Extremal Functions on Cayley Digraphs of Finite Cyclic Groups*

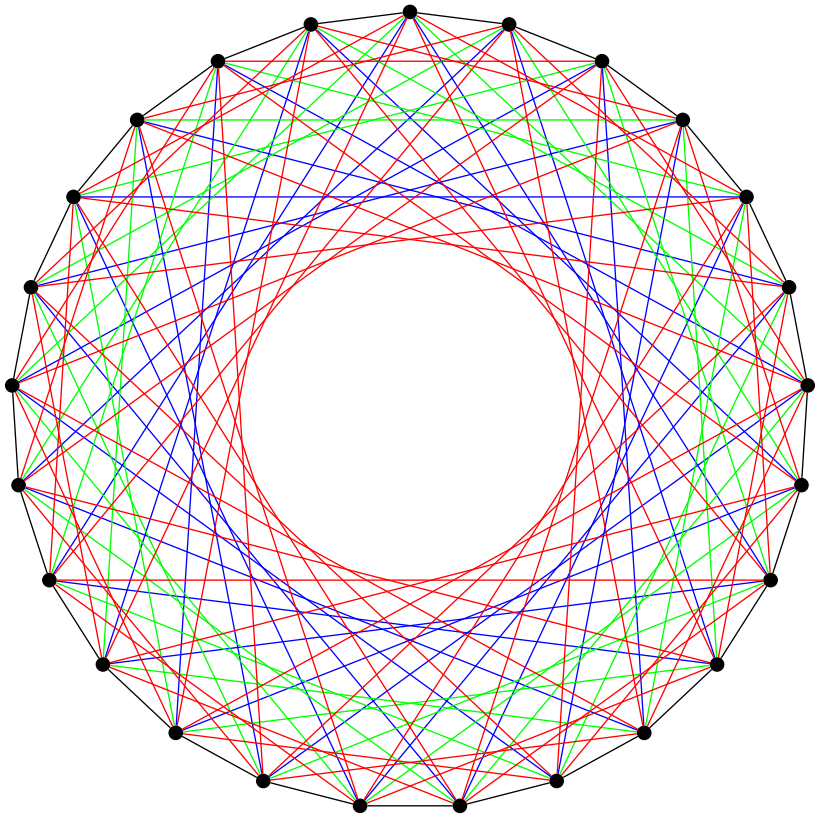
Jordan Blocher
Department of Mathematics
University of Nevada-Reno
Reno, Nevada, USA
jordanblocher@gmail.com

Samantha Hampton
Department of Mathematics
University of Arkansas
Fayetteville, Arkansas, USA
smhampto@uark.edu

Christopher Linden
Department of Mathematics
University of California at Los Angeles
Los Angeles, California, USA
lindenechris@gmail.com

February 5, 2014

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



Abstract

For positive integers d and k we define $m(d,k)$ to be the maximum positive integer m such that the *Cayley digraph* $\mathrm{Cay}(\mathbb{Z}_m, \mathscr{A})$ of $\mathbb{Z}_m$ generated by a set $\mathscr{A}$ of k positive integers has diameter less than or equal to d, where $\mathbb{Z}_m$ is the finite cyclic group of residue classes modulo m. In this paper we present new algorithms that lead to the computation of lower bounds for $m(d,k)$ with k small and fixed. These algorithms are detailed as a complement to the actual proof. We also consider $m(2,k)$ and establish a new lower bound, namely

$$m(2,k) \geq \frac{37}{121}k^2 + O(k) \qquad \text{as} \quad k \to \infty.$$

In this paper, we also use this lower bound to obtain a lower bound for $m(d,k)$ for any given positive integer d:

$$m(d,k) \geq \left(\frac{148}{121}\right)^{\lfloor \frac{d}{2} \rfloor} \left(\frac{k}{d}\right)^d + O(k^{d-1}) \qquad \text{as} \quad k \to \infty.$$

1 Introduction

Let Γ be a finite group with a subset $\mathscr{A}$. The *Cayley digraph*, denoted $\mathrm{Cay}(\Gamma, \mathscr{A})$, is a digraph with vertex set Γ, such that (x, y) is a directed edge if and only if $yx^{-1} \in \mathscr{A}$. The focus of this paper is the finite group $\mathbb{Z}_m$; we will denote the Cayley graph $\mathrm{Cay}(\mathbb{Z}_m, \mathscr{A})$ as $\mathrm{Cay}(m, \mathscr{A})$.

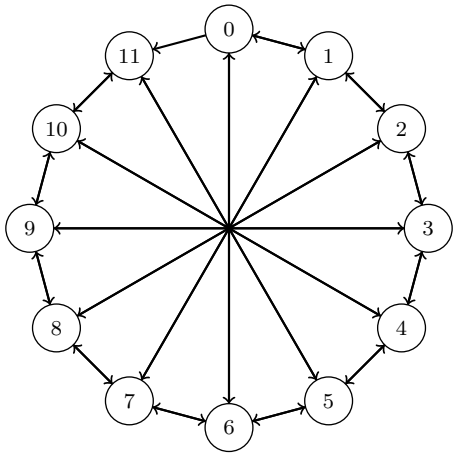


Figure 1: $\mathrm{Cay}(\mathbb{Z}_{12}, \{1, 6, 11\})$.

Note that $\mathrm{Cay}(\mathbb{Z}_{12}, \{1, 6, 11\})$ has the same diameter and degree as the 3-cube, but this graph contains 12 vertices. It is natural to ask for the maximum number of vertices a Cayley digraph could possibly have with given diameter and maximum degree. Cayley digraphs $\mathrm{Cay}(\mathbb{Z}_m, \mathscr{A})$ of $\mathbb{Z}_m$ are called *circulant* (di)graphs. In this paper, we focus on circulant graphs. However, n-cubes may not be as efficient as circulant graphs of equal degree and diameter. Cayley digraphs, and circulant graphs in particular are often used as models for interconnection networks. As such, it is naturally desirable to maximize the number of vertices which can be connected with constraints on diameter and degree. For any positive integer d we define

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

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

$$m(d, k) = \max\{m(d, \mathscr{A}) || \mathscr{A}| = k\},$$

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.

