УДК 512.54

M. Olshevskyi

DOI: https://doi.org/10.18523/2617-7080420217-19

DIAMETER SEARCH ALGORITHMS FOR DIRECTED CAYLEY GRAPHS

It is considered a well known diameter search problem for finite groups. It can be formulated as follows: find the maximum possible diameter of the group over its system of generators. The diameter of a group over a specific system of generators is the diameter of the corresponding Cayley graph. In the paper a closely related problem is considered. For a specific system of generators find the diameter of corresponding Cayley graph. It is shown that the last problem is polynomially reduced to the problem of searching the minimal decomposition of elements over a system of generators.

It is proposed five algorithms to solve the diameter search problem: simple down search algorithm, fast down search algorithm, middle down search algorithms, homogeneous down search algorithm and homogeneous middle down search algorithm.

The first two algorithms are universal. They can be applied to any finite group and its systems of generators. Moreover, the fast down search algorithm is an optimized version of the simple down search algorithm.

A property of strict growing fora system of generators is introduced. In this case the search process can be optimized by focusing only on those group elements, for which minimum decompositions potentially have the maximum possible length. Based on this property middle down search algorithm is introduced.

The main part of the paper is homogeneous theory. It is considered a series of groups with its systems of generators and some additional properties of them. It is defined a homogeneous property of these series. A binary equivalence relation relies on it. The main purpose of defining such a relation is preserving decompositions of elements from the same equivalence class. It is enough to find the minimum decomposition of only one representative of the equivalence class.

It is introduced homogeneous down search and homogeneous middle down search algorithms. These algorithms can be applied to groups that belong to homogeneous series of groups with systems of generators.

For every algorithm its correctness is shown. The complexity estimations for algorithms is discussed.

Keywords: Cayley graph, diameter of group, system of generators.

Introduction

The diameter search problem in group theory can be formulated as follows: for a finite group G find the maximum of its diameters $D(G)$ over all systems of generators of G. A few general results in this area are known. The most general conjecture was proposed by L. Babai and A. Seress in [1, Conjecture 1.7]:

Conjecture 1. *If G is a non-abelian finite simple group of order N, then $D(G) < (\log N)^C$ for the absolute constant C.*

The first family of finite simple groups, for which this conjecture was proved by H. Helfgott in [2], is $PSL_2(\mathbb{Z}/p\mathbb{Z})$, where p is a prime. For groups of Lie type an upper bound of the diameter was found by E. Breuillard, B. Green, and T. Tao in [3] and by L. Pyber and E. Szabó in [4]. For permutation groups upper bounds of diameters were presented by H. Helfgott and A. Seress in [5].

We can also consider in this domain another widely known problem, the minimum-length generators sequence search problem. Specifically, for a given finite group G, its system of generators S and a target element $g \in G$ find a shortest generator sequence realizing g. In particular, for permutation groups such a problem is NP-hard [6].

As a partial case of the diameter search problem one can deal with the diameter search for a finite group over a fixed system of generators. For example the diameter of $Sym(n)$ over $S = \{(1,k) | k \in \in 2, \dots, n\}$ was found in [7].

In this paper we consider the diameter search problem for directed Cayley graphs. We introduce different algorithms and discuss their properties.

The paper is organized as follows:

1. Section Introduction contains basic notations and decomposition problem description. The relation between decomposition problem and diameter search problem is demonstrated.
2. Section Simple down search algorithm introduces universal diameter search algorithm and

proves its correctness.
3. Section Fast down search algorithm introduces infinite decomposition trees and optimized version of simple down search algorithm. It is proved correctness of the algorithm.
4. Section Middle down search algorithm introduces strict growing property of a system of generators and diameter search algorithm, based on it. It is proved correctness of this algorithm.
5. Section Homogeneous theory introduces groups-generators series, properties of them and homogeneous equivalence between elements of groups.
6. Section Homogeneous down search algorithm introduces algorithm, which requires homogeneous property of groups-generators series. It is proved its correctness.
7. Section Homogeneous middle down search algorithm introduces diameter search algorithm, which requires both homogeneous property of groups-generators series and strict growing of system of generators. It is proved correctness of the algorithm.

Preliminaries

Unless otherwise specified in the paper we denote by G a finite group and by S a system of generators of G.

Basic notation. The following notations will be used:
1. $k \, mod \, m$ — the remainder of division of integer k by integer $m \neq 0$.
2. $\overline{n_1, n_2}$ — the set of natural numbers $\{n_1, \ldots, n_2\}$, where $n_1 \leq n_2$.
3. $f \circ g := g(f)$ — the right composition of mappings f, g.

We define an *index tuple* I as a tuple of pairwise different natural numbers, i.e. for some $n \geq 0$ we have

$$I = (i_1, i_2, \ldots, i_n), \quad i_j \neq i_k, j \neq k.$$

In other words, every index tuple is a linearly ordered finite set of natural numbers. We call n the cardinality of the index tuple I. Sometimes we abuse terminology and refer to index tuples as to sets with no ordering.

Let I, J be disjoint index tuples (i.e. they have no common elements) with cardinalities n_1, n_2 respectively. Then we define the concatataion of them as

$$I \sqcup J = (i_1, \ldots, i_{n_1}, j_1, \ldots, j_{n_2}).$$

Let I, J be index tuple with cardinalities n_1, n_2 respectively. Then their difference is defined as

$I \backslash J$ — the tuple of numbers from the set $I \backslash J$, ordered as in I.

Note that $I \backslash J$ can be empty.

Diameter search problem.

Definition 1. The (right) *Cayley graph* of G over S is a colored directed graph $Cay(G, S)$ constructed as follows:
1. the set of vertices is G;
2. the set of colors is S;
3. for any $g \in G$ and $s \in S$, the vertices g and $g \cdot s$ are connected by a directed edge of color s.

Since S generates G the Cayley graph of G over S is a strongly connected graph.

Remind that the *distance between two vertices* in a directed strongly connected graph is the length of the shortest oriented path which connects them. The *diameter of the graph* is the maximum of distances between its vertices.

Definition 2. The *diameter of the group* G with respect to the system of generators S is the diameter of the corresponding Cayley graph $Cay(G, S)$ of the group G over S:

$$D_S(G) = D(Cay(G, S)).$$

Definition 3. The *diameter of the group* G is defined as the maximum of diameters of G over its systems of generators:

$$D(G) = \max_{\langle S \rangle = G} D_S(G).$$

Decomposition problem. Every element g of G can be decomposed into a product

$$g = \prod_{k=1}^{l} s_{i_k}$$

of generators from S for some natural l. Corresponding tuple of generators $(s_{i_1}, \ldots, s_{i_k})$ will be called a *decomposition of the element g over S.* The *length* $|g|_S$ *of the element* g over S is the length of the shortest decomposition of g over S.

Let us formulate the following computational problem.

Decomposition problem: for a given group G and its system of generators S find the maximum of lengths of its elements over S.

Let g_1, g_2 be vertices from $Cay(G, S)$. Denote by $d(g_1, g_2)$ the distance between g_1 and g_2 over S.

