Astérisque

SERGEI BRODSKY

On groups generated by a pair of elements with small third or fourth power

Astérisque, tome 258 (1999), p. 255-279

<http://www.numdam.org/item?id=AST_1999__258__255_0>

Astérisque **258**, 1999, p. 255–279

ON GROUPS GENERATED BY A PAIR OF ELEMENTS WITH SMALL THIRD OR FOURTH POWER

by

Sergei Brodsky

Abstract. — The paper is devoted to an investigation of two-generated groups such that the $m-$th power of the generating pair contains less than 2^m elements . It is proved, in particular, that if the cube of the generating pair contains less than 7 elements or its fourth power contains less than 11 elements, then the group is solvable. Otherwise, it is not necessarily solvable. The proofs use computer calculations.

1. Introduction

Let G be a group. A finite subset M of G is called *a set with small $m-$th power* (m is some integer) if $|M^m| < |M|^m$ (here $M^m = \{a_1 \dots a_m | a_1, \dots, a_m \in M\}$ and $|.|$ denotes the cardinality of the set). The structure of the groups in which each $p-$element subset has a small $m-$th power (for some small p and m), as well as the structure of the set of all special elements [(1)], was investigated in papers [1-5,7], among others. Notice that the notion of identification pattern, which is introduced in the present paper, is close to the notion "type of square" which was introduced in [3], but we will not discuss the relationship between these concepts.

In this paper we are interested in the structure of groups generated by a two-element set $M = \{a, b\}$ with a small third and fourth power. The proofs are based on pure combinatorial considerations, and are ultimately reduced to enumerating a list of very concrete groups, unfortunately; the total number of cases which appear here is so large that we need to use a computer. All computer calculations were developed by the author on an IBM PC using self-made programs which were written in the frame-work of the mathematical package MATLAB-386 [(2)]. These programs provide a simplification of finite group presentations using Tietze transformations, a calculation

1991 ***Mathematics Subject Classification.*** — 20F05, 20F16.

Key words and phrases. — Corepresentations of groups, solvable groups, small subsets in groups.

Supported in part by the Israel Ministry of Absorption and the Rashi Foundation.

[(1)]The element $a \in G$ is called *special* if the set $\{a, b\}$ has the small $m-$th power for some fixed integer m and each $b \in G$.

[(2)]©The MathWorks, Inc., 1984-1991, version 3.5k.

of a commutator subgroups in the case of a finite index, and also recognition of groups of some types. The methods of programming are in some interest. Since their description would lead us too far from the topic of the present paper, the topic could be a subject of a separate publication. The results of the mentioned calculations are given in the Appendix.

Acknowledgment. — The author would like to thank Prof. Ya. Berkovich for the introduction into the subject of the investigations, as well as for useful discussions.

Let us formulate a general combinatorial assertion which will be needed below. Let A be a finite set, θ an equivalence relation on A, and $R \subseteq A \times A$. We say that the equivalence relation θ *is generated by* R, and write $\theta = \mathrm{eq}(R)$ if θ is the least equivalence relation contaning R. The relation θ will be called *independent* if θ is the minimal generating relation for its closure $\mathrm{eq}(R)$. The following lemma can be easily proved using induction on $|R|$.

Lemma 1. — *Let θ be an equivalence relation on the set A generated by a relation $R \subseteq A \times A$. Then $|A/\theta| \geq |A| - |R|$. If, in addition, R is independent, then $|A/\theta| = |A| - |R|$.*

2. Identification graphs and their properties

Let G be a group generated by two elements a and b: $G = \mathrm{gp}(a, b)$. We fix a and b as signature constants and regard the group G as the quotient-group of the free group $F = \langle a, b\rangle$. The natural epimorphism $\Phi_G : F \to G$ defines an equivalence relation on the group F which will be denoted by the symbol θ_G. We define $H(G)$ as the normal closure of the element ab^{-1} in G: $H(G) = (ab^{-1})^G$, and set $u_i = a^i b a^{-i-1}$ for each $i \in \mathbb{Z}$, so $H = \mathrm{gp}(u_i | i \in \mathbb{Z})$. For each element, or a subset P of $H(G)$, we let $P^{(s)}$ denote the element (the subset) $a^s P a^{-s}$; it is clear that $P^{(s)}$ can be obtained from P by adding s to all indices of the u-symbols. We also apply the same notation to elements and subsets of the Cartesian square $H_G \times H_G$: $(P, Q)^{(s)} = (P^{(s)}, Q^{(s)})$. Since $|\{a, b\}^m| = |\{a, b\}^m a^{-m}|$, the condition $|\{a, b\}^m| = n \leq 2^m$ $(m \geq 2)$ is equivalent to the condition $|H_m(G)| = n$ where $H_m(G) = \{a, b\}a^{-m}$. One can see that $H_m(G)$ consists of values in G of all strictly increasing positive words in symbols $u_0, \ldots, u_{m-1}$:

$$H_m(G) = \{u_{i_1} \ldots u_{i_k} \mid 0 \leq i_1 < \cdots < i_k \leq m-1,\ 0 \leq k < m\} \subseteq H(G).$$

We denote by U_m the set of all strictly increasing positive words in symbols $u_0, \ldots, u_{m-1}$ itself, so that $H_m(F) = \mathrm{gp}(U_m)$ and $H_m(G) = \mathrm{gp}(\Phi_G(U_m))$.

