Lecture 15 (summary)

This lecture is devoted to identifying an explicit sequence of quasirandom graphs, which are known as *Paley graph* (and are a specific instance of Cayley graphs). Fix a prime p such that $p \bmod 4 = 1$ and consider $\mathbb{Z}_p$ with addition and multiplication modulo p. Let S be the set of non-zero quadratic residues, i.e. $S = \{t^2, t \neq 0, t \in \mathbb{Z}_p\}$. Note that $|S| = (p-1)/2$ and $-1 \in S$. The graph P_p is the graph with vertex set $\mathbb{Z}_p$ such that two vertices x and y are adjacent if $x - y \in S$. We will show that the sequence of graphs (P_p) with p tending to infinity is quasirandom. By the results that we have established earlier, it is enough to show that $t(K_2, P_p) \to 1/2$ and $t(C_4, P_p) \to 1/16$. The former is trivial since the graph P_p is $|S|$-regular.

Recall that the adjacency matrix A of a graph G is the zero-one matrix with rows and columns indexed by the vertices of G such that the entry in a row which is indexed by v and a column which is indexed by v' is one iff vv' is an edge of G. We will show that the eigenvalues of the adjacency matrix of the graph P_p are the following: $\frac{p-1}{2}$ with multiplicity one, $\frac{\sqrt{p}-1}{2}$ with multiplicity $\frac{p-1}{2}$ and $\frac{-\sqrt{p}-1}{2}$ with multiplicity $\frac{p-1}{2}$. It would then follow that

$$t(C_4, P_p) = \frac{\operatorname{Tr} A^4}{p^4} = \frac{\left(\frac{p-1}{2}\right)^4 + \frac{p-1}{2}\left(\frac{\sqrt{p}-1}{2}\right)^4 + \frac{p-1}{2}\left(\frac{-\sqrt{p}-1}{2}\right)^4}{p^4} = \frac{1}{16} + O\left(\frac{1}{p}\right),$$

which implies $t(C_4, P_p) \to 1/16$ and so the sequence (P_p) is quasirandom.

Fix a prime p such that $p \bmod 4 = 1$. Let ω be the p-th root unity, i.e. $\omega = e^{\frac{2\pi\iota}{p}}$, and let $v_k \in \mathbb{C}^p$ for $k = 0, \ldots, p-1$ be the vector such

$$(v_k)_i = \omega^{ki}.$$

Observe that the vectors v_k, $k = 0, \ldots, p-1$, are orthogonal:

$$\langle v_k | v_{k'} \rangle = \sum_{i=0}^{p-1} \omega^{(k-k')i},$$

which is zero for all $k \neq k'$. On the other hand, each v_k, $k = 0, \ldots, p-1$, is an eigenvector:

$$(Av_k)_i = \sum_{s \in S} \omega^{k(i+s)} = (v_k)_i \sum_{s \in S} \omega^{ks}.$$

It follows that the values

$$\lambda_k = \sum_{s \in S} \omega^{ks}$$

are eigenvectors of the adjacency matrix of the graph P_p.

Note that $\lambda_0 = |S| = \frac{p-1}{2}$. Suppose that $k \in \{1, \ldots, p-1\}$ and observe that

$$\lambda_k = \sum_{s \in S} \omega^{ks} = \sum_{t \in \mathbb{Z}_p \setminus \{0\}} \omega^{kt^2} = \frac{1}{2}\left(-1 + \sum_{t \in \mathbb{Z}_p} \omega^{kt^2}\right).$$

We show that the last sum is equal to $\sqrt{p}$ or $-\sqrt{p}$ by considering its square (note that we use that -1 is a quadratic residue):

$$\begin{aligned}\left(\sum_{t\in\mathbb{Z}_p}\omega^{kt^2}\right)^2 &= \left(\sum_{t\in\mathbb{Z}_p}\omega^{kt^2}\right)\left(\sum_{t'\in\mathbb{Z}_p}\omega^{kt'^2}\right) = \left(\sum_{t\in\mathbb{Z}_p}\omega^{-kt^2}\right)\left(\sum_{t'\in\mathbb{Z}_p}\omega^{kt'^2}\right)\\ &= \sum_{t\in\mathbb{Z}_p}\sum_{t'\in\mathbb{Z}_p}\omega^{kt'^2-kt^2} = \sum_{t\in\mathbb{Z}_p}\sum_{\tau\in\mathbb{Z}_p}\omega^{k(t+\tau)^2-kt^2}\\ &= \sum_{t\in\mathbb{Z}_p}\sum_{\tau\in\mathbb{Z}_p}\omega^{k\tau(2t+\tau)} = \sum_{\tau\in\mathbb{Z}_p}\sum_{t\in\mathbb{Z}_p}\omega^{k\tau(2t+\tau)}\\ &= \sum_{\tau\in\mathbb{Z}_p}\sum_{t'\in\mathbb{Z}_p}\omega^{k\tau t'}.\end{aligned}$$

Note that the inner sum is zero whenever $\tau \neq 0$ and so the whole double is equal to p. It follows that

$$\lambda_k \in \{\frac{\sqrt{p}-1}{2}, \frac{-\sqrt{p}-1}{2}\}$$

for every $k \in \{1,\ldots,p-1\}$. Finally, as $\operatorname{Tr} A = 0$, the multiplicity of each of the eigenvalues $\frac{\sqrt{p}-1}{2}$ and $\frac{-\sqrt{p}-1}{2}$ is exactly $\frac{p-1}{2}$.

Exercise. *Show that $\omega(P_p) \leq \sqrt{p}$ for every prime p such that $p \bmod 4 = 1$.*