Theorem 1. *The diameter search problem is polynomial-time reducible to the decomposition problem.*

Proof. Let l be the diameter of the group G with respect to the system of generators S. It means that there exist vertices g_1, g_2 from $Cay(G, S)$ such that $d(g_1, g_2) = l$. It immediately implies $d(g_1, g_2) = d(e, h)$, where $h = g_2 \cdot g_1^{-1}$. Hence, the labels of the shortest path between e and $g_2 \cdot {g_1}^{-1}$ form a decomposition of h over S. The statement immediately follows.

An element $a \in G$ will be called *diameter element* of group G over S if its length over S equals to diameter of group G over S:

$$|a|_S = D_S(G).$$

Simple down search algorithm

Consider an algorithm of finding diameters that are based on breadth-first search algorithm [8] for graphs.

Algorithm 1: Simple down search algorithm

```
Input: $G$ — a group, $S$ — its system of
       generators
Result: Diameter $D_S(G)$
Initialization: $found = \{e\}$,
  $all = \{g | g \in G\}$, $current\_level = \{e\}$,
  $level = 0$;
while $found \neq all$ do
    $current\_level = current\_level \cdot S$;
    $found = found \bigcup current\_level$;
    $level = level + 1$;
end
Output: $level$
```

Theorem 2. *Simple down search algorithm is correct.*

Proof. We need to show that:

1. the algorithm has no "dead" loops;
2. the output of the algorithm is the diameter $D_S(G)$.

These two parts will be proved separately.

Part 1. Let a be arbitrary element of the group G. Since S generates G there exists a decomposition of a over S:

$$a = \prod_{k=1}^{l} s_{i_k}.$$

Therefore, the element a will belong to $found$ at the moment when $level = l$.

Since the group G is finite there exists n such that at the moment $level = n$ we obtain $found = = all$.

Part 2. Let us denote $D_S(G)$ by d. Suppose that $d \neq level$, where $level$ is the output of simple down search algorithm for group G over S. Consider two cases.

1. Assume that $d < level$. Then, for every element a of the group G there exists its decomposition over S with length $l \leq d$. The set $found$ is redefined in the algorithm on each loop. Hence, at the moment $level = d$ we have:

$$all = found = \{e\} \bigcup \Big(\bigcup_{l=1}^{d} \underbrace{S \dots S}_{l \text{ times}} \Big),$$

which means that $level \leq d$. A contradiction.

2. Assume that $d > level$. Then there exists an element a of the group G with length d over S. By the definition of *length over system of generators* there are no sets of indices $\{i_1, i_2, \cdots, i_l\}$, $l < d$ such that:

$$a = \prod_{k=1}^{l} s_{i_k}.$$

Therefore, the set $found$ does not contain the element a when the algorithm stops. This leads to a contradiction with the requirement that $found$ equals to all.

The proof is complete.

Proposition 3. *Let G be a finite group generated by S, $|S| = n$ and $D_S(G) = m$. Then the total number of multiplications in simple down search algorithms is bounded from above by $\frac{n \cdot (n^m - 1)}{n-1}$.*

Proof. At the moment $level = k + 1$ the algorithm needs to multiply every element of the previous level by every generator. Then we obtain the following number of multiplications: $|current\_level| \cdot |S| = |S|^k \cdot |S| = n^{k+1}$. As the result, the total number of multiplications will be

$$\sum_{k=1}^{m} n^{k+1} = \frac{n \cdot (n^m - 1)}{n - 1}.$$

The proof is complete.

Fast down search algorithm

We need to define additional structures in order to describe another algorithms, in particular fast down search algorithm. After that we will prove a few statements to connect simple down search algorithm and fast down search algorithm.

Infinite decomposition tree. Let G be a finite group, $S = \{s_1, s_2, \cdots, s_m\}$ be its system of generators. Consider infinite rooted m-ary tree $T(V, E)$. We introduce enumeration of vertices on each level of this tree. The vertices of the lth level will be enumerated by numbers from 1 to m^l, $l \geq 0$. We obtain that

1. the root is the first vertex of level 0.
2. the kth child of the tth vertex of level l will have index $((t-1) \cdot m + k)$ on level $(l + 1)$.

We also label vertices and edges of the tree $T(V, E)$ starting from level 0 as follows:

1. the root will be labeled by e.
2. the edge, which connects the kth vertex of level l with $([k/m] + 1)$th vertex of level $(l - 1)$, will be labeled by $k \, mod \, m$, $k \in 1, \dots, m^l$.
3. the kth vertex of level l will be labeled by the result of product: $b \cdot s_{k \, mod \, m}$, where b is the label of $([k/m] + 1)$th vertex of level $(l - 1)$, $k \in 1, \dots, m^l$.

We call such a tree the *infinite decomposition tree* of the group G over the system of generators S. A path in this tree will be identified with the sequence of labels on edges along this path.

Let T be the infinite decomposition tree of the group G over S.

Lemma 4. *An element a from G has decomposition $\prod\limits_{k=1}^{l} s_{i_k}$ if and only if the path $i_1, i_2, \cdots i_l$ connects the root vertex with the vertex labeled by a in T.*

Proof. Induction on the decomposition length l.

The basis: case $l = 1$.

Necessity. Let $a = s_{i_k}$ for $k \in 1, \ldots, m$. The equality $e \cdot s_{i_k} = a$ implies that the kth vertex on level 1 will have the label a.

Sufficiency. Let the kth vertex of the first level be labeled by a. Then, from the definition of the infinite decomposition tree we have $a = e \cdot s_{i_k}$. Then $a = s_k$. Hence, a has a decomposition of length 1, i.e. s_{i_k}.

Induction step: case $l+1$ under assumption that for l the statement holds.

Necessity. Let $a = \prod\limits_{k=1}^{l+1} s_{i_k}$. Under inductive assumption for the element $b = \prod\limits_{k=1}^{l} s_{i_k}$ we have: the path $i_1, i_2, \ldots, i_l$ connects the root with the vertex w labeled by b. The equality $a = b \cdot s_{i_{l+1}}$ implies that the (i_{l+1})th child v of the vertex w is labeled by a. Hence, $i_1, i_2, \ldots, i_{l+1}$ is a path from the root to w.

Sufficiency. Let $i_1, i_2, \ldots, i_{l+1}$ be a path, which connects the root with the vertex v labeled by a. The definition of the infinite decomposition tree implies the equality

$$a = b \cdot s_{i_{l+1}},$$

where b is a label of the vertex w, the parent of the vertex v.

From the inductive assumption we have that the product $\prod\limits_{k=1}^{l} s_{i_k}$ equals to the element b. Therefore, the product

$$(\prod_{k=1}^{l} s_{i_k}) \cdot s_{i_{l+1}} = \prod_{k=1}^{l+1} s_{i_k}$$

equals to the element a.

Proposition 5. *Let G be a group, S be its system of generators, l be a natural number.*

1. The diameter of the group G over the system of generators S equals to l if and only if l is the smallest level number in T such that every element of G appears at least once as a label of a vertex starting from level 0 up to level l.