For $S, T \in U_m$ we say that the pair (S, T) is an *irreducible m-pair* if exactly one of the words S, T begins with u_0 and exactly one of them ends with u_{m-1}. If the irreducible m-pair e has the form $(u_0 P, Q u_{m-1})$ we say that it is *positive*, otherwise e has the form $(u_0 P u_{m-1}, Q)$ and in this case we say that e is *negative*. In both cases we define $i(e) = P$ and $t(e) = Q$. The set of all positive irreducible m-pairs is denoted by I_m^+ and the set of all negative irreducible pairs is denoted as I_m^-.

For given $R \in U_m$, let $\tilde{R}$ be the word in symbols a and b which freely equals R; it is clear that $\tilde{R}$ is a positive word of length m. We say that an irreducible m-pair

(S,T) is *degenerate* if there exists some irreducible $(m-1)$-pair $(P,Q) \in \theta_G$ such that one of the words $\tilde{P}, \tilde{Q}$ is a subword of one of the words $\tilde{S}, \tilde{T}$. The following lemma is obvious.

Lemma 2. — *Let $\theta_0 = \theta_G \cap (U_{m-1} \times U_{m-1})$ and let (S,T) be a degenerate irreducible m-pair. Then $(S,T) \in \theta$ if and only if $(S,T) \in \mathrm{eq}(\theta_0 \cup \theta_0^{(1)} \cup \theta_0 u_{m-1} \cup u_0 \theta_0^{(1)})$.*

Let us now define the *positive identification m-graph* $\Gamma_m^+(G)$ of G as the oriented graph with the set of vertices $H_{m-2}^{(1)}$ and the set of edges $E_m^+(G) = (\Phi_G \times \Phi_G)(I_m^+ \cap \theta_G)$, and the *negative identification m-graph* $\Gamma_m^-(G)$ of G as the graph with the same set of vertices and the set of edges $E_m^-(G) = (\Phi_G \times \Phi_G)(I_m^- \cap \theta_G)$. The incidence relations in both these graphs are given by the following rule: if $e \in E_m^+ \cup E_m^-$ and $e = (\Phi_G \times \Phi_G)(e_0)$, where e_0 is some irreducible m-pair, then the initial vertex of e is $\Phi_G(i(e_0))$ and the terminal vertex of e is $\Phi_G(t(e_0))$.

The correctness of the last definition, as well as the validity of the following lemma, can be easily verified.

Lemma 3. — *Let $G = \mathrm{gp}(a,b)$ and $m \geq 2$. Then each vertex of the positive m-identification graph $\Gamma_m^+(G)$, and each vertex of the negative m-identification graph $\Gamma_m^-(G)$, has at most one incoming edge and at most one outgoing edge.*

For $e \in E_m^+(G) \cup E_m^-(G)$, we call e a *degenerate* edge if and only if the set $(\Phi_G \times \Phi_G)^{-1}(e)$ contains some degenerate irreducible pair. Lastly, let $\mathrm{def}_m(G)$ denote the total number of nondegenerate edges in the set $E_m^+(G) \cup E_m^-(G)$.

Lemma 4. — *Let $G = \mathrm{gp}(a,b)$ and $m \geq 2$. Then*

$$\mathrm{def}_m(G) \geq -2^m - |H_m(G)| + 4|H_{m-1}(G)|.$$

Proof. — Let $d = 2^{m-1} - |H_{m-1}(G)|$. Then, by Lemma 1, the trace θ_0 of the equivalence relation θ_G on the set U_{m-1} is generated by some relation R_0 of cardinality d. Since $U_m \times U_m = (U_{m-1} \times U_{m-1}) \cup (U_{m-1}^{(1)} \times U_{m-1}^{(1)}) \cup (U_{m-1}u_{m-1} \times U_{m-1}u_{m-1}) \cup (u_0 U_{m-1}^{(1)} \times u_0 U_{m-1}^{(1)})$, the trace θ of the equivalence relation θ_G on the set U_m can be represented as the union of their traces $\theta_0, \theta_1, \theta_2, \theta_3$ on the sets $U_{m-1}, U_{m-1}^{(1)}, U_{m-1}u_{m-1}, u_0 U_{m-1}^{(1)}$, respectively, and the relation $(I_G^+ \cup I_G^-) \cap \theta_G$. Each of the equivalence relations θ_k $(k = 1,2,3,4)$ is generated by a d-element relation $(R_0, R_0^{(1)}, R_0 u_{m-1}, u_0 R_0^{(1)}$, respectively). The union R of last the four relations contains no more than $4d$ elements. By Lemma 2, the difference $(I_G^+ \cup I_G^-) \cap \theta_G \setminus \mathrm{eq}(R)$ is contained in the set of all nondegenerate irreducible m-pairs from θ. Now let us define R_1 as the set which contains one $\Phi_G \times \Phi_G$ pre-image of each nondegenerate edge from $E_m^+(G) \cup E_m^-(G)$. Then $\theta_0 = \mathrm{eq}(R \cup R_1)$, and it only remains to apply Lemma 1.

