Generalised dihedral CI-groups

M. Muzychuk (joint work with E. Dobson and P. Spiga)

Ben-Gurion University of the Negev,
Israel

Webinar "Algebraic Graph Theory"
29 March, 2022, Bratislava, Slovakia

Cayley digraphs

Definition

Let $S \subseteq H$ be a subset of a finite group H. A Cayley digraph $\mathrm{Cay}(H,S)$ has H as a vertex set; two vertices $x, y \in H$ are connected iff $xy^{-1} \in S$.

1. $\mathrm{Cay}(H,S)$ is connected $\iff \langle S \rangle = H$;
2. $\mathrm{Cay}(H,S)$ is undirected $\iff S^{-1} = S$;
3. $\mathrm{Aut}(\mathrm{Cay}(H,S))$ contains H_R.

Isomorphism problem for Cayley graphs

Given two Cayley digraphs $\mathrm{Cay}(H,S)$ and $\mathrm{Cay}(H,T)$, decide whether or not $\mathrm{Cay}(H,S) \cong \mathrm{Cay}(H,T)$.

Two Cayley graphs $\mathrm{Cay}(H,S)$ and $\mathrm{Cay}(H,T)$ are Cayley isomorphic iff

$$\exists \varphi \in \mathrm{Aut}(H) : \mathrm{Cay}(H,S)^{\varphi} = \mathrm{Cay}(H,T) \iff S^{\varphi} = T.$$

CI-property (L. Babai, 1976)

Definition

A Cayley (di)graph $\mathrm{Cay}(H, S)$ has a Cayley Isomorphism property (CI-property for short) iff

$$\forall_{T \subseteq H}\ \mathrm{Cay}(H, T) \cong \mathrm{Cay}(H, S) \iff \exists_{\varphi \in \mathrm{Aut}(H)}\ T = S^{\varphi}. \tag{1}$$

H is a DCI-group if every subset S has CI-property.
H is a CI-group if every symmetric subset S has CI-property.
H is a $\mathrm{CI}^{(2)}$-group if it has CI-property for all colored Cayley digraphs over H.

$$\mathrm{CI}^{(2)} - \text{property} \implies \text{DCI-property} \implies \text{CI-property}$$

Problem (L. Babai & P. Frankl, 1976)

Which are the CI-groups?

Isomorphism problem for circulant graphs

Ádám's conjecture (1967): $\mathbb{Z}_n$ is a CI-group for every n

$\mathrm{Cay}(\mathbb{Z}_n, S) \cong \mathrm{Cay}(\mathbb{Z}_n, T) \iff \exists_{m \in \mathbb{Z}_n^*} T = mS.$

Theorem (Alspach & Parsons and Egorov & Markov, 1970)

Ádám's conjecture for digraphs fails if n is divisible by 8 or by an odd square.

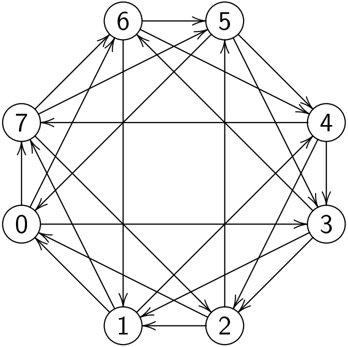
Ádám's conjecture is true if

1. n is a prime - Elspas & Turner, 1970;
2. $n = 2p, 3p, 4p$ - Babai 1977;
3. $n = pq, p \neq q$ are primes - C. Godsil (1977), Klin & Pöschel (1978), Alspach & Parsons (1979)

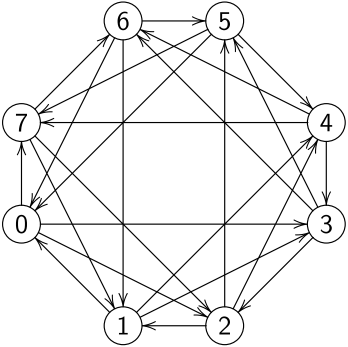
Example: $\mathbb{Z}_8$

Proposition (Elspas and Turner, 1970)

$\mathbb{Z}_8$ is not a DCI-group .



