Cayley graphs of order kp are hamiltonian for $k < 48$

Dave Witte Morris
University of Lethbridge, Alberta, Canada
http://people.uleth.ca/~dave.morris
Dave.Morris@uleth.ca

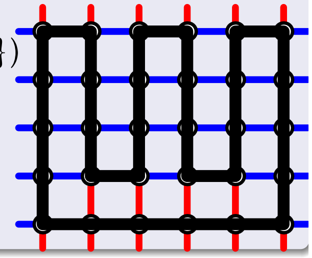
Abstract. For every generating set S of any finite group G, there is a corresponding Cayley graph $\mathrm{Cay}(G;S)$. It was conjectured in the early 1970's that $\mathrm{Cay}(G;S)$ always has a hamiltonian cycle, but there has been very little progress on this problem. Joint work with Kirsten Wilk has established the conjecture in the special case where the order of G is kp, with $k < 48$ and p prime. This was not previously known for values of k in the set $\{24, 32, 36, 40, 42, 45\}$.

Example

Cayley graph
$\mathrm{Cay}(\mathbb{Z}_m \oplus \mathbb{Z}_n; \{\pm(1,0), \pm(0,1)\})$

vertices: elements of $\mathbb{Z}_m \oplus \mathbb{Z}_n$
edges: $v — v \pm (1,0)$
and $v — v \pm (0,1)$

has hamiltonian cycle



Defn. $\mathrm{Cay}(G;S)$ for group G and $S \subseteq G$ with $S = S^{-1}$
vertices = elt's of G edge $v — vs$ for $v \in G$, $s \in S$
(assume **connected**, i.e., $\langle S \rangle = G$)

Exercise

G abelian $\Rightarrow \forall S$, $\mathrm{Cay}(G;S)$ has a hamiltonian cycle.

Exercise

G abelian $\Rightarrow \forall S$, $\mathrm{Cay}(G;S)$ has a hamiltonian cycle.

Open question (~1970)

¿Every connected Cayley graph has a hamiltonian cycle?

Recall. commutator subgroup $G' = \langle\, ghg^{-1}h^{-1} \mid g,h \in G \,\rangle$.
G abelian $\Leftrightarrow G' = \{e\} \Leftrightarrow |G'| = 1$.

Theorem (Marušič, Durnberger, Keating-Witte, 1985)

$\mathrm{Cay}(G;S)$ *has a ham cycle if* $|G'| = p$ (*prime*).

Work in progress. $\exists$ ham cyc if $|G'| = pq$. ($p \neq q$)

✓ G nilpotent [E. Ghaderpour & D. Morris]
✓ $|G|$ odd [D. Morris]
✓ $p = 2$ [D. Morris]

Open question (~1970)

¿Every connected Cayley graph has a hamiltonian cycle?

Theorem (2011–2013)

$\mathrm{Cay}(G;S)$ *has ham cycle if* $|G| = kp$
with p *prime and* $24 \neq k < 32$.
[Marušič, Kutnar, Šparl, Morris[2], Curran, Ghaderpour, Jungreis-Friedman (~1990)]

Theorem (D. Morris & K. Wilk, 2018⁺)

$\mathrm{Cay}(G;S)$ *has ham cycle if* $|G| = kp$ *with* $k < 48$.

Theorem (D. Morris & K. Wilk, 2018⁺)

$\mathrm{Cay}(G;S)$ *has ham cycle if* $|G| = kp$ *with* $k < 48$.

For fixed p:

- only finitely many values of kp ($1 \leq k < 48$)
- only finitely many groups G of order kp:
  gap has a list (e.g., order less than 1024)
- only finitely many Cayley graphs of G:
  gap code in Brandon Fuller's thesis
  (irredundant S up to $\mathrm{Aut}(G)$)
  (feasible up to order a few hundred)

Find ham cyc in each one by computer (LKH).
For ~100 vertices, typically less than a second.
(LKH can be applied to graphs with tens of thousands of vertices)

Theorem (D. Morris & K. Wilk, 2018⁺)

$\mathrm{Cay}(G;S)$ *has ham cycle if* $|G| = kp$ *with* $k < 48$.

Computer (LKH) deals with any finite set of primes so we may assume p is large: $p > k$.

