SOLVING EQUATIONS IN FREE NILPOTENT GROUPS

by

Michael H. Albert
Department of Mathematics
Carnegie Mellon University
Pittsburgh, PA 15213

and

John Lawrence
Department of Pure Mathematics
University of Waterloo
Waterloo Ontario N2L 3G1 Canada

Research Report No. 91-125 2

July 1991

Solving equations in free nilpotent groups

Michael H. Albert
Department of Mathematics
Carnegie Mellon University
Pittsburgh PA 15213, USA

John Lawrence
Department of Pure Mathematics
University of Waterloo
Waterloo Ontario N2L 3G1 Canada

June 11, 1991

Abstract

In this paper we show that any system of equations over a free nilpotent group of class c is either ***unitary*** or ***nullary***. In fact, such a system either has a most general solution (akin to the most general solution of a system of linear diophantine equations), or every solution has a proper generalization. In principle we provide an algorithm for determining whether or not a most general solution exists, and exhibiting it if it does. This requires solving a system of linear diophantine equations for approximately $c\binom{k}{c}$ different right hand sides, where k is the number of parameters which occur in a most general solution of the system in the variety of abelian groups.

1 Introduction

The process of solving equations is central to much of algebra. In a general setting, there are two questions to answer when presented with an equation: "Does a solution exist?", and "If so, what is the most general form of a solution?". In this paper we address these questions in the context of nilpotent groups. Before we begin, a discussion of the exact meaning of the second question is in order.

We work in a variety V (of groups – though the following remarks can be applied in a more general context.) A system Σ of equations in the variables

$\mathbf{x} = x_1, x_2, \ldots, x_n$ is a finite set of elements of the form:

$$t(\mathbf{x}) = 1$$

where t is a term in the language of groups, and 1 denotes the identity element. A *solution* of Σ in a group $G \in V$ is a sequence of elements $\mathbf{a} = a_1, a_2, \ldots, a_n$ from G such that $t(\mathbf{a}) = 1_G$ for each element of Σ. Another way to put this is that if $F_V(\mathbf{x})$ is the relatively free group in V with generators $\mathbf{x}$, then a solution of Σ is a homomorphism τ from $F_V(\mathbf{x})$ to G whose kernel contains each of the terms t which appear on the left hand side of the equations in Σ. The group in which we search for solutions will be the countably generated relatively free group of V – which we will denote F_ω.

Given two solutions τ_1 and τ_2 of Σ we say that τ_1 is *at least as general as* τ_2, and write $\tau_1 \leq \tau_2$ if there is an endomorphism $\alpha : F_\omega \longrightarrow F_\omega$ such that $\alpha\tau_1 = \tau_2$. Clearly $\leq$ is a transitive and reflexive relation, however it need not be anti-symmetric. There is a naturally associated equivalence relation $\sim$ defined by:

$$\sigma \sim \tau \quad \Longleftrightarrow \quad \sigma \leq \tau \text{ and } \tau \leq \sigma.$$

and a partial order on equivalence classes of this relation which is induced by $\leq$.

This definition of generalization is one which has been arrived at in the study of resolution methods of theorem proving, and term rewriting systems (where "solving equations" goes by the name of "unification"). It corresponds to the natural understanding of generalization as the following simple example illustrates:

Consider the single equation

$$2x + 3y + 6z = 0$$

in the variety of abelian groups. One solution is given by:

$$x = 0, y = 2a, z = -a$$

for any generator a of the free abelian group. Another solution is given by:

$$x = 3b, y = -b + 2c, z = -c,$$

for generators b and c. It is clear that the second solutions is more general than the first, and this is witnessed by any endomorphism which maps b to 0 and c to a. In fact the second solution is a *most general solution* to the equation: it is at least as general as any solution to the equation (for any other solution $x = s, y = t, z = u$, an endomorphism which sends c to $-u$ and b to $-t - 2u$ establishes this.) In fact, any system of equations in the variety of abelian groups has such a most general solution – which amounts to a general solution of the same system viewed as homogeneous linear diophantine equations. Simple Gaussian elimination (avoiding fractions) can be used to find such solutions but may lead to a "blow up" in the size of coefficients at intermediate points in the calculation. This problem can be avoided and polynomial time algorithms for solving such systems are known, see for example [2] and [1].

The generalization relation need not always behave so nicely. For example consider the equation:

$$xyx^{-1}y^{-1} = 1$$

in the variety of all groups. It is known that all solutions to this equation in a free group are of the form:

$$x = t^n, y = t^m$$

for some t and integers n and m. Any solution is generalized by one in which t is a generator and n and m are relatively prime. Among these more general solutions none has any strict generalization, but any two such solutions which differ in the exponents (by anything other than a sign change) are incomparable. Therefore, this single equation has an infinite set of most general solutions. In the variety of all groups it can be shown using the Nielsen-Schreier theorem, and the fact that free groups are Hopfian, that any system of equations has a set of most general solutions. At this time we do not know of any such system which has more than one, but only finitely many most general solutions (up to equivalence under automorphisms of the free group.)

Let us make our terminology a little more precise. A *most general solution* σ of Σ is one which has no proper generalization (i.e. if $\tau \leq \sigma$ then $\sigma \leq \tau$). We say that Σ is *unitary* if there is a single most general solution which generalizes every solution (this solution need not be unique); *finitary* if there are finitely many most general solutions, such that every solution is generalized by at least one of them; *infinitary* if there is an infinite family of most general solutions of this type; and nullary if none of the preceding cases occurs, which means that there is at least one solution which is not generalized by any most general solution. In terms of the partial order obtained from $\leq$ above, Σ is unitary if the order has a smallest element, finitary (infinitary) if the set of minimal elements is finite (infinite) and every element lies above a minimal element, and nullary if there is some element which does not lie above a minimal element.

