Finite Geometries and Extremal Problems

September 10, 2023

1 Affine plane over a field

Let us be given a field $\mathbb{F}$. The *affine plane* over the field $\mathbb{F}$ simply mimics the real Cartesian coordinate geometry of lines and points. The points are ordered pairs (x, y), where $x, y \in \mathbb{F}$. The lines have the form of $L_{a,b} = \{(x, y) : y = ax + b\}$ and the "vertical lines" $L_c = \{(c, y) : y \in \mathbb{F}\}$. Lines with the same slope (called parallel) have no point in common, and lines with different slopes have exactly one point in common. (We consider the vertical lines to be parallel with each other, with infinite slope.) If $\mathbb{F} = GF(q)$, then there are q^2 points and $q^2 + q$ lines (q of them vertical, q of them horizontal, $q(q-1)$ neither vertical nor horizontal). Equivalence classes of parallel lines contain $q + 1$ lines.

One can associate a meaning to the vague sentence "parallel lines meet at infinity". To every class of parallel lines assign a different new object, called *ideal point*, and declare that all ideal points (and no other points) lie on new line, called the *ideal line*. This may sound like a stretch of imagination, but the following rigorous algebraic construction is behind it.

2 Projective plane over a field

Define an equivalence relation over $(x, y, z) \neq (0, 0, 0)$ ordered triplets of the field $\mathbb{F}$ by $(x, y, z) \sim (x', y', z')$ if there exists a $0 \neq \lambda \in \mathbb{F}$ such that $x = \lambda x'$, $y = \lambda y'$, $z = \lambda z'$. This relation is clearly an equivalence relation, and its classes will be the *points* of the projective plane. Similarly, define an equivalence relation over $[A, B, C] \neq [0, 0, 0]$ ordered triplets of the field $\mathbb{F}$ by $[A, B, C] \sim [A', B', C']$ if there exists a $0 \neq \lambda \in \mathbb{F}$ such that $A = \lambda A'$, $B = \lambda B'$, $C = \lambda C'$. The equivalence classes of this relation will be called the *lines* of the projective plane. We will freely work with representatives of the equivalence classes instead of the equivalence classes, as usually it will be easy to see that changing the representative for another does not change the relation that we discuss. The number triplets representing points and lines are called *homogeneous coordinates* of the points and lines.

Consider a point represented by (x, y, z) and a line represented by $[A, B, C]$. We say that *the point is incident to the line* if $Ax + By + Cz = 0$. This relation is clearly invariant under changing the representatives.

Claim 1
(P1) For any two different lines, there is a unique point incident to both;

(P2) For any two different points, there is a unique line incident to both;
(P3) There are 4 points, such that no 3 of them are incident to the same line;
(P4) There are 4 lines, such that no 3 of them are incident to the same point.

The difference between (P1) and (P2) is only whether the notation is () or []. So it suffices to prove (P1). Consider representatives of two different lines, $[A_1, B_1, C_1]$ and $[A_2, B_2, C_2]$. We look for solutions of the system of homogeneous linear equations

$$\begin{aligned} A_1x + B_1y + C_1z &= 0 \\ A_2x + B_2y + C_2z &= 0. \end{aligned}$$

The assumption of two different lines mean $[A_1, B_1, C_1] \not\sim [A_2, B_2, C_2]$, therefore the coefficient matrix of the system of homogeneous linear equations has rank 2. The dimension of the solution space is number of variables minus rank, which is 1. This means that there must be an x, y, z solution triplet, and all other solution triplets are constant multiples of this. This means exactly one equivalence class of (x, y, z) solutions, in other words, a single point. We leave the proof to (P3) and (P4) to the homework problems.

It is not difficult to see that the affine plane over $\mathbb{F}$ is embedded in the projective plane over $\mathbb{F}$. Indeed, points represented by $(x, y, 1)$ in the projective plane are in 1-1 correspondence with the (x, y) points of the affine plane. We call such points of the projective plane *ordinary points*, while the points represented by $(x, y, 0)$ in the projective plane are called *ideal points*.

The affine line $L_{a,b}$ corresponds to the projective line $[a, -1, b]$, which is incident to the ideal point $(1, a, 0)$. The affine line L_c corresponds to the projective line $[1, 0, -c]$, which is incident to the ideal point $(c, 0, 1)$. The common ideal point of the vertical lines will be $(0, 1, 0)$, the ideal point of the parallel class of lines with slope a will be $(1, a, 0)$. The *ideal line* $[0, 0, 1]$ is not incident to any point $[x, y, 1]$ coming from the affine plane, but is incident to all ideal points. All other lines are *ordinary lines*.

I would like to note here that the ideal line in a projective plane over $\mathbb{F}$ is not essentially different from any other line. The difference is only in coordinatization. Removing any line from the projective plane over $\mathbb{F}$ we get an affine plane over $\mathbb{F}$ that can be coordinatized with ordered pairs of the field elements. Consider any 3×3 regular matrix T over $\mathbb{F}$. Write lines as row matrices with 3 columns and points as column matrices with 3 rows. T defines a permutation of lines and a permutation of points as

$$[A, B, C] \mapsto [A, B, C]T \quad \text{and} \quad (x, y, z)^T \mapsto T^{-1}(x, y, z)^T. \tag{2.1}$$

Clearly incidence between points and lines are inherited to the images. The ideal line can be mapped to any other line in this way. One may simply change the names of points and lines to the names of their pre-images under these permutations.

Some comments are due here about the solution of systems of linear equations over a field $\mathbb{F}$. The usual results connecting the solution to the rank of the coefficient matrix still hold, however, rank of the coefficient matrix over $\mathbb{F}$ can be different from the rank over $\mathbb{R}$, even for a 0-1 matrix. It still true over every field that the row rank is the same as the column rank, and they are equal

to the size of the largest square submatrix with noz-zero determinant. For example,

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

has rank 3 over $\mathbb{R}$, but has rank 2 over $GF(2)$.

Assume now that $\mathbb{F} = GF(q)$. Then the number of (x, y, z) ordered not all zero triplets is $q^3 - 1$. Every equivalence class will have exactly $q - 1$ elements. Hence the number of points (and similarly, the number of lines) is $q^2 + q + 1$.

Let us count now how many points are incident to any given line (or equivalently, how many lines are incident to any given point). Every representation of every line has some non-zero entry. So assume without loss of generality that it is the third entry, and represent the line by $[A, B, 1]$. The points represented by (x, y, z) incident to the line satisfy

$$Ax + By + z = 0.$$

Hence for every $x, y \in GF(q)$ there is a unique z solving this equation. This would give q^2 of the (x, y, z) triplets, but being $(0, 0, 0)$ forbidden, we are left with $q^2 - 1$. These triplets fall into equivalence classes of size $q - 1$, and therefore the number of equivalence classes is $q + 1$.

3 The real projective plane

The (x, y, z) triplets are points in $\mathbb{R}^3$, leaving out the all-zero triplets, they make the points in $\mathbb{R}^3 \setminus \{0\}$. An equivalence class of such triplets, $\{\lambda x, \lambda y, \lambda z) : \lambda \neq 0\}$, make a straight line through the origin, but without the origin. Restrict our interest to the points of unit sphere, which satisfy the equation $x^2 + y^2 + z^2 = 1$. Every straight line through the origin intersects the unit sphere in two antipodal points.

In the *Orthogonality Model* of the real projective plane, we represent *both* points (x, y, z) and lines $[A, B, C]$ by antipodal pairs of points on the unit sphere, which satisfy $x^2 + y^2 + z^2 = 1$ and $A^2 + B^2 + C^2 = 1$. Incidence between point and lione is represented by orthogonality of the vectors from the origin to any of the two points of the sphere representing the point and the line of the projective plane.

In the *Spheric Model* of the real projective plane, points of the real projective plane are still represented by pairs of antipodal points on the unit sphere. A line of the real projective plane represented by a not all zero triplet $[A, B, C]$, is incident to eqivalence classes of (x, y, z) points on the sphere, for which $Ax + By + Cz = 0$. This makes the intersection of the sphere with a plane passing through the origin: the intersection is a main circle. (Antipodal points on the main circle represent the same point of the real projective plane. Changing $[A, B, C]$ to an equivalent triplet does not change this main circle.) The ideal points of the real projective plane are antipodal pairs of points of the main circle $x^2 + y^2 = 1$. The ideal line is this main circle. The affine plane can be identified with one of the two open hemispheres that the main circle $x^2 + y^2 = 1$ cuts the sphere into. Ordinary points can be identified with points in the selected hemisphere. Ordinary lines are

intersections of the selected hemisphere with main circles. The geometry of these ordinary points and ordinary lines is the same as the geometry of points and lines in $\mathbb{R}^2$, if we only speak about incidences.

The main circle $x^2 + y^2 = 1$ of the sphere can be moved by an isometry (some linear transformation of $\mathbb{R}^3$) into any other main circle. Therefore the ideal line has no special role in projective geometry.

In elementary geometry, a conic section of $\mathbb{R}^2$ has equation

$$Ax^2 + By^2 + Cxy + Dx + Ey + F = 0 \tag{3.2}$$

with not all zero coefficients. Some conic sections, e.g., $x^2 + y^2 + 1 = 0$, do not have points, and therefore is considered *degenerate*. A single point, a line and the union of two lines are also considered degenerate conic sections. Such degenerate conic sections may arise in particular, if $A = B = C = 0$. We may get a single point from $x^2 + y^2 = 0$. The point sets of $xy = 0$ or $(x - y)(2x + 3y - 4) = 0$ are the union of two lines. It is well-known from geometry, that non-degenerate conics are ellipses, parabolas, and hyperbolas. We return to them later.

Conic sections of $\mathbb{R}^2$ can be extended to the real projective plane. It goes by homogeneization of their equations. A conic section of $\mathbb{R}^2$ with equation (3.2) can be extended into homogeneous coordinates by the substitutions $x \leftarrow \frac{x}{z}$, $y \leftarrow \frac{y}{z}$ and multiplying the resulting equation by z^2:

$$Ax^2 + By^2 + Cxy + Dxz + Eyz + Fz^2 = 0. \tag{3.3}$$

The new equation may have some solutions with $z = 0$ that were not there before the substitution. This is not a problem, but a feature, as the conic sections in the projective plane may have some additional ideal points. Formula (3.3) holds or do not hold for all elements of an equivalence class of (x, y, z) triplets. *Moving from (3.2) to (3.3) did not add any new ordinary points, i.e.,* $(x, y, 1)$ *solutions, to the conic section.*

The definition of a conic section in the real projective plane is

$$\{(x, y, z) : Ax^2 + By^2 + Cxy + Dxz + Eyz + Fz^2 = 0\}, \tag{3.4}$$

provided that not all coefficients are zero. The conic section is *non-degenerate*, if the polynomial in (3.3) cannot be factored into a product of linear polynomials and the coefficient matrix

$$\begin{pmatrix} A & C/2 & D/2 \\ C/2 & B & E/2 \\ D/2 & E/2 & F \end{pmatrix} \tag{3.5}$$

is regular.

(If (3.3) factors into two linear polynomials, then the point set is just the union of two lines of the real projective plane, so we have one or two lines in $\mathbb{R}^2$. If the conic has at most one ordinary point, then (3.5) is singular.) We can write (3.3) into an equivalent matrix equation form as

$$(x, y, z) \begin{pmatrix} A & C/2 & D/2 \\ C/2 & B & E/2 \\ D/2 & E/2 & F \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0. \tag{3.6}$$

Equation in $\mathbb{R}^2$	**Equation in homogeneous coordinates**	**Ideal points**
$x^2+y^2+1=0$	$x^2+y^2+z^2=0$	none
$x^2+y^2=0$	$x^2+y^2=0$	none
$x^2-y^2=0$	$x^2-y^2=0$	$(1,1,0)$ and $(1,-1,0)$

Table 1: Some degenerate conic sections.

Equation in $\mathbb{R}^2$	**Equation in homogeneous coordinates**	**Ideal points**
$x^2+y^2=1$	$x^2+y^2-z^2=0$	none
$x^2-y^2=1$	$x^2-y^2-z^2=1$	$(1,1,0)$ and $(1,-1,0)$
$y=x^2$	$x^2-zy=0$	$(0,1,0)$

Table 2: Some non-degenerate conic sections.

We show in a table how some conics extend to the projective plane and acquire some ideal points.

Finally, we show that the conic sections of the real projective plane can be transformed to each other by coordinate transformation. Let $\mathbf{u}=(x,y,z)^T$ and K the symmetric coefficient matrix of the conic section in (3.5). By Theorem 11(iii), a real symmetric matrix K is diagonizable by an orthogonal matrix M (with real entries), such that $M^T=M^{-1}$ and $M^TKM=D$. All entries in D are non-zero, as K was regular, and so was M, which has an inverse. We have that $\mathbf{u}^TK\mathbf{u}=0$ if and only if $(M^T\mathbf{u})^TD(M^T\mathbf{u})=0$, as $(M^T)^T(M^TKM)M^T=K$. So the same set of points in different coordinates can be written as $\mathbf{w}^TD\mathbf{w}$. Assume D has diagonal entries $\lambda_1,\lambda_2,\lambda_3$. Define the diagonal matrix N with entries $\frac{1}{\sqrt{|\lambda_1|}},\frac{1}{\sqrt{|\lambda_2|}},\frac{1}{\sqrt{|\lambda_3|}}$. Now all entries of N^TDN are ±1 numbers. So the coordinate transformation $\mathbf{v}=N\mathbf{w}$ transforms the conic into one with a diagonal matrix with all entries ±1. There cannot be 3 of $+1$'s or 3 of -1's, as then the conic would not have points, and by the coordinate transformations its points are bijectively corresponding to point set of the conic described by K. Hence we must have in the diagonal matrix two $+1$'s and one -1, or two -1's and one $+1$. But this two diagonal matrices define the very same conic.

At this point, we return to the question, why we assumed that (3.5) was regular. Denote this matrix by K and assume that it is singular. Diagonalization with matrix M still works out, but now D has some zero entries. So with $\mathbf{w}=(w_1,w_2,w_3)^T$ new variables, the quadratic form is

$$Sw_i^2+Tw_j^2=0, \tag{3.7}$$

with some S,T real coefficients and $i\neq j$ indices. Case 1: $ST\neq0$
This latter equation either only has the $w_i=w_j=0$ solution, or factors into a product of two linear polynomials in variables w_i,w_j. In the first subcase, unknowns x,y,z satisfy two independent homogeneous linear equations, hence the solution space is one dimensional. The solution space is a single point of the projective plane. In the second subcase, as w_i,w_j are linear combinations of x,y,z, (3.3) already can be written a product of two linear polynomials.
Case 2: $S=0,T\neq0$
$w_j^2=0$, where w_j is a linear combination of x,y,z. This is a line in the projective plane.

