On the automorphism group of a circulant graph

Ilya Ponomarenko

St. Petersburg Department of V.A.Steklov
Institute of Mathematics, Russia

June, 28th - July 3rd 2009, GEMS'09

Computational problems for circulant graphs

Definition.

A graph Γ is called circulant if the group $\mathrm{Aut}(\Gamma)$ contains a regular cyclic subgroup G.

Computational problems for circulant graphs

Definition.

A graph Γ is called circulant if the group $\mathrm{Aut}(\Gamma)$ contains a regular cyclic subgroup G.

The following problems for an n-vertex graph Γ can be solved in time polynomial in n:

Computational problems for circulant graphs

Definition.

A graph Γ is called circulant if the group $\mathrm{Aut}(\Gamma)$ contains a regular cyclic subgroup G.

The following problems for an n-vertex graph Γ can be solved in time polynomial in n:

- test whether or not Γ is circulant (Evdokimov-Ponomarenko 2003),

Computational problems for circulant graphs

Definition.

A graph Γ is called circulant if the group $\mathrm{Aut}(\Gamma)$ contains a regular cyclic subgroup G.

The following problems for an n-vertex graph Γ can be solved in time polynomial in n:

- test whether or not Γ is circulant (Evdokimov-Ponomarenko 2003),
- given a circulant graph Γ' test whether or not Γ and Γ' are isomorphic (Evdokimov-Ponomarenko 2003, Muzychuk 2004).

Computational problems for circulant graphs

Definition.

A graph Γ is called circulant if the group $\mathrm{Aut}(\Gamma)$ contains a regular cyclic subgroup G.

The following problems for an n-vertex graph Γ can be solved in time polynomial in n:

- test whether or not Γ is circulant (Evdokimov-Ponomarenko 2003),
- given a circulant graph Γ' test whether or not Γ and Γ' are isomorphic (Evdokimov-Ponomarenko 2003, Muzychuk 2004).

Theorem.

Given an n-vertex circulant graph Γ a set of generators for the group $\mathrm{Aut}(\Gamma)$ can be found in time polynomial in n.

Circulant graphs with primitive automorphism group, I

Definition.

Let $K \leq \mathrm{Sym}(V)$ be a transitive group. A set $U \subset V$ is a block for K if for any permutation $k \in K$ we have

$$U^k \cap U \neq \emptyset \;\Rightarrow\; U^k = U.$$

The singletons and $U = V$ are the trivial blocks. The group K is primitive if each block is trivial; otherwise, K is imprimitive.

Circulant graphs with primitive automorphism group, I

Definition.

Let $K \leq \mathrm{Sym}(V)$ be a transitive group. A set $U \subset V$ is a block for K if for any permutation $k \in K$ we have

$$U^k \cap U \neq \emptyset \ \Rightarrow \ U^k = U.$$

The singletons and $U = V$ are the trivial blocks. The group K is primitive if each block is trivial; otherwise, K is imprimitive.

Theorem (Burnside-Schur).

Every primitive finite permutation group containing a regular cyclic subgroup is either 2-transitive or isomorphic to a subgroup of the affine group $\mathrm{AGL}_1(p)$ where p is a prime.

Circulant graphs with primitive automorphism group, II

Corollary.

Let Γ be a circulant graph on n vertices. Then the group $K = \mathrm{Aut}(\Gamma)$ is primitive if and only if one of the following statements holds:

- Γ is a complete or empty graph (and then $K = \mathrm{Sym}(n)$),
- Γ is neither complete nor empty, and $n = p$ is a prime number (and then $K < \mathrm{AGL}_1(p)$).

Circulant graphs with primitive automorphism group, II

Corollary.

Let Γ be a circulant graph on n vertices. Then the group $K = \mathrm{Aut}(\Gamma)$ is primitive if and only if one of the following statements holds:

- Γ is a complete or empty graph (and then $K = \mathrm{Sym}(n)$),
- Γ is neither complete nor empty, and $n = p$ is a prime number (and then $K < \mathrm{AGL}_1(p)$).

Algorithm. (Γ is a circulant graph with vertex set V.)

- If Γ is a complete or empty graph, then $K = \mathrm{Sym}(V)$.

Circulant graphs with primitive automorphism group, II

Corollary.

