The Power of a Single Qubit: Two-Way Quantum Finite Automata and the Word Problem

Zachary Remscrim
Department of Mathematics, MIT, Cambridge, MA, USA
remscrim@mit.edu

Abstract

The two-way finite automaton with quantum and classical states (2QCFA), defined by Ambainis and Watrous, is a model of quantum computation whose quantum part is extremely limited; however, as they showed, 2QCFA are surprisingly powerful: a 2QCFA, with a single qubit, can recognize, with bounded error, the language $L_{eq} = \{a^m b^m : m \in \mathbb{N}\}$ in expected polynomial time and the language $L_{pal} = \{w \in \{a, b\}^* : w \text{ is a palindrome}\}$ in expected exponential time.

We further demonstrate the power of 2QCFA by showing that they can recognize the word problems of many groups. In particular 2QCFA, with a single qubit and algebraic number transition amplitudes, can recognize, with bounded error, the word problem of any finitely generated virtually abelian group in expected polynomial time, as well as the word problems of a large class of linear groups in expected exponential time. This latter class (properly) includes all groups with context-free word problem. We also exhibit results for 2QCFA with any constant number of qubits.

As a corollary, we obtain a direct improvement on the original Ambainis and Watrous result by showing that L_{eq} can be recognized by a 2QCFA with better parameters. As a further corollary, we show that 2QCFA can recognize certain non-context-free languages in expected polynomial time.

In a companion paper, we prove matching lower bounds, thereby showing that the class of languages recognizable with bounded error by a 2QCFA in expected *subexponential* time is properly contained in the class of languages recognizable with bounded error by a 2QCFA in expected *exponential* time.

2012 ACM Subject Classification Theory of computation → Formal languages and automata theory; Theory of computation → Quantum computation theory

Keywords and phrases finite automata, quantum, word problem of a group

Digital Object Identifier 10.4230/LIPIcs.ICALP.2020.139

Category Track B: Automata, Logic, Semantics, and Theory of Programming

Related Version Full version of the paper: `https://eccc.weizmann.ac.il/report/2019/107/`.

Acknowledgements The author would like to express his sincere gratitude to Professor Michael Sipser for many years of mentorship and support, without which this work would not have been possible, to Professors Richard Lipton and David Vogan for very helpful conversations, and to the anonymous reviewers for many suggestions.

1 Introduction

The theory of quantum computation has made amazing strides in the last several decades. Landmark results, like Shor's polynomial time quantum algorithm for integer factorization [31], Grover's algorithm for unstructured search [14], and the linear system solver of Harrow, Hassidim, and Lloyd [15], have provided remarkable examples of natural problems for which quantum computers seem to have an advantage over their classical counterparts. These theoretical breakthroughs have provided strong motivation to construct quantum computers. However, while significant advancements have been made, the experimental

47th International Colloquium on Automata, Languages, and Programming (ICALP 2020).
Editors: Artur Czumaj, Anuj Dawar, and Emanuela Merelli; Article No. 139; pp. 139:1–139:18

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany


quantum computers that exist today are still quite limited, and are certainly not capable of implementing, on a large scale, algorithms designed for general quantum Turing machines. This naturally motivates the study of more restricted models of quantum computation.

In this paper, our goal is to understand the computational power of a small number of qubits, especially the power of a single qubit. To that end, we study two-way finite automata with quantum and classical states (2QCFA), introduced by Ambainis and Watrous [1]. Informally, a 2QCFA is a two-way deterministic finite automaton (2DFA) that has been augmented with a quantum register of constant size, i.e., a constant number of qubits. The quantum part of the machine is extremely limited; however, the model is surprisingly powerful. In particular, Ambainis and Watrous [1] showed that a 2QCFA, using only one qubit, can recognize, with bounded error, the language $L_{eq} = \{a^m b^m : m \in \mathbb{N}\}$ in expected polynomial time and the language $L_{pal} = \{w \in \{a, b\}^* : w \text{ is a palindrome}\}$ in expected exponential time. This clearly demonstrated that 2QCFA are more powerful than 2DFA, which recognize precisely the regular languages [26]. Moreover, as it is known that two-way probabilistic finite automata (2PFA) can recognize L_{eq} with bounded error in exponential time [11], but not in subexponential time [13], and cannot recognize L_{pal} with bounded error in any time bound [10], this result also demonstrated the superiority of 2QCFA over 2PFA.

We investigate the ability of 2QCFA to recognize the word problem of a group. Informally, the word problem for a group G involves determining if the product of a finite sequence of group elements $g_1, \ldots, g_k \in G$ is equal to the identity element of G. Word problems for various classes of groups have a rich and well-studied history in computational complexity theory, as there are many striking relationships between certain algebraic properties of a group G and the computational complexity of its word problem W_G. For example, $W_G \in \mathsf{REG} \Leftrightarrow G$ is finite [3], $W_G \in \mathsf{CFL} \Leftrightarrow W_G \in \mathsf{DCFL} \Leftrightarrow G$ is a finitely generated virtually free group [23], and $W_G \in \mathsf{NP} \Leftrightarrow G$ is a finitely generated subgroup of a finitely presented group with polynomial Dehn function [5].

For a quantum model, such as the 2QCFA, word problems are a particularly natural class of languages to study. There are several results [6, 37, 36] which show that certain (generally significantly more powerful) QFA variants can recognize the word problems of particular classes of groups (see the excellent survey [2] for a full discussion of the many QFA variants). Moreover, there are also results concerning the ability of QFA to recognize certain languages that are extremely closely related to word problems; in fact, the languages L_{eq} and L_{pal} considered by Ambainis and Watrous [1] are each closely related to a word problem.

Fundamentally, the laws of quantum mechanics sharply constrain the manner in which the state of the quantum register of a 2QCFA may evolve, thereby forcing the computation of a 2QCFA to have a certain algebraic structure. Similarly, the algebraic properties of a particular group G impose a corresponding algebraic structure on its word problem W_G. For certain classes of groups, the algebraic structure of W_G is extremely compatible with the algebraic structure of the computation of a 2QCFA; for other classes of groups, these two algebraic structures are in extreme opposition.

In this paper, we show that there is a broad class of groups for which these algebraic structures are quite compatible, which enables us to produce 2QCFA that recognize these word problems. As a corollary, we show that L_{eq} can be recognized by a 2QCFA with better parameters than in the original Ambainis and Watrous result [1].

In a separate paper [27], we establish matching lower bounds on the running time of a 2QCFA (and, more generally, a *quantum Turing machine* that uses sublogarithmic space) that recognizes these word problems, thereby demonstrating the optimality of these results; this allows us to prove that the class of languages recognizable with bounded error by 2QCFA in expected *subexponential* time is properly contained in the class of languages recognizable with bounded error by 2QCFA in expected *exponential* time.

1.1 Statement of the Main Results

We begin by formally defining the word problem of a group; for more extensive background, see, for instance, [21]. Let $F(S)$ denote the free group on the set S. For sets S and R, where $R \subseteq F(S)$, let $\langle R^{F(S)} \rangle$ denote the normal closure of R in $F(S)$; we say that a group G has *presentation* $\langle S|R \rangle$ if $G \cong F(S)/\langle R^{F(S)} \rangle$, in which case we write $G = \langle S|R \rangle$. For a set S, we define the set of formal inverses S^{-1}, such that for each $s \in S$, there is a unique corresponding $s^{-1} \in S^{-1}$, and $S \cap S^{-1} = \emptyset$.

▶ **Definition 1.** Suppose $G = \langle S|R \rangle$, where S is finite. Let $\Sigma = S \sqcup S^{-1}$, let Σ^* denote the free monoid over Σ, let $\phi : \Sigma^* \to G$ denote the natural monoid homomorphism that takes each string in Σ^* to the element of G that it represents, and let 1_G denote the identity element of G. The word problem of G with respect to the presentation $\langle S|R \rangle$ is the language $W_{G=\langle S|R \rangle} = \{w \in \Sigma^* : \phi(w) = 1_G\}$ consisting of all strings that represent 1_G.

Note that if $G = \langle S|R \rangle$, then S (or more precisely the image of S in G under ϕ) is a generating set for G. We say that G is *finitely generated* if it has a generating set S that is finite. If G also has presentation $\langle S'|R' \rangle$, where S' is also finite, then for any complexity class $\mathcal{C}$ closed under inverse homomorphism, $W_{G=\langle S|R \rangle} \in \mathcal{C} \Leftrightarrow W_{G=\langle S'|R' \rangle} \in \mathcal{C}$ [16]. As each complexity class $\mathcal{C}$ considered in this paper is closed under inverse homomorphism, we will use W_G to denote the word problem of a finitely generated group G, and we will write $W_G \in \mathcal{C}$ if $W_{G=\langle S|R \rangle} \in \mathcal{C}$ for some (equivalently, every) presentation $\langle S|R \rangle$ of G with S finite.

We show that, for many groups G, the corresponding word problem W_G is recognized by a 2QCFA with "good" parameters. In order to state these results, we must make use of some terminology and notation concerning 2QCFA and various classes of groups whose word problems are of complexity theoretic interest. We define the 2QCFA model in Section 2. For other definitions and additional background, we refer the reader to the full version of this paper [28]. We use $\mathbb{R}_{>0}$ to denote the positive real numbers.

▶ **Definition 2.** For $T : \mathbb{N} \to \mathbb{N}$, $\epsilon \in \mathbb{R}_{>0}$, $d \in \mathbb{N}$, and $\mathbb{A} \subseteq \mathbb{C}$, let the complexity class $\mathsf{coR2QCFA}(T, \epsilon, d, \mathbb{A})$ consist of all languages $L \subseteq \Sigma^*$ for which there is a 2QCFA M, which has d quantum basis states and transition amplitudes in $\mathbb{A}$, such that, $\forall w \in \Sigma^*$, the following holds: M runs in expected time $O(T(|w|))$, $\Pr[M \text{ accepts } w] + \Pr[M \text{ rejects } w] = 1$, $w \in L \Rightarrow \Pr[M \text{ accepts } w] = 1$, and $w \notin L \Rightarrow \Pr[M \text{ rejects } w] \geq 1 - \epsilon$.

The focus on the transition amplitudes of a 2QCFA warrants a bit of additional justification, as while it is standard to limit the transition amplitudes of a Turing machine in this way, it is common for finite automata to be defined without any such limitation. For many finite automata models, applying such a constraint would be superfluous; for example, the class of languages recognized with bounded error and in expected time $2^{n^{o(1)}}$ by a 2PFA with no restriction at all on its transition amplitudes is precisely the regular languages [9]. However, the power of the 2QCFA model is quite sensitive to the choice of transition amplitudes. A 2QCFA with non-computable transition amplitudes can recognize undecidable languages, with bounded error and in expected polynomial time [29]; whereas, 2QCFA with transition amplitudes restricted to the algebraic numbers $\overline{\mathbb{Q}}$ can only recognize languages in $\mathsf{P} \cap \mathsf{L}^2$, even if permitted unbounded error and exponential time [34]. In particular, the algebraic numbers are arguably the "standard" choice for the permitted transition amplitudes of a quantum Turing machine (QTM). It is desirable for the definition of 2QCFA to be consistent with that of QTMs as such consistency makes it more likely that techniques developed for 2QCFA could be applied to QTMs. Therefore, $\overline{\mathbb{Q}}$ is the the natural choice for the permitted transition amplitudes of a 2QCFA, though we do also consider the impact of allowing transition amplitudes in the slightly broader class $\widetilde{\mathbb{C}} = \overline{\mathbb{Q}} \cup \{e^{\pi i r} : r \in (\overline{\mathbb{Q}} \cap \mathbb{R})\}$.

