Elementary equations and basic properties of groups

Contents

1 Commutativity

1.1 Commutativity equation $[x, y] = 1$

We start with the classical approach using induction on the total length of solutions. Then we demonstrate how to solve the equation using cancellation schemes.

Lemma 1 *Let $u, v \in F(A)$. If $uv = vu$ then there exists $w \in F(A)$ and integers m, n such that*

$$u = w^m, v = w^n$$

Proof. Induction on $|u| + |v|$.

If $|u| + |v| = 1$, then $u = 1$ or $v = 1$ and in this case the conclusion of the lemma is obvious. Suppose now that $|u|, |v| \geq 1$ and $|u| \leq |v|$.

Case 1. Assume that there is no cancellation in uv, i.e., $|uv| = |u| + |v|$. Then $|vu| = |uv| = |u| + |v|$ and there is no cancellation in vu. Hence vu and uv are reduced. Now from $uv = vu$ and $|u| \leq |v|$ we deduce that $v = u \circ v_1$. Therefore $uv_1 = v_1 u$ and $|v_1| < |v|$. By induction, u and v_1 (hence u and v) are powers of some $w \in F(A)$, as desired.

Case 2. Suppose u cancels completely in v. Then $v = u^{-1} \circ v_1$ and the equality $uv = vu$ takes the form $uu^{-1}v_1 = u^{-1}v_1 u$. The latter can be written as

$$uv_1 = v_1 u.$$

Since $|v_1| < |v|$ we can proceed by induction.

Case 3. There is a cancellation in uv, but u does not cancel completely in uv. In this event

$$u = u_1 \circ y, v = y^{-1} \circ v_1, \quad y \in A^{\pm 1}.$$

Then $uv = vu$ can be rewritten as

$$u_1 v_1 = y^{-1} v_1 u_1 y \tag{1}$$

Since $|v| \geq |u|$ and v does not cancel completely in uv, it follows that vu begins with y^{-1}. Similarly, u_1 does not cancel completely in $u_1 v_1$ (otherwise u cancels out in uv), therefore u_1 begins with y^{-1}. Hence $u_1 = y^{-1} \circ u_2 \circ y, v_1 = y^{-1} \circ v_1$ and it follows from (1) that

$$u_2 v_1 = v_1 y^{-1} u_2 y \tag{2}$$

Notice (comparing lengths) that cancellation must occur in the right-hand side of (2). There is only one possible place where the cancellation may occur, namely in $v_1 y^{-1}$, so $v_1 = v_2 \circ y$. In this event, $u = y^{-1} \circ u_2 \circ y, v = y^{-1} \circ v_2 \circ y$, and equality $uv = vu$ takes the form

$$u_2 v_2 = v_2 u_2.$$

Now the conclusion of the lemma follows by induction.

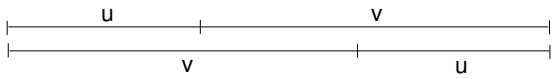
□

Corollary 1 *The set* $\{(w^n, w^m) | w \in F(A), n, m \in \mathbf{Z}\}$ *is the solution set of the equation* $[x, y] = 1$.

Now we illustrate the proof above by cancellation schemes.

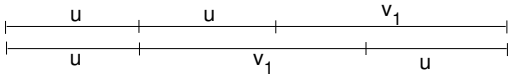
Let $u, v \in F(A)$ and $[u, v] = 1$. Consider all possible cancellation schemes in the product $uvu^{-1}v^{-1}$.

Case 1. No cancellation in uv. Then the corresponding scheme is the following:

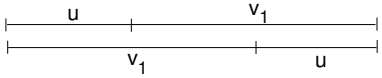


(we assume here that $|u| \leq |v|$).

Clearly, the point A divides v into two parts u and v_1 ($v = u \circ v_1$). Draw u on both occurrences of v in the scheme:



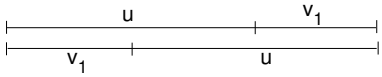
Cut out the common initial segment u from the scheme, the resulting scheme will be of the following type:



It is exactly the initial scheme provided $|u| \leq |v_1|$. We can repeat the process until this is possible and in finitely many steps (say, m_1 steps) we will have:

$$\begin{cases} v = u^{m_1} v_1, \ |u| > |v_1| \\ u = u \end{cases}$$

The resulting scheme will be like this:

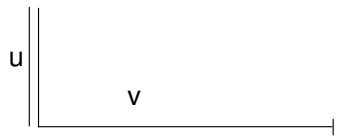


Now we see that $u = v_1 \circ u_1$ and we can again cut out the common initial segment v_1 from the scheme and proceed to do so until this is possible, i.e., until $|u_1| < |v_1|$. In finitely many steps, say K_1 steps, we will have

$$\begin{cases} v = u^{m_1} \circ v_1, \ |u_1| \leq |v_1| \\ u = v_1^{K_1} \circ u_1 \end{cases}$$

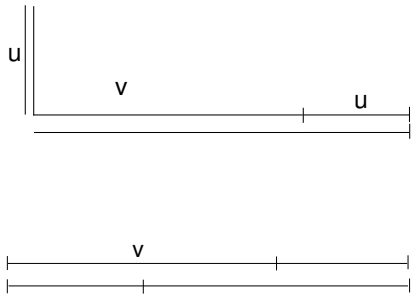
Now again we have the initial cancellation scheme and we can repeat the process again. Since, we cannot decrease the length of $|u|$ or $|v|$ forever, the process will stop eventually. At this point we will have $u_1 = 1$ or $v_1 = 1$. In any event, u and v will be powers of either u_1 or v_1.

Case 2. u cancels out in uv.



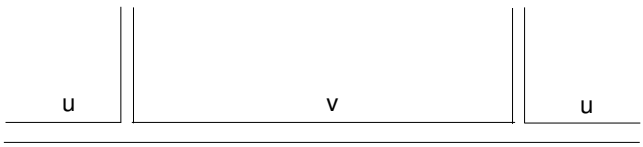
Then there exists only one possible scheme:

If we draw it in the following way



then we can see that the process from Case 1 will work in this case also.

Case 3. There is a cancellation in uv. Then there is a cancellation in vu and the corresponding scheme is as follows:



Let a be the first literal in u, i.e., $u = a \circ u_1$. Draw a in the scheme

Then we see that $u = a \circ u_2 \circ a^{-1}, v = a \circ v_2 \circ a^{-1}$.

