- Property $P_5(s)$: For every graph H on s vertices $N(H) = n^s p^{e(H)}(1 + o(1))$
- Property P_6: $N(C_4) = n^4 p^4 (1 + o(1))$

Obviously all of these properties are satisfied by the random graph $G(n,p)$. In a seminal paper, Chung, Graham, and Wilson proved that they are equivalent for every graph (sequence)!

Theorem A.26 *Let G be a (sequence of) (n,d,λ)-graph(s) with $d = pn$, with $p, 0 < p < 1$, a constant. Then P_1, P_2, $P_3(s)$ for some $s \geq 4$, $P_4(s)$ for some $s \geq 4$, P_5, P_6.*

The most suprising that the weak-looking property P_6 about the number of C_4 implies the bound on the second eigenvalue and the number of arbitrary fixed subgraph

Observe that the theorem cannot be true in this form for $d \ll n$. The C_4-free polarity graph discussed in Subsection 2.1.3 has the best possible quasi-random second eigenvalue $\sqrt{d}$ and still contains NO C_4, while the corresponding random graph with edge-probability $p = n^{-\frac{1}{2}}$ contains $\Theta(n^4 p^4) = \Theta(n^2)$ C_4.

A.5 Cayley graphs and Characters

All what was said so far about eigenvalues applies for any d-regular graph. The graphs we construct are often defined algebraically, in which case they are often possible to cast as *Cayley graphs* and their eigenvalues are most conveniently expressed in terms of the group's *characters*.

A.5.1 Cayley graphs

Given a group H and a subset $S \subseteq H$ with the properties that $0 \notin S$ and $S = -S$ (that is, for every $a, b \in H$, $a - b \in S$ if and only if $b - a \in S$), we define the Cayley graph $G(H,S) = G$ as follows:

- $V(G) = H$
- $E(G) = \{ab : a - b \in S\}$.

Examples

1. The Cayley graph $G((\mathbb{Z}_n, +), \{1, -1\})$ is just the cycle C_n.
2. The Cayley graph $G(\mathbb{F}_q^*, QR(q))$ is the Payley graph we defined in ....

It turns out that eigenvalues of Cayley graphs are connected to the more general concept of group characters. Below we define the general notion, but soon will concentrate on abelian groups, which come up in our applications.

A.5.2 Basics of characters of Abelian groups

The following are based partly on the notes of Babai [].

Let H be a finite abelian group. For the sake of the this exposition we mostly write the group operation additively (denoted by $+$), however later we will also use characters of multiplicative groups and even mix the two.

The homomorphisms of $(H, +)$ into the multiplicative group $(\mathbb{C}^*, \cdot)$ of the complex numbers are called *characters* of H. Formally, $\chi : H \to \mathbb{C}^*$ is a *character* of H if

$$\chi(a+b) = \chi(a)\chi(b) \text{ for every } a, b \in H.$$

How many characters are there? Just a few? Or many? Maybe an infinite number? We show that there are exactly as many characters as group elements and their structure is really restricted: they themselves form a group isomorphic to H.

Examples. **1.** One immediate example of a character is the *principal character* χ_0, which is defined by

$$\chi_0(a) = 1, \text{ for every } a \in H,$$

and exists for an arbitrary group H.

2. Another important example is the *quadratic residue character* ρ_q of the multiplicative group $(\mathbb{F}_q^*, \cdot)$ of a finite field:

$$\rho_q(x) = \begin{cases} 1 & \text{if } x \in QR(q) \\ -1 & \text{otherwise.} \end{cases}$$

The map ρ_q is a homomorphism because as we saw earlier in Appendix A.2, a square times a square or a non-square times a non-square is a square, while a square times a non-square is a non-square.

3. For the cyclic group $(\mathbb{Z}_n, +)$ an obvious choice transferring the (mod n) addition to complex multiplication is the character χ_1. For every $x \in \mathbb{Z}_n$ we define

$$\chi_1(x) = \omega^x,$$

where $\omega = e^{2\pi i \frac{x}{n}}$.

The fact that the quadratic residue character has only values 1 and -1 and the values of χ_1 are also roots of unity is not an accident: all character values must be some root of unity.

Exercise A.2 *Prove that*

- $\chi(a)$ *is a* $|H|^{th}$ *root of unity.*
- $\chi(-a) = \chi(a)^{-1} = \overline{\chi(a)}$

All the nth roots of unity, i.e., the values of the character χ_1, sum up to 0. This is again not a coincidence: the values of *any* non-principal character sum up to 0.