Example (direct product)

Take any group $\overline{G}$ of order k.
Then $G = \mathbb{Z}_p \times \overline{G}$ is a group of order kp:
$(z_1, h_1) * (z_2, h_2) = (z_1 + z_2, h_1 h_2)$

Example (semidirect product)

Choose homomorphism $\tau \colon \overline{G} \to \mathbb{Z}_p^*$.
Then $G = \mathbb{Z}_p \rtimes_\tau \overline{G}$ is a group of order kp:
$(z_1, h_1) * (z_2, h_2) = (z_1 + \tau(h_1)\, z_2, h_1 h_2)$

Example (semidirect product)

$|\overline{G}| = k$ and homomorphism $\tau\colon \overline{G} \to \mathbb{Z}_p^*$.

Then $G = \mathbb{Z}_p \rtimes_\tau \overline{G}$ is a group of order kp:

$(z_1, h_1) * (z_2, h_2) = (z_1 + \tau(h_1)\, z_2, h_1 h_2)$

Lemma (well known)

Every grp of order kp is a semidirect prod. $(p > k)$

Sylow's Theorem

- G has a subgroup $\mathbb{Z}_p$ of order p
- # conjugates of $\mathbb{Z}_p$ is $\equiv 1 \pmod{p}$ (& divides kp)

So # conjugates = 1. Therefore $\mathbb{Z}_p \triangleleft G$.

Schur-Zassenhaus Theorem

$N \triangleleft G$, $\gcd(|N|, |G/N|) = 1 \Rightarrow G \cong N \rtimes_\tau (G/N)$

(For $N = \mathbb{Z}_p$: $H^2(G/\mathbb{Z}_p, \mathbb{Z}_p) = 0$.)

Theorem (D. Morris & K. Wilk, 2018+)

Cay$(G;S)$ *has ham cycle if* $|G| = kp$ *with* $k < 48$.

∞ possibilities for Cay$(G;S)$ (order kp)

but only finitely many for Cay$(\overline{G};\overline{S})$. (order k)

Lift hamiltonian cycles in Cay$(\overline{G};\overline{S})$ to Cay$(G;S)$.

Recall $v - vs$ for $s \in S$.

Ham cyc = list $(s_1, \ldots, s_n)$ of elements of S such that

$e \xrightarrow{s_1} s_1 \xrightarrow{s_2} s_1 s_2 \xrightarrow{s_3} s_1 s_2 s_3 \xrightarrow{s_4} \ldots \xrightarrow{s_n} s_1 s_2 \cdots s_n$

is list of all elements of G (with $s_1 s_2 \cdots s_n = e$).

Lemma (Factor Group Lemma)

Given Cay$(G;S)$,

let $\overline{C} = (\overline{s_1}, \ldots, \overline{s_n})$ *be a ham cyc in* Cay$(\overline{G};\overline{S})$.

Then $\overline{s_1 s_2 \cdots s_n} = \overline{e}$, *so* $\pi_S \overline{C} := s_1 s_2 \cdots s_n \in \mathbb{Z}_p$.

If $\pi_S \overline{C} \neq 0$, *then* Cay$(G;S)$ *has a ham cyc.*

Proof. Let $z = \pi_S \overline{C}$.

$e \xrightarrow{s_1} g_1 \xrightarrow{s_2} g_2 \xrightarrow{s_3} \ldots \xrightarrow{s_{n-1}} g_{n-1}$ hits cosets of $\mathbb{Z}_p$

$\xrightarrow{s_n} z \xrightarrow{s_1} zg_1 \xrightarrow{s_2} zg_2 \xrightarrow{s_3} \ldots \xrightarrow{s_{n-1}} zg_{n-1}$

$\xrightarrow{s_n} z^2 \xrightarrow{s_1} z^2 g_1 \xrightarrow{s_2} z^2 g_2 \xrightarrow{s_3} \ldots \xrightarrow{s_{n-1}} z^2 g_{n-1}$

$\vdots$

$\xrightarrow{s_n} z^{p-1} \xrightarrow{s_1} z^{p-1} g_1 \xrightarrow{s_2} z^{p-1} g_2 \xrightarrow{s_3} \ldots \xrightarrow{s_{n-1}} z^{p-1} g_{n-1}$

$\xrightarrow{s_n} z^p = e$ hits all elements of G

Lemma (Factor Group Lemma)

Given Cay$(G;S)$,

let $\overline{C} = (\overline{s_1}, \ldots, \overline{s_n})$ *be a ham cyc in* Cay$(\overline{G};\overline{S})$.

Then $\overline{s_1 s_2 \cdots s_n} = \overline{e}$, *so* $\pi_S \overline{C} := s_1 s_2 \cdots s_n \in \mathbb{Z}_p$.

If $\pi_S \overline{C} \neq 0$, *then* Cay$(G;S)$ *has a ham cyc.*

Let's assume $G = \mathbb{Z}_p \times \overline{G}$.

