7	8	9	10
B'_2 :	0	1	2	11	12	13	14
B'_3 :	0	3	4	7	8	11	12
B'_4 :	0	3	4	9	10	13	14
B'_5 :	0	5	6	7	9	11	13
B'_6 :	0	5	6	8	10	12	14
B'_7 :	1	3	5	7	8	13	14
B'_8 :	1	3	5	9	10	11	12
B'_9 :	1	4	6	7	10	12	13
B'_{10} :	1	4	6	8	9	11	14
B'_{11} :	2	3	6	7	9	12	14
B'_{12} :	2	3	6	8	10	11	13
B'_{13} :	2	4	5	7	10	11	14
B'_{14} :	2	4	5	8	9	12	13

We seek to prove that the two are not isomorphic. To do this, consider the first three columns of the last table. Upon inspection, it can be seen B'_0 has the property that for each $i \neq 0$ there is a $j \neq 0$ such that $|B'_0 \cap B'_i \cap B'_j| = 3$.

Claim: No set B_i in $(X, \mathcal{B})$ has this property.

To see we must show that for each B_i there is a B_j and a B_k such that $|B_i \cap B_j \cap B_k| = 2$. This is sufficient, as if there is a forth set B_l such that $|B_0 \cap B_i \cap B_l| = 3$, then $B_0 \cap B_i \cap B_l = B_0 \cap B_i$ (as $\lambda = 3$) implying $|B_0 \cap B_i \cap B_j \cap B_l| = 2$. This violates the $\lambda = 3$ condition of this design.

We then must find such an example for each block in $(X, \mathcal{B})$. Each example shows that all three of the sets in the intersection do not have this property, so each example serves a triple purpose.

$B_0 \cap B_{13} \cap B_{14} = \{2, 4\}$; $B_1 \cap B_7 \cap B_8 = \{1, 7\}$;

$B_2 \cap B_9 \cap B_{12} = \{11, 14\}$; $B_3 \cap B_{10} \cap B_{11} = \{8, 12\}$; $B_4 \cap B_7 \cap B_{12} = \{3, 9\}$; $B_5 \cap B_7 \cap B_{11} = \{5, 13\}$; $B_6 \cap B_7 \cap B_9 = \{5, 11\}$;

Therefore this design is not isomorphic to its dual. □

Problem 26. *Given a graph G and its subgraph H, we say that H decomposes G if G is an edge-disjoint union of isomorphic copies of H. For example, $2K_2$ decomposes K_4 and C_5 decomposes K_5. Prove that K_{t+1} decomposes K_{t^2+t+1} if and only if there exists a projective plane of order t.*

Proof. (by David B. Chandler)

First suppose that K_{t+1} decomposes K_{t^2+t+1}. Then we define the points of the projective plane to be the $t^2 + t + 1$ vertices of K_{t^2+t+1}. We define the lines of the projective plane to be the sets of vertices which are connected in the individual copies of K_{t+1} which decompose K_{t^2+t+1}. Each pair of vertices

in K_{t^2+t+1} is connected by exactly one edge, and that edge lies in exactly one copy of K_{t+1} in the decomposition. Therefore, each pair of points determines exactly one line in the plane and $\lambda = 1$. The number of lines is the number of copies of K_{t+1} in K_{t^2+t+1}, hence it is $\frac{|K_{t^2+t+1}|}{|K_{t+1}|} = \frac{(t^2+t+1)(t^2+t)/2}{(t+1)t/2} = t^2+t+1$. Therefore we have the same number of lines as points. Finally, the degree of each vertex in K_{t^2+t+1} is t^2+t and t of those edges are in each copy of K_{t+1} with which that vertex is incident. Since $\frac{t^2+t}{t} = t+1$, then each point is in $t+1$ lines. Thus we have a 2–$(t^2+t+1, t+1, 1)$ symmetric design—a projective plane of order t.

Now suppose that there exists a projective plane of order t. Simply reverse the construction, calling the points of the plane the vertices of K_{t^2+t+1} and the lines of the plane the copies of K_{t+1} which decompose K_{t^2+t+1}. Every edge will be covered exactly once because each pair of points determines one line. □

Problem 27. *Let D be a (v, k, λ), difference set in a group G, $1 \leq \lambda \leq k \leq v$. Show that it can be used to construct a $2-(v, k, \lambda)$ design.*

This gives a general method of building SBIBDs from difference sets. Apply the method to build a SBIBD with parameters $(11, 5, 2)$. List all blocks of this design.

Proof. (by David Kravitz)

i. Here is the table of differences within this set:

	1	5	6	8
1	0	4	5	7
5	9	0	1	3
6	8	12	0	2
8	6	10	11	0

Certainly, every element in G can be written as a difference of two elements in exactly one way, as each element appears exactly once within the table.

ii. q is the number of elements in the field, so we know the first parameter is certainly q. It is a well-known fact that $f : x \longmapsto x^2$ is a 2-1 mapping on the $q-1$ nonzero elements on a field of order q. Thus, there are $\frac{q-1}{2}$ nonzero squares, and thus the second parameter is correct.
The last parameter is equal to exactly $\frac{1}{4}$ of the number of solutions (x, y) to the equation $x^2 - y^2 = a^2$, since if (x, y) is a solution then so is $(\pm x, \pm y)$. Now, we know that there are $q-1$ solutions (u, v) to the equation $uv = a^2$, as for any nonzero v we have the solution $(v^{-1}a^2, v)$. The question is how

many of these solutions (u, v) correspond to an equation (x, y). Since $x^2 - y^2 = (x + y)(x - y)$, so we have the equations $u = x + y, v = x - y$, implying $(x, y) = (\frac{1}{2}(u + v), \frac{1}{2}(u - v))$, so we have an (x, y) solution if and only if both $u + v$ and $u - v$ are nonzero. We need to know how many times they are zero.

$$u \pm v = v^{-1}a^2 \pm v = v(v^{-2}a^2 \pm 1)$$

So, there are two possible values of v making this zero, when $v = \pm a$. Thus, there are $q - 1 - 2 = q - 3$ solutions (x, y), and this means there are $\frac{1}{4}(q - 3)$ total solutions, and we are done.

□

Problem 28. *Let D be a (v, k, λ), difference set in a group G, $1 \leq \lambda \leq k \leq v$. Show that it can be used to construct a $2 - (v, k, \lambda)$ design.*

This gives a general method of building SBIBDs from difference sets. Apply the method to build a SBIBD with parameters $(11, 5, 2)$. List all blocks of this design.

Proof. (by F. Fiedler) Let $\mathcal{B} = \{D \cdot x \mid x \in G\}$ where G is written multiplicatively and $D \cdot x = \{d \cdot x \mid d \in D\}$ is the element-wise product. Let $\mathcal{P} = G$ as a set, $\mathcal{I}$ be inclusion. Then the incidence structure $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ is a 2-(v, k, λ) design with $v = |G|$, $k = |D|$, and λ.

Proof. Let $B_1, B_2 \in \mathcal{B}$. Hence there exist $x_1, x_2 \in G$ such that $B_1 = D \cdot x_1$ and $B_2 = D \cdot x_2$. Let e denote the identity in G.

$$\begin{aligned} \implies \qquad |B_1 \cap B_2| &= |\{(d_1, d_2) \mid d_1, d_2 \in D \wedge d_1 x_1 = d_2 x_2\}| \\ &= \left|\left\{(d_1, d_2) \mid d_1, d_2 \in D \wedge d_1^{-1} d_2 = x_1 x_2^{-1}\right\}\right| \\ &= \begin{cases} \lambda & \text{if } x_1 x_2^{-1} \neq e \\ k & \text{if } x_1 x_2^{-1} = e \end{cases} \end{aligned}$$

Thus, whenever $k \neq \lambda$, necessarily we have $x_1 \neq x_2$ if $B_1 \neq B_2$. Suppose $k = \lambda$. Since D is a difference set we have $\frac{k^2 - k}{v - 1} = \lambda = k$. This implies $k = v$ which we excluded (since it does not yield an *incomplete* block design). This means that the x_i are uniquely determined.

Hence two distinct blocks intersect in λ points. By construction there are $v = |G|$ blocks each of cardinality $k = |D|$. There are $v = |\mathcal{P}| = |G|$ points. If $x \in \mathcal{P}$ then there are $r = |D| = k$ blocks incident with x (by construction of $\mathcal{B}$ as shifts of D). Thus $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ is a 2-(v, k, λ) design. Note that G need not be abelian. □

Consider $\mathbb{Z}_{11}$, a cyclic group of order 11. Since $11 \equiv 3 \pmod 4$ the non-zero squares in $\mathbb{Z}_{11}$ form a (cyclic) difference set. Let $D = \{1, 3, 4, 5, 9\}$. By above result, the shifts of D by all elements of $\mathbb{Z}_{11}$ yield a 2-$(11, 5, 2)$ design ($\lambda = \frac{k^2-k}{v-1}$). Let B_i denote the shift of D by i.

B_0	1	3	4	5	9
B_1	2	4	5	6	10
B_2	0	3	5	6	7
B_3	1	4	6	7	8
B_4	2	5	7	8	9
B_5	3	6	8	9	10
B_6	0	4	7	9	10
B_7	0	1	5	8	10
B_8	0	1	2	6	9
B_9	1	2	3	7	10
B_{10}	0	2	3	4	8

□

Problem 29. *Let A be a nonsingular $n \times n$ matrix with real entries, and let a_i be the ith row of A_i, $i \in [n]$, considered as vectors in $\mathbb{R}^n$ with the standard inner product. Prove that*

$$|\det A| \leqslant ||a_1|| \cdots ||a_n|| ,$$

with equality iff every two rows are orthogonal.

Proof. (by Sukhendu Mehrotra) We consider the more general case when the row vectors of A are vectors in $\mathbb{C}^n$. It is clear from the Gram-Schmidt orthogonalization algorithm that there exits a lower-triangular matrix M with positive entries on its main diagonal such that MA is a unitary matrix U. Rewrite

$$MA = U$$

as

$$AU^{-1} = M^{-1}$$

Since U^{-1} is a unitary matrix, observe that $\det(A) = \det\left(M^{-1}\right)$. Also, note that the set of nonsingular $n \times n$ lower-triangular complex matrices (with positive entries on the main diagonal), T, is a multiplicative group, so that M^{-1} is lower-triangular (with positive entries on the main diagonal). Further note that the result is certainly true for all matrices in T. Thus, all we need to show in order to establish the result for *all* nonsingular matrices is to show that the product of the norms of the rows of A, and their relative directions are the same as those of the rows of M^{-1}. But this is clear, since U^{-1} is unitary and preserves norms and directions. This completes the proof. □

Problem 30. *Let L be a Latin square of order 6. Let Γ be a simple graph with $V(\Gamma) = \{v_{ij} : (i,j) \in [6]^2\}$. We say that each v_{ij} corresponds to the (i,j) cell of L. Define two vertices to be adjacent in Γ if and only if the corresponding cells of L lie in the same row, or the same column or contain the same entry. Let H be the adjacency matrix of Γ with each zero replaced by -1. Prove that H is a Hadamard matrix of order 36. Will a similar method lead to a Hadamard matrix if we start with an arbitrary Latin square of order $2t \geq 4$?*

Proof. (by Jason Williford) Let L' be an arbitrary Latin Square of order n, and construct the graph Γ' and the matrix H' as described above. As every entry of H' is -1 or 1, it is clear that the diagonal entries of $H'(H')^T$ will be n^2. We must prove all entries of $H'(H')^T$ not on the diagonal are zero.

Let us denote the entry of H' in the v_{ij} row and the v_{kl} column by $a_{ij,kl}$. Each entry of $H'(H')^T$ is of the form $\sum_{(k,l)\in[n]^2} a_{ij,kl}a_{mn,kl}$. The product $a_{ij,kl}a_{mn,kl} = 1$ iff $a_{ij,kl} = a_{mn,kl}$ which implies that v_{kl} is a mutual neighbor or a mutual non-neighbor of v_{ij} and v_{mn}. The product will be -1 otherwise.

Let $A_{ij,mn}$ be the set of mutual neighbors of v_{ij} and v_{mn}, and $B_{ij,mn}$ be the set of mutual non-neighbors of v_{ij} and v_{mn}. We will have $\sum_{(k,l)\in[n]^2} a_{ij,kl}a_{mn,kl} = 0$ iff there are as many ones as negative ones in this sum, therefore we have:

$|A_{ij,mn}| + |B_{ij,mn}| = n^2/2$

We have 4 cases to consider:

(i) The value of the (i,j) entry of L' is equal to the (m,n) entry of L'.

(ii) $i = m$

(iii) $j = n$

(iv) $i \neq m, j \neq n$ and the (i,j) and (m,n) entries of L' are not equal.

All cases are mutually exclusive by the properties of a Latin square.

In the first case, there are n-2 entries of L' with the same value as ij and mn, thus the corresponding vertices are in $A_{ij,mn}$. Also, $v_{in}, v_{mj} \in A_{ij,mn}$ as entries in the same row or column are connected in Γ'. Thus $|A_{ij,mn}| = n$. To count mutual non-neighbors, we ignore columns j and n and rows i and m, leaving $(n-2)^2$ entries. Also, in each of these remaining columns, there will be an entry equal to the ij entry (there must be one such entry in every column, and it cannot be in rows i or m as this would put two entries with the same value in the same row). Therefore $|B_{ij,mn}| = (n-2)^2 - n + 2$

Thus we have $(n-2)^2 + 2 = n^2/2$ which has the solutions $n = 2, 6$. Thus the resulting matrix is Hadamard only if $n = 2, 6$.

In the second case $i = m$, the $n-2$ vertices corresponding to the other entries in the ith row are mutual neighbors of v_{ij} and v_{in}. Also, there must be an entry in the nth column equal to entry (i,j), and an entry in the jth column equal to entry (i,n). Thus $|A_{ij,mn}| = n$.

To count mutual non-neighbors, we ignore the ith row and columns j and n. In each of the remaining columns of L' there will be one entry equal to the

(i,j) entry and one equal to the (i,n) entry, and neither of these will be in row i. This leaves $n-3$ entries in each column which are in $B_{ij,mn}$.

