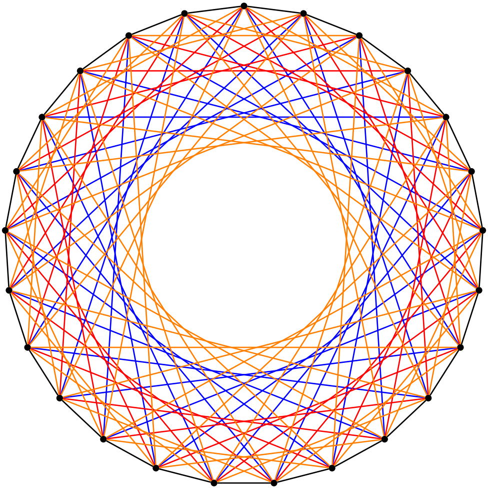
Extremal Cayley Graphs

Jordan Blocher, Christopher Linden, Samantha Hampton

REU - Texas State

28 June 2012



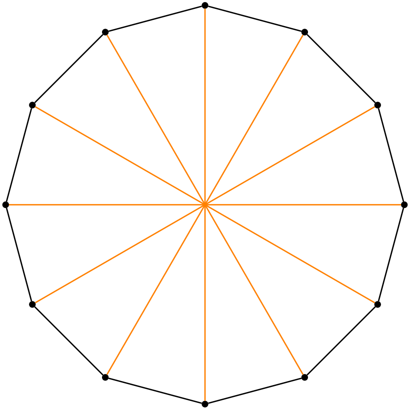
- $\mathrm{Cay}(\mathbb{Z}_{25}, \{\pm 1, \pm 4, \pm 6, \pm 8\})$

Introduction to Cayley Graphs

- Definition: Let Γ be a finite group with a subset A. The *Cayley digraph*, denoted Cay(Γ,A), is a digraph with vertex set Γ, such that (x,y) is a directed edge if and only if $yx^{-1} \in A$
- *Cayley digraphs* are vertex transitive.

Introduction to Cayley Graphs

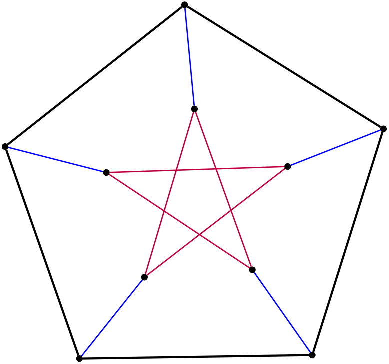
- The bicycle wheel



Cay($\mathbb{Z}_{12}$, $\{\pm 1, \pm 6,\}$)

Introduction to Cayley Graphs

- The Petersen Graph



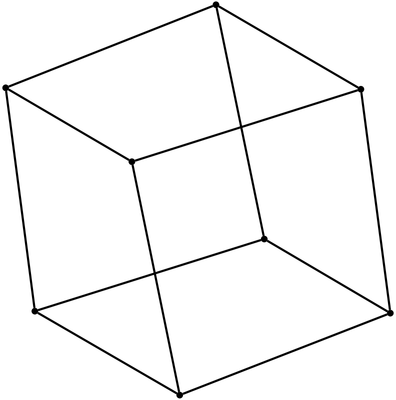
- This is not a Cayley digraph.

N-Cubes

- Definition: The Cayley digraph $Cay(\mathbb{Z}_2^n, \{e_1, e_2, \dots, e_n\})$
- Common choice for interconnection network designs
- The diameter of a network represents the maximum communication delay between two nodes in the network.
- For a fixed diameter and vertex degree, there are circulant graphs that contain more vertices than the corresponding n-cube.
- Hence, circulant graphs give better communication networks than cubes

N-Cubes

- The 3-Cube



- For positive integers d and k, we define:

$$m(d, A) = \max\{m \mid diam(Cay(\mathbb{Z}_m, A)) \leq d\},$$
$$m(d, k) = \max_{A:|A|=k} \{m(d, A)\}.$$

- Current known values include:

$$m(1, k) = k + 1,$$
$$m(d, 1) = d + 1, \text{ and}$$
$$m(d, 2) = \left\lfloor \frac{d(d+4)}{3} \right\rfloor + 1 \text{ for all } d \geq 2.$$

The following theorem can be used to construct large efficient generating sets A so that $m(d, A)$ is large by using small efficient generating sets.