2. In simple down search algorithm an element $a \in \in G$ appears at the moment $level = l$ if and only if there exists a path $i_1, i_2, \ldots, i_l$ which connects the root with the vertex v labeled by a in T.

Proof. 1. The diameter of the group G over S equals to l if and only if for every element a of G there exists a decomposition over S with length $\leq \leq l$. The last statement holds if and only if there exists a path with length $\leq l$ which connects the root with a vertex labeled by a. Therefore, for every element a of G there exists at least one vertex labeled by a on levels from 0 to l.

2. The element a appears in the simple down search algorithm at the moment $level = l$ if and only if there exists a sequence of generators $s_{i_1}, s_{i_2}, \ldots, s_{i_l} \in S$ such that $a = \prod\limits_{k=1}^{l} s_{i_k}$. From Lemma 4 it follows that the last statement holds if and only if the path $i_1, i_2, \ldots, i_l$ connects the root with vertex labeled by a.

The proof is complete.

Let v be a vertex of the tree T on level t. Recall that the *sub-tree $T|_v$ of T rooted at the vertex v* is the tree constructed from T as follows:

1. the root of new tree $T|_v$ is v.

2. the lth level of tree $T|_v$ consists of vertices from $(t+l)$th level of T which are directly connected to $(l-1)$th level of $T|_v$, $l \geq 1$. Labels of edges and vertices are preserved.

Denote by g_v the label of a vertex v in T.

Lemma 6. *Let v, w be vertices of T such that the labels of v and w are equal. Then the rooted trees T_v and T_w are isomorphic as labelled graphs.*

Proof. Note, that $T|_v$ and $T|_w$ are isomorphic as rooted m-ary trees. The natural isomorphism τ preserving enumeration of vertices on levels is defined as follows:

1. the kth vertex of the lth level of $T|_v$ is mapped to the kth vertex of the lth level of $T|_w$, $k \in \overline{1, C^l}$ $l \geq 0$;

2. an edge, which connects two vertices of the tree $T|_v$, is mapped to the edge, which connects images of corresponding vertices.

It is enough to show that isomorphism τ preserves labels of vertices.

Let a and b be labels of jth vertices on level l of corresponding trees $T|_v$ and T_w. Suppose that $a \neq b$. Then

$$g_v \cdot \prod_{k=1}^{l} s_{i_k} \neq g_w \cdot \prod_{k=1}^{l} s_{i_k}.$$

Hence, $g_v \neq g_w$. This leads to a contradiction with the equality of labels of v and w.

The proof is complete.

Denote by $Path_T(v, w)$ the shortest path from vertex v to vertex w in T.

Lemma 7. *Let an element $a \in G$ decomposes as $a = \prod_{k=1}^{l} s_{i_k}$ in S. If there exists $t \in \overline{1,l}$ such that the element $\prod_{k=1}^{t} s_{i_k}$ appears as a label of a vertex of T on level less then t then $|a|_S < l$.*

Proof. Denote by b the product $\prod_{k=1}^{t} s_{i_k}$. Then the vertex $v \in V$, which is defined by the path $i_1, i_2, \ldots, i_t$ starting from the root, will have label b. Note, that the element a decomposes as a product $\prod_{k=1}^{l} s_{i_k}$ if and only if the path $i_1, i_2, \cdots i_l$ connects the root of T_v with the vertex labeled by $g_v \cdot a$.

The assumption of the lemma implies that there exists a vertex $w \in V$ such that w is upper than v in T and w is also labeled by b. Since labelled trees $T|_v$ and $T|_w$ are isomorphic the vertices, which are defined by the path $i_{t+1}, \ldots, i_l$ from the root in trees $T|_v$ and T_w, have the same label a. From Lemma 4 it follows that

$$a = \prod_{k=1}^{l} s_{i_k} = \prod_{k \in Path_T(e,v)} s_k \cdot \prod_{k=t+1}^{l} s_{i_k} =$$

$$\prod_{k \in Path_T(e,w)} s_k \cdot \prod_{k=t+1}^{l} s_{i_k}.$$

Since w is upper than v, the length of the path $Path_T(e, w)$ is less than t. This leads to the inequality $|a|_S < l$.

The proof is complete.

Fast down search algorithm. In order to optimise the simple down search algorithm we use the results of the previous section. The main goal is to reduce the number of multiplications.

Algorithm 2: Fast down search algorithm

```
Input: $G$ — a group, $S$ — its system of
       generators
Result: Diameter $D_S(G)$
Initialization: $found = \{e\}$,
  $all = \{g | g \in G\}$, $current\_level = \{e\}$,
  $level = 0$;
while $found \neq all$ do
    $current\_level =$
      $= (current\_level \cdot S) \setminus found$;

    $found = found \bigcup current\_level$;
    $level = level + 1$;
end
Output: $level$
```

Theorem 8. *Fast down search algorithm is correct.*

Proof. We need to show that:

1. the algorithm has no dead loops;
2. the output of the algorithm is the diameter $D_S(G)$.

These two parts will be proved separately.

Part 1. There are no dead loops if and only if there exists a natural number n such that the algorithm will find all elements of group G (set $found$) at the moment $level = n$.

Suppose that there exists an element $a \in G$ which never appears in the set $found$. Consider a decomposition $\prod_{k=1}^{l} s_{i_k}$ of a over S. Since a is not contained in $found$, there exists $t \in \overline{1,l}$ such that the element $b = \prod_{k=1}^{t} s_{i_k}$ appeared on an earlier iteration of the algorithm. This means that there exists a shorter decomposition of b over S. From Lemma 4 it follows that the element b is a label of a vertex on the level which is upper then level t. Lemma 7 implies the inequality $|a|_S < k$. Hence, for every decomposition of a a shorter decomposition can be found. This immediately leads to a contradiction for the set of all lengths of decompositions of a over S is bounded from below.

Part 2. Let d_1 be the output of the simple down search algorithm with input G and S and let d_2 be the output of the fast down search algorithm. Note that directly from these definitions we have the inequality

$$d_1 \leq d_2.$$

Suppose, that $d_1 < d_2$. Then there exists an element of the group G such that it firstly appeared strongly after the d_1th step of the fast down search algorithm. Otherwise, first down search algorithm stops at the moment d_1.

Let the element $a \in G$ be such that:

1. a firstly appeared at the moment $level = d_2$ in the fast down search algorithm;
2. a firstly appeared at the moment $level = d_2 - r$ in the simple down search algorithm.

The second condition leads to the equality $|a|_S = = d_2 - r$. Proposition 5 implies that there exists a path $i_1, i_2, \ldots, i_{d_2 - r}$, which connects the root with the vertex labeled by a. Based on the fast diameter search algorithm, there exists a natural number t, $t \leq d_2 - r$, such that the element $b = \prod_{k=1}^{t} s_{i_k}$ appears earlier then $level = (d_2 - r)$. Lemma 7 implies that $|a|_S < d_2 - r$. A contradiction.

The proof is complete.