Case 2: $S = 0, T = 0$
D is the zero matrix, and therefore K is the zero matrix.

If we restrict the matrix equation (3.6) to the ordinary points $(x, y, 1)$, we get back precisely the definition of the conic in $\mathbb{R}^2$, (3.2). So the difference between ellipses, parabolas, and hyperbolas of $\mathbb{R}^2$ should be how they extend to the ideal points $(x, y, 0)$. From formula (3.4), ideal points $(x, y, 0)$ on the conic satisfy

$$Ax^2 + By^2 + Cxy = 0. \tag{3.8}$$

For an ideal point on the conic, (3.8) has solution in x, y, not simultaneously zero. If $A \neq 0$ or $B \neq 0$, we can solve (3.8) with the quadratic formula

$$x_{1,2} = \frac{-Cy \pm \sqrt{C^2y^2 - 4ABy^2}}{2A} \quad \text{or} \quad y_{1,2} = \frac{-Cx \pm \sqrt{C^2x^2 - 4ABx^2}}{2B}.$$

Case	**Discriminant** $C^2 - 4AB$	**Number of ideal points**	**Classification in** $\mathbb{R}^2$
$A \neq 0$ or $B \neq 0$	> 0	2	hyperbola or two crossing lines
$A \neq 0$ or $B \neq 0$	$= 0$	1	parabola or parallel lines
$A \neq 0$ or $B \neq 0$	< 0	0	ellipse or one point or no points
$A = 0$, $B = 0$, $C = 0$		1	line
$A = 0$, $B = 0$, $C \neq 0$		2	hyperbola or two crossing lines

Table 3: Classification of conic sections of $\mathbb{R}^2$.

The moral of Table 3 is that a non-degenerate conic section in $\mathbb{R}^2$ is ellipse, parabola or hyperbola, according to the number of ideal points its extension has in the projective plane.

4 Incidence structures

Consider two disjoint sets, $P \neq \emptyset$, whose elements are called *points*, and $L \neq \emptyset$, whose elements are called *lines*. There is a relation $I \subseteq P \times L$ called *incidence*. When $(p, \ell) \in I$, we also write $p \vdash \ell$, and say that p and ℓ are *incident*. We call (P, L, I) an *incidence structure*. If every element of a set of points is incident to the same line ℓ, we say that the point set is *collinear*. If every element of a set of lines is incident to the same point p, we say that the line set is *concurrent*.

Incidence structures (P_1, L_1, I_1) and (P_2, L_2, I_2) are considered *isomorphic*, if there are $f : P_1 \to P_2$ and $g : L_1 \to L_2$ bijections, such that $(p, \ell) \in I_1$ if and only if $(f(p), g(\ell)) \in I_2$.

From now on, assume now properties (P1) and (P2) from Claim 1 as axioms for our incidence structure. Let us denote the line determined by the points p, q by $L(p, q)$. Let us overview the possibilities (see Fig. 1):
(a) There is only one point, and zero, one or more lines incident to it. If zero lines are incident to the point, then there could be at most one line, which is not incident to any point.
(b) There is only one line, and zero, one or more points incident to it. If zero points are incident

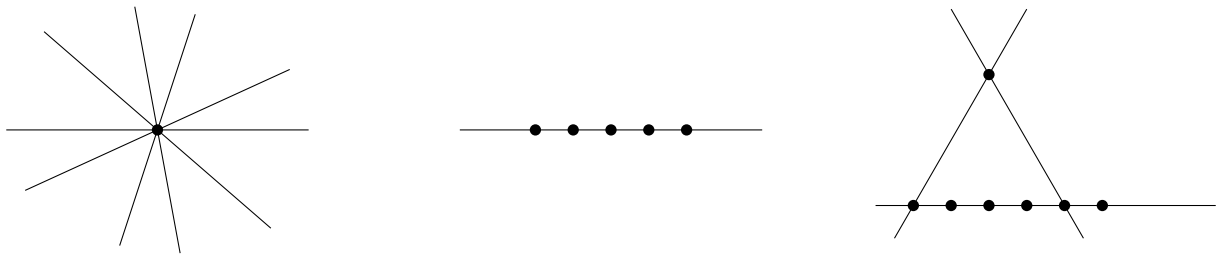

Figure 1: Incidence structures satisfying (P1)-(P2), but not (P3).

to the line, then there could be at most one point, which is not incident to any line.
(c) There are 3 non-collinear points, p, q, r. We have two possibilities:

(c1) (P3) holds.

(c2) There is one of the 3 lines $L(p,q)$, $L(p,r)$, $L(r,q)$, which must contain all further points, if there is any.

We prove that there are no more possibilities. Assume that there is a fourth point $s \vdash L(p,q)$, and a fifth point $t \vdash L(p,r)$. Then the lines $L(s,r)$ and $L(q,t)$ are distinct, and there is a point $z \vdash L(s,r)$ and $z \vdash L(q,t)$. z is different from each of p, q, r. Now the four points p, q, r, z verify (P3). See Fig. 2.

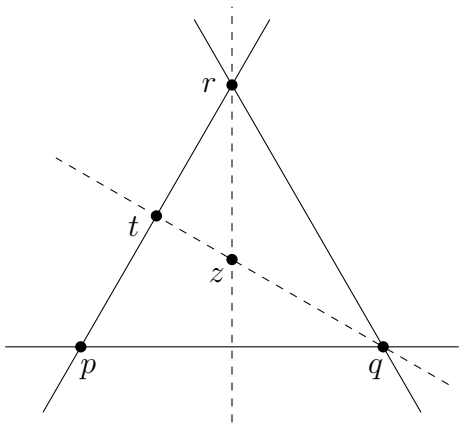

Figure 2: Finding the fourth point for (P3).

By (P1), with the exception of the degenerate case (a), two different lines are never incident with the very same set of points. Therefore, if we have at least 2 points, we may identify the lines with the sets of points, to which they are incident.

For an arbitrary relation $I \subset P \times L$, condsider the *transpose* of the relation $I^T \subset L \times P$ defined by $(\ell, p) \in I^T$ if and only if $(p, \ell) \in I$. Incidence structures (P, L, I) and (L, P, I^T) are called *dual* incidence structures. It is easy to see that dual incidence structures simultaneously satisfy properties (P1)-(P2), and simultaneously satisfy properties (P1)-(P2)-(P3)-(P4). Whether

(P, L, I) and (L, P, I^T) are isomorphic incidence structures is a natural question, which we later look into.

5 Projective planes

Assume that (P1), (P2), and (P3) holds in an incidence structure (P, L, I). Then this structure is called a *projective plane*. The dual of a projective plane is a projective plane. Changing in a statement about points, lines, and incidences the role of points and lines, we obtain the dual statement. Such a statement holds in every projective plane if and only if its dual holds in all projective planes.

It is easy to see that in projective plane P is finite if and only if L is finite. In such cases we speak about *finite projective planes*. For every finite projective plane (not just for the field based ones!), there exists an integer q, such that every point is incident $q + 1$ lines and every line is incident to $q + 1$ points. Furthermore, the both the number of points and the number of lines is $q^2 + q + 1$. See Homework Problems F3), F4). This q is called the *order* of the finite projective plane.

Not all known finite projective planes are field-based like the construction in Section 2. Other finite projective planes are constructed from some relaxation of the field structure, and then following a version of the construction in Section 2. Some necessary conditions for a number to be the order of a finite projective plane are known, but they are far from proving the old conjecture that if a finite projective plane exists, its order must be a prime power. There is no projective plane of order 6; a substantial computing project showed that there is no projective plane of order 10, and the existence of an order 12 projective plane is open.

For example, the following two theorems, well-known in real projective geometry, can be proved with manipulation of coordinates. They extend to every projective plane over a field, as the manipulation does not use anything beyond the axioms of a field. They are not true, however, for all projective planes. The smallest order for a finite projective plane that fails these theorems is 9.

Theorem 1 [Pappus] *For any two lines L_1, L_2 in the real projective plane, and any distinct points a_i, b_i, c_i on L_i, all different from the point $L_1 \cap L_2$, the three points $L(a_1, b_2) \cap L(a_2, b_1)$, $L(a_1, c_2) \cap L(a_2, c_1)$, $L(b_1, c_2) \cap L(b_2, c_1)$ are on one line. See Fig. 4.*

Note that in the Fano plane (see Fig. 3) there are only 3 points on a line, so the hypothesis of the implication in Pappus' theorem is never true. Therefore, in the Fano plane Pappus' theorem is vacuously true.

By a *triangle* in a projective plane we mean 3 points not on a single line. We say that two triangles, a_1, b_1, c_1 and a_2, b_2, c_2 are *perspective to a point*, if $L(a_1, a_2) \cap L(b_1, b_2) \cap L(c_1, c_2) \neq \emptyset$. We say that two triangles, a_1, b_1, c_1 and a_2, b_2, c_2 are *perspective to a line*, if the three points $L(a_1, b_1) \cap L(a_2, b_2)$, $L(a_1, c_1) \cap L(a_2, c_2)$, $L(c_1, b_1) \cap L(c_2, b_2)$ are on one line. See Fig. 5.

Theorem 2 [Desargues] *In the real projective plane, two triangles are perspective to a line if and only if they are perspective to a point.*

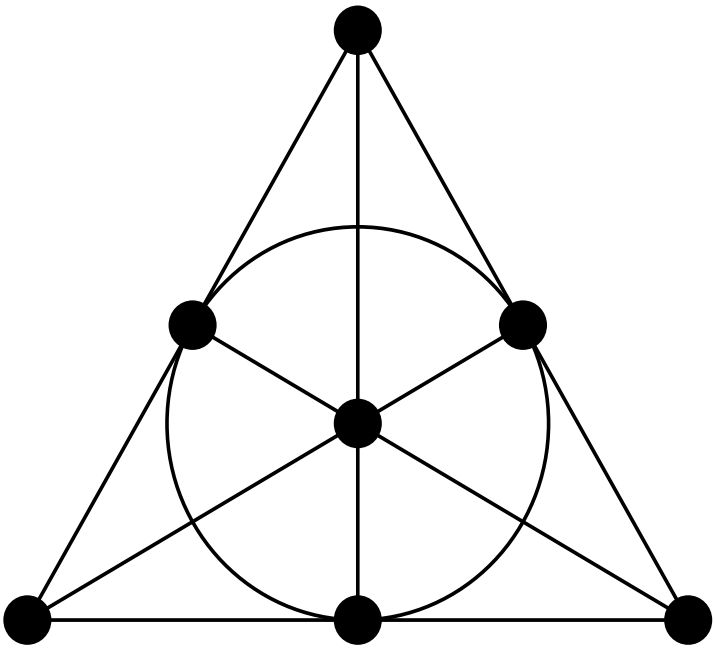

Figure 3: The Fano plane. From Wikipedia.

We leave the proof of Pappus' and Desargues' theorems to the homework problems.

Theorem 3 [Hessenberg] *If Pappus' Theorem holds in a projective plane, then Desargues' Theorem also holds in this plane.*

The converse of Hessenberg's Theorem holds in *finite* projective planes.

The natural structure preserving map between projective planes is *collineation*. For projective planes (P_1, L_1, I_1) and (P_2, L_2, I_2), f is a collineation from the first plane to the second, if $f : P_1 \to P_2$ is a bijection, and for any three points, p, q, r, if they are collinear in the first plane, then their images $f(p), f(q), f(r)$ are collinear in the second plane. In the Spheric Model of the real projective plane, every non-degenerate linear transformation of $\mathbb{R}^3$ induces a collineation.

Theorem 4 *(i) If f is a collineation, then the inverse bijection f^{-1} is also a collineation.*
(ii) There exists a collineation from projective plane (P_1, L_1, I_1) to projective plane (P_2, L_2, I_2) if and only if (P_1, L_1, I_1) and (P_2, L_2, I_2) are isomorphic as incidence structures.

To prove (i), assume that $f(p), f(q), f(r)$ are collinear in the second plane, say incident to line ℓ, but p, q, r are not collinear in the first plane. By the definition of collineation, f maps the all the points incident to the lines $L(p, q), L(p, r)$ and $L(q, r)$ into ℓ. Take now any x point of the first plane, which is not incident to any of these 3 lines. The line $L(x, p)$ has unique common point with $L(q, r)$, say y. We have $f(y) \vdash \ell$, and by collinearity, $f(y) \vdash \ell$, and as x, p, y are collinear, by collinearity $f(x) \vdash \ell$. So the bijection f maps all points of the first plane to the line ℓ of the

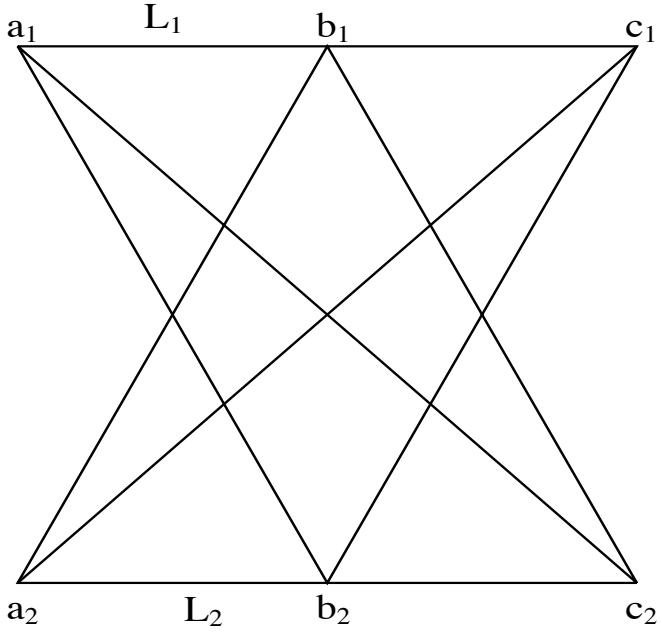

Figure 4: Pappus' Theorem. From Wikipedia.

second plane. But the second plane must have points not incident to line ℓ.
To prove (ii), assume that $f : P_1 \to P_2$ and $g : L_1 \to L_2$ are bijections preserving the incidence structures. Then f is a collineation from the first projective plane to the second. Indeed, if $p, q, r \in P_1$ and $\ell \in L_1$, such that $p \vdash \ell$, $q \vdash \ell$, and $r \vdash \ell$, then $f(p) \vdash g(\ell)$, $f(q) \vdash g(\ell)$, and $f(r) \vdash g(\ell)$.
Assume now that f is a collineation form the first projective plane to the second. We have to provide $P_1 \to P_2$ and $L_1 \to L_2$ bijections that preserve the incidence structures. We use the collineation itself for the bijection $f : P_1 \to P_2$. For any line $\ell \in L_1$, take two arbitrary different points, p, q, such that $\ell = L(p, q)$. We define $g(\ell)$ as $L(f(p), f(q))$. We must show that g is well-defined and that f and g preserve incidences.
Take any two points p', q', such that $\ell = L(p', q')$. Then any three of the points p, q, p', q' are collinear, hence any three of the points $f(p), f(q), f(p'), f(q')$ are collinear, as f was a collineation. Therefore $L(f(p), f(q)) = L(f(p'), f(q'))$, so g is well-defined.
Assume now $p \vdash \ell$ in the first projective plane. Take a $q \neq p$ such that $q \vdash \ell$. Now $f(p) \vdash L(f(p), f(q)) = g(\ell)$. Assume now $f(r) \vdash g(\ell)$ in the second projective plane. Assume that $g(\ell)$ was defined as $L(f(p), f(q))$ for some p, q points with $L(p, q) = \ell$. Now $f(r), f(p), f(q)$ are collinear in the second plane. In part (i) of the theorem we showed that the inverse of a collineation is also a collineation, so p, q, r are collinear, and hence $r \vdash \ell$.

