Some results on Cayley graphs

Elena Konstantinova

Sobolev Institute of Mathematics, Novosibirsk, Russia
e_konsta@math.nsc.ru

Conference on Vertex Operator Algebra and Related Topics

24–27 August, 2012, Shanghai Jiao Tong University

Cayley graphs

Let G be a group, and let $S \subset G$ be a set of group elements as a set of generators for a group such that $e \notin S$ and $S = S^{-1}$.

Definition

In the Cayley graph $\Gamma = Cay(G, S) = (V, E)$ vertices correspond to the elements of the group, i.e. $V = G$, and edges correspond to the action of the generators, i.e. $E = \{(g, gs) : g \in G, s \in S\}$.

The definition of Cayley graph was introduced by A. Cayley in 1878 to explain the concept of abstract groups which are generated by a set of generators in Cayley's time.

Properties

(i) Γ is a connected regular graph of degree $|S|$;
(ii) Γ is a vertex–transitive graph.

Some families of Cayley graphs

The complete graph K_n

is the Cayley graph for the additive group $\mathbb{Z}_n$ of integers modulo n whose generating set is the set of all non–zero elements of $\mathbb{Z}_n$.

The circulant

is the Cayley graph $Cay(\mathbb{Z}_n, S)$ where $S \subset \mathbb{Z}_n$ is an arbitrary generating set. The most prominent example is the cycle C_n.

The Pancake graph P_n

is the Cayley graph on the symmetric group Sym_n with generating set $\{r_i \in Sym_n, 1 \leqslant i < n\}$, where r_i is the operation of reversing the order of any substring $[1, i]$, $1 < i \leqslant n$, of a permutation π when multiplied on the right, i.e., $[\pi_1, \ldots, \pi_i, \pi_{i+1}, \ldots, \pi_n]r_i = [\pi_i, \ldots, \pi_1, \pi_{i+1}, \ldots, \pi_n]$.

P_n is well–known because of the Pancake problem (still open!)

Problems on Cayley graphs

Classical problems

- *classification;*
- *enumeration;*
- *isomorphism problem;*
- *diameter problem.*

Definition

The diameter of the Cayley graph $\Gamma = Cay(G, S)$ *is the maximum, over* $g \in G$, *of the length of a shortest expression for* g *as a product of generators:* $diam\,\Gamma = max_{g \in G} min_k\, g = s_1 \cdots s_k,\ s_i \in S$.

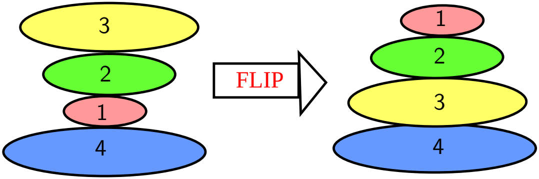
(Same as graph theoretic diameter.)

Applied problems

- *hamiltonicity (in computer science);*
- *Pancake problems (burnt and unburnt cases);*
- *sorting by reversals (in molecular biology);*
- *vertex reconstruction problem (in coding theory).*

Pancake problem: 1975, *American Mathematical Monthly* by *Jacob E. Goodman* (under the name "Harried Waiter")

"The chef in our place is sloppy, and when he prepares a stack of pancakes they come out all different sizes. Therefore, when I deliver them to a customer, on the way to the table I rearrange them (so that the smallest winds up on top, and so on, down to the largest on the bottom) by grabbing several pancakes from the top and flips them over, repeating this (varying the number I flip) as many times as necessary. If there are n pancakes, what is the maximum number of flips (as a function of n) that I will ever have to use to rearrange them?"



The Pancake problem and the Pancake graph

A stack of n pancakes is represented by a permutation on n elements and the problem is to find the least number of flips (prefix–reversals) needed to transform a permutation into the identity permutation.

This number of flips corresponds to the diameter D of the Pancake graph

The table of diameters for P_n, $4 \leqslant n \leqslant 19$, is presented below:

4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
4	5	7	8	9	10	11	13	14	15	16	17	18	19	20	22

Pancake problem: bounds

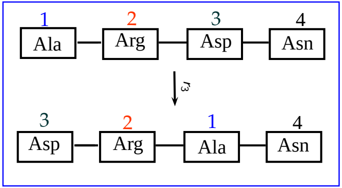
1979, Gates, Papadimitriou: $17n/16 \leqslant D \leqslant (5n+5)/3$

1997, Heydari, Sudborough: $15n/14 \leqslant D$

2007, Sudborough, etc.: $D \leqslant 18n/11$

Applications: molecular biology

Genomes are presented by a permutations:



The evolutionary distance: Palmer, Herbon, 1986

The prefix–reversal distance of two permutations is the least number d of prefix–reversals needed to transform one permutation into another:

$$X\text{: } (\underline{1, 5, 2}, 3, 4) \longrightarrow Y\text{: } (2, 5, 1, 3, 4)$$

Sorting permutations by reversal (prefix–reversals): NP–hard

Find, for a given permutation π, a minimal sequence d of reversals (prefix–reversals) that transforms π to the identity permutation I.

Applications: interconnection networks

1986, SIAM International Conference on Parallel Processing: "to use Cayley graphs as a tool to construct vertex–symmetric interconnection networks."

Interconnection networks are modeled by graphs: the vertices correspond to processing elements, memory modules, or just switches; the edges correspond to communication lines.