The main optimization of the fast down search algorithm compared to the simple down search algorithm is to skip previously founded elements of a group. The number of repetitions of elements depends on a group and its system of generators. Therefore, in general the number of multiplication, which are required for the fast down search algorithm, can be estimated only as in Proposition 3 by $\frac{n\cdot(n^m-1)}{n-1}$. However, in some cases this number can be reduced significantly.

Middle down search algorithm

In this section we present an algorithm that requires additional properties of generators.

Strictly growing system of generators.

An element $a \in G$ will be called *properly generated* over S if element for arbitrary $A \subset S, A \neq S$ we have $a \notin \langle A \rangle$.

This definition immediately leads to the following statements.

Lemma 9. *Every decomposition of a properly generated element contains every generator of S.*

Proof. Since every element belongs to the subgroup generated by the elements that appeared in its decomposition the statement follows.

Lemma 10. *The minimum possible length of a properly generated element over S is $|S|$.*

Proof. Immediately follows from Lemma 9.

A system of generators S of a group G will be called *strictly growing* if every diameter element a from G is properly generated.

Lemma 11. *Let G be a finite group, S be its strictly growing system of generators. Then the diameter of the group G over S is greater or equal to $|S|$.*

Proof. By Lemma 10 every diameter element has length over S greater or equal to $|S|$. This means that the diameter of G over S is not less than $|S|$.

The proof is complete.

Middle down search algorithm. Let G be a finite group, S be its strictly growing system of generators.

We introduce the following notions:

1. G_f — the set of all properly generated elements of the group G;

2. $D_f(S, m)$ — the set of all decompositions over S with length m such that every generator of S appears at least once in every decomposition, $m \geq$ $\geq |S|$;

3. P — the function on the set of decompositions, which converts a decomposition to the corresponding element.

Let a be an element of G with a decomposition in $D_f(S, m)$. Note, that in general it does not imply that a is properly generated.

Algorithm 3: Middle down search algorithm

```
Input: $G$ — a group, $S$ — its strictly
       growing system of generators
Result: Diameter $D_S(G)$
Initialization: $found = \emptyset$, $all = G_f$,
$level = |S| - 1$;
while $found \neq all$ do
    $level = level + 1$;
    for $decomp \in D_f(S, level)$ do
        $product = P(decomp)$;
        if $product \in G_f$ then
            $found = found \bigcup \{product\}$;
        end
    end
end
Output: $level$
```

Theorem 12. *Middle down search algorithm is correct.*

Proof. Since the system of generators S is strictly growing every diameter element is properly generated. Then the set of all diameter elements is a subset of G_f. This means that the diameter can be found as the lengths over S of elements from G_f are found. More precisely, the diameter is the maximum of these lengths:

$$D_S(G) = \max_{el \in G_f} |el|_S.$$

Hence, the main loop of the algorithm terminates after finite number of steps, i.e. after $D_S(G) - |S| +$ $+ 1$ steps.

Lemma 9 implies that for every properly generated element a minimum decomposition belongs to $D_f(S, level)$ for some natural number $level$. From Lemma 10 it follows that $level$ is not less than $|S|$. This explains why the main loop starts from $level = |S|$.

The proof is complete.

Proposition 13. *Let G be a finite group generated by a strictly growing system of generators S, $|S| = n$ and $D_S(G) = m$ for some $n, m \in \mathbb{N}$. Then the number of multiplications required by the middle down search algorithm is bounded from above by*

$$\sum_{t=n}^{m}(t-1)\cdot\sum_{k=0}^{n-1}(-1)^k\cdot\binom{n}{k}\cdot(n-k)^t.$$

Proof. Since the system of generators S is strictly growing the inequality $m \geq n$ holds. Hence, we need to obtain a product of every sequence of generators of lengths from n to m. Moreover, every such sequence must contain every generator from S

at least once. The total number of decompositions on the tth step equals

$$\sum_{k=0}^{n-1}(-1)^k \cdot \binom{n}{k} \cdot (n-k)^t.$$

Therefore, on the tth iteration of the algorithm the number of multiplications is not greater than

$$(t-1) \cdot \sum_{k=0}^{n-1}(-1)^k \cdot \binom{n}{k} \cdot (n-k)^t.$$

Hence, the total number of all multiplications from the nth to the mth step can be estimated from above as

$$\sum_{t=n}^{m}(t-1) \cdot \sum_{k=0}^{n-1}(-1)^k \cdot \binom{n}{k} \cdot (n-k)^t.$$

The proof is complete.

Homogeneous theory

In this section we consider series of groups with its systems of generators. We put additional conditions on them and obtain some useful properties. Then it gives us a possibility to introduce new algorithms.

Inductive limits of groups. Recall the notion of inductive limit of groups. Let $(I,<)$ be a directed set, $\{G(i)|i \in I\}$ be a family of indexed groups. Assume that there exist homomorphisms $h_{i,j} : G(i) \to G(j)$, $i,j \in I$, $i < j$, such that
1. $h_{i,i} = id$ over $G(i)$ for every $i \in I$;
2. $h_{i,k} = h_{i,j} \circ h_{j,k}$ for every $i,j,k \in I$, $i < j < k$.

For indices $i,j \in I$ and elements $x \in G(i)$, $y \in \in G(j)$ we write $x \sim y$ if there exists $k \in I$ such that

$$h_{i,k}(x) = h_{j,k}(x).$$

Then $\sim$ is an equivalence relation on the disjoint union of given groups that admits to define multiplication of equivalence classes induced by multiplication rules in given groups.

Definition 4. The *inductive limit* of the system $(G(i), h_{i,j})$, $i,j \in I$ is the group defined as

$$\lim_{\longrightarrow} G(i) = \bigsqcup_{i \in I} G(i)/\sim.$$

Homogeneous system of generators. Let $G(1) < G(2) < \ldots < G(n) < \ldots$, $n \in \mathbb{N}$ be an ascending group series. Let i,j be natural numbers, $i < j$. We define the homomorphism $h_{i,j}$ from $G(i)$ to $G(j)$ as the embedding mapping between these groups, i.e.

$$h_{i,j}(g) = g,\ g \in G(i).$$

Then the inductive limit of the system $(G(i), h_{i,j})$, $i,j \in \mathbb{N}$ is well-defined.

Definition 5. A ***groups-generators series*** $\mathbb{G}$ is the sequence of pairs $(G(n),\ SoG(n)|n \in \mathbb{N})$ such that:
1. $G(1) < G(2) < \ldots < G(n) < \ldots$ is an ascending group series;
2. $SoG(n)$ is a system of generators of $G(n)$ and

$$SoG(n) \subset SoG(n+1), n \in \mathbb{N}.$$

Let $\mathbb{G}$ be a groups-generators series.

Denote by $IL(\mathbb{G})$ the inductive limit of the system $(G(i), h_{i,j})$, $i,j \in \mathbb{N}$ with embedding mappings $h_{i,j}$.