$\mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 5\})$



$\mathrm{Cay}(\mathbb{Z}_8, \{1, 6, 5\})$

$$\mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 5\})^{(2,6)(3,7)} = \mathrm{Cay}(\mathbb{Z}_8, \{1, 6, 5\}) \ .$$

Example: $\mathbb{Z}_8$

Proposition

$\mathbb{Z}_8$ is a CI-group .

Proof.

Let $\Gamma = \mathrm{Cay}(\mathbb{Z}_8, S) \cong \Gamma' = \mathrm{Cay}(\mathbb{Z}_8, S')$. Then $|S| = |S'|$ and S, S' are unions of (some of) $S_1 = \{\pm 1\}, S_2 = \{\pm 2\}, S_3 = \{\pm 3\}, S_4 = \{4\}$.
W.l.o.g. $|S| = |S'| \leq 3$.
If $\Gamma \cong \Gamma'$ is connected then either $S = S_i, S' = S_{i'}$ or $S = S_i \cup S_4, S' = S_{i'} \cup S_4$ where $i, i' \in \{1, 3\}$. In both cases $\Gamma \cong_{Cayley} \Gamma'$.
If Γ is disconnected, then S, S' is one of the sets $\emptyset, S_2, S_4, S_2 \cup S_4$. In this case $|S| = |S'| \implies S = S'$.■ □

Corollary

CI-property $\not\Rightarrow$ DCI-property.

Necessary conditions for being a CI-group

After 45 years of intense research we do not have a complete answer to the above question. The necessary and sufficient conditions formulated below accumulate the results of L.Babai, P.Frankl, B. Alspach, T.D. Parsons, V.N.Egorov, A.I.Markov C.H.Li, M. Klin, R. Pöschel, P.Spiga, E.Dobson, M.E. Muzychuk, J. Morris, I. Kovacs, G. Ryabov, G. Somlai, M.Conder, C.E.Praeger, Z.P. Lu, P.P. Pálfy, Y.-Q. Feng, M.Y.Xu.

Necessary conditions for being a CI-group

Theorem

Let H be a CI-group. Then

1. If H has an element of order 9, then H is one of the following groups $D_{18}, Dic_{36}, \mathbb{Z}_2^2 \rtimes \mathbb{Z}_9, \mathbb{Z}_2^n \times \mathbb{Z}_9, n \leq 5$.
2. If H has an element of order 8, then $H \cong D(M,8)$ or $H \cong \mathbb{Z}_8$.
3. If H has no elements of orders $8, 9$, then H is a coprime direct product of groups from the following list:
   $\mathbb{Z}_p^r, r < 2p+3, \mathbb{Z}_4, D(M,2), D(M,3), D(M,4), Q_8, A_4$.

Here M is a direct product of elementary abelian groups;
$D(M,n) = M \rtimes \langle y \rangle, o(y) = n \in \{1,2,3,4,8\}$ where
$\gcd(n,|M|) = 1$ and $m^y = m^{-1}$ if $o(y) \neq 3$.

Necessary conditions for being a DCI-group

Theorem

Let H be a DCI-group. Then H is a coprime direct product of groups from the following list:

$$\mathbb{Z}_p^r, r < 2p+3, \mathbb{Z}_4, D(M,2), D(M,4), Q_8, A_4.$$

Sufficient conditions to be a DCI-group

Abelian DCI-groups

1. $\mathbb{Z}_4$ is a DCI-group;
2. An elementary abelian group of rank at most 5 is a DCI-group;
3. $\mathbb{Z}_2^r$ is DCI-group $\iff r \leq 5$;

We do not know whether $\mathbb{Z}_3^6, \mathbb{Z}_3^7$ are (D)CI-groups;
Problem. Find smallest $r(p)$ s.t. $\mathbb{Z}_p^{r(p)}$ is not a DCI-group.
$r(p) \leq 2p + 3$.

Non-abelian DCI-groups

1. Q_8 and A_4 are DCI-groups;
2. $D(\mathbb{Z}_n, 2), D(\mathbb{Z}_n, 4)$ are DCI-groups if $(n, \varphi(n)) = 1$ + extra arithmetical conditions on n.

Sufficient conditions to be a DCI-group

Conjecture (Kovacs & MM, 2009)

If A and B are DCI-groups of coprime orders, then $A \times B$ is a DCI-group.