We begin with a simple motivating example. For a finite alphabet Σ, a symbol $\sigma \in \Sigma$, and a word $w \in \Sigma^*$, let $\#(w, \sigma)$ denote the number of appearances of σ in w. Then the word problem for the group $\mathbb{Z}$ (the integers, where the group operation is addition) is the language $W_{\mathbb{Z}} = \{w \in \{a, b\}^* : \#(w, a) = \#(w, b)\}$. This language is closely related to the language $L_{eq} = \{a^m b^m : m \in \mathbb{N}\}$; in particular, $L_{eq} = (a^*b^*) \cap W_{\mathbb{Z}}$. More generally, the word problem for the group $\mathbb{Z}^k$ (the direct product of k copies of $\mathbb{Z}$) is the language $W_{\mathbb{Z}^k} = \{w \in \{a_1, b_1, \ldots, a_k, b_k\}^* : \#(w, a_i) = \#(w, b_i), \forall i\}$.

Ambainis and Watrous [1] showed that $L_{eq} \in \mathsf{coR2QCFA}(n^4, \epsilon, 2, \widetilde{\mathbb{C}})$, $\forall \epsilon \in \mathbb{R}_{>0}$. We note that the same method would easily imply the same result for $W_{\mathbb{Z}}$, and could be further adapted to produce a similar result for $W_{\mathbb{Z}^k}$. Our first main theorem generalizes and improves upon these results in several ways. Let $\widehat{\Pi}_1$ denote the collections of all finitely generated virtually abelian groups (i.e., all groups that have a finite-index subgroup isomorphic to $\mathbb{Z}^k$, for some $k \in \mathbb{N}$, where $\mathbb{Z}^0$ is the trivial group); we will explain this choice of notation shortly.

▶ **Theorem 3.** *$\exists C \in \mathbb{R}_{>0}$ such that $\forall G \in \widehat{\Pi}_1, \forall \epsilon \in \mathbb{R}_{>0}$, $W_G \in \mathsf{coR2QCFA}(n^3, \epsilon, 2, \widetilde{\mathbb{C}}) \cap \mathsf{coR2QCFA}(n^C, \epsilon, 2, \overline{\mathbb{Q}})$.*

By the above observation that $L_{eq} = (a^*b^*) \cap W_{\mathbb{Z}}$, the following corollary is immediate.

▶ **Corollary 4.** *$\exists C \in \mathbb{R}_{>0}, \forall \epsilon \in \mathbb{R}_{>0}$, $L_{eq} \in \mathsf{coR2QCFA}(n^3, \epsilon, 2, \widetilde{\mathbb{C}}) \cap \mathsf{coR2QCFA}(n^C, \epsilon, 2, \overline{\mathbb{Q}})$.*

The above corollary improves upon the result of Ambainis and Watrous [1] in two distinct senses. Firstly, using the same set of permissible transition amplitudes, our result has a better expected running time. Secondly, our result shows that L_{eq} can be recognized by a 2QCFA with transition amplitudes in $\overline{\mathbb{Q}}$, which still runs in expected polynomial time.

Let CFL denote the context-free languages (languages recognized by non-deterministic pushdown automata), OCL denote the one-counter languages (languages recognized by non-deterministic pushdown automata with single-symbol stack alphabet) and $\mathsf{poly{-}CFL}$ (resp. $\mathsf{poly{-}OCL}$) denote the intersection of finitely many context-free (resp. one-counter) languages. As $W_G \in \mathsf{poly{-}OCL} \Leftrightarrow G \in \widehat{\Pi}_1$ [17], the following corollary is also immediate.

▶ **Corollary 5.** *$\exists C \in \mathbb{R}_{>0}, \forall W_G \in \mathsf{poly{-}OCL}, \forall \epsilon \in \mathbb{R}_{>0}$, $W_G \in \mathsf{coR2QCFA}(n^3, \epsilon, 2, \widetilde{\mathbb{C}}) \cap \mathsf{coR2QCFA}(n^C, \epsilon, 2, \overline{\mathbb{Q}})$.*

Moreover, as $W_G \in \mathsf{poly{-}OCL} \cap \mathsf{CFL} \Leftrightarrow G$ is a finitely generated virtually cyclic group [17], the above corollary exhibits a wide class of non-context-free languages that are recognizable by a 2QCFA in polynomial time: the word problem of any group that is virtually $\mathbb{Z}^k$, $k \geq 2$.

Next, let F_k denote the free group of rank k, for $k \in \mathbb{N}$; in particular, F_0 is the trivial group, F_1 is the group $\mathbb{Z}$, and, for any $k \geq 2$, F_k is non-abelian. Notice that W_{F_2} is closely related to the language L_{pal}. Ambainis and Watrous [1] showed that, $\forall \epsilon \in \mathbb{R}_{>0}$, $\exists D \in \mathbb{R}_{\geq 1}$, such that $L_{pal} \in \mathsf{coR2QCFA}(D^n, \epsilon, 2, \overline{\mathbb{Q}})$, and the same method would show the same result for W_{F_2}. We show that the same result holds for any group built from free groups, using certain operations. Let $\widehat{\Pi}_2$ denote the collection of all finitely generated groups that are virtually a subgroup of a direct product of finitely many finite-rank free groups.

▶ **Theorem 6.** *$\forall G \in \widehat{\Pi}_2, \forall \epsilon \in \mathbb{R}_{>0}, \exists D \in \mathbb{R}_{\geq 1}$, such that $W_G \in \mathsf{coR2QCFA}(D^n, \epsilon, 2, \overline{\mathbb{Q}})$.*

As $W_G \in \mathsf{CFL} \Leftrightarrow G$ is a finitely generated virtually free group [23], we obtain the following.

▶ **Corollary 7.** *$\forall W_G \in \mathsf{CFL}, \forall \epsilon \in \mathbb{R}_{>0}, \exists D \in \mathbb{R}_{\geq 1}$, such that $W_G \in \mathsf{coR2QCFA}(D^n, \epsilon, 2, \overline{\mathbb{Q}})$.*

Consider the homomorphism $\pi : F_2 \times F_2 \to \mathbb{Z}$, where π takes each free generator of each copy of F_2 to a single generator of $\mathbb{Z}$; then $K = \ker \pi$ is finitely generated, but not finitely presented [32]. All groups G for which $W_G \in \mathsf{CFL} \cup \mathsf{poly{-}OCL}$ are finitely presented [16]. As $K \in \widehat{\Pi}_2$, we have the following corollary.

▶ **Corollary 8.** *There is a finitely generated group K, which is not finitely presented (hence, $W_K \notin \mathsf{CFL} \cup \mathsf{poly{-}OCL}$), where $\forall \epsilon \in \mathbb{R}_{>0}, \exists D \in \mathbb{R}_{\geq 1}$, such that $W_K \in \mathsf{coR2QCFA}(D^n, \epsilon, 2, \overline{\mathbb{Q}})$.*

▶ Remark 9. It is known that, if $G \in \widehat{\Pi}_2$, then $W_G \in \mathsf{poly{-}CFL}$ [7]. Moreover, it is conjectured that $\widehat{\Pi}_2$ is precisely the class of groups whose word problem is in $\mathsf{poly{-}CFL}$ [7] (cf. [8]).

We next consider a broader class of groups. Let $Z(H)$ denote the center of a group H, let $\mathrm{U}(d, \overline{\mathbb{Q}})$ denote the group of $d \times d$ unitary matrices with entries in $\overline{\mathbb{Q}}$, let $\mathrm{PU}(d, \overline{\mathbb{Q}}) = \mathrm{U}(d, \overline{\mathbb{Q}})/Z(\mathrm{U}(d, \overline{\mathbb{Q}}))$, and let $(\mathrm{PU}(d, \overline{\mathbb{Q}}))^k$ denote the direct product of k copies of $\mathrm{PU}(d, \overline{\mathbb{Q}})$.

▶ **Theorem 10.** *If G is a finitely generated group that is virtually a subgroup of $(\mathrm{PU}(d, \overline{\mathbb{Q}}))^k$, for some $d, k \in \mathbb{N}_{\geq 1}$, then $\forall \epsilon \in \mathbb{R}_{>0}, \exists D \in \mathbb{R}_{\geq 1}$, such that $W_G \in \mathsf{coR2QCFA}(D^n, \epsilon, d, \overline{\mathbb{Q}})$.*

In order to state our final main result, as well as to provide appropriate context for the results listed above, we define the classes of groups Σ_j and Π_j, for $j \in \mathbb{N}$, inductively. First $\Sigma_0 = \Pi_0 = \{\mathbb{Z}, \{1\}\}$ (i.e., both classes consist of the two groups $\mathbb{Z}$ and the trivial group $\{1\}$). We use $\times$ to denote the direct product and $*$ to denote the free product. For $j > 1$, we define $\Pi_j = \{H_1 \times \cdots \times H_t : t \in \mathbb{N}_{\geq 1}, H_1, \ldots, H_t \in \Sigma_{j-1}\}$ and $\Sigma_j = \{H_1 * \cdots * H_t : t \in \mathbb{N}_{\geq 1}, H_1, \ldots, H_t \in \Pi_{j-1}\}$. These groups comprise an important subclass of a particularly important class of groups: the right-angled Artin groups. Note that every $G \in \bigcup_j (\Pi_j \cup \Sigma_j)$ is finitely generated. Also note that the Π_j and Σ_j form a hierarchy in the obvious way. We further define $\widehat{\Pi}_j$ (resp. $\widehat{\Sigma}_j$) as the set of all finitely generated groups that are virtually a subgroup of some group in Π_j (resp. Σ_j), which also form a hierarchy in the obvious way.

In particular, $\widehat{\Pi}_1$ (resp. $\widehat{\Pi}_2$) is precisely the class of groups for which Theorem 3 (resp. Theorem 6) demonstrates the existence of a 2QCFA that recognizes the corresponding word problem with bounded error in expected polynomial (resp. exponential) time. We next consider the class $\widehat{\Pi}_3$. While the relationship of this class to the class of groups to which Theorem 10 applies is unclear to us, we can show that the word problem of any group in this class can be recognized by a 2QCFA with negative one-sided *unbounded* error. Let $\mathsf{coN2QCFA}(T, d, \mathbb{A})$ be defined as in Definition 2, except we now only require that $\Pr[N \text{ rejects } w] > 0, \forall w \notin L$.