It is clear that $m(1,k) = k+1$ and $m(d,1) = d+1$. In 1974 Wong and Coppersmith [**?**] proved that, for positive integers d and k,

$$\left\lfloor \frac{d}{k} + 1 \right\rfloor^k \leq m(d,k) \leq \binom{k+d}{k}.$$

To see the the upper bound, let $|\mathscr{A}| = k$ such that $\mathrm{diam}(Cay(\mathbb{Z}_m, \mathscr{A})) \leq d$. Noting that every element in $\mathbb{Z}_m$ is the sum of at most d not necessarily distinct elements of $\mathscr{A}$, and the commutativity of integers, we see that

$$m \leq \binom{k+1+d-1}{k} = \binom{k+d}{k},$$

thus proving the upper bound. Let

$$t = \left\lfloor \frac{d}{k} \right\rfloor + 1$$

and

$$\mathscr{A} = \{1, t, t^2, ..., t^{k-1}\}.$$

For any $x \in [0, t^k - 1]$ we have

$$x = \sum_{i=1}^{k-1} c_i t^i.$$

Since

$$\sum_{i=1}^{k} c_i \leq k(t-1) = k \left\lfloor \frac{d}{k} \right\rfloor \leq d,$$

we see that $d(0,x) \leq d$. Hence, $\mathrm{diam}(Cay(\mathbb{Z}_{t^k}, \mathscr{A}) \leq d$. Thus we see

$$m(d,k) \geq t^k = \left\lfloor \frac{d}{k} + 1 \right\rfloor^k.$$

Hsu and Jia [**?**] proved that

$$m(d,2) = \left\lfloor \frac{d(d+4)}{3} \right\rfloor + 1 \tag{1}$$

for all $d \geq 2$.

We will begin by examining 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 Algorithm to Construct a Lower Bound $m(d,k)$

We now provide an algorithm that takes as an input a set of generators and two sets of polynomial coefficients. 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 $[0, m-1]$.

2.1 Polynomial Construction

Let d be the diameter for $\mathrm{Cay}(m, \mathscr{A})$.
Our lower bound on $m(d,k)$ will be defined as a polynomial in terms of λ. Note that in the code, the representative data structures will be ordered from the higher-order to lower-order polynomial terms. 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.

2.1.1 Permutations of Generators and Coefficients

The permutations tested may be stored as data structures or file tables.

Given d define d_1 **fixed** to be $\frac{d}{\lambda}$. This will be the d referred to in the algorithm.

The purpose of the following data structures is to provide containers for the following: Define $\mathscr{A}$ to be a *set of generators*, $\mathscr{A} = (a_i)$ such that $a_i = \alpha_{i+1}a_{i+1}\lambda, \forall i \in [0, k-1]$, where a_i a sequence of nonnegative coefficients, and $|\mathscr{A}| = k$.
Define a *set of non-negative coefficients* $c_1, c_2, .., c_k$ such that $c_{i+1} < \alpha_i\lambda$.
Lastly, define a *second set of non-negative coefficients* $x_1, x_2, .., x_k$ such that $x_{i+1} < d - \sum_0^i x_i$. Assume that the set of generator combinations is defined as an upper-triangular two-dimensional array of unordered coefficients represented by tuples, the sequences of coefficients are defined as ordered lists of tuples.

Our representative polynomial can now be defined.

$$m(d,k) = a_1c_1 + a_2c_2 \cdots + a_kc_k = (\Pi_1^k\alpha_i)c_1\lambda^k + (\Pi_2^k\alpha_i)c_2\lambda^{k-1} \cdots (\alpha_k)c_k\lambda$$

Tuple Data Structure

```
template<TP, N>
class Tuple{

    vector<TP> data; // class contains an N-vector of type TP

    ...
};
```

Construction of the Coefficient Permutations

```
typedef Tuple<int, k> T;


// Construction of X-Coefficients
for(x1 = d; x1 >= 0; --x1)
{
  for(x2 = d - x1; x2 >= 0; --x2)
  {
     for(x3 = d - x1 - x2; x3 >= 0; --x3)
     {
        ...
            for(xk = d - x1 - x2 - x3 - .. - xk; xk >= 0; --xk)
            {
                 if(x1 + x2 + x3 + .. +xk <= d - k)
                 {
                      out << T(xk, xk-1, .. , x1); // In this case we are
                          storing in a data file.
```

```
                    ++size;
                }
            }
        ...
    }
  }
}

// Construction of M-Coefficients
for(int c1 = 1; c1 < (d^k / (k! * a1 * a2 * .. * ak-1)); ++c1)
{
  for(int c2 = 1; c2 < a1; ++c2)
  {
     for(int c3 = 1; c3 < a2; ++c3)
     {
         ...
             for(ck = 1; ck < ak-1; ++ck)
             {

                 out << T(ck, ck-1, .. , c1);
                 ++size;
             }
         ...
     }
  }
}

// Construction of Generators
for(a1 = 2; a1 < (d^k / k!); a1++) // We are using the trivial upper bound to
    constrain the size of the generators.
{
  for(a2 = 2; a2 < (d^k / k!); a2++)
  {
        ...
             if(a1 * a2 * .. * ak-1 < d^k / k!)
             {
                 out<< T(a1 * a2 *.. * ak-1, a2 * a3 * .. ak-1, ... , ak-1, 1)
                     ;
                 ++size;
             }
        ...
  }
}
```

2.1.2 Polynomial Construction

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 $d\mathscr{A}$ as a polynomial in terms of λ.

```
Polynomial P(Tuple A, Tuple Y);
```

Polynomial Data Structure

The basic polynomial data structure may be defined as follows:

```
class Polynomial{

    Tuple A;  // container for Generators
    Tuple Y;  // container for M-Coefficients or X-Coefficients
    int subtractions[k];
    ...
};
```

In the case where Polynomial P.Y is a container for the M-Coefficients, the class instance is a representation of the polynomial x. In the case where P.Y is a container for the X-Coefficients, the class instance is a representation of X'. P.Y[0] will refer to the largest polynomial coefficient. P.A[0] will refer to the largest corresponding generator.

2.1.3 Constructing a Representative Class of Polynomials

For all constructed polynomials $x = x_1a_1 + x_2a_2 + .. + x_ka_k$, 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.

Proposition 2.1. $\{(x_1, x_2, ..., x_k) | x_1 \leq c_1, x_2 \leq c_2, .., x_k \leq c_k,$ *and* $\sum_i x_i \leq d_1\}$ *define polynomials* x *that are considered to be* ***minimal****.*

Proposition 2.2. *The constructed polynomial* x *is defined to be* ***regular*** *if* $x \in [0, m-1]$.

We will use regular polynomials to determine whether or not $d\mathscr{A} = \mathbb{Z}_m$ 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 $(x_1, x_2, .., x_k)$ and $(c_1, c_2, .., c_k)$ from their respective polynomials.