The conjecture was proven to be true in the following cases:

1. A is cyclic of s.f. order or $\mathbb{Z}_4$ and B is cyclic of s.f. order;
2. A is cyclic of prime order and B is elementary abelian of rank at most 4;
3. $A = \mathbb{Z}_p^2$ and B is cyclic of a s.f. order;
4. $A = \mathbb{Z}_p^2$ and $B = \mathbb{Z}_q^2$;
5. $A = Q_8$ and B is of prime order;
6. A and B are products of elementary abelian groups s.t. $\pi(\mathrm{Hol}(A)) \cap \pi(B) = \emptyset$ and $\pi(\mathrm{Hol}(B)) \cap \pi(A) = \emptyset$.

Theorem (Dobson, 2018)

The conjecture is not true for CI-groups.

Main Result

Theorem (E. Dobson, P. Spiga, M. M. (2020))

If $D(M, n), n \in \{2, 4, 8\}$ is a CI-group, then for each prime $p \mid |M|$ a Sylow p-subgroup has order p or 9 (if $p = 3$). If $D(M, n)$ is a DCI-group, then, in addition, $n \neq 8$ and the Sylow 3-subgroup has order 3.

Remark. The group $D(\mathbb{Z}_3^2, 2)$ has a CI-property but has not a DCI-property.

Outline of the proof

Theorem (L. Babai, P. Frankl, 1976)

A subgroup of a (D)CI-group has (D)CI-property too.

Theorem (E. Dobson, J. Morris, 2015)

A quotient of a D(CI)-group is (D)CI-group too.

Theorem (E. Dobson, P. Spiga, M. M. (2020))

Let $p > 2$ be a prime. If $D(\mathbb{Z}_p^r, 2)$ is a CI-group, then $r = 1$ if $p > 3$ and $r = 1, 2$ for $p = 3$. If $D(\mathbb{Z}_p^r, 2)$ is a DCI-group, then $r = 1$.

Theorem (L. Babai, 1977)

The group $D(\mathbb{Z}_p, 2) \cong D_{2p}$ is a $\mathrm{CI}^{(2)}$-group.

How to check a CI-property for a given group H

The automorphism group $\mathrm{Aut}(\mathrm{Cay}(H,S))$ always contains a subgroup $H_R = \{h_R \mid h \in H\}$ where $x^{h_R} = xh, x \in H$,

Theorem (Babai, 1976)

A graph $\mathrm{Cay}(H,S), S \subseteq H$ has (D)CI-property iff any H-regular subgroup of $\mathrm{Aut}(\mathrm{Cay}(H,S))$ is conjugate to H_R.

Find all possible $\mathrm{Aut}(\mathrm{Cay}(H,S)), S \subseteq H$ and apply Babai's criterion.
Find all 2-closed overgroups of H_R and check which of them have more than one class of H-regular subgroups.

Definition

A subgroup $G \leq \mathrm{Sym}(\Omega)$ is 2-closed iff it is the full automorphism group of a colored graph on Ω.

The group and its action

Let $\mathbb{F}_p, p > 2$ be a prime field. In what follows $x, y, z \in \mathbb{F}_p$ and $a, b, c \in \{\pm 1\} \leq \mathbb{F}_p^*$. Define

$$G := \left\{ \begin{pmatrix} a & x & z \\ 0 & b & y \\ 0 & 0 & c \end{pmatrix} \middle| \, abc = 1 \right\}, D := \left\{ \begin{pmatrix} a & ax & \frac{ax^2}{2} \\ 0 & 1 & x \\ 0 & 0 & a \end{pmatrix} \right\},$$

$$H := \left\{ \begin{pmatrix} a & 0 & z \\ 0 & a & y \\ 0 & 0 & 1 \end{pmatrix} \right\}, K := \left\{ \begin{pmatrix} 1 & x & z \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} \right\},$$

Proposition

$D \cong D_{2p}$ and the action of G on $\Omega := \{Dg \mid g \in G\}$ is faithful.

