# Pseudorandom graphs

David Conlon

## What is a pseudorandom graph?

A pseudorandom graph is a graph that behaves like a random graph of the same edge density. For example, it might be the case that the graph has roughly the same edge density between any two large sets or that it contains roughly the same number of copies of every small graph $H$ as one would expect to find in a random graph. The purpose of this course will be to explore certain notions of pseudorandomness and to see what properties the resulting graphs have.

For much of the course, our basic object of study will be $(p, \beta)$-jumbled graphs, a concept introduced (in a very slightly different form) by Andrew Thomason in the 1980s. These are defined as follows.

**Definition 1** *A graph $G$ on vertex set $V$ is $(p, \beta)$-jumbled if, for all vertex subsets $X, Y \subseteq V(G)$,*

$$|e(X,Y) - p|X||Y|| \leq \beta\sqrt{|X||Y|}.$$

That is, the edge density between any two sets $X$ and $Y$ is roughly $p$, with the allowed discrepancy measured in terms of $\beta$. The normalisation may be explained by considering what happens in a random graph. In this case, the expected number of edges between $X$ and $Y$ will be $p|X||Y|$ and the standard deviation will be $\sqrt{p(1-p)|X||Y|}$. So $\beta$ is measuring how many multiples of the standard deviation our edge density is allowed to deviate by.

Of course, random graphs should themselves be pseudorandom. Recall that the binomial random graph $G(n,p)$ is a graph on $n$ vertices formed by choosing each edge independently with probability $p$. With high probability, this graph has density close to $p$. The next theorem, whose proof we shall leave as an exercise, says that these graphs are also $(p, O(\sqrt{pn}))$-jumbled with high probability.

**Theorem 1** *Let $p = p(n) \leq 0.99$. Then asymptotically almost surely, the binomial random graph $G(n,p)$ has the following property. For any two subsets $X, Y \subseteq V(G)$,*

$$|e(X,Y) - p|X||Y|| = O(\sqrt{pn|X||Y|}).$$

This result is in some sense best possible. Indeed, it was shown by Erdős, Goldberg, Pach and Spencer that a graph on $n$ vertices with $p \leq 0.99$ cannot be $(p, \beta)$-jumbled with $\beta = o(\sqrt{pn})$.

However, pseudorandom graphs would not be interesting were it not for the fact that there is a plentiful supply of explicit pseudorandom graphs. The standard example of such a graph is the Paley graph.

**Definition 2** *Suppose $q \equiv 1 \pmod 4$ is prime. The Paley graph $P_q$ is the graph with vertex set $\mathbb{Z}_q$, where $x$ and $y$ are joined if and only if $x - y$ is a quadratic residue.*

Note that the restriction that $q \equiv 1 \pmod 4$ is so that the definition is consistent. Indeed, in this case, $-1$ is a quadratic residue, which means that $x - y$ is a quadratic residue if and only if $y - x$ is. We will prove that the Paley graph $P_q$ is $(\frac{1}{2}, O(\sqrt{q}))$-jumbled. One proof of this result uses exponential sum estimates that go back to Gauss. However, we will take a slightly different, more general approach, proving that Paley graphs are pseudorandom in two steps. The first step is to show that so-called $(n, d, \lambda)$-graphs are pseudorandom. We will then show that a Paley graph is an $(n, d, \lambda)$-graph, completing the proof. However, we must first define what an $(n, d, \lambda)$-graph is.

## $(n, d, \lambda)$-graphs

The *adjacency matrix* of a graph $G = (V, E)$ on vertex set $V(G) = \{1, 2, \ldots, n\}$ is an $n \times n$ matrix $A$ whose entry $a_{ij}$ is equal to 1 if $(i, j) \in E(G)$ and 0 otherwise. Since this is a real symmetric matrix, it is diagonalisable. This means that there are $n$ real eigenvalues $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ and an orthonormal basis $B = \{v_1, v_2, \ldots, v_n\}$ composed of eigenvectors of $A$ such that $Av_i = \lambda_i v_i$. Note that the matrix $A$ can then be written as $A = \sum_{i=1}^{n} \lambda_i v_i v_i^t$. We also note the following important result, which follows from the Perron–Frobenius theorem or may be proved directly.

**Theorem 2** *Let $G$ be a $d$-regular graph with $n$ vertices and $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ be the eigenvalues of the adjacency matrix of $G$. Then $\lambda_1 = d$ and $-d \leq \lambda_i \leq d$ for all $2 \leq i \leq n$. Moreover, if $G$ is connected then the $\lambda_1$-eigenvector $v_1$ is proportional to $(1, 1, \ldots, 1)^t \in \mathbb{R}^n$ and $\lambda_i < d$ for all $i \geq 2$.*

With this information in hand, we may now define $(n, d, \lambda)$-graphs.