Proposition 2.3. *$\forall x \in d\mathscr{A}$ 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 $d\mathscr{A} \cong \mathbb{Z}_m$.*

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 $x_1, x_2, x_3, ..., x_k$. The resulting low-order coefficients are then forced to be non-negative by adding the generator associated with the next higher-order term.
The number of times that the representative set cycles $\mathbb{Z}_m$ as well as the number of times that a generator needs to be "borrowed" into the next lowest-order term is saved to use to create the intervals bounding the representative coefficients in the mathematical proof.

```
// Overloaded polynomial subtraction operator.
Polynomial Polynomial::operator-(Polynomial m)
{
    loop:
    while( Y > rhs.Y )
    {
        Y = T(Y[0] - rhs.Y[0], Y[1] - rhs.Y[1], Y[2] - rhs.Y[2], ... , Y[k]
            - rhs.Y[k]);
        ++subtractions[0];
    }
    while( Y[1] < 0 )
    {
        Y = T(Y[0], Y[1] + (A[0] / A[1]), Y[2], ... , Y[k]);
        ++subtractions[1];
    }
    while( Y[2] < 0 )
    {
        Y = T(Y[0], Y[1], Y[2] + (A[1] / A[2]), ... , Y[k]);
        ++subtractions[2];
    }
    while( Y[3] < 0 )
    {
        Y = T(Y[0], Y[1], Y[2], Y[3] + (A[2] / A[3]), ... , Y[k]);
        ++subtractions[3];
    }
```

```
    ...

    while( Y[k-1] < 0 )
    {
        Y = T(Y[0], Y[1], Y[2], Y[3] + (A[2] / A[3]), ... , Y[k-1] + (A[k-2]
            / A[k-1]));
        ++subtractions[k-1];
    }
    if( Y > rhs.Y ){ goto loop; }

    return *this;
}
```

2.1.4 Construction of the Polynomial Bound

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

We will require that our polynomial representative of m to be regular, in order to ensure $x' \cong x$.

Proposition 2.4. *Define x' to be **regular** if $\forall x_i, x_i < c_{i+1}$.*

```
\\ Define a class function to return m, the summation of our polynomial bound.
TP Polynomial::value()
{
    return (a1*y1 + a2*y2 +   + ak*yk);
}

\\ Define a class function to check that x' is regular
bool Polynomial::isRegular()const
{
        return (Y[1] < ( A[0] / A[1]) && Y[2] < (A[1] / A[2]) && .. && Y[k] < (
            A[k-1] / A[k]));
}
```

Proposition 2.5. *$\forall n \in \mathbb{Z}_m$, $\exists x$ such that $\bar{x} = \bar{x'} = n$, then $d\mathscr{A} \supseteq \mathbb{Z}_m$.*

We will use a boolean array in order to check the inclusion of $\mathbb{Z}_m$ in $d\mathscr{A}$. Note that in order for the polynomial comparison to function properly, the tuple comparisons should be done in lexigraphical order as for regular tuples, this corresponds to the actual polynomial order.

```
Polynomial mbest; // Container for our best lower bound m.

vector<bool> cover;
T A; // Container for a generating set.
T Q; // Container for a set of M-Coefficients
T x; // Container for a set of X-Coefficients.
// NOTE: The A, Q, and X tuples are retrieved from a file or data structure.

for(i = 0; i < sizeof(generators) // Number of generating sets. ; ++i)
{
    T A(ak, ak-1, .., a1);

    for(j = 0; j < sizeof(mcoeffs) // Number of m-coefficients. ; ++j)
    {
        T Q(ck, ck-1, .., c1);

        Polynomial M(A, Q); // Create initial polynomial representation of
            the lower bound.

        cover.clear();
        if((M.value() > mbest.value())) // Ignore M that are too small.
        {
            for(k = 0; k < sizeof(xcoeffs) // Number of x-coefficients. ; ++k)
            {
                T x(xk, xk-1, .., x1);

                Polynomial X(A, x); // Create our initial representative.
                Polynomial X_prime(X-M); // Enforce regularity.
                if(X_prime.wellFormed())
                {
                    cover.push_back(1);
                }
            }
            if(accumulate(cover.begin(),cover.end(),0) == M.value())
            {
                mbest = M; // Store improved lower bound.
            }
        }
    }
}
```

Parallelization

The looping nature of the program makes it a natural candidate for optimization using parallel processing techniques. In this case, we have used a cluster of computer nodes. The largest dataset that is iterated over is the M-Coefficients, and can be a "bottleneck" in the program. Parallelization solves this problem by allowing a number of nodes that compute

extremely large datasets to compute for an extended time or even without completion. These larger computations will not interfere with nodes that are computing bounds based on subsequent generating sets. The effect of the multiple processes is that we are able to check a larger set of generators, in fact checking up to the current trivial lower bound of $\frac{d^k}{k!}$.

2.2 Complexity of the Algorithm

2.2.1 Generators and Coefficients

The complexity of the algorithm depends both on the number of generators as well as the chosen diameter, however since our program deals with smaller values of k, and our chosen diameter may be arbitrarily large, we will formulate our complexity analysis in terms of d. As we are checking all permutations of generators up to the upper bound $\frac{d^k}{k!}$, we are able to treat the coefficient $\frac{1}{(k!)^k}$ as a constant term and express the compexity as an average case in big-$\mathcal{O}$ notation. The number of operations per loop in the construction of the generators is on the order of $\mathcal{O}(d^k)$. The construction of the coefficients to generate our representative polynomial m is dependent on the individual generating set for which it is being constructed. In the worst case, the generating set will have large generators, allowing for the outermost loop to finish quickly, however, this will make it possible for the inner loops to approach or surpass the complexity of the larger, outermost loop. The complexity in this case is $\mathcal{O}(\max_{a\in\mathscr{A}}(a\cdot d)^k)$, where for most $a \in \mathscr{A}$, $a < d$. In the best case, the generating set will have small coefficients, in which case the outermost loop will have complexity of $\Omega(\max_{a\in\mathscr{A}}(\frac{d}{a})^k)$, and the inner loops will finish quickly. The final complexity of the loop structure in this case can be described as $\Theta(d^k)$. Finally, the coefficients for our representative polynomial are generated in $\mathcal{O}(d^k)$.

2.2.2 Polynomial Bound

The generation of the polynomial bound is again a nested loop structure which checks each possible representative for each possible combination for each generating set that can be created where each generator is the largest possible multiple it can take for its position up to the trivial upper bound. We can describe the complexity of this main program as $\mathcal{O}(d^k)\cdot\Theta(d^k)\cdot\mathcal{O}(d^k) = \mathcal{O}(d^{k^3})$. As we found, the size of the coefficient set for the polynomial

bound depends largely on the specific generating set being examined, significantly affecting the complexity of the inner loops (or coefficient loops).