▶ **Theorem 11.** *If $G \in \widehat{\Pi}_3$, then $W_G \in \mathsf{coN2QCFA}(n, 2, \widetilde{\mathbb{C}})$.*

▶ Remark 12. $\mathbb{Z} * \mathbb{Z}^2 \in \Sigma_2 \subseteq \widehat{\Pi}_3$. It is conjectured [7, 18] that $W_{\mathbb{Z}*\mathbb{Z}^2} \notin \mathsf{poly{-}CFL} \cup \mathsf{coCFL}$.

Lastly, we consider 2QCFA with no restrictions on their transition amplitudes, as well as the measure-once one-way quantum finite automaton (MO-1QFA) defined by Moore and Crutchfield [22]. Let $\mathsf{coN1QFA}$ denote the class of languages recognizable with negative one-sided unbounded error by a MO-1QFA (with any constant number of states).

▶ **Theorem 13.** *If G is a finitely generated group that is virtually a subgroup of $(\mathrm{PU}(d))^k$, for some $d, k \in \mathbb{N}_{\geq 1}$, then $W_G \in \mathsf{coN2QCFA}(n, d, \mathbb{C}) \cap \mathsf{coN1QFA}$.*

Let $\mathcal{D}$ denote the class of groups to which the preceding theorem applies (which includes all groups to which all earlier theorems apply). Let S denote the stochastic languages (the class of languages recognizable by PFA with strict cut-points). By [6, Theorem 3.6], $\mathsf{coN1QFA} \subseteq \mathsf{coS}$, which implies the following corollary.

▶ **Corollary 14.** *If $G \in \mathcal{D}$, then $W_G \in \mathsf{coS}$.*

▶ Remark 15. For many $G \in \mathcal{D}$, the fact that $W_G \in \mathsf{coS}$ was already known: $W_{F_k} \in \mathsf{coS}$, $\forall k$ [6], which implies (by standard arguments from computational group theory, see for instance [23]) that $\forall G \in \widehat{\Pi}_2$, $W_G \in \mathsf{coS}$. However, for $G \in \mathcal{D} \setminus \widehat{\Pi}_2$, this result appears to be new.

2 Quantum Computation and the 2QCFA

In this section, we briefly recall the fundamentals of quantum computation and the definition of 2QCFA. For further background on quantum computation, see, for instance, [24, 35].

A natural way of understanding quantum computation is as a generalization of probabilistic computation. One may consider a probabilistic system defined over some finite set of states $C = \{c_1, \ldots, c_k\}$, where the state of that system, at any particular point in time, is given by a probability distribution over C. Such a probability distribution may be described by a vector $v = (v_{c_1}, \ldots, v_{c_k})$, where $v_c \in \mathbb{R}_{\geq 0}$ denotes the probability that the system is in state $c \in C$, and $\sum_c v_c = 1$, i.e., v is simply an element of $\mathbb{R}^k_{\geq 0}$ with L^1-norm 1.

Similarly, consider some finite set of *quantum basis states* $Q = \{q_1, \ldots, q_k\}$, which correspond to an orthonormal basis $|q_1\rangle, \ldots, |q_k\rangle$ of $\mathbb{C}^k$ (here and throughout the paper we use the standard bra-ket notation). The state of a quantum system over Q, at any particular time, is given by some *superposition* $|\psi\rangle = \sum_q \alpha_q |q\rangle$ of the basis states, where each $\alpha_q \in \mathbb{C}$ and $\sum_q |\alpha_q|^2 = 1$; i.e., a superposition $|\psi\rangle$ is simply an element of $\mathbb{C}^k$ with L^2-norm 1.

Let $\mathrm{U}(k)$ denote the group of $k \times k$ unitary matrices. Given a quantum system currently in the superposition $|\psi\rangle$, one may apply a transformation $t \in \mathrm{U}(k)$ to the system, after which the system is in the superposition $t|\psi\rangle$. One may also perform a *projective measurement in the computational basis*, which is specified by some partition $B = \{B_0, \ldots, B_l\}$ of Q. Measuring a system that is in the superposition $|\psi\rangle = \sum_q \alpha_q |q\rangle$ with respect to B gives the result $B_r \in B$ with probability $p_r := \sum_{q \in B_r} |\alpha_q|^2$; additionally, if the result of the measurement is B_r, then the state of the system *collapses* to the superposition $\frac{1}{\sqrt{p_r}} \sum_{q \in B_r} \alpha_q |q\rangle$. We emphasize that measuring a quantum system changes the state of that system.

We now define a 2QCFA, essentially following the original definition in [1]. Informally, a 2QCFA is a two-way deterministic finite automaton that has been augmented with a finite size quantum register. Formally, a 2QCFA M is given by an 8-tuple, $M = \{Q, C, \Sigma, \delta, q_{start}, c_{start}, c_{acc}, c_{rej}\}$, where Q (resp. C) is the finite set of quantum (resp. classical) states, Σ is a finite alphabet, δ is the transition function, $q_{start} \in Q$ (resp. $c_{start} \in C$) is the quantum (resp. classical) start state, and $c_{acc}, c_{rej} \in C$, where $c_{acc} \neq c_{rej}$, are the accepting and rejecting states. The *quantum register* of M is given by the quantum system with basis states Q. We define the tape alphabet $\Gamma := \Sigma \sqcup \{\#_L, \#_R\}$ where the two distinct symbols $\#_L, \#_R \notin \Sigma$ will be used to denote, respectively, a left and right end-marker.

Each step of the computation of the 2QCFA M involves either performing a unitary transformation or a projective measurement on its quantum register, updating the classical state, and moving the tape head. This behavior is encoded in the transition function δ. For each $(c, \gamma) \in (C \setminus \{c_{acc}, c_{rej}\}) \times \Gamma$, $\delta(c, \gamma)$ specifies the behavior of M when it is in the classical state c and the tape head currently points to a tape alphabet symbol γ. There are two forms that $\delta(c, \gamma)$ may take, depending on whether it encodes a unitary transformation or a projective measurement. In the first case, $\delta(c, \gamma)$ is a triple (t, c', h) where $t \in \mathrm{U}(|Q|)$ is a unitary transformation to be performed on the quantum register, $c' \in C$ is the new classical state, and $h \in \{-1, 0, 1\}$ specifies whether the tape head is to move left, stay put, or move right, respectively. In the second case, $\delta(c, \gamma)$ is a pair (B, f), where B is a partition of Q specifying a projective measurement, and $f : B \to C \times \{-1, 0, 1\}$ specifies the mapping from the result of that measurement to the evolution of the classical part of the machine, where, if the result of the measurement is B_r, and $f(B_r) = (c', h)$, then $c' \in C$ is the new classical state and $h \in \{-1, 0, 1\}$ specifies the movement of the tape head.

The computation of M on an input $w \in \Sigma^*$ is then defined as follows. If w has length n, then the tape will be of size $n + 2$ and contain the string $\#_L w \#_R$. Initially, the classical state is c_{start}, the quantum register is in the superposition $|q_{start}\rangle$, and the tape head points

to the leftmost tape cell. At each step of the computation, if the classical state is currently c and the tape head is pointing to symbol γ, the machine behaves as specified by $\delta(c,\gamma)$. If, at some point in the computation, M enters the state c_{acc} (resp. c_{rej}) then it immediately halts and accepts (resp. rejects) the input w. As quantum measurement is a probabilistic process, the computation of M is probabilistic. For any $w \in \Sigma^*$, we write $\Pr[M \text{ accepts } w]$ (resp. $\Pr[M \text{ rejects } w]$) for the probability that M will accept (resp. reject) the input w.

Let $\mathcal{T} = \{t \in \mathrm{U}(|Q|) : \exists (c,\gamma) \in ((C \setminus \{c_{acc}, c_{rej}\}) \times \Gamma) \text{ such that } \delta(c,\gamma) = (t,\cdot,\cdot)\}$ denote the set of all unitary transformations that M may perform. The *transition amplitudes* of M are the set of numbers $\mathbb{A}$ that appear as entries of some $t \in \mathcal{T}$.

3 Distinguishing Families of Representations

The landmark result of Lipton and Zalcstein [20] showed that, if G is a finitely generated linear group over a field of characteristic zero, then $W_G \in \mathsf{L}$. The key idea behind their logspace algorithm was to make use of a carefully chosen *representation* of the group G in order to recognize W_G (see, for instance, [19] or the full version of our paper [28] for the notation and terminology from representation theory used in this section). Our 2QCFA algorithm will operate in a similar manner; however, the constraints of quantum mechanics will require us to make many modifications to their approach.

A (unitary) representation of a (topological) group G is a continuous homomorphism $\rho : G \to \mathrm{U}(\mathcal{H})$, where $\mathcal{H}$ is a Hilbert space, and $\mathrm{U}(\mathcal{H})$ is the group of unitary operators on $\mathcal{H}$. The Gel'fand-Raikov theorem states that the elements of any locally compact group G are separated by its unitary representations; i.e., $\forall g \in G$ with $g \neq 1_G$, there is some $\mathcal{H}$ and some $\rho : G \to \mathrm{U}(\mathcal{H})$ such that $\rho(g) \neq \rho(1_G)$. For certain groups, stronger statements can be made; in particular, one calls a group maximally almost periodic if the previous condition still holds when $\mathcal{H}$ is restricted to be finite-dimensional.

The core idea of our approach to recognizing the word problem W_G of a particular group G is to construct what we have chosen to call a *distinguishing family of representations* (DFR) for G, which is a refinement of the above notion. Informally, a DFR is a collection of a small number of unitary representations of G, all of which are over a Hilbert space of small dimension, such that, for any $g \in G$ other than 1_G, there is some representation ρ in the collection for which $\rho(g)$ is "far from" $\rho(1_G)$, relative to the "size" of g. The following definition formalizes this, by introducing parameters to quantify the above fuzzy notions. In this definition, and in the remainder of the paper, let $\mathrm{U}(d)$ denote the group of $d \times d$ unitary matrices, let $M(d,\mathbb{A})$ denote the set of $d \times d$ matrices with entries in some set $\mathbb{A}$, let $\mathrm{U}(d,\mathbb{A}) = \mathrm{U}(d) \cap M(d,\mathbb{A})$, and let $G_{\neq 1} = G \setminus \{1_G\}$. For a group $G = \langle S|R\rangle$, let $l(g)$ denote the length of any $g \in G$ relative to the generating set S (i.e., $l(g)$ is the minimum value of m for which $\exists g_1, \ldots, g_m \in S \cup S^{-1}$ such that $g = \phi(g_1 \cdots g_m)$). For a representation $\rho : G \to \mathrm{U}(d)$, let $\chi_\rho : G \to \mathbb{C}$ denote the *character* of ρ (i.e., $\chi_\rho(g) = \mathrm{Tr}(\rho(g))$).

▶ **Definition 16.** Consider a group $G = \langle S|R\rangle$, with S finite. For $k \in \mathbb{N}_{\geq 1}, d \in \mathbb{N}_{\geq 2}$, $\tau : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ a monotone non-increasing function, and $\mathbb{A} \subseteq \mathbb{C}$, we define a $[k,d,\tau,\mathbb{A}]$-*distinguishing family of representations* (DFR) for G to be a set $\mathcal{F} = \{\rho_1, \ldots, \rho_k\}$ where the following conditions hold.

