SLOVAK UNIVERSITY OF TECHNOLOGY
FACULTY OF CIVIL ENGINEERING

Cayley graphs of given degree and diameter on linear groups

Bachelor Thesis

ï£¡tudijny program:	Matematicko-pocï£¡tacovï£¡ modelovanie
ï£¡tudijny odbor:	Aplikovanï£¡ matematika
ï£¡koliace pracovisko:	dopln ma
Vedï£¡ci diplomovej prï£¡ce:	dopln ma

BRATISLAVA 2018
Matï£¡ï£¡ Behun

Contents

1 Introduction

In its simplest form, networks can be modeled by graphs in a natural way in which network nodes are represented by vertices of the graph and links between nodes are represented by undirected edges of the graph. Restrictions on the network, such as limits on the number of links attached to a node, or limits on the number of links needed to connect any two nodes, or the length of a shortest circuit, then transform to restrictions on the graph model (for the indicated cases these would be restrictions on vertex degrees, on the diameter, and on the girth of the graph).

In graph theory this leads to two important problems: the *degree/diameter problem* to construct the largest possible graphs of a given maximum degree and a given diameter, and the *degree/girth problem* to construct the smallest possible regular graphs of a given degree and a given girth; in both cases the adjectives 'large' and 'small' refer to the order (i.e., the number of vertices) of a graph. The survey papers [8] and [4], respectively, contain a large amount of information on both problems. In this work we primarily address the degree/diameter problem restricted to Cayley graphs of certain two-dimensional linear groups, giving details in what follows.

2 The degree/diameter problem

2.1 The Moore bound

There is theoretical upper bound named after E. F. Moore for the largest order of a graph with given diameter $k \geq 1$ and maximum degree $d \geq 2$, which one can derive by building a spanning tree of such a graph. A fixed vertex v of such a graph has at most d neighbours at distance 1. Each of these neighbours has at most $d-1$ vertices at distance 1 from themselves, giving at most $d(d-1)$ vertices at distance 2 from v. Iterating this process ne obtains at most $d(d-1)^{i-1}$ vertices at distance i from v. By the diameter requirement, we have at most $d(d-1)^{k-1}$ vertices at distance k from v. Summing up, the largest order $n_{d,k}$ of a graph of maximum degree $d \geq 2$ and diameter $k \geq 1$ is at most $M_{d,k}$, the Moore bound for the pair (d,k), where

$$\begin{aligned} n_{d,k} \leq M_{d,k} &= 1 + d + d(d-1) + \cdots + d(d-1)^{k-1} \\ &= 1 + d(1 + (d-1) + \cdots + (d-1)^{k-1}) \\ &= \begin{cases} 1 + d\frac{(d-1)^k - 1}{d-2}, & \text{if } d > 2 \\ 2k+1, & \text{if } d = 2 \end{cases} \end{aligned} \tag{1}$$

2.2 Moore graphs

It is well known that equality in (1) holds only if $d = 2$ (for any $k \geq 1$), or $k = 1$ (for any $d \geq 2$), or for $k = 2$ and $d \in \{3, 7\}$, and possibly for the pair $(d,k) = (57, 2)$ but for no other $d \geq 2$ and $k \geq 1$. All the graphs for which $n_{d,k} = M_{d,k}$ are called *Moore graphs*; they are necessarily regular and in the order of the listed parameters they are cycles of length $2k+1$, complete graphs of order $d+1$, the Petersen graphs and the Hoffman-Singleton graph.

Research into the degree/diameter problem and into Moore graphs in particular was initiated by Hoffman and Singleton in [6] who proved that Moore graphs of diameter $k = 2$ can exist only for $d \in \{2, 3, 7\}$ and possibly 57, proving also their uniqueness except for the last case, and establishing also that the unique Moore graph of diameter 3 is the cycle of length 7. Their proofs exploit eigenvalues and eigenvectors of adjacency matrices (and the corresponding principal submatrices) of graphs.