We will see that for each $c > 1$ every system of equations in the variety of all nilpotent groups of class c is either unitary or nullary. In fact, if a system is nullary, then we will prove that every solution has a strict generalization. The proof will implicitly specify an algorithm which either finds the most general solution to a system of equations, or establishes that no such solution exists, and the main part of this algorithm involves solving the same system of linear diophantine equations (with differing right hand sides) roughly $c\binom{k}{c}$ times – hence the algorithm can be made polynomial, and in fact quite practical, at least for small values of c.

We hope that this paper will be accessible to a wide audience, and so we have attempted to make it as self-contained as possible. In particular section 2.1 contains a great deal of basic material. There is no doubt that an acquaintance with the material on nilpotent groups which can be found in [4] would be of more than a little value. The results and definitions which we require from this reference are collected at the beginning of the next section.

2 Results

2.1 Preliminaries

The language of groups contains symbols for multiplication, inverse, and the identity element (which we denote 1). To this language we add the commutator bracket:

$$[a,b]=a^{-1}b^{-1}ab$$

and the "left-normed commutators of weight $c+1$" defined inductively by:

$$[x_1,x_2,\ldots,x_{c+1}]=[[x_1,x_2,\ldots,x_c],x_{c+1}].$$

A group G is said to be nilpotent of class c ($c\geq 1$) if for all $g_1,g_2,\ldots,g_{c+1}\in G$,

$$[g_1,g_2,\ldots,g_{c+1}]=1.$$

So the groups which are nilpotent of class 1 are just abelian groups.

For any c, the nilpotent groups of class c form a *variety of groups* denoted $\mathcal{N}_c$, i.e. a class of groups closed under the formation of subgroups, quotient groups, and Cartesian products. In $\mathcal{N}_c$ (more generally in any variety), there exists, for every set X, a free group $F(X)$ generated by X, with the following universal mapping property:

> for every $G\in\mathcal{N}_c$ and every function $f:X\longrightarrow G$ there is a group homomorphism $f:F(X)\longrightarrow G$ which extends f.

Given a free group F in a variety, any subset X of F which generates F and has the above universal mapping property is referred to as a free generating set of F.

When we speak of "the" free group in a variety we will mean a countably generated free group on an unspecified generating set (from which we will occasionally pull elements).

The center of a free group of $\mathcal{N}_c$ is the group generated by all left normed commutators of weight c. This group is free abelian, and if the generating set is linearly ordered, has a basis consisting of all the left normed weight c commutators of generators, where the generators occur in strictly increasing order in the commutator. By "general nonsense" the quotient of a free group of $\mathcal{N}_c$ by its commutator subgroup is also a free abelian group, generated by the images of the generators of the original group (generally, the quotient by the dth term of the descending central series will be a free group in $\mathcal{N}_d$.)

The following specializes Theorem 42.31 of [4] to the situation at hand.

Proposition 1 *Let A be a subset of a free group F in $\mathcal{N}_c$. If the image of A under the natural homomorphism from F to F/F' is independent and generates a direct factor of F/F' then A can be extended to a free generating set of F.*

Finally we need the following fact, related to results of J. Lawrence in [3] whose proof we defer until section 2.4

Lemma 2 *Let F be the free group in $\mathcal{N}_c$, let r be a positive integer, and let p be a prime which is not a divisor of r. Then for all positive integers k there exists a positive integer $\phi(k)$ such that, for any $M > \phi(k)$, and any subset $\{u_{ij} : 1 \leq i \leq M, 1 \leq j \leq c\}$ of cM distinct elements of a free generating set the equation:*

$$z^p \prod_{j=1}^{k}[x_j, y_j] = (\prod_{i=1}^{M}[u_{i1}, u_{i2}, \ldots, u_{ic}])^r$$

has no solution in F.

We begin the proof of our general result with a consideration of the class 2 case. Although formally there is no difference between this case, and the induction step of the general proof, the technical details are somewhat less inhibiting, and the general idea of the proof is illustrated much more clearly.

2.2 Nilpotent class 2 groups

This section is devoted to proving the following theorem, followed by some examples of its application.

Theorem 3 *In the variety of nilpotent groups of class 2 every finite system of equations is either unitary or nullary. If a system is nullary then every solution has a proper generalization.*

In a free nilpotent group of class 2 every element can be written as a product of powers of distinct generators times a product of commutators. So, modulo the laws of this variety, we may assume that each equation in our system has the general form:

$$x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n} C = 1 \tag{1}$$

where

$$C = \prod_{i<j} [x_i, x_j]^{m_{ij}}$$

plays no visibly significant rôle in the rest of the proof.

We consider the same system of equations in the free abelian group. As all commutators are the identity here, only the powers of generators are important. As is traditional we rewrite the system additively, and in matrix form as:

$$M\mathbf{x} = 0 \tag{2}$$

Since the variety of abelian groups is unitary, equation (2) has a most general solution:

$$x_i = w_i(\mathbf{y}) \quad 1 \leq i \leq n \quad \mathbf{y} = y_1, y_2, \ldots, y_k.$$

which can be chosen in such a way that there are terms $t_j(\mathbf{x})$ so that for any solution $\mathbf{a}$ of equation (2), if we set:

$$b_j = t_j(\mathbf{a}) \quad 1 \leq j \leq k$$

then

$$a_i = w_i(\mathbf{b}) \quad 1 \leq i \leq n.$$

It follows that if $\mathbf{a}$ is a solution to the original equation (1), then for $b_j = t_j(\mathbf{a})$ and certain elements $P_1, P_2, \ldots, P_n$ of the commutator subgroup

$$a_i = w_i(\mathbf{b}) P_i.$$

Substituting in the original equations, using the fact that all commutators are central, and that

$$[xy, z] = [x, z][y, z]$$

in a nilpotent class 2 group, we obtain a system of equations of the form:

$$P_1^{m_1} P_2^{m_2} \ldots P_n^{m_n} = \prod_{i<j} [b_i, b_j]^{n_{ij}} \tag{3}$$

for certain integers n_{ij} which depend only on (1), and not on the particular solution chosen. Conversely, given any $\mathbf{b}$ and elements $P_1, P_2, \ldots, P_n$ of the commutator subgroup which satisfy (3), the elements $a_i = w_i(\mathbf{b}) P_i$ satisfy (1).