3 A New Lower Bound for $m(2,k)$

Let d and k be positive integers. Let $n(d,k)$ denote the largest positive integer n such that there exists a subset $\mathscr{A}$ of k positive integers with the property that every integer in the interval $[0,n]$ is the sum of at most d not necessarily distinct elements of $\mathscr{A}$. In other words,

$$n(d,k) = \max_{\substack{\mathscr{A}\subset\mathbb{Z}^+ \\ |\mathscr{A}|=k}} \{n \mid d\mathscr{A} \supseteq [0,n]\}.$$

Recall that $d\mathscr{A}$ denotes the set of all sums of at most d not necessarily distinct elements of $\mathscr{A}$. The computation of $n(d,k)$ is often referred as the *postage stamp problem*. The postage stamp problem is an old problem in number theory that has been studied extensively. See [**?**, **?**, **?**] for more information. A simple construction shows that

$$n(2,k) \geq \frac{1}{4}k^2 + O(k).$$

Rohrbach [**?**] conjectured in 1937 that

$$n(2,k) \sim \frac{1}{4}k^2, \tag{2}$$

Hämmerer and Hofmeister [**?**] proved in 1976 by an explicit construction of a 2-basis that

$$n(2,k) \geq \frac{5}{18}k^2 + O(k),$$

which disproves the conjecture of Rohrbach (**??**). The best known lower bound for $n(2,k)$ was proved by Mrose [**?**]

$$n(2,k) \geq \frac{2}{7}k^2 + \frac{12}{7}k + O(1) \qquad \text{as} \quad k \to \infty. \tag{3}$$

If $d\mathscr{A} \supseteq [0,n]$ then $d\mathscr{A} = \mathbb{Z}_{n+1}$. Therefore, for all positive integers d and k we have

$$m(d,k) \geq n(d,k) + 1.$$

This implies the best known lower bound for $m(2,k)$ in (**??**) before our result in this paper. Our proof uses a similar construction to one used by Torleiv Klove and Mossige used to prove the above lower bound on $n(2,k)$ in (**??**). We used a computer program to test candidates for the values that appeared in the proof as the subscripts μ, ν and η. It is likely that our result could be improved upon by a more complicated construction using a larger number of the same types of subsets. However, testing larger constructions becomes computationally difficult, and there is a theoretical limit of $1/3$ on the leading coefficient of such a construction. Any lower bound better than $\frac{1}{3}k^2 + O(k)$ would be of interest.

Theorem 3.1. *$m(2,k) \geq \dfrac{37}{121}k^2 + O(k)$ as $k \to \infty$.*

et $k \geq 14$ be an integer. Let $k_1 = \left\lfloor \dfrac{k-3}{11} \right\rfloor$. Let $m = 37k_1^2$. Define

$$\begin{aligned} I_\mu &= [\mu k_1^2, \mu k_1^2 + k_1], && \mu = 0, 4, 15, 26; \\ S_\nu &= \{\nu k_1^2 + ik_1 \mid i = 0, 1, ..., k_1 - 1\}, && \nu = 0, 1, 2, 3; \\ T_\eta &= \{\eta k_1^2 + i(k_1+1) \mid i = 0, 1, ..., k_1 - 1\}, && \eta = 10, 20, 30. \end{aligned}$$

Let $S = S_0 \cup S_1 \cup S_2 \cup S_3$, and define

$$\mathscr{A} = I_0 \cup I_4 \cup I_{15} \cup I_{26} \cup S \cup T_{10} \cup T_{20} \cup T_{30}.$$

Noting that $I_0 \cap S_0 = \{0\}$, and

$$|I_\mu| = k_1 + 1, \quad |S_\nu| = k_1, \quad \text{and} \quad |T_\eta| = k_1,$$

we see that

$$|\mathscr{A}| \leq 11k_1 + 3 \leq k.$$

We now prove that $\mathscr{A} + \mathscr{A} = \mathbb{Z}_m$. We begin by claiming $I_\mu + T_\eta \supseteq [(\mu+\eta)k_1^2, (\mu+\eta+1)k_1^2)$. Let $n \in [(\mu+\eta)k_1^2, (\mu+\eta+1)k_1^2)$. Then we can write n as

$$n = (\mu+\eta)k_1^2 + qk_1 + r,$$

where $0 \leq q < k_1$ and $0 \leq r < k_1$.

If $r \geq q$, then $0 \leq r - q < k_1$ and

$$n = \mu k_1^2 + (r-q) + \eta k_1^2 + q(k_1+1).$$

Since

$$\mu k_1^2 + (r-q) \in I_\mu \qquad \text{and} \qquad \eta k_1^2 + q(k_1+1) \in T_\eta,$$

we see that $n \in I_\mu + T_\eta$.

If $r < q$, then we must have $q \geq 1$ and $0 \leq k_1 + r - q + 1 \leq k_1$. Then

$$\mu k_1^2 + (k_1 + r - q + 1) \in I_\mu \qquad \text{and} \qquad \eta k_1^2 + (q-1)(k_1+1) \in T_\eta.$$

Hence

$$n = \mu k_1^2 + (k_1 + r - q + 1) + \eta k_1^2 + (q-1)(k_1+1) \in I_\mu + T_\eta.$$

Next we claim that $I_\mu + S_\nu \supseteq [(\mu+\nu)k_1^2, (\mu+\nu+1)k_1^2)$. Let $n \in [(\mu+\nu)k_1^2, (\mu+\nu+1)k_1^2)$. Then we can write n as

$$n = (\mu+\nu)k_1^2 + qk_1 + r = \mu k_1^2 + r + \nu k_1^2 + qk_1,$$

where $0 \leq q < k_1$ and $0 \leq r < k_1$, such that

$$\mu k_1^2 + r \in I_\mu \qquad \text{and} \qquad \nu k_1^2 + qk_1 \in S_\nu,$$

so $n \in I_\mu + S_\nu$.

Our final claim is $S + T_\eta \supseteq [(\eta+1)k_1^2, (\eta+4)k_1^2)$. Let $n \in [(\eta+1)k_1^2, (\eta+4)k_1^2)$. Then we can write n as

$$n = (\eta+\nu)k_1^2 + qk_1 + r,$$

where $1 \leq \nu \leq 3$, $0 \leq q < k_1$, and $0 \leq r < k_1$.

If $q \geq r$, then

$$n = \nu k_1^2 + (q-r)k_1 + \eta k_1^2 + r(k_1+1),$$

where $\nu k_1^2 + (q-r)k_1 \in S_\nu$ and $\eta k_1^2 + d(k_1+1) \in T_\eta$, so $n \in S_\nu + T_\eta$.