Clearly, we can cut out the segment labelled by a everywhere in the scheme and the resulting scheme will be the cancellation scheme for $[u_2, v_2] = 1$. It is easy to see that in finitely many steps we will cut out either the whole initial segment up to the point A, or we will cut out both pinches. In either case we will get the scheme from case 1) or case 2).

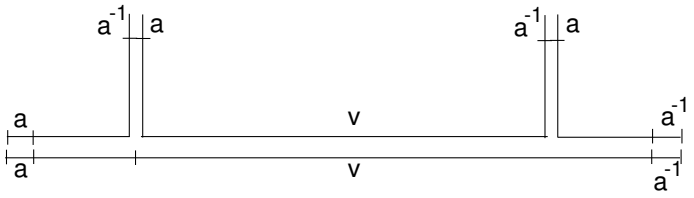
□

Exercise 1 *Define a long commutator* $[x, u_1, \ldots, u_n]$ *inductively as follows:*

$$[x, u_1, \ldots, u_n] = [[x, u_1, \ldots, u_{n-1}], u_n].$$

For given $u_1, \ldots, u_n \in F(A)$ *solve the equation*

$$[x, u_1, \ldots, u_n] = 1.$$



1.2 Centralizers in $F(A)$

Definition 1 *Let G be a group and M a subset of G. Then the set*

$$C_G(M) = \{g \in G | [g, m] = 1 \ \forall m \in M\}$$

is called the centralizer of M in G.

It is easy to see that $C_G(M)$ is always a subgroup of G. Sometimes we omit G from the notation and write $C(M)$.

Proposition 1 *Let F be a free group and M be a subset of F. If $M \neq \{1\}$, then the centralizer $C_F(M)$ is cyclic.*

Proof. If $g \in M$, then $C_F(M) \subseteq C_F(g)$. Therefore to prove the proposition it suffices to prove that the centralizer $C_F(g)$ of any non-trivial element $g \in F$ is cyclic. Let q_0 be the maximal root of g in F, then $g = {q_0}^k$ for some positive k. We claim that for any $f \in F$ if $[{q_0}^n, f] = 1$, then $[q_0, f] = 1$. Indeed, if ${q_0}^n f = f {q_0}^n$, then

$${q_0}^k = f {q_0}^k f^{-1} = (f q_0 f^{-1})^k$$

since k-roots of elements in F are unique (see Section 3.1), then $q_0 = f q_0 f^{-1}$, i.e., $[q_0, f] = 1$. It follows that $C_F(g) = C_F(q_0)$. Now if $f \in C_F(q_0)$, then by Lemma 1 q_0 and f are powers of some element $w \in F$. Since q_0 is not a proper power, then $q_0 = w^{\pm 1}$ and f is a power of q_0. Consequently, the maximal root q_0 is a generator of the centralizer $C_F(g)$. □

Let G be an arbitrary group. We denote by $\mathcal{C}(G)$ the set of all centralizers in G. It is not hard to see that $\mathcal{C}(G)$ forms a *lattice* with respect to inclusion. Indeed, the group $G = C(1)$ is the largest, and the center $Z(G) = C_G(G)$ is the smallest elements in $\mathcal{C}(G)$. Moreover,

$$C(X) \cap C(Y) = C(X \cup Y)$$

is the *greatest lower bound* for $C(X), C(Y)$ and the intersection of all centralizers in G containing $C(X) \cup C(Y)$ is a centralizer in G which is the *least upper bound* of $C(X), C(Y)$.

The centralizer lattice $\mathcal{C}(F)$ of a free non-abelian group is very simple since every two proper centralizers in F either coincide or intersect trivially. So the lattice looks like in the picture below.

Commutation properties of non-commutative transitive groups depend on the lattice $\mathcal{C}(G)$. We say that G satisfies the a.c.c. (d.c.c) on centralizers if the lattice $\mathcal{C}(G)$ satisfies this condition. Moreover, if there exists a uniform finite bound on the length of strictly ascending (or descending) chains of centralizers in G then we say that G has finite *centralizer dimension*. Algebraic structure of the lattice $\mathcal{C}(G)$ impose various properties on underlying groups.

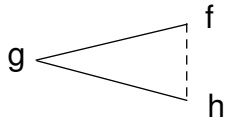
There are several interesting questions about centralizers of groups in a given class.

General questions: *Let $\mathcal{K}$ be a class of groups.*
1) *Describe groups G from $\mathcal{K}$ with d.c.c. on centralizers.*
2) *Describe groups G from $\mathcal{K}$ with finite c-dimension?*
3) *For a given lattice L describe groups G from $\mathcal{K}$ with $\mathcal{C}(G) \simeq L$.*

1.3 Commutative-transitive groups

Definition 2 *A group G is called* commutative-transitive *if the commutation is an equivalence relation on $G - \{1\}$, i.e., if $[g, f] = 1$ and $[g, h] = 1$ then $[f, h] = 1$ provided f, g, h are non-trivial elements of G.*

The *commutation graph* of G consists of elements from $G - \{1\}$ as vertices of this graph and two vertices q, h are connected by an edge if and only if $[g, h] = 1$. Now it is clear, that a group G is commutative-transitive if and only if in the commutation graph of G each connected component is a complete subgraph (i.e., any two vertices of the component are connected by an edge). So whenever we have two adjacent edges connecting g with f and h, then there exists an edge connecting f and h.



We refer to commutative-transitive groups as to CT groups.
The following lemma is obvious.

Lemma 2 *A group G is commutative-transitive if all proper centralizers of G are commutative.*

Examples 1 *The following groups are commutative -transitive.*

1) Free groups.

2) Torsion free hyperbolic groups (all centralizers are infinite cyclic).

3) Fully residually free groups.

4) Groups acting freely on Λ-trees.

Notice, that for a non-abelian CT group G the centralizer lattice $\mathcal{C}(G)$ is precisely the same as for a free non-abelian group F.

Exercise 2 *Let G be a torsion-free CT group. Prove that if $x, y \in G$ and $x^n = y^m$ then $x = y$.*

1.4 CSA groups

A subgroup H of a groups G is called *malnormal* if for any $g \in G$ the following condition holds:

$$H^g \cap H \neq 1 \Longrightarrow g \in H.$$

A group G is called a *CSA group* if every maximal abelian subgroup of G is malnormal. Observe, that every CSA group is commutative-transitive.

Lemma 3 *A group G is CSA if and only if all proper centralizers in G are abelian and malnormal.*

Proof. Exercise.

In particular, every CSA group is CT.

Theorem 1 *Let G be a torsion-free group such that every proper centralizer of G is cyclic. Then G is a CSA group.*

Proof. To follow.