We can now state the criterion which determines whether or not (1) is unitary.

Claim: If each system of linear diophantine equations:

$$M\mathbf{x} = \mathbf{n}_{ij} \quad 1 \leq i < j \leq k \tag{4}$$

has a solution then (1) is unitary. Otherwise it is nullary and every solution has a proper generalization.

Notice that we have $\binom{k}{2}$ systems of linear diophantine equations above, one for each pair of parameters b_i, b_j.

We now prove the claim above. First suppose that each of the systems (4) has a solution. Let $u_1, u_2, \ldots, u_k$ be a subset of the free generators of the free group in $\mathcal{N}_2$. Then because the systems (4) have solutions, we can find a solution of (3) in which each P is written as a product of commutators of the form $[u_i, u_j]$ $(1 \leq i < j \leq k)$. Take such a solution and consider the solution:

$$\tau : \begin{array}{rcl} x_1 & = & w_1(\mathbf{u})P_1(\mathbf{u}) \\ x_2 & = & w_2(\mathbf{u})P_2(\mathbf{u}) \\ & \vdots & \\ x_n & = & w_n(\mathbf{u})P_n(\mathbf{u}) \end{array} \tag{5}$$

of (1) which arises from it. Then this is a most general solution of (1).

To see this, consider any solution $\mathbf{a}$ of (1). As noted before the claim, there exist elements $\mathbf{b}$ and elements of the commutator subgroup $P'_1, P'_2, \ldots, P'_n$ such that:

$$\begin{array}{rcl} a_1 & = & w_1(\mathbf{b})P_1' \\ a_2 & = & w_2(\mathbf{b})P_2' \\ & \vdots & \\ a_n & = & w_n(\mathbf{b})P_n' \end{array}$$

The substitution which sends each u_j to b_j does not necessarily send $P_i(\mathbf{u})$ to P_i'. However, it does yield a solution $\mathbf{c}$ with the property that:

$$a_i = c_i Q_i \quad (1 \leq i \leq n)$$

and

$$Q_1^{m_1} Q_2^{m_2} \cdots Q_n^{m_n} = 1$$

for some $Q_1, Q_2, \ldots, Q_n$ in the commutator subgroup. Since the most general solution of (2) is in fact a most general solution in any torsion free abelian group, there exist $\hat{Q}_1, \hat{Q}_2, \ldots, \hat{Q}_k$ in the commutator subgroup such that:

$$Q_i = w_i(\hat{Q}_1, \hat{Q}_2, \ldots, \hat{Q}_k) \quad (1 \leq i \leq n).$$

Therefore, the substitution which sends u_j to $b_j \hat{Q}_j$ sends

$$w_i(\mathbf{u})P_i(\mathbf{u})$$

to

$$w_i(\mathbf{b})w_i(\hat{Q}_1, \hat{Q}_2, \ldots, \hat{Q}_k)P_i(\mathbf{b}) = w_i(\mathbf{b})P_i(\mathbf{b})Q_i = a_i$$

where to obtain the first result we use the fact that $[b_i\hat{Q}_i, b_j\hat{Q}_j] = [b_i, b_j]$ since the $\hat{Q}$ belong to the commutator subgroup. Thus τ is as general as any other solution, and so the equation (1) is unitary in this case.

Now consider the case where one of the linear diophantine systems in (4) does not have a solution. Without loss of generality suppose that it is the system with $i = 1$ and $j = 2$. This means that some integer linear combination of the rows of M has a prime factor q which is not a factor of the corresponding combination of the elements of and $\mathbf{n}_{12}$. We obtain a corresponding equation of the form:

$$(P_1^{m'_1} P_2^{m'_2} \ldots P_n^{m'_n})^q = [u_1, u_2]^{n'} \prod_{(i,j)\neq(1,2)} [u_i, u_j]^{n'_{ij}} \tag{6}$$

where q is not a divisor of n'.

Let $\mathbf{a}$ be any solution of (1), and let $b_j = t_j(\mathbf{a})$. So we have:

$$a_i = w_i(\mathbf{b})P'_i \quad (1 \leq i \leq n) \tag{7}$$

for some elements $P'_1, P'_2, \ldots, P'_n$ of the commutator subgroup. Also, from the above, there is a relationship of the form:

$$(P_1^{m'_1} P_2^{m'_2} \cdots P_n^{m'_n})^q = [b_1, b_2]^{n'} \prod_{(i,j)\neq(1,2)} [b_i, b_j]^{n'_{ij}} \tag{8}$$

where q is a prime which is not a divisor of n'.