Therefore we have $(n-2)(n-3)+n = n^2/2$ which has roots 2 and 6.

The third case is resolved in the same manner as the second case.

The last case cannot happen if n=2 (the diagonal entries must be equal) so we consider it for n=6 only. In row i and column j there must be an entry equal to entry (m,n), and in row m and column n there must be an entry equal to entry (i,j). Also $v_{in}, v_{mj} \in A_{ij,mn}$, for a total of 6 elements in $A_{ij,mn}$.

To count mutual non-neighbors, $v_{ij}, v_{mn} \in B_{ij,mn}$. Ignoring the i and m rows and j and n columns, there are 4 truncated columns left. The value of the (i,j) entry must appear in exactly three of these truncated columns. It will not appear in one truncated column as the value of entry (i,j) must appear in row m once, in a column other than j or n. Similarly, the value of the (m,n) entry will appear in 3 of these truncated columns, leaving $(4)^2-6$ entries which are in $B_{ij,mn}$, so total $|B_{ij,mn}| = (4)^2-6+2 = 12$

Therefore $|A_{ij,mn}| + |B_{ij,mn}| = 12+6 = 6^2/2$.

H' is then Hadamard iff $n = 2, 6$

□

Problem 31. *Let 2-(v,k,λ), $k \le v/2$, be a SBIBD and $n = k-\lambda$. Prove that $4n-1 \le v \le n^2+n+1$. So for a given n, $2-(4n-1, 2n-1, n-1)$ Hadamard designs and projective planes of order n are extremal with respect to v (if they exist).*

Proof. (by Felix Lazebnik) The restriction $k \le v/2$ will be used in the proof, but it is not necessary: if $k > v/2$, one can consider the complementary design. Since $k \le v/2$, then $\lambda(v-1) = k(k-1) \le v(v-2)/4 < (v-1)^2/4$. Hence $\lambda < (v-1)/4 < k/2$. Then $n = k-\lambda > k/2 > \lambda$. Therefore $1 \le \lambda \le n-1$. Let $f(\lambda) := v-1 = k(k-1)/\lambda = \frac{(n+\lambda)(n+\lambda-1)}{\lambda}$. The only critical point of $f(\lambda)$ on $[1, n-1]$, is $\lambda_0 = \sqrt{n^2-n}$. Since $f(1) = n^2+n$, $f(n-1) = 4n-2 < f(1)$, and $f(\lambda_0) = 2n+2\sqrt{n^2-n}-1 \in (4n-3, 4n-2)$, the maximum and minimum integer values of $f(\lambda)$ on $[1, n-1]$ are n^2+n and $4n-2$, respectively. □

The following elegant (though a little tricky) argument which establishes the same inequalities is from E.F. Assmus Jr. and J.D. Key, Designs and Their Codes, Cambridge University Press, Cambridge, 1993, p. 119.

Proof. Start with the relation $\lambda(v-1) = k(k-1)$. This implies that λ also divides $(k-\lambda)(k-\lambda-1) = n(n-1)$. Let $\lambda\mu = n(n-1)$. Since $n(n-1)$ is never a perfect square, $\lambda \ne \mu$. Then $(\lambda-\mu)^2 = v^2-4n(v-1) > 0$, hence $v^2-4n(v-1)-1 \ge 0$, i.e. $(v-1)(v-4n+1) \ge 0$, giving the lower bound, $4n-1$, for v. To get the upper bound, simply notice that for the positive integers λ and μ, we have $\lambda+\mu \le \lambda\mu+1$, so that $v = 2n+\lambda+\mu \le n^2+n+1$. □

Problem 32. *Given a $t-(v,k,\lambda)$ design. Show that each point belongs to the same number r of blocks. Express r in terms of t,v,k,λ.*

Proof. (by Sven Reichard) Let x be a point, and suppose it belongs to r blocks. Let us count pairs l,b, where b is a block, l is a set of t points, and $x \in l \subseteq b$.

If we choose l first, there are $\binom{v-1}{t-1}$ choices such that l contains x. Since l is contained in λ blocks, the total number is $\lambda\binom{v-1}{t-1}$.

If we choose b first, there are r choices for b. It contains k points altogether, so there are $\binom{k-1}{t-1}$ subsets of b containing x. We get a total of $r\binom{k-1}{t-1}$ pairs.

Comparing the two result, we find that

$$r = \frac{\lambda\binom{v-1}{t-1}}{\binom{k-1}{t-1}} = \frac{\lambda(v-1)!(k-t)!}{(k-1)!(v-t)!}$$

Since this expression doesn't depend on x, the statement is proven. □

Problem 33. *A conference matrix C of order n is an $n \times n$ matrix with zeros on the diagonal, all other entries equal to $+1$ or -1, and $CC^T = (n-1)I$.*

(i) Prove that if the order n of a conference matrix C is greater than one, then it is even.

(ii) Prove that by multiplying certain rows and columns of a conference matrix by -1, one can turn it into a symmetric conference matrix if $n \equiv 2 \pmod 4$, and into an antisymmetric matrix if $n \equiv 0 \pmod 4$.

(iii) If C is an antisymmetric matrix , then $I + C$ is a Hadamard matrix. Is the converse statement correct ?

(iv) Show how one can construct a Hadamard matrix of order $2n$ starting with a symmetric conference matrix of order n.

Proof. (by Vasyl Dmytrenko) First, note that after multiplication of some columns and rows of a conference matrix C by -1 we get a conference matrix. Indeed, multiplication, say, of columns is equivalent to multiplication by the respective diagonal matrix D with 1 and -1 entries on the diagonal. Then $(CD)(CD)^T = CDD^TC^T = CC^T = (n-1)I$, and the diagonal entries of CD are zeros.

Note also that, for any i and j, "simultaneous" permutations of i-th and j-th rows and i-th and j-th columns keeps C to be a conference matrix. It follows that, for any permutation matrix P, PCP is a conference matrix.

(i) Let $C = (c_{ij})$ be a conference n by n matrix, and let k be the number of columns containing the (nonzero) entries of the same sign in the first and the second rows. Since the scalar product of the rows is 0, the number of columns

with entries of opposite signs in these rows is also k, and there are additionally 2 columns with zero entries. Thus, we have $2 + k + k = n$, i.e. n is even.

(ii) For $n = 2$ the statement is trivial. Let $n \geq 4$. Multiply the columns of C to turn all nonzero entries of the first row to 1's. Then multiply the rows to get all 1's in the first column (except, of course, c_{11}) if $n \equiv 2 \pmod 4$, and transform these entries to -1's if $n \equiv 0 \pmod 4$. Show that we get a symmetric matrix in the first case and antisymmetric one in the second.

Let $x := c_{ij}$ be an entry of $C, 1 < i \neq j > 1$, and let $y := c_{ji}$. It is easy to see that, for any permutation matrix P, C and PCP have the same symmetry. Therefore, we may assume that $i = 2$ and $j = 3$.

Let $S := \{(c_{2i}, c_{3i}), 4 \leq i \leq n\}$, and let $k_1 = |\{s \in S : s = (1,1)\}|$, $k_2 = |\{s \in S : s = (1,-1)\}|$, $k_3 = |\{s \in S : s = (-1,1)\}|$, $k_4 = |\{s \in S : s = (-1,-1)\}|$. Counting the number of entries in a row and using orthogonality of rows, we get

$$\begin{aligned} k_1 + k_2 + k_3 + k_4 &= n - 3; && (0.6)\\ x + k_1 + k_2 - k_3 - k_4 &= 0; && (0.7)\\ y + k_1 - k_2 + k_3 - k_4 &= 0; && (0.8)\\ 1 + k_1 - k_2 - k_3 + k_4 &= 0. && (0.9) \end{aligned}$$

Now (1) + (4) gives

$$k_1 + k_4 = \frac{n-4}{2}, \tag{0.10}$$

and then from (1)

$$k_2 + k_3 = \frac{n-2}{2}, \tag{0.11}$$

Also, (2) − (3) and (2) + (3) yield

$$\begin{aligned} x - y &= 2(k_3 - k_2); && (0.12)\\ x + y &= 2(k_4 - k_1). && (0.13) \end{aligned}$$

¿From (8) $k_4 - k_1 = 1, 0$ or -1. Consider the possible cases.

If $k_4 = k_1 + 1$, then $x = y = 1$, and from (7) and (6) $k_2 = k_3 = \frac{n-2}{4}$. Therefore, $n \equiv 2 \pmod 4$, and since $x := c_{ij} = y := c_{ji}$ for any i and j, the matrix C is symmetric.

Similarly, $k_4 = k_1 - 1$ yields $x = y = -1$, $n \equiv 2 \pmod 4$, and C is symmetric.

Finally, if $k_4 = k_1$, then $x = -y$, $k_3 - k_2 = 1$ or -1, and (again from (6)) $k_3 = \frac{n-4}{4}$ or $k_3 = \frac{n}{4}$ respectively. In both cases we conclude that $n \equiv 0 \pmod 4$, and C is antisymmetric.

(iii) Let C be an $n \times n$ antisymmetric conference matrix. Then $n \equiv 0 \pmod 4$ by (ii). Set $H := I + C$. Then $HH^T = (I+C)(I+C)^T = I + C + C^T + CC^T = I + (n-1)I = nI$, since $C + C^T = 0$. Thus, H is a Hadamard matrix.

Now let H be a Hadamard matrix. Let $C := H - I$. Then, of course, C may not be a conference matrix even if $n \equiv 0 \pmod 4$. For example, if H is a

2×2 Hadamard matrix (there is the only such matrix up to column and row multiplications), then $H \otimes H$ is a Hadamard matrix, but $H \otimes H - I_4$ is not antisymmetric, therefore, is not a conference matrix.

(iv) Let C be an $n \times n$ symmetric conference matrix, $CC^T = (n-1)I_n$, $C = C^T$. Consider the matrix

$$H = \begin{pmatrix} I_n + C & -I_n + C \\ -I_n + C & -I_n - C \end{pmatrix}$$

Due to the symmetry of C, we get $HH^T =$

$$\begin{pmatrix} I_n + C + C^T + CC^T + I_n - C - C^T + CC^T & -I_n + C^T - C + CC^T + I_n + C^T - C - CC^T \\ -I_n - C^T + C + CC^T + I_n - C^T + C - CC^T & I_n - C^T - C + CC^T + I_n + C^T + C + CC^T \end{pmatrix}$$

$$= \begin{pmatrix} 2(I_n + CC^T) & 0 \\ 0 & 2(I_n + CC^T) \end{pmatrix} = \begin{pmatrix} 2nI_n & 0 \\ 0 & 2nI_n \end{pmatrix} = 2nI_{2n}.$$

Thus, H is a Hadamard $2n \times 2n$ matrix. □

Proof. (by Sukhendu Mehrotra)

(i) Assume $n > 2$, and let $C = (a_{ij})$. Since $CC^T = (n-1)\,I$, it is clear that there must be as many 1-1 pairs among the $((a_{1j}), (a_{2j}))$ as there are 1-(-1),(-1)-1 pairs. There are $n-2$ such pairs in all. Therefore, $n \equiv n-2 \equiv 0 \pmod 2$

(ii) (Following the hint in Van Lint and Wilson) Multiplying the columns of C by -1 if necessary, first covert all the entries in the first row to 1. Similarly, convert all the entries in the first column to 1 if $n \equiv 2 \pmod 4$, and -1 if $n \equiv 0 \pmod 4$, to obtain a matrix C'. Observe that any row-column permutation preserving the main diagonal of C' is represented by

$$PC'P^T$$

where P is a permutation matrix, and does not alter the symmetry or antisymmetry of C'. Thus, it suffices to show that the (2,3)-th entry of C' is the same as its (3,2)-th entry if $n \equiv 0 \pmod 4$, and the negative of its (3,2)-th entry otherwise.

Denote the (2,3)-th entry of C' by p and its (3,2)-th entry by q. Consider the case when $n \equiv 2 \pmod 4$. Denote the number of 1-1-1 triples occurring in the first three rows of C' by a, the number of 1-1-(-1) triples by b, the number of 1-(-1)-1 triples by c and the number of 1-(-1)-(-1) triples by d. As in the proof of the fact that Hadamard matrices of order greater than 2 have order a multiple of 4, obtain the equations

$$\begin{aligned} a + b + c + d &= n - 3 \\ a + b - c - d &= -p \\ a - b - c + d &= -1 \\ a - b + c - d &= -q \end{aligned}$$

Add these equations to obtain $4a = (n-4) - (p+q)$. The condition $n \equiv 2 \pmod 4$ requires $p+q = 2 or -2$, and thus $p = q$ in this case. This, and the observation above imply that C' is symmetric.

The other case is treated in exactly the same way.

(iii) The converse is false. The matrix B

$$\begin{bmatrix} 0 & 1 & -1 & 1 \\ 1 & 0 & 1 & -1 \\ -1 & 1 & 0 & 1 \\ 1 & -1 & 1 & 0 \end{bmatrix}$$

is not a conference matrix but $I + B$ *is* a Hadamard matrix.

(iv) The matrix

$$\begin{bmatrix} I+C & -I+C \\ -I+C & -I-C \end{bmatrix}$$

is easily seen to be a Hadamard matrix.

□

Problem 34. *(i) Is it possible to find eight binary vectors in $\mathbb{F}_2^6$ such that the distance between them is at least 3 ?*

(ii) Is it possible to find nine binary vectors in $\mathbb{F}_2^6$ such that the distance between them is at least 3 ?

Solution. (by Sukhendu Mehrotra)

(i) Consider the linear subspace of $\mathbb{F}_2^6$

$$\begin{aligned} \{&(0,0,0,0,0,0), \\ &(1,1,1,0,0,0), \\ &(0,0,1,1,1,0), \\ &(1,1,0,1,1,0), \\ &(0,1,0,1,0,1), \\ &(1,0,1,1,0,1), \\ &(0,1,1,0,1,1), \\ &(1,0,0,0,1,1)\} \end{aligned}$$

generated by $(1,1,1,0,0,0)), (0,0,1,1,1,0))$ and $(0,1,0,1,0,1))$. Since the minimum weight of this code is 3, it furnishes an example of eight vectors in $\mathbb{F}_2^6$ such that the minimum distance between them is 3.