**Definition 3** *A graph $G$ is said to be an $(n, d, \lambda)$-graph if it has $n$ vertices, every vertex has degree $d$ and, if $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ are the eigenvalues of the adjacency matrix of $G$, $|\lambda_i| \leq \lambda$ for all $i \geq 2$.*

We will now prove the surprising and fundamental fact that $(n, d, \lambda)$-graphs are $(\frac{d}{n}, \lambda)$-jumbled.

**Theorem 3** *Let $G$ be a $d$-regular graph with $n$ vertices, $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ be the eigenvalues of the adjacency matrix of $G$ and*

$$\lambda = \max_{2 \leq i \leq n} |\lambda_i|.$$

*Then, for any two sets $X, Y \subseteq V(G)$,*

$$\left| e(X, Y) - \frac{d|X||Y|}{n} \right| \leq \lambda \sqrt{|X||Y|}.$$

**Proof** Let $B = \{v_1, v_2, \ldots, v_n\}$ be an orthonormal basis of $B$ composed of eigenvectors of the adjacency matrix $A$. That is, $Av_i = \lambda_i v_i$ and $v_i^t v_i = 1$. Note that $A = \sum_{i=1}^{n} \lambda_i v_i v_i^t$ and write

$$A_1 = \lambda_1 v_1 v_1^t$$

and

$$A_2 = \sum_{i=2}^{n} \lambda_i v_i v_i^t,$$

so that $A = A_1 + A_2$.

Write $\chi_X$ and $\chi_Y$ for the characteristic vectors of $X$ and $Y$. That is, $\chi_X(i) = 1$ if $i \in X$ and 0 otherwise and similarly for $\chi_Y$. We may write $\chi_X$ and $\chi_Y$ as follows:

$$\chi_X = \sum_{i=1}^{n} \alpha_i v_i, \text{ where } \alpha_i = \chi_X^t v_i \text{ and } \sum_{i=1}^{n} \alpha_i^2 = \|\chi_X\|^2 = |X|,$$

$$\chi_Y = \sum_{i=1}^{n} \beta_i v_i, \text{ where } \beta_i = \chi_Y^t v_i \text{ and } \sum_{i=1}^{n} \beta_i^2 = \|\chi_Y\|^2 = |Y|.$$

Note now that the number of edges between $X$ and $Y$ is $\chi_X^t A \chi_Y$, so that

$$e(X,Y) = \chi_X^t A_1 \chi_Y + \chi_X^t A_2 \chi_Y.$$

We will show that the first term in this expression corresponds to the main term $\frac{d}{n}|X||Y|$ and the second to the error term. To see this, note that

$$\chi_X^t A_1 \chi_Y = \left(\sum_{i=1}^{n} \alpha_i v_i\right)^t (\lambda_1 v_1 v_1^t) \left(\sum_{j=1}^{n} \beta_j v_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_i \lambda_1 \beta_j (v_i^t v_1)(v_1^t v_j) = \alpha_1 \beta_1 \lambda_1$$

and

$$\chi_X^t A_2 \chi_Y = \left(\sum_{i=1}^{n} \alpha_i v_i\right)^t \left(\sum_{j=2}^{n} \lambda_j v_j v_j^t\right) \left(\sum_{k=1}^{n} \beta_k v_k\right) = \sum_{i=2}^{n} \alpha_i \beta_i \lambda_i.$$

Since $\lambda_1 = d$ and $v_1 = \frac{1}{\sqrt{n}}(1,1,\ldots,1)^t$, we have $\alpha_1 = \chi_X^t v_1 = |X|/\sqrt{n}$ and, similarly, $\beta_1 = |Y|/\sqrt{n}$, so $\chi_X^t A_1 \chi_Y = \frac{d}{n}|X||Y|$, as required. Moreover, by the ubiquitous Cauchy–Schwarz inequality,

$$|\chi_X^t A_2 \chi_Y| = |\sum_{i=2}^{n} \alpha_i \beta_i \lambda_i| \leq \lambda |\sum_{i=2}^{n} \alpha_i \beta_i| \leq \lambda \sqrt{\sum_{i=2}^{n} \alpha_i^2 \sum_{i=2}^{n} \beta_i^2} \leq \lambda \sqrt{|X||Y|},$$

completing the proof. □

In the next section, we will use this result to prove that a certain class of graphs, the so-called strongly regular graphs, are pseudorandom.