Corollary

$\overline{S} = \{\overline{s}_1, \ldots, \overline{s}_r\}$. *Ham cycs* $\overline{C}_1, \ldots, \overline{C}_r$ *in* Cay$(\overline{G};\overline{S})$.

If $p \nmid \det[\#_{\overline{s}_i} \overline{C}_j]$, *then* Cay$(G;S)$ *has a ham cyc.*

Corollary

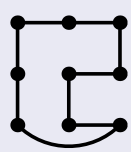
$\overline{S} = \{\overline{s}_1^{\pm 1}, \ldots, \overline{s}_r^{\pm 1}\}$. *Ham cycs* $\overline{C}_1, \ldots, \overline{C}_r$ *in* Cay$(\overline{G};\overline{S})$.

If $p \nmid \det[\#_{\overline{s}_i} \overline{C}_j]$, *then* Cay$(G;S)$ *has a ham cyc.*

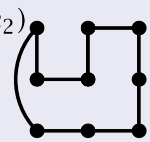
Example

Cay$(\overline{G};\overline{S})$ = Cay$(\mathbb{Z}_3 \times \mathbb{Z}_3; \{\pm e_1, \pm e_2\})$.

- $\overline{C}_1 = (e_2, e_2, e_1, e_1, -e_2, -e_1, -e_2, e_1, e_1)$
  $\#_{e_1} \overline{C}_1 = 2 - 1 + 2 = 3$,
  $\#_{e_2} \overline{C}_1 = 2 - 1 - 1 = 0$.



- $\overline{C}_2 = (e_1, e_1, e_2, e_2, -e_1, -e_2, -e_1, e_2, e_2)$
  $\#_{e_1} \overline{C}_2 = 2 - 1 - 1 = 0$,
  $\#_{e_2} \overline{C}_2 = 2 - 1 + 2 = 3$.



$\det[\#_{e_i} \overline{C}_j] = \det \begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix} = 9$. So $\exists$ ham cyc if $p \neq 3$.

Corollary

$\overline{S} = \{\overline{s}_1^{\pm 1}, \ldots, \overline{s}_r^{\pm 1}\}$. *Ham cycs* $\overline{C}_1, \ldots, \overline{C}_r$ *in* Cay$(\overline{G};\overline{S})$.

If $p \nmid \det[\#_{\overline{s}_i} \overline{C}_j]$, *then* Cay$(G;S)$ *has a ham cyc.*

Theorem (D. Morris & K. Wilk, 2018+)

Cay$(G;S)$ *has ham cycle if* $|G| = kp$ *with* $k < 48$.

Method of proof.

For each $k < 48$, group $\overline{G}$ of order k, gen set $\overline{S}$ of $\overline{G}$:

find $\overline{C}_1, \ldots, \overline{C}_r$ in Cay$(\overline{G};\overline{S})$, such that

$\det[\#_{\overline{s}_i} \overline{C}_j] \neq 0$. (exhaustive search, not LKH)

Cor provides ham cyc in Cay$(\mathbb{Z}_p \times \overline{G}; S)$ if $p \nmid$ det.

Otherwise (finitely many), apply LKH to $\mathbb{Z}_p \times \overline{G}$. □

How to handle semidirect products

Suppose G is not a direct product: $G = \mathbb{Z}_p \rtimes_\tau \overline{G}$.

$(z_1, h_1) * (z_2, h_2) = (z_1 + \tau(h_1)\, z_2, h_1 h_2)$

Lift $\tau \colon \overline{G} \to \mathbb{Z}_p^*$ to character $\widetilde{\tau} \colon \overline{G} \to \mu_{p-1}$.

Count $\#^{\tau}_{\overline{s}_i} \overline{C}_j$ is weighted by values of $\widetilde{\tau}$.

$\det[\#^{\tau}_{\overline{s}_i} \overline{C}_j]$ is an algebraic integer.
Need p not to divide the **norm** of the determinant.

If $p \mid \mathrm{Norm}(\det)$ (only finitely many),
apply LKH to $\mathbb{Z}_p \rtimes_\tau \overline{G}$.

- D. W. Morris and K. Wilk: Cayley graphs of order kp are hamiltonian for $k < 48$, *Art of Discrete and Applied Mathematics* (to appear). `https://arxiv.org/abs/1805.00149`
- K. Helsgaun: LKH – an effective implementation of the Lin-Kernighan heuristic (version 2.0.7), 2012. `http://www.akira.ruc.dk/~keld/research/LKH/`
- The GAP Group: GAP – Groups, Algorithms, and Programming. `https://www.gap-system.org`