It follows that $\mathbf{b}$ cannot be a subset of a generating set of the free nilpotent group of class 2, since the commutator subgroup of such a group is free abelian with generators $[b_i, b_j]$ among others, and hence the right hand side of (8) could not be a q^{th} power. By 1 this implies that the images $\bar{\mathbf{b}}$ of $\mathbf{b}$ modulo the commutator subgroup do not generate a direct factor of the free abelian group. So without loss of generality, there is a prime q, and a positive integer r which is not a multiple of q such that:

$$\bar{b}_1^r = \bar{b}_2^{\lambda_2} \bar{b}_3^{\lambda_3} \cdots \bar{b}_k^{\lambda_k} \bar{D}^q.$$

for some integers $\lambda_2, \lambda_3, \ldots, \lambda_k$, and some $D \in F$. Hence:

$$b_1^r = b_2^{\lambda_2} b_3^{\lambda_3} \cdots b_k^{\lambda_k} D^q C.$$

for some C in the commutator subgroup, and some $D \in F$. Let $u_1, u_2, \ldots$ be a sequence of generators which do not appear in any b_j or P' (from (7)), nor in

C or D. Let:

$$\begin{aligned} c_1 &= b_1 \prod_{s=1}^{M} [u_{2s}, u_{2s+1}] \\ c_j &= b_j \quad (2 \leq j \leq k) \end{aligned}$$

and consider the solution:

$$a'_i = w_i(\mathbf{c}) P'_i$$

of (1). This is a solution, because in general if we multiply the elements of **b** by elements of the commutator subgroup then the right hand side of (3) is unchanged, so no change is required in $P'_1, P'_2, \ldots, P'_n$.

The solution $\mathbf{a}'$ is at least as general as $\mathbf{a}$ because the homomorphism which sends each of the $u_1, u_2, \ldots$ to 1 and leaves the remaining generators unaffected sends $\mathbf{a}'$ to $\mathbf{a}$. On the other hand, suppose that there existed a homomorphism τ which sent $\mathbf{a}$ to $\mathbf{a}'$. Then, as $b_j = t_j(\mathbf{a})$ and $c_j = t_j(\mathbf{a}')$ (which follows from a direct computation using the fact that $\prod_{s=1}^{M} [u_{2s}, u_{2s+1}]$ is central), it must be the case that $\tau(b_i) = c_i$ for $1 \leq i \leq k$. In particular,

$$c_1^r = c_2^{\lambda_2} c_3^{\lambda_3} \cdots c_k^{\lambda_k} \tau(D)^q \tau(C).$$

and so,

$$(\prod_{s=1}^{M} [u_{2s}, u_{2s+1}])^r = \tau(D)^q \tau(C). \tag{9}$$

But C is the product of some fixed number k of commutators

$$C = \prod_{i=1}^{k} [w_{i_1}, w_{i_2}]$$

hence

$$\tau(C) = \prod_{i=1}^{k} [\tau(w_{i_1}), \tau(w_{i_2})]$$

so for sufficiently large M (depending on the number of commutators which occur in C) this together with (9) yields a contradiction (by Lemma 2 for $c = 2$.) So the new solution is a strict generalization of the original solution, and the equation is nullary.

Thus ends the proof of the theorem for nilpotent groups of class 2. It should be clear that the proof in fact specifies an algorithm for determining whether any particular system of equations is nilpotent. For examples of its application see the next section.

2.3 Nilpotent class c groups

We now aim to provide a classification of the unification type of systems of equations in nilpotent groups of class c, for all $c > 2$. As noted in the introduction it was not actually necessary to deal with the class 2 case separately, but having done so enables us to present the proof of this case in a somewhat less technical manner (which is to say, we omit some of the details which are handled in the same way as above). The theorem which we will prove is:

Theorem 4 *For every $c \geq 1$, every system of equations in variables*

$$x_1, x_2, \ldots, x_n$$

over the free nilpotent group of class c is either unitary or nullary. If a system is unitary, then there is a most general solution of the form:

$$x_i = w_i(y_1, y_2, \ldots, y_k) \quad \text{for } 1 \leq i \leq n$$

where $y_1, y_2, \ldots, y_k$ is a sequence of free generators, and there are terms:

$$t_1(\mathbf{x}), t_2(\mathbf{x}), \ldots, t_k(\mathbf{x}),$$

with the property that for any solution $\mathbf{a}$*:*

$$a_i = w_i(t_1(\mathbf{a}), t_2(\mathbf{a}), \ldots, t_k(\mathbf{a})) \quad \text{for } 1 \leq i \leq n.$$

If a system of equations is nullary, then every solution has a proper generalization.

The proof is by induction on c, the base case $c = 1$ of abelian groups certainly satisfy the conditions (in fact all equations are unitary), and also the case $c = 2$ was verified above. So we suppose that the result is true for all systems of equations over nilpotent groups of class less than c.

Let a system Σ of equations over the free nilpotent group of class c be given. Such a system may equally well be considered as a system over the free group of class $c - 1$, and so by the inductive hypothesis we may suppose that as such it is either unitary or nullary. We will see that in the latter case Σ remains nullary (a slight strengthening of the inductive hypothesis will be required to verify this). In the former case, Σ in class c will be either unitary or nullary, and we will also see that the required strengthening of the inductive hypothesis is valid. Let us begin with this case.

So Σ is a given set of equations such that in class $c - 1$ it is unitary, with a most general solution $x_i = w_i(\mathbf{y})$ and terms $t_1, t_2, \ldots, t_k$ as provided by the inductive hypothesis. Thus, if $u_1, u_2, \ldots, u_k$ are free generators, and we make the substitutions:

$$x_i = w_i(\mathbf{u})P_i \quad \text{for } 1 \leq i \leq n$$

in Σ where $P_1, P_2, \ldots, P_n$ are to stand for arbitrary elements of the center of the free nilpotent group of class c (which we recall equals the subgroup generated by the basic commutators of weight c); then we obtain a system of equations of the form:

$$P_i^{m_1} P_2^{m_2} \cdots P_n^{m_n} = \prod_{i_1 < i_2 < \cdots < i_c} [u_{i_1}, u_{i_2}, \ldots, u_{i_c}]^{n_{i_1, \ldots, i_c}}. \tag{10}$$

If this system has a solution then it has one with $P_1, P_2, \ldots, P_n$ elements of the subgroup generated by:

$$\{[u_{i_1}, u_{i_2}, \ldots, u_{i_c}] : i_1 < i_2 < \cdots < i_c\}$$

and we claim that if we choose any such solution $P_1(\mathbf{u}), P_2(\mathbf{u}), \ldots, P_n(\mathbf{u})$ then:

$$x_i = w_i(\mathbf{u}) P_i(\mathbf{u}) \quad \text{for } 1 \le i \le n \tag{11}$$

is a most general solution of Σ. Furthermore we can find terms $s_1, s_2, \ldots, s_k$ so that for any solution $\mathbf{a}$ of Σ,

$$a_i = w_i(s_1(\mathbf{a}), s_2(\mathbf{a}), \ldots, s_k(\mathbf{a})) P_i(s_1(\mathbf{a}), s_2(\mathbf{a}), \ldots, s_k(\mathbf{a})) \quad \text{for } 1 \le i \le n.$$

Of course it suffices to verify this last claim.