## Strongly regular graphs

**Definition 4** *A strongly regular graph $srg(n,d,\eta,\mu)$ is a $d$-regular graph on $n$ vertices in which every pair of adjacent vertices have exactly $\eta$ common neighbours and every pair of nonadjacent vertices have exactly $\mu$ common neighbours.*

Two simple examples of strongly regular graphs are the cycle of length 5, with parameters $(5,2,0,1)$, and the Petersen graph, with parameters $(10,3,0,1)$. More relevant to our purposes is the following lemma, which we leave as an exercise.

**Lemma 1** *The Paley graph $P_q$ is strongly regular, with parameters $(q,(q-1)/2,(q-5)/4,(q-1)/4)$.*

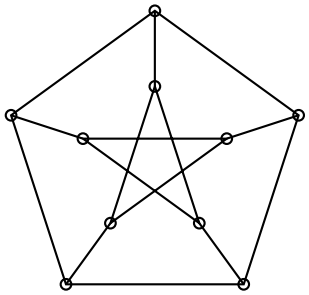

Figure 1: The Petersen graph, a strongly regular graph with parameters $(10, 3, 0, 1)$.

By combining this lemma with the following theorem, which bounds the eigenvalues of any strongly regular graph in terms of its parameters, we will finally have completed the proof that Paley graphs are $(\frac{1}{2}, O(\sqrt{n}))$-jumbled.

**Theorem 4** *Let $G$ be a connected strongly regular graph with parameters $(n, d, \eta, \mu)$. Then the eigenvalues of $G$ are $\lambda_1 = d$ with multiplicity $m_1 = 1$,*

$$\lambda_2 = \frac{1}{2}\left(\eta - \mu + \sqrt{(\eta-\mu)^2 + 4(d-\mu)}\right)$$

*with multiplicity*

$$m_2 = \frac{1}{2}\left(n - 1 + \frac{(n-1)(\mu-\eta) - 2d}{\sqrt{(\eta-\mu)^2 + 4(d-\mu)}}\right)$$

*and*

$$\lambda_3 = \frac{1}{2}\left(\eta - \mu - \sqrt{(\eta-\mu)^2 + 4(d-\mu)}\right)$$

*with multiplicity*

$$m_3 = \frac{1}{2}\left(n - 1 - \frac{(n-1)(\mu-\eta) - 2d}{\sqrt{(\eta-\mu)^2 + 4(d-\mu)}}\right).$$

**Proof** If $i \neq j$, the $(i, j)$-entry of the square $A^2$ of the adjacency matrix $A$ measures the number of common neighbours of vertex $i$ and vertex $j$, while if $i = j$, it measures the degree of vertex $i$. Letting $I$ be the $n \times n$ identity matrix and $J$ the $n \times n$ all-one matrix, the statement that $G$ is strongly regular is equivalent to the two conditions

$$AJ = dJ$$

and

$$A^2 = (d-\mu)I + \mu J + (\eta - \mu)A.$$

Since $G$ is $d$-regular and connected, $\lambda_1 = d$ is an eigenvalue with multiplicity 1 and eigenvector $e = (1, 1, \ldots, 1)^t$. Let $\lambda \neq d$ be another eigenvalue and $x \in \mathbb{R}^n$ the corresponding eigenvector. Then $x$ is orthogonal to $e$, which implies that $Jx = 0$. Therefore, applying the formula for $A^2$ above to $x$, we see that

$$\lambda^2 x = (d-\mu)x + (\eta - \mu)\lambda x.$$

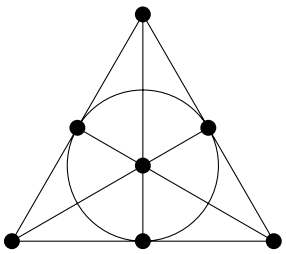

Figure 2: The Fano plane $PG(2,2)$.

This gives a quadratic equation for $\lambda$ whose solutions are exactly $\lambda_2$ and $\lambda_3$ in the theorem statement. For the multiplicities, note that

$$1 + m_2 + m_3 = n$$

and

$$Tr(A) = d + m_2\lambda_2 + m_3\lambda_3 = 0.$$

Solving these simultaneous equations gives the required answer. □

A number of examples of strongly regular graphs are given in the problem sets.

## Further examples

### The Erdős–Rényi graph

Let $q$ be a prime power and $PG(q,t)$ the projective space of dimension $t$, that is, each element is an equivalence class of non-zero vectors of length $t+1$ over the finite field of order $q$, where two vectors are taken as equivalent if one is a multiple of the other by an element in the field. This set has $n = (q^{t+1}-1)/(q-1)$ elements. The simplest example $PG(2,2)$, commonly known as the Fano plane, is drawn in Figure 2.

