On the isomorphism problem of Cayley graphs

Péter P. Pálfy
Alfréd Rényi Institute of Mathematics and
Eötvös University, Budapest, Hungary

Columbus, March **, 2010
I got my *candidate of science* degree in 1983.

Thesis title:  
*Group theoretical methods in combinatorics and universal algebra*

Informal supervisors: Ervin Fried and László Babai

From the Acknowledgements:  
“I am especially indebted to those who helped starting my research career:

Ervin Fried . . .

László Babai, whose continuous interest and encouragement helped me to overcome my laziness, and who taught me how to write mathematics papers.”
Circulant graphs

First chapter in my thesis:

*Isomorphism of circulant graphs — pronormal subgroups*

Ádám’s conjecture (1967): Two circulant graphs on $Z_n$ are isomorphic if and only if there is a $k$ coprime to $n$ such that the multiplication by $k$ modulo $n$ gives an isomorphism between the two graphs.


Final result: Muzychuk (1995, 1997) For undirected graphs Ádám’s conjecture is true in exactly the following cases:

$n = 2^j m$, where $m$ is an odd square-free number and $0 \leq j \leq 2$, or $n = 8, 9, 18$.

The density of this set is $7/\pi^2$. 
Cayley Isomorphism (CI) property

Generalization for arbitrary Cayley graphs

Babai (1977)

$G$ finite group, $S \subset G$ determine a **Cayley graph** $\text{Cay}(G, S)$ with vertex set $G$, where $(x, y)$ is an edge iff $yx^{-1} \in S$.

The right translations $x \mapsto xg$ are automorphisms of $\text{Cay}(G, S)$.

We assume $1 \notin S$ (no loops) and $S^{-1} = S$ (undirected edges).

**Definition.** $\text{Cay}(G, S)$ is a **CI-graph** if for every Cayley graph $\text{Cay}(G, T)$ which is isomorphic to $\text{Cay}(G, S)$ there is an automorphism $\alpha$ of the group $G$ which provides an isomorphism between the two Cayley graphs, that is $S^\alpha = T$.

$G$ is called a **CI-group** if every Cayley graph of $G$ is a CI-graph.
Generalization for arbitrary relational structures

Babai (1977) “concrete categories”

A relational structure on the base set $G$ is a **Cayley object** if the right translations $x \mapsto xg$ are all automorphisms of the structure. It is a **CI-object** if any isomorphic Cayley object can be obtained by applying an automorphism of the group $G$.

**Babai’s Lemma.** $\mathcal{R}$ is a CI-object iff

$$\varphi \rho G \varphi^{-1} \leq \text{Aut}(\mathcal{R}) \ (\varphi \in \text{Sym}(G)) \ \Rightarrow \ \exists \psi \in \text{Aut}(\mathcal{R}) : \ \varphi \rho G \varphi^{-1} = \psi \rho G \psi^{-1}.$$
Pronormal subgroups

Every Cayley object of $G$ is a CI-object iff any two regular permutation groups isomorphic to $G$ are conjugate inside the subgroup they generate. These are the so-called pronormal regular subgroups of the symmetric group.

$P^3$ (1987) The pronormal regular subgroups in symmetric groups are the following: cyclic groups of order $n$ with $(n, \varphi(n)) = 1$ and groups of order 4.

If the regular copy of a group $G$ is not pronormal in the symmetric group, then there is a relational structure with a single quaternary relation which is a Cayley object, but not a CI-object.
CI-graphs and CI-groups

Subgroups of CI-groups are CI-groups themselves.

Babai–Frankl (1979) The Sylow subgroups of CI-groups can be the following:
- elementary abelian $p$-groups ($Z_p^k$);
- $Z_4$, $Z_8$, $Q$;
- $Z_9$, ($Z_{27}$).

**Problem 1.** Which elementary abelian groups $Z_p^k$ are CI-groups?

$p = 2$: $Z_2^5$ is CI (Conder–Li, 1998), $Z_2^6$ is not CI (Nowitz, 1992)

$p$ odd: $Z_p^4$ is CI (Hirasaka–Muzychuk, 2001), $Z_p^k$ is not CI if $k = 2p - 1 + \binom{2p-1}{p}$ (Muzychuk, 2003), if $k = 4p - 2$ (Spiga, 2007), if $k = 2p + 3$ (Somlai, 2010+)
Structure of CI-groups

survey paper: Li (Discrete Mathematics, 2002)

CI-groups are solvable (Li, 1999)

severe structural restrictions (Li–Praeger, 1999; Li–Lu–Pálfy, 2007)

direct product of groups of pairwise coprime orders

Problem 2. If $G_1$ and $G_2$ are CI-groups of coprime order and none of them contains elements of order 8 or 9, is it true that $G_1 \times G_2$ is also a CI-group?

Dobson, 2002; Kovács–Muzychuk, 2009: $Z^2_p \times Z_q$
Li–Lu–P^3 (2007) If G is a coprime indecomposable CI-group, then G is one of the following:

\[ p \]-groups:
- elementary abelian \( p \)-groups \( \mathbb{Z}_p^k \),
- \( \mathbb{Z}_4, \mathbb{Z}_8, Q, \mathbb{Z}_9 \),

\( \{ p, q \} \)-groups:
- extension of an elementary abelian group \( \mathbb{Z}_p^k \) by a cyclic group of order \( n \) (\( n = 2, 3, 4 \) or 8), where the generator of the cyclic group acts on \( \mathbb{Z}_p^k \) as power automorphism \((x \mapsto x^r)\) of prime order,
- metabelian groups \( \mathbb{Z}_2^2 . \mathbb{Z}_3 = A_4, \mathbb{Z}_2^2 . \mathbb{Z}_9, \mathbb{Z}_9 . \mathbb{Z}_2 = D_9, \mathbb{Z}_9 . \mathbb{Z}_4 \).

The latter are CI-groups by the computer work of Conder–Li (1998)
Metabelian extensions

Let $E(p^k, n)$ be the extension of the elementary abelian group $Z_p^k$ by a cyclic group of order $n$ ($n = 2, 3, 4$ or $8$), where the generator of the cyclic group acts on $Z_p^k$ as power automorphism ($x \mapsto x^r$) of prime order (e.g., $r = -1$, if $n = 2, 4$ or $8$).

**Problem 3.** Is $E(p^k, n)$ a CI-group provided $Z_p^k$ is a CI-group?

True if the elementary abelian normal subgroup is just cyclic, $Z_p$:
- $n = 2$: Babai (1972)
- $n = 3$: Babai–Frankl (1979)
- $n = 4, 8$: Li–Lu–P$^3$ (2007)

Moreover, true for $E(3^2, 2)$ (Conder–Li, 1998)
Happy Birthday, Laci!

I wish you new discoveries, excellent students, and good health.