Examples 2 *The following groups are CSA:*

1) Free groups.

2) Torsion free hyperbolic groups (all centralizers are infinite cyclic).

3) Fully residually free groups.

4) Groups acting freely on Λ-trees.

Exercise 3 *Give a direct proof that a free group is CSA.*

1.5 Independent Centralizers

We say that a group G has *independent centralizers* if any two distinct proper centralizers C_1 and C_2 in G generate a subgroup $\langle C_1, C_2\rangle$ which is free product $C_1 * C_2$ (i.e., non-empty alternating products of non-trivial elements from C_1, C_2 are non-trivial in G).

For example, free groups and surface groups (with exception of the non-orientable group of genus 2) satisfy this property. If all proper centralizers in G are cyclic (as in the case of torsion-free hyperbolic groups) then the group G has independent centralizers if and only if every subgroup of G generated by two elements is free. Such groups are called *2-free*. In fact, it has been shown by Arjantseva and Olshanskii [**?**] that a "randomly chosen" group is 2-free. Fully residually free groups form another class of groups with independent centralizers (see [**?**]).

The following question is of considerable interest.

Problem 1 *Do the groups acting freely on Λ-trees have independent centralizers?*

2 Conjugacy

2.1 Cyclically reduced words and cyclic decomposition

Let $F(A)$ be a free group with basis $A = \{a_1, \ldots, a_n\}$.

Definition 3 *A reduced word $w = y_1 \cdots y_m,\ (y_i \in A^{\pm 1})$ is called cyclically reduced if $y_1 \neq y_m^{-1}$.*

For example, the word ${a_1}^{-1}a_2a_2$ is cyclically reduced, but the word ${a_1}^{-1}a_2a_1$ is not.

Lemma 4 *Let w be a reduced word from $F(A)$. Then there exists a cyclically reduced word $\overline{w}$ and a reduced word w_1 such that*

$$w = {w_1}^{-1} \circ \overline{w} \circ w_1. \tag{3}$$

Moreover, such words $\overline{w}$ and w_1 are unique.

Proof. We will read off $\overline{w}$ and w_1 from w using the following marking process. Let $w = y_1 \cdots y_m,\ (y_i \in A^{\pm 1})$ be a reduced word. Compare the initial literal y_1 with the final literal y_m. If $y_1 = {y_m}^{-1}$ then mark them both, and repeat

the process for the unmarked subword $y_2 \cdots y_{m-1}$. In the case $y_1 \neq {y_m}^{-1}$ we stop. Clearly, we will finish in $\leq |w|$ steps, and the unmarked subword is cyclically reduced, we denote it by $\overline{w}$. Meanwhile, the longest marked subword at the end of w is w_1. From the discussion above it follows that

$$w = {w_1}^{-1} \circ \overline{w} \circ w_1$$

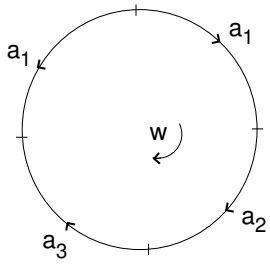
and the words $\overline{w}, w_1$ are uniquely determined by w. This proves the lemma. □

Definition 4 *Let w be an element of $F(A)$. Then the above decomposition*

$$w = {w_1}^{-1} \circ \overline{w} \circ w_1$$

is called the cyclic decomposition of w, and the word $\overline{w}$ is called the cyclically reduced form of w.

The cyclically reduced form of w has a simple visual interpretation. Every word $w \in F(A)$ defines a *cyclic word* w, which is the word w written on a circle in the clockwise orientation. For example, $w = a_1 a_2 a_3 {a_1}^{-1}$ defines the cyclic word

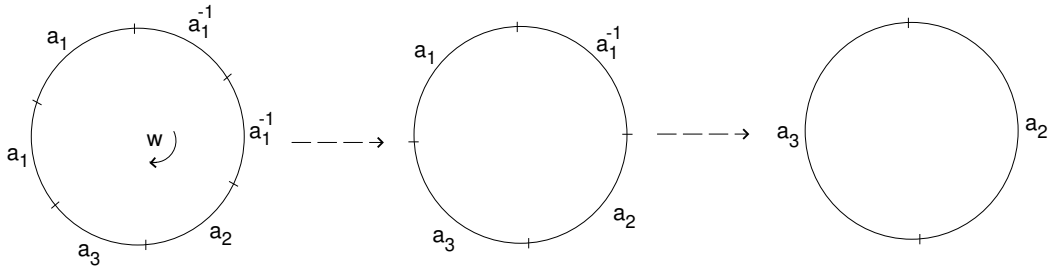


A *reduced cyclic word* is a cyclic word without neighbors of the type yy^{-1} ($y \in A^{\pm 1}$).

Every cyclic word can be transformed into a unique reduced cyclic word by means of elementary reductions exactly in the same way as for the ordinary words (see Section 1.2). Notice, that if w is a reduced word, then the reduction process for the cyclic word w is uniquely determined at each step, i.e., at each step there is only one possible elementary reduction to perform. For example, if

$$w = {a_1}^{-2} a_2 a_3 {a_1}^2$$

then the reduction process for w can be described as follows.



$$w = a_1^{-2}a_2a_3a_1^2 \;\rightarrow\; a_1^{-1}a_2a_3a_1 \;\rightarrow\; a_2a_3$$

or graphically:

This reduction procedure reflects the marking process from Lemma 7 (only instead of marking literals we delete them from the cyclic word). Therefore, the reduction of a cyclic word w results in the cyclic word $\overline{w}$. Hence, the cyclically reduced form of a word w is equal (as a cyclic word) to the reduction of a cyclic word w.

Starting with a word w we can form the corresponding cyclic word defined by w and then cut it back into a (linear) word. The resulting word depends on the cutting point and might be different from the initial word w. To describe all words that can occur here we need the following definition.

Definition 5 *Let $w = y_1 \cdots y_m$ $(y_i \in A^{\pm 1})$ be a word in $A^{\pm 1}$. A cyclic permutation of w is a word of the form $y_{i+1} \cdots y_m y_1 \cdots y_i$ $(1 \leq i \leq n)$.*

Clearly, two cyclic words defined by $u, v \in F(A)$ are equal if and only if u is a cyclic permutation of v (and hence, v is a cyclic permutation of u). Observe also, if $v = y_{i+1} \ldots y_m y_1 \ldots y_i$ is a cyclic permutation of $w = y_1 \cdots y_m$ then

$$(y_1 \cdots y_i)^{-1}\ w\ (y_1 \ldots y_i) = v.$$

So any cyclic permutation of w is a conjugate of w. Summarizing the discussion above we have the following

Proposition 2 *Let u, v be elements of $F(A)$. The following conditions are equivalent:*

1) u and v are conjugate in $F(A)$;

2) The cyclic words defined by u and v are equal;

3) $\overline{u}$ is a cyclic permutation of $\overline{v}$.