For projective planes, we return to the question whether (P, L, I) and (L, P, I^T) are isomorphic incidence structures. In view of Theorem 4, this is the case if and only if there is an $f : P \to L$ bijection, which is a collineation from (P, L, I) to its dual.

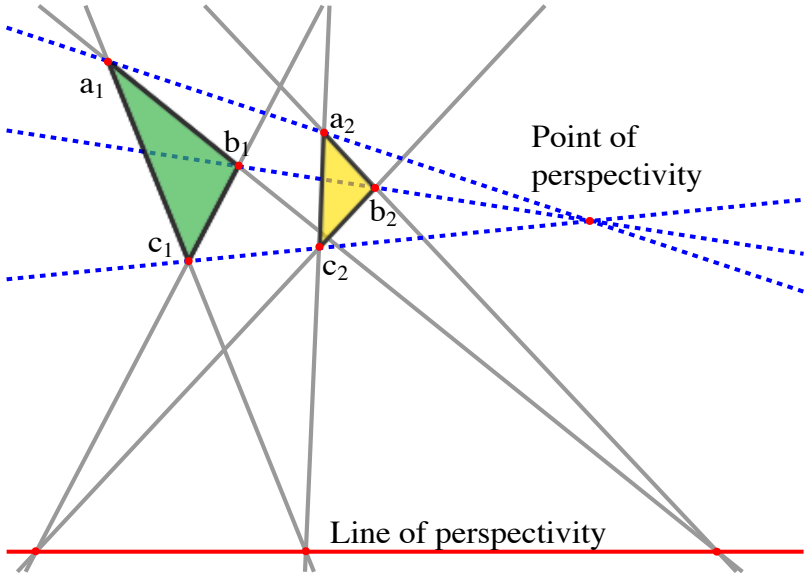

Figure 5: Perspectivity to a point and perspectivity to a line. From Wikipedia.

Given a pair of dual projective planes, (P, L, I) and (L, P, I^T), an $f : P \to L$ collineation is called a *polarity*. In view of Theorem 4 Part (ii), for every polarity f, there is a $g : L \to P$, such that f and g shows the isomorphism of the incidence structures (P, L, I) and (L, P, I^T). This g is obviously unique, and the choice $g = f^{-1}$ suffices by Theorem 4 Part (i). It is customary to extend f to an involution as $f : P \cup L \to P \cup L$ with $f\big|_L = g$, as the original f was not defined on L. A point and a line matched by f are referred to as a *pole* and its *polar*. The smallest finite projective plane without polarity has order 9.

If we have a polarity, then we have many, as the composition of a collineation and a polarity is a polarity (Homework problem). $f : P \to L$ involution is a polarity of the projective plane if and only if the following symmetry holds: for all p, q points

$$q \vdash f(p) \text{ if and only if } p \vdash f(q). \tag{5.9}$$

We define the *polarity graph* of f with vertex set P, by joining poles to the points of their polar lines. By (5.9) this is indeed a graph, as the relation is symmetric. The polarity graph is C_4-free, as two different lines intersect in one point. The polarity graph may have loops.

Field based projective planes do have polarities. For example,

$$f_1 : (x, y, z) \to [x, y, z] \tag{5.10}$$

is a polarity. In the real projective geometry, under this f_1 polarity, a pole is never incident to its polar, as no point of the real projective plane satisfies $x^2 + y^2 + z^2 = 0$. So the polarity graph has no loops. Such polarities are called *elliptic*, while other polarities called *hyperbolic*. For another example, take

$$f_2 : (x, y, z) \to [x, y, -z]. \tag{5.11}$$

(Note that if the field has characteristic 2, then simply $f_1 = f_2$.) It is easy to see that

$$g_2 = f_2 : [A, B, C] \to (A, B, -C).$$

A point represented by (x, y, z) is connected to itself in the polarity graph if and only if the point is incident to its polar line, i.e., $x^2 + y^2 = z^2$.

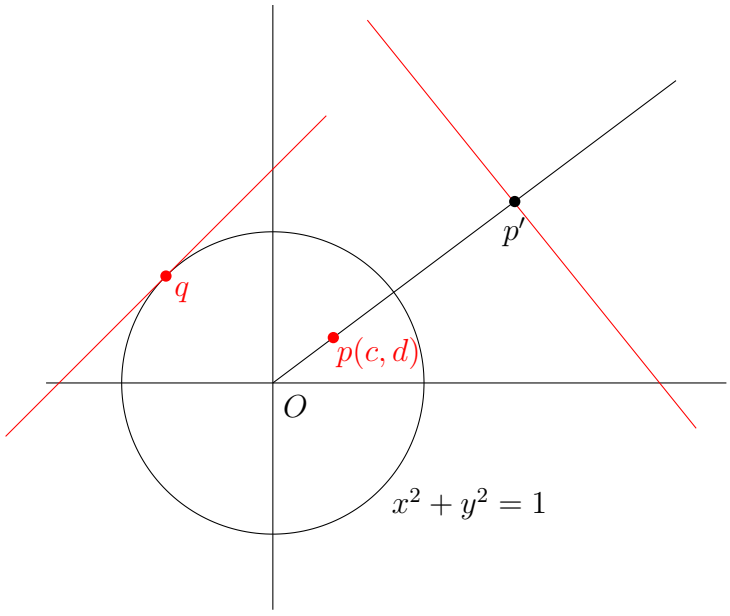

Figure 6: Polarity f_2 on the ordinary points.

Let us visualize now f_1 from (5.10) in the Spheric Model of the real projective plane. Consider the two antipodal points of the unit sphere representing the equivalence class of (x, y, z), which is the pole. The polar line is represented by the triplet $[x, y, z]$, which means the polar line is the "equator" of the unit sphere, perpendicular to the segment connecting the representatives of the pole.

Let us visualize now f_2 from (5.11) in the Spheric Model of the real projective plane. Consider the two antipodal points of the unit sphere representing the equivalence class of (x, y, z), which is the pole. The polar line is represented by the triplet $[x, y, -z]$. Some points are incident to their polar lines, some are not, for example point $(1, 0, 1)$ is incident, point $(1, 1, 0)$ is not. Exactly the points of the conic $x^2 + y^2 - z^2 = 0$ are incident to their polar line. Focus on the action of f_2 on the ordinary points, see Fig. 6. Ordinary point p can be represented as $(c, d, 1)$. The polar line of pole p is $[c, d, -1]$. The pole is incident to its polar line if and only if $c^2 + d^2 - 1 = 0$. The equation of the polar line of p, restricted to the affine plane, is $cx + dy = 1$. Hence the pole (c, d) is incident to its polar line if and only if p is a point of the unit circle. Consider the ray from $O = (0, 0)$ through $p = (c, d)$, and find a point p' on it such that $\overline{Op} \cdot \overline{Op'} = 1$. The polar line $cx + dy = 1$ is perpendicular to Op and passes through p' (see homework problems). If p is on the unit circle, then its polar line is the tangent line at p, as it is well-known that for the $p(x_0, y_0)$ point of the unit circle the equation of the tangent line is $x_0x + y_0y = 1$.

In the real projective plane, every K matrix of a non-degenerate conic in (3.5) defines a polarity by

$$(x,y,z) \mapsto [X,Y,Z] \quad \text{by} \quad [X,Y,Z] = (x,y,z)K.$$

Formula (5.9) hold, as (u,v,w) is incident to the polar line of $(x,y,z) \Leftrightarrow Xu+Yv+Zw=0 \Leftrightarrow$

$$(x,y,z)K\begin{pmatrix}u\\v\\w\end{pmatrix}=0 \Leftrightarrow (u,v,w)K^T\begin{pmatrix}x\\y\\z\end{pmatrix}=0 \Leftrightarrow (u,v,w)K\begin{pmatrix}x\\y\\z\end{pmatrix}=0 \Leftrightarrow$$

(x,y,z) is incident to the polar line of (u,v,w). A point is incident to its polar line if and only if the point belongs to the conic in question.

6 An intersection problem leading to finite projective planes

Theorem 5 *Assume that $A_i \subseteq [n]$ for $i=1,2,...,m$, and for any two sets $|A_i \cap A_j| = t \geq 1$. Then there is a t element set in the family, or the indicator functions of the sets are linearly independent in the linear space of $[n] \to \mathbb{R}$ functions over the field $\mathbb{R}$. Consequently, $m \leq n$.*

Let us denote the indicator function of the set A by χ_A, so $\chi_A : [n] \to \mathbb{R}$ and

$$\chi_A(a) = \begin{cases} 0, & \text{if } a \notin A \\ 1, & \text{if } a \in A. \end{cases}$$

Observe that the functions $[n] \to \mathbb{R}$ make a linear space V over $\mathbb{R}$. As clearly $\chi_{\{x\}} : x \in [n]$ is a basis, the dimension of this linear space is n. We make this linear space V an inner product space by defining $(f,g) = \sum_{x=1}^n f(x)g(x)$. Note that (f,g) is *bilinear*. i.e. with any fixed f it is a linear function of g, and with any fixed g, it is a linear function of f.

Let us return to the family of sets. If $|A_1| = t$, then the other sets partition the remaining $n-t$ elements, so $m-1 \leq n-t \leq n-1$. If all $|A_i| > t$, and the linear independence holds, then the size of a set of linearly independent vectors is at most the dimension, n.

Assume that there are not all zero real numbers such that $\sum_{i=1}^m c_i \chi_{A_i} = 0$, the identically zero function. Then

$$\begin{aligned} 0 &= \left(\sum_{i=1}^m c_i\chi_{A_i}, \sum_{i=1}^m c_i\chi_{A_i}\right) = \sum_{i=1}^m c_i^2\Big(\chi_{A_i},\chi_{A_i}\Big) + 2\sum_{1\leq i<j\leq m} c_ic_j\Big(\chi_{A_i},\chi_{A_j}\Big) \\ &= \sum_{i=1}^m c_i^2|A_i| + 2t\sum_{1\leq i<j\leq m} c_ic_j - t\sum_{i=1}^m c_i^2 + t\sum_{i=1}^m c_i^2 \\ &= \sum_{i=1}^m c_i^2\Big(|A_i|-t\Big) + t\Big(\sum_{i=1}^m c_i\Big)^2, \end{aligned}$$

showing that every c_i must be zero.

For general t, there is no classification of how $m=n$ can happen. There is however, the following theorem of Ryser that we do not prove. We call the *degree* of a point the number of A_i sets that contain it.

Theorem 6 [Ryser] *If a family of sets realizes $m = n$, then at most two different degrees may occur.*

However, for $t = 1$ we can give a kind of characterization.

Theorem 7 [Erdős-de Bruijn] *If for $t = 1$, a family of sets realizes $m = n$, then the family is*
(i) a singleton and all doubletons containing it; or
(ii) the lines of a finite projective plane; or
(iii) an $n-1$-element subset and all doubleton containing the leftover element.

Assume $m = n$. If there is a singleton in the system, the only possibility is (i). If there is no singleton, we may assume that every element of the underlying set is contained by at least one family member. (If not, there is a contradiction with Theorem 5.) We are going to show that property (P2) holds for our family of sets, if the sets are considered the lines. It will be left for the homework problems, that for $n \geq 2$, (P1) and (P2) imply $\big($(P3) or outcome (iii)$\big)$.

With a slight abuse of notation, we write χ_x instead of $\chi_{\{x\}}$ for $x \in [n]$. As χ_{A_i} $i = 1, 2, ..., n$ are linearly independent in an n-dimensional linear space, they form a basis, and we can express with them the elements of the other basis:

$$\chi_x = \sum_{i=1}^{n} \beta_{x,i} \chi_{A_i}.$$

We have

$$(\chi_x, \chi_{A_j}) = \sum_{i=1}^{n} \beta_{x,i} (\chi_{A_i}, \chi_{A_j}) = \Big(\sum_{i=1}^{n} \beta_{x,i}\Big) + \beta_{x,j}(|A_j| - 1).$$

Define $\beta_x = \sum_{i=1}^{n} \beta_{x,i}$ and observe

$$\beta_x + \beta_{x,j}(|A_j| - 1) = (\chi_x, \chi_{A_j}) = \begin{cases} 0, & \text{if } x \notin A_j \\ 1, & \text{if } x \in A_j. \end{cases}$$

As $|A_j| > 1$, we can solve the the last equation for $\beta_{x,j}$:

$$\beta_{x,j} = \frac{(\chi_x, \chi_{A_j}) - \beta_x}{|A_j| - 1}. \tag{6.12}$$

On there other hand,

$$\beta_x = \sum_{j=1}^{n} \beta_{x,j} = \sum_{j=1}^{n} \frac{(\chi_x, \chi_{A_j}) - \beta_x}{|A_j| - 1} = \sum_{j=1}^{n} \frac{(\chi_x, \chi_{A_j})}{|A_j| - 1} - \beta_x \sum_{j=1}^{n} \frac{1}{|A_j| - 1},$$

and

$$\beta_x \left(1 + \sum_{j=1}^{n} \frac{1}{|A_j| - 1}\right) = \sum_{\substack{j=1 \\ x \in A_j}}^{n} \frac{1}{|A_j| - 1}.$$

From here, we observe $0 < \beta_x < 1$ and based on (6.12),

$$x \in A_j \Leftrightarrow \beta_{x,j} > 0 \qquad \text{and} \qquad x \notin A_j \Leftrightarrow \beta_{x,j} < 0.$$

Finally, we show that for any $x \neq y$ elements from $[n]$, there is some A_j, such that $\{x, y\} \subseteq A_j$, as it was claimed. Consider

$$0 = (\chi_x, \chi_y) = \sum_{j=1}^{n} \beta_{x,j}(\chi_{A_j}, \chi_y) = \sum_{\substack{j=1 \\ y \in A_j}}^{n} \beta_{x,j}.$$

Note that the last sum does have non-zero terms: as y is contained by some A_j set, a term $\beta_{x,j} \neq 0$ is there. However, if this sum is 0, it must have both positive and negative terms. So find a j such that $y \in A_j$ and $\beta_{x,j} > 0$. As $x \in A_j$, the proof is complete.