(ii) It is not possible to find a code of size 9 with minimum distance 3 in $\mathbb{F}_2^6$. Assume, by way of contradiction, that such a code exists. Since there are only four possible choices for the first two coordinates of the codewords, at least three of the codewords begin with the same pair of coordinates. This implies the existence of a code of size 3 and minimum distance 3 in $\mathbb{F}_2^4$. No such code exists: For we may assume, without loss of generality, that the vector (1,1,1,1) belongs to the code, and this precludes the presence of vectors of weight 2 or 3 and disallows more than one vector from the remaining set of vectors of weight 1 or 0 in the code. □

Proof. (by David Chandler)

(i) Yes, it is possible to find eight binary vectors in F_2^6 such that the distance between any two of them is at least 3. Start with H, the check matrix for the binary Hamming code of length 7 and dimension 4. This code has 16 vectors. Arbitrarily delete one of the columns from H. Clearly the columns are still pairwise linearly independent. Thus the code determined by this check matrix has minimum distance at least 3. This code has length 6 and dimension $3 = 6-3$, the length minus the dimension of the check matrix, and has $8 = 2^3$ vectors.

(ii) It is not possible to find nine binary vectors in F_2^6 such that the distance between any two of them is at least 3. There are $2^6 = 64$ possible vectors in the code. Using the Hamming ball-packing constraint, we see that each code vector must be surrounded by 6 unused vectors of its own. Each of the nine codewords would occupy 7 vectors so altogether 63 out of 64 vectors must be within a distance of one of a codeword. Without loss of generality we can assume that the zero vector is a codeword. The minimum weight of the remaining codewords is 3. Consider vectors of weight 2. All but one of them must be within a distance 1 of a codeword, which has to have weight 3 since there are no codewords of weight 1 or 2. Each codeword of weight 3 is adjacent to 3 vectors of weight 2. There are $\binom{6}{2} = 15$ vectors of weight 2, at least 14 of which must be adjacent to exactly one codeword of weight 3, requiring that there be 5 codewords of weight 3. Rearranging the components if necessary, assume that (111000) is a codeword. Each pair of codewords of weight 3 must have in common a 1 in at most one position to have distance not less than 3. If (000111) were a codeword, no more codewords of weight 3 would fit, so the possibilities for the first three positions are $(100xxx)$, $(010xxx)$, and $(001xxx)$. The possibilities for the second three positions are $(xxx110)$, $(xxx101)$, and $(xxx011)$. Any pair of these have a common 1 in the last three positions, so there cannot be a common 1 in the first three positions. Nor can there be two common 1's in the second three positions. Clearly only three more codewords are possible of weight 3 for a total of four, making it impossible to construct the nine codewords of minimum distance 3.

Note that any 3 of the codewords just constructed form a basis for the linear code of eight words from part (i).

□

Problem 35. *(i) Let $p \in (0,1)$. Prove that $\binom{n}{pn} \sim 2^{n(H(p)+o(1))}$ for $n \to \infty$, where $H(p)$ is the entropy function.*

(ii) Let $p \in (0,1/2)$. Prove that

$$\sum_{i \le pn} \binom{n}{i} \le (1+pn)\binom{n}{pn} \sim 2^{n(H(p)+o(1))}, \qquad n \to \infty,$$

where $H(p)$ is the entropy function.

(iii) Assuming Shannon's theorem on the existence of optimal codes for binary symmetric channels, what can be said on the quality of the Varshamov-Gilbert bound?

Proof. (by Frank Fiedler)

(i) Consider $\binom{n}{pn}$ for $p \in (0,1)$. By Stirling's formula (cf. [Cam94]),

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \left(1 + O\left(\frac{1}{n}\right)\right)$$

We assume that this also holds for the extension of $n!$ to reals, and let $q = 1-p$. Then

$$\begin{aligned}\binom{n}{pn} &\sim \frac{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n \left(1 + O\left(\frac{1}{n}\right)\right)}{\sqrt{2\pi pn}\left(\frac{pn}{e}\right)^{pn} \left(1 + O\left(\frac{1}{pn}\right)\right) \sqrt{2\pi qn}\left(\frac{qn}{e}\right)^{qn} \left(1 + O\left(\frac{1}{qn}\right)\right)} \\ &= p^{-pn} q^{-qn} \frac{1 + O\left(\frac{1}{n}\right)}{\sqrt{2\pi npq}\left(1 + O\left(\frac{1}{pn}\right)\right)\left(1 + O\left(\frac{1}{qn}\right)\right)}\end{aligned}$$

which, recalling that $H(p) = -p\log_2 p - q\log_2 q$, translates to

$$= 2^{nH(p)} \frac{1 + O\left(\frac{1}{n}\right)}{\sqrt{2\pi npq}\left(1 + O\left(\frac{1}{pn}\right)\right)\left(1 + O\left(\frac{1}{qn}\right)\right)}$$

It remains to show that

$$\left(\frac{1 + O\left(\frac{1}{n}\right)}{\sqrt{2\pi npq}\left(1 + O\left(\frac{1}{pn}\right)\right)\left(1 + O\left(\frac{1}{qn}\right)\right)} \right) \sim 2^{n \cdot o(1)}$$

i.e.,

$$\frac{1}{n} \log_2 \left(\frac{1 + O\left(\frac{1}{n}\right)}{\sqrt{2\pi npq}\left(1 + O\left(\frac{1}{pn}\right)\right)\left(1 + O\left(\frac{1}{qn}\right)\right)} \right) \to 0$$

as $n \to \infty$. The argument of the $\log_2$ is of order $1+O(n)$. Using L'Hopital's rule this gives

$$\frac{1}{n} \log_2 \left(1 + O(n)\right) \sim o(1)$$

which completes the proof.

(ii) Since $p \in (0, 1/2)$, we have

$$\binom{n}{i} \leq \binom{n}{np}$$

for $0 \leq i \leq np$. Since $|\{i \mid 0 \leq i \leq np\}| \leq (1 + np)$, we get

$$\sum_{i \leq np} \binom{n}{i} \leq (1 + np) \binom{n}{np}$$

Now, $1 + np \sim 1 + O(n) = 2^{n \cdot o(1)}$ as before. Hence

$$\begin{aligned} (1 + np) \binom{n}{np} &\sim 2^{n \cdot o(1)} 2^{n(H(p) + o(1))} \\ &= 2^{n(H(p) + o(1))} \end{aligned}$$

(iii) Given a length n of code words over a binary alphabet and minimal distance d, Varshamov-Gilbert states that there exists a code C with the given parameters of minimal distance at least d such that

$$|C| \geq \frac{2^n}{\sum_{i=0}^{d-1} \binom{n}{i}}$$

The rate of transmission for such a code is $\frac{\log_2 |C|}{n}$ (required bandwidth over used band width in terms of "letters" per symbols sent). Let R denote this rate of transmission. Hence

$$\begin{aligned} R &\geq \frac{1}{n} \log_2 \left(\frac{2^n}{\sum_{i=0}^{d-1} \binom{n}{i}} \right) \\ &= 1 - \frac{1}{n} \log_2 \left(\sum_{i=0}^{d-1} \binom{n}{i} \right) \end{aligned}$$

Given $\varepsilon > 0$, if $R < 1 - H(p)$ then there is a code with rate at least R such that the nearest neighbor decoding method results in an error (per code word) of less than ε; if $R > 1 - H(p)$, then there is a lower bound on the error (Shannon's Theorem).

If we had $d - 1 \leq pn$ then $\sum_{i=0}^{d-1} \binom{n}{i} \leq \sum_{i \leq np} \binom{n}{i}$ and we would get $R \sim 1 - H(p)$ for large n. Hence if we choose $p \in (0, \frac{1}{2})$ such that $d - 1 \leq pn$ we have

$$-\frac{1}{n} \log_2 \left(\sum_{i=0}^{d-1} \binom{n}{i} \right) \sim H(p)$$

Thus, asymptotically there is a probability p of an error in a symbol such that the Varshamov-Gilbert bound gives the size of the code with optimal rate of transmission for an arbitrarily small decoding error ε.

□

Problem 36. *The* support *of any word in a code is the set of coordinate positions where its entries are non-zero. Let C be a binary perfect e-error-correcting code of length n. Then the supports of the codewords of smallest weight $2e + 1$ in C are the blocks of an $(e+1)$-$(n, 2e+1, 1)$ designs (with no blocks repeated). This links some interesting designs to some interesting codes. Do you know which ones?*

Proof. (by Frank Fiedler) First note that the problem as stated is not entirely correct. Consider $C = \{(1,0,0), (0,1,1)\}$. C is a perfect 1-error correcting binary code. It does not have any code words with support of size 3, hence it does not yield a design with the parameters desired. The problem is that $\vec{0} = (0,0,0) \notin C$. We can fix this by assuming $\vec{0} \in C$ (which anyway is true for linear codes) or equivalently considering supports with respect to some "origin" $v \in C$, *i.e.*, the support of $w \in \mathbb{F}_2$ are the non-zero coordinates of $w \oplus v$.

Let C be a binary perfect e-error correcting code of length n over $\mathbb{F}_2$. W.l.o.g., we may assume $\vec{0} \in C$.

Since $\vec{0} \in C$, the smallest weight is at least $2e+1$. Since C is perfect (*i.e.*, packing), this smallest weight is actually attained. Let $S \subset [n]$ be a set of $e+1$ coordinates. Let $w_S \in \mathbb{F}_2$ be the (unique) word with support S. C is perfect, hence there is a unique code word $c \in C$ (the center of the ball w_S belongs to) such that $\mathrm{d}(w_S, c) \leq e$. w_S has $e+1$ non-zero coordinates and the coordinates of c differ in at most e positions. Thus $1 \leq \mathrm{w}(c) \leq 2e+1$. c cannot be $\vec{0}$. Hence $\mathrm{w}(c) \geq 2e+1$, which implies $\mathrm{w}(c) = 2e+1$. Therefore, for every word w of weight $e+1$ (*i.e.*, whose support is of size $e+1$), there is a unique code word $c \in C$ that is non-zero on this support (and thus agrees with w on these coordinates).

Let $\mathcal{P} = [n]$, $\mathcal{B} = \{S \mid S \text{ is support of some } c \in C \text{ of weight } 2e+1\}$. There are n points (coordinates). Every block consists of $2e+1$ points. By above considerations, every set of distinct $e+1$ points is contained in a unique block. Hence $(\mathcal{P}, \mathcal{B})$ forms a $(e+1)$-$(n, b, 2e+1, r, 1)$ design.

By Tietäväinen (see [Cam94] p. 287), the only such codes with $e > 1$ are binary repetition codes with $n = 2e+1$ and a binary Golay code with $n = 23$, $e = 3$. Linear 1-error correcting codes are the Hadamard codes. All codes mentioned before are linear. Non-linear 1-error correcting codes may exist (they are actually the ones that do not have to include $\vec{0}$).

For the repetition codes we obtain trivial designs. The binary Golay code yields a 4-$(23, 253, 7, 77, 1)$ design, the Witt design W_{23}. It can be extended to a 5-$(24, 759, 8, 253, 1)$ design W_{24} by including a parity-check as a new coordinate [Cam94]. These designs are famous since their automorphism groups are the Mathieu groups M_{23} and M_{24}, respectively. These groups are the only non-trivial (meaning, not A_n or S_n) t-transitive groups with $t > 3$ (4-transitive and 5-transitive, respectively). □

Problem 37.

(i) Prove the nonexistence of a perfect binary 2-error-correcting code of order of length 90.

(ii) Let p be a prime. A linear code C is called self-dual if $C = C^{\perp}$. Is there a 4-dimensional self-dual code of length 8 over $\mathbb{F}_p$?

Proof. (by Felix Lazebnik)

(i) We follow the solution of this problem presented in [Cam94], p.288. Using the previous problem, the existence of such a code would imply the existence of a $3-(90, 5, 1)$ with no repeated blocks, or the existence of a $2-(88, 3, 1)$ design, see (16.1.2) in [Cam94]. Then by (16.1.3) in [Cam94], the number of blocks containing given two points is $\binom{88}{1}/\binom{3}{1} = 88/3$, a contradiction. □

Proof. (by Felix Lazebnik)

(ii) The answer is Yes. Let p be a prime. By Lagrange Theorem, $p-1$ can be written as a sum of four squares of integers. Let $p-1 = a^2+b^2+c^2+d^2$, where each $a, b, c, d \in \{0, \ldots, p-1\}$. If we consider a, b, c, d as elements $\mathbb{F}_p$, this gives $a^2+b^2+c^2+d^2 = -1$. Consider the following matrix G over $\mathbb{F}_p$:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & a & -b & -c & -d \\ 0 & 1 & 0 & 0 & b & a & -d & c \\ 0 & 0 & 1 & 0 & c & d & a & -b \\ 0 & 0 & 0 & 1 & d & -c & b & a \end{pmatrix}$$

The rows of the minor defined by the four last columns of G come from the product of the quaternions (do you see an Hadamard matrix behind it?). Each row of G is isotropic, and every pair of rows is orthogonal. The rank of G is 4. Therefore G is a generating matrix of a 4-dimensional self-dual code in $\mathbb{F}_p^8$.