Denote by $GDiff(n)$ the set of generators, which appear exactly on the nth, $n \geq 1$, i.e.
1. $GDiff(1) = SoG(1)$,
2. $GDiff(n) = SoG(n) \backslash SoG(n-1)$, $n \geq 2$.

Definition 6. The groups-generators series $\mathbb{G}$ is called ***uniform*** if:

$$\langle \bigcup_{k=1}^{t} GDiff(i_k) \rangle \simeq G(t),$$

for every index tuple $I = (i_i, i_2, \cdots, i_t)$ of cardinality t.

Let C be a natural number.

Definition 7. The groups-generators series $\mathbb{G}$ is called ***C-stable*** if:

$$|GDiff(t)| = C, t \geq 1.$$

Let the groups-generators series $\mathbb{G}$ be C-stable. Suppose that elements from $\bigcup_{n \geq 1} SoG(n)$ are enumerated

$$\bigcup_{n \geq 1} SoG(n) = \{s_i \in \mathbb{G}|i \in \mathbb{N}\}$$

and the following conditions hold:
1. $SoG(n) = \{s_1, s_2, ..., s_C, s_{C+1}, \ldots, s_{n \cdot C}\}$, $n \geq 1$
2. $GDiff(n) = \{s_{(n-1) \cdot C+1}, s_{(n-1) \cdot C+2}, \ldots, s_{n \cdot C}\}$, $n \geq 1$.

Let $I = (i_1, i_2, \cdots, i_t)$ be an index tuple. Define the mapping h_I^C from $\overline{1, t \cdot C}$ to $\bigcup_{k=1}^{t} \overline{(i_k - 1) \cdot C + 1, i_k \cdot C}$ by the rule:

$$h_I^C(x) = (i_{[(x-1)/C]+1} - 1) \cdot C + (x-1)\, mod C + 1$$

Note that the unique representation of $x = = (k-1) \cdot C + r$, $k \in \overline{1,n}$, $r \in \overline{1,C}$ leads to the equality

$$h_I^C((k-1) \cdot C + r) = (i_k - 1) \cdot C + r. \quad (1)$$

The last equality can be reinterpreted as follows: if x is the index of the rth generator of $GDiff(k)$, then $h_I^C(x)$ is the index of the rth generator of $GDiff(i_k)$.

Now define a mapping

$$\psi_I^C : SoG(n) \to \bigcup_{k=1}^{n} GDiff(i_k)$$

by the rule:

$$\psi_I^C(s_i) = s_{h_I^C(i)}.$$

We will use notations

1. $SoG_I(n) = \bigcup\limits_{k=1}^{n} GDiff(i_k)$;
2. $G_I(n) = \langle SoG_I(n) \rangle$.

Note that $SoG_I(n)$ is the image of $SoG(n)$ under ψ_I^C.

Definition 8. A uniform and C-stable groups-generators series $\mathbb{G}$ is called *homogeneous* if for every natural t and every index tuple I of cardinality t the mapping ψ_I^C can be extended to the group isomorphism between $G(t)$ and $G_I(t)$.

We will omit the letter C in notations ψ_I^C, h_I^C. We will use notations ψ_I, h_I instead, unless otherwise stated in this paper.

Homogeneous equivalence. Let $\mathbb{G}$ be a homogeneous groups-generators series. We define a binary relation $\overset{\mathsf{H}}{\simeq}$ on $IL(\mathbb{G})$.

Definition 9. Let a, b be elements from $IL(\mathbb{G})$. We write $a \overset{\mathsf{H}}{\simeq} b$ if there exist index tuples I, J of the same cardinality n such that:

1. $a \in G_I(n)$;
2. $b \in G_J(n)$;
3. $({\psi_I}^{-1} \circ \psi_J)(a) = b$.

Lemma 14. *The binary relation $\overset{\mathsf{H}}{\simeq}$ is an equivalency.*

Proof. Reflexivity. Let a be an element from $IL(\mathbb{G})$. The definition of the inductive limit implies the existing of natural n such that $a \in G(n)$. Then for the index tuple $I = (1, 2, \ldots, n)$:

$$a \in G_I(n) = G(n) \text{ and } ((\psi_I)^{-1} \circ \psi_I)(a) = id(a) = a.$$

Symmetricity. Let a, b be elements from $IL(\mathbb{G})$ and $a \overset{\mathsf{H}}{\simeq} b$. Then there exist index tuples I, J of the same cardinality n:

$$a \in G_I(n),\ b \in G_J(n) \text{ and } ((\psi_I)^{-1} \circ \psi_J)(a) = b.$$

From the definition of $\overset{\mathsf{H}}{\simeq}$ we obtain

$$a = ((\psi_I)^{-1} \circ \psi_J)^{-1}(b)$$

Then the equality

$$((\psi_I)^{-1} \circ \psi_J)^{-1}(b) = ((\psi_J)^{-1} \circ \psi_I)(b),$$

implies the equality

$$((\psi_J)^{-1} \circ \psi_I)(b) = a.$$

Transitivity. Let $a, b, c \in IL(\mathbb{G})$ be such that $a \overset{\mathsf{H}}{\simeq} b$ and $b \overset{\mathsf{H}}{\simeq} c$. From the definition of $\overset{\mathsf{H}}{\simeq}$ it follows that there exist index tuples I, J_1 of cardinality n_1 such that

$$a \in G_I(n_1), b \in G_{J_1}(n_1), ((\psi_I)^{-1} \circ \psi_{J_1})(a) = b, \tag{2}$$

and also exist index tuples J_2, K of cardinality n_2 such that

$$b \in G_{J_2}(n_2), c \in G_K(n_2), ((\psi_{J_2})^{-1} \circ \psi_K^C)(b) = c. \tag{3}$$

Denote by m the cardinality $|J_1 \bigcap J_2|$. Let

$$A = (\max_{i \in I} i + 1, \ldots, \max_{i \in I} i + n_2 - m),$$

$$B = (\max_{k \in K} k + 1, \ldots, \max_{k \in K} k + n_1 - m)$$

and define the following index tuples:

$$\overline{I} = I \sqcup A,$$

$$\overline{J_1} = J_1 \sqcup (J_2 \backslash J_1),$$

$$\overline{K} = K \sqcup B,$$

$$\overline{J_2} = J_2 \sqcup (J_1 \backslash J_2).$$

Denote by N the sum $n_1 + n_2 - m$. Then $|\overline{I}| =$ $= |\overline{J_1}| = |\overline{K}| = |\overline{J_2}| = N$.

Denote by g_1 the element $(\psi_I)^{-1}(a)$. Then $g_1 \in G(n_1)$. Equality (2) implies that $g_1 =$ $= (\psi_{J_1})^{-1}(b)$. Since $\overline{I} = I \sqcup A$ the inclusion $SoG_{\overline{I}} \supset SoG_I(G)$ holds. It implies that $G_{\overline{I}}(N) >$ $> G_I(n_1)$. Hence, we obtain

$$(\psi_{\overline{I}})^{-1}(a) = (\psi_I)^{-1}(a) = g_1. \tag{4}$$

Similarly, from the equality $\overline{J_1} = J_1 \sqcup B$ we obtain:

$$(\psi_{\overline{J_1}})^{-1}(b) = (\psi_{J_1})^{-1}(b) = g_1. \tag{5}$$

Denote by g_2 the element $(\psi_K)^{-1}(c)$. Equation (3) implies that $g_2 \in G(n_2)$. Similar to the previous case one can show that

1. $(\psi_{\overline{J_2}})^{-1}(b) = (\psi_{J_2})^{-1}(b) = g_2$,
2. $(\psi_{\overline{K}})^{-1}(c) = (\psi_K)^{-1}(c) = g_2$.