7 Graphs without C_3 or C_4

We study here two problems from extremal graph theory, as an introduction to estimations.

Theorem 8 [Mantel (1907)] *If a simple graph G on n vertices does not have a C_3, then its size e satisfies $e \leq \frac{n^2}{4}$.*

Clearly this is the best possible result, because of the complete bipartite graph $K_{\lceil \frac{n}{2} \rceil, \lfloor \frac{n}{2} \rfloor}$. Consider any edge ab of G. Let $d(x)$ denote the degree of the vertex x. As a and b cannot have common neighbors, each are joined to at most one out the other $n-2$ vertices, and as they are joined to each other,

$$n \geq d(a) + d(b).$$

Summing up for all edges,

$$ne \geq \sum_{ab \in E(G)} \Big(d(a) + d(b)\Big) = \sum_{x \in V(G)} d^2(x).$$

By the inequality of Quadratic and Arithmetic Means,

$$\sum_{x \in V(G)} d^2(x) \geq \frac{\left(\sum_{x \in V(G)} d(x)\right)^2}{n} = \frac{(2e)^2}{n}.$$

Solving the inequality for e we obtain the claim. Note that Mantel's Theorem has a far-reaching generalization in the form of Turán's Graph Theorem, which tells the maximum number of edges that a graph can have without a K_k, and the structure of graphs with the maximum number of edges. Note $C_3 = K_3$. Turán's Graph Theorem was further generalized by Erdős and Stone: suppose that H is a finite simple graph, with chromatic number $r \geq 2$. Then, the maximum number of edges in a simple graph on n vertices, of which H is not a subgraph, is

$$\left(\frac{r-2}{r-1} + o(1)\right)\binom{n}{2}.$$

This is an asymptotic formula, *except* when $r = 2$. Few excluded bipartite subgraph problems are completely solved. We discuss some excluded bipartite subgraph problems.

Theorem 9 [Reiman (1958)] *If a simple graph G on n vertices does not have a C_4, then its size e satisfies $e \leq \frac{n}{4}(1+\sqrt{4n-3})$.*

We make a double count again. Count $\{(u,\{v,w\}) : v \neq w, uv \in E(G), uw \in E(G)\}$. On the one hand, their number is *exactly* $\sum_{x\in V(G)} \binom{d(x)}{2}$. On the other hand, for every $\{v,w\} \subseteq V(G)$, there is at most one corresponding u, as two different u's with v,w would provide a C_4. Hence

$$\sum_{x\in V(G)} \binom{d(x)}{2} \leq \binom{n}{2}. \tag{7.13}$$

A homework problem finishes the proof of the theorem.

We show an alternative argument that we will use to set lower bounds for $\sum_i \binom{a_i}{k}$ for any positive integer k. So this is a bit of overkill here, which does not even provide the correct leading coefficient in Reiman's theorem, but it is often a useful tool.

First recall that a function $f(x)$ defined on an interval I is *concave up*, if the line segment connecting the points $(a,f(a))$ and $(b,f(b))$ for every $a,b \in I$ is never below the graph of the function. In terms of an inequality, for all $0 < \lambda < 1$,

$$f\Big(\lambda a + (1-\lambda)b\Big) \leq \lambda f(a) + (1-\lambda) f(b).$$

Theorem 10 [Jensen's Inequality] *For any $n \geq 1$ integer and $0 < \lambda_1, ..., \lambda_n$ with $\sum_{i=1}^n \lambda_i = 1$, if $x_1, ..., x_n$ fall into the interval I, where $f(x)$ is concave up, then*

$$f\Big(\sum_{i=1}^n \lambda_i x_i\Big) \leq \sum_{i=1}^n \lambda_i f(x_i).$$

Furthermore, if equality holds, then all x's must be belong to a subinterval, where $f(x)$ is linear, allowing a single point as an interval as well.

Recall that $\binom{x}{k}$ for every positive integer k is a polynomial of x defined by $\frac{(x)_k}{k!}$. This is a degree k polynomial and its roots are $0, 1, ..., k-1$. Therefore its derivative must have a root in $(i, i+1)$ for $i = 0, 1, ..., k-2$, which accounts for all of its $k-1$ roots, and similarly the second derivative has a root between any consecutive pairs of roots of the first derivative. [One can shorten this argument using a result of Gauss about the roots of the derivative of a complex polynomial, see Problem 14.] On the interval $[k-1, \infty)$ the function $\binom{x}{k}$ is concave up. (Not having any root of the second derivative in the interval, it cannot change concavity. In the second derivative of polynomial $\binom{x}{k}$ the dominant term is $\frac{x^{k-2}}{(k-2)!}$, as $x \to \infty$, and hence for sufficiently large x the second derivative is positive. The second derivative must be positive on the interval $[(k-1, \infty).)$ Defining a new function by

$$\binom{x}{k}^+ = \begin{cases} 0, & \text{if } x \leq k-1 \\ \binom{x}{k}, & \text{if } x \geq k-1, \end{cases}$$

we defined a concave up function on all real numbers. (If a segment connecting a zero valued point with some point of $(x_0, \binom{x_0}{k})$ would intersect the curve somewhere above the interval $(k-1, x_0)$, it would contradict that $\binom{x}{k}$ is concave up there.) Formula (7.13) can be continued with Jensen's Inequality as

$$n\binom{\frac{2e}{n}}{2}^+ \le n\binom{\frac{1}{n}\sum_{x\in V(G)} d(x)}{2}^+ \le \sum_{x\in V(G)} \binom{d(x)}{2}^+ \le \sum_{x\in V(G)} \binom{d(x)}{2} \le \binom{n}{2}. \tag{7.14}$$

Either $\frac{2e}{n} \le 2$ or $\frac{2e}{n} \ge 2$, we obtain the bound in the theorem in the form of $O(n^{3/2})$; as $e \le n$ in the first case, and $(\frac{2e}{n} - 1)^2 \le n - 1$ in the second case.

Now we create a graph on n vertices that have $cn^{3/2}$ edges and no C_4, when n is large enough. Knowing that finite projective planes over $GF(q)$ exists, the simplest construction for such a graph is the incidence bipartite graph of points and lines of a projective plane of order q. In the incidence bipartite graph, there is an edge between incident points and a lines. This bipartite graph has $|V| = 2(q^2+q+1)$ vertices and $|E| = (q+1)(q^2+q+1)$ edges. The graph is obviously C_4-free by (P1) and (P2), and the graph has $|E| \sim \frac{1}{2\sqrt{2}}|V|^{3/2}$ edges.

We can improve on the constant using the polarity graph defined in Section 5. Let the vertex set be the point set of the finite projective plane over $GF(q)$ for a prime power q, so $|V| = q^2+q+1$. The polarity graph is C_4-free. We use the polarity f_2 from (5.11). We can define conics in any projective plane over a field, as we did over the reals in (3.4). Over $GF(q)$, the conic $x^2+y^2=z^2$ has $q+1$ points, as all conics have exactly $q+1$ points (we skip the proof of this). If a point is not on the conic, it is connected to the $q+1$ points of its polar line. If a point is on the conic, it is connected to q points of its polar line, as we do not connect it to itself. Hence twice the number of edges is $(q+1)q + [q^2+q+1-(q+1)](q+1) = q(q+1)^2$, so the number of edges is $\frac{q}{2}(q+1)^2$.

Eventually Füredi proved that for $q \ge 15$, on q^2+q+1 vertices a C_4-free graph has at most $\frac{q}{2}(q+1)^2$ edges, which is tight for prime power q

There is a routine way to extend constructions for prime or prime power n—with some loss in the leading constant—to all sufficiently large n vertices. From Bertrand's Postulate (Tschebyseff's theorem), for any m positive integer, there is a prime in $[m, 2m]$. Hence for any m positive integer, there is a prime square in $[m^2, 4m^2]$. It is easy to see that for $n \ge 100$, there is a number of the form $4m^2$ in $[\frac{n}{2}, n]$, and there is a $p^2 \in [m^2, 4m^2] \subseteq [\frac{n}{8}, n]$, providing a construction on a smaller set of vertices that can be extended with isolated vertices at the cost of reducing the constant c in $cn^{3/2}$. The Prime Number Theorem implies that for any $\epsilon > 0$, for sufficiently large n, there is a prime in the interval $(n-\epsilon n, n)$. This would give better leading constant than the argument with Bertrand's Postulate, at the cost of an added error term.

8 Generalized Quadrangles

Let us be positive integers s, t. An incidence structure of set of points P and lines Q make a generalized quadrangle $GQ(s,t)$, if it satisfies the following 4 axioms:
(GQ1) Every line has exactly $s+1$ points

(GQ2) Every point is on exactly $t+1$ lines
(GQ3) Any two lines intersect in at most one point
(GQ4) For every point p and every line ℓ not passing through p, there is a unique line ℓ', such that ℓ' goes through p and ℓ' intersects ℓ.
As there is at most one line through any two points, switching the names of points and lines results in a *dual* generalized quadrangle $GQ(t,s)$.

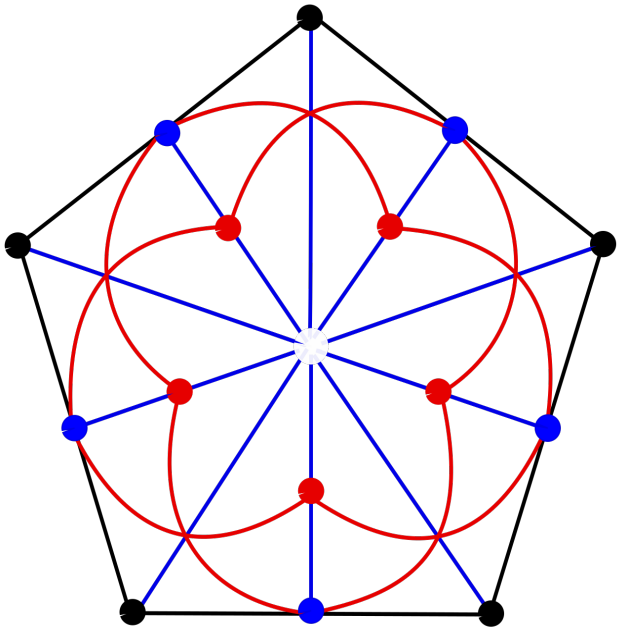

Figure 7: The Doily: $GQ(2,2)$. From Wikipedia.

An important property of generalized quadrangles is that they are *triangle free*. A triangle would contradict the uniqueness in (GQ4). Two points are called *collinear*, if there is a common line passing through them. A point is collinear with itself. We will denote this relation by $x \sim y$, although it is *not* an equivalence relation, and speak about the *collinearity graph*. Let us count the number of points. Take an arbitrary line ℓ. It has $s+1$ points. Any point $p \in \ell$ is incident to t additional lines, and those lines altogether have $st+1$ points. These $st+1$-sets points of points are disjoint for different p's, and by (GQ4) they cover all points. Hence the number of points is

$$|P| = (st+1)(s+1).$$

A dual count provides

$$|L| = (st+1)(t+1).$$

Let $x^\perp$ denote the neighborhood of the point x in the collinearity graph, in particular $x \in x^\perp$.

Observe that

$$\begin{aligned} x \sim y &\Rightarrow |x^\perp \cap y^\perp| = s+1, \\ x \not\sim y &\Rightarrow |x^\perp \cap y^\perp| = t+1. \end{aligned}$$

Hence the collinearity graph is a strongly regular graph. Eigenvalues of the adjacency matrix of strongly regular graphs, and their multiplicities can be explicitly computed. This gives a necessary divisibility condition for the existence of a $GQ(s,t)$,

$$s+t \Big| st(s+1)(t+1),$$

whose reason is that the fraction of these two numbers is the multiplicity of an eigenvalue in the adjacency matrix of the collinearity graph, and hence must be an integer. This will be shown in the next section. Further necessary conditions are the Higman's Inequalities require

$$s > 1 \text{ and } t > 1 \Rightarrow t \leq s^2 \text{ and } s \leq t^2. \tag{8.15}$$

For every positive integer z, there is a $GQ(z,1)$ defined by a $(z+1) \times (z+1)$ grid with its $z+1$ horizontal and $z+1$ vertical lines; there is a $GQ(1,z)$ defined by the vertex set of a complete bipartite graph $K_{z+1,z+1}$ as point set and the edge set as line set. For $s > 1, t > 1$ only the following generalized quadrangles are known to exist: for some prime power q,

$$\begin{aligned} (s,t) &= (q,q), \\ &= (q,q^2),(q^2,q) \\ &= (q^2,q^3),(q^3,q^2) \\ &= (q-1,q+1),(q+1,q-1). \end{aligned}$$

We show $GQ(2,2)$, known as the Doily, among the figures.

