

CAN YOU COMPUTE THE OPERATOR NORM?

TOBIAS FRITZ, TIM NETZER, AND ANDREAS THOM

(Communicated by Marius Junge)

ABSTRACT. In this note we address various algorithmic problems that arise in the computation of the operator norm in unitary representations of a group on a Hilbert space. We show that the operator norm in the universal unitary representation is computable if the group is residually finite-dimensional or amenable with a decidable word problem. Moreover, we relate the computability of the operator norm on the group $F_2 \times F_2$ to Kirchberg's QWEP Conjecture, a fundamental open problem in the theory of operator algebras.

1. INTRODUCTION

In this article we study various algorithmic problems related to the computation of the operator norm on group rings. Let us take some time and state the setup more precisely. Let A be a finite alphabet, let F_A be the free group on the set A , and let $R \subset F_A$ be a subset. We denote by $\Gamma := \langle A | R \rangle$ the group which is generated by the set A subject to relations R . The group Γ is equipped with a natural surjection $F_A \rightarrow \Gamma$, which we denote by $g \mapsto \bar{g}$. The kernel of this surjection is $\langle\langle R \rangle\rangle$, the normal subgroup generated by the set R . A triple (Γ, A, R) , as above, is called a *presented group*; it is called finitely presented if R is finite. We denote the integral group ring of a group Γ by $\mathbb{Z}\Gamma$, and the complex group ring by $\mathbb{C}\Gamma$. For $a \in \mathbb{Z}F_A$, we denote by \bar{a} its canonical image in $\mathbb{Z}\Gamma$.

We want to study the operator norm of \bar{a} , considered as an element in the universal group C^* -algebra $C_u^*\Gamma$ and the reduced group C^* -algebra $C_\lambda^*\Gamma$. We denote the universal C^* -norm on $\mathbb{C}\Gamma$ by $\|\cdot\|_u$ and the operator norm associated with the left-regular representation by $\|\cdot\|_\lambda$; more generally, we write $\|\cdot\|_\varphi$ for the semi-norm associated to any unitary representation $\varphi: \Gamma \rightarrow U(H_\varphi)$:

$$\|\varphi(a)\|_\varphi := \sup \{ \|\varphi(a)\xi\| \mid \xi \in H_\varphi, \|\xi\| \leq 1 \}.$$

For more information about these notions, consult the appendices in [5]. It is well-known that $\|\cdot\|_\lambda \leq \|\cdot\|_u$ with equality if and only if Γ is amenable; this is Kesten's theorem [15]. The natural trace on $\mathbb{C}\Gamma$ is denoted by $\tau: \mathbb{C}\Gamma \rightarrow \mathbb{C}$; it is given by the formula $\tau\left(\sum_{g \in \Gamma} a_g g\right) = a_e$. We denote the cone of hermitian squares in $\mathbb{C}\Gamma$ by $\Sigma^2\mathbb{C}\Gamma$, that is:

$$\Sigma^2\mathbb{C}\Gamma := \left\{ \sum_{i=1}^n a_i^* a_i \mid n \in \mathbb{N}, a_i \in \mathbb{C}\Gamma \right\}.$$

Received by the editors July 12, 2012 and, in revised form, January 15, 2013.
2010 *Mathematics Subject Classification*. Primary 43A20.

©2014 American Mathematical Society
Reverts to public domain 28 years from publication

We say that a real number $\alpha \in \mathbb{R}$ is *computable* if it can be approximated to any precision with rational numbers by a Turing machine or, equivalently, if there is an algorithm which produces two sequences of rational numbers $(p_n)_{n \in \mathbb{N}}$ and $(q_n)_{n \in \mathbb{N}}$ such that $(p_n)_{n \in \mathbb{N}}$ is monotone increasing, $(q_n)_{n \in \mathbb{N}}$ is monotone decreasing, and $\sup_n p_n = \alpha = \inf_n q_n$. Most numbers that we usually think of are computable by their very definition. Although there are only countably many computable numbers since there are only countably many possible algorithms, one has to think hard to give an explicit example of an uncomputable number. One is Chaitin's constant, whose binary expansion $\sum_{n \in \mathbb{N}} \varepsilon_n 2^{-n}$ encodes the halting problem. Here, $\varepsilon_n \in \{0, 1\}$ depending on whether the n -th machine in some explicit list of all Turing machines halts. Chaitin's constant is definable in the language of set theory but not computable. It is important for us that numbers defined in a much simpler language, the first-order language of real closed fields, *are* computable; this is Tarski's famous theorem about quantifier elimination, which we will apply several times. The distinction between computable and definable numbers goes back to Turing [33].

More generally, we want to speak about computable functions depending on an element in the integral group ring of a group.

Definition 1.1. Let (Γ, A, R) be a presented group. We say that a function $f: \mathbb{Z}\Gamma \rightarrow \mathbb{R}$ is computable if there exists an algorithm that takes as input an element $a \in \mathbb{Z}F_A$ and produces two sequences of rational numbers $(p_n)_{n \in \mathbb{N}}$ and $(q_n)_{n \in \mathbb{N}}$ such that

- (1) $(p_n)_{n \in \mathbb{N}}$ is monotone increasing,
- (2) $(q_n)_{n \in \mathbb{N}}$ is monotone decreasing, and
- (3) $\sup_n p_n = f(\bar{a}) = \inf_n q_n$.

