SPHERICAL QUADRATIC EQUATIONS IN FREE METABELIAN GROUPS

IGOR LYSENOK AND ALEXANDER USHAKOV

(Communicated by Pham Huu Tiep)

ABSTRACT. We prove that the Diophantine problem for spherical quadratic equations in free metabelian groups is solvable and, moreover, **NP**-complete.

1. INTRODUCTION

Let G be a group, X a set of variables, and F_X the free group on X . An *equation* in G is a formal equality $W = 1$ where $W \in G * F_X$. A *solution* of an equation $W = 1$ is a homomorphism $\alpha : G * F_X \rightarrow G$ such that $\alpha(W) = 1$ and $\alpha(g) = g$ for all $g \in G$. The *Diophantine problem* for a class of equations $\mathcal{C}$ is an algorithmic question to decide if a given equation $W = 1$ in $\mathcal{C}$ has a solution or not.

A word $W \in G * F_X$ and an equation $W = 1$ in G are *quadratic* if every variable $x \in X$ occurring in W occurs exactly twice (as x or x^{-1}). Let $\mathcal{C}_m$ be the class of quadratic equations of the form

$$z_1 c_1 z_1^{-1} \dots z_m c_m z_m^{-1} = 1, \quad c_1, \dots, c_m \in G, \quad z_1, \dots, z_m \in X$$

and

$$\mathcal{C} = \bigcup_{m=1}^{\infty} \mathcal{C}_m.$$

We call equations in $\mathcal{C}$ *spherical quadratic equations*. This reflects the fact that the surface corresponding to a quadratic word $W \in \mathcal{C}$ is a sphere with m disks removed (see [5]). Note that given a group G , the Diophantine problem for the classes of equations $\mathcal{C}_1$ and $\mathcal{C}_2$ are the word problem and the conjugacy problem in G , respectively. Solvability of these problems in free metabelian groups was proven in [6] and [7]. A nearly linear time algorithm (in the length of w) for the word problem was found in [8] and a polynomial time algorithm for the conjugacy problem was described in [14] (later improved in [13]).

In this note, we consider spherical quadratic equations in the free metabelian group M_n of rank $n \geq 2$. We prove that:

- For a fixed m , there exists a polynomial time algorithm solving the Diophantine problem for equations in $\mathcal{C}_m$.
- The Diophantine problem for $\mathcal{C}$ is **NP**-complete.

Received by the editors June 8, 2014 and, in revised form, August 25, 2014.

2010 *Mathematics Subject Classification*. Primary 20F16; Secondary 20F10, 68W30.

Key words and phrases. Free metabelian group, Diophantine problem, quadratic equation, **NP**-completeness.

The first author has been partially supported by the Russian Foundation for Basic Research.

The second author has been partially supported by NSA Mathematical Sciences Program grant number H98230-14-1-0128.

Recall that for every $n \geq 2$ the Diophantine problem for equations of the form $w(x_1, \dots, x_k) = c$ in M_n is undecidable (see [10]). Moreover, there exist $w = w(x_1, \dots, x_k)$ and $u \in M_n$ such that the class of equations $\{w = u^l \mid l \in \mathbb{Z}\}$ has the undecidable Diophantine problem. In particular, this implies undecidability of the general problem for all equations in M_n . Bibliography on solving special classes of equations in free metabelian groups is very scarce; we can only offer to the interested reader works by Baumslag, Mahler, and Lyndon [1, 4] who study solutions of equations of the form $x^n y^m z^l = 1$. Also, we want to mention recent papers by Remeslennikov and Romanovskii [9, 12] who describe algebraic sets over M_n in dimension 1. See also a recent survey [11].

Preliminaries: The free metabelian group. The free metabelian group M_n of rank n is the quotient $F_n/F_n^{(2)}$ of the free group F_n of rank n over its second derived subgroup $F_n^{(2)} = [F'_n, F'_n]$ (where F'_n denotes the commutator subgroup $[F_n, F_n]$). We fix a generating set

$$\{a_1, a_2, \dots, a_n\}$$

for M_n and by $x \mapsto \bar{x}$ we denote the natural epimorphism of M_n to the free abelian group $A_n = F_n/F'_n$. In particular, $\{\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n\}$ is a basis for A_n .