2.3 Graphs of order close to the Moore bound

To facilitate the explanations, any graph of maximum degree d and diameter k will be called a (d,k)-*graph*. Because for $d \geq 3$ and $k \geq 2$ there are only a few (d,k)-graphs of order equal to the value $M_{d,k}$ of the Moore bound, researchers have tried to construct (d,k)-graphs of order as close to $M_{d,k}$ as possible. For a (d,k)-graph of order $M_{d,k} - \delta$ the quantity δ is knwn as the *defect*, and then we speak about a $(d,k,-\delta)$-graph; we note that this terminology is only used for 'small' defects.

There are a number of results concerning graphs with small defect. For example, Erdös, Fajtlowitcz and Hoffman proved [3] that there is no graph of degree d and diameter 2 with $\delta = 1$ apart from the cycle of length 4. In the case of $\delta = 2$ and $d = 2$ all the $(d,k,-2)$-graphs are the cycles of length $2k-1$. For $\delta - 2$ and $d \geq 3$ only five graphs are known at present, namely, two $(3,2,-2)$-graphs of order 8, one $(4,2,-2)$-graph of order 15, one $(5,2,-2)$-graph of order 24, and one $(3,3,-2)$-graph of order 20; for details we refer to [8].

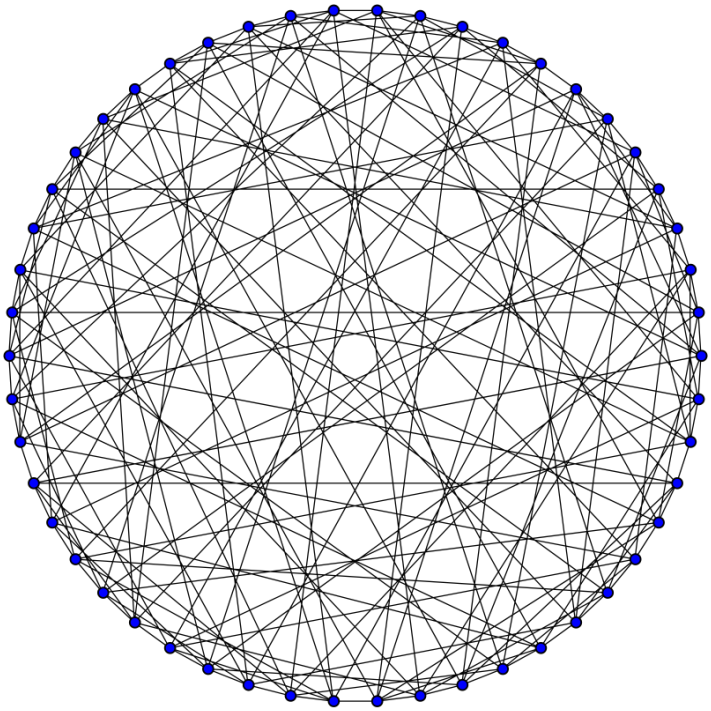

Figure 1: Hoffman-singleton graph is Moore graph with $d = 7$ and $k = 2$

2.4 Constructions of large graphs

A different approach to finding (d, k)-graphs of order close to the Moore bound is by constructing appropriate 'large' (d, k)-graphs. In most cases the constructions use combinatorics on words or algebraic structures such as groups and fields, so that the resulting graphs turn out to be rich in symmetries, or even vertex-transitive (and sometimes even Cayley).

For a long time one of the asymptotically best families was the one of the *undirected de Brujin graphs*, which are (d, k) graphs for even d and yield the lower bound

$$n_{d,k} \geq \left(\frac{d}{2}\right)^k.$$

This bound was improved by Baskoro and Miller [1] to

$$n_{d,k} \geq \left(\frac{d}{2}\right)^k + \left(\frac{d}{2}\right)^{k-1} \tag{2}$$

In the special case of diameter $k = 2$, modified Brown graphs can give for sufficiently large d the bound

$$n_{d,2} \geq d^2 - 2d^{1+\varepsilon}$$

where the number $\varepsilon < 1$ depends on results about gaps between consecutive prime numbers; see [2] for details about the current development.