Since index tuples $\overline{J_1}$ and $\overline{J_2}$ contains the same numbers, we have the equality $G_{\overline{J_1}}(N) = G_{\overline{J_2}}(N)$. Then the mapping

$$(\psi_{\overline{I}})^{-1} \circ \psi_{\overline{J_1}} : G_{\overline{I}}(N) \to G_{\overline{J_1}}(N)$$

maps a to b and the mapping

$$(\psi_{\overline{J_2}})^{-1} \circ \psi_{\overline{K}} : G_{\overline{J_2}}(N) \to G_{\overline{K}}(N)$$

maps b to c.

It follows that the composition

$$(\psi_{\overline{I}})^{-1} \circ \psi_{\overline{J_1}} \circ (\psi_{\overline{J_2}})^{-1} \circ \psi_{\overline{K}} : G_{\overline{I}}(N) \to G_{\overline{K}}(N) \tag{6}$$

maps a to c.

We are left to show that the composition (6) can be re-combined so that it is a product of two isomorphisms, according to the definition of $\overset{\mathsf{H}}{\simeq}$. It is enough to show that there exists an index tuple $I^{'}$ of cardinality N such that:

$$(\psi_{I'})^{-1} = (\psi_{\overline{I}})^{-1} \circ \psi_{\overline{J_1}} \circ (\psi_{\overline{J_2}})^{-1}.$$

Assume that $\overline{I} = (i_1, \ldots, i_N)$. Note that $\overline{J_1} = \overline{J_2}$. Hence, there exists a permutation $\pi : \overline{1, N} \to \overline{1, N}$ such that:
1. $\overline{J_1} = (j_{\pi(1)}, \ldots, j_{\pi(N)})$;
2. $\overline{J_2} = (j_1, \ldots, j_N)$.
Let s be arbitrary generator from $SoG(N)$. Then its index is $t = (k-1) \cdot C + r$ for some $k \in \overline{1, N}$, $r \in \overline{1, C}$. Then from (1) we obtain

$$h_{\overline{J_2}}(t) = (j_k - 1) \cdot C + r = (j_{\pi(t)} - 1) \cdot C + r,$$

$$(h_{\overline{J_1}})^{-1}((j_{\pi(t)} - 1) \cdot C + r) = (t-1) \cdot C + r,$$

$$(h_{\overline{I}})^{-1}((t-1) \cdot C + r) = (i_t - 1) \cdot C + r,$$

where t — position of j_t in J_2, which is mapped to j_k by π. Define the index tuple $I^{'} := (i_t | \pi(t) = = k, k \geq 1)$. Then

$$\psi_{I'}(s) = ((\psi_{\overline{J_2}}) \circ (\psi_{\overline{J_1}})^{-1} \circ \psi_{\overline{I}})(s).$$

From the definition of $\overset{\mathsf{H}}{\simeq}$ we obtain $(\psi_{I'}{}^{-1} \circ \psi_{\overline{K}})(a) = c$.

The proof is complete.

Definition 10. Elements $a, b \in IL(\mathbb{G})$ are called *homogeneously equivalent* if $a \overset{\mathsf{H}}{\simeq} b$.

Definition 11. The *homogeneous class* of an element $a \in IL(\mathbb{G})$ is the subset of all elements from $IL(\mathbb{G})$, which are homogeneously equivalent to a:

$$HC(a) = \{b \in IL(\mathbb{G}) | a \overset{\mathsf{H}}{\simeq} b\}.$$

Properties of a homogeneous class.

Lemma 15. *The set $\{e\}$ is the (trivial) homogeneous class of e.*

Proof. Let $a \in G(n)$ for some natural n. Suppose that $a \in HC(e), a \neq e$. From the definition of the homogeneous equivalence we obtain $e \overset{\mathsf{H}}{\simeq} a$. This means that there exist index tuples I, J of cardinallity n such that:

$$(\psi_I^{-1} \circ \psi_J)(e) = a.$$

Note that ψ_I, ψ_J are group isomorphisms. Hence, $\psi_I^{-1} \circ \psi_J$ is a group isomorphism as well. It means that

$$(\psi_I^{-1} \circ \psi_J)(e) = e,$$

which leads to a contradiction with ineaquality $a \neq \neq e$.

The proof is complete.

Lemma 16. *Let $a \in G_I(n)$, $b \in G_J(n)$ and $a \overset{\mathsf{H}}{\simeq} b$ for some index tuples I, J of cardinality n. Then*

$$|a|_{SoG_I(n)} = |b|_{SoG_J(n)}.$$

Proof. Denote by l the length $|b|_{SoG_J(n)}$. Suppose that

$$|a|_{SoG_I(n)} > l.$$

Then there exist generators $s_{j_1}, s_{j_2}, \ldots, s_{j_l} \in \in SoG_J(n)$ such that $b = \prod\limits_{k=1}^{l} s_{j_k}$.

Since the groups-generators series $\mathbb{G}$ is homogeneous the decomposition

$$\prod_{k=1}^{l} (\psi_J^{-1} \circ \psi_I)(s_{j_k}) = \prod_{k=1}^{l} s_{(h_J^{-1} \circ h_I)(j_k)} = a$$

is a decomposition of the element a over $SoG_I(n)$. Hence, $|a|_{SoG(n)} \leq l$. A contradiction.

Similarly the assumption $|a|_{SoG_I(n)} < l$ leads to a contradiction.

The proof is complete.

Lemma 16 gives rise to the following definition.

Let HC be a homogeneous class such that its intersection with G is non-trivial.

Definition 12. A *length of the homogeneous class* HC over S is defined as:

$$|HC|_S = |a|_S,$$

where a is an element from $HC \bigcap G$.

Lemma 17. *Let $a, b \in G(n)$, $a \overset{\mathsf{H}}{\simeq} b$ for some natural n. Then there exists an automorphism ψ of $G(n)$ such that:*

$$\psi(a) = b,$$

whose restriction on $SoG(n)$ is a permutation.

Proof. From $a \overset{\mathsf{H}}{\simeq} b$ it follows that for some index tuples I, J the mapping $\psi := (\psi_I)^{-1} \circ \psi_J$ is an automorphism of $G(n)$ such that

$$\psi(a) = b.$$

From the definition of mappings ψ_I, ψ_J it follows that the composition ψ is a permutation on $SoG(n)$.

