

# Computing Fault Tolerance of Cayley Graphs

**Beth Novick**

Department of Mathematical Sciences  
Clemson University

Joint Work with **Shuhong Gao**

Annals of Combinatorics 11 (2007) 161-171.

CanaDAM, May 25, 2009

# Outline

- Cayley Graphs and Computational Problems
- Fragments and Atoms
- Exchange Graphs
- Network Flow and Algorithm

**To define a Cayley graph we need  
a group  $G$  and a subset  $S \subseteq G$ .**

$G$ : any group

$S$  : any subset of  $G$  not containing the identity.

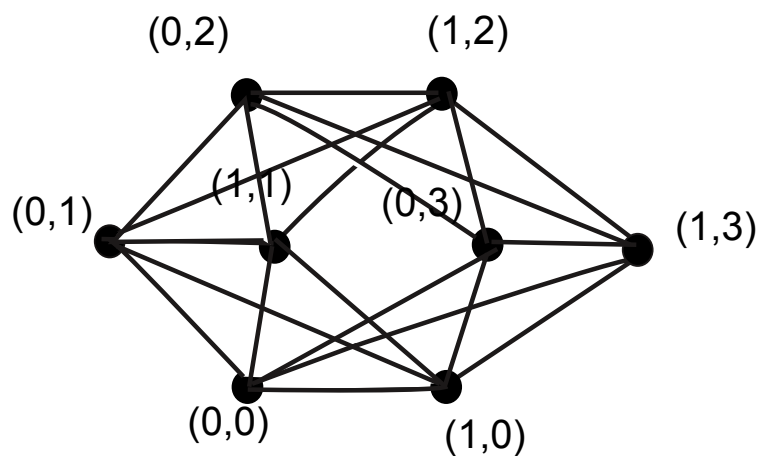
**Cayley graph**  $(G, S)$ : elements of  $G$  are vertices and, for  $x, y \in G$ , there is a directed edge from  $x$  to  $y$  iff  $x \cdot s = y$  for some  $s \in S$ .

Examples: cycles (directed and undirected), Hypercubes, truncated hypercubes, etc.

## Examples of Cayley graphs $(G, S)$ .

Consider  $(\mathbb{Z}_5^*, S)$  with  $S = \{2, 3\}$ .

Consider  $(\mathbb{Z}_2 \times \mathbb{Z}_4, S)$  with  $S = \{(1, 0), (0, 1), (0, 3), (1, 3), (1, 1)\}$ .



# Examples

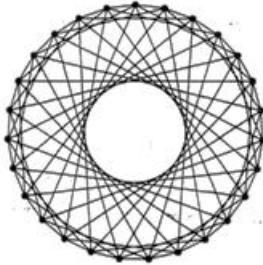


Figure 1:  $G = \mathbb{Z}_{27}$ ,  $A = \{1, 4, 17\}$  and  $S = A \cup A^{-1}$ . (D.F.Hsu)

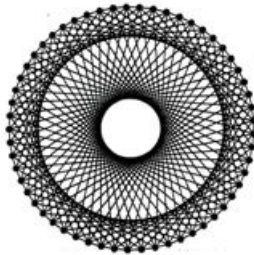


Figure 2:  $G = \mathbb{Z}_{57}$ ,  $A = \{1, 13, 33\}$  and  $S = A \cup A^{-1}$ . (D.F.Hsu)

# Properties of Cayley graphs make them good candidates for communication networks.

- Regular: each vertex has out-degree and in-degree  $|S|$ .
- Vertex transitive, provided it is strongly connected, that is, every element of  $G$  can be written as a product of elements from  $S$ .
- They have small degree and small diameters.
- They are useful for constructing good expander graphs.

## Fault tolerance and vertex connectivity are essentially the same.

The **fault tolerance** of a digraph  $\mathcal{X}$  is the largest number  $k$  such that failure of  $k$  nodes does *not* destroy the connectivity of the whole network.

If  $\kappa(\mathcal{X})$  is the cardinality of the smallest vertex cut then the fault tolerance of  $\mathcal{X} = \kappa(\mathcal{X}) - 1$ .

$(G, S)$  has **optimal fault tolerance** when the smallest vertex cut has cardinality  $|S|$ .

# Computational Problems

**Problem 1.** Given a finite group  $G$  and a subset  $S$  of  $G$ , decide if the Cayley graph  $(G, S)$  is strongly connected.

**Problem 2.** Given a finite group  $G$  and a subset  $S$  of  $G$ , compute the fault tolerance of  $(G, S)$ , assuming the graph is strongly connected.

**“Given a finite group  $G$ ”:** We assume that the group  $G$  is given by an *oracle* (or a *black box*). The oracle can perform various group operations, namely, product of two elements, the inverse of an element, and distinctness of two elements.