(a) $\forall j \in \{1,\ldots,k\}$, $\rho_j : G \to \mathrm{U}(d)$ is a representation of G.
(b) $\forall g \in G_{\neq 1}$, $\exists j \in \{1,\ldots,k\}$ such that $|\chi_{\rho_j}(g)| \leq d - \tau(l(g))$.
(c) $\forall \sigma \in S \cup S^{-1}, \forall j \in \{1,\ldots,k\}$, $\exists Y_1, \ldots, Y_t \in \mathrm{U}(d,\mathbb{A})$, such that $\rho_j(\sigma) = \prod_i Y_i$.

Suppose $\mathcal{F} = \{\rho_1, \ldots, \rho_k\}$ is a $[k, d, \tau, \mathbb{A}]$-DFR for $G = \langle S|R\rangle$. We write $I_d = 1_{\mathrm{U}(d)} \in \mathrm{U}(d)$ for the $d \times d$ identity matrix, $\ker(\rho_j) = \{g \in G : \rho_j(g) = I_d\}$ for the kernel of ρ_j, $Z(\mathrm{U}(d)) = \{e^{ir} I_d : r \in \mathbb{R}\}$ for the center of $\mathrm{U}(d)$, and $\mathrm{Pker}(\rho_j) = \{g \in G : \rho_j(g) = Z(\mathrm{U}(d))\}$ for the quasikernel of ρ_j. Clearly, $1_G \in \mathrm{Pker}(\rho_j), \forall j$, but, as ρ_j is not assumed to be P-faithful or even faithful, there may be $g \in G_{\neq 1}$ for which, for certain j, we have $g \in \mathrm{Pker}(\rho_j)$. However, due to the fact that $g \in \mathrm{Pker}(\rho_j)$ exactly when $|\chi_{\rho_j}(g)| = d$, the second defining property of a DFR guarantees not only that $\bigcap_j \mathrm{Pker}(\rho_j) = \{1_G\}$, but, much more strongly, that all $g \in G_{\neq 1}$ are "far from" being in $\bigcap_j \mathrm{Pker}(\rho_j)$. That is to say, $\forall g \in G_{\neq 1}, \exists j$ such that $|\chi_{\rho_j}(g)|$ is at distance at least $\tau(l(g))$ from having value d. The following proposition is then immediate, but we explicitly state it as it is the central notion in our quantum approach to the word problem.

▶ **Proposition 17.** *Suppose $G = \langle S|R\rangle$ has a $[k, d, \tau, \mathbb{A}]$-DFR $\mathcal{F} = \{\rho_1, \ldots, \rho_k\}$. Then, $\forall g \in G$, $g = 1_G \Leftrightarrow \forall j$, $|\chi_{\rho_j}(g)| = d$ and $g \in G_{\neq 1} \Leftrightarrow \exists j$ such that $|\chi_{\rho_j}(g)| \leq d - \tau(l(g))$.*

Note that, in the preceding proposition, $\rho_1 \oplus \cdots \oplus \rho_k : G \to \mathrm{U}(kd)$ is simply a faithful representation of G, decomposed into subrepresentations in a convenient way. Next, we establish some terminology that will better allow us to describe particular types of DFR.

▶ **Definition 18.** Suppose $\mathcal{F} = \{\rho_1, \ldots, \rho_k\}$ is a $[k, d, \tau, \mathbb{A}]$-DFR for a group G.
(a) If $\mathbb{A} = \overline{\mathbb{Q}}$ (equivalently, if $\rho_j(G) \subseteq \mathrm{U}(d, \overline{\mathbb{Q}}), \forall j$), we say $\mathcal{F}$ is an *algebraic* DFR.
(b) If $\rho_j(g)$ is a diagonal matrix $\forall j, \forall g$, then we say $\mathcal{F}$ is a *diagonal* DFR.
(c) If H is a finite-index overgroup of G, we say that H *virtually* has a $[k, d, \tau, \mathbb{A}]$-DFR.

When $\mathcal{F}$ is an algebraic DFR, we will often only write $[k, d, \tau]$ to denote its parameters. Note that only abelian groups have diagonal DFRs, and any DFR of an abelian group can be converted to a diagonal DFR; we define diagonal DFRs for convenience.

Using a $[k, d, \tau, \mathbb{A}]$-DFR for a group G, it will be possible to construct a 2QCFA that recognizes the word problem W_H of any finite-index overgroup H of G, where the parameters of the DFR will strongly impact the parameters of the resulting 2QCFA. In particular, in Section 4, we produce a 2QCFA with d quantum states and transition amplitudes in $\mathbb{A}$ that recognizes W_H, with expected running time approximately $O(\tau(n)^{-1})$. The goal is then to show that a wide collection of groups virtually have DFRs with good parameters.

3.1 Diophantine Approximation

Our constructions of DFRs rely crucially on certain results concerning Diophantine approximation. Most fundamentally, the Diophantine approximation question asks how well a particular real number α can be approximated by rational numbers. Of course, as $\mathbb{Q}$ is dense in $\mathbb{R}$, one can choose $\frac{p}{q} \in \mathbb{Q}$ so as to make the quantity $|\alpha - \frac{p}{q}|$ arbitrarily small; for this reason, one considers $\frac{p}{q}$ to be a "good" approximation to α only when $|\alpha - \frac{p}{q}|$ is small compared to a suitable function of q. One then considers α to be poorly approximated by rationals if, for some "small" constant $d \in \mathbb{R}_{\geq 2}$, $\exists C \in \mathbb{R}_{>0}$ such that, $\forall (p, q) \in \mathbb{Z} \times \mathbb{Z}_{\neq 0}$, we have $|\alpha - \frac{p}{q}| \geq C|q|^{-d}$, where the smallness of d determines just how poorly approximable α is. For $\alpha \in \mathbb{R}$, let $\|\alpha\| = \min_{m \in \mathbb{Z}} |\alpha - m|$ denote the distance between α and its nearest integer. Notice that $\left|\alpha - \frac{p}{q}\right| \geq C|q|^{-d}$, $\forall (p, q) \in \mathbb{Z} \times \mathbb{Z}_{\neq 0} \Leftrightarrow \|q\alpha\| \geq C|q|^{-(d-1)}$, $\forall q \in \mathbb{Z}_{\neq 0}$. Of particular relevance to us is the following result, due to Schmidt [30], that real irrational algebraic numbers are poorly approximated by rationals.

▶ **Proposition 19** ([30]). *$\forall \alpha_1, \ldots, \alpha_k \in (\mathbb{R} \cap \overline{\mathbb{Q}})$ where $1, \alpha_1, \ldots, \alpha_k$ are linearly independent over $\mathbb{Q}$, $\forall \epsilon \in \mathbb{R}_{>0}$, $\exists C \in \mathbb{R}_{>0}$ such that $\forall q \in \mathbb{Z}_{\neq 0}$, $\exists j$ such that $\|q\alpha_j\| \geq C|q|^{-(\frac{1}{k} + \epsilon)}$.*

We also require the following result concerning the Diophantine properties of linear forms in logarithms of algebraic numbers, due to Baker [4].

▶ **Proposition 20** ([4]). *Let* $L = \{\beta \in \mathbb{C}_{\neq 0} : e^{\beta} \in \overline{\mathbb{Q}}\}$. $\forall \beta_1, \dots, \beta_k \in L$ *that are linearly independent over* $\mathbb{Q}$, $\exists C \in \mathbb{R}_{>0}$ *such that,* $\forall (q_1, \dots, q_k) \in \mathbb{Z}^k$ *with* $q_{max} := \max_j |q_j| > 0$, *we have* $|q_1\beta_1 + \cdots + q_k\beta_k| \geq (eq_{max})^{-C}$.

Gamburd, Jakobson, and Sarnak [12] established a particular result concerning the Diophantine properties of $\mathrm{SU}(2, \overline{\mathbb{Q}})$. The following lemma generalizes their result to $\mathrm{U}(d, \overline{\mathbb{Q}})$; a proof of this lemma appears in the full version [28].

▶ **Lemma 21.** *Consider a group* $G = \langle S|R\rangle$, *with* S *finite, and a representation* $\rho : G \to \mathrm{U}(d, \overline{\mathbb{Q}})$. *Then* $\exists C \in \mathbb{R}_{\geq 1}$ *such that* $|\chi_\rho(g)| \leq d - C^{-l(g)}$, $\forall g \in (G \setminus \mathrm{Pker}(\rho))$.

3.2 Constructions of DFRs

We now show that a wide collection of groups virtually have DFRs with good parameters. We accomplish this by first constructing DFRs for only a small family of special groups. We then present several constructions in which a DFR for a group, or more generally a family of DFRs for a family of groups, is used to produce a DFR for a related group.

We begin with a straightforward lemma expressing a useful character bound. In this lemma, and throughout this section, we continue to write group operations multiplicatively, and so, for $g \in G$ and $h \in \mathbb{Z}$, if $h > 0$ (resp. $h < 0$) then g^h denotes the element of G obtained by combining h copies of g (resp. g^{-1}) with the group operation, and if $h = 0$ then $g^h = 1_G$. Let $S_1 = \{e^{ir} : r \in \mathbb{R}\} \subseteq \mathbb{C}^*$ denote the circle group and let $\mathrm{T}(d) \subseteq \mathrm{U}(d)$ denote the group of all $d \times d$ diagonal matrices where each diagonal entry lies in S_1. For $\mathbb{A} \subseteq \mathbb{C}$, let $S_1(\mathbb{A}) = S_1 \cap \mathbb{A}$ and $\mathrm{T}(d, \mathbb{A}) = \mathrm{T}(d) \cap M(d, \mathbb{A})$. Let $\mathbf{1}_d : G \to \mathrm{U}(d)$ denote the trivial representation of dimension d (i.e., $\mathbf{1}_d(g) = I_d = 1_{\mathrm{U}(d)}$, $\forall g \in G$). For a cyclic group $G = \langle a|R_G\rangle$ and for some $r \in \mathbb{R}$, define the representation $\widehat{\gamma}_r : G \to S_1 \cong \mathrm{U}(1)$ such that $a \mapsto e^{2\pi ir}$; furthermore, define the representation $\gamma_r : G \to \mathrm{T}(2)$ by $\gamma_r = \widehat{\gamma}_r \oplus \mathbf{1}_1$.

▶ **Lemma 22.** *Consider the cyclic group* $G = \langle a|R_G\rangle$. *Fix* $r \in \mathbb{R}$ *and define* $\gamma_r : G \to \mathrm{T}(2)$ *as above. Suppose that* $h \in \mathbb{Z}$ *and* $\epsilon \in \mathbb{R}_{>0}$ *satisfy* $\|hr\| \geq \epsilon$. *Then* $\chi_{\gamma_r}(a^h) \leq 2 - \frac{19\pi^2}{24}\epsilon^2$.