By Γ_n we denote the Cayley graph of A_n with respect to the generating set $\{\bar{a}_1, \dots, \bar{a}_n\}$. We view vertices of Γ_n as elements of A_n . The graph Γ_n may be naturally viewed as the 1-skeleton $U_n^{(1)}$ of the n -dimensional cubic complex U_n obtained by partitioning the euclidean space $\mathbb{R}^n$ into the union of unit n -cubes. By $C_1(\Gamma_n)$ we denote the free abelian group of 1-chains of Γ_n over $\mathbb{Z}$ (or flows over $\mathbb{Z}$ with finite support in the terminology of [8]), that is, the group of all formal linear combinations $k_1 e_1 + \dots + k_r e_r$ where $k_i \in \mathbb{Z}$ and e_i are edges of Γ_n .

All r -chains, r -cycles and homology groups are taken with integer coefficients and we use for them the standard notation $C_r(X)$, $Z_r(X)$ and $H_r(X)$.

A word $w \in F_n$ determines a unique edge path p_w in Γ_n labeled by w which starts at 1 (the vertex corresponding to the identity of A_n). It defines a 1-chain $\sigma(w)$ which is the algebraic sum of all edges traversed by p_w . It is not hard to see that the mapping $w \mapsto \sigma(w)$ induces a well-defined injective map $M_n \rightarrow C_1(\Gamma_n)$; that is, two words u and w define the same element of M_n if and only if $\sigma(u) = \sigma(w)$ (see [3, 8, 15]). For $g \in M_n$, we use the same notation $\sigma(g)$ for the image of g under the induced map. It is an easy exercise to check that for any $g, h \in M_n$,

$$(1) \quad \sigma(gh) = \sigma(g) + \bar{g}\sigma(h)$$

where $\bar{g}\sigma(h)$ is obtained by shifting $\sigma(h)$ by $\bar{g}$ (via the action of A_n on Γ_n).

For the boundary $\partial_1 \sigma(g)$ we obviously have

$$\partial_1 \sigma(g) = \bar{g} - 1.$$

This implies that $g \in M'_n$ if and only if $\sigma(g)$ is a 1-cycle. Since $\sigma(gh) = \sigma(g) + \sigma(h)$ if $g \in M'_n$, we get an isomorphism between M'_n and the group $Z_1(\Gamma_n)$ of 1-cycles of Γ_n (the last group coincides also with $H_1(\Gamma_n)$).

2. SPHERICAL QUADRATIC EQUATIONS

Let $W \in M_n * F_X$ be a word of the form

$$(2) \quad W = z_1 c_1 z_1^{-1} \cdot z_2 c_2 z_2^{-1} \cdot \dots \cdot z_m c_m z_m^{-1}, \quad c_i \in M_n.$$

Denote by Q the set of the involved constants c_i ,

$$Q = \{c_1, c_2, \dots, c_m\},$$

and let

$$L_Q = \langle \bar{c}_1, \dots, \bar{c}_m \rangle$$

be the subgroup of A_n generated by the images of c_i .

Let $\Delta_Q = \Gamma_n/L_Q$ be the quotient graph over the action of L_Q .

The action of the group A_n on Γ_n induces its action on U_n and we have $(U_n/L_Q)^{(1)} = \Delta_Q$. Since U_n is contractible, we have the exact chain complex:

$$0 \rightarrow C_n(U_n) \xrightarrow{\partial_n} C_{n-1}(U_n) \xrightarrow{\partial_{n-1}} \dots \rightarrow C_1(U_n) \xrightarrow{\partial_1} C_0(U_n) \rightarrow 0.$$

For $g \in M_n$, let $\tau_Q(g)$ denote the natural image of $\sigma(g)$ in $C_1(\Delta_Q)$. Denote also by γ_Q the natural projection $U_n \rightarrow U_n/L_Q$, so $\gamma_Q(\sigma(g)) = \tau_Q(g)$ for any $g \in M_n$.