Let Γ be a circulant graph on n vertices. Then the group $K = \mathrm{Aut}(\Gamma)$ is primitive if and only if one of the following statements holds:

- Γ is a complete or empty graph (and then $K = \mathrm{Sym}(n)$),
- Γ is neither complete nor empty, and $n = p$ is a prime number (and then $K < \mathrm{AGL}_1(p)$).

Algorithm. (Γ is a circulant graph with vertex set V.)

- If Γ is a complete or empty graph, then $K = \mathrm{Sym}(V)$.
- Find a regular cyclic group $G \leq K$ and identify G with V.

Circulant graphs with primitive automorphism group, II

Corollary.

Let Γ be a circulant graph on n vertices. Then the group $K = \mathrm{Aut}(\Gamma)$ is primitive if and only if one of the following statements holds:

- Γ is a complete or empty graph (and then $K = \mathrm{Sym}(n)$),
- Γ is neither complete nor empty, and $n = p$ is a prime number (and then $K < \mathrm{AGL}_1(p)$).

Algorithm. (Γ is a circulant graph with vertex set V.)

- If Γ is a complete or empty graph, then $K = \mathrm{Sym}(V)$.
- Find a regular cyclic group $G \leq K$ and identify G with V.
- Now, $K = GK_0$ where $K_0 = \{k \in \mathrm{Aut}(G) : k \in \mathrm{Aut}(\Gamma)\}$.

Sections of a transitive group

Let $K \leq \mathrm{Sym}(V)$ be a transitive group,

Sections of a transitive group

Let $K \leq \mathrm{Sym}(V)$ be a transitive group,
$U \subset V$ a block for K,

Sections of a transitive group

Let $K \leq \mathrm{Sym}(V)$ be a transitive group,
$U \subset V$ a block for K,
$E \subset V \times V$ a K-invariant equivalence relation, and

Sections of a transitive group

Let $K \leq \mathrm{Sym}(V)$ be a transitive group,
$U \subset V$ a block for K,
$E \subset V \times V$ a K-invariant equivalence relation, and
$U/E := U/(U \times U) \cap E$.

Sections of a transitive group

Let $K \leq \mathrm{Sym}(V)$ be a transitive group,
$U \subset V$ a block for K,
$E \subset V \times V$ a K-invariant equivalence relation, and
$U/E := U/(U \times U) \cap E$.

Definition.

The group $K_{U/E} = \{k_{U/E} : \ k \in K_{\{U\}}\}$ where $k_{U/E}$ is the permutation of U/E induced by k, is called a section of K. In particular, $K_{U/E} \leq \mathrm{Sym}(U/E)$.

Sections of a transitive group

Let $K \leq \mathrm{Sym}(V)$ be a transitive group,
$U \subset V$ a block for K,
$E \subset V \times V$ a K-invariant equivalence relation, and
$U/E := U/(U \times U) \cap E$.

Definition.

The group $K_{U/E} = \{k_{U/E} : \; k \in K_{\{U\}}\}$ where $k_{U/E}$ is the permutation of U/E induced by k, is called a section of K. In particular, $K_{U/E} \leq \mathrm{Sym}(U/E)$.

Generally, $K = \mathrm{Aut}(\Gamma)$ does not imply that $K_{U/E}$ is the automorphism group of some graph.

Primitive sections of $K = \mathrm{Aut}(\Gamma)$ for a circulant graph Γ

Let G be a regular cyclic subgroup of $K \leq \mathrm{Sym}(V)$. Set

$$V' = U/E, \qquad G' = G_{V'}, \qquad K' = K_{V'}$$

where $U \subset V$ is a block for K and E a K-invariant equivalence relation.

Primitive sections of $K = \mathrm{Aut}(\Gamma)$ for a circulant graph Γ

Let G be a regular cyclic subgroup of $K \leq \mathrm{Sym}(V)$. Set

$$V' = U/E, \qquad G' = G_{V'}, \qquad K' = K_{V'}$$

where $U \subset V$ is a block for K and E a K-invariant equivalence relation.

Theorem.

Suppose that the section K' is primitive. Then exactly one of the following statements holds:

- $|V'| \geq 4$ and $K' = \mathrm{Sym}(V')$ (giant section),
- $|V'|$ is a prime and $G' \leq K' \leq G'K'_0$ where $K'_0 \leq \mathrm{Aut}(G')$ (normal section).