Corollary 2 *The conjugacy problem in $F(A)$ is decidable.*

Proof. To check whether given two elements $u, v \in F(A)$ are conjugate in $F(A)$ or not it suffices to find their cyclically reduced forms $\overline{u}$ and $\overline{v}$, and check whether the cyclic words defined by $\overline{u}$ and $\overline{v}$ are equal or not. This can be done effectively.

□

Exercise 4 *What is the time complexity of the decision algorithm for the conjugacy problem in $F(A)$ indicated above?*

2.2 Solutions of the conjugacy equation $x^{-1}ux = v$

We have already seen in the previous section how one can effectively verify whether or not the equation

$$x^{-1}ux = v \tag{4}$$

has a solution in $F(A)$.

A similar method allows one to find a particular solution (if it exists) of this equation.

Indeed, suppose $x^{-1}ux = v$ for some $x \in F(A)$. Let

$$u = {u_1}^{-1} \circ \overline{u} \circ u_1, \quad v = {v_1}^{-1} \circ \overline{v} \circ v_1$$

be the cyclic decompositions of u and v. Then

$$x^{-1}{u_1}^{-1}\overline{u}u_1x = v^{-1}\overline{v}v_1$$

and

$$v_1x^{-1}{u_1}^{-1}\overline{u}u_1x{v_1}^{-1} = \overline{v}.$$

Hence $\overline{v}$ must be a cyclic permutation of $\overline{u}$ (otherwise, (4) has no solutions in $F(A)$). It follows that some initial segment of $\overline{u}$ (viewed as a word in generators $A^{\pm 1}$), say u_2, conjugates $\overline{u}$ into $\overline{v}$. Hence

$$v = v_1^{-1}u_2^{-1}\overline{u}u_2v_1$$

and the element $x = u_1^{-1}u_2v_1$ is a solution of the equation (4) (straightforward verification).

Clearly, there exists an effective algorithm to find a solution of the type $x = u_1^{-1}u_2v_1$ from above (check one by one all initial segments u_2 of the word $\overline{u}$).

Corollary 3 *The Conjugacy Search Problem is decidable in $F(A)$.*

Exercise 5 *What is the time complexity of the algorithm for solving the search conjugacy problem in $F(A)$ above?*

To describe all solutions of the equation (4) we rewrite it in the following form

$$[u, x] = g, \quad (here\ g = u^{-1}v). \tag{5}$$

This is a particular type of a *commutator equation* which we discuss in Section 1. Notice that if $x = b$ and $x = c$ are solutions of the equation 5 then $[u, b] = [u, c]$ which implies that $[u, cb^{-1}] = 1$. Hence, if b is a particular solution of (5), then all other solutions of (5) can be described as

$$x = yb,$$

where y is a solution of the homogeneous equation

$$[u, y] = 1. \tag{6}$$

We will see in Section 1.1 how to describe all solutions of this homogeneous equation.

Note. *Observe, that the description above reminds remotely the description of solution sets of liner systems of equations over an arbitrary ring or over an abelian group. Unfortunately, for equations over non-abelian groups, as we will see later, this situation is rather an exceptional one.*

3 Periodicity

3.1 Power equation $x^n = g$

For an element $g \in F(A)$ consider the *power equation*

$$x^n = g \ \ (n \in \mathbf{N}) \tag{7}$$

Lemma 5 *The power equation $x^n = g$ has at most one solution in $F(A)$.*

Proof. It follows immediately from the fact that free groups are torsion-free CT groups. However, it is very easy to see it directly. Indeed, $x^n = g$ has a unique solution if and only if $x^n = g^f$ has a unique solution for every (some) $f \in F$. Therefore, we may assume that g is cyclically reduced. In this case, a solution $x = u \in F$ is also cyclically reduced, hence u^n is reduced as written and equal to g. Thus, $n|u| = |g|$ and u is the initial segment of g of the length $|g|/n$, so uniquely defined.

Definition 6 *The Power Problem is decidable in a group G if there exists an algorithm which determines whether a power equation $x^n = g (g \in G, n \in N)$ has a solution in G or not.*

Lemma 6 *The Power Problem is decidable in a free group.*

Proof. Given a power equation $x^n = g$, $g \in F$. One can effectively find the cyclic decomposition of g:

$$g = g_1^{-1} \circ \bar{g} \circ g_1.$$

Notice that for any $u \in F$

$$u^n = g \Longleftrightarrow (g_1 u g_1^{-1})^n = \bar{g}.$$

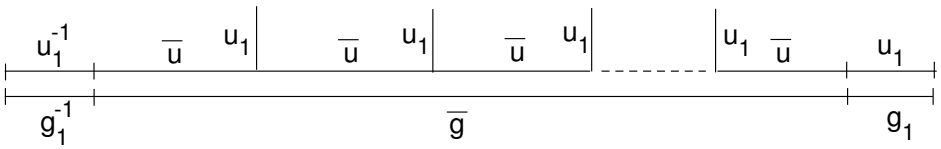
Hence, we may assume from the beginning that g is cyclically reduced. Then a solution u must be also cyclically reduced and as was mentioned above u is the initial segment of g of the length $|g|/n$. Thus to solve the equation $x^n = g$ one has only to take the initial segment u of G of length $|g|/n$ and check whether g is graphically equal to u^n or not.

□

Notice, that the argument above shows that for $n \geq |g|$ the equation $x^n = g$ has no solution in $F(A)$. Another remark is that if the power equation has a solution in $F(A)$, one can effectively find this solution in $O(|g|)$ steps. Notice, that there are finitely presented groups in which the power problem is undecidable.

The unique solution of the power equation $x^n = g$ is called the *n-th root* of g. The *maximal root* of g (or simply the *root*) is the n-th root of g with n maximal possible.

The following picture (a cancellation scheme) explains geometrically how to find a solution of a power equation $x^n = g$. If $x = u$ is a solution of this equation then we have the following cancellation scheme:



3.2 Periodic words

Let p be a cyclically reduced non-trivial word in $A^{\pm 1}$ which is not a proper power (we refer to such words as *periods*). A word is called *p-periodic* if it is a subword of p^n for some n.

