# Cayley graphs on abelian groups

Gabriel Verret

Rogla, May 18th, 2013

# Digraphs

A digraph $\Gamma$ is an ordered pair $(\mathcal{V}, \mathcal{A})$ where the vertex-set $\mathcal{V}$ is a finite non-empty set and the arc-set $\mathcal{A}$ is a binary relation on $\mathcal{V}$.

# Digraphs

A digraph $\Gamma$ is an ordered pair $(\mathcal{V}, \mathcal{A})$ where the vertex-set $\mathcal{V}$ is a finite non-empty set and the arc-set $\mathcal{A}$ is a binary relation on $\mathcal{V}$.

The elements of $\mathcal{V}$ and $\mathcal{A}$ are called vertices and arcs of $\Gamma$, respectively.

# Digraphs

A digraph $\Gamma$ is an ordered pair $(\mathcal{V}, \mathcal{A})$ where the vertex-set $\mathcal{V}$ is a finite non-empty set and the arc-set $\mathcal{A}$ is a binary relation on $\mathcal{V}$.

The elements of $\mathcal{V}$ and $\mathcal{A}$ are called vertices and arcs of $\Gamma$, respectively.

The digraph $\Gamma$ is called a graph when the relation $\mathcal{A}$ is symmetric.

# Digraphs

A digraph $\Gamma$ is an ordered pair $(\mathcal{V}, \mathcal{A})$ where the vertex-set $\mathcal{V}$ is a finite non-empty set and the arc-set $\mathcal{A}$ is a binary relation on $\mathcal{V}$.

The elements of $\mathcal{V}$ and $\mathcal{A}$ are called vertices and arcs of $\Gamma$, respectively.

The digraph $\Gamma$ is called a graph when the relation $\mathcal{A}$ is symmetric.

An automorphism of $\Gamma$ is a permutation of $\mathcal{V}$ which preserves the the relation $\mathcal{A}$.

# Cayley digraphs

Let $G$ be a finite group and let $S \subseteq G$.

# Cayley digraphs

Let $G$ be a finite group and let $S \subseteq G$.

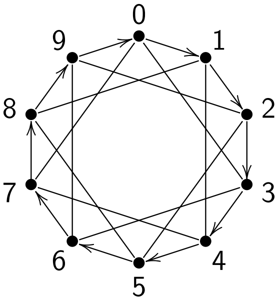
The Cayley digraph on $G$ with connection set $S$, denoted $\mathrm{Cay}(G, S)$, is the digraph with vertex-set $G$ and with $(g, h)$ being an arc if and only if $gh^{-1} \in S$.

# Cayley digraphs

Let $G$ be a finite group and let $S \subseteq G$.

The Cayley digraph on $G$ with connection set $S$, denoted $\mathrm{Cay}(G, S)$, is the digraph with vertex-set $G$ and with $(g, h)$ being an arc if and only if $gh^{-1} \in S$.

$\mathrm{Cay}(\mathbb{Z}_{10}, \{1, 3, 7\})$:



# Cayley digraphs, II

Note that $\mathrm{Cay}(G, S)$ may be disconnected and may have loops.

# Cayley digraphs, II

Note that $\mathrm{Cay}(G, S)$ may be disconnected and may have loops.

Easy observation : $\mathrm{Cay}(G, S)$ is a graph if and only if $S$ is inverse-closed, in which case it is called a Cayley graph.

## Cayley digraphs, II

Note that $\mathrm{Cay}(G, S)$ may be disconnected and may have loops.

Easy observation : $\mathrm{Cay}(G, S)$ is a graph if and only if $S$ is inverse-closed, in which case it is called a Cayley graph.

Easy result : $G$ acts regularly as a group of automorphisms of $\mathrm{Cay}(G, S)$ by right multiplication.

# Cayley digraphs, II

Note that $\mathrm{Cay}(G, S)$ may be disconnected and may have loops.

Easy observation : $\mathrm{Cay}(G, S)$ is a graph if and only if $S$ is inverse-closed, in which case it is called a Cayley graph.

Easy result : $G$ acts regularly as a group of automorphisms of $\mathrm{Cay}(G, S)$ by right multiplication.