Lemma 2.1. *If $\tau_Q(g) = 0$, then $g \in M'_n$.*

Proof. Let g be any element of M_n such that $\tau_Q(g) = 0$. We have $\tau_Q(g) = \gamma_Q(\sigma(g))$, where by definition, $\sigma(g)$ is the 1-chain in Γ_n defined by a path $p_{\hat{g}}$ starting at 1 and labeled by a word $\hat{g} \in F_n$ representing g . Since ∂_1 commutes with γ_Q we have $0 = \partial_1 \tau_Q(g) = \gamma_Q(\bar{g}) - 1$, that is, $\bar{g} \in L_Q$. This implies that $\gamma_Q(p_{\hat{g}})$ is a loop in Δ_Q and hence $0 = \tau_Q(g)$ is the image of $\gamma_Q(p_{\hat{g}})$ under the epimorphism $\pi_1(U_n/L_Q) \rightarrow H_1(U_n/L_Q)$. Now observe that U_n is the universal cover of U_n/L_Q , hence $\pi_1(U_n/L_Q) \simeq L_Q$ is abelian and the epimorphism $\pi_1(U_n/L_Q) \rightarrow H_1(U_n/L_Q)$ is in fact an isomorphism. Then $\gamma_Q(p_{\hat{g}})$ represents the trivial element of the fundamental group $\pi_1(U_n/L_Q)$ and its lift $\hat{g}$ is a loop and hence $\sigma(g)$ is a cycle. $\square$

For a word W of the form (2) consider the following two series of elements in M_n :

- (a) $[[a_i, a_j]^h, c_k]$ for all $h \in M_n$, $1 \leq i, j \leq n$ and $1 \leq k \leq m$;
- (b) $[c_i, c_j]$ for all $1 \leq i, j \leq m$.

Let H_Q be the subgroup generated by elements (a) and (b). Note that H_Q is an abelian group. It is easy to check that for any values $\alpha, \beta, \gamma = \pm 1$ an element $[[a_i^\alpha, a_j^\beta]^u, c_k]^\gamma$ is also an element of the form (a). For instance, $[[a_i, a_j]^u, c_k]^{-1} = [[a_j, a_i]^u, c_k]$.

Proposition 2.2. $\tau_Q(g) = 0$ if and only if $g \in H_Q$.

Proof. It is easy to check that $\tau_Q(g) = 0$ for every generator g of H_Q . Hence, sufficiency holds.

Now, assume that $\tau_Q(g) = 0$. It follows from Lemma 2.1 that $g \in M'_n$. Hence g can be identified with the corresponding 1-cycle $\sigma(g) \in Z_1(U_n)$. Obviously, the set $\{\sigma(g) \mid \tau_Q(g) = 0\}$ forms a subgroup of $Z_1(U_n)$ which is the kernel of the homomorphism $\gamma_* : Z_1(U_n) \rightarrow Z_1(U_n/L_Q)$ induced by the projection $\gamma : U_n \rightarrow U_n/L_Q$. Our goal is to compute $\ker(\gamma_*)$. To do this, we first compute the kernel of $C_2(U_n) \xrightarrow{\partial_2} Z_1(U_n) \xrightarrow{\gamma_*} Z_1(U_n/L_Q)$ and then take its image in $Z_1(U_n)$. Since we have a commutative diagram

$$\begin{array}{ccc} C_2(U_n) & \xrightarrow{\partial_2} & Z_1(U_n) \\ \downarrow \gamma_* & & \downarrow \gamma_* \\ C_2(U_n/L_Q) & \xrightarrow{\partial_2} & Z_1(U_n/L_Q) \end{array}$$

the kernel of $C_2(U_n) \xrightarrow{\partial_2 \gamma_*} Z_1(U_n/L_Q)$ is generated by $\ker(C_2(U_n) \rightarrow C_2(U_n/L_Q))$ and a set of preimages of generators for $\ker(C_2(U_n/L_Q) \xrightarrow{\partial_2} Z_1(U_n/L_Q))$.