We define a graph $G$ whose vertices are the points of $PG(q,t)$ and where two vertices $x = (x_0, x_1, \ldots, x_t)$ and $y = (y_0, y_1, \ldots, y_t)$ are adjacent if and only if $x_0y_0 + x_1y_1 + \cdots + x_ty_t = 0$, that is, their scalar product is zero. Note that this notion of adjacency is well defined. It is straightforward to check that $G$ is $d$-regular with $d = (q^t-1)/(q-1)$, though there may be some loops. However, there are $O(q^{t-1})$ vertices with loops. To calculate the eigenvalues of $G$, we again let $I$ be the $n \times n$ identity matrix and $J$ the $n \times n$ all-one matrix. Then

$$A^2 = \mu J + (d-\mu)I,$$

where $\mu = (q^{t-1}-1)/(q-1)$. As in the proof of Theorem 4, this easily implies that all eigenvalues apart from the largest have absolute value $\sqrt{d-\mu}$.

When $t = 2$, these graphs are known as Erdős–Rényi graphs. They are important in extremal graph theory, as they contain no cycles of length 4. We leave the verification of this property as an exercise.

### Alon's triangle-free graph

Consider the finite field with $2^k$ elements, with each element being represented by a binary vector of length $k$. If $a, b$ and $c$ are three such vectors, let $(a,b,c)$ be the binary vector of length $3k$ formed

by concatenating $a, b$ and $c$. Suppose that $k$ is not divisible by 3. Let $W_0$ be the set of all non-zero elements $\alpha$ of the finite field for which the leftmost bit of $\alpha^7$ is 0 and $W_1$ be the set of all non-zero elements $\alpha$ of the finite field for which the leftmost bit of $\alpha^7$ is 1. Since 3 does not divide $k$, 7 does not divide $2^k - 1$, which implies that $|W_0| = 2^{k-1} - 1$ and $|W_1| = 2^{k-1}$. This is because when $\alpha$ ranges over all non-zero elements of the field, so does $\alpha^7$.

Let $A_k$ be the graph whose vertex set are all $n = 2^{3k}$ binary vectors of length $3k$, where two vectors $u$ and $v$ are adjacent if and only if there exist $w_0 \in W_0$ and $w_1 \in W_1$ such that $u - v = (w_0, w_0^3, w_0^5) + (w_1, w_1^3, w_1^5)$. This is an example of a Cayley graph, where we join $u$ and $v$ if and only if their difference is in some prescribed subset of a finite group. (The Paley graph is another example.)

It is easy to show that $A_k$ is $2^{k-1}(2^{k-1} - 1)$-regular. It is also triangle free. To sketch the proof of this, let $U_0 = \{(w_0, w_0^3, w_0^5) | w_o \in W_0\}$, $U_1 = \{(w_1, w_1^3, w_1^5) | w_1 \in W_1\}$ and $S = U_0 + U_1$. It is possible to show that any six distinct vectors in $U_0 \cup U_1$ are linearly independent over the field with 2 elements. The statement that $A_k$ is triangle free is equivalent to the statement that no three non-zero vectors in $S$ add to zero. If $u_0 + u_1, u_0' + u_1'$ and $u_0'' + u_1''$ are three elements in $S$ that add to zero, then every vector in the sequence $(u_0, u_1, u_0', u_1', u_0'', u_1'')$ must appear twice. But this contradicts the fact that $U_0$ and $U_1$ are disjoint. Finally, the graph is also close to optimally pseudorandom, with $|\lambda_i| = O(2^k)$ for all $i \neq 1$. We omit the proof in this case, though the general idea is similar to the previous examples.

## Expander graphs

Perhaps the most famous and important class of pseudorandom graphs are those with bounded degree, commonly known as expander graphs. We describe one construction of such graphs, due to Lubotzky, Phillips and Sarnak below.

Let $p$ and $q$ be unequal primes, both congruent to 1 (mod 4), with $p$ a quadratic residue modulo $q$. Let $PSL(2, q)$ be the projective special linear group consisting of all $2 \times 2$ matrices over the field of order $q$ with determinant 1 with the normal subgroup consisting of $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ quotiented out. It is known that there are exactly $p + 1$ vectors $a = (a_0, a_1, a_2, a_3)$ such that $a_0$ is odd and positive, $a_1, a_2$ and $a_3$ are even and $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$. This follows from an identity of Jacobi, which says that the number of ways to write a positive integer $n$ as a sum of four squares is $8 \sum_{4 \nmid d, d|n} d$. For each such vector $a$, define the matrix $M_a \in PSL(2, q)$ by

$$M_a = \frac{1}{\sqrt{p}} \begin{pmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{pmatrix},$$

where $i$ satisfies $i^2 \equiv -1 \pmod{q}$. Note that the determinant of $M_a$ is indeed 1.