We know already that for $\mathbf{x}$ determined from $\mathbf{u}$ according to the substitution (11)

$$u_i = t_i(\mathbf{x}) \prod [u_{i_1}, u_{i_2}, \ldots, u_{i_c}]^{d_{i_1, \ldots, i_c}} \quad \text{for } 1 \le i \le k. \tag{12}$$

for some integers $d_{i_1, \ldots, i_c}$. This occurs because modulo the center of the free nilpotent group of class c:

$$u_i \cong t_i(\mathbf{x}) \quad \text{for } 1 \le i \le k. \tag{13}$$

But in any nilpotent group G of class c:

$$g_j \cong h_j \pmod{Z(G)} \quad \text{for } 1 \le j \le c$$

implies $[g_1, g_2, \ldots, g_c] = [h_1, h_2, \ldots, h_c]$ (in fact it already implies $[g_1, g_2] = [h_1, h_2]$). Using this fact and the congruences (13) we obtain from (12) the equation:

$$u_i = t_i(\mathbf{x}) \prod [t_{i_1}(\mathbf{x}), t_{i_2}(\mathbf{x}), \ldots, t_{i_c}(\mathbf{x})]^{d_{i_1, \ldots, i_c}} \quad \text{for } 1 \le i \le k.$$

So we may take s_i to be the term on the right hand side above (treating $\mathbf{x}$ once again as variable symbols).

What happens in the case that (10) does not have any solutions? In this case, some combination of these equations is of the form:

$$(P_i^{m'_1} P_2^{m'_2} \cdots P_n^{m'_n})^q = \prod_{i_1 < i_2 < \cdots < i_c} [u_{i_1}, u_{i_2}, \ldots, u_{i_c}]^{n'_{i_1, \ldots, i_c}}.$$

Where q is a prime which does not divide some $n'_{i_1,\dots,i_c}$.

Let $\mathbf{a}$ be an arbitrary solution of Σ. Because of the above relationships, if

$$b_j = t_j(\mathrm{a}) \quad \text{for } 1 \leq i \leq k$$

then without loss of generality there must be some relation of the form:

$$b_1^r = b_2^{\lambda_2} b_3^{\lambda_3} \cdots b_k^{\lambda_k} D^q C.$$

where C belongs to the commutator subgroup, $D \in F$ and q is a prime which does not divide r.

However,

$$a_i = w_i(\mathrm{b}) P_i^* \quad \text{for } 1 \leq i \leq n$$

for some P_i^* in the center of the free nilpotent group of class c, as the sequence $w_1, w_2, \dots, w_n$ is a most general solution of Σ in the free nilpotent group of class $c-1$, and hence certainly also in any torsion-free abelian group. Hence, if we set:

$$\begin{aligned} c_1 &= b_1 \prod_{s=0}^{m} [y_{cs+1}, y_{cs+2}, \dots, y_{cs+c-1}] \\ c_j &= b_j \quad (2 \leq j \leq k) \end{aligned}$$

where the $\mathbf{y}$ are free generators which do not occur in any of $\mathbf{b}$ or P_i^*, then

$$a'_i = w_i(\mathrm{c}) P_i^* \quad \text{for } 1 \leq i \leq n$$

is also a solution of Σ and $c_j = t_j(\mathrm{a}')$. But then as in the class 2 case, this solution strictly generalizes the original solution if M is chosen sufficiently large.

Now suppose that Σ is already nullary as a system of equations over the free nilpotent group of class $c-1$. From the discussion above, this implies that for some $w_1, w_2, \dots, w_n$ which reduce to a most general abelian solution of Σ and for some terms $t_1, t_2, \dots, t_k$, for any solution $\mathbf{a}$ of Σ in the free nilpotent group of class c, if $b_j = t_j(\mathrm{a})$ for $1 \leq j \leq k$, and if $\bar{b}_j$ for $1 \leq j \leq k$ denote the images of these elements in the free nilpotent group of class $c-1$ then without loss of generality:

$(A)_{c-1}$ For some integers $r, \lambda_2, \dots, \lambda_k$, some prime q which is not a divisor of r, some D in the free nilpotent group of class $c-1$ and some C in the commutator subgroup of this group:

$$\bar{b}_1^r = \bar{b}_2^{\lambda_2} \cdots \bar{b}_k^{\lambda_k} C D^q;$$

$(B)_c$ For some P_i^* in the commutator subgroup of the free nilpotent group of class c,

$$a_i = w_i(\mathrm{b}) P_i^* \quad \text{for } 1 \leq i \leq n.$$

Strictly speaking, the discussion above only guarantees $(A)_d$ and $(B)_d$ for some $d < c$. However, both these assertions contain factors which are to be chosen from the commutator subgroup, hence provided that they hold modulo some term in the lower central series of the free nilpotent group of class c, they will hold in the free nilpotent group of class c. The fact that $(A)_{c-1}$, $(A)_c$ and $(B)_c$ hold is the strengthening of the inductive hypothesis which we referred to above. But in the first part of the proof we saw that these relationships hold when Σ is nullary in class c and unitary in class $c-1$, and we are currently in the process of showing that they likewise hold when Σ is nullary in class $c-1$.