The regular subgroups

Proposition

1. $H \cong K \cong \mathrm{Dih}(\mathbb{Z}_p^2) = D(\mathbb{Z}_p^2, 2)$;
2. $H, K \trianglelefteq G$;
3. $D \cap H = D \cap K = 1$;
4. $DH = DK = G \Rightarrow H$ and K act regularly on Ω.

We identify Ω with H via $h \mapsto Dh$. Under this identification H acts as H_R and D acts via $h \mapsto h^d = d^{-1}hd$. Abbreviate

$$[a,(x,y)] := \begin{pmatrix} a & 0 & x \\ 0 & a & y \\ 0 & 0 & 1 \end{pmatrix} \in H, [a,z] := \begin{pmatrix} a & az & a\frac{z^2}{2} \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \in D$$

The suborbits

Thus the group $G = DH = HD$ acts on H as follows

$$[a,(x,y)]^{[b,(u,v)]} = [a,(x,y)] \cdot [b,(u,v)] = [ab,(xb+u, yb+v)]$$

$$[a,(x,y)]^{[b,z]} = \left[a, (-bzy + x, by) + (1-a)(z^2/2, -z)\right].$$

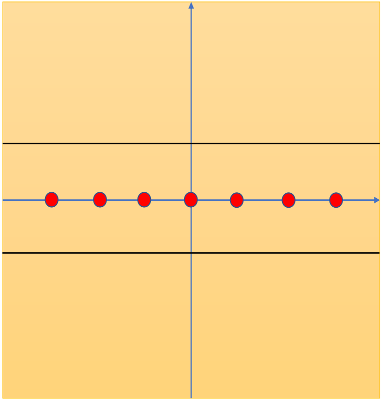
The point stabilizer $G_e = D$ has the following orbits:

1. singletons - $S_t = \{[1,(t,0)]\}$;
2. pair of horizontal lines - $L_t \cup L_{-t}$, where $L_t = \{[1,(z,t) \mid z \in \mathbb{F}\}$;
3. parabolas - $P_t = \{[-1,(t+z^2, 2z) \mid z \in \mathbb{F}\}$.

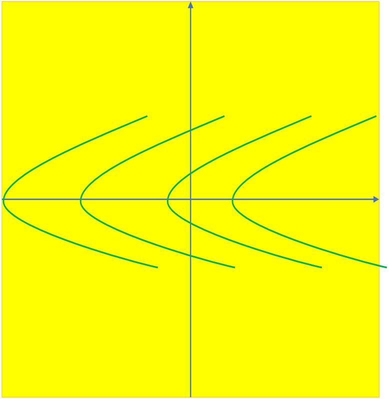
Every 2-orbit of G is a Cayley graph $\mathrm{Cay}(H,S)$ where S is one of the above D-orbits $\implies G \leq \bigcap_S \mathrm{Aut}(\mathrm{Cay}(H,S)) =: G^{(2)}$.

The suborbits

$[1, \mathbf{Z}_p^2]$



$[-1, \mathbf{Z}_p^2]$



The action (G, H) is 2-closed, i.e. $G^{(2)} = G$

- The action of $G_e^{(2)}$ on P_0 is faithful;
- The induced subgraph $\mathrm{Cay}(H, L_1 \cup L_{-1})_{P_0}$ is a cycle of length p.

Corollary

H is not $CI^{(2)}$-group.

Theorem

If $p \geq 5$, then there exists a symmetric union T of suborbits such that $\mathrm{Aut}(\mathrm{Cay}(H, T)) = G$. If $p = 3$ then there exists a non-symmetric T such that $\mathrm{Aut}(\mathrm{Cay}(H, T)) = G$. Any symmetric subset of $Dih(\mathbb{Z}_3^2)$ has CI-property. The group $Dih(\mathbb{Z}_3^3)$ contains a symmetric non-CI subset.

CI-property for k-ary relational Cayley structures

Definition

Given a group H, a tuple $\mathcal{R} = (R_1, R_2, ..., R_m), R_i \subseteq H^{k_i}$ of relations defined on a group H is called a relational Cayley structure over $H \iff$ every R_i is H_R-invariant. The arity of $\mathcal{R}$ is defined as $\max\{k_i\}_{i=1}^{m}$.

Definition

A group H has a CI-property w.r.t k-ary relational structures if any two H-invariant k-ary structures are isomorphic iff they are Cayley isomorphic.