□

Problem 38. *Prove that the dual of a Hamming code of length* $(q^d-1)/(q-1)$ *has minimum weight* q^{d-1} *and attains the Plotkin bound.*

Proof. (by Felix Lazebnik) Let $n = (q^d-1)/(q-1)$. We defined the Hamming code C as a linear code over $\mathbb{F}_q$ with the check matrix H, where H is a $d \times n$ matrix whose columns consist of non-zero representatives of each of the 1-dimensional subspaces of $\mathbb{F}_q^d$. Being a check matrix of C, H is the generator matrix of $C^\perp$. Since H has rank d, $|C^\perp| = q^d$. Consider a linear combination of rows of H which contains the greatest number of zero coordinates. Let I be the set of columns of H where these zero coordinates appear. Consider the corresponding $d \times |I|$ minor H' of H. Its row rank is at most $d-1$. Therefore the greatest number of linearly independent columns of H' is $d-1$. The space S that these columns span contains at most $(q^{d-1}-1)/(q-1)$ 1-dimensional subspaces. This set of all 1-dimensional subspaces of S contains all 1-dimensional subspaces defined by columns of H'. Therefore $|I| \le (q^{d-1}-1)/(q-1)$. Hence the minimum weight of $C^\perp$ is at least $(q^d-1)/(q-1) - (q^{d-1}-1)/(q-1) = q^{d-1}$.

For the Plotkin bound: $\theta = 1-1/q$, minimum distance $t \ge q^{d-1}$, $n = (q^d-1)/(q-1)$. The upper bound $\frac{t}{t-\theta n}$ on $|C^\perp|$ decreases with t. Therefore we have

$$\frac{t}{t-\theta n} \le \frac{q^{d-1}}{q^{d-1} - (1-\frac{1}{q})\frac{q^d-1}{q-1}} = q^d = |C^\perp|.$$

This implies $t = q^{d-1}$ and that the code is extremal. □

Problem 39. *Let H be an Hadamard matrix of order n. Normalize the first column to -1 and then delete it; then change -1 to 0 throughout. Show that the code C whose words are the resulting rows attains the Plotkin bound. When this code is linear?*

Proof. (by Vasyl Dmytrenko) Let H be an Hadamard matrix of order n. Then the length of the code C is $l = n - 1$. Since any two rows of H are differ in half of the positions, and one common position for all rows is deleted, any two codewords are differ exactly in $d = n/2$ positions, and obviously d is the minimal distance of the code C.

Now our code is binary, therefore, $\theta = 1 - \frac{1}{q} = \frac{1}{2}$. $d = \frac{n}{2} = \frac{n-1}{2} = \theta l$, therefore, the Plotkin bound holds for the code C:

$$|C| = n = \frac{\frac{n}{2}}{\frac{n}{2} - \frac{n-1}{2}} = \frac{d}{d - \theta l},$$

and the code attains the bound.

Suppose that the code C is linear. Denote the matrix, whose rows are codewords of C, also by C. Let C_i be the i-th row of the matrix C, and let $\{c_1, \ldots, c_m\}$ be a basis of the vector space $V = \{c_1, \ldots, c_n\}$. Since a binary vector space of dimension m consists of 2^m vectors, we conclude that $n = 2^m$. It is shown in [HO] that the binary code C is linear if and only if the Hadamard matrix is of Sylvester type (we thank Dr. Qing Xiang for this reference). Here we prove the sufficiency of this result only.

Let $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Consider the Hadamard matrix $H_{2^m} = H^{\otimes m} := H_2 \otimes \cdots \otimes H_2$ (m times). Let B_n, $n = 2^m$, be the corresponding 0-1-matrix, and let $C_n = J_n - B_n$, where J_n is the $n \times n$ matrix, whose entries are 1's. Show by induction on m that the rows of C_n form a binary vector space of dimension m (compare with [VL]).

For $m = 1$ the statement is evident. Let $\{c_1, \ldots, c_m\}$ be a basis of the row-space of C_n. Then $B_{2n} = \begin{pmatrix} B_n & B_n \\ B_n & J_n - B_n \end{pmatrix}$, and

$$C_{2n} = J_{2n} - B_{2n} = \begin{pmatrix} J_n - B_n & J_n - B_n \\ J_n - B_n & B_n \end{pmatrix} = \begin{pmatrix} C_n & C_n \\ C_n & J_n - C_n \end{pmatrix}.$$

It follows that the row-space of C_{2n} is spanned by $t_i := (c_1, c_i)$, $i = 1, \ldots, m$, and $t_{m+1} := (0, \ldots, 0, 1, \ldots, 1)$ (n 0's and n 1's). Since $|C_{2n}| = 2^{m+1}$, $\{t_1, \ldots, t_{m+1}\}$ is a basis of the row-space of C_{2n}.

It remains to note that the first column of B_n consists of 1's for any n, i.e. the first coordinates of the row-vectors of the C_n are zeros, and we can omit (delete) the first coordinate.

Thus, for every $n = 2^m$ a code C_n obtained by our procedure from a Hadamard matrix H_n is linear. We want to remark that if the rule of making -1's in the first column is not specified, we may not be getting a linear code. For example,

if $H = \begin{pmatrix} -1 & 1 & 1 & 1 \\ -1 & -1 & 1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix}$, then $C = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ is not linear.

In all such cases the rank of the obtained matrix is $m+1$ and one can complete the obtained matrix to a matrix of a linear binary code of size $n = 2^{m+1}$. □

Problem 40. *Let C be a binary code with the generator matrix*

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Decode the following received words by using the syndrome decoding method:

(i) (1,1,0,1,0,1,1)

(ii) (0,1,1,0,1,1,1)

(iii) (0,1,1,1,0,0,0)

Proof. (by David Kravitz) First we need a check matrix H. Here is my H:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Multiplying GH^T gives

$$GH^T = \begin{pmatrix} 2 & 0 & 2 \\ 2 & 0 & 2 \\ 2 & 2 & 0 \\ 2 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

It is trivial to show that the 4 rows of G and the 3 rows of H are linearly independent in F_2^7. Therefore, H is a sufficient check matrix. One more thing to point out, given a vector $v \in F_2^4$, say $v = (a, b, c, d)$, we get $vG = (a, b, c, d, a+b, c+d, a+b+c+d)$. Thus, if we have a vertex $vG = (a, b, c, d, a+b, c+d, a+b+c+d)$, we know that $v = (a, b, c, d)$.

(i) $w_1 = (1, 1, 0, 1, 0, 1, 1) \Rightarrow w_1 H^T = (2, 2, 2) = (0, 0, 0)$.
The minimal weight vector u_1 such that $u_1 H^T = (0, 0, 0)$ is of course $\overline{0}$.
Therefore, we get $v_1 G = c_1 = w_1 - \overline{0} = w_1 = (1, 1, 0, 1, 0, 1, 1)$.
As pointed out above, this vector is equal to $v_1 G$, where $v_1 = (1, 1, 0, 1)$.

(ii) $w_2 = (0,1,1,0,1,1,1) \Rightarrow w_2 H^T = (3,2,2) = (1,0,0)$.
The minimal weight vector u_2 such that $u_2 H^T = (1,0,0)$ is e_7.
(No vectors weight 0 work, this one works with weight 1.)
$\therefore v_2 G = c_2 = w_2 - e_7 = (0,1,1,0,1,1,0) \Rightarrow v_2 = (0,1,1,0)$.

(iii) $w_3 = (0,1,1,1,0,0,0) \Rightarrow w_3 H^T = (0,2,1) = (0,0,1)$.
The minimal weight vector u_3 such that $u_3 H^T = (0,0,1)$ is equal to e_2.
$\therefore v_3 G = c_3 = w_3 - e_2 = (0,0,1,1,0,0,0) \Rightarrow v_3 = (0,0,1,1)$.

□

Problem 41. *Let C be a linear code of length n and dimension k over F_q. Prove that if the generator matrix of C has no column of all zeros, then the sum of the weights of all codewords of C is $n(q-1)q^{k-1}$.*

Proof. (by Jason Williford)

Let G be the generator matrix of C, $W(C)$ denote the sum of the weights of all vectors in C, and $v(i)$ denote the ith entry of a vector $v \in C$. Let $A_i = \{v \in C : v(i) \neq 0\}$. Then $\sum_{i \in [n]} |A_i| = W(C)$.

Fix i. As G has no column of all zeros, $\exists u \in G$ such that $u(i) \neq 0$. Using row reduction with $u(i)$ as our pivot, we obtain a new generator matrix G', where $u(i)$ is the only element in the ith column which is not zero. The vectors in $G' \backslash \{u\}$ form a $k-1$ dimensional subspace D. All vectors $v \in C$ can be written as $v = \lambda u + w$ for some $\lambda \in F_q, w \in D$. As $w(i) = 0 \ \forall w \in D$, then if $\lambda \neq 0$ then $v(i) \neq 0$. With $|D| = q^{k-1}$ choices for w and $q-1$ choices for nonzero λ, $|A(i)| = (q-1)q^{k-1} \ \forall i \in [n]$.

Thus $\sum_{i \in [n]} |A_i| = n(q-1)q^{k-1} = W(C)$. □

Problem 42. *Let R_d be the rate of the Hamming code over $\mathbb{F} - q$ whose check matrix has d rows. Find $\lim_{d \to \infty} R_d$.*

Proof. (by Jason Williford) Let H be the check matrix of a Hamming code C, and H have d rows. Then the length of the code C must be $(q^d - 1)/(q-1)$, and a generator matrix of C must have $(q^d - 1)/(q-1) - d$ rows. Therefore $R_d = Log_q(q^{(q^d-1)/(q-1)-d})/((q^d-1)/(q-1)) = 1 - d(q-1)/(q^d-1)$ and $\lim_{d \to \infty} R_d = 1 - \lim_{d \to \infty} d(q-1)/(q^d-1)$

As both $\lim_{d \to \infty} d(q-1) \to \infty$ and $\lim_{d \to \infty}(q^d - 1) \to \infty$ we may employ L'Hospital's rule to get $(q-1)(Ln(q))^{-1} \lim_{d \to \infty} 1/(q^d) \to 0$, therefore $\lim_{d \to \infty} R_d = 1$. □

Problem 43. *Consider the linear code C over $\mathbb{F}_3$ of length 12 and dimension 6 with a generator matrix $(I\ A)$, where A is as follows:*

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix}$$

(i) Prove that C is self-dual.

(ii) Prove that the minimum distance of C is 6.

Proof. (by Sven Reichard and Felix Lazebnik)

(i) We have to show that any two not necessarily distinct rows of $(I\ A)$ are orthogonal. This implies $C \leq C^\perp$, and a dimension argument shows $C = C^\perp$.

Each row of $(I\ A)$ has 6 non-zero entries. Since $x^2 = 1$ for $x \in \mathbb{F}_3^*$, and $6 \equiv 0 \mod 3$, this implies that each row of $(I\ A)$ is isotropic.

It remains to show that any two distinct rows are orthogonal. Let B be the matrix obtained by deleting the first row and the first column of A,

$$B = \begin{pmatrix} 0 & 1 & 2 & 2 & 1 \\ 1 & 0 & 1 & 2 & 2 \\ 2 & 1 & 0 & 1 & 2 \\ 2 & 2 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 0 \end{pmatrix}$$

and let its rows be denoted as $r_i, i \in [1, 5]$. Note that B is circulant, so it suffices to consider pairs containing the first row. For $2 \leq i \leq 5$, r_1 and r_i have zeros in the first and i-th column, and they agree in exactly one column. Hence their inner product is $0 + 0 + 1 + 2 + 2 = -1$. Since the corresponding rows in A coincide in one additional column (the first column of A), they are orthogonal.

Finally, since each row of B has the entry sum of 0, they are orthogonal to the all-one vector; hence the first row of $(I\ A)$ is orthogonal to all other rows.

(ii) The minimal distance in a linear code is equal to its minimum weight. Therefore now we investigate the weights of all codewords of C. The key is the fact that since every row of $(I\ A)$ is isotropic, its weight is divisible by 3.

The weight of any row of $(I\ A)$ is 6.

The weight of any linear combination of any two rows of $(I\ A)$ with nonzero coefficients is at least 4, since they contain two column disjoint 2×2 minors

with zeros on one diagonal and nonzeros on another. Being divisible by 3, it must be at least 6.

The weight of a linear combination with nonzero coefficients of any three rows of $(I\ A)$ is at least 4. Due to the I part in $(I\ A)$, it is equivalent to the statement that the weight of a linear combination of arbitrary three rows of A is at least 1. Let $1 \le i < j < k \le 6$ be the indices of the rows. If $i = 1$, then the 3×6 matrix formed by the rows contains a minor of the form

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & a \\ 1 & a & 0 \end{pmatrix},$$

where $a \neq 0$. It is nonsingular, and therefore only the trivial linear combination of its rows has weight zero.

If $i > 1$, then the 3×6 matrix formed by the rows contains a minor of the form

$$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & a & 1 \end{pmatrix}.$$

This matrix is nonsingular, and therefore only the trivial linear combination of its rows has weight zero.

The weight of any linear combination of any four or more rows of $(I\ A)$ is at least 4, due to the I part in $(I\ A)$. Being divisible by 3, it must be at least 6.

□

Remark. By a similar but more involved argument one can show that the binary (24,12) Golay code has minimum distance 8 (see Vera Pless, Introduction to the Theory of Error-Correcting Codes, John Willey & Sons, Inc, 1982, p. 28-29). As was pointed to us by Qing Xiang, the ternary code considered above is a member of an infinite family of so-called *symmetry codes* $C(p)$, where $p = 2 \pmod 3$. These are $(2p+2, p+1)$ ternary codes with generator matrix $(I\ S_p)$, where S_p is $(p+1) \times (p+1)$ obtained from the $p \times p$ Jacobsthal matrix $Q = (\chi(j-i))$, $i, j \in \mathbb{F}_p$, χ is the Legendre symbol, in the following way: attach to Q from the top and from the left a row and a column of p 1's, and put 0 as the $(1,1)$ entry (see Vera Pless' book, p. 131-134). By the time the book was published, minimum distance of $C(p)$ was not known for $p > 29$, nor the behavior of its ratio to $2p+2$ as p gets large.

Here's a computer assisted proof of (ii) that the minimal distance of the code is 6.