From $(A)_{c-1}$ we may deduce $(A)_c$ i.e.

$$b_1^r = b_2^{\lambda_2} \cdots b_k^{\lambda_k} C D^q$$

for some C in the commutator subgroup of the free nilpotent group of class c. From $(B)_c$ if we form $\mathbf{c}$ and $\mathbf{a}'$ as above:

$$\begin{aligned} c_1 &= b_1 \prod_{s=0}^{M} [y_{cs+1}, y_{cs+2}, \ldots, y_{cs+c-1}] \\ c_j &= b_j \quad (2 \leq j \leq k) \\ a_i' &= w_i(\mathbf{c}) P_i^* \quad (1 \leq i \leq n) \end{aligned}$$

we will still have a solution. But then from $(A)_c$ (which now holds with $\mathbf{c}$ in place of $\mathbf{b}$ everywhere) this will be a proper generalization of the solution $\mathbf{a}$ provided that M is chosen sufficiently large.

2.4 An important technical lemma

This section is devoted to the proof of Lemma 2 which we restate here for convenience:

Lemma *For all positive integers k non-zero integers r and primes p which do not divide r, there is a positive integer $\phi(k)$ such that, for any $M > \phi(k)$, the equation:*

$$z^p \prod_{j=1}^{k} [x_j, y_j] = (\prod_{i=1}^{M} [u_{i1}, u_{i2}, \ldots, u_{ic}])^r$$

has no solution in any free group in $\mathcal{N}_c$ in which $\{u_{il} : 1 \leq i \leq M, 1 \leq l \leq c\}$ is a subset of cM elements of a free generating set.

Proof: The proof is similar to the argument in [3]. We first construct a finite group H_c which is a nilpotent class c p-group, generated by a sequence $a_1, a_2, \ldots, a_c$, such that $[a_1, a_2, \ldots, a_c]$ is not a pth power. Then we exhibit a homomorphism from the free group in $\mathcal{N}_c$ to H_c which sends the left hand side of the equation above to $[a_1, a_2, \dots, a_c]$, while sending each of the commutators on the right to 1.

Consider the $\mathbf{Z}_{p^2}$-algebra generated by $x_1, x_2, \dots, x_c$ with the following relations:

1. Any monomial containing more than one occurrence of any variable is 0,
2. $x_i x_j = x_j x_i$ for all $i, j \in \{2, 3, \dots c\}$

Observe that in this algebra, if M is a sum of monomials of degree at least one then:

$$M^{c+1} = 0$$

since any monomial in M^{c+1} contains a repeated variable.

Let G_c be the group of units of this algebra of the form $1 + M$ where M is a sum of monomials of degree at least 1. The group G_c is a p-group since for any such monomial M, if n is such that

$$p^2 \text{ is a divisor of } \binom{p^n}{1}, \binom{p^n}{2}, \dots, \binom{p^n}{c}$$

then:

$$(1+M)^{p^n} = 1 + \sum_{j=1}^{c} \binom{p^n}{j} M^j = 1$$

If M and N are such sums which in addition are homogeneous in each variable, then $(1-M)^{-1} = 1 + M$ and $(1-N)^{-1} = 1 + N$ and furthermore:

$$[1-M, 1-N] = 1 + MN - NM. \tag{14}$$

Note that $MN - NM$ is also homogeneous in each variable.

Let:

$$a_i = 1 - x_i \quad \text{so} \quad a_i^{-1} = 1 + x_i$$

and let H_c be the multiplicative subgroup of G_c generated by $a_1, a_2, \dots, a_c$.

For each j between 1 and c, $a_j a_1 a_j^{-1}$ contains x_1 in each of its non-constant monomials, and hence commutes with $a_1 = 1 + x_1$. Therefore the normal subgroup $\langle a_1 \rangle$ of H_c generated by a_1 is abelian. Certainly the subgroup generated by $a_2, a_3, \dots, a_c$ is also abelian since x_i and x_j commute for $i, j > 1$.

It is clear that:

$$[a_1, a_2, \dots, a_c] \neq 1$$

since from (14) it will equal

$$1 + \sum_{X \subseteq \{2,3,\dots n\}} (-1)^{|X|} (\prod_{j \in X} a_j) a_1 (\prod_{k \not\in X} a_k).$$

On the other hand, any commutator of $a_1, a_2, \ldots, a_c$ of weight greater than c contains a repeated symbol, hence is equal to 1. Thus H_c is nilpotent of class c. It remains to show that $[a_1, a_2, \ldots, a_c]$ is not a pth power.

Suppose otherwise, namely that for some M which is sum of monomials all of degree at least 1:

$$(1 + M)^p = [a_1, a_2, \ldots, a_c]$$

We first claim that M contains a monomial of degree less than c whose coefficient is not a multiple of p. Otherwise, $M = pN + Y$ where N is a sum of monomials of degree at least one, and Y is sum of monomials of degree c, and:

$$(pN + Y)^2 = p^2N^2 + pNY + pYN + Y^2 = 0.$$

Hence:

$$(1 + pN + Y)^p = 1 + p(pN + Y) = 1 + pY.$$

But none of the coefficients of $[a_1, a_2, \ldots, a_c]$ are multiples of p so this is not possible.

So choose a monomial m from M of smallest degree whose coefficient is not a multiple of p. Thus:

$$M = pA + m + B$$

for some A which is a sum of monomials of degree at least one, and B which is a sum of monomials whose degree is at least as great as the degree of m. Then:

$$\begin{aligned}(1 + pA + m + B)^p &= 1 + p(pA + m + B) + \text{terms of higher degree than } m \\ &= 1 + p(m + B) + \text{terms of higher degree than } m,\end{aligned}$$

and this cannot equal $[a_1, a_2, \ldots, a_c]$ since it contains a monomial of degree less than c.