Proposition A.27 *For any character $\chi \neq \chi_0$,*

$$\sum_{a \in H} \chi(a) = 0.$$

Proof. Let $b \in H$ be such that $\chi(b) \neq 1$; such an element b exists since χ is not principal. Then, using that $a \to a + b$ is a bijection from H to H, we have that

$$\sum_{a \in H} \chi(a) = \sum_{a \in H} \chi(a+b) = \left(\sum_{a \in H} \chi(a) \right) \chi(b).$$

Then the claim follows. □

Let $\hat{H}$ be the set of characters. It will turn out that H has exactly $|H|$ characters. Even more, there is a natural group structure on $\hat{H}$ and the two groups are isomorphic.

Proposition A.28 *$\hat{H}$ is an abelian group with the operation $\cdot$, defined by*

$$(\chi \cdot \psi)(a) := \chi(a)\psi(a).$$

Proof. Exercise. □

The group H and its group of characters are isomorphic.

Theorem A.29 *$H \cong \hat{H}$.*

Proof. We establish the proof in two steps. First we explicitely give the characters of the cyclic group $(\mathbb{Z}_n, +)$.

Proposition A.30 *Let ω be an arbitrary primitive n^{th} root of unity (i.e. $\omega^i = 1$ if and only if $n|i$) and define the map $\chi_j : \mathbb{Z}_n \to \mathbb{C}^*$ by $\chi_j(a) := \omega^{ja}$. Then*

- *χ_j is a character for every $j \in \mathbb{Z}_n$.*
- *the mapping sending $j \in \mathbb{Z}_n$ to $\chi_j \in \hat{\mathbb{Z}}_n$ is an isomorphism between $\mathbb{Z}_n$ and $\hat{\mathbb{Z}}_n$.*

Proof. The first statement follows easily from the definition: $\chi_j(a+b) = \omega^{j(a+b)} = \omega^{ja}\omega^{jb} = \chi_j(a)\chi_j(b)$.
For the second statement let us see first that the mapping is a homomorphism from $(\mathbb{Z}_n, +)$ to $(\hat{\mathbb{Z}}_n, \cdot)$. Indeed, $j + \ell \in \mathbb{Z}_n$ is mapped to $\chi_{j+\ell} = \chi_j \cdot \chi_\ell$. The mapping is injective, since $\chi_j(1) = \chi_\ell(1)$ would mean that $\omega^{j-\ell} = 1$ and since ω is primitive, we have n dividing $j - \ell$, so $j = \ell$. Let us see finally that the mapping is surjective. Let χ be an arbitrary character of $(\mathbb{Z}_n, +)$. Since $\chi(1)$ is an nth root of unity by Exercise ... and ω is primitive, there is a j, such that $\chi(1) = \omega^j$. Then, since χ is a character, $\chi(a) = \chi(1 + \cdots + 1) = \chi(1)^a = \omega^{ja} = \chi_j(a)$ for every $a \in \mathbb{Z}_n$, so χ is identical to χ_j. □

Secondly we show how to obtain the characters of a direct sum from the characters of its summands.

Proposition A.31 *If $H = H_1 \times H_2$, then $\hat{H} \cong \hat{H}_1 \times \hat{H}_2$*

Proof. Exercise □

To conclude the proof of Theorem A.29 note that any finite abelian group is the direct product of cyclic groups, hence by the previous two proposition

$$H \cong \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_r} \cong \hat{\mathbb{Z}}_{s_1} \times \cdots \times \hat{\mathbb{Z}}_{s_r} \cong \hat{H}.$$

□

Example Let $H = \overbrace{\mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}^{k}$. Then $\hat{H} = \{\chi_w : w \in \{0,1\}^k\}$, where $\chi_w(a) = (-1)^{w \cdot a}$ and $w \cdot a = \sum_{i=1}^{k} w_i a_i$ is the usual scalar product of vectors.