Clearly, $\ker(C_2(U_n) \rightarrow C_2(U_n/L_Q))$ is generated by all 2-chains of the form

$$s - \bar{c}_k s, \quad s \in U_n^{(2)}.$$

For the kernel of $C_2(U_n/L_Q) \xrightarrow{\partial_2} Z_1(U_n/L_Q)$, we have two types of generators. First, there are generators for the image of $\partial_3 : C_3(U_n/L_Q) \rightarrow C_2(U_n/L_Q)$. These are boundaries $\partial_3 E$ of all 3-cubes $E \in (U_n/L_Q)^{(3)}$. These generators vanish when mapped to $Z_1(U_n)$. Second, there are the generators for $H_2(U_n/L_Q)$ which can be easily computed as follows.

As a topological space, U_n/L_Q is homeomorphic to the direct product of a finite number of copies of the real line $\mathbb{R}$ and circles S^1 . Clearly, $H_2(U_n/L_Q)$ is generated by all embedded tori $S^1 \times S^1$ for all distinct factors S^1 . Each factor S^1 represents a 1-cycle $\gamma(\rho)$ where ρ is a linear combination of 1-cycles $\tau_Q(c_i)$. This implies that $H_2(U_n/L_Q)$ is generated by the images under γ of all 2-cycles in U_n with boundaries $\sigma([c_i, c_j])$.

Summarizing, we get the following set of generators for the kernel of the homomorphism $(Z_1(U_n) \xrightarrow{\gamma!} \text{to } Z_1(U_n/L_Q))$: boundaries of all 2-cycles $s - \bar{c}_k s$, $s \in U_n^{(2)}$ and all 1-cycles of the form $\sigma([c_i, c_j])$. The boundaries of 2-cubes $s \in U_n^{(2)}$ are of the form $\sigma([a_i, a_j]^h)$, $h \in M_n$ and we have

$$\partial_2(s - \bar{c}_k s) = \sigma([a_i, a_j]^h) - \sigma(c_k[a_i, a_j]^h c_k^{-1}) = \sigma([a_i, a_j]^h, c_k).$$

This gives elements (a). The 1-cycles $\sigma([c_i, c_j])$ give elements (b). Thus, necessity holds. $\square$

Lemma 2.3. *Let H'_Q be the subgroup of M_n generated by all elements (a). Then $[[c_i, c_j], h] \in H'_Q$ for any $1 \leq i, j \leq m$ and $h \in M_n$.*

Proof. Observe that the following identities hold in M_n :

$$(3) \quad [uv, x] = [u, x][v, x],$$

$$(4) \quad [[x, y], z] = [[x, z], y] \cdot [[z, y], x],$$

for any $u, v \in M'_n$ and $x, y, z \in M_n$. Since M'_n is abelian, we have $[u, h] = [u, h^g]$ for any $u \in M'_n$ and $g, h \in M_n$. This obviously implies that H'_Q is a normal subgroup of M_n . Furthermore, by (3) we see that H'_Q contains all elements $[u, c_i]$ where $u \in M'_n$. Finally, it follows from (4) that $[[c_i, c_j], h] = [[c_i, h], c_j] \cdot [[h, c_j], c_i]$. $\square$

Note that $\tau_Q(u_i c_i u_i^{-1})$ is a 1-cycle in Δ_Q obtained by the shift of $\tau_Q(c_i)$ by the element $\bar{u}_i$ (under the action of A_n). The next proposition states that deciding if a given spherical equation has a solution is equivalent to finding shifts of the 1-cycles $\tau_Q(c_i)$ in Δ_Q with trivial algebraic sum.

Proposition 2.4. *The equation $W = 1$ has a solution if and only if there exist elements $u_1, u_2, \dots, u_m \in M_n$ satisfying*

$$(5) \quad \sum_{i=1}^m \tau_Q(u_i c_i u_i^{-1}) = 0.$$

Proof. For $\tilde{g} = (g_1, \dots, g_m) \in (M_n)^m$ define:

$$W(\tilde{g}) = g_1 c_1 g_1^{-1} g_2 c_2 g_2^{-1} \dots g_m c_m g_m^{-1}.$$

Let $\tilde{u}$ be a solution of the equation $W = 1$, i.e., we have $W(\tilde{u}) = 1$. By (1),