Lemma 18. *Let HC be a homogeneous class and a be a properly generated element from $HC \bigcap G(n)$ over $SoG(n)$ for some natural n. Then every element of $HC \bigcap G(n)$ is properly generated over $SoG(n)$.*

Proof. Let b be an element from $HC \bigcap G(n)$. Suppose that b is not properly generated over $SoG(n)$. Then there exists a decomposition $D = (s_{i_1}, \dots, s_{i_l})$ of b over $SoG(n)$ such that $SoG(n) \backslash D \neq \emptyset$ as sets. Note that a, b belong to the same group $G(n)$. Since $b \in HC$ we have $b \overset{\mathsf{H}}{\simeq} a$. Then from Lemma 17 for b, a implies that there exists an automorphism of $G(n)$ such that

$$\psi(b) = a.$$

The homogeneous property of groups-generators series $\mathbb{G}$ implies that $\psi(D) = (\psi(s_{i_1}), \dots, \psi(s_{i_l}))$ is a decomposition of the element a over $SoG(n)$. Moreover, the restriction of ψ on $SoG(n)$ is a permutation. Hence, $SoG(n) \backslash \psi(D) \neq \emptyset$ as sets. It means, that the element a is not properly generated over $SoG(n)$. A contradiction.

The proof is complete.

Proposition 19. *Let HC be a homogeneous class and $a \in HC \bigcap G(n)$ for some natural n. If a is a diameter element of $G(n)$, then every element of $HC \bigcap G(n)$ is a diameter element of $G(n)$.*

Proof. Directly implies from the previous lemma.

Homogeneous down search algorithm

Let $\mathbb{G}$ be a homogeneous groups-generators series, n be a natural number. Assume that $G = G(n)$, $S = SoG(n)$.

Let HC be a homogeneous class such that $HC \bigcap G \neq \emptyset$. Fix an element $hc \in HC \bigcap G$. We define the product

$$HC * S = \{HC(hc \cdot s) | s \in S\}, \qquad (7)$$

Lemma 20. *The product (7) of the homogeneous class HC and the system of generators S is well defined.*

Proof. Let hc_1, hc_2 be different elements from $HC \bigcap G$. Lemma 17 for hc_1, hc_2 states that there exists an automorphism ψ of G such that:

$$\psi(hc_1) = hc_2.$$

Since elements from the same group both index tuples I and J consist of numbers $\{1, 2, \dots, n\}$. Therefore, there exists a permutation $\pi : I \cdot C \to J \cdot C$ such that:

$$\psi(s_i) = s_{\pi(i)}$$

for every $i \in \overline{1, n \cdot C}$. Note that $n \cdot C = |S|$.

Let $i, j \in \overline{1, |S|}$ be indices of generators in S, $\pi(i) = j$. Then

$$hc_2 \cdot s_j = hc_2 \cdot s_{\pi(i)} = \psi(hc_1) \cdot \psi(s_i) = \psi(hc_1 \cdot s_i).$$

The definition of homogeneous equivalence implies that $hc_2 \cdot s_j \in HC(hc_1 \cdot s_i)$. Hence, for every generator $s_j \in S$ there exists unique $s_i \in S$ such that

$$hc_2 \cdot s_j \in HC(hc_1 \cdot s_i).$$

The definition of homogeneous equivalent now implies the equality

$$HC(hc_2 \cdot s_j) = HC(hc_1 \cdot s_i).$$

Then moving through all generators of S we have:

$$\{HC(hc_2 \cdot s) | s \in S\} = \{HC(hc_1 \cdot s) | s \in S\}.$$

The proof is complete.

The following down search algorithm is based on homogeneous classes.

Algorithm 4: Homogeneous down search algorithm

```
Input: $G$ — a group, $S$ — its system of
       generators
Result: Diameter $D_S(G)$
Initialization: $found = \{HC(e)\}$,
 $all = \{HC(g) | g \in G\}$,
 $current\_level = \{HC(e)\}$, $level = 0$;
while $found \neq all$ do
    $previous\_level, current\_level =$
      $current\_level, \{\}$;
    for $HC \in previous\_level$ do
        $current\_level =$
          $= current\_level \bigcup HC * S$;
    end
    $current\_level =$
      $= current\_level \backslash found$;
     $found = found \bigcup current\_level$;
    $level = level + 1$;
end
Output: $level$
```

Lemma 21. *Let $a \in G$, $|a|_S = l$. Then l is the number of iterations of the main loop of homogeneous down search algorithm required to obtain the homogeneous class $HC(a)$.*

Proof. Induction on l.

The basis: case $l = 1$. Note that on the initialization phase of the algorithm we have equalities

$$current\_level = found = \{HC(e)\}.$$

Hence, when $level = 1$ and $CL = current\_level$ the following set of homogeneous classes will appear:

$$(\bigcup_{HC \in CL} HC * S) \setminus found =$$
$$= (HC(e) * S) \setminus \{HC(e)\} =$$
$$= \{HC(e \cdot s) | s \in S\} \setminus \{HC(e)\} = \{HC(s) | s \in S\}.$$

Let $|a|_S = 1$. Then there exists $i \in \overline{1,|S|}$ such that $a = s_i$. From previous equalities for *current_level* it follows that the class $HC(s_i)$ will appear on the first iteration of the main loop.

From the other hand, let $HC(a)$ appears on the first iteration of the main loop. Then, from previous equalities for *current_level* it follows that there exists $s \in S$ such that $HC(s)$ appears as a product $e \cdot s$ on the first step of the main loop and equality $HC(s) = HC(a)$ holds.

Lemma 17 implies that there exists an automorphism ψ of G such that:

$$\psi(s) = a.$$

Note that by the same Lemma, ψ is a permutation on S. Then there exists $j \in \overline{1,|S|}$ such that $\psi(s) = s_j = a$. Hence, $|a|_S = |s_j|_S = 1$.

Inductive step: case $l+1$ *under assumption that for* l *the statement holds.*

Let $|a|_S = l + 1$. Then there exist $i_1, i_2, \dots, i_{l+1} \in \overline{1,|S|}$ such that:

$$a = \prod_{k=1}^{l+1} s_{i_k}.$$

Then the element $b = \prod\limits_{k=1}^{l} s_{i_k}$ has length l. Otherwise, the length of a over S is less than $l+1$. Then, by inductive assumption, $HC(b)$ appears on the lth step of the algorithm. Lemma 21 implies that $HC(a) = HC(b \cdot s_{i_{l+1}})$. Then $HC(a)$ appears on the $(l+1)$th iteration of the algorithm. Otherwise, the element a appears on the same previous level. It leads to a contradiction with inductive assumption.

Let $HC(a)$ appears on the $(l+1)$th step of the algorithm. Then for some $b \in G$ and $s \in S$ we have the equality

$$HC(a) = HC(b \cdot s).$$

The inductive assumption implies $|b|_S = l$. The last equality leads to equality $b \cdot s = (\prod\limits_{k=1}^{l} s_{i_k}) \cdot s$ for some $s_{i_k} \in S$. This decomposition is minimal for $b \cdot s$. Otherwise, $HC(b \cdot s) = HC(a)$ appears earlier than on $(l+1)$th level. Therefore $|a|_S = |HC|_S = l + 1$.