Inner product and orthonormal basis

$\mathbb{C}^H := \{f : H \to \mathbb{C}\}$ is an n-dimensional linear space over $\mathbb{C}$. We define an inner product on $\mathbb{C}^H$:

$$\langle f, g \rangle = \frac{1}{n} \sum_{a \in H} \overline{f(a)} g(a).$$

Corollary A.32 *(First orthogonality relation) For any $\chi, \psi \in \hat{H}$,*

$$\langle \chi, \psi \rangle = \begin{cases} 1 & \textit{if } \chi = \psi \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. Exercise. □

Corollary A.33 *$\hat{H}$ forms an orthonormal basis in $\mathbb{C}^H$.*

Corollary A.34 *Every $f \in \mathbb{C}^H$ can be written uniquely as the linear combination of characters:*

$$f = \sum_{\chi \in \hat{H}} c_\chi \chi,$$

where $c_\psi = \langle \psi, f \rangle$ are called the Fourier coefficients *of f.*

Proof. By the previous Corollary the characters form an orthonormal basis in $\mathbb{C}^H$, so we can express f uniquely as their linear combination $f = \sum c_\chi \chi$ with $c_\chi \in \mathbb{C}$. Taking the inner product of both sides with any fixed character ψ from the left, we see by the first orthogonality relation that all terms cancel except $\langle \psi, f \rangle$ and c_ψ. □

Bounding the deviation from the average

For us, the main application of the discrete Fourier transform is the estimation of the deviation of a function from its average, via the non-principal Fourier coefficients.

Proposition A.35 *Let $f : H \to \mathbb{C}$ be an arbitrary function on an abelian group H. Then for every $a \in H$ we have*

$$\left| f(a) - \frac{1}{|H|} \sum_{x \in H} f(x) \right| \le \Phi(f)|H|,$$

where $\Phi(f) = \max\{|\langle \chi, f \rangle| : \chi \in \widehat{H}, \chi \neq \chi_0\}$.

Proof. Conveniently, the Fourier coefficient of f corresponding to the principal character is equal to the average value of f. Indeed,

$$\langle \chi_0, f \rangle = \frac{1}{|H|} \sum_{x \in H} \overline{\chi}_0(x) f(x) = \frac{1}{|H|} \sum_{x \in H} f(x).$$

Then, writing f in the Fourier basis of characters, we have

$$\left| f(a) - \frac{1}{|H|} \sum_{x \in H} f(x) \right| = \left| \sum_{\chi \in \widehat{H}} \langle \chi, f \rangle \chi(x) - \frac{1}{|H|} \sum_{x \in H} f(x) \right| = \left| \sum_{\substack{\chi \in \widehat{H} \\ \chi \neq \chi_0}} \langle \overline{\chi}, f \rangle \chi(a) \right|$$
$$\le \sum_{\substack{\chi \in \widehat{H} \\ \chi \neq \chi_0}} |\langle \overline{\chi}, f \rangle| \cdot |\chi(a)| \le \Phi(f)|H|.$$

□

Remark: The Fourier coefficients of a function $f : H \to \mathbb{C}$ naturally define a function $\hat{f}$ on the character group $\widehat{H}$. For every $\chi \in \widehat{H}$ we set

$$\hat{f}(\chi) := |H| \langle \overline{\chi}, f \rangle = \sum_{x \in H} \chi(x) f(x).$$

The function $\hat{f} : \hat{H} \to \mathbb{C}$ is called the (discrete) *Fourier transform* of f. The formula

$$f = \sum_{\chi \in \hat{H}} \frac{1}{n} \hat{f}(\overline{\chi}) \chi.$$

obtained by writing f in the Fourier basis is usually called the *Inverse Fourier Transform.* Since our applications of the discrete Fourier transform do not really go beyond the basics, we prefer avoiding the us of the notation $\hat{f}$ in our proofs.

Quasi-randomness of Cayley-graphs

For a subset $S \subseteq H$ let us define

$$\Phi(S) = \max\{|H|\widehat{\mathbb{1}}_S(\chi) : \chi \in \hat{H}, \chi \neq \chi_0\}.$$

Just to have an idea about how large $\Phi(S)$ is let us calculate an upper bound (why is it that??): $|H|\widehat{\mathbb{1}}_S(\chi_0) = |H|\frac{1}{|H|}\sum_{s\in S}\chi_0(s) = |S|$. For a lower bound see the following small Claim

Claim 6

$$\Phi(S) \geq \sqrt{|S|}2,$$

provided $|S| \leq \frac{n}{2}$.

Let now $S \subseteq H$ be a subset such that $S = -S$. The Cayley graph $G = G(H, S)$ is defined on the vertex set $V(G) = H$. Two vertices $u, v \in V$ are adjacent if $v - u \in S$. In other words, the neighborhood of each vertex $w \in H$ is the set $w + S$ and thus the Cayley graph is d-regular with $d = |S|$.