Proof. We have $\chi_{\gamma_r}(a^h) = e^{2\pi ihr} + 1 = 2e^{\pi ihr}\cos(\pi hr)$. Clearly, $\epsilon \leq \frac{1}{2}$. Therefore,

$$|\chi_{\gamma_r}(a^h)| = 2|\cos(\pi hr)| \leq 2\cos(\pi\epsilon) \leq 2\left(1 - \frac{(\pi\epsilon)^2}{2} + \frac{(\pi\epsilon)^4}{24}\right) \leq 2 - \frac{19\pi^2}{24}\epsilon^2. \qquad \blacktriangleleft$$

We first construct DFRs for a very narrow class of special groups: (i) $\mathbb{Z}_m = \langle a|a^m\rangle$, the integers modulo m, where the group operation is addition, (ii) $\mathbb{Z} = \langle a|\rangle$, the integers, where the group operations is addition, and (iii) $F_2 = \langle a, b|\rangle$ the (non-abelian) free group of rank 2.

▶ **Lemma 23.** $\mathbb{Z}_m = \langle a|a^m\rangle$ *has a diagonal algebraic* $\left[1, 2, \frac{19\pi^2}{24m^2}\right]$*-DFR,* $\forall m \in \mathbb{N}_{\geq 2}$.

Proof. Fix $m \in \mathbb{N}_{\geq 2}$ and let $r = \frac{1}{m}$. Define $\gamma_r : \mathbb{Z}_m \to \mathrm{T}(2)$ as above, and notice that $\gamma_r(\mathbb{Z}_m) \subseteq \mathrm{T}(2, \overline{\mathbb{Q}})$. Consider any $q \in \mathbb{Z}_m$, where $q \not\equiv 0 \mod m$. Then q can be expressed as $q = a^h$, for $h \in \mathbb{Z}$, $h \not\equiv 0 \mod m$. As $\|hr\| \geq \frac{1}{m}$, Lemma 22 implies $|\chi_{\gamma_r}(q)| \leq 2 - \frac{19\pi^2}{24m^2}$. Therefore, $\{\gamma_r\}$ is a diagonal algebraic DFR for $\mathbb{Z}_m$, with the desired parameters. $\blacktriangleleft$

▶ **Lemma 24.** $\forall \delta \in \mathbb{R}_{>0}, \exists C \in \mathbb{R}_{>0}$, $\mathbb{Z} = \langle a|\rangle$ *has a diagonal* $[1 + \lfloor \frac{2}{\delta} \rfloor, 2, Cn^{-\delta}, \widetilde{\mathbb{C}}]$*-DFR.*

Proof. Let $k = 1+\lfloor \frac{2}{\delta} \rfloor$ and $\eta = \frac{\delta}{2} - \frac{1}{k} > 0$. Fix $\alpha_1, \ldots, \alpha_k \in (\overline{\mathbb{Q}} \cap \mathbb{R})$ such that $1, \alpha_1, \ldots, \alpha_k$ are linearly independent over $\mathbb{Q}$. For each $j \in \{1, \ldots, k\}$ define the representation $\gamma_{\alpha_j} : \mathbb{Z} \to \mathrm{T}(2)$ as above, and notice that $\gamma_{\alpha_j}(\mathbb{Z}) \subseteq \mathrm{T}(2, \widetilde{\mathbb{C}})$. By Proposition 19, $\exists D \in \mathbb{R}_{>0}$, such that $\forall q \in \mathbb{Z}_{\neq 0}$ (i.e., $\forall q \in \mathbb{Z}$ where $q \neq 0 = 1_{\mathbb{Z}}$), $\exists j$ such that $\|q\alpha_j\| \geq D|q|^{-(\frac{1}{k}+\eta)} = D|q|^{-\frac{\delta}{2}}$. Therefore, for any $q \in \mathbb{Z}_{\neq 0}$, if we take j as above, then by Lemma 22 (with $r = \alpha_j$, $\epsilon = D|q|^{-\frac{\delta}{2}}$, and $h = q$) we have $|\chi_{\gamma_{\alpha_j}}(q)| \leq 2 - \frac{19\pi^2}{24} D^2 |q|^{-\delta}$. Therefore, $\{\gamma_{\alpha_1}, \ldots, \gamma_{\alpha_k}\}$ is a diagonal $[1 + \lfloor \frac{2}{\delta} \rfloor, 2, \frac{19\pi^2}{24} D^2 n^{-\delta}, \widetilde{\mathbb{C}}]$-DFR for $\mathbb{Z}$. ◀

▶ **Lemma 25.** *$\exists C_1, C_2 \in \mathbb{R}_{>0}$ such that $\mathbb{Z} = \langle a | \rangle$ has a diagonal algebraic $[1, 2, C_2 n^{-C_1}]$-DFR.*

Proof. As in Proposition 20, let $L = \{\beta \in \mathbb{C}_{\neq 0} : e^\beta \in \overline{\mathbb{Q}}\}$ and notice that $\pi i \in L$. Let $R = \{r \in ((\mathbb{R} \setminus \mathbb{Q}) \cap (0,1)) : 2\pi i r \in L\}$ (e.g., $\hat{r} = \frac{1}{2\pi} \cos^{-1}\left(\frac{3}{5}\right)$ is irrational and has $e^{2\pi i \hat{r}} = \frac{3+4i}{5}$, and so $\hat{r} \in R$). Fix $r \in R$. By definition, $2\pi i r \in L$, which immediately implies $\pi i r \in L$. Also by definition, $r \notin \mathbb{Q}$, which implies $\pi i r$ and πi are linearly independent over $\mathbb{Q}$. Therefore, by Proposition 20, $\exists D \in \mathbb{R}_{>0}$ such that $\forall (q, m) \in \mathbb{Z}^2$ where $q_{max} := \max(|q|, |m|) > 0$, we have $|q\pi i r - m\pi i| \geq (e q_{max})^{-D}$.

For fixed $q \in \mathbb{Z}_{\neq 0}$ and varying $m \in \mathbb{Z}$, $|q\pi i r - m\pi i|$ attains its minimum when $m = \mathrm{round}(qr)$, the closest integer to qr. Notice that $|\mathrm{round}(qr)| \leq |q|$, as $r \in (0,1)$ and $q \in \mathbb{Z}$. Therefore, for any $q \in \mathbb{Z}_{\neq 0}$, we have

$$\|qr\| = \min_{m \in \mathbb{Z}} |qr - m| = \frac{1}{\pi} \min_{m \in \mathbb{Z}} |q\pi i r - m\pi i| = \frac{1}{\pi} |q\pi i r - \mathrm{round}(qr)\pi i| \geq \frac{1}{\pi} |eq|^{-D}.$$

Define $\gamma_r : \mathbb{Z} \to \mathrm{T}(2)$ as above. By Lemma 22, $|\chi_{\gamma_r}(q)| \leq 2 - \frac{19}{24} |eq|^{-2D}$. Clearly, $\gamma_r(\mathbb{Z}) \subseteq \mathrm{T}(2, \overline{\mathbb{Q}})$. Therefore, $\{\gamma_r\}$ is a diagonal algebraic $[1, 2, \frac{19}{24} e^{-2D} n^{-2D}]$-DFR for $\mathbb{Z}$. ◀

▶ Remark 26. We note that the above constructions of DFRs for $\mathbb{Z}$ are quite similar to the technique used by Ambainis and Watrous [1] to produce a 2QCFA that recognizes L_{eq} (cf. [6, 25]). In particular, their approach relied on the fact that the number $\sqrt{2} \in \overline{\mathbb{Q}}$ is poorly approximated by rationals; our constructions make use of more general Diophantine approximation results. This allows us to produce 2QCFA with improved parameters.

▶ **Lemma 27.** *$\exists C \in \mathbb{R}_{\geq 1}$, such that $F_2 = \langle a, b | \rangle$ has an algebraic $[1, 2, C^{-n}]$-DFR.*

Proof. First, define the representation $\pi : F_2 \to SO(3, \mathbb{Q})$ by

$$a \mapsto \frac{1}{5} \begin{pmatrix} 3 & -4 & 0 \\ 4 & 3 & 0 \\ 0 & 0 & 5 \end{pmatrix} \text{ and } b \mapsto \frac{1}{5} \begin{pmatrix} 5 & 0 & 0 \\ 0 & 3 & -4 \\ 0 & 4 & 3 \end{pmatrix}.$$

This is the "standard" faithful representation of F_2 into SO(3) used in many treatments of the Banach-Tarski paradox. Recall that SU(2) is the double cover of SO(3), i.e., $\mathrm{SU}(2)/Z(\mathrm{SU}(2)) \cong \mathrm{SO}(3)$. Then π induces a homomorphism $\widehat{\pi} : F_2 \to \mathrm{SU}(2)/Z(\mathrm{SU}(2))$ in the obvious way, which, by the universal property of the free group, can be lifted to the representation $\rho : F_2 \to \mathrm{SU}(2, \overline{\mathbb{Q}})$ given by

$$a \mapsto \frac{1}{\sqrt{5}} \begin{pmatrix} 2+i & 0 \\ 0 & 2-i \end{pmatrix} \text{ and } b \mapsto \frac{1}{\sqrt{5}} \begin{pmatrix} 2 & i \\ i & 2 \end{pmatrix}.$$

As π is faithful, we conclude that $\rho(g) \notin Z(\mathrm{SU}(2))$, $\forall g \in (F_2 \setminus 1_{F_2})$. Therefore, by Lemma 21, $\{\rho\}$ is an algebraic $[1, 2, C^{-n}]$-DFR for F_2. ◀

▶ Remark 28. Note that the proof of the preceding lemma uses, fundamentally, the same construction used by Ambainis and Watrous [1] to produce a 2QCFA for L_{pal} (which is closely related to F_2). The algebraic structure of F_2 allows a substantially simpler argument.

We now present several constructions of new DFRs from existing DFRs. We emphasize that all results in the following lemmas are constructive in the sense that, given the supposed DFR or collection of DFRs, each corresponding proof provides an explicit construction of the new DFR. Due to space restrictions, all proofs are omitted and may be found in the full version [28]. We begin by considering conversions of a DFR of a group G to a DFR with different parameters of the same group G. For $C \in \mathbb{R}_{>0}$, let $\eta_C : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ be given by $\eta_C(n) = Cn$.

▶ **Lemma 29.** *Suppose $\mathcal{F}$ is a $[k, d, \tau, \mathbb{A}]$-DFR for a group $G = \langle S|R\rangle$, with S finite. The following statements hold.*

- **(i)** *G has a $[1, kd, \tau, \mathbb{A}]$-DFR.*
- **(ii)** *If $d' \in \mathbb{N}$ and $d' > d$, then G has a $[k, d', \tau, \mathbb{A}]$-DFR.*
- **(iii)** *Suppose G also has presentation $\langle S'|R'\rangle$, with S' finite. Then $\exists C \in \mathbb{R}_{>0}$ such that $\mathcal{F}$ is also a $[k, d, \tau \circ \eta_C, \mathbb{A}]$-DFR for $G = \langle S'|R'\rangle$.*

Moreover, if $\mathcal{F}$ is a diagonal DFR, then each newly constructed DFR is also diagonal.