$$(6) \quad 0 = \sigma(W(\tilde{u})) = \sigma(u_1 c_1 u_1^{-1}) + \bar{h}_1 \sigma(u_2 c_2 u_2^{-1}) + \dots + \bar{h}_{m-1} \sigma(u_m c_m u_m^{-1})$$

where $h_i = u_1 c_1 u_1^{-1} \dots u_i c_i u_i^{-1}$. By the definition of Δ_Q , shifting of a chain $t \in C_1(\Delta_Q)$ by $h \in L_Q$ does not change t . Hence

$$\bar{h}_{i-1} \tau_Q(u_i c_i u_i^{-1}) = \tau_Q(u_i c_i u_i^{-1})$$

and applying γ_* to the both sides of (6) we get (5). This proves the “ $\Rightarrow$ ” part.

Now assume that $u_1, u_2, \dots, u_m \in M_n$ satisfy (5). Define a set:

$$S = S_W = \{W(\tilde{g}) \mid \tilde{g} \in (M_n)^m\}.$$

Clearly, $W = 1$ has a solution if and only if $1 \in S$. We claim that

$$SH_Q \subseteq S,$$

i.e., S is a union of H_Q -cosets. It is sufficient to prove that $Sh \subseteq S$ for any element h of the form (a) or (b).

For any $\tilde{g} = (g_1, g_2, \dots, g_m)$ and $h \in M_n$ we have

$$W(g_1, \dots, g_{k-1}, g_k [a_j, a_i]^{hd}, g_{k+1}, \dots, g_m) = W(\tilde{g}) \cdot [[a_i, a_j]^h, c_k]$$

where $d = (g_{k+1} c_{k+1} g_{k+1}^{-1} \dots g_m c_m g_m^{-1})^{-1}$. This proves $SH'_Q \subseteq S$. Similarly,

$$W(g_1, \dots, g_{j-1}, c_i g_j, g_{j+1}, \dots, g_m) = W(\tilde{g}) \cdot [c_i, c_j] \cdot [[c_i, c_j], f]$$

where $f = g_j (g_{j+1} c_{j+1} g_{j+1}^{-1} \dots g_m c_m g_m^{-1})^{-1}$. By Lemma 2.3, $[[c_j, c_i], f] \in H'_Q$. Using the already proved fact that $SH'_Q \subseteq S$ we see that $Sh \subseteq S$ for any h of the form (b) and hence $SH_Q = S$ as required.

As we have seen in the proof of “ $\Rightarrow$ ”, equality (5) can be rewritten as

$$\tau_Q(u_1 c_1 u_1^{-1} \dots u_m c_m u_m^{-1}) = 0.$$

Hence, by Proposition 2.2, $u_1 c_1 u_1^{-1} \dots u_m c_m u_m^{-1} \in H_Q \cap S$. Now it follows from the equality $SH_Q = S$ that $1 \in S$. Therefore, $W = 1$ has a solution. $\square$

Corollary 2.5. *The equation $W = 1$ is solvable if and only if there exists a tuple $\tilde{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_m) \in (A_m)^n$ such that*

$$(7) \quad \alpha_1 \tau_Q(c_1) + \alpha_2 \tau_Q(c_2) + \dots + \alpha_m \tau_Q(c_m) = 0.$$

Proof. As observed above, the condition $\sum_{i=1}^m \tau_Q(u_i c_i u_i^{-1}) = 0$ in Proposition 2.4 can be rewritten as

$$\tau_Q(u_1 c_1 u_1^{-1}) + \tau_Q(u_2 c_2 u_2^{-1}) + \dots + \tau_Q(u_m c_m u_m^{-1}) = 0.$$

It remains to notice that $\tau_Q(u_i c_i u_i^{-1}) = \bar{u}_i \tau_Q(c_i)$ since $\tau_Q(c_i)$ is a 1-cycle in Δ_Q . $\square$

Remark. It is not hard to see from the proof of Proposition 2.4 that tuples $\tilde{\alpha}$ represent solutions of the equation $W = 1$ in the following way: given a tuple $\tilde{\alpha}$ satisfying (7), there exists a solution $\tilde{u}$ of $W = 1$ such that $u_i \in \alpha_i L_Q$, $i = 1, 2, \dots, m$.

