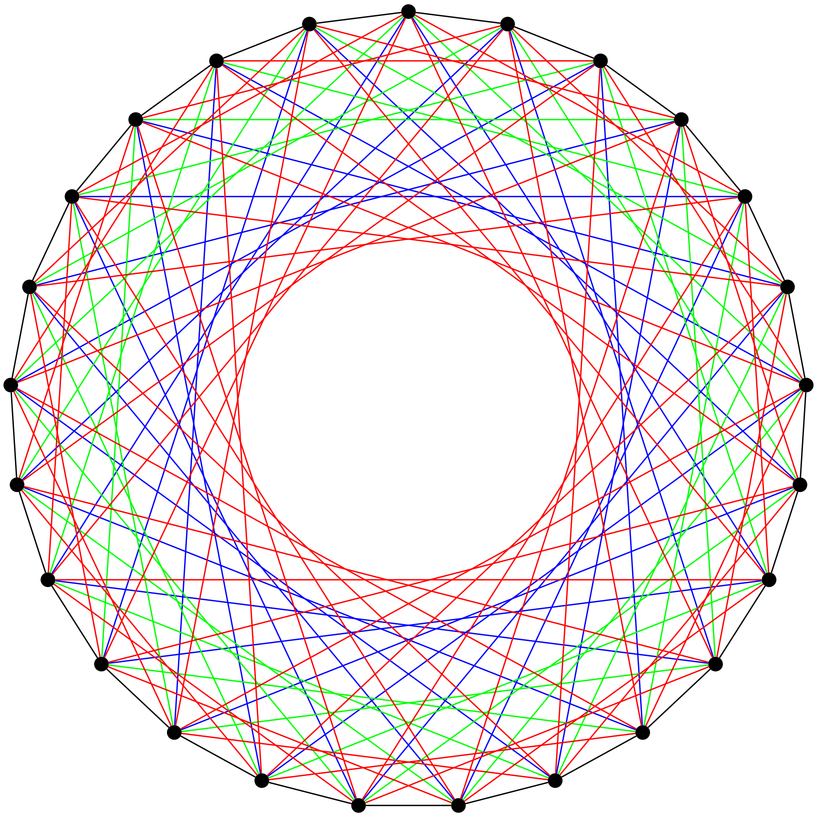
Cayley Digraphs of Finite Cyclic Groups with Minimal Diameter*

Jordan Blocher† Christopher Linden‡ Samantha Hampton§

July 2, 2012



*Supported in part by National Science Foundation (NSF).

†Department of Mathematics, University of Nevada-Reno, Reno, NA, USA. jordanblocher@gmail.com.

‡University of California Los Angeles, Los Angeles, CA,USA

§Department of Mathematics, University of Arkansas, Fayetteville, AR, USA

Abstract

For positive integers d and k let $m(d,k)$ be defined to be the maximum modulus m such that there exists a generating set A of the *Cayley digraph* Cay(m, A) with cardinality equal to k such that the diameter of Cay(m, A) is less than or equal to d.

1 Introduction

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. In this paper we will be working with $\mathbb{Z}_m$ as our vertex set, and will denote these Cayley graphs as Cay(m,A).

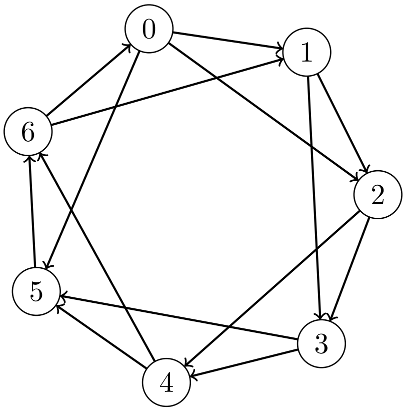


Figure 1: Cay($\mathbb{Z}_7$, {1,2}).

An important property of Cayley digraphs is the Cayley digraph Cay(m,A) is vertex-symmetric. This property allows us to define extremal functions for these digraphs. For any positive integer d we define

$$m(d,A) = \ max\{m|diam(Cay(m,A)) \leq d\},$$

the largest positive integer m such that the diameter, d(m,A), of the Cayley digraph Cay(m,A) is less than or equal to d. For positive integers d and k,

$$m(d,k) = max\{m(d,A)| \text{ there exists a set A with } |A| = k\},$$

the maximum modulus m such that there exists a generating set with cardinality equal to k and the diameter of the Cayley digraph is less than or equal to d.