Let A be the c-generated relatively free algebra in the variety generated by H_c (and fix generators $b_1, b_2, \ldots, b_c$ of A). Since H_c is finite, so is A. Let $N = |\mathsf{A}|$. Since H_c is generated by c elements, it is a homomorphic image of A.

Returning to our equation:

$$z^p \prod_{j=1}^{k} [x_j, y_j] = (\prod_{i=1}^{M} [u_{i1}, u_{i2}, \ldots, u_{ic}])^r$$

suppose that $M > N^{2k+1}$. If we have a solution to this equation in the free group of $\mathcal{N}_c$:

$$D^p \prod_{j=1}^{k} [p_j, q_j] = (\prod_{i=1}^{M} [u_{i1}, u_{i2}, \ldots, u_{ic}])^r$$

then we may assume that $p_1, p_2, \ldots, p_k$ and $q_1, q_2, \ldots, q_k$ are contained in the subgroup generated by

$$\{u_{il} : 1 \leq i \leq M,\, 1 \leq l \leq c\}.$$

This subgroup is of course also free on this set of generators. Consider the homomorphisms from this group to A determined as follows:

$$\theta_i := \begin{cases} u_{ij} \mapsto b_j & 1 \leq l \leq c \\ u_{sj} \mapsto 1 & s \neq i \end{cases}$$

Now define a map $\psi : \{1, 2, \ldots M\} \to \mathsf{A}^{2k}$ by:

$$\psi(i) = (\theta_i(p_1), \theta_i(p_2), \ldots, \theta_i(p_k), \theta_i(q_1), \theta_i(q_2), \ldots, \theta_i(q_k)) \qquad \text{for } 1 \leq i \leq M$$

Since $M > N^{2k+1}$ and $N = |\mathsf{A}|$ there exist N distinct elements i of $\{1, 2, \ldots, M\}$ for which the values $\psi(i)$ are all the same. Since the maps θ_i can be permuted by permuting our generating set, we may for convenience assume that:

$$\psi(1) = \psi(2) = \cdots = \psi(N).$$

Since $b_1, b_2, \ldots, b_c$ is a sequence of free generators for A this means that in any group of the variety containing A, and in particular in H_c, for any tuple $\bar{x}$ of length c, and $\bar{1}$ a c-tuple of 1's, and for each $1 \leq j \leq k$:

$$\begin{aligned} p_j(\bar{1}, \ldots, \bar{1}, \bar{x}, \bar{1}, \ldots, \bar{1}, \ldots) &= p_j(\bar{1}, \ldots, \bar{1}, \bar{1}, \bar{1}, \ldots, \bar{x}, \ldots) \\ q_j(\bar{1}, \ldots, \bar{1}, \bar{x}, \bar{1}, \ldots, \bar{1}, \ldots) &= q_j(\bar{1}, \ldots, \bar{1}, \bar{1}, \bar{1}, \ldots, \bar{x}, \ldots) \end{aligned}$$

provided that both occurrences of $\bar{x}$ are in the first N blocks.

Now consider the homomorphism γ from the free group in $\mathcal{N}_c$ to H_c defined by:

$$u_{il} \mapsto \begin{cases} a_l & \text{for } \ 1 \leq i \leq N, 2 \leq l \leq c \\ a_1 & \text{for } \ i = 1, l = 1 \\ 1 & \text{otherwise} \end{cases}$$

Let $\bar{a} = a_1, a_2, \ldots, a_c$, and $\hat{a} = 1, a_2, \ldots, a_c$. Then for $1 \leq j \leq k$:

$$p_j(\overbrace{\hat{a}, \hat{a}, \ldots, \hat{a}}^{N}, \bar{1}, \ldots, \bar{1}) = p_j(\hat{a},'\bar{1}, \ldots, \bar{1}, \bar{1}, \ldots, \bar{1})^N = 1$$

The first equality follows from the relations above, and the fact that the subgroup of H_c generated by $a_2, \ldots, a_n$ is abelian. The second comes from the fact that $N = |\mathsf{A}|$ and H_c is a homomorphic image of A. The same calculation yields:

$$q_j(\overbrace{\hat{a}, \hat{a}, \ldots, \hat{a}}^{N}, \bar{1}, \ldots, \bar{1}) = 1.$$

Hence, for $1 \leq j \leq k$,

$$\begin{aligned} \gamma(p_j) &= p_j(\bar{a}, \overbrace{\hat{a}, \hat{a}, \ldots, \hat{a}}^{N-1}, \bar{1}, \ldots, \bar{1}) \in \langle a_1 \rangle \\ \gamma(q_j) &= q_j(\bar{a}, \overbrace{\hat{a}, \hat{a}, \ldots, \hat{a}}^{N-1}, \bar{1}, \ldots, \bar{1}) \in \langle a_1 \rangle \end{aligned}$$

since $\bar{a} \cong \hat{a} \pmod{\langle a_1 \rangle}$. But since $\langle a_1 \rangle$ is abelian, this implies that:

$$\gamma(D^p \prod_{j=1}^{k} [p_j, q_j]) = \gamma(D)^p$$

while

$$\gamma((\prod_{i=1}^{M} [u_{i1}, u_{i2}, \ldots, u_{ic}])^r) = [a_1, a_2, \ldots, a_c]^r$$

which is not a pth power by the above (recall that p is not a divisor of r.) This contradiction concludes the proof. ■

3 Examples

We will now illustrate the technique of solving systems of equations in nilpotent class 2 groups with two detailed examples.