Our next step is to give an effective bound on the size of a tuple $\tilde{\alpha}$ satisfying (7). For $\gamma \in A_n$ by $|\gamma|$ we denote the word length of γ in the generators $\{\bar{a}_1, \bar{a}_2, \dots, \bar{a}_n\}$ of A_n . For $x \in M_n$, $|x|$ denotes the word length of x in the generators $\{a_1, a_2, \dots, a_n\}$.

Proposition 2.6. *If a tuple $\tilde{\alpha}$ satisfies (7), then there exists another tuple $\tilde{\alpha}' = (\alpha'_1, \alpha'_2, \dots, \alpha'_m) \in (A_n)^m$ satisfying (7) such that $|\alpha'_i| \leq 2 \sum_j |c_j|$ for all $i = 1, \dots, m$.*

Proof. Denote

$$\tau_i = \alpha_i \tau_Q(c_i), \quad i = 1, \dots, m.$$

Given a 1-chain $\rho \in C_1(\Delta_Q)$,

$$\rho = \sum_{i=1}^r k_i e_i, \quad k_i \neq 0, \quad e_i \in E(\Delta_Q), \quad e_i \neq e_j \text{ for } i \neq j,$$

define

$$\text{supp}(\rho) = \{e_1, \dots, e_r\}.$$

Denote $I = \{1, \dots, m\}$. We call a non-empty subset $J \subseteq I$ a *cluster* if $\text{supp}(\tau_i) \cap \text{supp}(\tau_j) = \emptyset$ for any $i \in J$ and $j \notin J$. It follows from the definition that if J_1 and J_2 are clusters with non-empty intersection, then $J_1 \cap J_2$ is again a cluster. Hence I can be partitioned into a finite disjoint union of minimal clusters,

$$I = J_1 \uplus J_2 \uplus \dots \uplus J_t.$$

(Another view on minimal clusters: draw a graph with the set of vertices I where two vertices i and j are joined with an edge iff $\text{supp}(\tau_i) \cap \text{supp}(\tau_j) \neq \emptyset$. Then minimal clusters are connected components of this graph.)

We introduce an integer-valued distance function $d(e, f)$ on the set $E(\Delta_Q)$ of edges of Δ_Q . By definition, the distance between edges e and f is the distance between their midpoints in the graph Δ_Q (where all edges are assumed to have the length 1). For example, $d(e, f) = 1$ if and only if e and f are distinct and have a common vertex. The following statements hold:

- (i) If J is a cluster, then $\sum_{i \in J} \tau_i = 0$.
- (ii) If J is a cluster, then $\sum_{i \in J} (\alpha_i + \beta) \tau_Q(c_i) = 0$ for any $\beta \in A_n$.
- (iii) If J is a minimal cluster, then

$$\text{diam} \left(\bigcup_{i \in J} \text{supp}(\tau_i) \right) \leq \sum_{i \in J} |c_i|.$$

We say that a minimal cluster J is trivial if $J = \{j\}$ which happens if and only if $\text{supp}(\tau_j) = \emptyset$. If $\text{card}(J) > 1$, then we call J non-trivial. Clearly, $\text{supp}(\tau_j) \neq \emptyset$ for any j in a non-trivial cluster J .

Now, consider an arbitrary minimal cluster J . If J is trivial, then set α'_j to $(0, \dots, 0) \in A_n$. If J is non-trivial, then we choose any $j \in J$ and the origin $\beta \in A_n$ of an arbitrary edge $e \in \text{supp}(\tau_j)$ and set α'_j to $\alpha'_j - \beta$ for every $j \in J$. It follows from (ii) that so defined $\tilde{\alpha}'$ satisfies (7) and from (iii) that $|\alpha'_i| \leq 2 \sum_j |c_j|$. $\square$

Proposition 2.7. *Let $n, m \in \mathbb{N}$. Given a tuple $(c_1, \dots, c_m) \in M_n^m$ and a tuple $(\alpha_1, \dots, \alpha_m) \in A_n^m$ satisfying $|\alpha_i| \leq 2 \sum_j |c_j|$ it requires polynomial time in $\sum_{j=1}^m |c_j|$ to check (7).*