Next, we show that a DFR of G and a DFR of H can be used to produce a DFR of $G \times H$, the direct product of G and H. In the following, for a group Q, let $[q_1, q_2] = q_1^{-1}q_2^{-1}q_1q_2$ denote the commutator of elements $q_1, q_2 \in Q$. For functions $\tau, \tau' : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$, we define the function $\tau^{\min}_{\tau,\tau'} : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ by $\tau^{\min}_{\tau,\tau'}(n) := \min(\tau(n), \tau'(n))$, $\forall n \in \mathbb{R}_{>0}$.

▶ **Lemma 30.** *Consider groups $G = \langle S_G|R_G\rangle$ and $H = \langle S_H|R_H\rangle$, with S_G and S_H finite, and $S_G \cap S_H = \emptyset$. Let $R_{com} = \{[g, h] : g \in S_G, h \in S_H\}$. If G has a $[k, d, \tau, \mathbb{A}]$-DFR and H has a $[k', d', \tau', \mathbb{A}]$-DFR, then $G \times H = \langle S_G \sqcup S_H|R_G \cup R_H \cup R_{com}\rangle$ has a $[k+k', \max(d, d'), \tau^{\min}_{\tau,\tau'}, \mathbb{A}]$-DFR. Moreover, if G and H have diagonal DFRs with the above parameters, then $G \times H$ has a diagonal DFR with the above parameters.*

Now, we show that a DFR of a group G can be used to produce a DFR of a finitely generated subgroup of G, or of a finite-index overgroup of G.

▶ **Lemma 31.** *Suppose $\mathcal{F}_G$ is a $[k, d, \tau, \mathbb{A}]$-DFR for a group $G = \langle S_G|R_G\rangle$, with S_G finite. The following statements hold.*

- **(i)** *Suppose $H \leq G$, where $H = \langle S_H|R_H\rangle$, with S_H finite. Then $\exists C \in \mathbb{R}_{>0}$ such that H has a $[k, d, \tau \circ \eta_C, \mathbb{A}]$-DFR. If, moreover, $\mathcal{F}_G$ is a diagonal DFR, then H will also have a diagonal DFR with the claimed parameters.*
- **(ii)** *Suppose $G \leq Q$, where $Q = \langle S_Q|R_Q\rangle$, with S_Q finite, $S_G \subseteq S_Q$, and $r := [Q : G]$ finite. Then $\exists C \in \mathbb{R}_{>0}$ such that Q has a $[k, dr, \tau \circ \eta_C, \mathbb{A}]$-DFR.*

▶ Remark 32. By the preceding lemma, any group G that virtually has a DFR also has a DFR, but with worse parameters. As will be shown, it is possible to recognize W_G using a DFR for a finite-index subgroup of G, thereby avoiding this worsening of parameters.

We now construct DFRs, with good parameters, for a wide class of groups. Recall that any finitely generated abelian group G admits a unique decomposition $G \cong \mathbb{Z}^r \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}$, where m_i divides m_{i+1}, $\forall i \in \{1, \ldots, t-1\}$, and each $m_i \in \mathbb{N}_{\geq 2}$. Let $R(r, m_1, \ldots, m_t) = \{a_i^{m_i} : i \in \{1, \ldots, t\}\} \cup \{[a_i, a_j] : i, j \in \{1, \ldots, r+t\}\}$.

▶ **Lemma 33.** *Consider the finite (hence finitely generated) abelian group $G = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t} = \langle a_1, \ldots, a_t|R(0, m_1, \ldots, m_t)\rangle$. If $t = 0$ (i.e., G is the trivial group), then G has a diagonal algebraic $[1, 2, 2]$-DFR. Otherwise, G has a diagonal algebraic $\left[t, 2, \frac{19\pi^2}{24m_t^2}\right]$-DFR.*

Proof. If $t = 0$, the claim is obvious. Suppose $t > 0$. By Lemma 23, each factor $\mathbb{Z}_{m_i} = \langle a | a^{m_i} \rangle$ has a diagonal algebraic $\left[1, 2, \frac{19\pi^2}{24m_i^2}\right]$-DFR. Notice that $m_1 \leq \cdots \leq m_t$, as each m_i divides m_{i+1}. The existence of the desired DFR follows from Lemma 30. ◀

▶ **Theorem 34.** *$\exists C_1 \in \mathbb{R}_{>0}$ such that, for any finitely generated abelian group $G = \mathbb{Z}^r \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t} = \langle a_1, \ldots, a_{r+t} | R(r, m_1, \ldots, m_t) \rangle$, the following statements hold.*

- **(i)** *$\exists C_2 \in \mathbb{R}_{>0}$ such that G has a diagonal algebraic $\left[r + t, 2, C_2 n^{-C_1}\right]$-DFR.*
- **(ii)** *$\forall \delta \in \mathbb{R}_{>0}$, $\exists C_3 \in \mathbb{R}_{>0}$, such that G has a diagonal $\left[r\left(1 + \lfloor \frac{2}{\delta} \rfloor\right) + t, 2, C_3 n^{-\delta}, \widetilde{\mathbb{C}}\right]$-DFR.*

Proof. By Lemma 25, $\exists D_1, D_2 \in \mathbb{R}_{>0}$ such that $\mathbb{Z}$ has a diagonal algebraic $[1, 2, D_2 n^{-D_1}]$-DFR, which we call $\mathcal{F}$. We set $C_1 = D_1$. Let $H_1 = \mathbb{Z}^r$ and $H_2 = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}$. If $r = 0$, both claims follow trivially from Lemma 33. Suppose $r > 0$.

- **(i)** Using the DFR $\mathcal{F}$ of $\mathbb{Z}$, Lemma 30 implies H_1 has a diagonal algebraic $[r, 2, D_2 n^{-C_1}]$-DFR $\mathcal{H}_1$. If $t = 0$, then $G = H_1$; therefore, $\mathcal{H}_1$ is the desired DFR for G, with $C_2 = D_2$, and we are done. If $t > 0$, Lemma 33 implies H_2 has a diagonal algebraic $\left[1, 2, \frac{19\pi^2}{24m_t^2}\right]$-DFR $\mathcal{H}_2$. Set $C_2 = \min(D_2, \frac{19\pi^2}{24m_t^2})$. By Lemma 30, we conclude $G = H_1 \times H_2$ has a DFR with the claimed parameters.
- **(ii)** By Lemma 24, $\exists D \in \mathbb{R}_{>0}$ such that $\mathbb{Z}$ has a diagonal $\left[1 + \lfloor \frac{2}{\delta} \rfloor, 2, Dn^{-\delta}, \widetilde{\mathbb{C}}\right]$-DFR, $\mathcal{F}'$. The remainder of the proof is analogous to that of part (i), using $\mathcal{F}'$ in place of $\mathcal{F}$. ◀

As in Section 1.1, $\widehat{\Pi}_1$ denotes the set of all finitely generated virtually abelian groups. For $G \in \widehat{\Pi}_1$, there is a unique $r \in \mathbb{N}$ such that G is virtually $\mathbb{Z}^r$. We have the following corollary.

▶ **Corollary 35.** *$\exists C \in \mathbb{R}_{>0}$ such that, $\forall G \in \widehat{\Pi}_1$, the following holds.*

- **(i)** *$\exists D \in \mathbb{R}_{>0}, \exists K \in \mathbb{N}_{\geq 1}$, such that G virtually has a diagonal algebraic $[K, 2, Dn^{-C}]$-DFR.*
- **(ii)** *$\forall \delta \in \mathbb{R}_{>0}$, $\exists D \in \mathbb{R}_{>0}, \exists K \in \mathbb{N}_{\geq 1}$, G virtually has a diagonal $\left[K, 2, Dn^{-\delta}, \widetilde{\mathbb{C}}\right]$-DFR.*

Next, we consider groups that can be built from finitely generated free groups.

▶ **Lemma 36.** *$\forall r \in \mathbb{N}$, $\exists C \in \mathbb{R}_{\geq 1}$, $F_r = \langle a_1, \ldots, a_r | \rangle$ has an algebraic $[1, 2, C^{-n}]$-DFR.*

Proof. As $F_0 = \{1\}$ and $F_1 = \mathbb{Z}$, Theorem 34 immediately implies the claim when $r \in \{0, 1\}$. Next, consider the case in which $r = 2$. By Lemma 27, $\exists C \in \mathbb{R}_{\geq 1}$ such that $F_2 = \langle a_1, a_2 | \rangle$ has an algebraic $[1, 2, C^{-n}]$-DFR. Finally, suppose $r > 2$. By the Nielsen-Schreier theorem, F_2 has a finite-index subgroup isomorphic to F_r; the claim immediately follows from Lemma 31(i). ◀

▶ **Theorem 37.** *Suppose $G = \langle S | R \rangle$, with S finite, such that $G \leq F_{r_1} \times \cdots \times F_{r_t}$, for some $r_1, \ldots, r_t \in \mathbb{N}$. Then $\exists C \in \mathbb{R}_{\geq 1}$ such that G has an algebraic $[t, 2, C^{-n}]$-DFR.*

Proof. By Lemma 36, each F_{r_i} has an algebraic $[1, 2, C_i^{-n}]$-DFR, for some $C_i \in \mathbb{R}_{\geq 1}$. Lemma 30 implies that $F_{r_1} \times \cdots \times F_{r_t}$ has an algebraic $[t, 2, C^{-n}]$-DFR, where $C = \max_i C_i$, and Lemma 31(i) then implies G has a DFR with the claimed parameters. ◀

As in Section 1.1, $\widehat{\Pi}_2$ denotes the class of finitely generated groups that are virtually a subgroup of a direct product of finitely-many finite-rank free groups.

▶ **Corollary 38.** *$\forall G \in \widehat{\Pi}_2, \exists K \in \mathbb{N}_{\geq 1}, \exists C \in \mathbb{R}_{\geq 1}$, such that G virtually has an algebraic $[K, 2, C^{-n}]$-DFR.*

We conclude with a "generic" construction that covers all groups that have algebraic DFRs. We remark that while this does partially subsume all other results in this section, it does not do so completely, as the earlier constructions of DFRs, for certain particular groups, yield better parameters.