2.5 Graph lifting

Graph lifting is a technique by which one may produce 'large' graphs with certain required properties from suitable 'small' graphs. The technique is well-known in topological and algebraic graph theory and for historical and mathematical details we refer to the monograph [5]. The technique can be described in the language of the so-called voltage assignments, which we briefly present next.

Let G be a graph. Although our graphs are undirected, we will preassign a direction to every edge. An edge with a preassigned direction is an *arc*. If e is an arc of G, by the symbol e^{-1} we denote the *reverse* of e, obtained simply by changing the preassigned direction on the edge. Let $D(G)$ be the set of all arcs of G; it follows that the size of $D(G)$ is twice the number of edges of G.

Let G be a graph as above and let Γ be a finite group. The mapping

$$\alpha : D(G) \to \Gamma$$

will be called a *voltage assignment* if $\alpha(e^{-1}) = (\alpha(e))^{-1}$, for any arc $e \in D(G)$.

Out of the graph G and the voltage assignment α as introduced above one can construct a 'larger' graph, called the *lift* of G (under the assignment α) and denoted G^α. The vertex set and the dart set of the new graph are defined as follows:

$$V(G^\alpha) = V(G) \times \Gamma$$
$$E(G^\alpha) = E(G) \times \Gamma$$

with the condition that if an arc e emanates from a vertex u and terminates in a vertex v in the *base graph* G, then for every $g \in \Gamma$ there is a dart (e, g) emanating from the vertex (u, g) and terminating in the vertex $(v, g\alpha(e))$. It follows that right multiplication by $\alpha(e)$ permutes the terminal vertices of arcs (e, g) emanating from the vertices (u, g). At the same time this right multiplication induces a group of automorphisms of the lift acting freely on vertices and isomorphic to the *voltage group* Γ. Note that G^α can be considered to be an undirected graph, because the arcs (e, g) and $(e^{-1}, g\alpha(e))$ are reverse of each other.

This procedure can be reversed in the following sense, cf. [5]. Let $\tilde{G}$ be a graph and let Γ be a group of automorphisms of $\tilde{G}$ that acts freely on vertices of $\tilde{G}$. Then $\tilde{G}$ is a lift of a 'smaller' graph, denoted $\tilde{G}/\Gamma$ and called a *quotient*, which is obtained from $\tilde{G}$ by letting Γ-orbits of the vertex set and the arc set of $\tilde{G}$ to be vertices and arcs of the quotient, with incidence inherited from $\tilde{G}$.

Of course, degrees of all the vertices (u, g) in the lift are equal to the degree of u in the base graph. An advantage of lifting is that the diameter of the lift can be conveniently controlled by properties of the base graph G and the voltage assignment α as well. A *walk* of length ℓ in G is any sequence $W = e_1 e_2 \dots e_\ell$ of consecutive arcs of G, and the voltage $\alpha(W)$ of the walk is simply the product $\alpha(W) = \alpha(e_1)\alpha(e_2)\cdots\alpha(e_\ell)$. Then (cf. e.g. the survey [8]), the lift G^α has diameter at most k if for any two vertices u, v of G and for any element $g \in \Gamma$ there is a walk W of length at most k emanating from u and terminating at v such that $\alpha(W) = g$; in the case when $u = v$ we also require that $g \neq 1$.

A number of the largest currently known d, k-graphs can be described as lifts. For example, all the graphs giving the values of $n_{3,7}$, $n_{3,8}$, $n_{4,4}$, $n_{5,3}$, $n_{5,5}$, $n_{6,3}$, $n_{6,4}$, $n_{7,3}$, $n_{14,3}$ and $n_{16,2}$ obtained by computer search turn out to be lifts [8].