Proof : Let $x \in G$ and let $\sigma_x : G \longrightarrow G$, $\sigma_x(g) = gx$. Then $gh^{-1} = gxx^{-1}h^{-1} = \sigma_x(g)\sigma_x(h)^{-1}$, hence $(g, h)$ is an arc of $\mathrm{Cay}(G, S)$ if and only if $(\sigma_x(g), \sigma_x(h))$ is. This shows that $\sigma_x$ is an automorphism of $\mathrm{Cay}(G, S)$. Clearly $\sigma_x\sigma_y = \sigma_{yx}$ hence $\{\sigma_x \mid x \in G\}$ is a group of automorphisms of $\mathrm{Cay}(G, S)$.

# Digraphical regular representation

If $G$ is the full automorphism group of $\mathrm{Cay}(G, S)$, then it is called a DRR.

# Digraphical regular representation

If $G$ is the full automorphism group of $\mathrm{Cay}(G, S)$, then it is called a DRR.

Babai (1980) showed that apart from 5 small exceptions, every finite group $G$ has a subset $S$ such that $\mathrm{Cay}(G, S)$ is a DRR.

# Digraphical regular representation

If $G$ is the full automorphism group of $\mathrm{Cay}(G, S)$, then it is called a DRR.

Babai (1980) showed that apart from 5 small exceptions, every finite group $G$ has a subset $S$ such that $\mathrm{Cay}(G, S)$ is a DRR.

In 1982, Babai and Godsil made the following conjecture:

### Conjecture

*Let $G$ be a group of order $n$. The proportion of subsets $S$ of $G$ such that $\mathrm{Cay}(G, S)$ is a DRR goes to $1$ as $n \to \infty$.*

# Digraphical regular representation

If $G$ is the full automorphism group of $\mathrm{Cay}(G, S)$, then it is called a DRR.

Babai (1980) showed that apart from 5 small exceptions, every finite group $G$ has a subset $S$ such that $\mathrm{Cay}(G, S)$ is a DRR.

In 1982, Babai and Godsil made the following conjecture:

### Conjecture

*Let $G$ be a group of order $n$. The proportion of subsets $S$ of $G$ such that $\mathrm{Cay}(G, S)$ is a DRR goes to $1$ as $n \to \infty$.*

Philosophically, this conjecture says that almost all Cayley digraphs have automorphism group as small as possible.

# Digraphical regular representation

If $G$ is the full automorphism group of $\mathrm{Cay}(G, S)$, then it is called a DRR.

Babai (1980) showed that apart from 5 small exceptions, every finite group $G$ has a subset $S$ such that $\mathrm{Cay}(G, S)$ is a DRR.

In 1982, Babai and Godsil made the following conjecture:

### Conjecture

*Let $G$ be a group of order $n$. The proportion of subsets $S$ of $G$ such that $\mathrm{Cay}(G, S)$ is a DRR goes to $1$ as $n \to \infty$.*

Philosophically, this conjecture says that almost all Cayley digraphs have automorphism group as small as possible.

Babai and Godsil proved the conjecture for nilpotent groups of odd order.

# Graphical regular representation

A DRR which is a graph is called a GRR (for graphical regular representation).

# Graphical regular representation

A DRR which is a graph is called a GRR (for graphical regular representation).

The naive corresponding conjecture for graphs is false, for simple reasons.

# Graphical regular representation

A DRR which is a graph is called a GRR (for graphical regular representation).

The naive corresponding conjecture for graphs is false, for simple reasons.

Let $A$ be an abelian group and let $\iota : A \longrightarrow A$, $\iota(a) = a^{-1}$. Then $\iota$ is an automorphism of $A$. Moreover, $\iota \neq 1$ unless $A \cong (\mathbb{Z}_2)^n$.

# Graphical regular representation

A DRR which is a graph is called a GRR (for graphical regular representation).

The naive corresponding conjecture for graphs is false, for simple reasons.

Let $A$ be an abelian group and let $\iota : A \longrightarrow A$, $\iota(a) = a^{-1}$. Then $\iota$ is an automorphism of $A$. Moreover, $\iota \neq 1$ unless $A \cong (\mathbb{Z}_2)^n$.