First we construct the generator matrix G:

```
gap> A := [[0,1,1,1,1,1],[1,0,1,2,2,1],[1,1,0,1,2,2],
> [1,2,1,0,1,2], [1,2,2,1,0,1],[1,1,2,2,1,0]];;
```

```
gap> I := IdentityMat(6); [ [ 1, 0, 0, 0, 0, 0 ], [ 0, 1, 0, 0, 0,
0 ],
  [ 0, 0, 1, 0, 0, 0 ], [ 0, 0, 0, 1, 0, 0 ],
  [ 0, 0, 0, 0, 1, 0 ], [ 0, 0, 0, 0, 0, 1 ] ]
gap> G := List([1..6], x -> Concatenation(I[x], A[x])); [ [ 1, 0,
0, 0, 0, 0, 0, 1, 1, 1, 1, 1 ],
  [ 0, 1, 0, 0, 0, 0, 1, 0, 1, 2, 2, 1 ],
  [ 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 2, 2 ],
  [ 0, 0, 0, 1, 0, 0, 1, 2, 1, 0, 1, 2 ],
  [ 0, 0, 0, 0, 1, 0, 1, 2, 2, 1, 0, 1 ],
  [ 0, 0, 0, 0, 0, 1, 1, 1, 2, 2, 1, 0 ] ]
```

Now we want this as a matrix over $F = \mathbb{F}_3$, so we multiply it by $1 \in F$.

```
gap> F := GF(3); GF(3) gap> G := G*One(F); [ [ Z(3)^0, 0*Z(3),
0*Z(3), 0*Z(3), 0*Z(3), 0*Z(3),
    0*Z(3), Z(3)^0, Z(3)^0, Z(3)^0, Z(3)^0, Z(3)^0 ],
  [ 0*Z(3), Z(3)^0, 0*Z(3), 0*Z(3), 0*Z(3), 0*Z(3),
    Z(3)^0, 0*Z(3), Z(3)^0, Z(3), Z(3), Z(3)^0 ],
  [ 0*Z(3), 0*Z(3), Z(3)^0, 0*Z(3), 0*Z(3), 0*Z(3),
    Z(3)^0, Z(3)^0, 0*Z(3),  Z(3)^0, Z(3), Z(3) ],
  [ 0*Z(3), 0*Z(3), 0*Z(3), Z(3)^0, 0*Z(3), 0*Z(3),
    Z(3)^0, Z(3), Z(3)^0,  0*Z(3), Z(3)^0, Z(3) ],
  [ 0*Z(3), 0*Z(3), 0*Z(3), 0*Z(3), Z(3)^0, 0*Z(3),
    Z(3)^0, Z(3), Z(3), Z(3)^0, 0*Z(3), Z(3)^0 ],
  [ 0*Z(3), 0*Z(3), 0*Z(3), 0*Z(3), 0*Z(3), Z(3)^0,
    Z(3)^0, Z(3)^0, Z(3), Z(3), Z(3)^0, 0*Z(3) ] ]
```

(`Z(3)` is GAP's notation for a primitive element of $\mathbb{F}_3$.) C is the vector space over F generated by the rows of G.

```
gap> C := VectorSpace(F, G); <vector space over GF(3), with 6
generators>
```

Next we define the weight as the number of nonzero entries,

```
gap> weight := function(v)
> return Length(Filtered(v, x -> x <> 0*x));
> end;
function( v ) ... end gap> weight(G[1]); 6
```

and calculate the list of weights of all elements.

```
gap> weights := List(Elements(C), weight);;
```

The minimum of this list is of course 0,

```
gap> Minimum(weights); 0
```

but if we look at the list as a multiset,

```
gap> Collected(weights); [ [ 0, 1 ], [ 6, 264 ], [ 9, 440 ], [ 12,
24 ] ]
```

we see that the minimal nonzero weight is 6.

This problem was not assigned during math 689

Problem 44. *The $n_1 \times n_2$ matrices over $GF(2)$ clearly form a vector space V of dimension $n_1 n_2$ over it. Let C_i be an $[n_i, k_i, d_i]$ binary code, $i = 1, 2$. Let C be a subset of V consisting of those matrices for which every row, respectively column, is a codeword in C_1, respectively C_2. Show that C is an $[n_1 n_2, k_1 k_2, d_1 d_2]$. This code is called direct product of C_1 and C_2.*

Proof. (by Carl Devore) Suppose the codewords are thought of as row vectors. In any linear $[n, k]$-code, we can fix a set of k of the digit positions to contain arbitrarily chosen digits; the remaining $n - k$ digits will then be determined. These k positions can be chosen to correspond to any k linearly independent columns of the generator matrix. We call these k positions the **information positions** (this is my modification of what is called "*information digits*" in *Information Theory*, Robert B. Ash, Dover, New York, 1990 (orig., Wiley, New York, 1965), chapter 4, "Error-Correcting Codes", section 4.3 "Parity-check coding."5). It is clear that for any sequence of k symbols, there exists a codeword in which this sequence appears in the information positions. Since k is also the column rank of the generator matrix, the remaining $n - k$ positions are completely determined by this choice.

Now we pass to the actual proof.

If C is indeed a linear code, that its length is $n_1 n_2$ is obvious.

Let's count how many ways we can construct an $X \in C$. Fix a set of information positions for C_1. By choosing k_1 elements of C_2 (repetition allowed) to fill the columns corresponding to these positions, the remaining $n_1 - k_1$ columns of X are determined. How many ways can these k_1 columns be chosen? Since $|C_2| = q^{k_2}$, it can done $q^{k_1 k_2}$ ways, so $|C| = q^{k_1 k_2}$. That C is closed under addition and scalar multiplication follows from C_1 and C_2 being closed under those operations. So C is a subspace of $GF(q)^{n_2 \times n_1}$ with $q^{k_1 k_2}$ elements, and hence $dim(C) = k_1 k_2$.

To determine the weight of C, choose $X \in C$, $X \neq 0$. Each nonzero column has at least d_2 nonzero entries, so there are at most $n_2 - d_2$ rows that are identically zero. In each of the remaining d_2 rows, there are at least d_1 nonzero entries. Therefore X has at least $d_1 d_2$ nonzero entries. As X was an arbitrary nonzero element of C, the weight of C is at least this. To see that this lower bound is achieved, choose $x \in C_1$ of weight d_1 and $y \in C_2$ of weight d_2, both considered as column vectors. Then $yx^t \in C$, and the weight of yx^t is $d_1 d_2$. □

This problem was not assigned during math 689

Problem 45. *Which binary cyclic codes of length 7 are self-orthogonal?*

Proof. (by Carl Devore) The irreducible factors of $x^7+1 \in GF(2)[x]$ are $1+x$, $1+x+x^3$, and $1+x^2+x^3$. As there are 3 factors, there are $2^3 = 8$ possible generators $g(x)$ for cyclic codes. If a code is self-orthogonal, then $1+x$ must divide $g(x)$, so this reduces the number of cases to $8/2 = 4$. In the following table, let $h(x) = (x^7+1)/g(x)$. The second column is the factorization of the reciprocal polynomial of $h(x)$.

$g(x)$	$x^{deg(h)}h(x^{-1})$
$1+x$	$(1+x+x^3)(1+x^2+x^3)$
x^7+1	1
$(1+x)(1+x+x^3)$	$1+x+x^3$
$(1+x)(1+x^2+x^3)$	$1+x^2+x^3$

We see that in the last three cases the reciprocal polynomial of $h(x)$ divides $g(x)$, so for these three, $\langle g(x)\rangle$ is a self-orthogonal code.

The accompanying Maple program will list the generators of all binary cyclic self-orthogonal codes of length n for any odd n. For example, there are $243 = 7^3$ such codes of length $63 = 2^6-1$ and $27 = 3^3$ such codes of length $31 = 2^5-1$. (Perhaps there's a pattern there that the program could help clarify.) □

This problem was not assigned during math 689

Problem 46. *Let C be a binary cyclic code of odd length n. Let*

$$g(x) \in GF(2)[x]/(x^n-1)$$

be the generator polynomial of C. Then we know that $g(x)h(x) = x^n-1$ for some $h(x) \in GF(2)[x]$. Suppose that $e(x)$ is the idempotent generator of $\langle g(x)\rangle$. Show that $1+e(x)$ is the idempotent generator of $\langle h(x)\rangle$.

Proof. (by Carl Devore) First note that $(1+e(x))^2 = 1+e(x)^2 = 1+e(x)$ so that $1+e(x)$ is an idempotent.

Any $a(x) \in \langle h(x)\rangle$ can be expressed as $b(x)h(x)$ for some $b(x)$. Hence

$$(1+e(x))a(x) = a(x)+e(x)a(x) = a(x)+e(x)b(x)h(x).$$

Since $e(x) \in \langle g(x)\rangle$, $e(x) = c(x)g(x)$ for some $c(x)$. Therefore, in $GF(2)[x]/(x^n-1)$,

$$(1+e(x))a(x) = a(x)+c(x)g(x)b(x)h(x) = a(x)+c(x)b(x)(x^n-1) = a(x).$$

So $1+e(x)$ is an identity element in $\langle h(x)\rangle$, and any element of $\langle h(x)\rangle$ can be (trivially) expressed as a multiple of $1+e(x)$. Therefore $\langle h(x)\rangle = \langle 1+e(x)\rangle$. □

Problem 47. *A component of order 2 in a graph is called an isolated edge.*

(i) Find the expected number of isolated edges in $G \in \mathcal{G}(n,p)$.

(ii) Find the expected number of isolated vertices in $G \in \mathcal{G}(n,p)$.

Solution. (by Felix Lazebnik) (i) List all $N = \binom{n}{2}$ 2-element subsets of vertices of G arbitrarily. Let X_i, $1 \leq i \leq N$, be a random variable which takes value 1 if the i-th pair of vertices is an isolated edge in G, and takes value 0 otherwise. Then $X = \sum_{i=1}^{N} X_i$ counts the number of isolated edges in G. Since all $E(X_i)$ are equal, $E(X) = \sum_{i=1}^{N} E(X_i) = NE(X_1)$. Let $\{a,b\}$ be the first pair of vertices. Then $ab \in E(G)$ with probability p and any other vertex of G is adjacent to none of them with probability $(1-p)^2$. Since there are $n-2$ other vertices,

$$E(X) = NE(X_1) = \binom{n}{2} p(1-p)^{2(n-2)}.$$

□

(ii) List all n vertices of G arbitrarily. Let Y_i, $1 \leq i \leq n$, be a random variable which takes value 1 if the i-th vertex is isolated in G, and takes value 0 otherwise. Then $Y = \sum_{i=1}^{n} Y_i$ counts the number of isolated vertices of G. Since all $E(Y_i)$ are equal, $E(Y) = \sum_{i=1}^{n} E(Y_i) = nE(Y_1)$. The first vertex is non-adjacent to any other vertex with probability $1-p$. Therefore it is adjacent to none of them with probability $(1-p)^{n-1}$. Hence

$$E(Y) = nE(Y_1) = n(1-p)^{n-1}.$$

□

Problem 48.

(i) Let $X = X(G)$ be the number of edges of $G \in \mathcal{G}(n,p)$ that are not in a triangle. Find $E(X)$

(ii) For fixed $p \in (0,1)$, do almost all $G \in \mathcal{G}(n,p)$ have every edge as a side of a triangle? (Do not use any powerful theorems we did not prove in class).

We present two essentially identical proofs of (i). The first presentation follows a more standard pattern and is shorter.

Solution. (by Felix Lazebnik) (i) List all $N = \binom{n}{2}$ 2-element subsets of vertices of G arbitrarily. Let X_i, $1 \leq i \leq N$, be a random variable which takes value 1

if the i-th pair of vertices is not in a triangle of G, and takes value 0 otherwise. Then $X = \sum_{i=1}^{N} X_i$ counts the number of edges in G. Since all $E(X_i)$ are equal, $E(X) = \sum_{i=1}^{N} E(X_i) = NE(X_1)$. Let $\{a, b\}$ be the first pair of vertices. Then $ab \in E(G)$ with probability p and any other vertex of G is adjacent to at most one of them with probability $1 - p^2$. Since there are $n - 2$ other vertices,

$$E(X) = NE(X_1) = \binom{n}{2} p(1 - p^2)^{n-2}.$$

□

Solution. (by Carl Devore) (i) Let Y be the number of edges of G that *are* in some triangle. By the linearity of expectation, $E(X) = E(e(G) - Y) = E(e(G)) - E(Y) = \binom{n}{2}p - E(Y)$. Given $\{u, v\} \subset V$, $P(uv \text{ is in a } \triangle) =$

$$P(uv \text{ is in a } \triangle \mid uv \in E)P(uv \in E) + P(uv \text{ is in a } \triangle \mid uv \notin E)P(uv \notin E)$$

$$= P(uv \text{ is in a } \triangle \mid uv \in E)p + 0(1 - p) = P(uv \text{ is in a } \triangle \mid uv \in E)p.$$

$P(uv \text{ is in a } \triangle \mid uv \in E) = P(\exists x \in V - \{u, v\} \text{such that} \{xu, xv\} \subset E) =$ $1 - P(\forall x \in V - \{u, v\}, \{xu, xv\} \nsubseteq E)$. Given $x \in V - \{u, v\}$, $P(\{xu, xv\} \nsubseteq E) = 1 - P(\{xu, xv\} \subset E) = 1 - p^2$. Since the edge choices for distinct x can be made independently, $P(uv \text{ is in a } \triangle) = (1 - (1 - p^2)^{n-2})p$. Note that this probability is for $\{u, v\}$ *any* 2-subset of V, not necessarily an edge. There are $\binom{n}{2}$ independent choices for these 2-subsets, so $E(X) = \binom{n}{2}p - E(Y) = \binom{n}{2}p - \binom{n}{2}(1 - (1 - p^2)^{n-2})p = \binom{n}{2}p(1 - p^2)^{n-2}$.

(ii) By Markov's inequality, $P(X \geq 1) \leq E(X)$. For a fixed p, $E(X)$ is a product of a quadratic polynomial of n and the exponential function of n with base in $(0, 1)$. Hence, $E(X) \to 0$ (very rapidly) as $n \to \infty$. Thus the probability that G has an edge that is not in a triangle goes to 0. Therefore, the probability that all edges are in some triangles goes to 1.

□

Problem 49.