**Question: Are there polynomial time algorithms for the above problems?** <sup>8</sup>

**We need to be careful about what we consider polynomial time.**

**Polynomial time:** the number of group operations used is bounded by a polynomial in  $|S|$  and  $\log |G|$ .

**Warning:** One can not examine all the vertices in the graph!

# Answers

## Problem 1: **still open**

It is open even for the special case:  $G$  is the multiplicative group of a finite field  $\mathbb{F}_q$  and  $S = \alpha$ . In this case, the graph  $(G, S)$  is strongly connected iff  $\alpha$  a primitive element (i.e.  $\alpha$  has multiplicative order  $q - 1$ ):

Consider  $G = \mathbb{F}_{2^n}^*$ ,  $n = 10,000$ .  $\mathbb{F}_{2^n} = \mathbb{F}_2[x]/f(x)$  where  $f(x)$  is irreducible of degree  $n$ .

$\alpha$  is presented in the basis  $(1, x, \dots, x^{n-1}) \bmod f(x)$ .

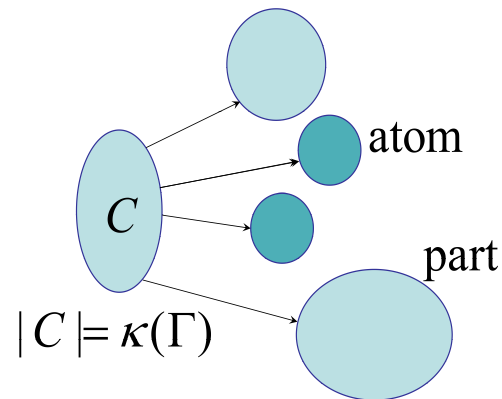
$(G, \{\alpha, \alpha^{-1}\})$  is connected iff has order  $2^n - 1$ .

## Problem 2: **yes**

## To see how to answer problem 2 we need to 'fragments' and 'atoms'.

Watkins (1970): For any digraph  $\mathcal{X}$  and any vertex cut  $C \subseteq V(\mathcal{X})$ , the strongly connected components of  $\mathcal{X} \setminus C$  are called the **fragments** of  $\mathcal{X}$  induced by  $C$ .

A fragment is called an **atom** if it is induced by a minimum vertex cut and it has minimum cardinality among all such fragments.



**The are two ways a vertex set can be a fragment.**

11

For any subset  $A$  of  $V(\mathcal{X})$ , we denote

$$N^+(A) = \{v \in V(\mathcal{X}) \setminus A : [u, v] \in E(\mathcal{X}) \text{ for some } u \in A\},$$

$$N^-(A) = \{v \in V(\mathcal{X}) \setminus A : [v, u] \in E(\mathcal{X}) \text{ for some } u \in A\},$$

called **the positive or negative neighborhood** of  $A$ , respectively.

If  $A$  is an atom, then  $N^+(A)$  or  $N^-(A)$  is a vertex cut (of minimum cardinality), called *positive* or *negative* atom, respectively.

## Three Structural Theorems

**Theorem 1** (W. Watkins 1970 and Y.O. Hamidoune 1977): Let  $\mathcal{X}$  be any strongly connected vertex transitive digraph with a positive atom. Then its positive atoms form a partition of all the vertices.

**Theorem 2** (Y.O. Hamidoune 1984): Assume that the Cayley graph  $(G, S)$  is strongly connected and contains positive atoms. Let  $A$  be the positive atom of  $(G, S)$  containing 1. Then  $A = \langle S \cap A \rangle$  and every positive atom is of the form  $aA$ ,  $a \in G$ , i.e. a left coset of  $A$ .

**Theorem 3** (Gao and N. 2007):  $A \subseteq S \cdot S^{-1} = \{a \cdot b^{-1} : a, b \in S\}$ .

# Consequences of our structural theorem

- A very simple proof that ‘exchange graphs’ are optimally fault tolerant.
- An efficient algorithm for computing fault tolerance in connected Cayley graphs. (Polynomial in an appropriate sense.)

# Exchange Graphs

C. Godsil (1981):

$S_n$ : the symmetric group of permutations on  $\{1, 2, \dots, n\}$ .

$\Gamma$ : any graph (undirected) on the vertex set  $\{1, 2, \dots, n\}$ .

Each edge  $(i, j)$  of  $\Gamma$  corresponds to a transposition in  $S_n$  that exchanges  $i$  and  $j$ .

**Fact.**  $(S_n, \Gamma)$  is connected iff  $\Gamma$  is connected.

# Exchange Graphs have Optimal Fault Tolerance

**Theorem 4** (Gao, N.). The connectivity of  $(S_n, \Gamma)$  is equal to  $|E(\Gamma)|$ , the number of edges in  $\Gamma$ .