Finally, we give Cameron's proof to Higman's inequalities (8.15). Take two non-collinear points, $x \not\sim y$. Define a point set by

$$V = \{z \in P : \ x \not\sim z \text{ and } y \not\sim z\}.$$

We are going to find the number of the elements d of V, by an inclusion-exclusion argument:

$$d = |V| = (s+1)(st+1) - 2 - 2(t+1)s + (t+1). \tag{8.16}$$

Indeed, from a total of $(s+1)(st+1)$ points, x and y comes out, and also all the points on the lines passing through them. This is $(t+1)s$ for each, but $|x^\perp \cap y^\perp| = t+1$. Write

$$V = \{z_1, ..., z_d\}$$

for some d. Set

$$t_i = |\{u \in P : u \sim x \text{ and } u \sim y \text{ and } u \sim z_i\}|.$$

Count now ordered pairs $(z_i, u) \in V \times (x^\perp \cap y^\perp)$ with $z_i \sim u$ in two ways. On the one hand, it is $\sum_{i=1}^d t_i$. On the other hand, there are $t+1$ lines passing through x. For each of these lines, there is a unique point u such that $u \sim y$. This gives us $t+1$ possible u points. We show that each of this points can be paired with $(t-1)s$ possible z_i's. Indeed, any point different from u on any other line than the already used 2 passing through u can be a z_i, and only those points can be z_i's. Hence

$$\sum_{i=1}^{d} t_i = (t+1)(t-1)s.$$

Count now ordered triplets $(z_i, u, u') \in V \times (x^\perp \cap y^\perp) \times (x^\perp \cap y^\perp)$, where $u \neq u'$, $u \sim z_i$, and $u' \sim z_i$ in two ways. On the one hand, for a fixed z_i, there are t_i choices for u and then $t_i - 1$ choices for u'. On the other hand, like in the previous double counting argument, we have $t+1$ choices for u. u' cannot be on the line of u and x, but on every other line passing through x, there is a unique possible u' collinear with y. z_i must be on a line passing through u', but that line cannot be the $u'x$ or the $u'y$ line. There are $t-1$ choices for this line. As $u \not\sim u'$ (otherwise u, u', y is a triangle), $|u^\perp \cap (u')^\perp| = t+1$, where x and y takes two of these $t+1$ elements, and $t-1$ choices are left for z_i. We conclude

$$\sum_{i=1}^{d} t_i(t_i - 1) = (t+1)t(t-1).$$

Adding up the two identities obtained by double counting, we have

$$\sum_{i=1}^{d} t_i^2 = (t+1)(t-1)(s+t).$$

Now observe that

$$\begin{aligned} 0 &\leq \sum_{i=1}^{d} \left(\frac{\sum_{j=1}^d t_j}{d} - t_i \right)^2 = \frac{1}{d^2} \sum_{i=1}^{d} \left(\Big(\sum_{j=1}^{d} t_j\Big) - d t_i \right)^2 \\ &= \frac{1}{d^2} \left(d\Big(\sum_{j=1}^{d} t_i\Big)^2 + \Big(d^2 \sum_{j=1}^{d} t_i^2\Big) - 2d\Big(\sum_{i=1}^{d} t_i\Big)^2 \right) \\ &= \frac{1}{d} \left(\Big(d \sum_{i=1}^{d} t_i^2\Big) - \Big(\sum_{i=1}^{d} t_i\Big)^2 \right). \end{aligned}$$

Hence

$$(t+1)^2(t-1)^2 s^2 = \Big(\sum_{i=1}^{d} t_i\Big)^2 \leq d \sum_{i=1}^{d} t_i^2 = d(t+1)(t-1)(s+t).$$

Dividing by $(t+1)(t-1)$ (recall $t > 1$ and $s > 1$) and substituting $d = |V|$ from (8.16), this inequality boils down to

$$t(s-1)(s^2 - t) \geq 0$$

as needed.

9 Strongly regular graphs

9.1 Some review of linear algebra

We need some basic facts from linear algebra. Let I denote the $n \times n$ unit matrix, and let J denote the $n \times n$ all one matrix. For an $n \times n$ matrix A, let ${}_iA_j$ denote the j^{th} entry in the i^{th} row of A. Let the *trace* of A be $\mathrm{Tr}(A) = \sum_i {}_i[A]_i$, i.e., the sum of the entries on the main diagonal. We use A^T to denote the transpose of the matrix A, so A is *symmetric* if and only if $A = A^T$. We use overline for conjugation of complex numbers, so a matrix A is real if and only if $A = \overline{A}$. We use that $(AB)^T = B^T A^T$, the transpose of a number is itself, and that matrix multiplication is associative without further explanation.
Recall that *eigenvalues* of an $n \times n$ complex matrix A are numbers λ, such that $\det(A - \lambda I) = 0$. Observe that λ is an eigenvalue of A if and only if there is an $\mathbf{z} \neq \mathbf{0}$ vector with $A\mathbf{z} = \lambda\mathbf{z}$. (In this case we say that $\mathbf{z}$ is an *eigenvector* corresponding to the eigenvalue λ.) Indeed, $\det(A - \lambda I) = 0$ if and only if the matrix $A - \lambda I$ has rank less than n over $\mathbb{C}$ if and only if the system of homogeneous linear equations $(A - \lambda I)\mathbf{z} = \mathbf{0}$ has a non-trivial solution. We need the following well-known facts:

Theorem 11 *Assume that A is a symmetric real $n \times n$ matrix.*
(i) The polynomial $\det(A - \lambda I)$ has degree n and has n real roots, $\lambda_1, \lambda_2, ..., \lambda_n$, with possible repetition.
(ii) There exists unit length real eigenvectors $\mathbf{x}_i$ corresponding to the eigenvalue λ_i, which are orthogonal to each other.
(iii) There exists an $n \times n$ matrix M, such that $M^{-1} = M^T$ and $M^T A M = D$, where D is the diagonal matrix with entries $\lambda_1, \lambda_2, ..., \lambda_n$.
(iv) $Tr(A) = \sum_i \lambda_i$.

Proof. (i) Expanding the determinant into $n!$ terms gives a polynomial with leading term into linear factors, with complex roots $\lambda_1, \lambda_2, ..., \lambda_n$, with possible repetition. We only have to show that these roots are real. Let λ be an eigenvalue of A with a corresponding $\mathbf{z}$ eigenvector. We have

$$\begin{aligned} A\mathbf{z} &= \lambda\mathbf{z}, \quad \text{multiplying (9.17) with } \overline{\mathbf{z}}^T \text{ from the left} && (9.17)\\ \overline{\mathbf{z}}^T A\mathbf{z} &= \overline{\mathbf{z}}^T \lambda\mathbf{z} = \lambda\overline{\mathbf{z}}^T\mathbf{z}, \quad \text{conjugating (9.17)} && (9.18)\\ A\overline{\mathbf{z}} &= \overline{A}\overline{\mathbf{z}} = \overline{\lambda}\overline{\mathbf{z}}, \quad \text{multiplying (9.19) with } \overline{\mathbf{z}}^T \text{ from the left} && (9.19)\\ \mathbf{z}^T A\overline{\mathbf{z}} &= \mathbf{z}^T\overline{\lambda}\overline{\mathbf{z}} = \overline{\lambda}\mathbf{z}^T\overline{\mathbf{z}}. && (9.20) \end{aligned}$$

Observe that $\mathbf{z}^T\overline{\mathbf{z}}$ is a non-zero real number, as $\mathbf{z} \neq \mathbf{0}$. Finally,

$$\overline{\lambda}\mathbf{z}^T\overline{\mathbf{z}} =^{(9.20)} \mathbf{z}^T A\overline{\mathbf{z}} = (\overline{\mathbf{z}}^T A\mathbf{z})^T =^{(9.18)} (\lambda\overline{\mathbf{z}}^T\mathbf{z})^T = \lambda\mathbf{z}^T\overline{\mathbf{z}}.$$

Dividing through by $\mathbf{z}^T\overline{\mathbf{z}}$ we obtain that $\overline{\lambda} = \lambda$, i.e., λ is real.
(ii) Assume that $\lambda_i \neq \lambda_j$, with corresponding eigenvectors $\mathbf{x}_i, \mathbf{x}_j$. We show that the eigenvectors are orthogonal. Indeed,

$$\lambda_j(\mathbf{x}_i^T\mathbf{x}_j) = \mathbf{x}_i^T(\lambda_j\mathbf{x}_j) = \mathbf{x}_i^T(A\mathbf{x}_j) = (\mathbf{x}_i^T A)\mathbf{x}_j = (A\mathbf{x}_i)^T\mathbf{x}_j = (\lambda_i\mathbf{x}_i)^T\mathbf{x}_j = \lambda_i\mathbf{x}_i^T\mathbf{x}_j.$$

If $\mathbf{x}_i^T \mathbf{x}_j \neq 0$, then $\lambda_i = \lambda_j$, a contradiction. Finally, normalize every $\mathbf{x}_i$ to make it a unit vector.

If A has eigenvalues with multiplicities, we can use a general position argument. We need some tools. (α) Roots of a complex polynomial depend continuously on the coefficients (intuitively obvious, but not trivial). (β) For polynomials $f(z) = a_0 z^d + a_1 z^{d-1} + \cdots + a_d$ with $a_0 \neq 0$ and $g(z) = b_0 z^e + b_1 z^{e-1} + \cdots + b_e$ with $b_0 \neq 0$ in $\mathbb{C}[z]$, there is a multivariate polynomial $\mathrm{Res}(f,g) = \mathrm{Res}(a_0, a_1, ..., a_d; b_0, b_1, ..., b_e)$, called the *resultant*, such that the resultant is the zero polynomial if and only if f and g share at least one root. Take this without proof. To be more concrete, $\mathrm{Res}(f,g)$ is the following $(d+e) \times (d+e)$ determinant:

$$\mathrm{Res}(f,g) = \det \underbrace{\begin{pmatrix} a_0 & \cdots & a_d & \cdots & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \cdots & a_0 & \cdots & a_d \\ b_0 & \cdots & b_e & \cdots & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \cdots & b_0 & \cdots & b_e \end{pmatrix}}_{d+e} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \\ a \end{matrix}}\right\} e \\ \\ \left.\vphantom{\begin{matrix} a \\ a \\ a \\ a \\ a \end{matrix}}\right\} d \end{matrix}$$

In words, in the first row $a_0, a_1, ..., a_d$ is extended with $e-1$ zeros, and this row is cyclically shifted until a_d hits the right side in the e^{th} row. Then $b_0, b_1, ..., b_e$ is extended with $d-1$ zeros, and this row is cyclically shifted until b_e hits the right side in the $(e+d)^{th}$ row.

(γ) $f(z) \in \mathbb{C}[z]$ has multiple roots if and only if $\mathrm{Res}(f, f')$ is identically zero. ($\mathrm{Res}(f, f')$ is called the *discriminant* of f.)

Assume that we have a B_m symmetric matrix with entries at most $1/m$ in absolute value, such that $A + B_m$ has n distinct eigenvalues, $\lambda_i^{(m)}$, corresponding to orthogonal unit eigenvectors $\mathbf{x}_i^{(m)}$. Let $m \to \infty$. Based on (α), select a $\lambda_i^{(m)}$ subsequence (for convenience, still superscripted with m) such that for every i, $\lambda_i^{(m)} \to \lambda_i$ as $m \to \infty$. Now the $\mathbf{x}_i^{(m)}$ sequences live in a sphere, a bounded closed set, therefore a subsequence of them converges for every i. By continuity argument, the limits are pairwise orthogonal unit eigenvectors of A, corresponding to its eigenvalues.

But why do we have such B_m matrices? For $1 \leq i \leq j \leq n$, consider arbitrary b_{ij} numbers in $-1/m < b_{ij} < 1/m$ and extend the definition for $1 \leq j < i \leq n$ by $b_{ji} = b_{ij}$. Compose the symmetric B_m matrix from the b_{ij} entries. Consider the polynomial $\chi(\lambda) = \det(A + B_m - \lambda I)$, in which the coefficients are numbers that depend on the b_{ij} and a_{ij} numbers. By (γ), $A + B_m$ has repeated eigenvalues if and only if $\mathrm{Res}(\chi, \chi')$ is zero. Considering now $\mathrm{Res}(\chi, \chi')$ as a multivariate polynomial with the b_{ij} variables, while the a_{ij} are still fixed numbers, this multivariate polynomial must be identically zero—not just in the small range! Consider now a D $n \times n$ diagonal matrix with n different numbers on the diagonal, say $c_1, c_2, ..., c_n$. Clearly $\chi_D(\lambda) = \det(D - \lambda I)$ has n different roots, and hence $\mathrm{Res}(\chi_D, \chi_D')$ is non-zero. But $\mathrm{Res}(\chi_D, \chi_D')$ can be obtained by assigning values to b_{ij} in the identically zero polynomial as $b_{ii} \leftarrow c_i - a_{ii}$ and for $i \neq j$, $b_{ij} = -a_{ij}$.

(iii) It is easy to see that $M = (\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_n)$ i.e., putting together the columns of the orthogonal unit eigenvectors from part (ii) suffices: $M^T M = I$ as the $\mathbf{x}_i$ vectors are orthogonal unit vectors, $AM = (\lambda_1 \mathbf{x}_1, \lambda_2 \mathbf{x}_2, ..., \lambda_n \mathbf{x}_n)$ and $M^T A M = D$.

(iv) First observe that for any $n \times n$ matrices A, B, we have $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$. Indeed, both traces

are equal to $\sum_i \sum_j ({}_iA_j) \cdot ({}_jB_i)$. Next, $\mathrm{Tr}(A) = \mathrm{Tr}(M^{-1}DM) = \mathrm{Tr}(MM^{-1}D) = \mathrm{Tr}(D) = \sum_i \lambda_i$.

9.2 Definition of strongly regular graphs

A *strongly regular graph* with parameters (n, k, λ, μ) is k-regular simple graph on n vertices, such that any two neighbors share exactly λ common neighbors and any two non-neighbors share exactly μ common neighbors. This is a very strong requirement, which implies numerous restrictions on the parameters. For example, the identity

$$k(k - \lambda - 1) = \mu(n - k - 1) \tag{9.21}$$

holds. Indeed, fix a vertex v, its neighbors $N(v)$ and non-neighbors $V(G)\setminus(N(v)\cup\{v\})$. $|N(v)| = k$ and $|V(G) \setminus (N(v) \cup \{v\})| = n - k - 1$. On the one hand, the number of edges between neighbors and non-neighbors is $\mu(n-k-1)$. On the other hand, count them in a different way: each $u \in N(v)$ has k neighbors. One of them is v, and exactly λ of them is in $N(v)$. All others, namely $k - 1 - \lambda$ edges from u go to non-neighbors of v.

Another example, the complement of a strongly regular graph is also strongly regular, and it has parameters $(n, n - k - 1, n - 2k + \mu - 2, n - 2k + \lambda)$ (Homework problem).

A strongly regular graph is disconnected if and only if it is not a complete graph and $\mu = 0$, i.e., disjoint union of at least two copies $K_{\lambda+1}$'s. The complements of the graphs just mentioned, are the edgless graph, and complete multipartite graphs with equal class sizes. These are considered *trivial* strongly regular graphs and are often excluded from the class of strongly regular graphs.

For a simple graph G on $V(G) = \{1, 2, ..., n\}$, the *adjacency matrix* $A = A(G)$ of G is defined by

$${}_i[A]_j = \begin{cases} 0 & \text{if } i = j, \\ 1 & \text{if } i \neq j,\ \{i, j\} \in E(G), \\ 0 & \text{if } i \neq j,\ \{i, j\} \notin E(G). \end{cases}$$

For the adjacency matrix A of a graph G of order n, the equation

$$AJ = JA = kJ \tag{9.22}$$

is equivalent to the fact that G is a k-regular graphs. For the adjacency matrix of the strongly regular graph G with parameters (n, k, λ, μ), the following matrix identity holds:

Based on case analysis for the i, j entry of the matrix, we show the matrix identity

$$A^2 - (\mu - \lambda)A + (\mu - k)I = \mu J. \tag{9.23}$$

We check the identity in 3 cases for 3 different kind of entries: (i, i) diagonal entries show $k + 0 + (\mu - k) = \mu$; $i \neq j$, $\{i, j\} \in E(G)$ entries show $\lambda + (\mu - \lambda) + 0 = \mu$; and $i \neq j$, $\{i, j\} \notin E(G)$ entries show $\mu + 0 + 0 = \mu$. It is easy to see that identities (9.22) and (9.23) together imply that G is strongly regular with parameters (n, k, λ, μ). From numerical coefficents in (9.23) we can figure out the parameters: first read μ on the right hand side, then figure out k and λ from the coefficients of A and I.