Lemma 7 *Let p and q be two periods. If p^n and q^m have a common initial segment of length at least $|p| + |q|$ then $p = q$.*

Proof. If $|p| = |q|$ then the statement is obvious. Suppose $|p| \geq |q|$. Then we have the following diagram.

So $q_1 q_2 = q_2 q_1$ and $q = q_1 \circ q_2$. From the commutativity of q_1 and q_2 it follows that there exists w such that $q_1 = w^{n_1}$ and $q_1 = w^{n_2}$. Hence, $q = w^{n_1+n_2}$ and since $p = q^k q_1, k \geq 1$ then $p = w^{(n_1+n_2)k+n_1}$. Now, since p and q are periods then it follows that $p = w = q$.

□

Can one strengthen the result above by shortening the length of the common initial segment ?

Lemma 8 (Improved version) *Let p and q be two periods. If p^n and q^m have a common initial segment of length at least $|p| + |q| - \gcd(|p|, |q|)$ then $p = q$.*

Proof. If $|p| = |q|$ then the statement is obvious. Suppose $|p| \geq |q|$.

Case 1. Suppose $\gcd(|p|, |q|) = 1$. We are going to show that p and q are equal to a leter from $A^{\pm 1}$. It suffices to show that the first $|p| - 1$ letters in p are equal. Indeed, in this event q is a power of some letter from $A^{\pm 1}$ and it follows that $|q| = 1$. Thus, from the precondition of the lemma we have $|p| = 1$.

Let u be the common initial subword of p^n and q^m, and $u(i)$ be the i-th letter of u. From periodicity of u we have

$$u(i + |q|) = u(i),\ 1 \leq i \leq |p| - 1,$$

$$u(j + |p|) = u(j),\ 1 \leq j \leq |q| - 1.$$

Now suppose $1 \leq i, j \leq |p| - 1$ and

$$j = i + |q| \pmod{|p|}.$$

Then either $j = i + |q|$ or $j = i + |q| - |p|$, and in the latter case $j \leq |q| - 1$.

Hence, from the equalities above we have

$$u(j) = u(i + |q|) = u(i)$$

in the former case, and

$$u(j) = u(j + |p|) = u(i + |q|) = u(i)$$

in the latter one.

Now, observe that $|p|$ and $|q|$ are relatively prime, so $|q|$ generates $\mathbb{Z}_{|p|}$ and for every $1 \leq i, j \leq |p| - 1$ there is a number k such that $j = k|q| + i$. Thus $u(j) = u(i)$ for every $1 \leq i, j \leq |p| - 1$, as required.

Case 2. If $\gcd(|p|, |q|) = d > 1$ then

$$p = p_1 p_2 \cdots p_s,\ q = q_1 q_2 \cdots q_t,$$

where $|p_1| = |p_2| = \cdots = |p_t| = |q_1| = |q_2| = \cdots = |q_s| = d$. Viewing p_i, q_j as letters in a new alphabet one gets into the **Case 1**, so $p = p_1 = q$ and $|p| = |q|$.

□

Lemma 9 *Let $f, g \in F$ be non-proper powers. If f^n and g^m have a common initial segment of length at least $|f| + |g|$ then $f = g$.*

Proof. Suppose

$$f = a^{-1} \circ \bar{f} \circ a,\ g = b^{-1} \circ \bar{g} \circ b$$

are cyclic decompositions of f and g

We may assume that $|a| \geqslant |b|$, so $a = a_1 \circ b$.

a) $|a_1| \leqslant |\bar{g}|$

Since $|a_1| \leqslant |\bar{g}|$ then $\bar{g} = g_1 \circ g_2$, where $g_1 = a_1^{-1}$. It follows that $\bar{f}$ and $g_2 \circ g_1$ satisfy the conditions of Lemma 7 since $|\bar{f}| + |g_2 \circ g_1| \leqslant |f| + |g| - |b| - |a_1|$, and we have $\bar{f} = g_2 \circ g_1$. But then there is a cancellation between $\bar{f}$ and a_1 which is impossible unless $a_1 = g_1 = 1$. Hence, $\bar{f} = \bar{g},\ a = b$ and we are done.

b) $|a_1| > |\bar{g}|$

Then $a_1^{-1} = \bar{g}^k \circ a_2^{-1}$, where $|a_2| \leqslant |\bar{g}|$ and $k \in \mathbb{N}$. From a) it follows that $a_2 = 1,\ \bar{f} = \bar{g}$. But then there is a cancellation between $\bar{f}$ and $a_1 = \bar{g}^{-k}$ - contradiction unless $k = 0$. Thus, $\bar{f} = \bar{g},\ a = b$.

□

For elements $u, v \in F$ we define $c(u, v)$ as the length of the maximal common initial segment of u and v. Clearly, one can define $c(u, v)$ in terms of length:

$$c(u, v) = \frac{1}{2}(|u| + |v| - |v^{-1}u|).$$

Observe, that $c(u^{-1}, v)$ measures the cancellation in uv (i.e., the length of the maximal segment of u or v that cancels in uv).

Lemma 9 shows that if $f \neq g$ then $c(f^n, g^m) \leq |u| + |v|$.

3.3 Big powers in groups

In this section we discuss groups satisfying the so-called *big powers* condition. In this form it was introduced in [**?**] and studied in [**?**].

Let G be a group and $u = (u_1, ..., u_k)$ be a sequence of non-trivial elements of G. We say that:

1) u is in a *general position* if neighbors in u do not commute:

$$[u_i, u_{i+1}] \neq 1 \quad for\ every\ i = 1, ...k-1;$$

2) u is *independent* if there exists an integer n such that for any integers $\alpha_1, \ldots, \alpha_k \geq n$

$$u_1{}^{\alpha_1} ... u_k^{\alpha_k} \neq 1.$$

Sometimes we refer to a sequence in a general position as to a *generic* sequence, or a *commutation-free* sequence. The positive integer n from 2) (if it exists) is called a *separation boundary* for u.

Definition 7 *A group G satisfies the* big powers condition *(BP) if any sequence of elements of G in a general position is independent. Such groups are called* BP-groups.

It is clear that (BP) is a *local* property, i.e., a group G satisfies (BP) if and only if every finitely generated subgroup of G does. Since a single non-trivial element forms a generic sequence it implies that every BP-group is torsion-free.

Theorem 2 *A free group F is a BP group.*

Proof. Follows from Lemma 9 (exercise).