Let $G_{p,q}$ be the Cayley graph with vertex set $PSL(2, q)$ defined by joining $u$ and $v$ if and only if $uv^{-1} = M_a$ for some $a$. It is possible to show that if $q > 2\sqrt{p}$, then $G_{p,q}$ is a connected $(p+1)$-regular graph with $q(q^2 - 1)/2$ vertices. Using some very deep results in number theory, one may show that all eigenvalues except the largest have absolute value at most $2\sqrt{p}$. By a result of Alon and Boppana, this is asymptotically optimal.

## Quasirandom graphs

A fundamental result of Chung, Graham and Wilson states that for graphs of density $p$, where $p$ is a fixed positive constant, the property of being $(p, o(n))$-jumbled is equivalent to a number of other properties that one would typically expect in a random graph. The following theorem details some of these many equivalences.

**Theorem 5** *For any fixed $0 < p < 1$ and any sequence of graphs $(G_n)_{n\in\mathbb{N}}$ with $|V(G_n)| = n$ the following properties are equivalent.*

- $P_1$: *$G_n$ is $(p, o(n))$-jumbled, that is, for all subsets $X, Y \subseteq V(G_n)$, $|e(X,Y) - p|X||Y|| = o(n^2)$;*
- $P_2$: *$e(G_n) \geq p\binom{n}{2} + o(n^2)$, $\lambda_1(G_n) = pn + o(n)$ and $|\lambda_2(G_n)| = o(n)$, where $\lambda_i(G_n)$ is the $i$th largest eigenvalue, in absolute value, of the adjacency matrix of $G_n$;*
- $P_3$: *for all graphs $H$, the number of labeled induced copies of $H$ in $G_n$ is $(1-p)^{\binom{t}{2}-\ell}p^\ell n^t + o(n^t)$, where $t = v(H)$ and $\ell = e(H)$;*
- $P_4$: *$e(G_n) \geq p\binom{n}{2} + o(n^2)$ and the number of labeled cycles of length 4 in $G_n$ is at most $p^4n^4 + o(n^4)$.*

Any graph sequence which satisfies any (and hence all) of these properties is said to be *$p$-quasirandom*. The most surprising aspect of this theorem, already hinted at in Thomason's work, is that if the number of cycles of length 4 is as one would expect in a binomial random graph then this is enough to imply that the edges are very well-spread. We will prove a simplified version of this result below.

**Theorem 6** *Suppose that $G$ is a graph on $n$ vertices which is regular of degree $pn$ and contains $p^4n^4 + \epsilon^4 n^4$ labeled cycles of length 4. Then, for all $X, Y \subseteq V(G)$,*

$$|e(X,Y) - p|X||Y|| \leq \epsilon n^2.$$

**Proof** Let $G(x,y)$ be the characteristic function for the edges of $G$. That is, $G(x,y) = 1$ if $xy$ is an edge of $G$ and 0 otherwise. Let us write $g(x,y) = G(x,y) - p$ and note that

$$\sum_y g(x,y) = \sum_y G(x,y) - pn = 0.$$

The number of labeled cycles in $G$ is

$$\begin{aligned}
&\sum_{x,x',y,y'} G(x,y)G(y,x')G(x',y')G(y',x) \\
&= \sum_{x,x',y,y'} \big(p + g(x,y)\big)\big(p + g(y,x')\big)\big(p + g(x',y')\big)\big(p + g(y',x)\big) \\
&= pn^4 + 4pn^2 \sum_{x,y} g(x,y) + 4p^2 n \sum_{x,y,y'} g(x,y)g(x',y) + 2p^2 \sum_{x,x',y,y'} g(x,y)g(x',y') \\
&+ 4p \sum_{x,x',y,y'} g(x,y)g(y,x')g(x',y') + \sum_{x,x',y,y'} g(x,y)g(y,x')g(x',y')g(y',x).
\end{aligned}$$

Each term in this expression, apart from the first and the last, are 0. For example,

$$\sum_{x,x',y,y'} g(x,y)g(y,x')g(x',y') = \sum_{x',y} \left( \sum_x g(x,y) \right) g(y,x') \left( \sum_{y'} g(x',y') \right) = 0.$$