2.6 Cayley graphs

Let Γ be a group and let $S \subset \Gamma$ be a symmetric unit-free generating set for Γ; that is, we require that $S = S^{-1}$ and $1 \notin S$. The *Cayley graph* $C(\Gamma, S)$ is the graph with vertex set Γ in which vertices a, b are adjacent if $a^{-1}b \in S$. Observe that now the group Γ acts regularly and hence freely on the vertex set of $C(\Gamma, S)$ as a group of automorphisms, so that the quotient graph $C(\Gamma, S)/\Gamma$ has just one vertex. By the remark in the previous section about groups of automorphisms acting freely in vertices it follows that Cayley graphs are simply lifts of one-vertex graphs (which will in general contain multiple loops and semi-edges but we will not go into the corresponding details).

The diameter testing of lifts now easily translates into testing diameter of Cayley graphs as follows: A Cayley graph $C(\Gamma, S)$ has diameter at most k if and only if every element of Γ can be expressed as a product of at most k elements of the generating set S. Equivalently, the diameter of a Cayley graph $C(\Gamma, S)$ is *equal* to k if and only if k is the smallest number such that every element of Γ can be expressed as a product of at most k elements of S.

By $Cay_{d,k}$ we denote the largest order of a Cayley (d, k)-graph. In [7] it was proved that for every fixed $d \geq 3$ and $c \geq 2$ there is a set A of natural numbers with positive density s.t. $C_{d,k} \leq M_{d,k} - c$ for all $k \in A$.

The currently best available lower bound on $C_{d,2}$ was obtained by Šiagiová and Širáň [9] and reads as follows. Let $D = \{2^{2m+\mu} + (2+\delta)2^{m+1} - 6, m \geq 1, \mu \in \{0, 1\}\}$. Then, for every $d \in D$ one has $C_{d,2} > d^2 - 6\sqrt{2}d^{3/2}$.

In the special case of Cayley graphs of diameter $k = 2$ on Abelian groups there is a relatively straightforward lower bound of the form

$$n_{d,2} \geq \lfloor \frac{d+2}{2} \rfloor \lceil \frac{d+2}{2} \rceil$$

obtained by considering the product of cyclic groups $Z_{\lfloor (d+2)/2 \rfloor} \times Z_{\lceil (d+2)/2 \rceil}$, with generating set consisting of all pairs (x_1, x_2) with one of the entries equal to zero.

2.7 General linear and special linear groups

Linear groups are usually described in terms of linear transformations of vector spaces over general fields. For our purposes it will be sufficient to work with a more concrete description and restricted to finite fields. Let q be a power of a prime and let $GF(q)$ be the Galois field of order q. The *general linear group* $GL(m, q)$ consists of all non-singular $m \times m$ matrices over $GF(q)$ under multiplication of matrices in the usual sense. By an elementary fact in group theory the order of $GL(m, q)$ is equal to $(q^m - 1)(q^m - q) \cdots (q^m - q^{n-1})$. The *special linear group* $SL(m, q)$ is the subgroup of $GL(m, q)$ consisting of matrices with determinant equal to 1; its order is $|SL(m, q)| = |GL(m, q)|/(q - 1)$.

We will be particularly interested in the case $m = 2$ and $q = p$ for some prime numbers p, and in Cayley graphs of diameter 2 arising from the groups $SL(2, p)$. To the best of our knowledge such a study has not appeared in the available literature.

3 Results

3.1 Example of Cayley graph

For example we generate Cayley graph on group $SL(2,3)$ with order $|SL(2,3)| = 24$ consiting of

