Groups and Graphs
Lecture I: Cayley graphs

Vietri, 6-10 giugno 2016

A **GRAPH** is a pair $\Gamma = (V, E)$ where

- V - set of vertices - is a non-empty set;
- E - set of edges - is a subset of $V^{[2]} = \{\{x, y\} \mid x, y \in V,\ x \neq y\}$

---

vertices $x, y \in V$ are adjacent if $\{x, y\} \in E$ (write $x \sim y$)

- a walk in Γ is a sequence of vertices $x_0, x_1, \ldots, x_n$ such that $x_{i-1} \sim x_i$ for every $i = 1, \ldots n$;
- a path is a walk in which all edges $\{x_{i-1}, x_i\}$ are distinct, in this case n is the *length* of the path;
- a path $x_0, x_1, \ldots, x_n$ is simple if all vertices are distinct, except possibly for $x_0 = x_n$;
- a cycle is a simple path with $x_0 = x_n$ (n-cycle).

- A graph $\Gamma = (V, E)$ is connected if for any $x, y \in V$ there is a path
$$x = x_0, x_1, \ldots, x_n = y$$
(in general have *connected components*).
- A tree is a connected graph with no non-trivial cycles. This is equivalent to say that for any pair of distinct vertices x, y of Γ there is one and only one path from x to y.

If $\Gamma = (V, E)$ is connected a distance is defined in V; for $x, y \in V$,

$d_\Gamma(x, y)$ is the *minimal length of a path connecting x to y*.

- The diameter of a connected graph Γ is
$$diam(\Gamma) = \sup\{d_\Gamma(x, y) \mid x, y \in V\}.$$
- If the graph Γ is not a tree, the girth $g(\Gamma)$ of Γ is the *minimal length of a non-trivial cycle in* Γ.

degree: for $x \in V$, $deg_\Gamma(x) = |\{e \in E | x \in e\}|$. If Γ is finite

$$2|E| = \sum_{x \in V} deg_\Gamma(x).$$

For $k \geq 0$, Γ is k-regular if $deg_\Gamma(x) = k$ for every $x \in V$ (Γ is regular if it is k-regular for some k).

- Given a set of vertices V, the complete graph on V is $(V, V^{[2]})$. If $|V| = n$ denote it by K_n: K_n is $(n-1)$-regular.
- A graph is 1-regular if and only if all its connected components are just an edge.
- A finite graph is 2-regular if and only if all its connected components are cycles.
- a 3-regular graph is called 'cubic'.

An isomorphism of the graph $\Gamma = (V, E)$ to the graph $\Gamma' = [V', E']$ is a bijection $\alpha : V \to V'$ that preserves edges, i.e.

$$\forall x, y \in V : \ \{x, y\} \in E \Leftrightarrow \{\alpha(x), \alpha(y)\} \in E'.$$

The set of all automorphisms $Aut(\Gamma)$ of a graph Γ is a group.

- A graph $\Gamma = \Gamma = (V, E)$ is vertex–transitive if $Aut(\Gamma)$ acts transitively on V.

(Abstract) groups are automorphism groups of a graph

Theorem (Frucht, 1938)

Every group is the automorphism group of a (cubic) graph.

(later extended to several other classes of graphs).

Use of automorphism group is instrumental in enumerating results on graphs.

The Classification of finite simple groups has been applied (by considering their automorphism group) to prove many important results for classes of (highly) regular graphs.

Theorem (Sims conjecture)

There exists a function $f : \mathbb{N} \to \mathbb{N}$, *such that if* $\Gamma = (V, E)$ *is a* d*-regular vertex-transitive graph, then for every group* $G \leq Aut(\Gamma)$ *that acts primitively on* V, $|G_x| \leq f(d)$ *for every* $x \in V$.

But: most graphs have trivial automorphism group.

On the other hand, knowing that a group act as automorphisms on a graph may allow important (often elegant) insight on the group structure.
The most famous result in this direction is

Theorem (Serre)

A group is free if and only if it acts freely on a tree.

This is the starting point of the Bass-Serre theory of *graphs of groups*.

In finite groups theory, the language of graphs is used

- In the revision of the proof of classification of FSG (*amalgam method*).
- In the study of permutation groups.
- In encoding certain numerical features os given group:

  If Ω is a set of positive integers $\neq 1$, the *prime divisor* graph $\Pi(\Omega)$, is the graph whose vertices are all prime divisors of the elements of Ω, and two primes p, q are adjacent if there is $n \in \Omega$ such that $pq|n$.
  For G a finite group, such graphs have been studied when Ω is:

  – the set of the orders of non-trivial elements of G (the *prime graph* of G)

  – the set of the degrees of the irreducible $\mathbb{C}$-representations of G;

  – the set of the lengths of the conjugacy classes of G;

  – the set of the subdegrees, when G is a permutation group.

none of these topics will be treated in these lectures...

CAYLEY GRAPHS

– G a group
– $S \subseteq G$ such that $1 \notin S$ and $S^{-1} = S$ (symmetric set)

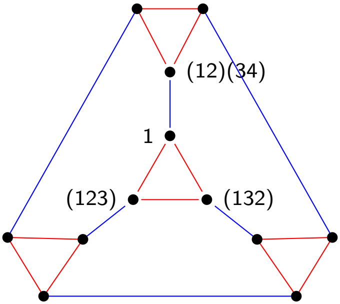
The Cayley graph $\Gamma[G, S]$ is the graph

- vertex set : G
- $\{x, y\}$ is an edge iff $y = xs$ for some $s \in S$.