**Proof.** Suppose  $\kappa(S_n, \Gamma) < |E(\Gamma)|$ . Then the atom  $A$  containing 1 has size at least 2 and is a subset of

$$\Gamma \cdot \Gamma^{-1} = \{(i, j)(a, b) : (i, j), (a, b) \in E(\Gamma)\}.$$

Furthermore,  $A$  is generated by  $A \cap \Gamma$  and, as  $|A| \geq 2$ , in particular  $A \cap \Gamma \neq \emptyset$ . Thus there is a 2-cycle of  $\Gamma$  that lies in  $\Gamma \cdot \Gamma^{-1}$ , impossible.

# Network Flow and Algorithm

**We assume the the Cayley graph is connected, or equivalently work with the connected component containing 1.**

Let  $G$  be any finite group and  $S \subset G$  not containing 1.

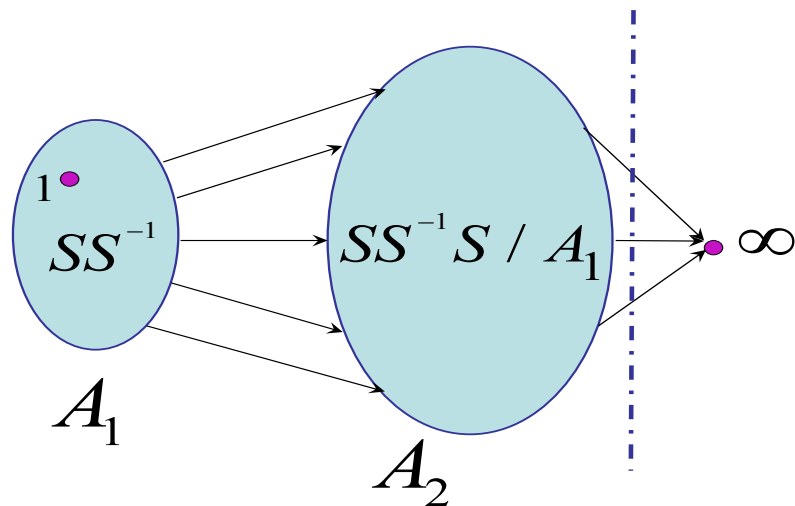
Let  $G_0$  be the subgroup generated by  $S$ . Then the Cayley graph  $(G_0, S)$  is the connected component of  $\mathcal{X}$  that contains the identity 1. **We denote this component by  $\mathcal{X}_0$ , i.e.,  $\mathcal{X}_0 = (G_0, S)$ .**

We create the smaller graph,  $\bar{X}_0$ .

**Lemma.** Suppose  $G_0 \neq A_1 \cup A_2$ . Then  $\kappa(\mathcal{X}_0)$  is equal to the maximum flow from 1 to  $v_\infty$  in  $\bar{\mathcal{X}}_0$  (with each edge of capacity 1).

**Proof.** We show  $\kappa(X_0) = \kappa(\bar{X}_0)$ :

Create the smaller graph,  $\bar{X}_0$ .



$A \subseteq SS^{-1}$  (Using structural theorem.)

$N^+(A) \subseteq A_1 \cup A_2$

Find maximum flow in  $\bar{X}_0$ .

# Network Flow and Algorithm

## Algorithm:

Input: a black box (oracle) for a group  $G$  and  $S \subset G$

Output: Fault tolerance of the connected components of the Cayley graph  $(G, S)$

Step 1: Compute the vertices in  $A_1$  and  $A_2$

Step 2: If  $G = A_1 \cup A_2$  then compute the connectivity of  $(G, S)$ , say  $k$ .

Step 3: Otherwise construct the network  $\overline{\mathcal{X}}_0$ .

Step 4: Find the maximum flow from 1 to  $v_\infty$ , say  $k$ .

Return  $k - 1$ .

Note that the network  $\overline{\mathcal{X}}_0$  has at most  $|S|^3 + 1$  vertices. So the algorithm runs in polynomial time.

**Hence we have solved our Problem 2.**

**Theorem 5**(Gao, N.) If a strongly connected Cayley digraph  $X = (G, S)$  is given by the set  $S$  together with a black box that efficiently provides inverses, multiplication and recognition of the identity element, then the connectivity  $\kappa(X)$  may be determined in time polynomial in  $|S|$  and  $\log |G|$ .

In other words the number of calls to the oracle is at most  $|S|^c$  for some constant  $c$ .

# Open Problems

**Fact.** Computing fault tolerance of Cayley graphs is easy!

**Open Problem 1:** Is there a polynomial time algorithm to decide the connectedness of Cayley graphs!

**Open Problem 2:** Which Cayley graphs are Hamiltonian?

# Open Problems

**Open Problem 3:** Star diameters and routing on Cayley graphs?

Shuhong Gao, Beth Novick and Ke Qiu, *From Hall's Matching Theorem to Optimal Routing on Hypercubes*, Journal of Combinatorial Theory, Series B 74, 291-301 (1998).

Shuhong Gao and D. Frank Hsu, *Short containers in Cayley graphs*, to appear in Discrete Applied Mathematics.