If $q < r$, then

$$n = (\nu-1)k_1^2 + (k_1+q-r)k_1 + \eta k_1^2 + r(k_1+1),$$

where

$$(\nu-1)k_1^2 + (k_1+q-r)k_1 \in S_{\nu-1} \qquad \text{and} \qquad \eta k_1^2 + r(k_1+1) \in T_\eta.$$

Hence $n \in S_{\nu-1} + T_\eta \subseteq S + T_\eta$. It is clear that, in $\mathbb{Z}_{37k_1^2}$,

$$\begin{aligned}
[45k_1^2, 46k_1^2) &= [8k_1^2, 9k_1^2), \\
[46k_1^2, 47k_1^2) &= [9k_1^2, 10k_1^2), \\
[56k_1^2, 57k_1^2) &= [19k_1^2, 20k_1^2).
\end{aligned}$$

Therefore, we have proved that the entire interval $[0, m) = \mathbb{Z}_m$ can be *covered* as follows:

$$\begin{aligned}
I_0 + S &\supseteq [0, 4k_1^2), \\
I_4 + S &\supseteq [4k_1^2, 8k_1^2), \\
I_{15} + T_{30} &\supseteq [45k_1^2, 46k_1^2) = [8k_1^2, 9k_1^2), \\
I_{26} + T_{20} &\supseteq [46k_1^2, 47k_1^2) = [9k_1^2, 10k_1^2), \\
I_0 + T_{10} &\supseteq [10k_1^2, 11k_1^2), \\
S + T_{10} &\supseteq [11k_1^2, 14k_1^2), \\
I_4 + T_{10} &\supseteq [14k_1^2, 15k_1^2), \\
I_{15} + S &\supseteq [15k_1^2, 19k_1^2), \\
I_{26} + T_{30} &\supseteq [56k_1^2, 57k_1^2) = [19k_1^2, 20k_1^2), \\
I_0 + T_{20} &\supseteq [20k_1^2, 21k_1^2), \\
S + T_{20} &\supseteq [21k_1^2, 24k_1^2), \\
I_4 + T_{20} &\supseteq [24k_1^2, 25k_1^2),
\end{aligned}$$

$$\begin{aligned}
I_{15} + T_{10} &\supseteq [25k_1^2, 26k_1^2), \\
I_{26} + S &\supseteq [26k_1^2, 30k_1^2), \\
I_0 + T_{30} &\supseteq [30k_1^2, 31k_1^2), \\
S + T_{30} &\supseteq [31k_1^2, 34k_1^2), \\
I_4 + T_{30} &\supseteq [34k_1^2, 35k_1^2), \\
I_{15} + T_{20} &\supseteq [35k_1^2, 36k_1^2), \\
I_{26} + T_{10} &\supseteq [36k_1^2, 37k_1^2).
\end{aligned}$$

It now follows that

$$\mathscr{A} + \mathscr{A} \supseteq [0, 37k_1^2).$$

Hence

$$\begin{aligned} m(2,k) &\geq 37k_1^2 \\ &= 37 \cdot \left\lfloor \frac{k-2}{11} \right\rfloor^2 \\ &> 37 \left(\frac{k-2}{11} - 1 \right)^2 \\ &= \frac{37}{121}k^2 - \frac{962}{121}k + \frac{6253}{121} \\ &= \frac{37}{121}k^2 + O(k) \qquad \text{as} \quad k \to \infty. \end{aligned}$$

Theorem **??** is proved.

4 Extension to the General Case

Theorem 4.1. *For any integer $d \geq 2$, as $k \to \infty$, we have*

$$m(d,k) \geq \left(\frac{148}{121}\right)^{\lfloor \frac{d}{2} \rfloor} \left(\frac{k}{d}\right)^d + O(k^{d-1}).$$

Before we start the proof of Theorem **??**, we state and prove the following addition lemma for $m(d,k)$.

Lemma 4.1. *Given positive integers k_1, k_2, $d_1 \geq 2$ and $d_2 \geq 2$, we have*

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

Proof of Lemma **??**. Let $\mathscr{A}_1$ and $\mathscr{A}_2$ be sets of positive integers such that $m(d_1,\mathscr{A}_1) = m(d_1,k_1)$ and $m(d_2,\mathscr{A}_2) = m(d_2,k_2)$. Since $d_1, d_2 \geq 2$ we have that $m(d_1,k_1)$ is greater than every element in $\mathscr{A}_1$, and similarly for $m(d_2,k_2)$ and $\mathscr{A}_2$. So let $\mathscr{A} = \mathscr{A}_1 \cup \{m(d_1,k_1) \cdot x \mid x \in \mathscr{A}_2\}$. Then it suffices to show that $\mathscr{A}$ is a (d_1+d_2)-basis for $\mathbb{Z}_{m(d_1,k_1)m(d_2,k_2)}$. We do this by writing $n \in \mathbb{Z}_{m(d_1,k_1)m(d_2,k_2)}$ as $xm(d_1,k_1) + r$ where $x \in \mathbb{Z}_{m(d_2,k_2)}$ and $r \in \mathbb{Z}_{m(d_1,k_1)}$. Then $xm(d_1,k_1) \in d_1\mathscr{A}_1\{m(d_1,k_1) \cdot x \mid x \in \mathscr{A}_2\}$ and $r \in d_2\mathscr{A}_1$, so $n \in (d_1+d_2)\mathscr{A}$. □

Proof of Theorem **??**. Let $d = 2q + r$ where $q = \left\lfloor \frac{d}{2} \right\rfloor$ and $k = du + v$ where $u = \left\lfloor \frac{k}{d} \right\rfloor$. We separate the calculation into two cases. Case 1: If $r = 0$, then

$$\begin{aligned} m(d,k) &= m(2q, du+v) \\ &= m(2q, (2q)u+v) \\ &\geq m(2q, 2qu) \geq m(2,2u)^q \\ &\geq \left(\frac{37}{121}(2u)^2 + O(u)\right)^q \\ &= \left(\frac{148}{121}\left(\frac{k-v}{d}\right)^2 + O(u)\right)^{\frac{d}{2}} \\ &= \left(\frac{148}{121}\right)^{\frac{d}{2}}\left(\frac{k}{d}\right)^d + O(k^{d-1}) \end{aligned}$$