Example 1 *The pair of equations:*

$$\begin{aligned} x_1^{-5}\, x_2^2\, x_3\, x_4^5\, [x_2, x_3]^3 &= 1 \\ x_1^{-1}\, x_2\, x_3^{-1}\, x_4^4\, [x_1, x_2]\, [x_1, x_3]\, [x_2, x_4]\, [x_3, x_4]^{-1} &= 1 \end{aligned}$$

has a most general solution in the variety of nilpotent class 2 groups.

The abelian reduction of this system:

$$\begin{aligned} x_1^{-5}\, x_2^2\, x_3\, x_4^5 &= 1 \\ x_1^{-1}\, x_2\, x_3^{-1}\, x_4^4 &= 1 \end{aligned}$$

has a most general solution:

$$\begin{aligned} x_1 &= uv^2 \\ x_2 &= u^{-1}v \\ x_3 &= u^2v^3 \\ x_1 &= uv \end{aligned}$$

In a nilpotent class 2 group:

$$\begin{aligned} & (uv^2)^{-5}(u^{-1}v)^2(u^2v^3)(uv)^5 = \\ & \qquad (v^{-2}u^{-1})^5(u^{-1}v)^2(u^2v^3)(uv)^5 \\ = & \quad [u,v]^{(-1)(-2-4-6-8-10)+(-1)(-10-9)+2(-8)+1(-5-4-3-2-1)} \\ = & \quad [u,v]^{18} \end{aligned}$$

and similarly,

$$(uv^2)^{-1}(u^{-1}v)(u^2v^3)^{-1}(uv)^4 = [u,v]^2.$$

Further:

$$\begin{aligned} [x_1, x_2] &= [u,v]^3 \\ [x_1, x_3] &= [u,v]^{-1} \\ [x_1, x_4] &= [u,v]^{-1} \\ [x_2, x_3] &= [u,v]^{-5} \\ [x_2, x_4] &= [u,v]^{-2} \\ [x_3, x_4] &= [u,v]^{-1}. \end{aligned}$$

Therefore:

$$\begin{aligned} x_1^{-5}\, x_2^2\, x_3\, x_4^5\, [x_2, x_3]^3 &= [u,v]^3 \\ x_1^{-1}\, x_2\, x_3^{-1}\, x_4^4\, [x_1, x_2]\, [x_1, x_3]\, [x_2, x_4]\, [x_3, x_4]^{-1} &= [u,v]^3. \end{aligned}$$

So with $x_1 = uv^2P_1$, $x_2 = u^{-1}vP_2$, $x_3 = u^2v^3P_3$, $x_4 = uvP_4$ we obtain:

$$\begin{aligned} P_1^{-5}\, P_2^2\, P_3\, P_4^5 &= [u,v]^{-3} \\ P_1^{-1}\, P_2\, P_3^{-1}\, P_4^4 &= [u,v]^{-3}. \end{aligned}$$

which has a particular solution:

$$P_1 = [u,v]^{-1},\ P_2 = [u,v]^{-4},\ P_3 = P_4 = 1$$

so we obtain a most general solution to the original system:

$$\begin{aligned} x_1 &= uv^2[u,v]^{-1} \\ x_2 &= u^{-1}v[u,v]^{-4} \\ x_3 &= u^2v^3 \\ x_1 &= uv \end{aligned}$$

Example 2 *The pair of equations:*

$$\begin{aligned} x_1^{-5}\, x_2^2\, x_3\, x_4^5\, [x_2, x_3]^2 &= 1 \\ x_1^{-1}\, x_2\, x_3^{-1}\, x_4^4\, [x_1, x_2]\, [x_1, x_3]\, [x_2, x_4]\, [x_3, x_4]^{-1} &= 1 \end{aligned}$$

does not have a most general solution in the variety of nilpotent class 2 groups.

This example differs from the first only in the exponent of $[x_2, x_3]$ in the first equation. The analysis of the abelian solution is therefore the same, but this time we are led to the equations:

$$\begin{aligned} P_1^{-5}\,P_2^2\,P_3\,P_4^5 &= [u,v]^{-8} \\ P_1^{-1}\,P_2\,P_3^{-1}\,P_4^4 &= [u,v]^{-3}. \end{aligned}$$

and consequently (remembering that P_1, P_2, P_3, P_4 commute:

$$P_2^{-3}\,P_3^6\,P_4^{-15} = [u,v]^7.$$

Since the exponent on the right is not a multiple of 3, this system does not have a most general solution.

4 Conclusion

We have shown that there is a close connection between solving systems of equations in nilpotent groups and doing so in abelian groups. Similar methods can be used to show that some systems of equations in other varieties of groups (particularly those which are generated by a finite group) are also nullary. In fact, the proof in this paper applies to any variety of groups which is nilpotent, contains the groups H_c used in the techical lemma for each prime p, and such that each free group is residually a finite p-group for each p. A particular variety of this type is the intersection of the variety of metabelian groups and $\mathcal{N}_c$. However, a complete classification of systems of equations in an arbitrary variety of groups would seem to be very difficult. We list a few of the more interesting open cases of such questions below:

Question 1 *In the variety of all groups is there an equation or system of equations which is finitary but not unitary?*

Question 2 *Can systems of equations in solvable groups, in particular in metabelian groups, be classified as above?*

Question 3 *Can the unification type of the variety generated by a finite group G be determined?*

References

[1] T.J. Chou and G.E. Collins. Algorithms for the solution of systems of linear diophantine equations. *SIAM Journal of Computing*, 11:687–708, 1982.

[2] Costas S. Iliopoulos. Worst-case complexity bounds on algorithms for computing the canonical structure of infinite abelian groups and solving systems of linear diophantine equations. *SIAM Journal of Computing*, 18:658–669, 1989.

[3] J. Lawrence. The definability of the commutator subgroup in a variety generated by a finite group. *Canad. Math. Bull.*, 28:505–507, 1985.

[4] H. Neumann. *Varieties of groups.* Springer Verlag, Berlin, Heidelberg, New York, 1967.