(i) Let $X(G)$ be the number of vertices of $G \in \mathcal{G}(n, p)$ not in a triangle. Find $E(X)$.

(ii) For a fixed $p \in (0, 1)$, do almost all graphs in $\mathcal{G}(n, p)$ have the property that every vertex is in a triangle? (Do not use any powerful theorems we did not prove in class).

Proof. (by Vasyl Dmytrenko) (i) Let $1, 2, , \ldots, n$ be the vertices of G, and let $X_i(G)$ be the random variable defined to be 1 or 0 according to whether the i-th vertex is a vertex of a triangle or not. Then, by the linearity of expectation, $E(X) = E(X_1) + E(X_2) + \cdots + E(X_n)$. Since $E(X_1) = E(X_2) = \cdots = E(X_n)$, $E(X) = nE(X_1)$. There are $\binom{n-1}{2}$ possible triangles with the vertex 1, and for

any three vertices the probability that they do not form a triangle is $1-p^3$. Therefore, $E(X_1) = (1-p^3)^{\binom{n-1}{2}}$, and $E(X) = n(1-p^3)^{\binom{n-1}{2}}$.

(ii) By the Markov's inequality $P[X \geq 1] \leq E(X) = n(1-p^3)^{\binom{n-1}{2}} \to 0$ as $n \to \infty$ for any fixed p, $0 < p < 1$. Therefore, $P[X = 0] \to 1$, i.e. almost all graphs have the property that every vertex is in a triangle. □

Problem 50. *Let $T \in \mathcal{T}(n, 1/2)$– the set of all tournaments of order n. A 2-subset of vertices of T is called* **bad** *if no other player wins over both of its members. Let $X(T)$ be the number of bad 2-subsets.*

(i.) Find the smallest value of n such that $E(X) < 1$. (Therefore we know that for this value of n there exists a tournament without bad 2-subsets.)

(ii.) Show that Paley tournament on 7 vertices has no bad 2-subsets. This shows that the value of n obtained by the method of part (i) is not the best.

Solution. (by David Kravitz)

(i) Suppose we randomly choose a 2-subset of vertices $\{u, v\}$ from a tournament with order n. There are $n-2$ other vertices, let us choose one of them at random, say x. The probability that x beats both u and v is clearly $(\frac{1}{2})^2 = \frac{1}{4}$, so the probability that x *does not* beat both of them is $\frac{3}{4}$.
Now, it is easy to see that the probability that there is no vertex which beats both u and v is equal to $(\frac{3}{4})^{n-2}$, as there are $n-2$ other vertices, so this is the probability that any 2-subset is bad. Since there are $\binom{n}{2}$ possible 2-subsets, we see that $E(X) = \binom{n}{2}(\frac{3}{4})^{n-2}$. Call this f_n.
It is easy to see that $\frac{f_{n+1}}{f_n} = (\frac{3}{4}) \cdot \frac{n+1}{n-1}$, and this is less than 1 for all $n > 7$. Therefore, f_n is decreasing once $n > 7$. Since $f_{20} \approx 1.07$ and $f_{21} \approx .89$, we see that the smallest n such that $E(x) < 1$ is $n = 21$.

(ii) We are going to construct a design as follows: For every $i = 0..6$, let edge i be the set of all elements $x \in F_q$ such that $x - i$ is a square. This is a $2-(7,3,1)$ design with the following "edges", in order from 0 to 6:

$$[1,2,4], [2,3,5], [3,4,6], [4,5,0], [1,5,6], [2,6,0], [1,3,0]$$

Our Paley tournament is easy to construct from this, for example edge $0 = [1,2,4]$ implies that $1 \to 0, 2 \to 0, 4 \to 0$ are directed edges. From this design, it is trivial to see that there are no bad pairs, for if there was a bad pair then there would be two edges with no points in common, a contradiction.

□

Problem 51. *Let H be a graph obtained by deleting an edge from K_4. In class we found a threshold function for the property that almost all graphs contain H as a subgraph. Check the expression in the formula for $E(X^2)$ which represents the contribution of the terms corresponding the intersections of vertex sets of two copies of H in 2 vertices. Use the exposition from E.M. Palmer's book.*

Proof. (David Chandler) We want to check that $\sum E(X_iX_j) = \binom{n}{2,2,2,n-6}(11p^{10} + 25p^9)$ where the sum is over all ordered pairs of four element sets of vertices which intersect in exactly two vertices and $X_i, X_j \in \{0, 1, 6\}$ are the numbers of copies of H in the respective subgraphs. We identify 2 vertices as belonging to the first subgraph but not to the second, two vertices in the intersection, two in only the second subgraph, and $n-6$ vertices in neither, so $\binom{n}{2,2,2,n-6}$ is the number of ways to choose the vertices. There are 11 possible edges in the union of the two subgraphs, one possible shared edge and 5 possible edges lying in each subgraph alone. X_iX_j can be nonzero if we have 9, 10, or 11 edges. With probability p^{11} we have all 11 edges and $X_iX_j = 36$. With probability $(1-p)p^{10}$ we have all the edges except the shared one and $X_iX_j = 1$. With probability $10(1-p)p^{10}$ we have all the edges in one subgraph but 5 edges in the other, giving $X_iX_j = 6$. With probability $25(1-p)^2p^9$ we have one edge other than the shared one missing from each subgraph, and again $X_iX_j = 1$. Thus, in this situation,

$$E(X_iX_j) = 36p^{11} + (1-p)p^{10} + 6 \cdot 10(1-p)p^{10} + 25(1-p)^2p^9 = 11p^{10} + 25p^9$$

verifying the term.

Asymptotically, as $p \to 0$ and $N \to \infty$, our term becomes $(n^6/8)(25p^9)$. □

Problem 52. *Let H be a graph obtained by deleting an edge from K_4. In class we found a threshold function for the property that almost all graphs contain H as a subgraph. Check the expression in the formula for $E(X^2)$ which represents the contribution of the terms corresponding the intersections of vertex sets of two copies of H in 3 vertices. Use the exposition from E.M. Palmer's book.*

Proof. (by Felix Lazebnik) Let I, J be the ith and the jth 4-element subset of $V(G)$, and let for any $A \subset V(G)$, $G[A]$ denote the subgraph of G induced by A. We remind ourselves that for each i the random variable X_i counts the number of subgraphs of G isomorphic to H having I as their vertex set. Then $X_i(G) = 0, 1, 6$, depending on $e(G[I]) \leq 4, = 5, = 6$, respectively.

Suppose $|I \cap J| = 3$. Then these sets can be written as $I = \{a, x, y, z\}$ and $J = \{x, y, z, b\}$, respectively. For $X_i X_j(G) = X_i(G)X_j(G)$ to be positive, both $e(G[I])$ and $e(G[J])$ has to be at least 5. This leads to a partition of all graphs on which $X_i X_j > 0$ into five classes C_t, $0 \leq t \leq 5$, listed below. For each class, $X_i(G)X_j(G)$ is constant for all $G \in C_t$. As usually, Prob(C_t) =Prob$\{G : G \in C_t\}$.

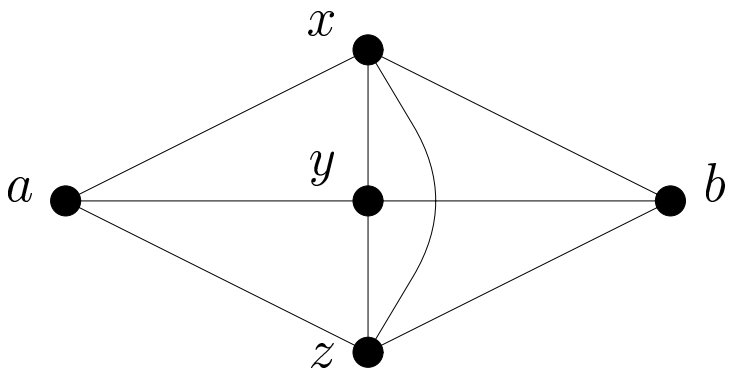

Figure 7: Vertex Labels for isomorphism classes (see next page)

- $C_1 = \{G : G[I \cap J] \cong K_3, G[I] \cong G[J] \cong K_4\}$, $X_i(G)X_j(G)\text{Prob}(C_1) = 6 \cdot 6 \cdot p^9 = 36p^9$
- $C_2 = \{G : G[I \cap J] \cong K_3, G[I] \cong H, G[J] \cong K_4\}$, $X_i(G)X_j(G)\text{Prob}(C_2) = 1 \cdot 6 \cdot (3(1-p)p^2) \cdot p^6 = 18(1-p)p^8$
- $C_3 = \{G : G[I \cap J] \cong K_3, G[I] \cong K_4, G[J] \cong H\}$, $X_i(G)X_j(G)\text{Prob}(C_3) = 6 \cdot 1 \cdot p^6(3(1-p)p^2) = 18(1-p)p^8$
- $C_4 = \{G : G[I \cap J] \cong K_3, G[I] \cong G[J] \cong H\}$, $X_i(G)X_j(G)\text{Prob}(C_4) = 1 \cdot 1 \cdot p^3 \cdot (3(1-p)p^2) \cdot (3(1-p)p^2) = 9(1-p)^2p^7$
- $C_5 = \{G : G[I \cap J] \cong P_3, G[I] \cong G[J] \cong H\}$, $X_i(G)X_j(G)\text{Prob}(C_5) = 1 \cdot 1 \cdot (3 \cdot (1-p)p^8) = 3(1-p)p^8$

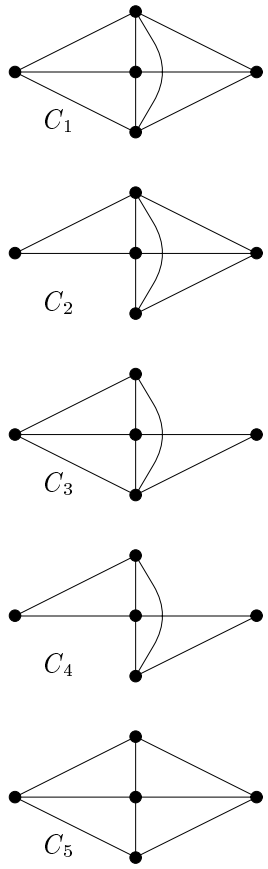

Figure 8: Isomorphism classes

Therefore

$$E(X_iX_j) = \sum_{t=1}^{5} \sum_{G \in C_t} X_i(G)X_j(G)\text{Prob}(G) =$$

$$36p^9 + 18(1-p)p^8 + 18(1-p)p^8 + 9(1-p)^2p^7 + 3(1-p)p^8 =$$

$$6p^9 + 21p^8 + 9p^7.$$

There are $\binom{n}{1,3,1,n-5}$ ways to chose an ordered pair (I, J) of 4-element subsets of $V(G)$ such that $|I \cap J| = 3$. Therefore the contribution of these pair to $E(X^2)$ is

$$\binom{n}{1,3,1,n-5} \left(6p^9 + 21p^8 + 9p^7\right).$$

□

Problem 53. *Find a value of n, as small as you can, for which you know that there is a simple graph of order n with the girth at least 12 and the chromatic number at least 9.*

Proof. (by David Chandler) ¿From Alon & Spencer, *The Probabilistic Method*, "High Girth and High Chromatic Number," handed out in class, we know that, given another condition below, there exists a graph G^* with girth $> l$ and with chromatic number $\chi(G^*) \geq \frac{z^\theta}{6 \ln z}$. $\theta < \frac{1}{l}$ but θ can be arbitrarily close to $\frac{1}{l}$, and l can be arbitrarily close to the next lower girth number. The number of vertices of G^* will be $\lceil z/2 \rceil$, where G^* is derived from an original graph G having z vertices . Using Maple with standard precision, I determined that taking $z = 1.301128 \times 10^{40}$ and $\theta = 1/11$ we get a value greater than 8.000000088, or at least 9 for the chromatic number. Meanwhile, the girth is greater than $l = 11$ so it is at least 12.

This graph will exist, provided that the probabilities of two exceptions sum to less than 1 (where edges are assigned probability $p = z^{\theta-1}$). The first exception is that the original graph G could have more than $z/2$ cycles of length up to 11. In our case $E[X] \leq \sum_{i=3}^{l} \frac{n^{\theta i}}{2i} = .59156859 \times 10^{39}$, where X is the number of cycles which have to be deleted, and this number is much less than $z/2$, meaning by Markov's Theorem that X has low probability of exceeding $z/2$.

The second exception would be for the independence number $\alpha(G)$ to be greater than $x = \lceil (3/p) \ln n \rceil$. In our case,

$$\Pr[\alpha(G) \geq x] < [ne^{-p(x-1)/2}]^x < ne^{-p(x-1)/2} = .873704044 \times 10^{-20}$$

In our case given that almost all graphs of the given vertex size have girth greater than 11 and chromatic number greater than 8, it would seem likely that the vertex size could be much smaller. In fact a member of a known family of graphs with high girth and chromatic number would be a good candidate to find a lower n. □

Problem 54. *Let $G \in \mathcal{G}(n,p)$, where $p \in (0,1)$ is fixed. $0 \leq p \leq 1$. Define a random variable $X(G)$ to be the number of edges of G.*

(a) Find $E(X)$ and $\sigma(X)$.