Elementary facts:

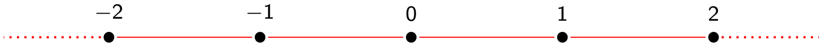
- $\Gamma[G, S]$ is k-regular for $k = |S|$;
- $\Gamma[G, S]$ is connected if and only if $G = \langle S \rangle$

The Cayley graph $\Gamma[A_4, S]$ for $S = \{(123), (132), (12)(34)\}$

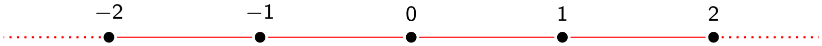


(123) and (132) : red edges
(12)(34) : blue edges

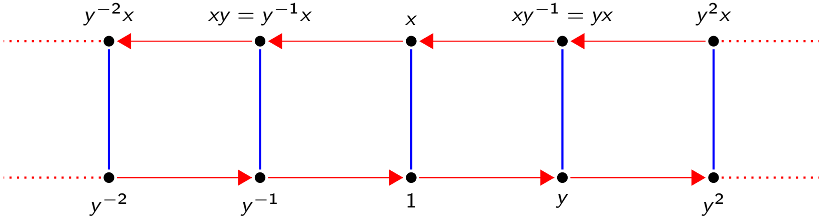
1) The Cayley graph $\Gamma[\mathbb{Z}, \{1, -1\}]$



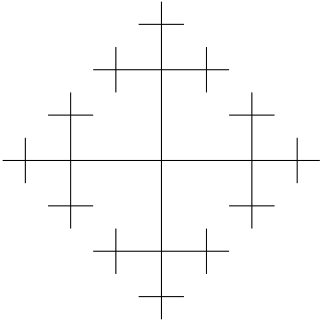
1) The Cayley graph $\Gamma[\mathbb{Z}, \{1, -1\}]$



2) $D = \langle x, y \mid x^2 = 1,\ y^x = y^{-1} \rangle$ the infinite dihedral group; the Cayley graph $\Gamma[D, \{x, y\}]$ looks like



3) the nieghborouhood of a vertex in the Cayley graph for the rank 2 free-group F_2 in its free generators (and their inverses):



$\Gamma = \Gamma[G, S]$ a Cayley graph for the group G.

For any $g \in G$, the left multiplication $\lambda_g : x \mapsto gx$ (for all $x \in G$), is a permutation on the vertex set G of Γ and for any $\{x, xs\} \in E(\Gamma)$

$$\lambda_g(\{x, xs\}) = \{gx, (gx)s\} \in E(\Gamma).$$

Thus, λ_g is an automorphism of the graph Γ; and we have an injective homomorphism $G \to Aut(\Gamma)$ given by $g \mapsto \lambda_{g^{-1}}$ (for all $g \in G$).

In conclusion, G is isomorphic to a subgroup of $Aut(\Gamma)$ which is transitive (indeed regular) on vertices. Cayley graphs are **vertex–transitive**.

- *A graph Γ is a Cayley graph if and only if $Aut(\Gamma)$ contains a regular subgroup on vertices.*

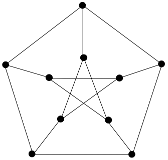
Many vertex-transitive graphs are Cayley, e.g. the *n-hypercube* Q_n:

- $V(Q_n) = \{0,1\}^n$
- $\{a = (a_1, \ldots, a_n), b = (b_1, \ldots b_n)\}$ is an edge iff a and b differ for exactly one component.

Q_n is the Cayley graph $\Gamma\left[(\mathbb{Z}/2\mathbb{Z})^n, \{e_1, \ldots, e_n\}\right]$ where

$$e_i = (0, 0, \ldots, 1, 0, \ldots, 0) \;\; (1 \text{ in the } i \cdot th \text{ position})$$

The Petersen graph: vertex-transitive but not Cayley



Question (Lovász)

Is any Cayley graph of a finite group G, with $|G| \geq 3$, hamiltonian?

Answer is YES if

- G abelian (Marusic 1983);
- G a p-group for a prime p (Witte 1986);
- $G = S_n$ and S made of transpositions;
- some other 'small' cases.

Theorem (Pak and Radoičić, 2009)

Every finite G with $|G| \geq 3$ has a generating set S of size $|S| \leq \log_2 |G|$, such that the Cayley graph $\Gamma[G, S]$ contains a Hamiltonian cycle.

In a Cayley graph $\Gamma = \Gamma[G, S]$, distance between vertices (elements of G) has a very clear meaning:

If $x \in G$, then $d_\Gamma(1, x)$ is the minimal length $\ell_S(x)$ of a product of elements $s \in S$ which equals x. By G-action, if $x, y \in G$ then $d_\Gamma(x, y) = \ell_S(x^{-1}y)$.

For $d \in \mathbb{N}$ let $B(1, r) = \{x \in G \mid \ell_S(x) \leq r\}$ (the ball of radius d). Then

$$B(1, r) = \{s_1 \dots s_r \mid s_i \in S \cup \{1\}\}.$$

Hence, if $|S| = k$,

$$|B(1, r)| \leq k^{r+1}.$$

The diameter of Γ is the minimal $d \geq 0$ such that $G = B(1, d)$; thus

$$diam(\Gamma[G, S]) \geq \frac{\log |G|}{\log k}.$$

It is not difficult to show that, if G is a finite abelian group, S a symmetrical set of generators of G of size k, then

$$diam(\Gamma[G,S]) \geq \frac{1}{e}|G|^{1/k}$$

Theorem (Babai, Kantor and Lubotzky)

There is a constant C such that every non-abelian finite simple group G has a set of generators S with $|S| = 7$, for which the diameter of the Cayley graph $\Gamma[G,S]$ is at most $C \log_2 |G|$.

Conjecture (Babai and Seress)

There exist a constant $c > 0$ such that for every non-abelian finite simple group G, and **every** *Cayley graph Γ on G, $diam(\Gamma) \leq (\log_2 |G|)^c$.*

(more to come...)