▶ **Theorem 39.** *Consider a group $G = \langle S|R\rangle$, with S finite, where G is not the trivial group. Suppose G has a faithful representation $\pi : G \to \mathrm{U}(l, \overline{\mathbb{Q}})$. Then π has a (unique, up to isomorphism) set of irreducible subrepresentations $\{\pi_j : G \to \mathrm{U}(d_j, \overline{\mathbb{Q}})\}_{j=1}^m$ such that $\pi \cong \pi_1 \oplus \cdots \oplus \pi_m$. Let $d_{\max} = \max_j d_j$. Define the value d as follows: if $\bigcap_j \mathrm{Pker}(\pi_j) = \{1_G\}$, let $d = d_{\max}$, otherwise, let $d = d_{\max} + 1$. Partition the non-trivial π_j into isomorphism classes (i.e., only consider those π_j which are not the trivial representation; π_{j_1} and π_{j_2} belong to the same isomorphism class if $\pi_{j_1} \cong \pi_{j_2}$) and let k denote the number of isomorphism classes that appear. Then $\exists C \in \mathbb{R}_{\geq 1}$ such that G has an algebraic $[k, d, C^{-n}]$-DFR.*

Proof. Notice that, as G is not the trivial group, $d \geq 2$. Assume that the π_j are ordered such that $\pi_1, \ldots, \pi_k$ are representatives of the k distinct isomorphism classes of the non-trivial representations that appear among the π_j. For each $j \in \{1, \ldots, k\}$, define the representation $\rho_j = \pi_j \oplus \mathbf{1}_{d-d_j} : G \to \mathrm{U}(d, \overline{\mathbb{Q}})$. By Lemma 21, $\forall j \in \{1, \ldots, k\}, \exists C_j \in \mathbb{R}_{\geq 1}$ such that, $\forall g \notin \mathrm{Pker}(\rho_j)$, $|\chi_{\rho_j}(g)| \leq d - C_j^{-l(g)}$. Set $C = \max_j C_j$.

Next, notice that $\bigcap_j \mathrm{Pker}(\rho_j) = \{1_G\}$. If $\bigcap_j \mathrm{Pker}(\pi_j) = \{1_G\}$, then this is obvious. Suppose $\bigcap_j \mathrm{Pker}(\pi_j) \neq \{1_G\}$. Then $d = d_{\max} + 1 > d_j$, $\forall j$, which implies $\rho_j = \pi_j \oplus \mathbf{1}_{t_j}$, where $t_j := d - d_j \geq 1$. Therefore, for each j, $\rho_j(G) \cap Z(\mathrm{U}(d, \overline{\mathbb{Q}})) = I_d$, and so, by definition, $\mathrm{Pker}(\rho_j) = \ker(\rho_j)$. As π is faithful, $\{1_G\} = \bigcap_{j=1}^m \ker(\pi_j) = \bigcap_{j=1}^k \ker(\rho_j) = \bigcap_{j=1}^k \mathrm{Pker}(\rho_j)$.

Thus, $\forall g \in G_{\neq 1}$, $\exists j$ such that $g \notin \mathrm{Pker}(\rho_j)$, which implies $|\chi_{\rho_j}(g)| \leq d - C_j^{-l(g)} \leq d - C^{-l(g)}$. Therefore, $\{\rho_1, \ldots, \rho_k\}$ is an algebraic $[k, d, C^{-n}]$-DFR for G. ◀

3.3 Projective DFRs

A DFR $\mathcal{F} = \{\rho_1, \ldots, \rho_j\}$ of a group G is a set of unitary representations of G, i.e., group homomorphisms $\rho_j : G \to \mathrm{U}(d)$. We next consider a slight generalization. A *projective* unitary representation of G is a group homomorphism $\rho : G \to \mathrm{PU}(d) = \mathrm{U}(d)/Z(\mathrm{U}(d))$. We may (non-uniquely) lift any such ρ to a function $\widehat{\rho} : G \to \mathrm{U}(d)$ (i.e., $\gamma \circ \widehat{\rho} = \rho$, where $\gamma : \mathrm{U}(d) \to \mathrm{PU}(d)$ is the canonical projection). Note that $\widehat{\rho}$ is not necessarily a group homomorphism and that certain projective representations ρ cannot be lifted to an ordinary representation. However, for any two lifts, $\widehat{\rho}_1$ and $\widehat{\rho}_2$, of ρ, we have $|\chi_{\hat{\rho}_1}(g)| = |\chi_{\hat{\rho}_2}(g)|$, $\forall g \in G$. Therefore, the function $|\chi_\rho(\cdot)| : G \to \mathbb{R}$ given by $|\chi_\rho(g)| = |\chi_{\hat{\rho}}(g)|$ is well-defined.

We then define a $[k, d, \tau, \mathbb{A}]$-PDFR as a set of projective representations $\mathcal{F} = \{\rho_1, \ldots, \rho_j\}$ that satisfies Definition 16 where "representation" is replaced by "projective representation" in that definition. As we will observe in the following section, the same process that allows a DFR for a group G to be used to produce a 2QCFA for the word problem W_G, can also be applied to a PDFR. If a PDFR consists entirely of representations into $\mathrm{PU}(d, \overline{\mathbb{Q}}) = \mathrm{U}(d, \overline{\mathbb{Q}})/Z(\mathrm{U}(d, \overline{\mathbb{Q}}))$, we say it is an *algebraic* PDFR. The following variant of Theorem 39 follows by a precisely analogous proof.

▶ **Theorem 40.** *Suppose the group $G = \langle S|R\rangle$, with S finite, has a family $\mathcal{F} = \{\rho_1, \ldots, \rho_k\}$ of projective representations $\rho_j : G \to \mathrm{PU}(d, \overline{\mathbb{Q}})$, such that $\bigcap_j \ker(\rho_j) = \{1_G\}$. Then $\exists C \in \mathbb{R}_{\geq 1}$ such that $\mathcal{F}$ is an algebraic $[k, d, C^{-n}]$-PDFR for G.*

3.4 Unbounded-Error DFRs

If $\mathcal{F} = \{\rho_1, \ldots, \rho_k\}$ is a DFR for a group G, then $\bigcap_j \mathrm{Pker}(\rho_j) = \{1_G\}$. However, a crucial element in the definition of a DFR is the requirement that, much more strongly, all $g \in G_{\neq 1}$ are "far" from being in $\bigcap_j \mathrm{Pker}(\rho_j)$; in particular, if $\mathcal{F}$ is a $[k, d, \tau, \mathbb{A}]$-DFR, then $\forall g \in G_{\neq 1}, \exists j$ such that $|\chi_{\rho_j}(g)| \leq d - \tau(l(g))$. This requirement is essential in order for our construction

of a 2QCFA, that recognizes W_G using a DFR for G, to operate with *bounded* error. We next consider a generalization of a DFR, where this requirement is removed, which will then yield a 2QCFA that recognizes W_G with *unbounded* error.

We say $\mathcal{F} = \{\rho_1, \ldots, \rho_k\}$ is an *unbounded-error* $[k, d, \mathbb{A}]$-DFR for a group $G = \langle S|R\rangle$ if the conditions of Definition 16 hold, where Definition 16(b) is replaced by Definition 16(b)': $\forall g \in G_{\neq 1}$, $\exists j$ such that $|\chi_{\rho_j}(g)| < d$. This condition is equivalent to $\bigcap_j \mathrm{Pker}(\rho_j) = \{1_G\}$.

Note that, by Lemma 21, any algebraic unbounded-error $[k, d]$-DFR is also an algebraic $[k, d, C^{-n}]$-DFR, for some $C \in \mathbb{R}_{\geq 1}$; furthermore, as noted in the discussion following Definition 18, only a finitely generated abelian group could have a diagonal unbounded-error $[k, d]$-DFR, and all finitely generated abelian groups were shown to have DFRs in Theorem 34. Therefore, in order to obtain something new, we must consider unbounded-error DFRs that are neither algebraic nor diagonal. Due to space restrictions, we omit the proof of the following theorem, which may be found in the full version [28].

▶ **Theorem 41.** *$\forall G \in \widehat{\Pi}_3, \exists k \in \mathbb{N}$ such that G virtually has an unbounded-error $[k, 2, \widetilde{\mathbb{C}}]$-DFR.*

4 Recognizing the Word Problem of a Group with a 2QCFA

Consider a group $G = \langle S|R\rangle$, with S finite. As before, let $\Sigma = S \sqcup S^{-1}$, let $\phi : \Sigma^* \to G$ denote the natural map that takes each string in Σ^* to the element of G that it represents, and let $W_G := W_{G=\langle S|R\rangle} = \{w \in \Sigma^* : \phi(w) = 1_G\}$ denote the word problem of G with respect to the given presentation. Suppose $\mathcal{F} = \{\rho_1, \ldots, \rho_k\}$ is a $[k, d, \tau, \mathbb{A}]$-DFR (or PDFR) for G. By Proposition 17, if $w \in W_G$, then $|\chi_{\rho_j}(\phi(w))| = d$, $\forall j$, and if $w \notin W_G$, then $\exists j$ where $|\chi_{\rho_j}(\phi(w))| \leq d - \tau(l(\phi(w)))$. Let $G_j = \{g \in G : |\chi_{\rho_j}(g)| \leq d - \tau(l(g))\}$. A 2QCFA can recognize W_G by checking if $\phi(w) \in \bigcup_j G_j = G_{\neq 1}$. The well-known Hadamard test may be used to estimate $\chi_{\rho_j}(\phi(w)) = \mathrm{Tr}(\rho_j(\phi(w)))$; however, as we wish to produce a 2QCFA that has as few quantum states as possible, we wish to avoid the use of ancilla, and so we follow a slightly different approach. We begin by defining several useful 2QCFA subroutines.

▶ **Definition 42.** Suppose M is a 2QCFA with $d \geq 2$ quantum basis states $Q = \{q_1, \ldots, q_d\}$, quantum start state $q_1 \in Q$, and alphabet Σ.

(a) Suppose $|\psi_1\rangle = \sum_q \alpha_q |q\rangle$ and $|\psi_2\rangle = \sum_q \beta_q |q\rangle$, where $\alpha_q, \beta_q \in \overline{\mathbb{Q}}, \forall q \in Q$. There are (many) $t \in \mathrm{U}(d, \overline{\mathbb{Q}})$ such that $t|\psi_1\rangle = |\psi_2\rangle$. Let $\mathcal{T}_{|\psi_1\rangle \to |\psi_2\rangle}$ denote an arbitrary such t.

(b) Let $\pi : G \to \mathrm{U}(d)$ be a representation of G and let $|\psi\rangle = \sum_q \beta_q |q\rangle$, where $\beta_q \in \overline{\mathbb{Q}}$, $\forall q \in Q$. Then the *unitary round* $\mathcal{U}(\pi, |\psi\rangle)$ is a particular sub-computation of M on w, defined as follows. The round begins with the quantum register in the superposition $|q_1\rangle$ and the tape head at the right end of the tape. On reading $\#_R$, M performs the unitary transformation $\mathcal{T}_{|q_1\rangle \to |\psi\rangle}$ to its quantum register, and moves its head to the left. On reading a symbol $\sigma \in \Sigma$, M performs the unitary transformation $\pi(\phi(\sigma))$ to the quantum register and moves its head left. When the tape head first reaches the left end of the tape (i.e., the first time the symbol $\#_L$ is read), M performs the identity transformation to its quantum register, and does not move its head, at which point the round ends. As ϕ is a (monoid) homomorphism and π is a (group) homomorphism, we immediately conclude that, at the end of the round, the quantum register is in the superposition $\pi(\phi(w))|\psi\rangle$.