Obviously, the values of a computable function $f: \mathbb{Z}\Gamma \rightarrow \mathbb{R}$ are all computable real numbers; the converse does not hold. Many decision problems in group theory have been studied, the most famous being the *word problem* [6, 7, 26]. Here, given a finitely presented group (Γ, A, R) , the task is to find an algorithm which decides whether an input $g \in F_A$ satisfies $\bar{g} = e_\Gamma$ or not.

Remark 1.2. Note that the computability of the functions $a \mapsto \|a\|_u$ or $a \mapsto \|a\|_\lambda$ immediately gives a solution to the word problem. Indeed, for $g \in F_A$, we have either $\|\bar{g} - e_\Gamma\| = 0$ or $\|\bar{g} - e_\Gamma\| \geq 1$, depending on whether g is trivial in Γ or not. Hence, a computation of the operator norm in the sense above gives a decision procedure.

Our first result is the following converse of the previous remark for the class of amenable groups.

Theorem 1.3. *Let (Γ, A, R) be a finitely presented amenable group. Then, the word problem for (Γ, A, R) is decidable if and only if the function*

$$\mathbb{Z}\Gamma \ni a \mapsto \|a\|_\lambda \in \mathbb{R}$$

is computable.

In general, amenable groups need not have a decidable word problem, as was shown by Kharlampovich [16].

Generally speaking, while it is easy for a given $g \in F_A$ to find a certificate that $\bar{g} = e_\Gamma$, if that is the case, it is hard (and sometimes impossible) to get a certificate that $\bar{g} \neq e_\Gamma$, if that is the case. In order to provide the second certificate, one needs additional information about Γ . Let us recall a fundamental result of Mostowski and McKinsey and explain its proof, since it serves as a motivation for our work.

Theorem 1.4 (Mostowski [25], McKinsey [23]). *Every finitely presented residually finite group (Γ, A, R) has a decidable word problem.*

Proof. The algorithm does a parallel search for $w \in \langle\langle R \rangle\rangle$ and for finite quotients $\varphi: \Gamma \rightarrow H$ with $\varphi(w) \neq 0$. The first search is done by enumerating all elements in $\langle\langle R \rangle\rangle$ and comparing them with w . The second search is done by enumerating all A -tuples of permutations, checking whether they satisfy all relations in R , and computing w on the A -tuple of permutations. Since Γ is residually finite, at some point one of the searches must terminate. \square

Therefore, showing undecidability of the word problem is one strategy (maybe not the most promising) for proving that a group is not residually finite. The converse is not true: the Baumslag-Solitar group $BS(2, 3)$ is not residually finite [3], but has, as a 1-relator group, a decidable word problem [21].

In this note, we study the property of a group being residually finite-dimensional (RFD) (see Definition 2.4), a certain strengthening of residual finiteness, and show that it implies computability of the norm in the universal group C^* -algebra. The largest known class of RFD groups contains free groups, Fuchsian groups and many Kleinian groups (see Lubotzky-Shalom [20] and the remarks after Definition 2.4). For more information on property RFD and related notions consult Brown-Ozawa [9]. Our main result is the following theorem.

Theorem 1.5. *Let (Γ, A, R) be a finitely presented RFD group. Then, Γ has a decidable word problem and the function*

$$\mathbb{Z}\Gamma \ni a \mapsto \|a\|_u \in \mathbb{R}$$

is computable.

The proof of Theorem 1.3 and Theorem 1.5 follow closely the basic idea of the proof of Theorem 1.4 that we have outlined above. Whereas there is always a sequence of upper bounds, a sequence of lower bounds requires more information about the group and can be provided if the group is RFD or amenable with a decidable word problem.

It is a famous open problem in the theory of operator algebras whether the group $F_2 \times F_2$ is RFD, now called Kirchberg's Conjecture [17]. In principle, a strategy to disprove Kirchberg's Conjecture is to show that the norm in the universal group C^* -algebra of $F_2 \times F_2$ is in fact not computable. This is not as unreasonable as it may sound, since there are many relatively easy computational problems related to $F_2 \times F_2$, which are known to be unsolvable (see the remarks in Section 4).

Let us return to the problem of actually computing the operator norm. Once one is in the situation that some number, such as the operator norm of some specific element $a \in \mathbb{Z}\Gamma$, is computable, one has to face the following problem. Suppose another computable number α is given in the form of a machine that computes it. Can we decide whether $\|a\| = \alpha$? This again is hard, and in general it is impossible to decide if two machines compute the same number. However, we can circumvent this problem in special cases.

Theorem 1.6. *Let F_A be a free group on the finite set A . Then there is an algorithm which takes as input $a \in \mathbb{Z}F_A$ and computes a definition of $\|a\|$ in the first order language of real closed fields. In particular, if α is any other number defined in the first order language of real closed fields, then it is decidable whether $\|a\| = \alpha$ holds or not.*

Thanks to Tarski’s theorem, the definition of some number α in the first order language of real closed fields takes the form

$$(p(\alpha) = 0) \wedge (q_1(\alpha) > 0) \wedge \cdots \wedge (q_n(\alpha) > 0)$$

for some $n \in \mathbb{N}$ and polynomials $p, q_1, \dots, q_n \in \mathbb{Z}[t]$.

Theorem 1.6 can be used to give algorithms that decide some useful properties. For example, it is decidable whether $a \in \mathbb{Z}F_A$ is invertible in $C_u^*(F_A)$ or not. It is not known at the moment whether this result extends to all RFD groups. There are other variations on Theorem 1.6. For example we can show, using similar techniques, that there is an algorithm that takes a self-adjoint element $a \in \mathbb{Z}F_A$ as input and produces definitions of real numbers μ_1, μ_2 such that the spectrum of a in $C_u^*(F_A)$ has the form $[\mu_1, \mu_2] \subset \mathbb{R}$.

