DIOPHANTINE PROPERTIES OF ELEMENTS OF SO(3)

V. KALOSHIN AND I. RODNIANSKI

Abstract

A number $\alpha \in \mathbb{R}$ is diophantine if it is not well approximable by rationals, i.e. for some $C, \varepsilon > 0$ and any relatively prime $p, q \in \mathbb{Z}$ we have $|\alpha q - p| > C q^{-1-\varepsilon}$. It is well-known and is easy to prove that almost every $\alpha$ in $\mathbb{R}$ is diophantine. In this paper we address a noncommutative version of the diophantine properties. Consider a pair $A, B \in SO(3)$ and for each $n \in \mathbb{Z}_+$ take all possible words in $A, A^{-1}, B,$ and $B^{-1}$ of length $n$, i.e. for a multiindex $I = (i_1, j_1, \ldots, i_m, j_m)$ define $|I| = \sum_{k=1}^{m}(|i_k| + |j_k|) = n$ and $W_n(A, B) = \{W_I(A, B) = A^{i_1}B^{j_1} \ldots A^{i_m}B^{j_m} \}$.\textsuperscript{1}

Gamburd–Jakobson–Sarnak [GJS] raised the problem: prove that for Haar almost every pair $A, B \in SO(3)$ the closest distance of words of length $n$ to the identity, i.e. $s_{A,B}(n) = \min_{|I|=n} \|W_I(A, B) - E\|$, is bounded from below by an exponential function in $n$. This is the analog of the diophantine property for elements of $SO(3)$. In this paper we prove that $s_{A,B}(n)$ is bounded from below by an exponential function in $n^2$. We also exhibit obstructions to a “simple” proof of the exponential estimate in $n$.

1 Introduction

The classical result of metric number theory on Diophantine properties of numbers says the following: for any $\varepsilon > 0$ and a.e. $\alpha \in \mathbb{R}$ there is a constant $C = C(\alpha) > 0$ such that the map $n\alpha(\text{mod }1)$ satisfies the property $n\alpha(\text{mod }1) > C|n|^{-1-\varepsilon}$ for every integer $n$ [Kh].

Diophantine properties of numbers arise in various problems in metric number theory [Kh], smooth dynamical systems, holomorphic dynamics [HK], KAM theory [He], [L], [Mo], and others.

Generalizations of the metric number theory led to the development of the theory of simultaneous Diophantine approximations and even Dio-

\textsuperscript{1}The first author is partially supported by the Sloan Dissertation Fellowship and the American Institute of Mathematics Five-year Fellowship.
phantine approximations on manifolds. In the latter case consider manifold $M \subset \mathbb{R}^n$ defined by $n$ analytic functions $f_1, \ldots, f_n : U \subset \mathbb{R}^d \to \mathbb{R}$, $M = \{f(x) : x \in U\}$. Assume that functions $1, f_1, \ldots, f_n$ are linearly independent over $\mathbb{R}$. One of the central questions of the theory is the following conjecture made by Sprindžuk in 1980 and recently proved by D. Kleinbock and G. Margulis [KIM]:

Any manifold $M \subset \mathbb{R}^n$ of the above type is extremal, i.e. for almost all $y \in M$ and any $\epsilon > 0$ there exists a positive constant $D(y)$ such that for all $q \in \mathbb{Z}^n$ and $p \in \mathbb{Z}$

$$|q \cdot y + p| \geq \frac{D(y)}{||q||^{1+\epsilon}}.$$  \hfill (1)

Here $q \cdot y = \sum_{i=1}^{n} q_i y_i$ and $||q|| = \max_{1 \leq i \leq n} |q_i|$.

In fact, Kleinbock-Margulis prove even a stronger statement that $M$ is strongly extremal (approximation in the sense of (1) is replaced by the notion of multiplicative approximation). The proof is based on the correspondence between the approximation properties of vectors $y \in \mathbb{R}^n$ and the behavior of certain orbits in the space of unimodular lattices in $\mathbb{R}^{n+1}$.

The analogue of the Diophantine property can be also formulated in the noncommutative setting. As far as we know very little is known in this case. However, some intuition has already been developed for the group $SU(2)(SO(3))$. We say that $g_1, \ldots, g_k \in SU(2)$ are Diophantine if there exists a positive constant $D(g_1, \ldots, g_k)$ such that for any $n \geq 1$ and any word $W_n$ in $g_1, \ldots, g_k$ of length $n$

$$||W_n \pm E|| \geq D^{-n}.$$  \hfill (2)

Our interest to the problem of Diophantine approximations on the group $SO(3)$ stems mainly from the question formulated in the list of open problems in the paper of A. Gamburd, D. Jakobson, and P. Sarnak (Problem 4): The Haar generic elements $(g_1, g_2, \ldots, g_k) \in SU(2)^k$ in the sense of measure are Diophantine [GJS]. The paper [GJS] provides an elementary solution of Ruziewicz problem asserting that the Haar measure on $\mathbb{S}^2$ is the unique finitely additive $SO(3)$ invariant measure defined on Lebesgue sets.

In what follows it is more convenient for us to pass to the group $SO(3)$ and restrict our attention to the case of two generators. Consider a subgroup $F$ generated by two elements $A, B \in SO(3)$. The group $SO(3)$ would have a Diophantine property if for almost all rotations $A, B \in SO(3)$ in the sense of measure and all reduced words $W_n \in F$ of length $n$ in $A, B, A^{-1}, B^{-1}$,

$$||W_n - E|| \geq D(A, B)^{-n}.$$  \hfill (2)