Primitive sections of $K = \mathrm{Aut}(\Gamma)$ for a circulant graph Γ

Let G be a regular cyclic subgroup of $K \leq \mathrm{Sym}(V)$. Set

$$V' = U/E, \qquad G' = G_{V'}, \qquad K' = K_{V'}$$

where $U \subset V$ is a block for K and E a K-invariant equivalence relation.

Theorem.

Suppose that the section K' is primitive. Then exactly one of the following statements holds:

- $|V'| \geq 4$ and $K' = \mathrm{Sym}(V')$ (giant section),
- $|V'|$ is a prime and $G' \leq K' \leq G'K'_0$ where $K'_0 \leq \mathrm{Aut}(G')$ (normal section).

Question. *Is it true that any non-abelian composition factor of K is an alternating group?*

Composition series of a circulant graph Γ

Using the association scheme theory one can construct in polynomial time a uniquely determined

composition series of Γ, i.e. the series of equivalence relations $E_i \subset V \times V$, $i = 0, \ldots, m$, such that

- $E_0 \subset E_1 \subset \cdots \subset E_m$,

Composition series of a circulant graph Γ

Using the association scheme theory one can construct in polynomial time a uniquely determined

composition series of Γ, i.e. the series of equivalence relations $E_i \subset V \times V$, $i = 0, \ldots, m$, such that

- $E_0 \subset E_1 \subset \cdots \subset E_m$,
- $|V/E_0| = |V|$ and $E_m = V \times V$,

Composition series of a circulant graph Γ

Using the association scheme theory one can construct in polynomial time a uniquely determined

composition series of Γ, i.e. the series of equivalence relations $E_i \subset V \times V$, $i = 0, \ldots, m$, such that

- $E_0 \subset E_1 \subset \cdots \subset E_m$,
- $|V/E_0| = |V|$ and $E_m = V \times V$,
- E_i is K-invariant, $i = 0, \ldots, m$,

Composition series of a circulant graph Γ

Using the association scheme theory one can construct in polynomial time a uniquely determined

composition series of Γ, i.e. the series of equivalence relations $E_i \subset V \times V$, $i = 0, \ldots, m$, such that

- $E_0 \subset E_1 \subset \cdots \subset E_m$,
- $|V/E_0| = |V|$ and $E_m = V \times V$,
- E_i is K-invariant, $i = 0, \ldots, m$,
- K_{X/E_i} is primitive, $X \in V/E_{i+1}$, $i = 0, \ldots, m-1$.

Composition series of a circulant graph Γ

Using the association scheme theory one can construct in polynomial time a uniquely determined

composition series of Γ, i.e. the series of equivalence relations $E_i \subset V \times V$, $i = 0, \ldots, m$, such that

- $E_0 \subset E_1 \subset \cdots \subset E_m$,
- $|V/E_0| = |V|$ and $E_m = V \times V$,
- E_i is K-invariant, $i = 0, \ldots, m$,
- K_{X/E_i} is primitive, $X \in V/E_{i+1}$, $i = 0, \ldots, m-1$.

Moreover, for all i and X one can test within the same time whether the section K_{X/E_i} is giant or normal.

Composition series of a circulant graph Γ

Using the association scheme theory one can construct in polynomial time a uniquely determined

composition series of Γ, i.e. the series of equivalence relations $E_i \subset V \times V$, $i = 0, \ldots, m$, such that

- $E_0 \subset E_1 \subset \cdots \subset E_m$,
- $|V/E_0| = |V|$ and $E_m = V \times V$,
- E_i is K-invariant, $i = 0, \ldots, m$,
- K_{X/E_i} is primitive, $X \in V/E_{i+1}$, $i = 0, \ldots, m-1$.

Moreover, for all i and X one can test within the same time whether the section K_{X/E_i} is giant or normal.

Let $\mathrm{gs}(\Gamma)$ be the number of giant sections in this series.

Case $\mathrm{gs}(\Gamma) > 0$

Suppose that there is a giant section

$$K' = K_{V'} = \mathrm{Sym}(V')$$

with $V' = X/E_i$ for some $i \in \{0, \ldots, m-1\}$ and $X \in V/E_{i+1}$.