Proposition

If H has a $\mathrm{CI}^{(k+1)}$-property, then it has a $\mathrm{CI}^{(k)}$-property.

Palfy's Theorem

Theorem (Palfy, 1987)

A group H has a $\mathrm{CI}^{(k)}$-property for every $k \in \mathbb{N}$ iff
$H \cong \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_n$ where $(n, \varphi(n)) = 1$.

$\mathrm{CI}^{(4)}$-property

The groups mentioned above are the only groups which have a $\mathrm{CI}^{(4)}$-property.

Open Problem

Classify all $\mathrm{CI}^{(3)}$-groups.

Towards a classification of $\mathrm{CI}^{(3)}$-groups

Theorem (Babai, 1977)

A dihedral group $D_{2p}, p > 2$ a prime is a $\mathrm{CI}^{(3)}$-group.

Theorem (Dobson (2003), Dobson & Spiga (2013))

If G is a CI-group with respect to color ternary relational structures, then $G = U \times V, \gcd(|U|, |V|) = 1$ where

1. U is cyclic of odd order ℓ;
2. $V \in \{\mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_2^2, Q_8, \mathbb{Z}_2^3, \mathbb{Z}_2^4, D(\mathbb{Z}_m, 2), D(\mathbb{Z}_m, 4)\}$, m is odd;
3. $\gcd(m\ell, \varphi(m\ell)) = 1$;
4. if $G_2 \cong \mathbb{Z}_4, Q_8$, then every prime $p \mid \ell$ satisfies $p \equiv 3 \pmod 4$;
5. $m\ell$ is coprime with $|\mathrm{Aut}(G_2)|$.

Necessary conditions for being a $\mathrm{CI}^{(3)}$-group

Theorem (Dobcon, MM, Spiga 2021)

If $\exp(G_2) = 4$ then every prime divisor $p \mid m$ satisfies $p \equiv 3 (\mathrm{mod}\ 4)$.

Theorem

If G is a CI-group with respect to color ternary relational structures, then $n := |G_{2'}|$ satisfies $\gcd(n, \varphi(n)) = 1$ and

1. $G \cong \mathbb{Z}_n \times G_2$, $G_2 \in \{\mathbb{Z}_2^r, Q_8\}$, $r \leq 4$, with $\gcd(|\mathrm{Aut}(G_2)|, n) = 1$;
2. $G \cong \mathbb{Z}_{n/m} \times D(\mathbb{Z}_m, 2)$;
3. $G \cong \mathbb{Z}_n \times \mathbb{Z}_4$ or $G \cong \mathbb{Z}_{n/m} \times D(\mathbb{Z}_m, 4)$ where every prime $p \mid n$ satisfies $p \equiv 3 (\mathrm{mod}\ 4)$.

Sufficient conditions for being a $\mathrm{CI}^{(3)}$-group

Theorem (Dobson, 2003)

Let n satisfy $\gcd(n, \varphi(n)) = 1$. Then $\mathbb{Z}_{2n}$ is a $\mathrm{CI}^{(3)}$-group. The group $\mathbb{Z}_{4n}$ is $\mathrm{CI}^{(3)}$-group if and only if every prime $p \mid n$ satisfies $p \equiv 3 \pmod 4$.

Theorem (Dobson, MM, Spiga 2021)

Let n satisfy $\gcd(n, \varphi(n)) = 1$. Then

1. $\mathbb{Z}_{n/m} \times D(\mathbb{Z}_m, 2)$ is a $\mathrm{CI}^{(3)}$-group,and, therefore, a $\mathrm{CI}^{(2)}$-group;
2. if $3 \nmid n$, then $\mathbb{Z}_{n/m} \times D(\mathbb{Z}_m, 4)$ is a $\mathrm{CI}^{(3)}$-group if and only if every prime $p \mid n$ satisfies $p \equiv 3 \pmod 4$;
3. $D(\mathbb{Z}_3, 4)$ is a $\mathrm{CI}^{(3)}$-group;
4. if $3 \nmid n$, then $\mathbb{Z}_{n/m} \times D(\mathbb{Z}_m, 4)$ is a $\mathrm{CI}^{(2)}$-group;

Thank you!