Therefore, the number of labeled cycles in $G$ is

$$p^4 n^4 + \sum_{x,x',y,y'} g(x,y)g(y,x')g(x',y')g(y',x),$$

so we may conclude, from the assumption in the theorem, that

$$\sum_{x,x',y,y'} g(x,y)g(y,x')g(x',y')g(y',x) \leq \epsilon^4 n^4.$$

We will now estimate the number of edges between $X$ and $Y$ by observing that

$$e(X,Y) = \sum_{x \in X, y \in Y} G(x,y) = p|X||Y| + \sum_{x \in X, y \in Y} g(x,y).$$

To prove the theorem, it therefore suffices to show that

$$|\sum_{x \in X, y \in Y} g(x,y)| \leq \epsilon n^2.$$

We will again write $\chi_X$ and $\chi_Y$ for the characteristic vectors of $X$ and $Y$. The required result now follows from the Cauchy–Schwarz inequality, since

$$\begin{aligned}
\left( \sum_{x \in X, y \in Y} g(x,y) \right)^4 &= \left( \sum_{x,y} g(x,y)\chi_X(x)\chi_Y(y) \right)^4 \\
&= \left( \sum_x \left( \sum_y g(x,y)\chi_Y(y) \right) \chi_X(x) \right)^4 \\
&\leq \left( \sum_x \left( \sum_y g(x,y)\chi_Y(y) \right)^2 \right)^2 \left( \sum_x \chi_X(x) \right)^2 \\
&= |X|^2 \left( \sum_{x,y,y'} g(x,y)g(x,y')\chi_Y(y)\chi_Y(y') \right)^2 \\
&= |X|^2 \left( \sum_{y,y'} \left( \sum_x g(x,y)g(x,y') \right) \chi_Y(y)\chi_Y(y') \right)^2 \\
&\leq |X|^2 \left( \sum_{y,y'} \left( \sum_x g(x,y)g(x,y') \right)^2 \right) \left( \sum_{y,y'} \chi_Y(y)\chi_Y(y') \right) \\
&= |X|^2|Y|^2 \sum_{x,x',y,y'} g(x,y)g(y,x')g(x',y')g(y',x) \leq \epsilon^4 n^8.
\end{aligned}$$

Taking the fourth root completes the proof. In fact, the same proof gives the slightly stronger bound $\epsilon n\sqrt{|X||Y|}$, which is in good accord with the usual definition of jumbledness. □

For sparse graphs, an analogue of Theorem 5 does not hold. In this setting, it is natural to generalise the jumbledness condition for dense graphs by considering graphs which are $(p, o(pn))$-jumbled. Otherwise, we would not even have control over the density in the whole set. However, it is no longer the case that being $(p, o(pn))$-jumbled implies that the number of copies of any subgraph $H$ agrees with the expected count. For $H = K_{3,3}$ and $p = n^{-1/3}$, it is easy to see this by taking the random graph $G_{n,p}$ and changing three vertices $u$, $v$ and $w$ so that they are each connected to everything else. This does not affect the property of being $(p, o(pn))$-jumbled but it does affect the $K_{3,3}$ count, since as well as the roughly $p^9n^6 = n^3$ copies of $K_{3,3}$ that one expects in a random graph, one gets a further $\Omega(n^3)$ copies of $K_{3,3}$ containing all of $u$, $v$ and $w$.

We have already seen some examples of quasirandomness graphs, such as the Paley graph. Surprisingly, it is the case that every dense graph can be split into a bounded number of vertex subsets so that the bipartite graphs between most pairs of vertex subsets satisfy the bipartite analogue of quasirandomness. This is the famous Szemerédi regularity lemma, which we state after some preliminary definitions.

**Definition 5** *A bipartite graph $G = (U, V; E)$ is said to satisfy DISC$(p, \epsilon)$ if, for all $X \subseteq U$ and all $Y \subseteq V$,*

$$|e(X, Y) - p|X||Y|| \leq \epsilon|U||V|.$$

*Moreover, a partition $V(G) = V_1 \cup \cdots \cup V_k$ of the vertex set of a graph $G$ is said to be equitable if $||V_i| - |V_j|| \leq 1$ for all $i$ and $j$.*

**Theorem 7 (Szemerédi's regularity lemma)** *For every $\epsilon > 0$, there exists a positive integer $M$ such that every graph $G$ has an equitable partition into $k \leq M$ pieces for which all but at most $\epsilon k^2$ pairs of vertex subsets $(V_i, V_j)$ satisfy DISC$(p_{ij}, \epsilon)$ for some $p_{ij}$.*

We will not prove this theorem here, referring the reader instead to the original paper by Szemerédi, which is both short and well written. However, we do note one important consequence of the regularity lemma, the triangle removal lemma.