Then one can find in polynomial time

- a set $S \subset K$ such that K' is generated by $\{s_{V'} : s \in S\}$,

Case $\mathrm{gs}(\Gamma) > 0$

Suppose that there is a giant section

$$K' = K_{V'} = \mathrm{Sym}(V')$$

with $V' = X/E_i$ for some $i \in \{0, \dots, m-1\}$ and $X \in V/E_{i+1}$.

Then one can find in polynomial time

- a set $S \subset K$ such that K' is generated by $\{s_{V'} : s \in S\}$,
- a circulant graph $\Gamma' = (V, E')$ with $\mathrm{gs}(\Gamma') < \mathrm{gs}(\Gamma)$,

Case $\mathrm{gs}(\Gamma) > 0$

Suppose that there is a giant section

$$K' = K_{V'} = \mathrm{Sym}(V')$$

with $V' = X/E_i$ for some $i \in \{0, \dots, m-1\}$ and $X \in V/E_{i+1}$.

Then one can find in polynomial time

- a set $S \subset K$ such that K' is generated by $\{s_{V'} : s \in S\}$,
- a circulant graph $\Gamma' = (V, E')$ with $\mathrm{gs}(\Gamma') < \mathrm{gs}(\Gamma)$,

such that

$$\mathrm{Aut}(\Gamma) = K = \mathrm{Aut}(\Gamma')\langle S\rangle.$$

Case $\mathrm{gs}(\Gamma) > 0$

Suppose that there is a giant section

$$K' = K_{V'} = \mathrm{Sym}(V')$$

with $V' = X/E_i$ for some $i \in \{0, \ldots, m-1\}$ and $X \in V/E_{i+1}$.

Then one can find in polynomial time

- a set $S \subset K$ such that K' is generated by $\{s_{V'} : s \in S\}$,
- a circulant graph $\Gamma' = (V, E')$ with $\mathrm{gs}(\Gamma') < \mathrm{gs}(\Gamma)$,

such that

$$\mathrm{Aut}(\Gamma) = K = \mathrm{Aut}(\Gamma')\langle S\rangle.$$

This reduces the problem to circulant graphs without giant sections.

Case $\mathrm{gs}(\Gamma) = 0$

Suppose that all the sections in the composition series are normal,

$$K_i \leq G_i \,\mathrm{Aut}(G_i) =: G^{(i)}, \qquad i = 0, \ldots, m-1$$

where $K_i = K_{U_{i+1}/E_i}$ and $G_i =_{U_{i+1}/E_i}$ with U_i being the class of E_i containing $1 \in G$. (We recall that G is identified with V).

Case $\mathrm{gs}(\Gamma) = 0$

Suppose that all the sections in the composition series are normal,

$$K_i \leq G_i \,\mathrm{Aut}(G_i) =: G^{(i)}, \qquad i = 0, \ldots, m-1$$

where $K_i = K_{U_{i+1}/E_i}$ and $G_i =_{U_{i+1}/E_i}$ with U_i being the class of E_i containing $1 \in G$. (We recall that G is identified with V).

Then

$$K \leq \mathrm{Wr}(K_1, \ldots, K_m) \leq \mathrm{Wr}(G^{(1)}, \ldots, G^{(m)}) := K^*$$

where $\mathrm{Wr}(\cdots)$ denotes the iterated wreath product in the imprimitive action (e.g. $\mathrm{Wr}(K_1, K_2, K_3) = (K_1 \wr K_2) \wr K_3$.)

Case $\mathrm{gs}(\Gamma) = 0$. Algorithm

Thus, given a circulant graph Γ with $\mathrm{gs}(\Gamma) = 0$ one can find in polynomial time a solvable group K^* such that

$$\mathrm{Aut}(\Gamma) = K \leq K^*.$$

Case $\mathrm{gs}(\Gamma) = 0$. Algorithm

Thus, given a circulant graph Γ with $\mathrm{gs}(\Gamma) = 0$ one can find in polynomial time a solvable group K^* such that

$$\mathrm{Aut}(\Gamma) = K \leq K^*.$$

Theorem (Babai-Luks, 1983).

Let $K^* \leq \mathrm{Sym}(V)$ be a solvable group. Then given a graph Γ with the vertex set V, a set of generators of the group $\mathrm{Aut}(\Gamma) \cap K^*$ can be found in time $n^{O(1)}$ where $n = |V|$.