The article is organized as follows. In Section 2, we study the norm in the universal representation and prove Theorem 1.5 and Theorem 1.6. Theorem 1.3 is proved in Section 3. In Section 4, we discuss a relation with Kirchberg’s QWEP Conjecture and speculate about a relationship with some algorithmic problems related to the group $F_2 \times F_2$, which are known to be undecidable.

2. COMPUTABILITY OF THE NORM IN THE UNIVERSAL REPRESENTATION

The following lemma provides the key to the computation of a sequence of upper bounds. It can be regarded as a special case of a strict Positivstellensatz due to Schmüdgen [31].

Lemma 2.1. *Let $a \in \mathbb{Z}\Gamma$. Then,*

$$\|a\|_u = \inf \{ \lambda \in \mathbb{R}_{\geq 0} \mid \lambda^2 - a^*a \in \Sigma^2\mathbb{C}\Gamma \}.$$

Proof. Clearly, $\Sigma^2\mathbb{C}\Gamma \subseteq (C_u^*\Gamma)_+ := \{x^*x \mid x \in C_u^*\Gamma\}$. Conversely, we claim that $x + \varepsilon 1 \in \Sigma^2\mathbb{C}\Gamma$ for every $x \in (C_u^*\Gamma)_+ \cap \mathbb{C}\Gamma$ and $\varepsilon > 0$. If this were not the case for some x , then the Riesz extension theorem [2] would guarantee the existence of a linear map $\varphi : \mathbb{C}\Gamma \rightarrow \mathbb{C}$ with $\varphi(\Sigma^2\mathbb{C}\Gamma) \subseteq \mathbb{R}_+$ and $\varphi(x) < 0$. For this, it is essential that 1 is an algebraic interior point in $\Sigma^2\mathbb{C}\Gamma$, as shown in [11]. The GNS construction turns this φ into a unitary representation π_φ with the property that $\pi_\varphi(x) \not\geq 0$ so that $x \notin (C_u^*\Gamma)_+$. \square

If (Γ, A, R) is a finitely presented group, then one can find a convergent sequence of upper bounds on $\|a\|_u$ as follows. Let $F_{A,n}$ be the set of elements in F_A with word length less than or equal to n . Let us write $Q(A, R)$ for the quadratic module in $\mathbb{C}F_A$ generated by $\{1 - r \mid r \in R\}$. More precisely, we set

$$Q(A, R) := \left\{ \sum_{r \in R \cup \{0\}} \sum_{k=1}^{n_r} b_{r,k}^* (1 - r) b_{r,k} \mid n_i \in \mathbb{N}, b_{i,k} \in \mathbb{C}F_A, \forall i \in R \cup \{0\} \right\}.$$

Obviously, $Q(A, R)$ is a convex cone, and functionals on $\mathbb{C}F_A$ which are positive on $Q(A, R)$ are in bijection with positive functionals on $\mathbb{C}\Gamma$. In particular, the proof of Lemma 2.1 yields

$$(1) \quad \|\bar{a}\|_u = \inf \{ \lambda \in \mathbb{R}_{\geq 0} \mid \lambda^2 - a^*a \in Q(A, R) \}$$

for all $a \in \mathbb{Z}F_A$. Here, \bar{a} denotes the canonical image of a in $\mathbb{Z}\Gamma$.

We define $Q_n(A, R)$ to be the subset of those elements in $Q(A, R)$ which have a representation with all $b_{i,k} \in \mathbb{C}F_{A,n}$. Then $Q_n(A, R)$ is finite-dimensional, and $\bigcup_n Q_n(A, R) = Q(A, R)$. In fact,

$$Q_n(A, R) = \left\{ \sum_{r \in R \cup \{0\}} \sum_{g, h \in F_{A,n}} C_{r,g,h} g^{-1}(1-r)h \mid (C_{r,g,h})_{g,h \in \Gamma_n} \in \bigoplus_{r \in R \cup \{0\}} M_{F_{A,n}}(\mathbb{C})_+ \right\}.$$

For $a \in \mathbb{Z}F_A$, we consider all $n \geq n_0$ where n_0 is such that $a \in \mathbb{C}F_{A,n_0}$ and $\Lambda - a^*a \in Q_{n_0}(A, R)$ for some $\Lambda \in \mathbb{R}$. Then by equation (1),

$$(2) \quad \|a\|_u^2 \leq \min \left\{ \Lambda \in \mathbb{R} \mid \begin{array}{l} \exists (C_{r,g,h})_{g,h \in \Gamma_n} \in \bigoplus_{r \in R \cup \{0\}} M_{F_{A,n}}(\mathbb{C})_+ \\ \text{with } \Lambda - a^*a = \sum_{r \in R \cup \{0\}} \sum_{g,h} C_{r,g,h} g^{-1}(1-r)h \end{array} \right\},$$

where the right-hand side is now just a semidefinite programming problem in matrices $\bigoplus_{r \in R \cup \{0\}} M_{F_{A,n}}(\mathbb{C})$. As shown in equation (1), this bound becomes tight for $n \rightarrow \infty$. So, computing the value of the semidefinite program by bounding it from above with an accuracy of, say, $1/n$ provides a convergent sequence of upper bounds on $\|a\|_u$. For more details on semidefinite programming see, for example, [34]. This shows the following:

Corollary 2.2. *For any finitely presented group (Γ, A, R) there is an algorithm computing a convergent sequence of upper bounds on $\|\cdot\|_u$ on $\mathbb{Z}\Gamma$.*

Semidefinite programming duality provides another point of view on (2). We claim that

$$(3) \quad \|a\|_u^2 \leq \max \{ \varphi(a^*a) : \varphi : \mathbb{C}F_A \rightarrow \mathbb{C}, \varphi(Q_n(A, R)) \subseteq \mathbb{R}_{\geq 0}, \varphi(1) = 1 \},$$

where the right-hand side is a semidefinite program dual to (2) for $n \geq n_0$, and the two optimal values coincide. To see this, note first that both semidefinite programs are feasible: (2) is feasible by the assumption $n \geq n_0$; (3) is feasible since $(-1) \notin Q_n(A, R)$ and by the Hahn-Banach theorem. Therefore, for any feasible solutions $(C_{r,g,h})_{g,h}$ and φ ,

$$(4) \quad \varphi(a^*a) \leq \Lambda - \varphi \left(\sum_{r \in R \cup \{0\}} \sum_{g,h} C_{r,g,h} g^{-1}h \right) \leq \Lambda.$$

We claim that there are φ and $(C_{r,g,h})_{g,h}$ for which this bound is tight. This is so since $\Lambda - a^*a$ lies, for the optimal Λ , on the boundary of the cone $Q_n(A, R)$ so that there exists a functional $\varphi : \mathbb{C}F_{A,n} \rightarrow \mathbb{C}$ with $\varphi(\Lambda - a^*a) = 0$. This φ is optimal since $\varphi(a^*a) = \Lambda$, which saturates (4).

We end the discussion of semidefinite programming by noting that these ideas not only apply to the universal C^* -norm on group rings, but on any $*$ -algebra with a finite presentation in terms of generators and equality or positivity relations for linear combinations of words in those generators. This has been worked out in

more detail in [29] as “noncommutative polynomial optimization” (note that the “primal” and “dual” conventions of [29] are opposite to ours). Many applications and particular cases had already been studied earlier; this includes hierarchies of semidefinite programs for commutative moment problems [18] and noncommutative moment problems arising in quantum information theory [28].

If there was any way to understand efficiently how fast the sequence of upper bounds converges, then one could turn Corollary 2.2 into an actual computation of the operator norm in the sense of Definition 1.1. However, this seems to be out of reach even for reasonable groups and is impossible in general, as it would imply decidability of the word problem by Remark 1.2. This is in contrast to the commutative case, for which convergence bounds have been derived [8, 12]. In order to provide interesting lower bounds on the norm in the universal representation, we have to make additional assumptions on Γ .

In the following, we need basic properties of the unitary dual of a discrete group. For details about the unitary dual and the Fell topology on it, consult the informative appendices in [5].

Lemma 2.3. *Let Γ be a group and let Φ be a set of unitary representations which is dense in the unitary dual of Γ . Then for every $a \in \mathbb{Z}\Gamma$,*

$$\|a\|_u = \sup \{ \|\varphi(a)\|_\varphi \mid \varphi \in \Phi \}.$$

Proof. This is well-known and an immediate consequence of the definition of the Fell topology on the unitary dual. \square

Let us now give a definition of property RFD.

Definition 2.4. A group Γ is called *residually finite-dimensional (RFD)* if the set of finite-dimensional unitary representations is dense in the unitary dual of Γ .

Note that if Γ is finitely generated and RFD, then finite-dimensional representations must separate the elements of Γ , and Γ follows to be residually finite by Mal’cev’s theorem [22].

Finitely generated Fuchsian groups and fundamental groups of closed hyperbolic 3-manifolds which fiber over the circle are known to be RFD; see [20]. Indeed, it is well-known that free groups are RFD; see for example Theorem 2.2 in [20]. Theorem 2.8 in [20] shows that surface groups and fundamental groups of closed hyperbolic 3-manifolds that fiber over the circle have RFD. Now, it is easy to see that RFD passes to finite index extensions. This implies the claim for Fuchsian groups since every Fuchsian group contains a free group or a surface group with finite index. That every fundamental group of a closed hyperbolic 3-manifold admits a subgroup of finite index that fibers over the circle is known as Thurston’s Virtual Fibration Conjecture.

We write f for the direct sum of all finite-dimensional unitary representations of Γ . The following observation can be regarded as an alternative definition of RFD:

Lemma 2.5. *Γ is RFD if and only if $\|\cdot\|_u = \|\cdot\|_f$ on $\mathbb{Z}\Gamma$.*

Proof. Again by definition of the Fell topology, we know that $\|\cdot\|_u = \|\cdot\|_f$ on $\mathbb{C}\Gamma$ if and only if Γ is RFD. By homogeneity of norms and density of the inclusion $\mathbb{Q} \subseteq \mathbb{R}$, the assumption $\|\cdot\|_u = \|\cdot\|_f$ on $\mathbb{Z}\Gamma$ implies that this equality also holds on $\mathbb{R}\Gamma$, and the problem is to show that this implies the equality on all of $\mathbb{C}\Gamma$.