Case 2: If $r = 1$, then

$$\begin{aligned} m(d,k) &= m(2q+1, du+v) \\ &= m(2q+1, (2q+1)u+v) \\ &\geq m(2q+1, 2qu+u) \geq m(2,2u)^q \cdot m(1,u) \\ &\geq \left(\frac{37}{121}(2u)^2 + O(u)\right)^q \cdot (u+1) \\ &= \left(\frac{148}{121}u^2 + O(u)\right)^{\frac{d-1}{2}} \cdot (u+1) \\ &= \left(\frac{148}{121}^{\frac{d-1}{2}} u^{d-1} + O(u^{d-2})\right) \cdot (u+1) \\ &= \frac{148}{121}^{\frac{d-1}{2}} u^d + O(u^{d-1}) \\ &= \left(\frac{148}{121}\right)^{\frac{d-1}{2}}\left(\frac{k}{d}\right)^d + O(k^{d-1}) \end{aligned}$$

Hence

$$m(d,k) \geq \left(\frac{148}{121}\right)^{\lfloor \frac{d}{2} \rfloor}\left(\frac{k}{d}\right)^d + O(k^{d-1}).$$

The proof of Theorem **??** is complete. □

5 A Lower Bound of $m(d, 4)$.

In 1974, Wong and Coppersmith proved that

$$m(d,k) \geq \left(\frac{d}{k}+1\right)^k.$$

In the case when $k = 4$, this gives the lower bound to be

$$m(d,k) \geq \left(\frac{d}{4}\right)^4 + O(d^3).$$

Jia later improved this lower bound, and proved that

$$m(d,4) \geq 2.048\left(\frac{d}{4}\right)^4 + O(d^3) \qquad \text{as} \quad d \to \infty.$$

In 1992, Chen and Gu proved that

$$m(d,4) \geq 3.2768\left(\frac{d}{4}\right)^4 + \mathcal{O}(d^3) \qquad \text{as} \quad d \to \infty.$$

In this paper we will show that

$$m(d,4) \geq \frac{512}{243}\left(\frac{d}{4}\right)^4 + O(d^3) \approx 2.106996\left(\frac{d}{4}\right)^4 + O(d^3).$$

This is not an improvement on the 1992 bound, but is instead given as an example of a proof of a lower bound derived from our computational algorithm.

Theorem 5.1. *As $d \to \infty$,*

$$m(d,4) \geq \frac{512}{243}\left(\frac{d}{4}\right)^4 + O(d^3) \approx 2.106996\left(\frac{d}{4}\right)^4 + O(d^3).$$

Proof. Let $d \geq 11$ be an integer and let $\lambda = \left\lfloor \frac{d-2}{9} \right\rfloor$. Define

$$\begin{aligned}
\alpha &= 3\lambda, \\
\beta &= 3\lambda\alpha, \\
\gamma &= 3\lambda\beta, \\
m &= 2\lambda\gamma + \lambda\beta + \lambda\alpha + \lambda.
\end{aligned}$$

Let $A = \{1, \alpha, \beta, \gamma\}$. Then

$$\begin{aligned} m &= 2\lambda d + \lambda c + \lambda b + \lambda \\ &= 54\lambda^4 + 9\lambda^3 + 3\lambda^2 + \lambda \\ &= \frac{512}{243}\left(\frac{d}{4}\right)^4 + O(d^3). \end{aligned}$$

Let dA denote the set of all sums of at most d not necessarily distinct elements of a generating set A of $\mathbb{Z}_m$. Then for this proof we need to show that $dA = \mathbb{Z}_m$ such that the Cayley digraph $\mathrm{Cay}(m, A)$ has diameter $d(m, A) \leq d$.

Every integer n such that $0 \leq n < m$ can be expressed in the following way:

$$n = w + x\alpha + y\beta + z\gamma$$

where

$$0 \leq w \leq 3\lambda, \quad 0 \leq x \leq 3\lambda, \quad 0 \leq y \leq 3\lambda, \quad 0 \leq z \leq 2\lambda.$$

Thus we only need to show, for every $0 \leq n < m$, there exists nonnegative integers δ_1, δ_2, δ_3, and δ_4 such that we can write n as

$$n \equiv \delta_1 + \delta_2\alpha + \delta_3\beta + \delta_4\gamma$$

where

$$\delta_1 + \delta_2 + \delta_3 + \delta_4 \leq d.$$

We now consider the following cases:

Case 1. $0 \leq x_3 < \lambda$. The following subcases need to be considered:
Subcase 1.a. If $2\lambda \leq x_1 < 3\lambda$ then $0 \leq x_0 < 2\lambda$.
If $0 \leq x_1 < 2\lambda$, we have

$$x_0 + x_1 + x_2 + x_3 \leq 3\lambda + 2\lambda + 3\lambda + \lambda = 9\lambda \leq d,$$

which implies that $n = x_0 + x_1\alpha + x_2\beta + x_3\gamma \in dA$.
If $2\lambda \leq x_1 < 3\lambda$ and $0 \leq x_0 < 2\lambda$, we have

$$x_0 + x_1 + x_2 + x_3 \leq 2\lambda + 3\lambda + 3\lambda + \lambda = 9\lambda \leq d,$$

which implies that $n = x_0 + x_1\alpha + x_2\beta + x_3\gamma \in dA$.

Subcase 1.b. $2\lambda \le x_2 < 3\lambda$, $2\lambda \le x_1 < 3\lambda$, $2\lambda \le x_0 < 3\lambda$.
We have

$$\begin{aligned} n \equiv n + m &= x_0 + x_1\alpha + x_2\beta + x_3\gamma + \lambda + \lambda\alpha + \lambda\beta + 2\lambda\gamma \\ &= x_0 + \lambda + (x_1 + \lambda)\alpha + (x_2 + \lambda)\beta + (x_3 + 2\lambda)\gamma \\ &= x_0 - 2\lambda + (x_1 - 2\lambda + 1)\alpha + (x_2 + \lambda + 1)\beta + (x_3 + 2\lambda)\gamma. \end{aligned}$$

Noting that

$$x_0 - 2\lambda \ge 0, x_1 - 2\lambda + 1 \ge 0, x_2 + \lambda + 1 \ge 0, \text{ and } x_3 + 2\lambda \ge 0,$$

we see that

$$\begin{aligned} x_0 - 2\lambda + x_1 - 2\lambda + 1 + x_2 + \lambda + 1 + x_3 + 2\lambda = x_0 + x_1 + x_2 + x_3 - \lambda + 2 \\ \le 3\lambda + 3\lambda + 3\lambda + \lambda - \lambda + 2 \\ = 9\lambda + 2 \le d, \end{aligned}$$

which implies that $n = x_0 + x_1\alpha + x_2\beta + x_3\gamma \in dA$.