The proof is complete.

Corollary 22. *Let* HC *be a homogeneous class and* HC *appears on the* l*th step of homogeneous down search algorithm for* G *and* S*. Then* $|el|_S = l$ *for every* $el \in HC \bigcap G$.

Proof. Let $a \in HC \bigcap G$. Lemma 21 implies that if HC appears on the lth step of the algorithm then $|a|_S = l$.

The proof is complete.

Theorem 23. *Homogeneous down search algorithm is correct.*

Proof. The algorithm terminates if and only if $found = all$. This equality holds if and only if every homogeneous class with non-trivial intersection with G appears at least once. This statement follows from Lemma 21 and existence of the minimum decomposition for every element.

Moreover, the last level of the algorithm contains homogeneous classes of elements of G, which have the maximum length over S. It means that if algorithm stops on step l, then from Corollary 22 it follows

$$|el|_S = l = D_S(G)$$

for every $HC \in last_level$ and every $el \in HC \bigcap G$.

The proof is complete.

Homogeneous middle down search algorithm

Let $\mathbb{G}$ be a homogeneous groups-generators series, n be a natural number. Assume that $G = G(n)$, $S = SoG(n)$.

Let HC be a homogeneous class with nontrivial intersection with G. Recall that

$$HC \cdot S = \{HC(hc \cdot s) | s \in S\},$$

where hc is a fixed element from the intersection $HC \bigcap G$.

We will use the following notations:

1. G_{fh} is the set of all properly generated homogeneous classes of the group G over S.

2. $D_{fh}(S, m)$ is the set of all decompositions over S of length m such that the following property holds:
if some element of a homogeneous class has a decomposition of length m then $D_{fh}(S, m)$ contains at least one decomposition of length m of some element of this homogeneous class, i.e

$$\text{if } D \in D_f(S, m),\ P(D) \in HC \text{ then}$$

$$\text{there exists } DH \in D_{fh}(S, m)$$

$$\text{such that } P(DH) \in HC.$$

Algorithm 5: Homogeneous middle down search algorithm

```
Input: $G$ — a group, $S$ — its strictly growing system of generators
Result: Diameter $D_S(G)$
Initialization: $found = \emptyset$, $all = G_{fh}$, $level = |S| - 1$;
while $found \neq all$ do
    $level = level + 1$;
    for $decomp \in D_{fh}(S, level)$ do
        $product = HC(P(decomp))$;
        if $product \in G_{fh}$ then
            $found = found \bigcup product$;
        end
    end
end
Output: $level$
```

Theorem 24. *The homogeneous middle down search algorithm is correct.*

Proof. Let m be the iteration of homogeneous middle down search algorithm when $found = all$. Let $D_S(G) = l$ for some natural l.

Suppose that $a \in G$ is a diameter element of G. Then strictly growing property implies that the element a is properly generated. Lemma 10 implies that the length of a over S is not less than $|S|$. It follows that the minimum decomposition of the element a belongs to $D_f(S, l)$. Homogeneous property implies that $D_{fh}(S, l)$ contains a decomposition defining a product homogeneously equivalent to a. And this decomposition has the same length l. Therefore, we have the inequality

$$m \geq l.$$

Let HC be a homogeneous class. Suppose that HC is found on step greater than l. It follows that there is no decomposition of HC with length from $|S|$ to l. Lemma 16 implies that there is no decomposition of any element from $HC \bigcap G$ with length from $|S|$ to l. But the diameter element of G has length l. It means that there exists a decomposition of an element from $HC \bigcap G$ of length stricktly less than $|S|$. From Lemma 10 it follows that every element of $HC \bigcap G$ is not properly generated. Hence, HC is not in G_{fh}. We obtain the inequality

$$m \leq l.$$

Therefore, we have the equality $m = l$.

The proof is complete.

References

1. Laszlo Babai and Akos Seress, "On the diameter of permutation groups", European Journal of Combinatorics. **13** (4), 231–243 (1992).
2. Harald A. Helfgott, "Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$", Annals of Mathematics. **167**, 601–623 (2008).
3. Emmanuel Breuillard and Ben Green and Terence Tao, *Approximate subgroups of linear groups* (2010).
4. Laszlo Pyber and Endre Szabo, *Growth in finite simple groups of Lie type of bounded rank* (2011).
5. Harald A. Helfgott and Akos Seress, "On the diameter of permutation groups", Ann. Math. **179** (2), 611–658 (2014).
6. S. Even and O. Goldreich, "The minimum-length generator sequence problem is NP-hard", Journal of Algorithms. **2** (3), 311–313 (1981).
7. S. Akers and B. Krishnamurthy and D. Harel, *The Star Graph: An Attractive Alternative to the n-Cube* (1987).
8. Thomas H. Cormenand, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein, *Introduction to Algorithms.* Third Edition (The MIT Press, 2009).

Ольшевський М. С.

АЛГОРИТМИ ПОШУКУ ДІАМЕТРА ОРІЄНТОВАНИХ ГРАФІВ КЕЛІ

Розглянуто добре відому задачу пошуку діаметра скінченної групи. Вона формулюється так: знайти найбільший серед діаметрів групи відносно її систем твірних. Діаметром групи є діаметр графа Келі, що будується на основі групи та її системи твірних. У цій роботі розглянуто підзадачу задачі пошуку діаметра групи, а саме, задачу знаходження діаметра групи відносно заданої системи твірних. Показано, що ця задача поліноміально зводиться до задачі пошуку мінімальних розкладів елементів.

Для розв'язання задачі знаходження діаметра групи відносно заданої системи твірних запропоновано п'ять алгоритмів: простий алгоритм пошуку вниз, швидкий алгоритм пошуку вниз, серединний алгоритм пошуку вниз, однорідний алгоритм пошуку вниз та однорідний серединний алгоритм пошуку вниз.

Перші два алгоритми є універсальними, а інші вимагають виконання додаткових умов на *системи твірних.*

Для алгоритму серединного спуску введено поняття строго зростаючої системи твірних. За виконання цієї умови, пошук мінімальних розкладів потенційних найдовших розкладів можна почати одразу ж із певної множини.

Введено окрему теорію однорідності. В ній розглядануто ряди груп та їх систем твірних, що задовольняють певним додатковим умовам. Введено властивість однорідності таких рядів та відношення еквівалентності їх елементів. Основною метою введення такого відношення є збереження розкладів її елементів в одному класі. Ця властивість дає можливість обраховувати мінімальний розклад лише для представника класу еквівалентності.

Для алгоритмів однорідного пошуку вниз та однорідного серединного пошуку вниз необхідною умовою застосування є належність групи до однорідного генеративного ряду груп. Тоді задача знаходження мінімальних розкладів елементів зводиться до знаходження мінімальних розкладів представників класів еквіваленції.

Показано, що всі описані алгоритми є коректними. Зроблено оцінки складності їх роботи.

Ключові слова: граф Келі, діаметр групи, система твірних.

Матеріал надійшов 25.10.2021