The inequality which was obtained in Lemma 4 provides us with good necessary conditions for a group to be generated by a pair with a small power. However, we need a more detailed version of this result which also includes some sufficient conditions.

Lemma 5. — *Let* $G = \mathrm{gp}(a, b)$ *and* $H_{m-1}(G) \geq 2^{m-1} - 1$ $(m \geq 2)$. *Then*

$$\mathrm{def}_m(G) = -2^m - |H_m(G)| + 4|H_{m-1}(G)|.$$

Proof. — Let $H_{m-1}(G) = 2^{m-1}$. Preserving the notations which were introduced in the Proof of Lemma 4, we have here that $R = \varnothing$ and R_1 coinsides with $E_m^+(G) \cup E_m^-(G)$. Lemma 3 asures us that the last relation is independent. By Lemma 1, the inequality of Lemma 4 becomes an exact equality.

Let now $H_{m-1}(G) = 2^{m-1} - 1$. In this case R consists of four pairs, and one can verify that it is independent. Repeating the previous argument, and bearing in mind that the definition of a nondegenerate edge provides the independence of the united relation R_1 we again have an exact equality - instead of the inequality - in Lemma 4.

The fact that the quotient group $G/H(G)$ is cyclic reduces the investigation of the group $G(\Gamma)$ to an investigation of the group $H(G)$. The following lemma shows that in nontrivial situations this group is finitely generated.

Lemma 6. — *Let* $|H_m(G)| < 2^m$. *Then* $H(G) = \mathrm{gp}(u_0, \ldots, u_{m-2})$.

Proof. — If $m = 1$ then $u_0 = 1$ and $H = 1$. Hence, we may assume that $m \geq 2$. Without loss of generality, we may also assume that $|H_{m-1}(G)| = 2^{m-1}$. By Lemma 4, $\mathrm{def}_m(G) \geq 1$, and thus there exists an irreducible m-pair (S, T) such that G satisfies the equality $S = T$ - implying that G also satisfies the equality $S^{(i)} = T^{(i)}$ for each $i \in \mathbb{Z}$. Therefore, for each $i \in \mathbb{Z}$, $u_i \in \mathrm{gp}(u_{i-m+1}, \ldots, u_{i-1})$ and $u_i \in \mathrm{gp}(u_{i+1}, \ldots, u_{i+m-1})$. Now, using induction on i, one can prove that for each $i \in \mathbb{Z}$, $u_i \in \mathrm{gp}(u_0, \ldots, u_{m-2})$.

It should be noted that in the case $m = 2$ Lemma 6 asserts that the group H is cyclic. (In fact, this assertion is obvious and well known).

3. Identification patterns and their universal groups

Let us consider a finite sequence $\Gamma = \langle E_2^+, E_2^-, \ldots, E_m^+, E_m^- \rangle$ such that the set E_k^+ of its *positive k-edges* and the set of E_k^- of its *negative k-edges* consist of positive and negative irreducible k-pairs, respectively $(2 \leq k \leq m)$. For each $e \in E_k^+ \cup E_k^-$, we define the *initial* vertex of e as $i(e)$ and the *terminal* vertex of e as $t(e)$; so for each $2 \leq k \leq m$ we obtain two oriented graphs with the set of vertices U_{k-2}: the *positive k-graph of* Γ which will be denoted by $(\Gamma)_k^+$, and the *negative k-graph of* Γ which will be denoted by $(\Gamma)_k^-$. We write $e = (w_1, w_2)_k^+$ (or $e = (w_1, w_2)_k^-$) if e is a positive (or a negative) k-edge with the initial vertex w_1 and the terminal vertex w_2. If we need to describe any such sequence in a concrete situation, we do this by enumerating of its edges. Further, we consider the sequence of groups $\{H_k(\Gamma) | 2 \leq k \leq m\}$ which are defined in the set of generators $\{u_i | i \in \mathbb{Z}\}$ by the sets of relations $\bigcup \{\mathcal{R}_k(\Gamma)^{(s)} | s \in \mathbb{Z}\}$, where $\mathcal{R}_k(\Gamma) = \{u_0 i(e) = t(e) u_{p-1}^{\varepsilon(e)} | e \in E_p^+ \cup E_p^-,\ 2 \leq p \leq k\}$, $\varepsilon(e) = 1$ for $e \in E_p^+$ and $\varepsilon(e) = -1$ for $e \in E_p^-$. For each of these groups, the natural epimorphism $\Phi_{\Gamma,k} : U_k \to H_k$ defines the equivalence relation on the group U_k which is denoted by