The class of BP-groups is quite broad. Every torsion-free abelian group satisfies (BP) since one-element sequences are the only generic ones in abelian groups. Any torsion-free hyperbolic group, or any subgroup of it, is a BP-group. To describe some other examples of BP-groups recall that a group G *discriminates* a group H if for any finite set of nontrivial elements $h_1, \ldots, h_k \in H$ there exists a homomorphism $\phi : H \to G$ such that $h_i^{\phi} \neq 1$ for $i = 1, \ldots, k$. It is not hard to see that any group discriminated by a BP-group is a BP-group [**?**], in particular, fully residually free groups are BP-groups. We refer to [**?**] for a detailed discussion of BP-groups.

4 Recognition Problem

4.1 Verbal structure of elements. Recognition problem

4.2 Verbal subgroups: genus and width

4.3 Recognition of commutators. Wicks' theorem

Let G be a group and g be an element of G. The equation

$$[x, y] = g$$

has a solution in G if and only if g is a commutator in G. It follows that the Diophantine problem is decidable for the class of commutator equations

$$\{[x, y] = g | g \in G\}$$

if and only if there exists an effective procedure for recognizing commutators in G.

The following result shows that there exists an algorithm for recognizing commutators in free groups.

Theorem 3 *(Wicks'). Let F be a free group, g an element in F, and $\bar{g}$ the cyclically reduced form of g. Then g is a commutator in F if and only if some cyclic permutation of $\bar{g}$ is of the form*

$$a \circ b \circ c \circ a^{-1} \circ b^{-1} \circ c^{-1} \tag{8}$$

for some $a, b, c \in F$.

$\triangleright$ Notice first, that since g and $\bar{g}$ are conjugated then if one of them is a commutator, then the other one also does. So we may assume from the beginning that g is cyclically reduced, i.e., $g = \bar{g}$.

Observe now, that for any group G and any elements $a, b, c \in G$ one has

$$abca^{-1}b^{-1}c^{-1} = (ab)(ca^{-1})(ab)^{-1}(ca^{-1})^{-1}$$

so the element $abca^{-1}b^{-1}c^{-1}$ is always a commutator. This proves the "if" part of the theorem.

Now suppose g is a commutator. Obviously, every commutator $u^{-1}v^{-1}uv$ can be presented as a product $abca^{-1}b^{-1}c^{-1}$ (say $a = u^{-1}, b = v^{-1}, c = 1$), but there may be some cancellation in there. The point is to find such a presentation without cancellation.

Let

$$g' = abca^{-1}b^{-1}c^{-1} \tag{9}$$

be a presentation of some cyclic permutation g' of g with the minimal total length $|a| + |b| + |c|$ among all such presentations. We claim, that in this event there is no cancellation in the product $abca^{-1}b^{-1}c^{-1}$. To prove this it suffices to consider all possible cases where cancellation may occur in (9).

Suppose, for example, that $b = b_1 \circ y, c = y^{-1} \circ c_1$. Then

$$abca^{-1}b^{-1}c^{-1} = ab_1c_1a^{-1}y^{-1}{b_1}^{-1}{c_1}^{-1}y.$$

Conjugating by a, we obtain the following cyclic permutation of g' (hence of g):

$$b_1c_1a^{-1}y^{-1}{b_1}^{-1}{c_1}^{-1}ya = b_1c_1(a^{-1}y^{-1})b_1^{-1}c_1^{-1}(a^{-1}y^{-1})^{-1}$$

with a shorter total length of representatives $|b_1|+|c_1|+|a|+|y| < |a|+|b|+|c|$ - contradiction. A similar argument shows that cancellation does not occur in all other places, which proves the theorem.

□

Corollary 4 *Commutators are effectively recognizable in free groups.*

Proof. Indeed, let g be an element of a free group F. We can effectively find the cyclically form $\bar{g}$ of g. If $|\bar{g}|$ is of odd length, then $\bar{g}$ (as well as g) is not a commutator. If $|\bar{g}|$ is of even length, then we can take the left half of $\bar{g}$ and partition in into all possible products of the type $a \circ b \circ c$.

Now for every such partition abc we check whether the right half of $\bar{g}$ is equal to $a^{-1}b^{-1}c^{-1}$ or not. If yes, then g is a commutator, if not, then we take one by one all cyclic permutations of $\bar{g}$ and repeat the process for each of them. □

Exercise 6 *What is the complexity of the algorithm to recognize commutators in $F(A)$ described above?*

Exercise 7 *Let $u, v \in F(A)$ and $[u, v] \neq 1$. Then equation*

$$[u, v] = x^n$$

has a solution if and only if $n = \pm 1$.

5 Description of solutions of the equation $[x, y] = g$

In this section we describe all solutions of the equation

$$[x, y] = g$$

in a free group $F = F(A)$. This equation was studied first by A.Malcev, since then it is called sometimes the Malcev's equation.

Malcev's description of solutions is very instructive, it illustrates the main ideas and gives and gives a method to describe solution sets of arbitrary quadratic equations over free groups.

5.0.1 Elementary transformations

The following lemma shows how one can obtain infinitely many solutions of the equation $[x, y] = g$ from a given particular solution $x = u, y = v$.

Lemma 10 *Let (u, v) be a solution of an equation*

$$[x, y] = g.$$

Then pairs

$$(v^m u, v) \text{ and } (u, u^m v), m \in \mathbf{Z}$$

are also solutions of this equation.

$\triangleright$. This follows immediately from the following identities:

$$[v^m u, v] = [v^m, v]^u [u, v] = [u, v] = g;$$

$$[u, u^m v] = [u, v][u, u^m]^v = [u, v] = g.$$

So starting from a solution (u, v) we can generate infinitely many other solutions:

$$(u, v) \to (v^{m_1} u, v) \to (v^{m_1} u, (v^{m_1} u)^{m_2} v) \to (((v^{m_1} u)^{m_2} v)^{m_3}, (v^{m_1} u)^{m_2} v) \to \dots$$

Now we introduce the following elementary transformations on pairs of elements from F:

$$U : (u, v) \to (vu, v)$$

$$V : (u, v) \to (u, uv).$$

Clearly, this transformation U, V has inverses

$$U^{-1} : (u, v) \to (v^{-1}u, v)$$

$$V^{-1} : (u, v) \to (u, u^{-1}v).$$

By U^m, V^m we denote the product of the m consequent transformation of the type U, V correspondingly.