**Theorem 8 (Triangle removal lemma)** *For any $\epsilon > 0$, there exists $\delta > 0$ such that any graph on $n$ vertices with fewer than $\delta n^3$ triangles can be made triangle free by removing at most $\epsilon n^2$ edges.*

The statement of this lemma is deceptively simple. Until very recently, the only known proof for this result used the regularity lemma and gave a bound for $\delta^{-1}$ which was a tower of 2s of height polynomial in $\epsilon^{-1}$. However, this was recently improved by Fox, so that $\delta^{-1}$ can now be bounded by a tower of 2s of height logarithmic in $\epsilon^{-1}$. Though still enormous, this bound is better than one could possibly hope to achieve using the regularity lemma.

The reason the triangle removal lemma is seen as important is that it implies the following fundamental result of Roth.

**Theorem 9 (Roth's theorem)** *For every $\delta > 0$, there exists $n_0$ such that if $n \geq n_0$, then every subset of $\{1, 2, \ldots, n\}$ of order at least $\delta n$ contains an arithmetic progression of length 3.*

The same statement also holds for arithmetic progressions of length $k$, for any $k$, but this result, known as Szemerédi's theorem, is significantly more difficult. There are now many proofs of Szemerédi's theorem, but the natural generalisation of the proof outlined above requires the development of a hypergraph regularity lemma and a hypergraph removal lemma.

## Properties of pseudorandom graphs

### Independence number

The *independence number* $\alpha(G)$ of a graph $G$ is the size of the largest set of vertices in $G$ containing no edge. For jumbled graphs, we may upper bound the independence number as follows.

**Lemma 2** *Suppose that $G$ is a $(p, \beta)$-jumbled graph. Then*

$$\alpha(G) \leq \beta/p.$$

**Proof** If $U$ is an independent set in $G$, then, by the definition of $(p, \beta)$-jumbledness,

$$|2e(U) - p|U|^2| = p|U|^2 \leq \beta|U|,$$

so the result follows. □

In particular, when $G$ is an $(n, d, \lambda)$-graph, we get $\alpha(G) \leq \frac{\lambda n}{d}$. Even when $\lambda = O(\sqrt{d})$, which is as small as possible, this only gives $\alpha(G) = O(\frac{n}{\sqrt{d}})$. This is in sharp contrast with random graphs, where we know that, for $d = pn$, $\alpha(G(n,p)) = \Theta(\frac{n}{d}\log d)$. However, though it differs greatly from the situation for random graphs, there are optimally pseudorandom graphs for which Lemma 2 is sharp.

One example for which the lemma is sharp is the Paley graph $P_q$, where $q = p^2$ is the square of a prime. In this case, every element of the subfield $GF(p)$ is a quadratic residue in $GF(p^2)$, as $GF(p^2)$ is a splitting field for $X^2 - a$ for all $a \in GF(p)$. We may then form an independent set of order $p$ by taking a quadratic non-residue $\beta$ and considering the coset $\beta GF(p)$.

By Lemma 2, we see that Alon's triangle-free pseudorandom graph $A_k$ contains no independent set of order larger than some appropriate multiple of $n^{2/3}$. Thus, we may use Alon's graph to show that the off-diagonal Ramsey number $r(3,t) = \Omega(t^{3/2})$. To date, this is the best known constructive lower bound for this quantity.

### Connectivity

The *edge connectivity* of a graph is the smallest number of edges that can be deleted so as to make the graph disconnected, while the *vertex connectivity* is defined similarly with vertices replacing edges. If we consider $(p, \beta)$-jumbled graphs, we can say essentially nothing about their connectivity, since it is possible to add an isolated vertex or a small collection of isolated vertices without changing the jumbledness property significantly. However, if we also assume a minimum degree condition, we can recover something. We will restrict attention here to $(n, d, \lambda)$-graphs, following Krivelevich and Sudakov.

**Theorem 10** *Let $G$ be an $(n, d, \lambda)$-graph with $d - \lambda \geq 2$. Then the edge connectivity of $G$ is $d$.*

**Proof** It will be enough to show that there are at least $d$ edges between any vertex set $U$, with $|U| \leq n/2$, and its complement. We will split into two cases, depending on the order of $U$. If $1 \leq |U| \leq d$, then each vertex in $U$ has degree at least $d - |U| + 1$ in the complement of $U$. Therefore,

$$e(U, U^c) \geq |U|(d - |U| + 1) \geq d.$$

If $d \leq |U| \leq n/2$, we use that the graph is $(\frac{d}{n}, \lambda)$-jumbled to conclude that

$$e(U, U^c) \geq \frac{d}{n}|U|(n - |U|) - \lambda\sqrt{|U|(n - |U|)} \geq \frac{d - \lambda}{n}|U|(n - |U|) \geq |U| \geq d,$$

as required. □

A similar result holds for vertex connectivity, though the proof, which we omit, is a little more complicated. We refer the reader to the survey paper of Krivelevich and Sudakov for further details.