$$SL(2,3) = \left\{ \begin{bmatrix}1&0\\0&1\end{bmatrix}, \begin{bmatrix}0&1\\2&0\end{bmatrix}, \begin{bmatrix}0&1\\2&1\end{bmatrix}, \begin{bmatrix}0&1\\2&2\end{bmatrix}, \begin{bmatrix}0&2\\1&0\end{bmatrix}, \begin{bmatrix}0&2\\1&1\end{bmatrix}, \begin{bmatrix}0&2\\1&2\end{bmatrix}, \begin{bmatrix}1&0\\1&1\end{bmatrix}, \begin{bmatrix}1&0\\2&1\end{bmatrix}, \begin{bmatrix}1&1\\0&1\end{bmatrix}, \begin{bmatrix}1&1\\1&2\end{bmatrix}, \begin{bmatrix}1&1\\2&0\end{bmatrix}, \begin{bmatrix}1&2\\0&1\end{bmatrix}, \begin{bmatrix}1&2\\1&0\end{bmatrix}, \begin{bmatrix}1&2\\2&2\end{bmatrix}, \begin{bmatrix}2&0\\0&2\end{bmatrix}, \begin{bmatrix}2&0\\1&2\end{bmatrix}, \begin{bmatrix}2&0\\2&2\end{bmatrix}, \begin{bmatrix}2&1\\0&2\end{bmatrix}, \begin{bmatrix}2&1\\1&1\end{bmatrix}, \begin{bmatrix}2&1\\2&0\end{bmatrix}, \begin{bmatrix}2&2\\0&2\end{bmatrix}, \begin{bmatrix}2&2\\1&0\end{bmatrix}, \begin{bmatrix}2&2\\2&1\end{bmatrix} \right\}.$$

For generating set S with three pairs of elements and its inverses

$$S = \left\{ \begin{bmatrix}1&1\\1&2\end{bmatrix}, \begin{bmatrix}2&2\\2&1\end{bmatrix}, \begin{bmatrix}2&2\\0&2\end{bmatrix}, \begin{bmatrix}2&1\\0&2\end{bmatrix}, \begin{bmatrix}0&2\\1&1\end{bmatrix}, \begin{bmatrix}1&1\\2&0\end{bmatrix} \right\}$$

Cayley graph $C(SL(2,3), S)$ has order 24, $d = 6$ and $k = 2$.

```
sub generate_cayley_graph
{
  my ($generating_set_ref, $zp) = @_;
  my @multiplication_results;
  my %generating_nodes;

  my @generating_set = @{ $generating_set_ref };
  my @keys;
  my @stack;

  foreach my $gs_element ( @generating_set ) {
    insert_hash(\%generating_nodes, $gs_element, $zp);
    push @keys, compute_hash($gs_element, $zp);
    push @stack, $gs_element;
  }

  my $current_node = $stack[0];

  while(@stack) {
    foreach my $generating_element (@generating_set) {
      my $multiplication_result = ($current_node x $generating_element) % $zp;
      insert_result(\@multiplication_results, $current_node, $multiplication_result, $zp);

      if(find_hash(\%generating_nodes, $multiplication_result, $zp)) {
        insert_hash(\%generating_nodes, $multiplication_result, $zp);
        push @keys, compute_hash($multiplication_result, $zp);
        push @stack, $multiplication_result;
      }
    }

    shift @stack;

    if(@stack) {
      $current_node = $stack[0];
    }
  }

  return ( \@keys, \@multiplication_results, $generating_set_ref, $zp);
}
```

Algorithm 1 Cayley graph generation

Require: $generation\_set[], n$

```
stack[] ← generation_set[]
stack_element ← stack[0]
while stack[] not empty do
    for all generating_element ← generation_set[] do
        multiplication_result ← (stack_element * generating_element) mod n
        multiplication_results[stack_element] append multiplication_result
        stack[] append multiplication_result
    end for
    shift to the left stack[]
    stack_element ← stack[0]
end while
return multiplication_results
```