Current known bounds include

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

We will begin by examine the case when k = 3. The current bounds for this case, as $d \to \infty$, are

$$\frac{176}{2197}d^3 + O(d^2) \leq m(d,3) \leq \frac{1}{14 - 3\sqrt{3}}(d+3)^3.$$

2 The Algorithm

We now provide an algorithm that takes as an input a set of generators as well as two other permutation sets. These inputs are used to test the ability of a generated lower bound to provide a set covering for our Cayley Graph. The algorithm iterates through permutations of the generating set and possible coverings, giving as an output the maximal generating set as well as the optimal polynomial bound.

The algorithm takes advantage of the fact that there exists a one-to-one correspondance between representations of the residual classes of $\mathbb{Z}_m$ and the set of integers $[0, m-1]$.

Let d be the diameter for $\text{Cay}(m, A)$.

Given d define d_1 **fixed** *to be $\frac{d}{\lambda}$. Define $\mathcal{A}$ to be a* **set of generators**, *$\mathcal{A} = \{(a_i) | a_{i+1} = \alpha_i a_i, \forall i \in [0, k-1]\}$, with a_i a sequence of nonnegative coefficients, and $|\mathcal{A}| = k$. Also define a set of* **non-negative coefficients** *$c_1, c_2, .., c_k$ such that $a_{i+1} = \alpha_i a_i \lambda$.*

(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.)

Our lower bound on $m(d,k)$ will be defined as $m(d,k) = a_i c_i \lambda$. To determine the validity of the lower bound, we compute every point in $d\mathcal{A}$ as a polynomial in terms of λ.

Let $\{(x_1, x_2, ..., x_n) | x_1 \leq c_1, x_2 \leq c_2, .., x_k \leq c_k$, and $\sum_i x_i \leq d_1\}$ define polynomials x that are considered to be minimal.

For all constructed polynomials $x = x_1 a_1 + x_2 a_2 + .. + x_k a_k$, we define a representative $x' \in [1, m-1]$ to which we will map all congruent polynomials, forming our residue class $\bar{x}$ of regular polynomials.

$\forall n \in \mathbb{Z}_m$, where n is the residue class of $\mathbb{Z}_m$, if $\exists x$ such that $\bar{x} = \bar{x'} = n$, then $d\mathcal{A} = \mathbb{Z}_m$.

Let $\{(x_1, x_2, ..., x_n) | x_1 \leq c_1, x_2 \leq c_2, .., x_k \leq c_k$, and $\sum_i x_i \leq d_1\}$ define polynomials x that are considered to be minimal.

For all constructed polynomial $x = x_1 a_1 + x_2 a_2 + .. + x_k a_k$, we define a representative $x' \in [1, m-1]$ to which we will map all congruent polynomials, forming our residue class $\bar{x}$ of regular polynomials.

The constructed polynomial x is defined to be regular if $x \in [0, m-1]$. In *this way we are able to check $d\mathcal{A} = \mathbb{Z}_m$ by only considering a single covering of $\mathbb{Z}_m$.*

Note that a regular polynomial need not be minimal.

The constructed polynomial x is defined to be regular if $x \in [0, m-1]$. In this way we are able to check $d\mathcal{A} = \mathbb{Z}_m$ by only considering a single covering of $\mathbb{Z}_m$.

Note that a regular polynomial need not be minimal.

We check for regularity by comparing the coefficients $(x_1, x_2, x_3, .., x_k)$ and $(c_1, c_2, .., c_k)$ from their respective polynomials.

$\forall x \in d\mathcal{A}$ if $x \notin [0, m-1]$, we can identify x with point $x' = (x'_1, x'_2, .., x'_k) \in [0, m-1]$ congruent to x $(mod\ m)$. Then if every point $n \in \mathbb{Z}_m$ is either equal to some x or x', then $d\mathcal{A} \cong \mathbb{Z}_m$.

Consider the case, $x > m(d, k)$, where x is not regular. We perform a recursive polynomial subtraction of the coefficients where c_1, c_2, c_3 is subtracted term-by-term from $x_1, x2, x3, ..., x_n$. The resulting low-order coefficients are then forced to be positive by adding the generator associated with the next higher-order term.

For example, a resulting polynomial that has been forced to be well formed may look as, $[\lambda(x_1 - 2c_1) + 1]a_1 + [\lambda(x_2 - 2c_2) + 2]a_2 + [\lambda(x_3 - 2c_3) + 1]a_3 + ... + [\lambda(x_k - 2c_k) + 3]a_k$.

To construct a lower bound, we systematically check combinations of generators $\mathcal{A}$ and coefficients, and record the largest m (and corresponding generators) such that a covering by $d\mathcal{A}$ is achieved.

2.1 Pseudocode

```
for all $X = (ax_1 + bx_2 + cx_3 + .. + zx_n), M = (\alpha a + \beta b + \gamma c + .. + \psi z)$ do
    X - M
end for
```