9.3 Spectrum of strongly regular graphs

Eigenvalues and eigenvectors of graphs refer to eigenvalues and eigenvectors of their adjacency matrices. As the adjacency matrix is a real symmetric matrix, graphs of order n have n real eigenvalues, possibly with multiplicities. The following Claim is among the homework problems:
Claim. For a k-regular graph G, k is its largest eigenvalue, and if the graph is connected, this eigenvalue has multiplicity one. The all 1 vector is its eigenvector.

Theorem 12 *For a connected strongly regular graph G with parameters (n, k, λ, μ), where $n \geq 3$, there are 2 eigenvalues other than k, and they come with multiplicities*

$$\frac{1}{2}\left(n - 1 \pm \frac{(n-1)(\mu-\lambda) - 2k}{\sqrt{(\mu-\lambda)^2 + 4(k-\mu)}}\right).$$

Proof. Let $A = A(G)$ be the adjacency matrix of this graph. Our analysis is based on (9.23). We already know that k is an eigenvalue of A with eigenvector $(1, 1, ..., 1)^T$ and k has multiplicity one as G is connected. Assume that θ is a further eigenvalue of A with eigenvector $\mathbf{u}$. Apply both sides of (9.23) to $\mathbf{u}$. Note that $(1, 1, ..., 1)^T\mathbf{u} = 0$ (as they are eigenvectors belonging to different eigenvalues), and therefore $J\mathbf{u} = \mathbf{0}$. We conclude

$$\Big(\theta^2 - (\mu-\lambda)\theta + (\mu-k)\Big)\mathbf{u} = \mathbf{0}.$$

Hence $\theta^2 - (\mu-\lambda)\theta + (\mu-k) = 0$, and by the quadratic formula, the eigenvalues are

$$\theta_{1,2} = \frac{1}{2}\left(\lambda - \mu \pm \sqrt{(\lambda-\mu)^2 + 4(k-\mu)}\right).$$

Note that $r_1 \neq r_2$. Let us list all eigenvalues of A: k has multiplicity 1, θ_1 with multiplicity m_1 and θ_2 with multiplicity m_2. We have a system of two linear equations in variables m_1, m_2:

$$\begin{aligned} n &= 1 + m_1 + m_2 \\ 0 &= k + m_1\theta_1 + m_2\theta_2, \end{aligned}$$

where the first equation counts the eigenvalues, while the second uses that $0 = \mathrm{Tr}(A) =$ sum of eigenvalues. Solving this system of equations yields the theorem.
A comment.
Observe that if m_1 and m_2 integers are not equal, then $\sqrt{(\lambda-\mu)^2 + 4(k-\mu)}$ is integer, which implies that the eigenvalues θ_1 and θ_2 are also integers, as $\lambda - \mu$ and $\sqrt{(\lambda-\mu)^2 + 4(k-\mu)}$ must have the same parity.

We have already seen an example of a strongly regular graph: the collinearity graph of $GQ(s, t)$ (after deleting the loops) is a strongly regular graphs with parameters

$$\Big((st+1)(s+1), s(t+1), s-1, t+1\Big).$$

This is connected for $s > 1$.

Theorem 13 *If a generalized quadrangle $G(s,t)$ exists, then*

$$s+t \Big| s^2(st+1) \quad \textit{and} \quad s+t \Big| st(s+1)(t+1).$$

If $s = 1$ or $t = 1$, then the divisibilities always hold. For $s > 1, t > 1$, the multiplicities in Thdorem 12 for the strongly regular collinearity graph boil down to $\frac{s^2(st+1)}{s+t}$ and $\frac{st(s+1)(t+1)}{s+t}$.

9.4 The Friendship Graph

The *Friendship Graph* is defined in the following way: a finite graph, in which any two different vertices have a single common neighbor.

Theorem 14 [Friendship Theorem] *In the Friendship Graph, there is a vertex, which is connected to every other vertex. For $n \geq 3$, a Friendship Graph exists only on odd number of vertices, and it consists of a few triangles, such that one vertex of each triangle is merged into a single vertex (see Fig. 8).*

The meat of the theorem is the existence of the vertex, which is connected to every other vertex, from which the other claims easily follow. The first part of proving the Friendship Theorem is that if there is no such vertex, then the graph is regular. In that case it would be strongly regular, and based on what we already know about strongly regular graphs, such strongly regular graph does not exist on more than 3 vertices.

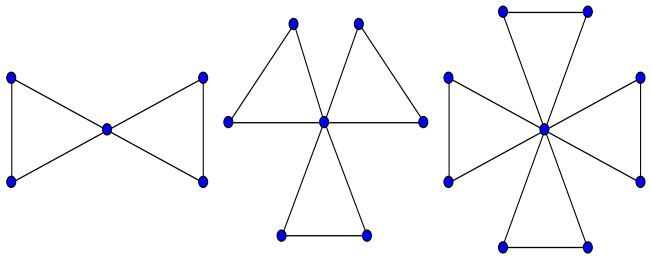

Figure 8: Friendship Graphs. From Wikipedia.

Assume that $n \geq 4$ and a Friendship Graph has no vertex joined to every other vertices. Consider two vertices, u and v, not joined by an edge. We are going to prove that $d(u) = d(v)$. Let f be unique common neighbor of u and v, and let u have further neighbors $w_1, ..., w_\ell$. Each w_i has a common neighbor z_i with v, and those z_i vertices are distinct. Otherwise $z_a = z_b$ and u would have two common neighbors. Hence $d(u) \leq d(v)$, without any assumption distinguishing u from v, hence $d(u) = d(v)$. Furthermore, any vertex not joined to *both* u and v must have the same degree. Only vertex f may have a different degree. If there is a vertex z, such that f is not joined to z, then $d(f) = d(z) = d(u)$.

So if the Friendship Theorem fails, then there is a strongly regular graph with parameters $(n, k, 1, 1)$. We can use Theorem 12, as the Friendship Graph is connected. The fraction in the multiplicities of eigenvalues boils down to $\frac{k}{\sqrt{k-1}}$, which must be integer. Setting $a = \sqrt{k-1}$, $k = a^2 + 1$, and $\frac{k}{\sqrt{k-1}} = a + \frac{1}{a}$, which implies $a = 1$, $k = 2$. As 2-regular graphs are union of disjoint cycles, the only possible regular Friendship Graph is K_3, which has a vertex joined to all other vertices.

9.5 Paley graph

Given an odd prime p, define the $\chi(x)$ function on residue class x with zero in $x = 0$, 1 on quadratic residues and -1 on quadratic non-residues. $\chi(x)$ is a multiplicative function, i.e., for all x, y we have $\chi(xy) = \chi(x)\chi(y)$. $\sum_x \chi(x) = 0$, where the summation goes for residue classes. Observe the following identity for any odd prime p and any c non-zero residue class mod p :

$$\sum_{\substack{x \\ \text{residue class}}} \chi(x)\chi(x+c) = \sum_{\substack{x\neq 0 \\ \text{residue class}}} \chi(x)\chi(x+c) = \sum_{\substack{x\neq 0 \\ \text{residue class}}} \chi^2(x)\chi(1+cx^{-1})$$

$$= \sum_{\substack{x\neq 0 \\ \text{residue class}}} \chi(1+cx^{-1}) = \sum_{\substack{y\neq 0 \\ \text{residue class}}} \chi(1+y) = -\chi(1) = -1. \tag{9.24}$$

Assume now that the prime p has the form $4k + 1$. Then, by Euler's Lemma, -1 is a quadratic residue mod p. Define the *Paley graph* in the following way: vertices are the residue classes mod $p = 4k+1$, and two different residue classes, x and y, are joined by an edge, if $x - y$ is a quadratic residue mod p. This is a graph, as $x - y$ is a quadratic residue if and only if $y - x$ is a quadratic residue, as -1 is a quadratic residue, and product of quadratic residues is a quadratic residue.

The Paley graph is a $\frac{p-1}{2}$-regular graph, as exactly half of the non-zero residue classes is quadratic residue.

Based on the above, if the rows and columns of a Q matrix are indexed with the residue classes $1, 2, ..., p$, and ${}_i[Q]_j = \chi(i - j)$, then

$$Q^2 = pI - J \quad \text{and} \quad QJ = JQ = \text{all zero matrix}. \tag{9.25}$$

We have

$$AJ = JA = \frac{p-1}{2}J \tag{9.26}$$

as the Paley graph was $\frac{p-1}{2}$-regular. It is easy to see that the adjacency matrix A of the Paley graph is $A = \frac{1}{2}(Q + J) - \frac{1}{2}I$. Based on this,

$$Q^2 = (2A - J + I)^2 = 4A^2 + J^2 + I - 4AJ - 2J + 4A = 4A^2 + 4A + I - (p-1)J,$$

combined with (9.25) yields

$$A^2 + A + \frac{1-p}{4}I = \frac{p-1}{4}J. \tag{9.27}$$

Combining (9.26) and (9.27), the comments after (9.23) show that

Theorem 15 *For a $p = 4k+1$ prime, the Paley graph is strongly regular with parameters $(p, \frac{p-1}{2}, \frac{p-5}{4}, \frac{p-1}{4})$.*

For $p = 5$, the Paley graph is C_5. The Paley graph construction generalizes to make a strongly regular graph with vertex set $GF(q)$, where q is a prime power of the form $4k+1$.

10 Bipartite graphs of girth eight

We will find useful the following matrix inequality of Atkinson, Watterson, and Moran (1960), which, like the theorem after it, was originally developed to estimate allele distributions in future generations. Let $\sigma(B)$ denote the sum of all entries of the matrix B.

Theorem 16 *Let A denote an $m \times n$ matrix of non-negative entries. We have*

$$mn\sigma(AA^TA) \geq \sigma(A)^3.$$

Mulholland and Smith (1959), Blakley and Roy (1965) proved

Theorem 17 *For a symmetric $n \times n$ matrix A with non-negative entries*

$$n^{k-1}\sigma(A^k) \geq \sigma(A)^k.$$

Sidorenko (1991) found a common generalization of the previous two theorems:

Theorem 18 *Let A denote an $m \times n$ matrix of non-negative entries. Then*

$$m^{\lfloor \frac{k}{2} \rfloor} n^{\lfloor \frac{k-1}{2} \rfloor} \sigma(\underbrace{AA^TAA^T....}_{k \text{ factors}}) \geq \sigma(A)^k.$$

Assume now that G is a bipartite graph of girth 8—in other words, it has no C_4's and C_6's. Let the sizes of the partite classes be m and n, and let the number of edges be e. Let P_3 denote the number of *paths* of 3 edges and 4 vertices in G. (Recall that paths are not allowed to repeat edges or vertices. A 3-path must have its endpoints in different partite sets.) Any pair of vertices can be the endpoints of at most one path in P_3 by the girth condition. Hence

$$P_3 \leq mn - e.$$

An easy count shows that

$$P_3 = \sum_{xy \in E(G)} (d(x)-1)(d(y)-1),$$

where $d(x)$ denotes the degree of vertex x. Expanding further

$$P_3 = e + \sum_{xy \in E(G)} d(x)d(y) - \sum_{xy \in E(G)} \Big(d(x)+d(y)\Big) = e + \sum_{xy \in E(G)} d(x)d(y) - \sum_{x \in V(G)} d^2(x).$$

Let A denote the bipartite incidence matrix of the graph G. In other words, its rows and columns are indexed by the elements of the partite classes and ${}_xA_y = 1$ if $xy \in E(G)$, otherwise zero. Clearly

$$\sum_{xy \in E(G)} d(x)d(y) = \sigma(AA^TA).$$

Hence

$$\begin{aligned} \frac{e^3}{mn} &= \frac{\sigma(A)^3}{mn} \le \sigma(AA^TA) = \sum_{xy \in E(G)} d(x)d(y) \\ &= \#P_3 - e + \sum_{x \in V(G)} d^2(x) \le mn - 2e + \sum_{x \in V(G)} d^2(x). \end{aligned}$$

If $\sum_{x \in V(G)} d^2(x) = O(mn)$, we would get $e = O((nm)^{2/3})$. This could be obtained under two alternative conditions (see homework problems):

Theorem 19 *If the bipartite graph G has girth at least 8, and*
(a) every vertex has degree at least 2, or
(b) $n = O(m^2)$ and $m = O(n^2)$,
then $e = O((nm)^{2/3})$.

This leaves an interesting open problem when a bipartite graph of girth 8 can have $\Omega((nm)^{2/3})$ edges. If there is a generalized quadrangle with m points and n lines, this is the case. Take for the bipartite graph the incidence bipartite graph of the generalized quadrangle. Indeed, if $(s,t) = (q,q)$, then $(m,n,e) \approx (q^3, q^3, q^4)$, $m = n$, $e = \Theta((mn)^{2/3})$;
$(s,t) = (q^2, q^3)$, then $(m,n,e) \approx (q^7, q^8, q^{10})$, $m = \Theta(n^{7/8})$, $e = \Theta((mn)^{2/3})$;
$(s,t) = (q, q^2)$, then $(m,n,e) \approx (q^4, q^5, q^6)$, $m = \Theta(n^{4/5})$, $e = \Theta((mn)^{2/3})$.
Also, if $n = \binom{m}{2}$, we can put a tree with $\Theta(m^2)$ edges between the n, m elements in the two classes, and not have any cycle. Note $(nm)^{2/3} = \Theta(m^2)$, $m = \Theta(n^{1/2})$, $e = \Theta((mn)^{2/3})$.

There is a range of n, m, however, when we cannot have $\Theta((mn)^{2/3})$ edges in a bipartite graph of girth at least 8. Recall the Ruzsa-Szemerédi Theorem in the following positive form:

Theorem 20 *There is a function $h(m) \to \infty$, such that if we have b triplets on m vertices. such that triplets intersect in at most one vertex and there is no 3-cycle of triplets, then $b \le m^2/h(m)$.*

Theorem 21 *Assume that the $G = G(n,m)$ bipartite graph has girth at least 8. Assume that n and m satisfy the following two inequalities:*
(i) $\frac{m^2}{h(m)^{3/2}} = o(n)$; and
(ii) $n = O\Big(\frac{m^2}{h(m)}\Big)$.
Then $e(G) = o\Big((mn)^{2/3})\Big)$.