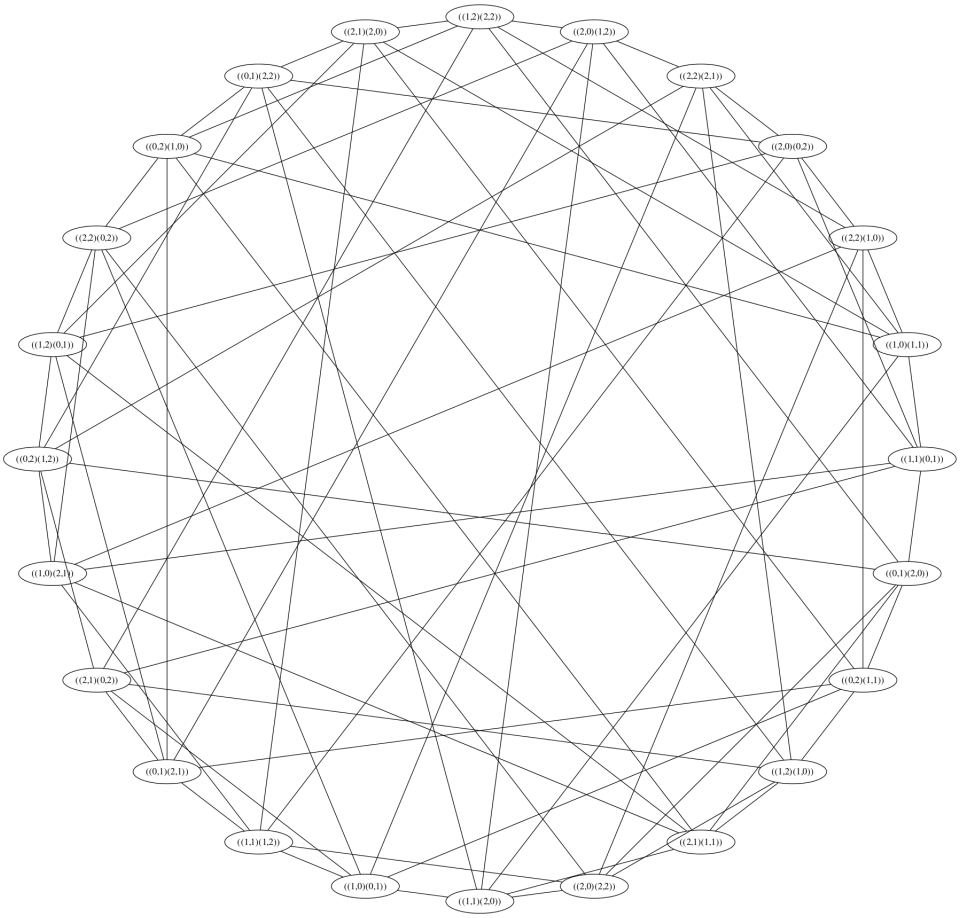

Figure 2: Output of circos [10] of $C(SL(2,3),S)$

Bibliography

[1] E. T. Baskoro and M. Miller, On the construction of networks with minimum diameter, Australian Computer Science Communications C 15 (1993) 739Ű743.

[2] D. Bevan, G. Erskine and R. Lewis, Large circulant graphs of fized diameter and arbitrary degree, Ars Math. ontemp. 13 (2017), 275–29.

[3] P. Erdős, S. Fajtlowicz and A.J. Hoffman, Maximum degree in graphs of diameter 2, Networks 10 (1980), 87–90.

[4] G. Exoo and R. Jajcay, Dynamic cage survey, Electr. J. Combin. 15 (2008), Dynamic Survey DS16.

[5] J. L. Gross and T. W. Tucker, Topological Graph Theory. Wiley, 1987 and Dover, 2001.

[6] A. J. Hoffman and R. R. Singleton, On Moore graphs with diameter 2 and 3, IBM J. Res. Develop. 4 (1960), 497–504.

[7] R. Jajcay, M. Mačaj and J. Širáň,

[8] M. Miller and J. Širáň, Moore graphs and beyond: A survey, 2nd Ed., Electr. J. Combin. 2013, Dynamic Survey DS15.

[9] J. Šiagiová and J. Širáň, Approaching the Moore bound for diameter two by Cayley graphs, J. Combin. Theory Ser. B 102 (2012) 470–473.

[10] Circo, http://circos.ca