(b) Use Chebyshev's inequality to show that for any $\epsilon \geq 0$, the number $X(G)$ of edges of almost all graphs satisfy

$$(1-\epsilon)p\binom{n}{2} < X(G) < (1+\epsilon)p\binom{n}{2}$$

Proof. (by David Chandler)

(a) The expected number of edges is the number of possible edges times the probability of each edge actually being there:

$$E(X) = p\binom{n}{2}$$

A calculation is required to compute $\sigma(X)$. Here we avoid it by using the well known fact for binomially distributed random variables (which is similar, but a more general computation. It can be found in most books on Probability).

$$\sigma(X) = (var(X))^{1/2} = (p(1-p)\binom{n}{2})^{1/2}$$

(b) Chebyshev's inequality states that

$$E[(X-\mu)^2] \geq (\epsilon\mu)^2 P(|X-\mu| \geq \epsilon\mu)$$

where μ can be taken to be $E(X) = p\binom{n}{2}$. Substituting the known variance we get

$$p(1-p)\binom{n}{2} \geq (\epsilon\mu)^2 P(|X-\mu| \geq \epsilon\mu)$$

or

$$P(|X-\mu| \geq \epsilon\mu) < \frac{p(1-p)\binom{n}{2}}{p^2\binom{n}{2}^2\epsilon^2}$$

which goes to zero as $n \to \infty$. □

Problem 55. *Go over the proof of the existence of bipartite k-regular expanders from P. Sarnak's book. Present all details of the proof that $\frac{(II)}{(n!)^k} \to 0$ when $n \to \infty$.*

Proof. (by David Kravitz)

$$(II) = \sum_{n/3 \leq t \leq n/2} \sum_{t \leq m \leq 3t/2} \binom{n}{t}\binom{n}{m}\left(\frac{m!(n-t)!}{(m-t)!}\right)^k$$

$(m!)/(m-t)!$ is maximized when m is as large as possible, so we create an upper bound when $m = 3t/2$, and so $(m-t) = t/2$.

$\binom{n}{m}$ is as large as possible when $m = n/2$.

$$(II) \leq \sum_{n/3 \leq t \leq n/2} \sum_{t \leq m \leq 3t/2} \binom{n}{t} \binom{n}{n/2} \left(\frac{(3t/2)!(n-t)!}{(t/2)!} \right)^k$$

Nothing inside the summation now is dependent on m, so we may use the formula $\sum_1^n c = cn$ to find the "inner sum". We sum m from $t/2$ to $3t/2$, and $3t/2 - t/2 + 1 = t + 1$.

$$(II) \leq \sum_{n/3 \leq t \leq n/2} (t+1) \binom{n}{t} \binom{n}{n/2} \left(\frac{(3t/2)!(n-t)!}{(t/2)!} \right)^k$$

$\binom{n}{t}$ is maximized when $t = n/2$, and $t+1$ is certainly bounded above by n since $t \leq \frac{n}{2}$. This eliminates t from the first three terms of the summation, so we may take them "out front".

$$(II) \leq n \binom{n}{n/2} \binom{n}{n/2} \sum_{n/3 \leq t \leq n/2} \left(\frac{(3t/2)!(n-t)!}{(t/2)!} \right)^k \leq n 2^n 2^n \sum_{n/3 \leq t \leq n/2} \left(\frac{(3t/2)!(n-t)!}{(t/2)!} \right)^k$$

$$\Rightarrow (II) \leq 2^{2n} n \sum_{n/3 \leq t \leq n/2} \left(\frac{(3t/2)!(n-t)!}{(t/2)!} \right)^k$$

Now, suppose that $x \in [n/3, n/2]$ maximizes the function of t which stands under the summation sign in the expression above (in Sarnak's book it is denoted by h_t). We then get an upper bound if we put this x value in for t. Because our quantity is now not dependent on t, and $n/2 - n/3 + 1 = n/6 + 1 < n$, this gives us the following:

$$(II)/(n!)^k \leq 2^{2n} n \cdot n \left(\frac{(3x/2)!(n-x)!}{(x/2)!(n)!} \right)^k$$

Here it was claimed that the x value causing the maximum is always at one of the endpoints. To show this, I will use the function $h_{t+2} - h_t$. This way as opposed to $h_{t+1} - h_t$ gives much more pleasant quotients of factorials. After simplifying this difference we get this:

$$\frac{(3t/2)!(n-t-2)!}{(t/2-1)!} \left[(3t/2+1) - (t/2+1)(n-t-1)(n-t) \right]$$

All we need to know is whether or not the function is positive or negative so we look only at the inside, which is

$$(3t/2+1)-(t/2+1)(n-t-1)(n-t)$$

We want to show now that it is always negative when $n/3 < t < n/2$, and in the process we will show that it has its highest value on this interval at $t = n/2$.

- Putting in $t = n/2$ or $t = n/3$ gives a negative value whenever $n > 4$. Thus, if this function were non-negative somewhere on the interval then the derivative must be zero somewhere in the interval.
- Since the function is cubic with negative leading coefficient, the derivative is a "down" parabola, and its vertex is at $t = 2n/3 - 1$ which is not in our interval. Both $t = n/2$ and $t = n/3$ give positive values for the derivative. This shows that the derivative must be positive on the whole interval.
- The fact that the derivative is positive also tells us that the maximum occurs at $t = n/2$. Sarnak said that it occurs on one of the endpoints, but this shows it must occur on the right endpoint.

We only need one case, $t = n/2$. This gives the following:

$$(II)/(n!)^k \leq 2^{2n} n^2 \left(\frac{(3n/4)!(n/2)!}{(n/4)!(n)!} \right)^k$$

I computed this limit by using Maple and it is 0 for any $k \geq 7$. □

Problem 56. *Go over the proof of the existence of bipartite k-regular expanders from P. Sarnak's book. Give all necessary details to justify the statement that there are bipartite k-regular expanders which are simple graphs. You can do it for $k = 5$ and $c = 3/2$ only.*

Proof. (by Carl Devore)

Some comments on Peter Sarnak's proof of the existence of bipartite k-regular expanders from his book Some Applications of Modular Forms (Cambridge Univ. Press, 1990):

(i) Sarnak's construction yields a bipartite k-regular multigraph rather than a simple graph.

(ii) The construction can be modified to yield a simple graph. With the new construction, minor changes can be made to Sarnak's argument — reaching the equivalent conclusion that, for $k \geq 5$, almost all bipartite k-regular simple graphs are expanders.

(i) First note that a 1-regular graph cannot possibly be an expander for any c strictly greater than 1. Sarnak fails to mention this restriction on k.

Second, note that Sarnak's construction yields a multigraph, not a simple graph: Two of the selected permutations could be the same. Even if we insist on using distinct permutations, there is nothing to prevent a particular vertex in I from being mapped to a particular vertex in O by two different permutations.

Given that we have a bipartite multigraph X, we can now verify that the construction guarantees that X is k-regular. Use induction on k, the number of permutations. For $k = 1$, since we are using a permutation (a bijection), it is clear that X is 1-regular. If we have a k-regular bipartite multigraph X, it is clear that if we add one more permutation, we get a $(k+1)$-regular bipartite multigraph.

(ii) If we make some restrictions on the choice of the permutations, we can guarantee that the construction yields a simple graph. The surprising fact which will emerge is that, for n sufficiently large, this will reduce the number of graphs under consideration by a factor which depends on k but not on n. Specifically, whereas there are exactly $(n!)^k$ bipartite k-regular multigraphs, there are approximately $(n!)^k \exp(-\binom{k}{2})$ bipartite k-regular simple graphs for n sufficiently large.

To see this, suppose that we have selected the first permutation, π_1, so that we have a 1-regular graph. There are $n!$ ways to choose π_1. In selecting π_2, we must have $\forall i \in I : \ \pi_2(i) \neq \pi_1(i)$. This corresponds to a derangement of $[n]$, so there are approximately $n!/e$ choices for π_2. In selecting π_3, we must have

$$\forall i \in I : \ \pi_3(i) \neq \pi_2(i) \ \wedge \ \pi_3(i) \neq \pi_1(i).$$

Proceeding in this manner, we see that constructing a k-regular bipartite graph on $2n$ vertices by this technique is equivalent to constructing a $k \times n$ Latin rectangle. It follows from Proposition 6.5.2 in Peter J Cameron's *Combinatorics* (Cambridge, 1994) that this can be done in at least

$$\prod_{i=0}^{k-1} n! \left(\frac{n-i}{n}\right)^n = (n!)^k \prod_{i=1}^{k-1} \left(1 - \frac{i}{n}\right)^n$$

ways. For n sufficiently large, each factor in the latter product is approximately e^{-i} whence that product simplifies to $\exp(-\binom{k}{2})$. Therefore, for n sufficiently large, the number of choices $\pi = (\pi_1, \ldots, \pi_k)$ is at least $(n!)^k \exp(-\binom{k}{2})$.

Now Sarnak's count of the number of bad π's for particular subsets of I and O in 3.1.7 will be an overestimate, but we will see that doesn't matter. When we take the limits as $n \to \infty$ — this time dividing by $(n!)^k \exp(-\binom{k}{2})$ — the limits must still go to 0 because the extra factor does not depend on n.

□

Problem 57. *Show that for every graph H there exists a function $p = p(n)$ such that $\lim_{n\to\infty} p(n) = 0$ but almost every graph $G \in \mathcal{G}(n,p)$ contains an induced copy of H.*

Proof. (by Jason Williford) We have shown in class that for each fixed p, $0 < p < 1$, almost all graphs will have H as an induced subgraph. Let $Q_{n,p}$ be the event that the random graph on n vertices has H as an induced subgraph.

For fixed p, we have $P(Q_{n,p}) \to 1$ as $n \to \infty$. Consider $P(Q_{n,p})$ and $P(Q_{n+1,p})$. Let $T_{n+1,p}$ be the event that the random graph on $n+1$ vertices has an induced subgraph H which does not have some fixed v_j as a vertex, and $R_{n+1,p}$ the event where the random graph has H as an induced subgraph, but all induced subgraphs of G isomorphic to H contain v_j .

Clearly $P(Q_{n+1,p}) = P(R_{n+1,p} \cup T_{n+1,p}) = P(R_{n+1,p}) + P(T_{n+1,p}) - P(R_{n+1,p} \cap T_{n+1,p}) \geq P(T_{n+1,p})$.

Also $P(T_{n+1,p}) = P(Q_{n,p})$ (in the event $T_{n,p}$, the edges of v_j are of no consequence, it is simply the probability that H appears on the other n vertices). Therefore $P(Q_{n+1,p}) \geq P(Q_{n,p})$, making the sequence $P(Q_{n,p})$ nondecreasing if p is fixed.

Now we are ready to construct $p(n)$. Let $p(1) = \frac{1}{2}$. Let m_2 be the least integer greater than one such that $P(Q_{m_2,\frac{1}{4}}) \geq \frac{3}{4}$. Let $p(i) = \frac{1}{2}$ if $i \leq m_2$ and $p(m_2) = \frac{1}{4}$.

We proceed as follows: let m_i be the least integer greater than m_{i-1} such that $P(Q_{m_i,\frac{1}{2^i}}) \geq 1 - \frac{1}{2^i}$. Define $p(j) = \frac{1}{2^i}$ if $m_i \leq j < m_{i+1}$. Then $P(Q_{n,p(n)}) \to 1$ as $n \to \infty$, but $p(n) \to 0$.

(Note: The sequence $P(Q_{n,p(n)})$ is not necessarily nondecreasing, however we can be sure that for $n \geq m_i$, $P(Q_{n,p(n)}) \geq 1 - \frac{1}{2^i}$ and this assures convergence to 1. □

Problem 58. *(i) For every $k \geq 1$ find the threshold function for the property that $\Delta(G) \geq k$.*

(ii) Given a positive integer d, is there a threshold function for the property of containing the d-dimensional binary cube as a subgraph? If so, which? If not, why not?

(iii) Give an example of a graph property which has no threshold function. Justify.

Proof. (by Carl Devore) (i) Let $k \in \mathbb{N}$ be given. We show that if $p = p(n)$. If $pn^{1+1/k} \to 0$, then almost no $G \in \mathcal{G}(n,p)$ have $\Delta(G) \geq k$; if $pn^{1+1/k} \to \infty$, then almost all $G \in \mathcal{G}(n,p)$ have $\Delta(G) \geq k$.

Consider the star $K_{1,k}$. This is a tree of order $k+1$ and size k. For any graph G, $\Delta(G) \geq k$ iff G has $K_{1,k}$ as a subgraph. Any tree is connected and balanced, so $K_{1,k}$ satisfies the hypotheses of Erdős and Rényi's theorem (Theorem 3.1.2 in *Graphical Evolution* by E H Palmer (Wiley, 1985)). The conclusion is now immediate from that theorem.

In particular, if $pn^2 = o(1)$ (corresponding to $k = 1$), then almost all graphs are empty (certainly in accordance with intuition and with the handwritten chart "The Evolution of Random Graphs"), and if $pn^{3/2} \to \infty$, then almost all graphs have a non-isolated edge (also in accordance with the chart).

(ii) Let $d \in \mathbb{N}$ be given. Let $p = p(n)$. Let H be the d-dimensional binary cube. We show that if $pn^{2/d} \to 0$, then almost no $G \in \mathcal{G}(n,p)$ have H as a subgraph; if $pn^{2/d} \to \infty$, then almost all $G \in \mathcal{G}(n,p)$ have H as a subgraph.

H has order 2^d, size $d2^{d-1}$, and is connected and balanced (any regular graph is balanced). The conclusion is now immediate from Erdős and Rényi's theorem.

Once again, we see that in particular if $pn^2 \to 0$, then almost all graphs are empty.

Also of interest is that if $pn \to \infty$, then almost all graphs have a 4-cycle. But Erdős and Rényi's theorem cannot be used to find threshold functions that distinguish particular cycle sizes. That theorem tells us that for any fixed k, if $pn \to \infty$, then almost all graphs have a k-cycle.

(iii) Not every graph property has a threshold function. In particular, no matter what $p(n)$ is, almost no $G \in \mathcal{G}(n,p)$ is 1-regular.

The property of being 1-regular is a rare and subtle property: if edges are added to or removed from the graph, the property will no longer hold; if the size remains constant, but an edge is moved, the property will no longer hold. In fact, for any probability function, almost no graphs are 1-regular. To see this, let's suppose for the sake of argument that n is even so that it is possible to have a 1-regular graph. In order to expect there to be "almost any" 1-regular graphs, the expected number of edges must be $n/2 = \binom{n}{2}p \;\Rightarrow\; p = 1/(n-1)$. Thus $p = o\left(\frac{\log n}{n}\right)$, and by Palmer's 3.1.20 we know that almost all graphs have isolated vertices and hence almost no graphs are 1-regular.