Exercise A.3 *Give a proof of the following on the language of characters:*
Let $\langle H, +\rangle$ *be an abelian group and* S *be a subset, such that* $S = -S$*. Let* G *be the corresponding Cayley graph. For any subsets* $B, C \subseteq V(G)$*,*

$$\left|e(B,C) - |B||C|\frac{|S|}{|H|}\right| \leq \Phi(S)\sqrt{|B||C|}.$$

Solution:
The following theorem shows that the closer $\Phi(S)$ is to the lower bound of the Claim the stronger pseudorandom properties the corresponding Cayley graph exhibits.

Theorem A.36 *For any subsets* $B, C \subseteq V(G(S))$*,*

$$\left|e(B,C) - |B||C|\frac{|S|}{|H|}\right| \leq \Phi(S)\sqrt{|B||C|},$$

where $e(B,C)$ *denotes the number of ordered pairs* $(u,v) \in B \times C$*, such that* $uv \in E(G(S))$*.*

Proof.

$$
\begin{aligned}
e(B,C) &= \sum_{u\in B}\sum_{v\in C}\sum_{s\in S}\mathbb{1}_{\{0\}}(u+s-v)\\
&= \sum_{u\in B}\sum_{v\in C}\sum_{s\in S}\sum_{\chi\in\widehat{H}}\widehat{\mathbb{1}}_{\{0\}}(\chi)\chi(u+s-v)\\
&= \sum_{\chi\in\widehat{H}}\sum_{u\in B}\sum_{v\in C}\sum_{s\in S}\frac{1}{|H|}\chi(u)\chi(s)\chi(-v)\\
&= \sum_{\chi\in\widehat{H}}\frac{1}{|H|}(\sum_{u\in B}\chi(u))(\sum_{s\in S}\chi(s))(\sum_{z\in -C}\chi(z))\\
&= \frac{|B||C||S|}{|H|}+\sum_{\chi\neq\chi_0}\frac{1}{|H|}(\sum_{u\in B}\chi(u))(|H|\widehat{\mathbb{1}}_S(\chi))(\sum_{z\in -C}\chi(z))
\end{aligned}
$$

On the one hand $|(|H|\widehat{\mathbb{1}}_S(\chi))|\leq\Psi(S)$.
On the other hand by the Cauchy-Schwartz-inequality

$$
\begin{aligned}
\left|\sum_{\chi\neq\chi_0}(\sum_{u\in B}\chi(u))(\sum_{z\in -C}\chi(z))\right| &\leq \sum_{\chi\neq\chi_0}\left|\sum_{u\in B}\chi(u)\right|\left|\sum_{z\in -C}\chi(z)\right|\\
&\leq \sum_{\chi\in\widehat{H}}\left|\sum_{u\in B}\chi(u)\right|\left|\sum_{z\in -C}\chi(z)\right|\\
&\leq \sqrt{\sum_{\chi\in\widehat{H}}\left(\sum_{u\in B}\chi(u)\right)^2}\sqrt{\sum_{\chi\in\widehat{H}}\left(\sum_{z\in -C}\chi(z)\right)^2}\\
&\leq \sqrt{\sum_{\chi\in\widehat{H}}\left(|H|\widehat{\mathbb{1}}_B(\chi)\right)^2}\sqrt{\sum_{\chi\in\widehat{H}}\left(|H|\widehat{\mathbb{1}}_{-C}(\chi)\right)^2}\\
&\leq |H|^2\sqrt{\langle\mathbb{1}_B,\mathbb{1}_B\rangle}\sqrt{\langle\mathbb{1}_{-C},\mathbb{1}_{-C}\rangle}\\
&\leq |H|^2\sqrt{\frac{|B|}{|H|}}\sqrt{\frac{|-C|}{|H|}}\\
&\leq |H|\sqrt{|B|}\sqrt{|C|}
\end{aligned}
$$

and the theorem follows. □

The following is an easy corollary.

Corollary A.37 *Let $G=G(H,S)$ be a Cayley graph. Then*

$$\alpha(G)\leq\frac{\Phi(S)|H|}{|S|}.$$

Proof. Let I be an independent set of maximum size, that is $|I| = \alpha(G)$. By Theorem A.36 we have that

$$\left| e(I,I) - |I|^2 \frac{|S|}{|H|} \right| \leq \Phi(S)|I|.$$

Since $e(I,I) = 0$, we have $|I|^2 \frac{|S|}{|H|} \leq \Phi(S)|I|$, which implies the statement. □

The following simple proposition shows that in fact we already proved Theorem A.36 and Corollary A.37 in the previous section.