Theorem

Let $d_1 \geq 2$, $d_2 \geq 2$, $k_1 \geq 1$, and $k_2 \geq 1$ be integers. Then

$$m(d_1 + d_2, k_1 + k_2) \geq m(d_1, k_1)m(d_2, k_2).$$

Proof

Let $A_s = \{0 < a_{s1} < a_{s2} < \cdots < a_{sk_s}\}$ be a set of integers with

$$m(d_s, A_s) = m(d_s, k_s) = m_s \qquad \text{for} \quad s = 1, 2.$$

We may assume, without loss of generality, that $a_{sk_s} < m_s$ for $s = 1, 2$. Define

$$A = A_1 \cup \{m_1 a_{2j} \mid j = 1, 2, \ldots, k_2\}.$$

Since $|A| = k_1 + k_2$, we only need to prove that A is a $(d_1 + d_2)$-basis for $\mathbb{Z}_{m_1 m_2}$.

Let n be any nonnegative integer. Since A_1 is an d_1-basis for $\mathbb{Z}_{m_1}$, we see that

$$n \equiv \sum_{i=1}^{k_1} x_i a_{1i} \pmod{m_1},$$

where x_i's are nonnegative integers with $\sum_{i=1}^{k_1} x_i \leq d_1$. Assume

$$n = \sum_{i=1}^{k_1} x_i a_{1i} + q m_1$$

for some integer q.

It follows from the fact that A_2 is a d_2-basis for $\mathbb{Z}_{m_2}$ that

$$q = \sum_{j=1}^{k_2} y_j a_{2j} + pm_2,$$

where y_j's are nonnegative integers with $\sum_{j=1}^{k_2} y_j \leq d_2$, and p is an integer.

Therefore,

$$n \equiv \sum_{i=1}^{k_1} x_i a_{1i} + \sum_{j=1}^{k_2} y_j m_1 a_{2j} \pmod{m_1 m_2},$$

where

$$\sum_{i=1}^{k_1} x_i + \sum_{j=1}^{k_2} y_j \leq d_1 + d_2.$$

This implies that $n \in (d_1 + d_2)A_0$, where $A_0 = A \cup \{0\}$. Hence, A is a $(d_1 + d_2)$-basis for $\mathbb{Z}_{m_1 m_2}$. Therefore,

$$m(d_1, k_1)m(d_2, k_2) = m_1 m_2 \leq m(d_1 + d_2, k_1 + k_2).$$

The proof is complete.

The General Case

- By repeated application of this inequality, and using lower bounds for small values of k we can construct a bound for general k

Computability of m(d,k)

Let d be the diameter for $\mathrm{Cay}(m, k)$.
Given d define fixed d_1 to be $\frac{d}{\lambda}$, also define $a_1 = \frac{a}{\lambda}$, $b_1 = \frac{b}{\lambda}$, and $c_1 = \frac{c}{\lambda b}$, etc.., so λ is a large number determined by d. The parameter λ will not appear in the code, but it enables us to compute a lower bound as a function of d.

Computability of m(d,k) for small fixed k

Our lower bound on $m(d, k)$ will be defined as $m = \alpha\lambda a_1 + \beta\lambda b_1 + \gamma\lambda c_1 + \ldots\ \psi\lambda z_1$. To determine the validity of the lower bound, we compute every point in dA as a polynomial in terms of λ.

Computability of m(d,k) for small fixed k

Take $(x_1, x_2, ..., x_n)$ such that $x_1 \leq b_1, x_2 \leq c_1, .., x_n \leq \psi$ and $\sum_i x_i \leq d$
For all polynomials $x_1 a + x_2 b + .. + x_n k$, we reduce to a unique minimal representation by comparing the coefficients $(x_1, x_2, x_3, .., x_n)$ and $(\alpha, \beta, \gamma, .., \psi)$ and removing dependent linear combinations.

Computability of m(d,k) for small fixed k

$\forall x = (x_1, x_2, .., x_k) \in dA$ if $x \notin \mathbb{Z}_m$, we can identify x with point $x' = (x'_1, x'_2, .., x'_k) \in \mathbb{Z}_m$ congruent to x $(mod\ \ m)$. Then if every point $n \in \mathbb{Z}_m$ is either equal to some x or x', $dA = \mathbb{Z}_m$.
To construct a lower bound, we systematically check combinations of generators A and coefficients, and record the largest m (and corresponding generators) such that a covering by dA is achieved.