Case 2. $\lambda \le x_3 < 2\lambda$. The following subcases need to be considered:
Subcase 2.a. $0 \le x_2 < 2\lambda$. If $2\lambda \le x_1 < 3\lambda$ then $0 \le x_0 < 2\lambda$.
If $0 \le x_1 < 2\lambda$, we have

$$x_0 + x_1 + x_2 + x_3 \le 2\lambda + 2\lambda + 2\lambda + 3\lambda = 9\lambda \le d,$$

which implies that $n = x_0 + x_1\alpha + x_2\beta + x_3\gamma \in dA$.
If $2\lambda \le x_1 < 3\lambda$ and $0 \le x_0 < 2\lambda$, we have

$$x_0 + x_1 + x_2 + x_3 \le 2\lambda + 2\lambda + 3\lambda + 2\lambda = 9\lambda \le d,$$

which implies that $n = x_0 + x_1\alpha + x_2\beta + x_3\gamma \in dA$.

Subcase 2.b. $\lambda \le x_2 < 2\lambda$, $2\lambda \le x_1 < 3\lambda$, $2\lambda \le x_0 < 3\lambda$.
We have

$$\begin{aligned} n \equiv n + m &= x_0 + x_1\alpha + x_2\beta + x_3\gamma + \lambda + \lambda\alpha + \lambda\beta + 2\lambda\gamma \\ &= x_0 + \lambda + (x_1 + \lambda)\alpha + (x_2 + \lambda)\beta + (x_3 + 2\lambda)\gamma \\ &= x_0 - 2\lambda + (x_1 - 2\lambda + 1)\alpha + (x_2 + \lambda + 1)\beta + (x_3 + 2\lambda)\gamma. \end{aligned}$$

Noting that

$$x_0 - 2\lambda \geq 0,\ x_1 - 2\lambda + 1 \geq 0,\ x_2 + \lambda + 1 \geq 0,\ \text{and } x_3 + 2\lambda \geq 0,$$

we see that

$$\begin{aligned} x_0 - 2\lambda + x_1 - 2\lambda + 1 + x_2 + \lambda + 1 + x_3 + 2\lambda &= x_0 + x_1 + x_2 + x_3 - \lambda + 2 \\ &\leq 3\lambda + 3\lambda + 2\lambda + 2\lambda - \lambda + 2 \\ &= 9\lambda + 2 \leq d, \end{aligned}$$

which implies that $n = x_0 + x_1\alpha + x_2\beta + x_3\gamma \in dA$.

Subcase 2.c. $2\lambda \leq x_2 < 3\lambda$. If $\lambda \leq x_1 < 2\lambda$ then $0 \leq x_0 < 2\lambda$.
If $0 \leq x_1 < \lambda$, we have

$$x_0 + x_1 + x_2 + x_3 \leq 3\lambda + \lambda + 3\lambda + 2\lambda = 9\lambda \leq d,$$

which implies that $n = x_0 + x_1\alpha + x_2\beta + x_3\gamma \in dA$.
If $\lambda \leq x_1 < 2\lambda$ and $0 \leq x_0 < 2\lambda$, we have

$$x_0 + x_1 + x_2 + x_3 \leq 2\lambda + 2\lambda + 3\lambda + 2\lambda = 9\lambda \leq d,$$

which implies that $n = x_0 + x_1\alpha + x_2\beta + x_3\gamma \in dA$.

Subcase 2.d. $2\lambda \leq x_2 < 3\lambda$, $\lambda \leq x_1 < 2\lambda$, $2\lambda \leq x_0 < 3\lambda$.
We have

$$\begin{aligned} n \equiv n + m &= x_0 + x_1\alpha + x_2\beta + x2_3\gamma + \lambda + \lambda\alpha + \lambda\beta + 2\lambda\gamma \\ &= x_0 + \lambda + (x_1 + \lambda)\alpha + (x_2 + \lambda)\beta + (x_3 + 2\lambda)\gamma \\ &= x_0 - 2\lambda + (x_1 + \lambda + 1)\alpha + (x_2 - 2\lambda)\beta + (x_3 + 2\lambda + 1)\gamma. \end{aligned}$$

Noting that

$$x_0 - 2\lambda \geq 0,\ x_1 + \lambda + 1 \geq 0,\ x_2 - 2\lambda \geq 0,\ \text{and } x_3 + 2\lambda + 1 \geq 0,$$

we see that

$$\begin{aligned} x_0 - 2\lambda + x_1 + \lambda + 1 + x_2 - 2\lambda + x_3 + 2\lambda + 1 &= x_0 + x_1 + x_2 + x_3 - \lambda + 2 \\ &\leq 3\lambda + 2\lambda + 3\lambda + 2\lambda - \lambda + 2 \\ &= 9\lambda + 2 \leq d, \end{aligned}$$

which implies that $n = x_0 + x_1\alpha + x_2\beta + x_3\gamma \in dA$.

Subcase 2.e. $2\lambda \leq x_2 < 3\lambda$, $2\lambda \leq x_1 < 3\lambda$, $0 \leq x_0 < 2\lambda$.
We have

$$\begin{aligned} n \equiv n + m &= x_0 + x_1\alpha + x_2\beta + x_3\gamma + \lambda + \lambda\alpha + \lambda\beta + 2\lambda\gamma \\ &= x_0 + \lambda + (x_1 + \lambda)\alpha + (x_2 + \lambda)\beta + (x_3 + 2\lambda)\gamma \\ &= x_0 + \lambda + (x_1 - 2\lambda)\alpha + (x_2 - 2\lambda + 1)\beta + (x_3 + 2\lambda + 1)\gamma. \end{aligned}$$

Noting that

$$x_0 + \lambda \geq 0,\ x_1 - 2\lambda \geq 0,\ x_2 - 2\lambda + 1 \geq 0,\ \text{and } x_3 + 2\lambda + 1 \geq 0,$$

we see that

$$\begin{aligned} x_0 + \lambda + x_1 - 2\lambda + x_2 - 2\lambda + 1 + x_3 + 2\lambda + 1 &= x_0 + x_1 + x_2 + x_3 - \lambda + 2 \\ &\leq 2\lambda + 3\lambda + 3\lambda + 2\lambda - \lambda + 2 \\ &= 9\lambda + 2 \leq d, \end{aligned}$$

which implies that $n = x_0 + x_1\alpha + x_2\beta + x_3\gamma \in dA$.