Advantages in using Cayley graphs as network models:

- *vertex–transitivity (the same routing algorithm is used for each v);*
- *hierarchical structure (allows recursive constructions);*
- *high fault tolerance (the maximum number of vertices that need to be removed and still have the graph remain connected);*
- *small degree and diameter.*

Pancake graphs $\equiv$ Pancake networks (1,900,000 results in Google)

Computing the diameter is difficult

NP–hard for elementary abelian 2–groups (Even, Goldreich 1981)

Definition (informal)

A decision problem is in the complexity class NP if the yes answer can be checked in polynomial time.

Definition (informal)

A decision problem is NP–complete if it is in NP and all problems in NP can be reduces to it in polynomial time.

Definition (informal)

A decision problem is NP–hard if all problems in NP can be reduces to it in polynomial time.

How large can be the diameter?

The diameter can be very small:

$$diam\,\Gamma(G,G)=1.$$

The diameter also can be very big:

$$G=\langle x\rangle\cong\mathbb{Z}_n,\quad diam\,\Gamma(G,x)=\lfloor\frac{n}{2}\rfloor.$$

In general, G with large abelian factor group may have Cayley graphs with diameter proportional to |G|.

$(3 \times 3 \times 3)$–Rubik's cube)

It has 6 faces and $|Rubik| = 43,252,003,274,489,856,000$ *positions.*

If $G = Rubik$ *is a group of all positions, and* S *is defined by rotation s.t.* $Rubik := \langle S \rangle$ *then the diameter* $d(3 \times 3 \times 3)$ *for* $Cay(G,S)$ *is the best solution for the worst position.*

1981, Morwen Thistlethwaite: $18 \le d(3 \times 3 \times 3) \le 52$.
1995, Michael Reid: $20 \le d(3 \times 3 \times 3) \le 29$.
2010, Tomas Rokicki, etc.: $diam(3 \times 3 \times 3) = 20$.

Every position of Rubik's Cube can be solved in twenty moves or less.

The diameter problem: non–abelian case

Computing the diameter of an arbitrary Cayley graph over a set of generators is NP–hard. General upper and lower bounds are very difficult ro obtain. Moreover, there is a fundamental difference between Cayley graphs of abelian and non–abelian groups.

Babai, Kantor, Lubotzky, 1989

Every non–abelian finite simple group G has a set of ≤ 7 generators such that the resulting Cayley graph has diameter $O(\log |G|)$.

So, they have shown that each non–abelian simple group has a set of at most seven generators that yields a Cayley graph with logarithmic diameter (with constant factors).

However, this property does not hold for Cayley graphs of abelian groups.

The diameter problem: abelian case

Annexstein, Baumslag, 1993

Let G be an abelian group with a generating set S of size r. The Cayley graph $Cay(G, S)$ has the following diameter bound:

$$diam(Cay(G, S)) \geqslant \frac{1}{e}|G|^{1/r}.$$

The diameter problem: non–abelian case again

On the other hand, in 1988 it was conjectured by Laszlo Babai and Akos Seress for non–abelian groups that the diameter will always be small.

Conjecture: Babai, Seress, 1988

There exist a constant c such that for every non–abelian finite simple group G, the diameter of every Cayley graph of G is $\leqslant (\log |G|)^c$.

It was reformulated for the diameter of groups.

Definition

The diameter of a group is $diam(G) := max_S \, diam \, \Gamma(G, S)$.

Conjecture: Babai, Seress, 1992

There exist a constant c such that for every non–abelian finite simple group G its diameter is $diam(G) = O(\log^c |G|)$.

The diameter of groups

Definition

The diameter of a group is $diam(G) := max_S\, diam\, \Gamma(G,S)$.

Conjecture: Babai, Seress, 1992

There exist a constant c such that for every non–abelian finite simple group G its diameter is $diam(G) = O(log^c |G|)$.

Conjecture is true for:

- the projective special linear group $PSL(2,p)$, $PSL(3,p)$ (Helfgott, 2008, 2010);
- Lie–type groups of bounded rank (Pyber, Szabo, 2011, and Breuillard, Green, Tao, 2011).

Alternating groups???

The diameter of the symmetric group

As it was conjectured, the diameter of the symmetric group of degree n is polynomially bounded in n.

The best known upper bound was exponential in $\sqrt{n \log n}$, namely

Babai, Seress, 1988

If G is either Sym_n or A_n then the diameter $diam(G) \leqslant exp((1+o(1))\sqrt{n \log n}) = exp((1+o(1))\sqrt{\log |G|})$.

We write $exp(x) = e^x$.

On the diameter of permutation groups

Recently it was obtained a quasipolynomial upper bound.

Definition

A function $f(n)$ is called quasipolynomial if $\log(f(n))$ is a polynomial function on $\log n$.

Helfgott, Seress, 2011

If G is either Sym_n or A_n then the diameter

$$diam(G) \leqslant exp(O((\log n)^4 \log\log n)) = exp((\log\log|G|)^{O(1)}.$$

We write $exp(x) = e^x$.

The proof is difficult!

Proof techniques in Helfgott, Seress, 2011

1. Subset versions of theorems of Babai, Pyber about 2–transitive groups and Bochert, Liebeck about large cardinality subgroups of A_n.

2. combinatorial arguments, using random walks of quasipolynomial length on various domains to generate permutations that approximate properties of truly random elements of A_n.

3. Previous results on diam(A_n): Babai, Seress, 1988; Babai, Seress, 1992; Babai, Beals, Seress, 2004.

5. Seress: "Arguments are mostly combinatorial: the full symmetric group is a combinatorial rather than a group theoretic object."