We will say that two pairs (u_1, v_1) and (u_2, v_2) are equivalent ($(u_1, v_1) \sim (u_2, v_2)$) if one can transform (u_1, v_1) into (u_2, v_2) by a finite chain of elementary transformations. Clearly, $\sim$ is an equivalence relation on pairs

By Lemma 10 if (u, v) is a solution of $[x, y] = g$, then the equivalence class $[(u, v)]$ provides infinitely many other solutions of this equation. It follows that the solution set $V([x, y] = g)$ of the equation is a union of equivalence classes:

$$V([x, y] = g) = \cup_{i \in I}[(u_1, v_i)].$$

One may view the transformations U, V as automorphisms of the free group $F(x, y)$ which fix the commutator $[x, y]$. Indeed, let ϕ and ψ be automorphisms of $F(x, y$ defined by

$$\phi_U : x \to yx, y \to y, a \to a(a \in A),$$

$$\phi_V : x \to x, y \to xy, a \to a(a \in A).$$

Then ϕ_U and ϕ_V are (Nielsen) automorphisms of $F(x, y)$ and

$$\phi_U([x, y]) = [x, y], \phi_V([x, y]) = [x, y].$$

If we denote by $A_{U,V}$ the subgroup of $Aut(F(x, y))$ generated by ϕ_U and ϕ_V then $A_{U,V}$ induces a group of automorphism of the group $G = F[x, y]/[x, y] = g$ which fix the constants from A. Therefore, if

$$\psi : x \to u, y \to v$$

is a solution of $[x, y] = g$ in $F(A)$ then for any automorphism $\phi \in A_{U,V}$ $\psi\phi : G \to F(A)$ is also a solution of the equation.

5.1 Minimal solutions

Our goal now is to prove that one can effectively find a finite collection of solutions $(u_1, v_1), \ldots, (u_n, v_n)$ such that

$$V([x, y] = g) = [(u_1, v_1)] \cup \cdots \cup [(u_n, v_n)].$$

To this end we need the following

Definition 8 *A solution (u, v) of the equation $[x, y] = g$ is called minimal if it has the minimal total length $|u| + |v|$ among all solutions in its equivalence class $[(u, v)]$.*

Lemma 11 *Let (u, v) be a minimal solution of the equation $[x, y] = g$. Then in each of the products*

$$uv, v^{-1}u, u^{-1}v^{-1}$$

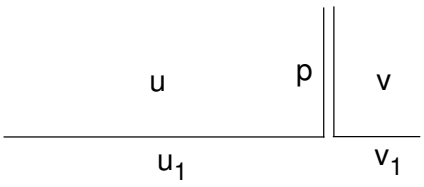
the total cancellation can not be greater than $\min\left\{\frac{|u|}{2}, \frac{|v|}{2}\right\}$

Proof. Observe, that for arbitrary $u, v \in F(A)$ the following conditions are equivalent:

1) more than half of v cancels out in uv;

2) $|uv| < |u|$

This can be seen from the corresponding cancellation scheme:



Indeed,

$$|uv| = |u_1| + |v_1| < |u| \Leftrightarrow |v_1| < |p|.$$

Now, let (u, v) be a minimal pair.

Case 1. Consider the product uv.

Suppose, that more than half of v cancels out in uv. Then $|uv| < |u|$. In this case

$$(u, v) \sim (u, uv) \sim (v^{-1}, uv)$$

and $|v^{-1}| + |uv| = |v| + |uv| < |v| + |u|$ - contradiction with the minimality of (u, v).

Suppose, that more then half of u cancels out in uv. Then $|uv| < |v|$ and the equivalence

$$(u, v) \sim (u, uv)$$

shows that (u, v) is not minimal ($|u| + |uv| < |u| + |v|$).

Case 2. Suppose more than half of u cancels out in the product $v^{-1}u$. Then $|v^{-1}| < |v^{-1}| = |v|$. In this case

$$(u, v) \sim (u, uv)$$

and $|u| + |uv| < |u| + |v|$ - contradiction.

Suppose that more than half of v cancels out in $v^{-1}u$. Then

$$|v^{-1}u| = |u|.$$

Hence,

$$(u, v) \sim (v^{-1}u, v)$$

and $|v^{-1}u| + |v| < |u| + |v|$ - contradiction.

Case 3. $u^{-1}v^{-1}$.

If more than half of u^{-1} cancels out in $u^{-1}v^{-1}$, then $|u^{-1}v^{-1}| = |vu| < |v|$. Hence

$$(u, v) \sim (vu, v) \sim (vu, u^{-1})$$

and $|vu| + |u^{-1}| < |v| + |u|$ contradiction. If more than half of v^{-1} cancels out in $u^{-1}v^{-1}$ then $|u^{-1}v^{-1}| < |u^{-1}| = |u|$. Now

$$(u, v) \sim (vu, v)$$

and $|vu| + |v| = |u^{-1}v^{-1}| + |v|$ - contradiction.

Actually, it suffices to consider just the first case, the two others are similar.

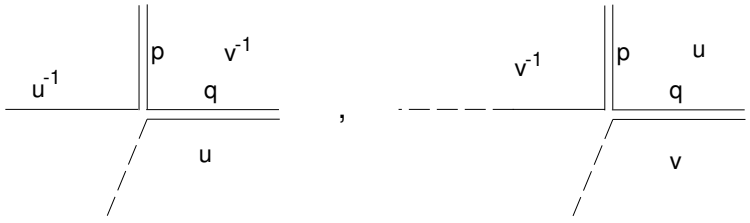
Corollary 5 *Let (u, v) be a minimal solution of the equation $[x, y] = g$ ($g \neq 1$). Then at least one literal from each of the factors u^{-1}, v^{-1}, u, v occurs in the reduced form of $u^{-1}v^{-1}uv$.*

$\triangleright$. By the lemma above at most half of each factor can cancel out in the products $u^{-1}v^{-1}, v^{-1}u, uv$. Hence if u has odd length, then the literal in the middle of u does not cancel out in the product $v^{-1}uv$. Similarly, if v^{-1} is of odd length, then it does not cancel completely in $u^{-1}v^{-1}u$.

Suppose now that u is of even length, $u = pq, |p| = |q|$. If u cancels out completely in $v^{-1}uv$, then $p = q^{-1}$ and $u = 1$. This implies $g = 1$-contradiction. Hence u does not cancel completely in $v^{-1}uv$, as well as v^{-1} in $u^{-1}v^{-1}u$.

It follows that reducing v^{-1} in $u^{-1}v^{-1}uv$ we do not have cancellation schemes of the types:

Hence, neither of the factors u^{-1}, v^{-1}, u, v cancels out completely in $u^{-1}v^{-1}uv$.