Let $\mathrm{Cay}(A, S)$ be a Cayley graph on $A$. Then $\iota$ is an automorphism of $\mathrm{Cay}(A, S)$: since $S$ is inverse-closed, $gh^{-1} \in S$ if and only if $\iota(gh^{-1}) \in S$ but $\iota(gh^{-1}) = \iota(g)\iota(h)^{-1}$.

# Graphical regular representation

A DRR which is a graph is called a GRR (for graphical regular representation).

The naive corresponding conjecture for graphs is false, for simple reasons.

Let $A$ be an abelian group and let $\iota : A \longrightarrow A$, $\iota(a) = a^{-1}$. Then $\iota$ is an automorphism of $A$. Moreover, $\iota \neq 1$ unless $A \cong (\mathbb{Z}_2)^n$.

Let $\mathrm{Cay}(A, S)$ be a Cayley graph on $A$. Then $\iota$ is an automorphism of $\mathrm{Cay}(A, S)$: since $S$ is inverse-closed, $gh^{-1} \in S$ if and only if $\iota(gh^{-1}) \in S$ but $\iota(gh^{-1}) = \iota(g)\iota(h)^{-1}$.

Conclusion : if $A$ is an abelian group and $A \ncong (\mathbb{Z}_2)^n$, then no Cayley graph on $A$ is a GRR.

# Corresponding conjectures

**Conjecture (Babai, Godsil, Imrich, Lóvasz, 1982)**

*Let $G$ be a group of order $n$ which is neither generalized dicyclic nor abelian. The proportion of inverse-closed subsets $S$ of $G$ such that $\mathrm{Cay}(G, S)$ is a GRR goes to $1$ as $n \to \infty$.*

# Corresponding conjectures

**Conjecture (Babai, Godsil, Imrich, Lóvasz, 1982)**

*Let $G$ be a group of order $n$ which is neither generalized dicyclic nor abelian. The proportion of inverse-closed subsets $S$ of $G$ such that $\mathrm{Cay}(G, S)$ is a GRR goes to $1$ as $n \to \infty$.*

**Conjecture (Babai, Godsil 1982)**

*Let $A$ be an abelian group of order $n$. The proportion of inverse-closed subsets $S$ of $A$ such that $\mathrm{Aut}(\mathrm{Cay}(A, S)) = \langle A, \iota \rangle$ goes to $1$ as $n \to \infty$.*

# Corresponding conjectures

### Conjecture (Babai, Godsil, Imrich, Lóvasz, 1982)

*Let $G$ be a group of order $n$ which is neither generalized dicyclic nor abelian. The proportion of inverse-closed subsets $S$ of $G$ such that $\mathrm{Cay}(G, S)$ is a GRR goes to $1$ as $n \to \infty$.*

### Conjecture (Babai, Godsil 1982)

*Let $A$ be an abelian group of order $n$. The proportion of inverse-closed subsets $S$ of $A$ such that $\mathrm{Aut}(\mathrm{Cay}(A, S)) = \langle A, \iota \rangle$ goes to $1$ as $n \to \infty$.*

This is now a theorem. (Dobson, Spiga, V.)

# Corresponding conjectures

### Conjecture (Babai, Godsil, Imrich, Lóvasz, 1982)

*Let $G$ be a group of order $n$ which is neither generalized dicyclic nor abelian. The proportion of inverse-closed subsets $S$ of $G$ such that $\mathrm{Cay}(G, S)$ is a GRR goes to $1$ as $n \to \infty$.*

### Conjecture (Babai, Godsil 1982)

*Let $A$ be an abelian group of order $n$. The proportion of inverse-closed subsets $S$ of $A$ such that $\mathrm{Aut}(\mathrm{Cay}(A, S)) = \langle A, \iota \rangle$ goes to $1$ as $n \to \infty$.*

This is now a theorem. (Dobson, Spiga, V.) We also proved the digraph conjecture for abelian groups.