We decompose $\mathbb{C}\Gamma = \mathbb{R}\Gamma \oplus i \cdot \mathbb{R}\Gamma$. By assumption, the two norms coincide on each of the two summands; moreover, for $a, b \in \mathbb{R}\Gamma$,

$$\|a + ib\|_u = \|a - ib\|_u, \quad \|a + ib\|_f = \|a - ib\|_f,$$

since every representation of Γ has a complex conjugate, and taking complex conjugates preserves finite-dimensionality. Now it follows from elementary estimates like [13, Prop. 5.6] that $\|\cdot\|_u$ and $\|\cdot\|_f$ differ on $\mathbb{C}\Gamma$ at most by a factor of 2. So,

$$\|\cdot\|_f \leq \|\cdot\|_u \leq 2\|\cdot\|_f.$$

In particular, the C^* -completions $C_u^*\Gamma$ and $C_f^*\Gamma$ are canonically isomorphic and the canonical surjection

$$\varphi : C_u^*\Gamma \rightarrow C_f^*\Gamma$$

is an isomorphism. Now the assertion follows from the uniqueness of the norm on a C^* -algebra. \square

We are now ready to prove Theorem 1.5.

Proof of Theorem 1.5. The first assertion is clear by Theorem 1.4, since the assumption implies that Γ is residually finite.

In view of Corollary 2.2 it remains to provide a convergent sequence of lower bounds on the operator norm in the universal representation. Let $a \in \mathbb{Z}F_A$. Let $n \in \mathbb{N}$ and consider the set

$$X(n) = \{(u_a)_{a \in A} \in U(n)^A \mid r((u_a)_{a \in A}) = 1 \forall r \in R\} \subseteq U(n)^A.$$

Clearly, $X(n)$ is a compact real algebraic subset of $\mathbb{R}^{|A| \cdot 2n^2}$. Denote by $D(n) = \{\xi \in \mathbb{C}^n \mid \|\xi\| \leq 1\}$ and the function

$$f_n : X(n) \times D(n) \rightarrow \mathbb{R}, \quad f_n((u_a)_{a \in A}, \xi) := \|a((u_a)_{a \in A})\xi\|^2.$$

Denote the maximum of f_n on $X(n) \times D(n)$ by α_n . By the previous lemmas and the assumptions on Γ , we have

$$\|\bar{a}\|_u = \sup \left\{ \alpha_n^{1/2} \mid n \in \mathbb{N} \right\}.$$

Thanks to Tarski's real quantifier elimination [32], each α_n is computable, and therefore $(\alpha_n^{1/2})_{n \in \mathbb{N}}$ is the required sequence of lower bounds. This proves the claim. \square

Again, note that this theorem and its proof directly generalize from group $*$ -algebras to arbitrary finitely presented $*$ -algebras.

Question 2.6. *The group $\Gamma = SL_3(\mathbb{Z})$ is known not to be RFD (see [4]). Is the function*

$$\mathbb{Z}\Gamma \ni a \mapsto \|a\|_u \in \mathbb{R}$$

computable?

We now turn to the proof of Theorem 1.6. We need the following lemma.

Lemma 2.7. *Let $a \in \mathbb{Z}F_A$, $n = |A|$, and let $d \in \mathbb{N}$ be the length of the longest word appearing in the support of a . There exists a unitary representation $\pi : F_A \rightarrow U(k)$ of dimension $k := 2(2n)^d$ and a unit vector $\xi \in \mathbb{C}^k$ such that $\|a\|_u = \|\pi(a)\xi\|_\pi$.*

Proof. The proof is an application of what is known as Choi’s trick [10, Theorem 7], which gives an efficient proof that the group $\Gamma = F_A$ is RFD. Let $a \in \mathbb{Z}\Gamma$. It is a standard consequence of the compactness of the state space of $C_u^*\Gamma$ that the operator norm $\|a\|_u$ is achieved at some vector in some unitary representation. Let $\sigma: F_A \rightarrow U(H_\sigma)$ be a unitary representation and let $\xi' \in H_\sigma$ be a unit vector with $\|a\|_u = \|\sigma(a)\xi'\|_\sigma$. Consider H , the linear span of $\sigma(g)\xi$ for all g with lengths less than or equal to d . The dimension of H is at most $2n^d$. Let p be the orthogonal projection from H_σ onto H and denote the generators of F_A by v_1, \dots, v_n .

We set

$$u_i := \begin{pmatrix} p\sigma(v_i)p & \sqrt{1_H - p\sigma(v_i)p\sigma(v_i)^*p} \\ \sqrt{1_H - p\sigma(v_i)^*p\sigma(v_i)p} & -p\sigma(v_i)^*p \end{pmatrix} \in \mathcal{L}(H \oplus H).$$

It is easy to check that u_1, \dots, u_n are unitary, and we let π be the unitary representation on $H \oplus H$ associated with them. Again, it is easy to check that $\pi(a)(\xi', 0)^t = (\sigma(a)\xi, 0)$, and hence $\|a\|_u = \|\pi(a)\xi\|_\pi$ for the unit vector $\xi = (\xi', 0)^t$. This finishes the proof. \square

We are now ready to prove Theorem 1.6.

Proof of Theorem 1.6. Using the notation of the proof of Theorem 1.5, Lemma 2.7 gives that $\|a\|_u = \alpha_k$ for some sufficiently large and computable integer k . Clearly, α_k is defined in the first order language of real closed fields. Moreover, the equation $\alpha = \alpha_k$ is decidable if α is defined in the same language, again thanks to Tarski’s theorem. \square

As a corollary to Theorem 1.6, we can now solve algorithmic problems that require precise information about the spectrum of some element in the integral group ring.