**Theorem 11** *There exists a constant $c$ such that if $G$ is an $(n, d, \lambda)$-graph, then the vertex connectivity of $G$ is at least*

$$d - c\frac{\lambda^2}{d}.$$

In particular, when $\lambda$ is on the order of $\sqrt{d}$, this is within a constant of $d$.

## Hamiltonicity

A *Hamilton cycle* is a cycle that passes through all the vertices of a graph. In order to study this concept in pseudorandom graphs, it is again necessary to restrict attention to graphs with a minimum degree condition. Working with $(n, d, \lambda)$-graphs, Krivelevich and Sudakov proved the following result.

**Theorem 12** *There exists a constant $c$ such that if $G$ is an $(n, d, \lambda)$-graph with*

$$\lambda \leq c\frac{(\log\log n)^2}{\log n \log\log\log n}d,$$

*then $G$ contains a Hamilton cycle.*

They also conjecture that $\lambda \leq cd$ for some sufficiently small $c > 0$ should be sufficient.

## Counting small subgraphs

In this section, we will try to count the number of copies of a fixed subgraph in a pseudorandom graph. We will focus on the case of triangles, leaving the study of more general graphs to the problem sets.

**Theorem 13** *Let $G$ be a $(p, \beta)$-jumbled graph with $\beta = o(p^2 n)$. Then $G$ contains $(1 + o(1))p^3\binom{n}{3}$ triangles.*

**Proof** For each vertex $v$, let $d(v)$ be the order of its neighbourhood $N(v)$. Then the number of triangles in the graph is

$$\Delta = \frac{1}{3}\sum_v e(N(v)).$$

By jumbledness, we know that

$$|2e(N(v)) - pd(v)^2| \leq \beta d(v).$$

Therefore,

$$\Delta = \frac{1}{6}p\sum_v d(v)^2 \pm \beta \sum_v d(v).$$

To estimate this quantity, note that

$$\sum_v d(v) = 2e(G) = pn^2 \pm \beta n = pn^2 \pm o(p^2n^2) = (1+o(1))pn^2.$$

This implies that $\beta \sum_v d(v) = o(p^3n^3)$, so it suffices to estimate $\sum_v d(v)^2$.
Suppose that $U$ is a subset of $V(G)$, consisting of vertices $u$ for which $d(u) \geq (1+\delta)pn$. Then

$$\delta p|U|n \leq |e(U, V(G)) - p|U|n| \leq \beta\sqrt{|U|n}.$$

This easily implies that $|U| \leq \beta^2/\delta^2p^2n = o(p^2n/\delta^2)$. Similarly, $U'$, the set of vertices $u$ for which $d(u) \leq (1-\delta)pn$ has order $o(p^2n/\delta^2)$. Therefore,

$$\sum_v d(v)^2 = (1\pm\delta)^2p^2n^3 \pm o(p^2n/\delta^2)n^2 = (1+o(1))p^2n^3,$$

provided $\delta$ tends to zero sufficiently slowly. Substituting back into the formula for $\Delta$ implies the required result. □

Again, Alon's example shows that Theorem 13 is sharp. Indeed, his example has $\beta = O(p^2n)$ and contains no triangles at all. This means that as $\beta$ drops in size there is a very sharp shift from pseudorandom graphs which contain no triangles at all to pseudorandom graphs which contain approximately the same number of triangles that would appear in a random graph.

An extension of Theorem 13 shows that if $G$ is a $(p,\beta)$-jumbled graph with $\beta = o(p^{t-1}n)$, then $G$ contains $(1+o(1))p^{\binom{t}{2}}\binom{n}{t}$ copies of $K_t$. It is widely believed that this result is tight, but for $t \geq 4$ there is no example proving that this is the case. Finding such constructions is one of the outstanding open problems about pseudorandom graphs.

**Further material.** Throughout these notes, I have borrowed/stolen extensively from the excellent survey paper on 'Pseudorandom graphs' by Krivelevich and Sudakov. Together with the recent paper 'Extremal results in sparse pseudorandom graphs' by Fox, Zhao and myself, this paper could form the basis for an extended version of this lecture series. It would also be possible to look more closely at expander graphs, for which we recommend the survey paper 'Expander graphs and their applications' by Hoory, Linial and Wigderson, or, for the most exciting recent breakthrough, to the paper 'Interlacing polynomials I: Bipartite Ramanujan graphs of all degrees' by Marcus, Spielman and Srivastava.