# An important idea

**Lemma**

*Let $A$ be a group of order $n$. The number of subsets of $A$ which are fixed setwise by some element of $\mathrm{Aut}(A) \setminus \{1\}$ is at most $2^{3n/4+o(n)}$.*

**Proof.**

Note that $A$ is at most $\lfloor \log_2(n) \rfloor$-generated and hence $|\mathrm{Aut}(A)| \leq n^{\log_2(n)} \leq 2^{o(n)}$. We now count the number of subsets which are fixed setwise by a given $\varphi \in \mathrm{Aut}(A) \setminus \{1\}$. Let $\mathbf{C}_A(\varphi)$ denote the elements of $A$ that are fixed by $\varphi$. Note that $\varphi$ induces orbits of length 1 on $\mathbf{C}_A(\varphi)$ and of length at least 2 on $A \setminus \mathbf{C}_A(\varphi)$. Let $c = |\mathbf{C}_A(\varphi)|$. The number of subsets of $A$ which are fixed setwise by $\varphi$ is at most $2^{c+(n-c)/2} = 2^{n/2+c/2}$. Since $\mathbf{C}_A(\varphi)$ is a subgroup of $A$, we have $c \leq n/2$ and $n/2 + c/2 \leq 3n/4$. $\square$

# Outline of proof ideas

### Lemma

*Let $A$ be a group of order $n$. The number of subsets of $A$ which are fixed setwise by some element of $\mathrm{Aut}(A) \setminus \{1\}$ is at most $2^{3n/4+o(n)}$.*

# Outline of proof ideas

**Lemma**

*Let $A$ be a group of order $n$. The number of subsets of $A$ which are fixed setwise by some element of $\mathrm{Aut}(A) \setminus \{1\}$ is at most $2^{3n/4+o(n)}$.*

Note that the total number of subsets is $2^n$ and $\frac{2^{3n/4+o(n)}}{2^n} \to 0$.

# Outline of proof ideas

**Lemma**

*Let $A$ be a group of order $n$. The number of subsets of $A$ which are fixed setwise by some element of $\mathrm{Aut}(A) \setminus \{1\}$ is at most $2^{3n/4+o(n)}$.*

Note that the total number of subsets is $2^n$ and $\frac{2^{3n/4+o(n)}}{2^n} \to 0$. It follows that the "important" case is when $A$ is self-normalizing in $\mathrm{Aut}(\mathrm{Cay}(A, S))$.

# Outline of proof ideas

## Lemma

*Let $A$ be a group of order $n$. The number of subsets of $A$ which are fixed setwise by some element of $\mathrm{Aut}(A) \setminus \{1\}$ is at most $2^{3n/4+o(n)}$.*

Note that the total number of subsets is $2^n$ and $\frac{2^{3n/4+o(n)}}{2^n} \to 0$. It follows that the "important" case is when $A$ is self-normalizing in $\mathrm{Aut}(\mathrm{Cay}(A,S))$.

What we actually do is study transitive permutation groups containing a self-normalizing regular abelian subgroup.

# Outline of proof ideas

**Lemma**

*Let $A$ be a group of order $n$. The number of subsets of $A$ which are fixed setwise by some element of $\mathrm{Aut}(A) \setminus \{1\}$ is at most $2^{3n/4+o(n)}$.*

Note that the total number of subsets is $2^n$ and $\frac{2^{3n/4+o(n)}}{2^n} \to 0$. It follows that the "important" case is when $A$ is self-normalizing in $\mathrm{Aut}(\mathrm{Cay}(A, S))$.

What we actually do is study transitive permutation groups containing a self-normalizing regular abelian subgroup.

We prove some structural results and then "count" how often things can "go wrong".

# Outline of proof ideas

### Lemma

*Let $A$ be a group of order $n$. The number of subsets of $A$ which are fixed setwise by some element of $\mathrm{Aut}(A) \setminus \{1\}$ is at most $2^{3n/4+o(n)}$.*

Note that the total number of subsets is $2^n$ and $\frac{2^{3n/4+o(n)}}{2^n} \to 0$. It follows that the "important" case is when $A$ is self-normalizing in $\mathrm{Aut}(\mathrm{Cay}(A, S))$.

What we actually do is study transitive permutation groups containing a self-normalizing regular abelian subgroup.

We prove some structural results and then "count" how often things can "go wrong".

In the graph case, there are some extra complications.

# Future work

We plan to have a look at some other families of group in the near future.

# Future work

We plan to have a look at some other families of group in the near future.

1. 2-groups,
2. nilpotent groups,
3. certain classes of solvable groups, etc..