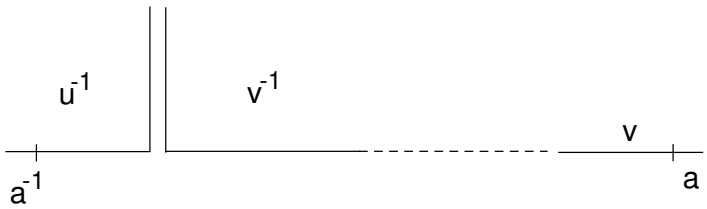


Lemma 12 *If (u, v) is a minimal solution of the equation $[x, y] = g(g \neq 1)$ then $|u| + |v| \leq |g|$.*

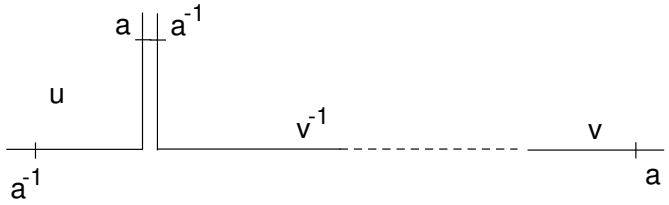
$\triangleright$. Suppose g is not cyclically reduced, say $g = a^{-1} \circ g_1 \circ a$. If we do not have pinches in a cancellation scheme for

$$u^{-1}v^{-1}uv,$$

then $|u^{-1}| + |v^{-1}| + |u| + |v| = |g|$ and the conclusion of the lemma holds. Suppose we have at least one pinch in the cancellation scheme for $u^{-1}v^{-1}uv$; say the scheme is of the type:



then we can see that we have:



hence $u = a^{-1} \circ u_1 \circ a, v = v_1 \circ a, g = {g_1}^a$.

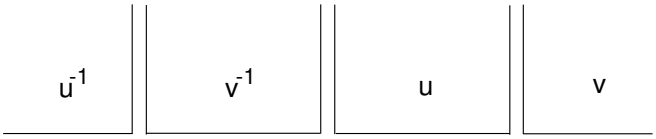
Now, $[u_1, av_1] = g_1$ and (u_1, av_1) is a minimal solution of the equation $[x, y] = g_1$. By induction on $|g|$ we have

$$|u_1| + |av_1| \leq |g_1|$$

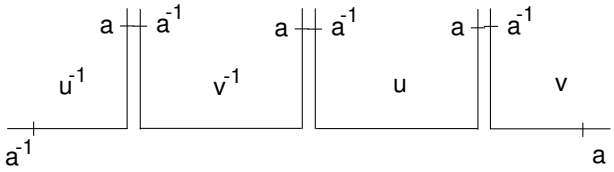
hence

$$|u| + |v| = |a^{-1} \circ u_1 \circ a| + |v_1 \circ a| \leq |a^{-1} \circ g_1 \circ a| = |g|.$$

Suppose now, that g is cyclically reduced. Then there is no cancellation scheme with all three non-trivial pinches:

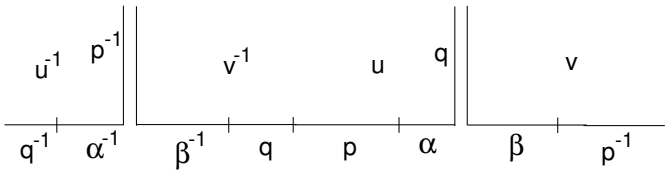


Indeed, in this event we have



So $u = a^{-1} \circ u_1 \circ a, v = a^{-1} \circ v_1 \circ a$, and hence g is not cyclically reduced-contradiction. It implies, that we have to consider the schemes of the following type (with at least one trivial pinch):

Assume, $|p| \geq |q|$. Then we have the following scheme:



where $u = p\alpha q, v = q^{-1}\beta p^{-1}$. Hence

$$q^{-1}\alpha^{-1}\beta^{-1}qp\alpha\beta p^{-1} = g \tag{10}$$

Hence

$$|u| + |v| = |p| + |\alpha| + |q| + |q| + |\beta| + |p| \leq |g|.$$

Remark 1 *Notice, that from (10) we have*

$$q^{-1}\alpha^{-1}\beta^{-1}qp\alpha\beta p^{-1} = g.$$

Hence the cyclic permutation of g:

$$\alpha^{-1}\beta^{-1}(qp)\alpha\beta(p^{-1}q^{-1})$$

is the Wicks' form of the type

$$a \circ b \circ c \circ a^{-1} \circ b^{-1} \circ c^{-1}.$$

It shows that Wicks' forms for the cyclic word g come from the minimal solutions of $[x, y] = g$.

Corollary 6 *Let $g \in F(A)$ and $g \neq 1$. Then there are only finitely many minimal solutions of the commutator equation*

$$[x, y] = g.$$

If $(u_1, v_1), \ldots, (u_n, v_n)$ are minimal solutions of the equation above, then the solution set of this equation is a finite union of the equivalence classes:

$$[(u_1, v_1)] \cup \cdots \cup [(u_n, v_n)].$$

Moreover, one can effectively find the set of minimal solutions $(u_1, v_1), \cdots, (u_n, v_n)$.

Corollary 7 *Let $F = F(a, b, \ldots)$. Then the solution set of the equation $[x, y] = [a, b]$ is equal to the equivalence class $[(a, b)]$, and (a, b) is the only minimal solution of this equation.*

$\triangleright$. Indeed, if (u, v) is a minimal solution of $[x, y] = [a, b]$, then $|u|+|v| \leq 4$. If $|u| = 1$, then $|v| = 1$ (since in this case u does not cancel in $[u, v]$). In this event $u = 1, v = b$. If $|u| = 2 = |v|$, then

$$u^{-1} = a^{-1}p^{-1}, v^{-1} = pc$$

(since $[a, b]$ begins with a^{-1}) , and also $v = c^{-1}p^{-1}$ has to end on b. It follows $p = b^{-1}$, and substituting into $[u, v]$ we see that $[u, v] \neq [a, b]$. So the case $|u| = |v| = 2$ is not possible.

$\square$

We described completely the solution set of the equation $[x, y] = g$.

Digression

It turns out that the methods we discussed here can be generalized into much more general situations. In fact, they are some of the most powerful methods in the theory of free groups. The transformations U, V are particular types of so-called Nielsen elementary transformations, the idea of minimal pairs gives rise to the notation of N-reduced sets, Wicks' forms exists for an arbitrary quadratic equation over free groups and the idea of estimation of the length of a minimal solution of an equation in terms of length of its coefficients is the principal one in Makanin's solution of the Diophantine problem over free groups