Corollary 2.8. *There is an algorithm that takes as input $a \in \mathbb{Z}F_A$ and decides whether a is invertible in the universal group C^* -algebra.*

Proof. For $a = \sum_g a_g g \in \mathbb{Z}F_A$, we write $\|a\|_1 := \sum_g |a_g|$. It is clear that $\|a\|_u \leq \|a\|_1$ for all $a \in \mathbb{Z}F_A$. Now, the element $a \in \mathbb{Z}F_A$ is invertible in $C_u^*F_A$ if and only if $a^*a \in \mathbb{Z}F_A$ is invertible. Let $\Lambda \in \mathbb{Z}$ be a computable upper bound for $\|a^*a\|_u$ such as $\|a\|_1^2$. Then the spectral theorem implies that $\|\Lambda - a^*a\|_u = \Lambda$ if and only if a^*a is not invertible in $C_u^*F_A$. This proves the claim, since Theorem 1.6 provides a decision procedure for this equality. \square

3. LOWER BOUNDS ON THE NORM IN THE LEFT-REGULAR REPRESENTATION

In this section we provide a convergent sequence of lower bounds on the norm in the left-regular representation. In the case of amenable groups, this leads to a computation of the natural norm on the integral group ring, using Corollary 2.2 and the fact that $\|\cdot\|_\lambda = \|\cdot\|_u$. Note that formulas for norms in left-regular representations for certain classes of groups and elements have already been obtained in [1, 19] for example.

Recall that the group ring $\mathbb{Z}\Gamma$ naturally comes equipped with the trace

$$\tau: \mathbb{Z}\Gamma \rightarrow \mathbb{Z}, \quad \sum_g a_g g \mapsto a_e,$$

which extends uniquely to a tracial state on $C_\lambda^*\Gamma$. This trace is faithful; i.e., we have that $\tau(a^*a) = 0$ implies $a = 0$. The following result is well-known, and we include a proof for convenience.

Lemma 3.1. *Let $a \in \mathbb{Z}\Gamma$. Then,*

$$\|a\|_\lambda = \sup \left\{ \tau(b^*a^*ab)^{1/2} \mid b \in \mathbb{C}\Gamma, \tau(b^*b) \leq 1 \right\} = \sup \left\{ \tau((a^*a)^n)^{1/2n} \mid n \in \mathbb{N} \right\}.$$

Proof. By definition, $\ell_2(\Gamma)$ is the completion of $\mathbb{C}\Gamma$ with respect to the norm $b \mapsto \tau(b^*b)^{1/2}$, and it carries a natural action of Γ by left multiplication. This directly implies the first equation.

We now consider the second equation. The inequality $\tau((a^*a)^n) \leq \|a^*a\|_\lambda^n \leq \|a\|_\lambda^{2n}$ is clear, so that the main task is proving the other direction. We work in the group von Neumann algebra $\mathcal{N}\Gamma$. Fix any $\varepsilon > 0$ and consider the spectral projection p defined by applying Borel functional calculus to a^*a with respect to the indicator function of the interval $[\|a^*a\|_\lambda - \varepsilon, \|a^*a\|_\lambda]$. Then $a^*a \geq (\|a^*a\|_\lambda - \varepsilon)p$, so that

$$\tau((a^*a)^n) \geq \tau((\|a^*a\|_\lambda - \varepsilon)^n p) = (\|a^*a\|_\lambda - \varepsilon)^n \tau(p).$$

Faithfulness of τ together with $p \neq 0$ implies $\tau(p) > 0$, so that the right-hand side of

$$\tau((a^*a)^n)^{1/2n} \geq (\|a^*a\|_\lambda - \varepsilon)^{1/2} \tau(p)^{1/2n}$$

tends to $(\|a^*a\|_\lambda - \varepsilon)^{1/2}$ as $n \rightarrow \infty$. The conclusion follows since ε was arbitrary. \square

Note that the proof, and therefore the lemma, applies similarly to any von Neumann algebra equipped with a faithful tracial state τ . We are now ready to prove Theorem 1.3.

Proof of Theorem 1.3. Concerning (1) \Rightarrow (2), Lemma 3.1 provides a convergent sequence of computable lower bounds and Lemma 2.1 a convergent sequence of computable upper bounds. (2) \Rightarrow (1) was essentially answered in Remark 1.2: We are able to algorithmically decide for $g \in F_A$ whether $\|1 - \bar{g}\|_\lambda = 0$ or $\|1 - \bar{g}\|_\lambda \geq 1$, and it is easy to see that one of the two cases must occur. \square

4. RELATION TO THE KIRCHBERG'S QWEP CONJECTURE

Let us finish this note with a question and a relation to some famous open problems in the theory of operator algebras.

Question 4.1. *Consider $A = \{x, y, z, w\}$ and*

$$\Gamma = F_2 \times F_2 = \langle x, y, z, w \mid [x, z], [x, w], [y, z], [y, w] \rangle.$$

Is the function $\mathbb{Z}\Gamma \ni a \mapsto \|a\|_u \in \mathbb{R}$ computable?