Proof. The sum in (7) is an algebraic sum of edges in Δ_Q traversed by paths $\alpha_i \tau_Q(c_i)$. We clearly can construct such a sum in polynomial time because we can efficiently distinguish vertices in Δ_Q using Gauss elimination. $\square$

Corollary 2.8. *The Diophantine problem for the class of spherical equations is in NP.*

Proof. For a certificate we can take a tuple $\tilde{\alpha}$ satisfying (7) with bound $|\alpha_i| \leq 2 \sum_j |c_j|$. $\square$

Corollary 2.9. *The Diophantine problem for the class $\mathcal{C}_m$ of spherical equations in M_n with a bounded number of variables is in $\mathbf{P}$.*

Proof. The size of the set of all possible certificates $\{(\alpha_1, \dots, \alpha_m) \mid |\alpha_i| \leq 2 \sum_{j=1}^m |c_j|\}$ can be bounded above by a polynomial $\left(2 \sum_{j=1}^m |c_j|\right)^{nm}$. $\square$

To prove $\mathbf{NP}$ -completeness of the Diophantine problem for an equation $W = 1$ we use $\mathbf{NP}$ -completeness of the *Square packing puzzle problem* (see [2]):

- *Input:* A tuple of positive integers $(n_1, n_2, \dots, n_k)$ written in the unary notation (i.e. the size of the input is $\sum_i n_i$).
- *Question:* Can the set of k square pieces of sizes $n_1 \times n_1, \dots, n_k \times n_k$ be exactly packed into the square box of area $n_1^2 + n_2^2 + \dots + n_k^2$?

For a k -tuple $\tilde{n} = (n_1, \dots, n_k) \in \mathbb{N}^k$ satisfying $n_0 = \sqrt{n_1^2 + \dots + n_k^2} \in \mathbb{N}$ define a word $W_{\tilde{n}} \in M_2 * F_{\{z_0, z_1, \dots, z_k\}}$:

$$W_{\tilde{n}} = z_0[a_2^{n_0}, a_1^{n_0}]z_0^{-1} \cdot \prod_{i=1}^k z_i[a_1^{n_i}, a_2^{n_i}]z_i^{-1}.$$

Theorem 2.10. *The Diophantine problem for an equation $W_{\tilde{n}} = 1$ in M_2 is $\mathbf{NP}$ -complete.*

Proof. Fix a tuple $\tilde{n}$. The set Q associated with $W_{\tilde{n}}$ is

$$Q = \{[a_1^{n_0}, a_2^{n_0}]^{-1}, [a_1^{n_1}, a_2^{n_1}], \dots, [a_1^{n_k}, a_2^{n_k}]\}.$$

The corresponding subgroup L_Q of A_2 is trivial and Δ_Q is simply the Cayley graph of $\mathbb{Z}^2$ relative to the standard generators $\{\bar{a}_1, \bar{a}_2\}$. Hence, for every $c = [a_1^{n_i}, a_2^{n_i}] \in Q$, $\tau(c)$ is the grid $(n_i \times n_i)$ -square contour starting at $(0, 0)$. It follows from Corollary 2.5 that the set of k squares given by $\tilde{n}$ can be packed into the $(n_0 \times n_0)$ -square if and only if the equation $W_{\tilde{n}} = 1$ has a solution. We get a reduction to the Square packing puzzle problem. $\square$

Observe that an equation $W = 1$ in M_2 has a solution if and only if it has a solution when viewed as an equation in M_n for $n \geq 2$. We immediately get:

Corollary 2.11. *For any $n \geq 2$, the Diophantine problem for the class of spherical quadratic equations in M_n is $\mathbf{NP}$ -complete.*