Proposition A.38 *The spectrum of the Cayley graph $G(H,S)$ is the n-element multiset $\{\sum_{s\in S} \chi(s) : \chi \in \widehat{H}\} = \{|H|\widehat{\mathbb{1}}_S(\chi) : \chi \in \widehat{H}\}$. The eigenvectors are the n characters. In particular, the eigenvectors do not depend on S.*

Proof.

$$(A\chi)_v = \sum_{w\in G w-v\in S} \chi(w) = \sum_{s\in S} \chi(v+s) = \left(\sum_{s\in S} \chi(s) \right) \chi(v).$$

Hence χ is indeed an eigenvector with eigenvalue $\sum_{s\in S} \chi(s)$ □

Character sum estimates

The following famous theorem of Weil states that the values of a polynomial substituted into a non-principal character behave uniformly (in some weak sense) .

Theorem A.39 (Weil) *Let q be a prime power and let χ be a multiplicative character of $\mathbb{F}_q^*$ of order d, extended to $\mathbb{F}_q$ by $\chi(0) = 0$. Then for any polynomial $f(x) \in \mathbb{F}_q[x]$ which has precisely m distinct zeros and is not a dth power (over the algebraic closure) we have*

$$\left| \sum_{x\in\mathbb{F}_q} \chi(f(x)) \right| \leq (m-1)\sqrt{q}.$$

Note that Proposition A.27 is a special case of Weil's theorem for $f(x) = x$.

In light of how hard it is to *estimate* the sum of characters (Weil's theorems about various character sums are highly non-trivial), it is refreshing to see the simple proof of the following *precise formula* involving the additive *and* multiplicative charecters of a finite field together.

Theorem A.40 *(Gaussian sums) Let $\mathbb{F}$ be a finite field and let χ be a character of the additive group of $\mathbb{F}$, while let ψ be a character of the multiplicative group of $\mathbb{F}$. Then*

$$\left| \sum_{C\in\mathbb{F} C\neq 0} \chi(C)\psi(C) \right| = \begin{cases} |\mathbb{F}| - 1 & \text{if } \chi = \chi_0 \text{ and } \psi = \psi_0 \\ 0 & \text{if } \chi = \chi_0 \text{ and } \psi \neq \psi_0 \\ 1 & \text{if } \chi \neq \chi_0 \text{ and } \psi = \psi_0 \\ \sqrt{|\mathbb{F}|} & \text{if } \chi \neq \chi_0 \text{ and } \psi \neq \psi_0, \end{cases}$$

where χ_0 is the pricipal additive character and ψ_0 is the prinicipal multiplicatice character.

Proof. In fact the whole proof is just applying Proposition A.27 over and over again; the first three cases being quite straightforward. To appply Proposition A.27 for the fourth case, we need a couple of simple manipulations.

$$\begin{aligned}
\left|\sum_{C\neq 0}\chi(C)\psi(C)\right|^2 &= \left(\sum_{C\neq 0}\chi(C)\psi(C)\right)\overline{\left(\sum_{C\neq 0}\chi(C)\psi(C)\right)} \\
&= \sum_{C\neq 0}\sum_{D\neq C,0}\chi(C)\psi(C)\overline{\chi(C)\psi(C)} + \sum_{C\neq 0}\chi(C)\psi(C)\overline{\chi(C)\psi(C)} \\
&= \sum_{C\neq 0}\sum_{D\neq C,0}\chi(C-D)\psi\left(\frac{C}{D}\right) + \sum_{C\neq 0}|\chi(C)|^2\,|\psi(C)|^2
\end{aligned}$$

Each character value is a root of unity, thus its norm is 1 implying that the second term consits of sum of 1s and thus equal to $|\mathbb{F}|-1$. To manipulate the first term we change variables.

$$\begin{aligned}
\sum_{C\neq 0}\sum_{D\neq C,0}\chi(C-D)\psi\left(\frac{C}{D}\right) &= \sum_{W\neq 0,1}\sum_{D\neq 0}\chi(D(W-1))\psi(W) \\
&= \sum_{W\neq 0,1}(-1)\cdot\psi(W) \\
&= 1
\end{aligned}$$

The next to last ineaquality follows from Proposition A.27 since for a fixed $W \neq 1$ the values $D(W-1)$ run through the nonzero elements of $\mathbb{F}$, while D runs through the nonzero elements of $\mathbb{F}$. The last inequality also follows from Proposition A.27; this time employed for the multiplicative character ψ.

$\square$