Kirchberg's seminal work [17] shows that a positive answer to the famous Connes Embedding Problem is equivalent to $F_2 \times F_2$ being RFD. The question whether $F_2 \times F_2$ (or equivalently $F_n \times F_n$ for any $n \geq 2$) is RFD is generally known as a version of Kirchberg's QWEP Conjecture. Consult [30] and the references therein for more details about these fundamental conjectures. By Theorem 1.5, a positive solution to any of these conjectures would also imply a positive answer to Question 4.1. This elucidates the importance of the computability of $\|\cdot\|_u$ on the group ring $\mathbb{Z}(F_n \times F_n)$: if this norm is not computable, this would refute Connes Embedding Problem and Kirchberg's QWEP Conjecture. On the other side, if this norm is computable, and its computation would even turn out to be practical, this would be very interesting

for applications in quantum information theory concerning the maximal quantum violations of Bell inequalities [14].

We want to end by recalling Mihaïlova's construction from [24], which shows that rather reasonable algorithmic questions, which are known to be solvable for free groups and surface groups, become intractable for products of free groups. Our initial hope was that we might be able to relate the computability of $\|\cdot\|_u$ on $\mathbb{Z}(F_n \times F_n)$ to the decidability of some of these decision problems for $F_n \times F_n$, which have been studied so extensively. In particular, the hope was to relate it to the *membership problem* for finitely generated subgroups of $F_n \times F_n$. In general, for a subgroup $\Lambda \subset \Gamma$, the membership problem takes some $g \in \Gamma$ as input and asks us to decide whether $g \in \Lambda$ or $g \notin \Lambda$; typically, one assumes that the word problem for Γ is decidable and Λ is finitely generated by some finite set which is part of the input. Mihaïlova's construction [24] provides examples of finitely generated subgroups of $F_n \times F_n$ for which this problem is undecidable. Let $\Gamma = \langle g_1, \dots, g_n | R \rangle$ be a finitely presented group, let $\pi: F_n \rightarrow \Gamma$ be the natural surjection, and consider the kernel pair

$$(5) \quad \Lambda := \{(g, h) \in F_n \times F_n \mid \pi(g) = \pi(h)\}.$$

It is easy to see that the subgroup $\Lambda \subset F_n \times F_n$ is generated by $R \times \{e\}$ and a diagonal copy of F_n . Hence, $\Lambda \subset F_n \times F_n$ is finitely generated by some explicit set of generators. Moreover, the word problem for the finitely presented group Γ is equivalent to the membership problem for the inclusion $\Lambda \subset F_2 \times F_2$. Indeed, $(v, w) \in \Lambda$ if and only if $\pi(v^{-1}w) = e$ in Γ . Combining this with the existence of finitely presented groups with undecidable word problem [3, 16, 27], Mihaïlova showed:

Proposition 4.2 (Mihaïlova). *The membership problem for finitely generated subgroups of $F_n \times F_n$ is not decidable for any $n \geq 2$.*

We think that this result supports the point of view that a positive answer to Question 4.1 is too much to hope for.

ACKNOWLEDGMENTS

The research of the first author was supported by ERC. Research at Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Economic Development and Innovation. Part of this research was done when the second author visited the University of Leipzig in 2012. We thank the anonymous referee for a helpful comment that improved the statement of Corollary 2.2.

REFERENCES

- [1] Charles A. Akemann and Phillip A. Ostrand, *Computing norms in group C^* -algebras*, Amer. J. Math. **98** (1976), no. 4, 1015–1047. MR0442698 (56 #1079)
- [2] N. I. Akhiezer, *The classical moment problem and some related questions in analysis*, Translated by N. Kemmer, Hafner Publishing Co., New York, 1965. MR0184042 (32 #1518)
- [3] Gilbert Baumslag and Donald Solitar, *Some two-generator one-relator non-Hopfian groups*, Bull. Amer. Math. Soc. **68** (1962), 199–201. MR0142635 (26 #204)
- [4] Bachir Bekka, *Operator-algebraic superrigidity for $SL_n(\mathbb{Z})$, $n \geq 3$* , Invent. Math. **169** (2007), no. 2, 401–425, DOI 10.1007/s00222-007-0050-5. MR2318561 (2008m:46115)
- [5] B. Bekka, P. de la Harpe, and A. Valette, *Kazhdan's property (T)*, New Mathematical Monographs, vol. 11, Cambridge University Press, Cambridge, 2008. MR2415834 (2009i:22001)

