Journal of Algebra 477 (2017) 516–539

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

On the dimension of matrix embeddings of torsion-free nilpotent groups

Funda Gul, Armin Weiß [*]

Stevens Institute of Technology, Hoboken, NJ, USA

ARTICLE INFO

Article history:
Received 27 June 2016
Available online 1 February 2017
Communicated by Derek Holt

Keywords:
Nilpotent groups
Nickel's algorithm
Jennings' embedding
Mal'cev basis
Unitriangular matrix group

ABSTRACT

Since the work of Jennings (1955), it is well-known that any finitely generated torsion-free nilpotent group can be embedded into unitriangular integer matrices $UT_N(\mathbb{Z})$ for some N. In 2006, Nickel proposed an algorithm to calculate such embeddings. In this work, we show that if $UT_n(\mathbb{Z})$ is embedded into $UT_N(\mathbb{Z})$ using Nickel's algorithm, then $N \geq 2^{n/2-2}$ if the standard ordering of the Mal'cev basis (as in Nickel's original paper) is used. In particular, we establish an exponential worst-case running time of Nickel's algorithm.

On the other hand, we also prove a general exponential upper bound on the dimension of the embedding by showing that for any torsion free, finitely generated nilpotent group the matrix representation produced by Nickel's algorithm has never larger dimension than Jennings' embedding. Moreover, when starting with a special Mal'cev basis, Nickel's embedding for $UT_n(\mathbb{Z})$ has only quadratic size. Finally, we consider some special cases like free nilpotent groups and Heisenberg groups and compare the sizes of the embeddings.

[*] Corresponding author.
E-mail address: armin.weiss@fmi.uni-stuttgart.de (A. Weiß).

http://dx.doi.org/10.1016/j.jalgebra.2017.01.027
0021-8693/© 2017 Elsevier Inc. All rights reserved.

1. Introduction

A classical result due to Jennings [5] shows that every finitely generated torsion-free nilpotent group (τ-group) can be embedded into some group of unitriangular matrices over the integers. Embeddings into matrix groups are desirable for various reasons: they allow to apply the powerful tool of linear algebra to prove new results about the groups; moreover, many computations can be performed efficiently with matrices – in particular, the word problem for linear groups can be solved in logarithmic space [8]. Embeddings of nilpotent groups are the basic building blocks for embeddings of polycyclic groups (see e. g. [9]), which are of particular interest because of their possible application in non-commutative cryptography [2]. For instance, in [12], matrix embeddings were used to break such a cryptosystem based on the conjugacy problem in a certain class of polycyclic groups.

Since Jennings' embedding (1955), several other descriptions of such embeddings [4,6] have been given and also algorithms [9,1,13] for computing such embeddings from a given Mal'cev presentation. The presumably most efficient of these algorithms is due to Nickel [13]: it uses the multiplication polynomials associated to the Mal'cev basis in order to compute a G-submodule of the dual space of the group algebra $\mathbb{Q}G$ – an approach similar to the description of the embedding in [6, Section 17.2]. The multiplication polynomials were first described by Hall [4]; they can be computed with the *Deep Thought* algorithm [7].

Up to now there are no bounds known neither on the running time nor on the dimension of the embedding obtained by Nickel's algorithm. In [3], a polynomial bound for both is claimed; however, there is a gap in the proof. Indeed, here we prove these results to be wrong: our main result (Theorem 3.9) establishes the lower bound of $N \geq 2^{n/2-2}$ for the embedding of $UT_n(\mathbb{Z})$ (with the standard Mal'cev basis as in Nickel's paper) into $UT_N(\mathbb{Z})$ computed by Nickel's algorithm. In particular, we establish an exponential blow-up for the dimension, which also implies an exponential running time since the output has to be written down. On the other hand, we show the upper bound $N \leq 3^n$. Moreover, by reordering the Mal'cev basis of $UT_n(\mathbb{Z})$, Nickel's algorithm produces an embedding of size only $\mathcal{O}(n^2)$. Our exponential lower bounds also imply that for breaking cryptographic systems based on polycyclic groups the usage of matrix embeddings (at least with the known algorithms to compute them) might not be feasible if the platform group is properly chosen (with nilpotent subgroups of high class).

We also prove a general upper bound on Nickel's embedding and show that for any torsion-free nilpotent group the dimension of Nickel's embedding is never larger than the dimension obtained by Jennings' embedding. In order to do so, we derive a general bound on the degree (or more precisely, weight) of the multiplication polynomials, which follows by a length argument on the words appearing during the collection process.

Moreover, in Section 6 we consider other special classes of groups and compare Nickel's and Jennings' embedding: in free nilpotent groups both embeddings have approximately the same dimension. In contrast, for generalized Heisenberg groups Nickel's algorithm