Subcase 2.f. $2\lambda \leq x_2 < 3\lambda$, $2\lambda \leq x_1 < 3\lambda$, $2\lambda \leq x_0 < 3\lambda$.
We have

$$\begin{aligned} n \equiv n + m &= x_0 + x_1\alpha + x_2\beta + x_3\gamma + \lambda + \lambda\alpha + \lambda\beta + 2\lambda\gamma \\ &= x_0 + \lambda + (x_1 + \lambda)\alpha + (x_2 + \lambda)\beta + (x_3 + 2\lambda)\gamma \\ &= x_0 - 2\lambda + (x_1 - 2\lambda + 1)\alpha + (x_2 - 2\lambda + 1)\beta + (x_3 + 2\lambda + 1)\gamma. \end{aligned}$$

Noting that

$$x_0 - 2\lambda \geq 0,\ x_1 - 2\lambda + 1 \geq 0,\ x_2 - 2\lambda + 1 \geq 0,\ \text{and } x_3 + 2\lambda + 1 \geq 0,$$

we see that

$$\begin{aligned} x_0 - 2\lambda + x_1 - 2\lambda + 1 + x_2 - 2\lambda + 1 + x_3 + 2\lambda + 1 &= x_0 + x_1 + x_2 + x_3 - 4\lambda + 3 \\ &\leq 3\lambda + 3\lambda + 3\lambda + 2\lambda - 4\lambda + 3 \\ &= 7\lambda + 2 \leq d, \end{aligned}$$

which implies that $n = x_0 + x_1\alpha + x_2\beta + x_3\gamma \in dA$.

Case 3. $2\lambda \leq x_3 < 3\lambda$. The following subcases need to be considered:
Subcase 3.a. $0 \leq x_2 < \lambda$. If $2\lambda \leq x_1 < 3\lambda$ then $0 \leq x_0 < 2\lambda$.
If $0 \leq x_1 < 2\lambda$, we have

$$x_0 + x_1 + x_2 + x_3 \leq 3\lambda + 2\lambda + \lambda + 3\lambda = 9\lambda \leq d,$$

which implies that $n = x_0 + x_1\alpha + x_2\beta + x_3\gamma \in dA$.
If $2\lambda \leq x_1 < 3\lambda$ and $0 \leq x_0 < 2\lambda$, we have

$$x_0 + x_1 + x_2 + x_3 \leq 2\lambda + 3\lambda + \lambda + 3\lambda = 9\lambda \leq d,$$

which implies that $n = x_0 + x_1\alpha + x_2\beta + x_3\gamma \in dA$.

Subcase 3.b. $0 \leq x_2 < \lambda$, $2\lambda \leq x_1 < 3\lambda$, $2\lambda \leq x_0 < 3\lambda$.
We have

$$\begin{aligned} n \equiv n + m &= x_0 + x_1\alpha + x_2\beta + x_3\gamma + \lambda + \lambda\alpha + \lambda\beta + 2\lambda\gamma \\ &= x_0 + \lambda + (x_1 + \lambda)\alpha + (x_2 + \lambda)\beta + (x_3 + 2\lambda)\gamma \\ &= x_0 - 2\lambda + (x_1 - 2\lambda + 1)\alpha + (x_2 + \lambda + 1)\beta + (x_3 + 2\lambda)\gamma. \end{aligned}$$

Noting that

$$x_0 - 2\lambda \geq 0,\ x_1 - 2\lambda + 1 \geq 0,\ x_2 + \lambda + 1 \geq 0,\ \text{and } x_3 + 2\lambda \geq 0,$$

we see that

$$\begin{aligned} x_0 - 2\lambda + x_1 - 2\lambda + 1 + x_2 + \lambda + 1 + x_3 + 2\lambda &= x_0 + x_1 + x_2 + x_3 - \lambda + 2 \\ &\leq 3\lambda + 3\lambda + \lambda + 3\lambda - \lambda + 2 \\ &= 9\lambda + 2 \leq d, \end{aligned}$$

which implies that $n = x_0 + x_1\alpha + x_2\beta + x_3\gamma \in dA$.

Subcase 3.c. $\lambda \leq x_2 < 2\lambda$ and $0 \leq x_1 < 2\lambda$. If $\lambda \leq x_1 < 2\lambda$ then $0 \leq x_0 < \lambda$.
If $0 \leq x_1 < \lambda$, we have

$$x_0 + x_1 + x_2 + x_3 \leq 3\lambda + \lambda + 2\lambda + 3\lambda = 9\lambda \leq d,$$

which implies that $n = x_0 + x_1\alpha + x_2\beta + x_3\gamma \in dA$.
If $\lambda \leq x_1 < 2\lambda$ and $0 \leq x_0 < \lambda$, we have

$$x_0 + x_1 + x_2 + x_3 \leq \lambda + 2\lambda + 2\lambda + 3\lambda = 8\lambda \leq d,$$

which implies that $n = x_0 + x_1\alpha + x_2\beta + x_3\gamma \in dA$.

Thus we have shown that every element $0 \leq n < m$ is contained in dA, which implies the diameter of the Cayley digraph $\mathrm{Cay}(\mathbb{Z}_m, A)$ is less than or equal to d. Hence,

$$m(d,4) \geq 2.048\left(\frac{d}{4}\right)^4 + O(d^3) \qquad \text{as} \quad d \to \infty. \qquad \square$$

6 Open Problems

1. Finding a non-trivial lower bound for $m(3,k)$, $m(4,k)$, etc.

2. For $n(d,k)$ it is known that for every positive integer k the limit

$$\lim_{d\to\infty} \frac{n(d,k)}{d^k}$$

exists, and the value is known for $k = 1$, 2 and 3. It is not known whether or not

$$\lim_{d\to\infty} \frac{m(d,k)}{d^k}$$

exists for every k, and the value is only known for $k = 1$ and 2.

3. The limits

$$\lim_{d\to\infty} \frac{m(d,k)}{n(d,k)} \text{ and } \lim_{k\to\infty} \frac{m(d,k)}{n(d,k)}$$

are also of interest, if they exist.

4. We may define the undirected version of our extremal function $M(d,k)$ to be the largest M such that there exists of symmetric set $\mathscr{A}$ of k elements and their additive inverses such that $\mathrm{diam}(Cay(\mathbb{Z}_M, \mathscr{A})) \leq d$. Little is known about $M(d,k)$, for fixed d and $k \geq 3$.

5. We may also define the average version of our extremal function $\bar{m}(d,k)$ to be the largest m such that there exists a set $\mathscr{A}$ of k elements such that the average distance between any two vertices in $Cay(\mathbb{Z}_m, \mathscr{A})$ is less than d. New lower bounds for $k \geq 3$ would be interesting for this function as well.

6. Although this paper is primarily concerned with lower bounds, upper bounds on $m(d,k)$ (and related functions) are also of interest.