REFERENCES

- [1] Gilbert Baumslag and Kurt Mahler, *Equations in free metabelian groups*, Michigan Math. J. **12** (1965), 417–420. MR0181665 (31 #5892)
- [2] Erik D. Demaine and Martin L. Demaine, *Jigsaw puzzles, edge matching, and polyomino packing: connections and complexity*, Graphs Combin. **23** (2007), no. suppl. 1, 195–208, DOI 10.1007/s00373-007-0713-4. MR2320628 (2008e:05030)
- [3] Carl Droms, Jacques Lewin, and Herman Servatius, *The length of elements in free solvable groups*, Proc. Amer. Math. Soc. **119** (1993), no. 1, 27–33, DOI 10.2307/2159821. MR1160298 (93k:20051)
- [4] Roger C. Lyndon, *Equations in free metabelian groups*, Proc. Amer. Math. Soc. **17** (1966), 728–730. MR0195929 (33 #4125)

- [5] I. G. Lysenok and A. G. Myasnikov, *A polynomial bound for solutions of quadratic equations in free groups* (Russian, with Russian summary), Tr. Mat. Inst. Steklova **274** (2011), no. Algoritmicheskie Voprosy Algebrы i Logiki, 148–190, DOI 10.1134/S0081543811060101; English transl., Proc. Steklov Inst. Math. **274** (2011), no. 1, 136–173. MR2962940
- [6] Wilhelm Magnus, *On a theorem of Marshall Hall*, Ann. of Math. (2) **40** (1939), 764–768. MR0000262 (1,44b)
- [7] Jane Matthews, *The conjugacy problem in wreath products and free metabelian groups*, Trans. Amer. Math. Soc. **121** (1966), 329–339. MR0193130 (33 #1351)
- [8] A. Myasnikov, V. Roman’kov, A. Ushakov, and A. Vershik, *The word and geodesic problems in free solvable groups*, Trans. Amer. Math. Soc. **362** (2010), no. 9, 4655–4682, DOI 10.1090/s0002-9947-10-04959-7. MR2645045 (2011k:20059)
- [9] V. N. Remeslennikov and N. S. Romanovskii, *Irreducible algebraic sets in a metabelian group* (Russian, with Russian summary), Algebra Logika **44** (2005), no. 5, 601–621, 638, DOI 10.1007/s10469-005-0032-x; English transl., Algebra Logic **44** (2005), no. 5, 336–347. MR2195022 (2007b:20073)
- [10] V. A. Roman’kov, *Equations in free metabelian groups* (Russian), Sibirsk. Mat. Zh. **20** (1979), no. 3, 671–673, 694. MR537377 (80k:20040)
- [11] Vitalii Roman’kov, *Equations over groups*, Groups Complex. Cryptol. **4** (2012), no. 2, 191–239, DOI 10.1515/gcc-2012-0015. MR3043434
- [12] N. S. Romanovskii, *Algebraic sets in a metabelian group* (Russian, with Russian summary), Algebra Logika **46** (2007), no. 4, 503–513, 529, DOI 10.1007/s10469-007-0026-y; English transl., Algebra Logic **46** (2007), no. 4, 274–280. MR2363556 (2009b:20054)
- [13] Alexander Ushakov, *Algorithmic theory of free solvable groups: randomized computations*, J. Algebra **407** (2014), 178–200, DOI 10.1016/j.jalgebra.2014.02.014. MR3197157
- [14] Svetla Vassileva, *Polynomial time conjugacy in wreath products and free solvable groups*, Groups Complex. Cryptol. **3** (2011), no. 1, 105–120, DOI 10.1515/GCC.2011.005. MR2806083 (2012d:20075)
- [15] A. M. Vershik and S. V. Dobrynin, *Geometrical approach to the free solvable groups*, Internat. J. Algebra Comput. **15** (2005), no. 5-6, 1243–1260, DOI 10.1142/S0218196705002657. MR2197831 (2006m:20049)

DEPARTMENT OF MATHEMATICAL LOGIC, STEKLOV INSTITUTE OF MATHEMATICS, GUBKINA STR. 8, 119991 MOSCOW, RUSSIA – AND – DEPARTMENT OF MATHEMATICAL SCIENCES, STEVENS INSTITUTE OF TECHNOLOGY, HOBOKEN, NEW JERSEY 07030

E-mail address: igor.lysenok@gmail.com

DEPARTMENT OF MATHEMATICAL SCIENCES, STEVENS INSTITUTE OF TECHNOLOGY, HOBOKEN, NEW JERSEY 07030

E-mail address: aushakov@stevens.edu