As $h(m) \to \infty$, there is a range of n numbers such that

$$\frac{m^2}{h(m)^{3/2}} << n < \frac{m^2}{h(m)}.$$

We are talking about such $n = n(m)$ values. For each vertex v in the n-side of G, group the vertices incident to v into triplets in the m-side, with at most two neighbors left out for every v. So $e(G) \le 2n+3b$, if we created b triples. As the graph has no 4 and 6-cycles, the Ruzsa-Szemerédi Theorem applies for the triplets and

$$b \le \frac{m^2}{h(m)}.$$

By assumption (ii),

$$n = O\Big(\frac{m^2}{h(m)}\Big).$$

Summing up

$$e(G) = O\Big(\frac{m^2}{h(m)}\Big). \tag{10.28}$$

On the other hand, multiplying (i) by m,

$$\frac{m^3}{h(m)^{3/2}} = o(nm),$$

and raising to 2/3 power,

$$\frac{m^2}{h(m)} = o\Big((nm)^{2/3}\Big). \tag{10.29}$$

Combining (10.28) with (10.29) gives the theorem.

11 Graphs without $K_{t,t}$

C_4-free graphs (see Theorem 9) also can be thought of as $K_{2,2}$-free graphs. Therefore Reiman's Theorem can be generalized in the direction "how many edges a graph on n vertices can have if it has no $K_{t,t}$". The proof uses Jensen's Inequality for modified binomial coefficients, as in Section 7.

Theorem 22 (Kővári-Sós-Turán) *Assume that for some t with $2 \le t \le n$, the n-vertex graph G has no $K_{t,t}$. Then $e(G) = O\Big(n^{2-\frac{1}{t}}\Big)$, where the constant in the $O(.)$-term is absolute, does not depend on n or t.*

First note that for $2 \le t \le n$, $t = O(n^{1-\frac{1}{t}})$ in $[2, n]$. Indeed, the t-derivative $(tn^{\frac{1}{t}})' = n^{1/t} - \frac{\log n}{t} n^{1/t}$ is positive in the interval $(\log n, n]$, therefore the function $tn^{\frac{1}{t}}$ is increasing there. However, in the right endpoint $t = n$, the function is $n^{1+\frac{1}{n}} = O(n)$. For $2 \le t \le \log n$, we have $tn^{\frac{1}{t}} \le n^{1/2} \log n = O(n)$. Therefore, $tn^{\frac{1}{t}} = O(n)$ and $t = O(n^{1-\frac{1}{t}})$ in $[2, n]$. To repeat the arguments in (7.14), count in G stars with t leaves in two ways, to obtain

$$n\binom{\frac{2e}{n}}{t}^+ \le n\binom{\frac{1}{n}\sum_{x\in V(G)} d(x)}{t}^+ \le \sum_{x\in V(G)} \binom{d(x)}{t}^+ \le \sum_{x\in V(G)} \binom{d(x)}{t} \le (t-1)\binom{n}{t}. \tag{11.30}$$

Either $\frac{2e}{n} \le 4t$ or $\frac{2e}{n} \ge 4t$. In the first case $e \le 2nt = O(n^{2-\frac{1}{t}})$, as required.

In the second case, (11.30) gives

$$n\frac{(\frac{2e}{n}-t)^t}{t!} \le n\binom{\frac{2e}{n}}{t} = n\left(\frac{\frac{2e}{n}}{t}\right)^+ \le (t-1)\binom{n}{t} \le (t-1)\frac{n^t}{t!},$$

which is, by algebra, equivalent to

$$2e \le (t-1)^{\frac{1}{t}} n^{2-\frac{1}{t}} + nt,$$

and nt should be estimated like in the first case.

For $t = 2$ and 3 the Kővári-Sós-Turán theorem is tight, and it is conjectured to be tight for any t as $n \to \infty$. Section 7 verified it for $t = 2$. We outline Brown's construction for $t = 3$ and leave the details to Problem 15. Consider the unit distance graph in $\mathbb{R}^3$: vertices are the points, edges are pairs of points at unit distance apart. This graph is $K_{3,3}$-free. Indeed, if x, y, z are 3 vertices, the common neighbors of x and y live in the intersection of two unit spheres, i.e. in a circle. Similary do the the common neighbors of x and z, and the two circles cannot be the same. All common neighbors of x, y and z are in the intersection of the circles, which has at most 2 points. The discrete analogue is the following. Take for V the affine 3-space over $GF(p)$, where p is an odd prime, and take for α a quadratic residue, if $p = 4k + 3$, and take for α a quadratic non-residue, if $p = 4k + 1$. So $V = \{(x, y, z) : x, y, z \in GF(p)\}$, and join (x, y, z) and (a, b, c) with an edge, if $(a - x)^2 + (b - y)^2 + (c - z)^2 = \alpha$. The formula $(a - x)^2 + (b - y)^2 + (c - z)^2$ is being used as substitute of distance working in affine spaces over an arbitrary field.

Theorem 22 can be extended for graphs not containing $K_{s,t}$ for some $2 \le t \le s \le n$ with $e = O\left(s^{\frac{1}{t}} n^{2-\frac{1}{t}}\right)$ (see homework problems). For fixed s and t, as $n \to \infty$, this bound is just $e = O\left(n^{2-\frac{1}{t}}\right)$. Kollár, Rónyai and Szabó constructed $K_{s,t}$-free graphs with that many edges for arbitrary fixed $t \ge 2$ and $s \ge t! + 1$.

12 Forbidden even cycles

Erdős noted that forbidding odd cycles does not have serious effect on the number of edges of a graph. This observation was one of the earliest uses of the probabilistic method.

Claim 2 *From any graph G, one can delete at most half of the number of edges and obtain a bipartite graph.*

Set two boxes, A and B, and toss a fair coin independently for every vertex. For a Head, put the vertex in A, for a Tail, put the vertex in B. Make a bipartite graph by keeping only those edges whose endpoints are in different boxes. For every edge f, the probability that its endpoints end up in different boxes is 1/2. By the linearity of expectation, the expected number of edges between A and B is $\frac{1}{2}e(G)$. There must be an outcome of the random process that has at least as many edges between A and B as the expectation.

Erdős and Simonovits in the 1960's proved the following:

Theorem 23 *If G has n vertices and has no C_{2k} cycle for some $k \geq 2$, then*

$$e \leq c_k n^{1+\frac{1}{k}}.$$

We prove a weaker version of this theorem:

Theorem 24 *If G has n vertices and has no cycles of length up to $2k$ for some $k \geq 2$, then*

$$e < n^{1+\frac{1}{k}} + n.$$

Define the *density* $\rho(H)$ for a (simple) graph H with at least one vertex as $\frac{|E(H)|}{|V(H)|}$. Let G' be the subgraph of G with at least one vertex that has the maximum density among those subgraphs. As G itself is in the domain of maximization, $\rho(G') \geq \rho(G)$. We claim that all vertices in G' have at least $\rho(G')$ neighbors in G'. Simple calculation shows that the removal of a vertex with fewer neighbors would increase the density, and G' must have more than one vertex if G had any edge at all. Assume that G has at least $n^{1+\frac{1}{k}} + n$ edges. Then $\rho(G') \geq \rho(G) \geq n^{\frac{1}{k}} + 1$, and every vertex of G' has at least $n^{\frac{1}{k}} + 1$ neighbors in G'. To reach a contradiction, we show that G' has more than n vertices. Namely starting at any vertex u of G', we build a tree in G' by adding $n^{\frac{1}{k}}$ neighbors of u, then adding $n^{\frac{1}{k}}$ neighbors to each neighbor, etc., in k steps. There is no overlapping among the vertices of the tree, as G had no cycles up to $2k$. On the other hand, in the k^{th} step we generated $n = (n^{\frac{1}{k}})^k$ vertices, in addition to those generated in earlier steps.

Note that Theorem 24 is even easier to prove in the form $e = O(n^{1+\frac{1}{k}})$ if G is d-regular. Indeed, like in the proof of Theorem 19,

$$\binom{n}{2} - e(G) \geq \#k\text{-paths} = \#k\text{-walks} - \#\text{non-path } k\text{-walks}. \tag{12.31}$$

The number of k-walks is at least $\frac{1}{2}nd^k$ (not equal because of closed walks), and the number of non-path k-walks is at most nkd^{k-1}, as they must take a step backward somewhere on the recently used edge. The inequality

$$\frac{n^2}{2} \geq nd^k(\frac{1}{2} - \frac{k}{d})$$

implies the claim. Indeed, if $\frac{k}{d} \leq \frac{1}{4}$, then $\frac{n^2}{2} \geq \frac{1}{4}nd^k$, and $2n^{k+1} \geq n^k d^k = \big(2e(G)\big)^k$. If $\frac{k}{d} \geq \frac{1}{4}$, then $4k \geq d$ and $4kn \geq dn = 2e(G)$.

If we drop the assumption of regularity, formula (12.31) still holds. Denote the average degree by $\bar{d}$, and the adjacency matrix with A, by Theorem 17,

$$2\#k\text{-walks} \geq \sigma(A^k) \geq \frac{\sigma(A)^k}{n^{k-1}} = \frac{(n\bar{d})^k}{n^{k-1}} = n(\bar{d})^k.$$

However, estimating the number of non-path k-walks can be a pain, like in Theorem 19.

13 Generalized polygons

Generalized polygons, introduced by Jacques Tits, make a common generalization of finite projective planes and generalized quadrangles.
Let us be given positive integers s, t and an $n \geq 3$. An incidence structure of finite sets of points and lines make a finite *generalized polygon* (more precisely, *generalized n-gon of (s,t) type*), $GP_n(s,t)$, if they satisfy the following axioms:
(GP1) Every line has exactly $s+1$ points
(GP2) Every point is on exactly $t+1$ lines
(GP3) Any two lines intersect in at most one point
(GP4) The girth of the incidence bipartite graph of points and lines is exactly twice the diameter n of the incidence bipartite graph of points and lines.
(Clearly in any graph of even girth, the girth is at most twice the diameter. Forests have inifinite girth. The point above is *exactly* twice, which includes the statement that the incidence bipartite graph has a cycle.) The name generalized polygon (generalized n-gon) is explained as follows. Take the vertices of an n-gon for points, and the pairs of vertices on an edge for lines. Clearly $s = t = 1$ and (GP1-3) hold. The girth of the incidence bipartite graph is $2n$ and the diameter is n.

As there is at most one line through any two points in a $GP_n(s,t)$, switching the names of points and lines results in a *dual* generalized polygon $GP_n(t,s)$.

We prove that a finite projective plane of order q is a $GP_3(q,q)$. Indeed, (GP1) and (GP2) follow from the facts that in a finite projective plane of order q, points are incident to $q+1$ lines and lines are incident to $q+1$ points. (See homework problem F3).) (GP3) follows from (P1). To prove (GP4), we show that the girth of the incidence bipartite graph is 6 and the diameter of the incidence bipartite graph is 3. In the incidence bipartite graph of the finite projective plane we never find any odd cycle, there are no C_4's, but there are C_6's, i.e., any 3 non-collinear points together with the 3 lines they determine a C_6 in the incidence bipartite graph. Hence the girth is 6. The diameter is 3, as from point P to point Q we can go on a 2-edge path in the incidence bipartite graph (P, $L(PQ)$ line, Q) and from point P to line ℓ we can go on a 3-edge path (take an arbitrary $Q \in \ell$, and go on P, $L(PQ)$ line, Q, ℓ).

We show that a $GP_3(s,t)$ is either a finite projective plane of order $q = s = t$, or $s = t = 1$ and the incidence structure is a triangle consisting of 3 points and 3 lines. Recall that in $GP_3(s,t)$, the diameter of the incidence bipartite graph is 3, while the girth of it is 6. Half of the statement of (P1) is provided by (GP3). If lines ℓ_1 and ℓ_2 of $GP_3(s,t)$ are not incident to a common point, then their distance in the incidence bipartite graph is at least 4, contradicting the assumption on the diameter. The same kind of distance argument shows, that points p_1, p_2 of $GP_3(s,t)$ must be incident to a common line. By (GP3), this line must be unique, and we have (P2). In Section 4 we listed the structures that satisfy axioms (P1) and (P2). Structures listed in (a) and (b) have diameter less than 3, with the exception of a single point and a single line, which are not incident. In this case the diameter is infinite. If (c1) holds, then we have a finite projective plane, and $s = t =$ the order of the finite projective plane. If (c2) holds, then by (GP2), we have $|L(p,q)| = |L(p,r)| = |L(r,q)| = s+1$, and as at most one of these 3 lines can have more than 2

points, $s = 1$ and $t = 1$.

The arguments above explain why the generalized 3-gon is also called a *generalized triangle*.

We prove that a generalized quadrangle $GQ(s,t)$ is an $GP_4(s,t)$. Indeed, in a $GQ(s,t)$ there are no 3 lines and 3 points making a triangle, as it would contradict axiom (GQ4). Hence there are no C_6's in the incidence bipartite graph. There are no C_4's in the incidence bipartite graph by axiom (GQ3). Hence, the girth of the incidence bipartite graph is at least 8. On the other hand, it is not more than 8, as there are C_8's in the incidence bipartite graph of $GQ(s,t)$. Take an arbitrary point Q and two distinct lines, ℓ_1, ℓ_2 passing through Q (by (GQ2) and t being a positive integer, $t+1 \geq 2$). Take $Q' \in \ell_2$, $Q' \neq Q$ (by $s+1 \geq 2$), and $\ell_3 \ni Q'$, $\ell_3 \neq \ell_2$, and a new point on P on ℓ_3 by a similar argument. By (GQ4), there is a (unique) line ℓ_4, such that $P \in \ell_4$ and ℓ_4 intersects ℓ_1 in some point. Now $\ell_1, \ell_2, \ell_3, \ell_4$ and the intersection points define a C_8 in the incidence bipartite graph. Therefore the girth is 8. Let us show that the diameter is 4. It suffices to show that the diameter is at most 4. To walk from a point P to a line ℓ not passing through P, take the unique line ℓ' passing through P and intersecting ℓ. Now P, ℓ', $\ell' \cap \ell$, ℓ is a 3-path in the incidence bipartite graph. To walk from a point P to a point Q, a 2-path suffices if P and Q are collinear. If not, take a line ℓ passing through Q, walk to ℓ as above, and use a 4^{th} edge to move from ℓ to Q.