- [6] William W. Boone, *The word problem*, Ann. of Math. (2) **70** (1959), 207–265. MR0179237 (31 #3485)
- [7] V. V. Borisov, *Simple examples of groups with unsolvable word problem* (Russian), Mat. Zametki **6** (1969), 521–532. MR0260851 (41 #5471)
- [8] F. Brandão and A.W. Harrow, *Quantum de Finetti theorems under local measurements with applications*, 2012. arXiv:1210.6367.
- [9] Nathaniel P. Brown and Narutaka Ozawa, *C^* -algebras and finite-dimensional approximations*, Graduate Studies in Mathematics, vol. 88, American Mathematical Society, Providence, RI, 2008. MR2391387 (2009h:46101)
- [10] Man Duen Choi, *The full C^* -algebra of the free group on two generators*, Pacific J. Math. **87** (1980), no. 1, 41–48. MR590864 (82b:46069)
- [11] Jakob Cimprič, *A representation theorem for Archimedean quadratic modules on $*$ -rings*, Canad. Math. Bull. **52** (2009), no. 1, 39–52, DOI 10.4153/CMB-2009-005-4. MR2494309 (2010c:46154)
- [12] A. Doherty and S. Wehner, *Convergence of SDP hierarchies for polynomial optimization on the hypersphere*, 2012. arXiv:1210.5048.
- [13] T. Fritz, *Operator system structures on the unital direct sum of C^* -algebras*, 2010. arXiv:1011.1247. To appear in Rocky Mountain J. Math.
- [14] T. Fritz, *Tsirelson’s problem and Kirchberg’s conjecture*, Rev. Math. Phys. **24** (2012), 1250012. MR2928100
- [15] Harry Kesten, *Symmetric random walks on groups*, Trans. Amer. Math. Soc. **92** (1959), 336–354. MR0109367 (22 #253)
- [16] O. G. Kharlampovich, *A finitely presented solvable group with unsolvable word problem* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **45** (1981), no. 4, 852–873, 928. MR631441 (82m:20036)
- [17] Eberhard Kirchberg, *On nonsemisplit extensions, tensor products and exactness of group C^* -algebras*, Invent. Math. **112** (1993), no. 3, 449–489, DOI 10.1007/BF01232444. MR1218321 (94d:46058)
- [18] Jean B. Lasserre, *Global optimization with polynomials and the problem of moments*, SIAM J. Optim. **11** (2000/01), no. 3, 796–817, DOI 10.1137/S1052623400366802. MR1814045 (2002b:90054)
- [19] Franz Lehner, *Computing norms of free operators with matrix coefficients*, Amer. J. Math. **121** (1999), no. 3, 453–486. MR1738412 (2001j:46100)
- [20] Alexander Lubotzky and Yehuda Shalom, *Finite representations in the unitary dual and Ramanujan groups*, Discrete geometric analysis, Contemp. Math., vol. 347, Amer. Math. Soc., Providence, RI, 2004, pp. 173–189, DOI 10.1090/conm/347/06272. MR2077037 (2005e:22011)
- [21] W. Magnus, *Das Identitätsproblem für Gruppen mit einer definierenden Relation* (German), Math. Ann. **106** (1932), no. 1, 295–307, DOI 10.1007/BF01455888. MR1512760
- [22] A. Malcev, *On isomorphic matrix representations of infinite groups* (Russian, with English summary), Rec. Math. [Mat. Sbornik] N.S. **8** (50) (1940), 405–422. MR0003420 (2,216d)
- [23] J. C. C. McKinsey, *The decision problem for some classes of sentences without quantifiers*, J. Symbolic Logic **8** (1943), 61–76. MR0008991 (5,85a)
- [24] K. A. Mihaïlova, *The occurrence problem for free products of groups* (Russian), Mat. Sb. (N.S.) **75** (117) (1968), 199–210. MR0222179 (36 #5231)
- [25] A. Włodzimierz Mostowski, *On the decidability of some problems in special classes of groups*, Fund. Math. **59** (1966), 123–135. MR0224693 (37 #292)
- [26] P. S. Novikov, *On algorithmic unsolvability of the problem of identity* (Russian), Doklady Akad. Nauk SSSR (N.S.) **85** (1952), 709–712. MR0052436 (14,618h)
- [27] P. S. Novikov, *On the algorithmic insolvability of the word problem in group theory*, American Mathematical Society Translations, Ser 2, Vol. 9, American Mathematical Society, Providence, R. I., 1958, pp. 1–122. MR0092784 (19,1158b)
- [28] M. Navascués, S. Pironio, and A. Acín, *A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations*, New Journal of Physics **10** (2008), no. 7, 073013.
- [29] S. Pironio, M. Navascués, and A. Acín, *Convergent relaxations of polynomial optimization problems with noncommuting variables*, SIAM J. Optim. **20** (2010), no. 5, 2157–2180, DOI 10.1137/090760155. MR2650843 (2011d:90075)

- [30] Narutaka Ozawa, *About the QWEP conjecture*, Internat. J. Math. **15** (2004), no. 5, 501–530, DOI 10.1142/S0129167X04002417. MR2072092 (2005b:46124)
- [31] Konrad Schmüdgen, *Noncommutative real algebraic geometry—some basic concepts and first ideas*, Emerging applications of algebraic geometry, IMA Vol. Math. Appl., vol. 149, Springer, New York, 2009, pp. 325–350, DOI 10.1007/978-0-387-09686-5-9. MR2500470 (2010m:13036)
- [32] Alfred Tarski, *A decision method for elementary algebra and geometry*, 2nd ed., University of California Press, Berkeley and Los Angeles, Calif., 1951. MR0044472 (13,423a)
- [33] A. M. Turing, *On computable numbers, with an application to the Entscheidungsproblem*, Proc. London Math. Soc. **S2-42**, no. 1, 230, DOI 10.1112/plms/s2-42.1.230. MR1577030
- [34] *Handbook of semidefinite programming*, Theory, algorithms, and applications, edited by Henry Wolkowicz, Romesh Saigal and Lieven Vandenbergh. International Series in Operations Research & Management Science, 27, Kluwer Academic Publishers, Boston, MA, 2000. MR1778223 (2001k:90001)

PERIMETER INSTITUTE FOR THEORETICAL PHYSICS, 31 CAROLINE STREET NORTH, WATERLOO, ONTARIO, CANADA N2L 2Y5

E-mail address: `tfritz@perimeterinstitute.ca`

UNIVERSITY OF LEIPZIG, PF 100920, 04009 LEIPZIG, GERMANY

E-mail address: `tim.netzer@math.uni-leipzig.de`

UNIVERSITY OF LEIPZIG, PF 100920, 04009 LEIPZIG, GERMANY

E-mail address: `andreas.thom@math.uni-leipzig.de`