This can also be seen by counting the 1-regular graphs on n labeled vertices ($(n-1)!!$ — the double factorial) and counting the graphs of size $n/2$ on n labeled vertices

$$\binom{\binom{n}{2}}{n/2}.$$

The latter is much larger.

The general principle is that in $\mathcal{G}(n,p)$, we can only use the probability function to control the size of the graphs, not the placement of the individual edges. Graph properties that are not closely related to size are not good candidates for having threshold functions. □

Problem 59. *(Erdős-Moser Theorem (1955)). A set $x_1, x_2, \ldots, x_k$ of positive integers is said to have distinct sums if all sums $\sum_{i \in S} x_i$, $S \subset [k]$, are distinct. Let $f(n)$ denote the maximal k for which there exists a set $\{x_1, x_2, \ldots, x_k\} \subset [n]$ with distinct sums.*

(i) Show that $\{2^i \mid 0 \leq i \leq \log_2 n\}$ is a set with distinct sums. Derive from here that

$$f(n) \geq 1 + \lfloor \log_2 n \rfloor.$$

(ii) Show that $2^{f(n)} < nf(n), n \geq 3$. Derive from here that there exists a constant C such that such that for sufficiently large n,

$$f(n) < \log_2 n + \log_2 \log_2 n + C.$$

We will improve this upper bound on $f(n)$ by using The Second Moment method. Let $\{x_1, x_2, \ldots, x_k\}$ be a fixed set with distinct sums. Let (Ω_k, Pr) be the probability space of all subsets of $[k]$ where for each subset $A \in \Omega_k$, $Pr(A) = 2^{-k}$. Let $X(A) = \sum_{i \in A} x_i$ be a random variable on (Ω_k, Pr).

(iii) Show that $\mu = E[X] = \frac{1}{2}(x_1 + \ldots + x_k)$.

(iv) Show that $\sigma^2 = Var[X] = \frac{1}{4}(x_1^2 + \ldots + x_k^2) \leq \frac{n^2 k}{4}$.

(v) By using Chebychev's inequality, show that for any $\lambda > 1$,

$$Pr(|X - \mu| < \frac{\lambda n \sqrt{k}}{2}) \geq 1 - \frac{1}{\lambda^2}.$$

(vi) Explain that X takes any particular value with probability 0 or 2^{-k} and use it to show that for any $\lambda > 1$,

$$Pr(|X - \mu| < \frac{\lambda n \sqrt{k}}{2}) \leq 2^{-k} \lambda n \sqrt{k}.$$

(vii) Use (v) and (vi) to get $n \geq \frac{2^k}{\sqrt{k}} \frac{1 - \lambda^{-2}}{\lambda}$.

(viii) Show that while $\lambda = \sqrt{3}$ gives an optimal result, any choice of $\lambda > 1$ gives that there exists a constant C such that for sufficiently large n,

$$f(n) < \log_2 n + \frac{1}{2} \log_2 \log_2 n + C.$$

Comments. *R. Guy and J. Convey have shown that $f(2^m) \geq m + 2$ fr $m \geq 23$. P. Erdős asked for a proof or disproof that $f(n) \leq \log_2 n + C$ for some constant C.*

Proof. (by Felix Lazebnik) This presentation is based on the one from N. Alon and J.H. Spencer book "*The Probabilistic Method*", Section 4.6, John Willey & Sons, 1992.

(i) The statement follows from the uniqueness of the representation of a positive integer in the positional system with base 2. The later can be easily proven by induction. For $n = 1$, $1 = 2^0$ and the representation is unique, since any other power of 2 or a sum of at least two powers of 2 will be greater than 1. Suppose the uniqueness is proven for all k, $1 \leq k < n$. Let

$$n = 2^{i_1} + 2^{i_2} + \cdots + 2^{i_s} = 2^{j_1} + 2^{j_2} + \cdots + 2^{j_t} ,$$

where

$$i_1 > i_2 > \cdots > i_s \geq 0 \quad \text{and} \quad j_1 > j_2 > \cdots > j_t \geq 0$$

are sequences of integers. Then the greatest power of 2 which divides n is 2^{i_s} from the first representation and 2^{j_t} from the second. Therefore $i_s = j_t$. Since $n - 2^{i_s} < n$, then its base 2 representation is unique due to the induction hypothesis. So

$$i_1 = j_1, \ \ldots, \ i_{s-1} = j_{s-1} ,$$

and the statement is proven for $k = n$.

(ii) Let $X = \{x_1, x_2, \ldots, x_{f(n)}\} \subseteq [n]$ be a distinct sum set of the greatest cardinality. Then there are $2^{f(n)}$ distinct values for the sums of elements from X (including the empty subset which corresponds to zero sum). Now we notice that the sum of elements of any subset of X is an integer from the set $\{0, 1, \ldots, nf(n)\}$. Thus $2^{f(n)} \leq nf(n) + 1$. It is also clear that a distinct sum set can not contain two equal elements, so the largest sum can not be greater than $n + (n-1) + \cdots + (n - f(n) + 1)$ which is strictly less than $nf(n)$. Thus $2^{f(n)} < nf(n)$ for $n \geq 3$. This implies that $f(n) < \log_2 n + \log_2 f(n)$, and therefore $f(n) < \log_2 n + \log_2 [\log_2 n + \log_2 f(n)] < \log_2 n + \log_2 (2 \log_2 n) = \log_2 n + \log_2 \log_2 n + 1$. In the second inequality we used that $f(n) < n$ for $n \geq 3$.

(iii)

$$\mu = E[X] = \sum_{A \in \Omega_k} X(A)\, Pr(A) = \sum_{A \in \Omega_k} \left(\sum_{i \in A} x_i \right) Pr(A) = \sum_{i=1}^{k} x_i =$$

$$\left(\sum_{A \ni i} Pr(A) \right) = \sum_{i=1}^{k} x_i \cdot \frac{1}{2} = \frac{1}{2}(x_1 + x_2 + \cdots + x_k) .$$

We used the fact that the probability of the event that A contains a fixed element $i \in [k]$ is $2^{k-1} \cdot 2^{-k} = \frac{1}{2}$, since there are exactly 2^{k-1} subsets of $[k]$ containing i.

(iv) $\sigma^2 = E[X^2] - \mu^2$. Therefore we evaluate $E[X^2]$.

$$E[X^2] = \sum_{A \in \Omega} X^2(A)\, Pr(A) = \sum_{A \in \Omega} \left(\sum_{i \in A} x_i \right)^2 Pr(A) = \sum_{i \in [k]} x_i^2 \left(\sum_{\substack{A \ni i \\ A \in \Omega}} Pr(A) \right) +$$

$$\sum_{1\le i\neq j\le k} x_i x_j \left(\sum_{\substack{A\ni i,j \\ A\in\Omega}} Pr(A) \right) = \frac{1}{2} \sum_{i\in[k]} x_i^2 + \frac{1}{4} = \sum_{1\le i\neq j\le k} x_i x_j \,.$$

We used that the probability of the event that A contains a fixed element $i \in [k]$ is $\frac{1}{2}$ and the probability of the event that A contains two fixed distinct elements $i, j \in [k]$ is $2^{k-2} \cdot 2^{-k} = \frac{1}{4}$. Therefore

$$\sigma^2 = E[X^2] - \mu^2 = \frac{1}{4} \sum_{i\in[k]} x_i^2 \le \frac{n^2 k}{4} \,,$$

since $x_i \in [n]$.

(v) From Chebychev's inequality we have

$$Pr\left(|X - \mu| \ge \frac{\lambda n\sqrt{k}}{2} \right) < \frac{Var[X]}{\frac{\lambda^2 n^2 k}{4}} \le \frac{1}{\lambda^2} \,,$$

where the last inequality follows from (iv). This proves the statement.

(vi)

$$Pr(X = a) = Pr\left(\left\{ A \,|\, A \subset [k] \quad \text{and} \quad \sum_{i\in A} x_i = a \right\} \right) .$$

If a is the sum of some elements of $\{x_1, x_2, \ldots, x_k\}$, then it corresponds to a unique subset of $[k]$, since $\{x_1, x_2, \ldots, x_k\}$ is a distinct sum set. Therefore $Pr(X = a) = 2^{-k}$. If a is not the value of the sum of elements of $\{x_1, x_2, \ldots, x_k\}$, then $Pr(X = a) = 0$. The open interval of real numbers

$$I = \left(\mu - \frac{\lambda n\sqrt{k}}{2} \,,\ \mu + \frac{\lambda n\sqrt{k}}{2} \right)$$

contains at most $\lambda n\sqrt{k}$ integers. Therefore

$$Pr\left(|X - \mu| < \frac{\lambda n\sqrt{k}}{2} \right) = Pr\left(\left\{ A \,|\, A \subset [k] \quad \text{and} \quad \sum_{i\in A} x_i \in I \right\} \right) \le 2^{-k}\, \lambda n\sqrt{k} \,.$$

(vii) Obvious.

(viii) The inequality obtained in (vii) holds for every $\lambda > 1$. For $\lambda = \sqrt{3}$, the expression $\frac{1-\lambda^{-2}}{\lambda}$ achieves its greatest value equal $\frac{2\sqrt{3}}{9}$ (simple calculus). Therefore, assuming $\lambda = \sqrt{3}$, we get $2^k < 4n\sqrt{k}$. Therefore

$$k < \log_2 n + \frac{1}{2} \log_2 k + 2 < \log_2 n + \frac{1}{2} \log_2(\log_2 n + \frac{1}{2} \log_2 k + 2) + 2 <$$

$$\log_2 n + \frac{1}{2} \log_2(4 \log_2 n) + 2 = \log_2 n + \frac{1}{2} \log_2 \log_2 n + 4 \,.$$

This implies the statement. □

Problem 60. *Let $X(\pi)$ denote the number of fixed points in a random permutation from S_n. Assume that each permutation has probability $1/(n!)$. Find $E(X)$ and the standard deviation $\sigma(X)$. What does the Chebyshev's inequality say about the probability that a random permutation has at least 11 fixed points?*

Proof. (by Frank Fiedler)

The number of derangements on i points is

$$i! \sum_{j=0}^{i} \frac{(-1)^j}{j!}$$

So with x_i being the number of permutations fixing exactly i points,

$$\begin{aligned} E(X) &= \sum_{i=0}^{n} i \frac{x_i}{n!} \\ &= \left(\sum_{i=0}^{n} \frac{i}{n!} \binom{n}{i} (n-i)! \left(\sum_{j=0}^{n-i} \frac{(-1)^j}{j!} \right) \right) \\ &= \sum_{i=0}^{n} \frac{1}{(i-1)!} \left(\sum_{j=0}^{n-i} \frac{(-1)^j}{j!} \right) \end{aligned}$$

It is fairly easy to show that asymptotically $E(X) \to e^1 e^{-1} = 1$. However, we can count the average number of fixed points exactly:

$$\begin{aligned} E(X) &= \frac{1}{n!} \left| \{(\pi, i) \mid 1 \leq i \leq n \wedge \pi \in S_n\} \right| \\ &= \frac{1}{n!} \left| \{(\pi, i) \mid \pi \in S_n \wedge \pi(i) = i\} \right| \cdot \binom{n}{1} \\ &= \frac{1}{n!} (n-1)!\, n \\ &= 1 \end{aligned}$$

Thus $E(X) = 1$ and we obtain an interesting identity

$$1 = \sum_{i=0}^{n} \frac{1}{(i-1)!} \left(\sum_{j=0}^{n-i} \frac{(-1)^j}{j!} \right)$$

Now consider the variance of X.

$$\begin{aligned}
\mathsf{Var}(X) &= E\left((X-1)^2\right) \\
&= E(X^2) - 2E(X) + 1 \\
&= E(X^2) - 1 \\
&= \left(\sum_{i=0}^{n} i^2 \frac{x_i}{n!}\right) - 1 \\
&= \left(\sum_{i=1}^{n} \frac{i}{(i-1)!} \left(\sum_{j=0}^{n-i} \frac{(-1)^j}{j!}\right)\right) - 1
\end{aligned}$$

Again, we can count this accurately. The average number of ordered pairs of fixed points is

$$\begin{aligned}
E(X^2) &= \frac{1}{n!} \left|\{(\pi, i, j) \mid \pi \in S_n \wedge \pi(i) = i, \pi(j) = j\}\right| \\
&= \frac{1}{n!} \left(\left|\{(\pi, i, i) \mid \pi \in S_n \wedge \pi(i) = i\}\right|\right. \\
&\quad \left. + \left|\{(\pi, i, j) \mid \pi \in S_n \wedge \pi(i) = i \wedge i \neq j\}\right|\right) \\
&= \frac{1}{n!} \left((n-1)!\, n + (n-2)!\, n\, (n-1)\right) \\
&= 2
\end{aligned}$$

Hence $\sigma(X) = \left(E(X^2) - 1\right)^{1/2} = (2-1)^{1/2} = 1$. Using Chebychev's inequality with $t = 10$,

$$\begin{aligned}
P(X \geq 11) &= P\left(|X - 1| \geq 10\right) \\
&\leq \frac{\mathsf{Var}(X)}{10^2} \\
&= \frac{1}{100}
\end{aligned}$$

In other words, most permutations have very few fixed points. □

References

[Bol78] B. Bollobás. *Extremal Graph Theory.* Academic Press, N.Y., 1978, pp. 303–304.

[BF] L.Babai, P.Frankl. *Linear Algebra Methods in Combinatorics.* University of Chicago, 1972.

[Ya] I.M.Yaglom. *Geometric Transformation III.* New Math Library, **24**. The Math. Ass. of America.

[Cam94] P.J. Cameron. *Combinatorics: Topics, Techniques, Algorithms.* Cambridge University Press, 1994.

[HO] N. Hamada and H. Ohmori, On the BIBD-design having the minimum p-rank, *Journal of Combinatorial Theor, Ser. A* **18** (1975), 131-140.

[VL] J. H. Van Lint, Coding, decoding and combinatorics, in "Applications of Combinatorics", R.J. Wilson Ed., 1982, Shiva Publ.Limited, p. 69.