Next we prove that a $GP_4(s,t)$ is a $GQ(s,t)$. Indeed, GQ(1-3) are literally the same as GP(1-3). Only (GQ4) has to be proved. Assume now a point p and a line ℓ not incident to p in $GP_4(s,t)$. They are non-adjacent vertices in different classes of the incidence bipartite graph, whose distance must be odd. As their distance is at most 4, their distance must be 3. This must be realized by an p, ℓ', q, ℓ sequence, in which consecutive terms are incident. This existence is exactly what (GQ4) requires. The uniqueness of this sequence follows from girth of the incidence bipartite graph being 8.

The arguments above explain why the generalized 4-gon is interchangeably called a *generalized quadrangle*.

There exist $GP_6(s,t)$, for $(s,t) = (q,q), (q^3,q), (q,q^3)$, for any prime power q. They are called *generalized hexagons*. We count the number of points and lines in $GP_6(s,t)$. Take an arbitrary point p. Let L_i (P_i) denote the set of lines (points), which are exactly at distance i from p in the incidence bipartite graph. Note that $L_i = \emptyset$ unless i is odd, and $P_i = \emptyset$ unless i is even, as we are in a bipartite graph, and $P_0 = \{p\}$. It follows from the girth assumption that

$$\begin{aligned}
|P_0| &= 1 \\
|L_1| &= |P_0|(t+1) = t+1 \\
|P_2| &= |L_1|s = (t+1)s \\
|L_3| &= |P_2|t = t(t+1)s \\
|P_4| &= |L_3|s = t(t+1)s^2 \\
|L_5| &= |P_4|t = t^2(t+1)s^2.
\end{aligned}$$

By the diameter assumption, for $i > 6$, $L_i = P_i = \emptyset$. So the last thing to figure out is $|P_6|$. Take any $\ell \in L_5$. By $s \geq 1$, $|\ell| \geq 2$. ℓ must have a point in P_4, but cannot have one in P_0 or P_2.

Furthermore, it cannot have two points in P_4 by the girth assumption. So we have a $q \in P_6$. We claim that q is incident to exactly $t+1$ lines of L_5. Indeed, q is incident to exactly $t+1$ lines, and those lines cannot be in L_1, L_3, and in L_i for any $i \geq 7$. Therefore $|P_6| = \frac{|L_5|s}{t+1} = t^2s^3$. Summing up the results,

$$\begin{aligned} |P| = |\cup_i P_i| &= \sum_{i=0,2,4,6} |P_i| = 1 + (t+1)s + t(t+1)s^2 + t^2s^3 = (s+1)(1+st+s^2t^2) \\ |L| = |\cup_i L_i| &= \sum_{i=1,3,5} |L_i| = (t+1) + (t+1)st + (t+1)s^2t^2 = (t+1)(1+st+s^2t^2). \end{aligned}$$

How to construct C_{2k}-free graphs with $\Omega(n^{1+\frac{1}{k}})$ edges? We can do it for $k = 2, 3, 5$. For other values of k such constructions are not known. For $k = 2$, the incidence bipartite graph of projective planes works, the incidence bipartite graph of a $GP_3(q, q)$ is free of C_4's and has about $2q^2$ vertices and q^3 edges. For $k = 3$, we discussed that the incidence bipartite graph of $GQ(q, q) = GP_4(q, q)$ is free of C_6's and has about $2q^3$ vertices and about q^4 edges. For $k = 5$, for any prime power q, there exists a generalized hexagon $GP_6(q, q)$, which has girth 12, and therefore is C_{10}-free. Using the calculation above, $|P| = |L| \sim q^5$, and the number of vertices in the incidence bipartite graph is $|P|+|L| \sim 2q^5$, while the number of edges in incidence bipartite graph is $(t+1)|P| = (s+1)|L| \sim q^6$.

Unfortunately, we do not get very far with this generalization, as the Feit-Higman theorem asserts that

Theorem 25 *If $GP_n(s, t)$ exists for $n \geq 3, s \geq 2, t \geq 2$, then $n \in \{3, 4, 6, 8\}$. Furthermore, if $n = 8$, then $s \neq t$.*

For simplicity, we disallowed in the discussion above the degenerate case $n = 2$, which is allowed in the literature by simultaneusly dropping the condition (GP3). Going this way would allow the structure $GP_2(s, t)$, in which each of $s+1$ points are incident to each of $t+1$ lines. The incidence bipartite graph of this structure is the complete bipartite graph $K_{s+1,t+1}$, which has diameter 2 and girth 4.

14 Hadamard matrices

An $n \times n$ *Hadamard matrix* has ± 1 entries and its rows are orthogonal. This is equivalent to the identity

$$HH^T = nI. \tag{14.32}$$

Transposing (14.32) shows that if H is an Hadamard matrix, then so is H^T. In other words, the columns of H are also orthogonal. Multiplying a row or a column of a Hadamard matrix with -1 leaves us with another Hadamard matrix. Two Hadamard matrices are considered *equivalent*, if one can be obtained from the other with a sequence of these kind of operations. An Hadamard matrix is *normalized*, if the entries in its first row and column are all 1's. Every Hadamard matrix is equivalent to a normalized Hadamard matrix. For example, $H_1 = 1$ and $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ are

Hadamard matrices. It is easy to see that if $n \geq 3$ and an $n \times n$ Hadamard matrix exists, then $4|n$. Indeed, without loss of generality we may assume that the Hadamard matrix of order n is normalized. Then, as the second row is orthogonal to the first, the second row must contain k of 1's and k of -1's. Let a be the number of 1's in the third row, which are located under one of the k 1's of the second row, let b be the number of -1's in the third row, which are located under one of the k 1's of the second row, let c be the number of 1's in the third row, which are located under one of the k -1's of the second row, and let d be the number of -1's in the third row, which are located under one of the k -1's of the second row. As the first and second rows are orthogonal,

$$a + b - c - d = 0,$$

as the first and third rows are orthogonal,

$$a - b + c - d = 0.$$

Summing up these two equations, we get $a = d$ and $b = c$. As the second and third rows are orthogonal,

$$a - b - c + d = 0,$$

and hence $a = b$. Finally, $n = a = b + c + d = 4a$. A long standing conjecture is that whenever you $4|n$, there exists an $n \times n$ Hadamard matrix. This conjecture has been proved for many families of multiples of n.

Hadamard's inequality claims that for an $n \times n$ real matrix A with entries a_{ij},

$$\det(A) \leq \prod_j \sqrt{\sum_i a_{ij}^2}. \tag{14.33}$$

If you are willing to believe that the determinant of a matrix is the signed volume of the parallelepiped determined by column vectors of the matrix, each vector going out from the origin, then it is clear that for vectors with given length, the volume is clearly maximized when the vectors are orthogonal.

Hadamard matrices satisfy Hadamard's inequality with *equality*, as $\prod_j \sqrt{\sum_i a_{ij}^2} = (\sqrt{n})^n$; and taking the determinant of the matrix equation (14.32), while using the product theorem of determinants, gives

$$\det(H)^2 = \det(H)\det(H^T) = \det(HH^T) = \det(nI) = n^n.$$

We are going to provide infinitely many constructions for Hadamard matrices. First, we define *tensor product of matrices*. Let $A = (a_{ij})$ be an $m \times n$, and B a $k \times \ell$ matrix. The tensor product $A \otimes B$ is the following $(mk) \times (n\ell)$ matrix, written for convenience in block form:

$$\begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}.$$

The following theorem is easy to see, and the proof is left as a homework problem:

Theorem 26 *Tensor product of Hadamard matrices is a Hadamard matrix.*

Starting with H_2, the theorem above provides a Hadamard matrix for every $n = 2^k$. Consider now a $p = 4k + 3$ prime. We construct a $(p + 1) \times (p + 1)$ Hadamard matrix, with a construction that is rather similar to the construction of the Paley graph. First observe that the calculation in (9.24) works for a $p = 4k+3$ prime as well. The matrix ${}_i[Q]_j = \chi(i-j)$ is no longer symmetric for $p = 4k + 3$, in fact, $Q^T = -Q$ as -1 is quadratic non-residue by Euler's Lemma. Formula (9.25) is substituted by $QQ^T = pI - J$ and $QJ = JQ =$ all zero matrix. Now it is easy to see that the following matrix, named after Paley, is Hadamard:

$$\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ -1 & & & & \\ \vdots & & & I+Q & \\ -1 & & & & \end{pmatrix}. \tag{14.34}$$

Hadamard matrices have lots of applications in engineering and science. I show one application, weighing matrices, which appears in a number of more realistic measurement problems.

We have a two-pan scale and we can read the difference of the weights of the two sides. Every measurement comes with a random error term from a certain distribution. This distribution is the same for every measurement. The expected value of a measurement is the correct weight difference of the items in the pans. The error of different measurements are independent. The error has expectation 0 and variance σ^2, i.e., the result of a measurement is a random variable X, with $\mathcal{E}[(X - \mathcal{E}[X])^2] = \sigma^2$.

Assume that we have n objects indexed by $1, 2, ..., n$ that we have to weigh. We want to beat the error term somehow. We achieve a factor of k gain on the variance, if we average out the results of k measurements $X^1, X^2, ..., X^k$ of the same object:

$$\mathcal{E}\left[\left(\frac{\sum_{i=1}^k X^i}{k} - \mathcal{E}\Big[\frac{\sum_{i=1}^k X^i}{k}\Big]\right)^2\right] = \frac{1}{k^2}\mathcal{E}\big[\sum_{i=1}^k (X^i - \mathcal{E}(X^i))^2\big] = \frac{1}{k^2}\sum_{i=1}^k \mathcal{E}\big[(X^i - \mathcal{E}(X^i))^2\big] = \frac{\sigma^2}{k}.$$

If we want to gain a factor of k on the variance for the weight of every object in this way, we have to make nk measurements.

Assume know that we have an $n \times n$ Hadamard matrix H. We make n measurements of combinations of objects. For the i^{th} measurement, we put item j into the left pan if ${}_iH_j = 1$ and into the right pan if ${}_iH_j = -1$. Let w_j denote the true weight of the j^{th} item. The result of the i^{th} measurement is a random variable

$$X_i = \sum_j {}_i[H]_j w_j + Y_i,$$

where Y_i is the error of the i^{th} measurement, which is of the same distribution as the error of any measurement. Observe

$$H^T \begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_n \end{pmatrix} = H^T H \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{pmatrix} + H^T \begin{pmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_n \end{pmatrix} = \begin{pmatrix} nw_1 \\ nw_2 \\ \vdots \\ nw_n \end{pmatrix} + H^T \begin{pmatrix} Y_1 \\ Y_2 \\ \vdots \\ Y_n \end{pmatrix},$$

$$nw_\ell - \sum_i \ell[H^T]_i X_i = -\sum_i \ell[H^T]_i Y_i \text{ and}$$

$$\mathcal{E}\Big[\Big(nw_\ell - \sum_i \ell[H^T]_i X_i\Big)^2\Big] = \mathcal{E}\Big[\Big(\sum_i \ell[H^T]_i Y_i\Big)^2\Big] = \sum_i \mathcal{E}[Y_i^2] = n\sigma^2,$$

and finally, for every ℓ, we can estimate the weight of the ℓ^{th} item with a weighted average such that

$$\mathcal{E}\Big[\Big(w_\ell - \frac{1}{n}\sum_i \ell[H^T]_i X_i\Big)^2\Big] = \sigma^2/n.$$

With the help of an $n \times n$ Hadamard matrix, we made n measurements to estimate the weight of n items with variance σ^2/n. If we measured n times each item as in our first naive method, we get the same variance, but at the cost of making n^2 measurements.

15 Homework Problems

F1) Show that in a projective plane over a field there are indeed 4 points, such that no 3 of them are incident to the same line.
F2) Show that in an incidence structure satisfying (P1) and (P2), properties (P3) and (P4) are equivalent.
F3) (a) Show that in a finite projective plane (as defined in section 5) the number of points and the number of lines is the same, and equals $q^2 + q + 1$ for some positive integer q.
(b) The number of lines incident to any given point equals to the number of points incident to any given line, and equals $q + 1$, with the same q as in part (a).
F4) Show that the Fano plane is a projective plane over a field.
F5) Prove Pappus' and Desargues' theorems.
F6) Show that for $n \geq 2$, (P1) and (P2) imply $\big($(P3) or outcome (iii)$\big)$ in Theorem 7.
F7) Derive Theorem 9 from (7.13).
F8) For any positive numbers a_i,

$$(a_1 a_2 \cdots a_n)^{1/n} \leq \frac{a_1 + a_2 + \cdots + a_n}{n} \leq \sqrt{\frac{a_1^2 + a_2^2 + \ldots + a_n^2}{n}}.$$

Verify both inequalities from Jensen's inequality. Characterize cases of equality.
F9) Verify Jensen's inequality by induction on n.
F10) Verify that the polar line $cx + dy = 1$ is perpendicular to Op and passes through p' (see end of Section 5).
F11) Verify Theorem 19 under condition (a).
F12) Verify Theorem 19 under condition (b).
F13) Assume that $2 \leq t \leq s \leq n$ and the graph G on n vertices is $K_{s,t}$-free. Show that $e = O(s^{\frac{1}{t}} n^{2-\frac{1}{t}})$, where the constant in the $O(.)$-sign is independent of t, s, n.
F14) Let $f(z)$ be a polynomial with complex coefficients. Identifying complex numbers $z = xi + y$ with the (x, y) points in the plane, the convex hull of the roots of $f(z)$ contains all roots of the derivative $f'(z)$.

F15) Assume that p is an odd prime. Take for the vertex set V of a graph the points of the affine 3-space over $GF(p)$, i.e. $\{(x, y, z) : x, y, z \in GF(p)\}$, and join (x, y, z) and (a, b, c) with an edge, if $(a - x)^2 + (b - y)^2 + (c - z)^2 = \alpha$. Select for α a quadratic residue, if $p = 4k + 3$, and select for α a quadratic non-residue, if $p = 4k + 1$.
a) Show that this graph is $K_{3,3}$-free.
b) Show that $|E| \geq c|V|^{2-1/3}$ for sufficiently large p.
F16) Show that the composition of a polarity and a collineation is a polarity.
F17) The complement of a strongly regular graph with parameters (n, k, λ, μ) is a strongly regular graph with parameters $(n, n - k - 1, n - 2k + \mu - 2, n - 2k + \lambda)$.
F18) For a k-regular graph G, k is its largest eigenvalue, and if the graph is connected, this eigenvalue has multiplicity one.
F19) Verify that the matrix in (14.34) is Hadamard.
F20) Find the discriminant of the polynomial $ax^2 + bx + c$.
F21) Prove Hadamard's Matrix Inequality (14.33) using the method of Lagrange multipliers.
F22) Verify Theorem 26.