(c) For $t \in \mathrm{U}(d)$, a *measurement round* $\mathcal{M}(\pi, |\psi\rangle, t)$ is a sub-computation of M that begins with the unitary round $\mathcal{U}(\pi, |\psi\rangle)$. Then M performs the unitary transformation t, and does not move its head. After which M performs the quantum measurement specified by the partition $B = \{B_0, B_1\}$ of Q given by $B_0 = \{q_2, \ldots, q_d\}$ and $B_1 = \{q_1\}$, producing some *result* $r \in \{0, 1\}$; then M records r in its classical state, and does not move its head, at which point the round is over.

▶ **Lemma 43.** *Consider a group $G = \langle S|R\rangle$, with S finite, and let $W_G = W_{G=\langle S|R\rangle}$. The following statements hold.*

- **(i)** *If G has a diagonal $[k, d, C_1 n^{-C_2}, \mathbb{A}]$-DFR (or PDFR), for some $C_1, C_2 \in \mathbb{R}_{>0}$, then $\forall \epsilon \in \mathbb{R}_{>0}$, $W_G \in \mathsf{coR2QCFA}(n^{\lceil C_2 \rceil + 2}, \epsilon, d, \overline{\mathbb{Q}} \cup \mathbb{A})$.*
- **(ii)** *If G has a $[k, d, C_1^{-n}, \mathbb{A}]$-DFR (or PDFR), for some $C_1 \in \mathbb{R}_{\geq 1}$, then $\forall \epsilon \in \mathbb{R}_{>0}$, $\exists C_2 \in \mathbb{R}_{\geq 1}$ such that $W_G \in \mathsf{coR2QCFA}(C_2^n, \epsilon, d, \overline{\mathbb{Q}} \cup \mathbb{A})$.*
- **(iii)** *If G has an unbounded-error $[k, d, \mathbb{A}]$-DFR (or PDFR), then $W_G \in \mathsf{coN1QFA} \cap \mathsf{coN2QCFA}(n, d, \overline{\mathbb{Q}} \cup \mathbb{A})$.*

Proof Sketch. Suppose $\mathcal{F} = \{\rho_1, \ldots, \rho_k\}$ is a $[k, d, \tau, \mathbb{A}]$-DFR of G. Consider any $w \in \Sigma^*$. A 2QCFA M can perform a constant number of measurement rounds (i.e., the number of rounds only depends on k and d, not on $|w|$) using any representation ρ_j such that the following holds: (1) if $\phi(w) \in G_j \subseteq G_{\neq 1}$, then, with probability $\Omega(\tau(|w|))$, the results of those measurement rounds will allow M to be able to conclude *with certainty* that $w \notin W_G$, (2) if $\phi(w) = 1_G \notin G_j$, then the results of those measurement rounds will *never* cause M to incorrectly conclude that $w \notin W_G$. After running this procedure approximately $\tau(n)$ times, for each j, the following holds: (1) if $\phi(w) \in G_{\neq 1} = \bigcup_j G_j$, then $\phi(w) \in G_j$ for at least some j, and so, with probability $\Omega(1)$, M is able to conclude (with certainty) that $w \notin W_G$, (2) if $\phi(w) = 1_G$, then M will never incorrectly conclude that $w \notin W_G$. As soon as M performs a measurement round whose result allows it to conclude that $w \notin W_G$, M immediately rejects. In order to correctly accept all $w \in W_G$, M will run a procedure between measurement rounds that will cause it to accept *any* input w with some small probability, and otherwise continue; by setting this acceptance probability small enough, we assure that any $w \notin W_G$ is not (incorrectly) accepted with high probability. A formal proof can be found in the full version [28]. ◀

Moreover, if H is a finite-index subgroup of G, a 2QCFA that recognizes W_G can be constructed from a 2QCFA that recognizes W_H.

▶ **Lemma 44.** *Consider a group $H = \langle S_H|R_H\rangle$, with S_H finite, and suppose that A_H is a 2QCFA that recognizes W_H, which operates in the manner of our proof of Lemma 43. Further suppose G is a group such that $H \leq G$ and $[G : H]$ is finite. Then G admits a presentation $G = \langle S_G|R_G\rangle$, with S_G finite, such that there is a 2QCFA A_G that recognizes W_G. Moreover, A_G has the same acceptance criteria, asymptotic expected running time, number of quantum basis states, and class of transition amplitudes as A_H.*

Using the above results, and the constructions of DFR from Section 3, the theorems stated in Section 1.1 concerning the recognizability of word problems by 2QCFA easily follow; proofs of the above results and of these theorems appear in the full version [28].

5 Discussion

In this paper, we have shown that 2QCFA can recognize the word problems of many groups. In particular, let $\widehat{\Pi}_1$ (resp. $\widehat{\Pi}_2$) denote the collection of all finitely generated groups that are virtually abelian (resp. virtually a subgroup of a direct product of finitely-many finite-rank free groups), and let $\mathcal{Q}$ denotes the class of groups for which Theorem 10 applies. Then a 2QCFA, with a single-qubit quantum register and algebraic number transition amplitudes, can recognize, with one-sided bounded error, the word problem W_G of any $G \in \widehat{\Pi}_1$ (resp. $G \in \widehat{\Pi}_2$) in expected polynomial (resp. exponential) time. Moreover, if allowed a quantum register of any constant size, such a 2QCFA may recognize the word problem of any group $G \in \mathcal{Q}$ with one-sided bounded error in expected exponential time.

In a companion paper [27], we establish a lower bound on the running time of any 2QCFA (with any size quantum register and no restrictions placed on its transition amplitudes) that recognizes a word problem W_G with bounded error (even under the more generous notion of two-sided bounded error); more strongly, we establish a lower bound on the running time of *any quantum Turing machine* that uses *sublogarithmic* space, though we will not discuss that here. In particular, we show that, $\forall G \in \mathcal{Q} \setminus \widehat{\Pi}_1$, W_G *cannot* be recognized by such a 2QCFA is expected time $2^{o(n)}$. Therefore, the algorithm exhibited in this paper for recognizing the word problem of any group $G \in \mathcal{Q} \setminus \widehat{\Pi}_1$ has (essentially) optimal expected running time; moreover, we have obtained the first provable separation between the classes of languages recognizable with bounded error by 2QCFA in expected exponential time and in expected subexponential time. In that same paper, we also show that if a 2QCFA of this most general type recognizes a word problem W_G in expected polynomial time, then $G \in \mathcal{G}_{vNilp}$, where $\mathcal{G}_{vNilp}$ denotes the finitely generated virtually nilpotent groups, and $\widehat{\Pi}_1 \subsetneq \mathcal{G}_{vNilp}$. This naturally raises the following question.

▶ Open Problem 1. Is there a group $G \in (\mathcal{G}_{vNilp} \setminus \widehat{\Pi}_1)$ such that W_G can be recognized by a 2QCFA with bounded error in expected polynomial time?

We have shown that the (three-dimensional discrete) Heisenberg group $H \in (\mathcal{G}_{vNilp} \setminus \widehat{\Pi}_1)$ is "complete" for this question, in the sense that if W_H *cannot* be recognized with bounded error by a 2QCFA in expected polynomial time, then no such G can [27].

Let $\mathcal{G}_{vSolvLin}$ denote the finitely generated virtually solvable linear groups over a field of characteristic zero, and note that $\mathcal{G}_{vNilp} \subsetneq \mathcal{G}_{vSolvLin}$. Furthermore, note that $W_G \in \mathsf{L}$, $\forall G \in \mathcal{G}_{vSolvLin}$ [20]. However, every $G \in \mathcal{G}_{vSolvLin} \setminus \widehat{\Pi}_1$ *does not* have a faithful finite-dimensional unitary representation (see, for instance, [33, Proposition 2.2]) and, therefore, does not have a DFR (even an unbounded-error DFR); this prevents the techniques of this paper from producing a 2QCFA that recognizes the corresponding W_G.

▶ Open Problem 2. Is there a finitely generated group G that does not have a faithful finite-dimensional unitary representation (for example, any $G \in \mathcal{G}_{vSolvLin} \setminus \widehat{\Pi}_1$ or any finitely generated infinite Kazhdan group) such that W_G can be recognized with bounded error by a 2QCFA at all (i.e., in any time bound)?

Consider the group $\mathbb{Z} * \mathbb{Z}^2 \in \Sigma_2 \subsetneq \widehat{\Pi}_3$, and note that $\mathbb{Z} * \mathbb{Z}^2 \notin \widehat{\Pi}_2$. The complexity of $W_{\mathbb{Z}*\mathbb{Z}^2}$ has been considered by many authors and it is conjectured that $W_{\mathbb{Z}*\mathbb{Z}^2} \notin \mathsf{poly{-}CFL}$ [7] (cf. [8]) and that $W_{\mathbb{Z}*\mathbb{Z}^2} \notin \mathsf{coCFL}$ [18]. By Theorem 11, $W_{\mathbb{Z}*\mathbb{Z}^2}$ is recognizable with one-sided *unbounded* error by a 2QCFA. We ask the following questions.

▶ Open Problem 3. Can $W_{\mathbb{Z}*\mathbb{Z}^2}$ be recognized by a 2QCFA with bounded error? More generally, is $W_{\mathbb{Z}*\mathbb{Z}^r}$ recognizable by a 2QCFA with bounded error, $\forall r \in \mathbb{N}$?

▶ Open Problem 4. Does $\mathbb{Z} * \mathbb{Z}^2$ have an algebraic DFR. More generally, does $\mathbb{Z} * \mathbb{Z}^r$ have an algebraic DFR, $\forall r \in \mathbb{N}$? Even more generally, is the class of groups which have algebraic DFRs closed under free product?

References

1 Andris Ambainis and John Watrous. Two-way finite automata with quantum and classical states. *Theoretical Computer Science*, 287(1):299–311, 2002.

2 Andris Ambainis and Abuzer Yakaryılmaz. Automata and quantum computing. *arXiv preprint*, 2015. `arXiv:1507.01988`.

3 Ao V Anisimov. Group languages. *Cybernetics and Systems Analysis*, 7(4):594–601, 1971.

4 Alan Baker. *Transcendental number theory*. Cambridge university press, 1990.

5 J-C Birget, A Yu Ol'shanskii, Eliyahu Rips, and Mark V Sapir. Isoperimetric functions of groups and computational complexity of the word problem. *Annals of Mathematics*, pages 467–518, 2002.

6 Alex Brodsky and Nicholas Pippenger. Characterizations of 1-way quantum finite automata. *SIAM Journal on Computing*, 31(5):1456–1478, 2002.

7 Tara Brough. Groups with poly-context-free word problem. *Groups Complexity Cryptology*, 6(1):9–29, 2014.

8 Tullio Ceccherini-Silberstein, Michel Coornaert, Francesca Fiorenzi, Paul E Schupp, and Nicholas WM Touikan. Multipass automata and group word problems. *Theoretical Computer Science*, 600:19–33, 2015.

9 Cynthia Dwork and Larry Stockmeyer. A time complexity gap for two-way probabilistic finite-state automata. *SIAM Journal on Computing*, 19(6):1011–1023, 1990.

10 Cynthia Dwork and Larry Stockmeyer. Finite state verifiers i: The power of interaction. *Journal of the ACM (JACM)*, 39(4):800–828, 1992.

11 Rūsiņš Freivalds. Probabilistic two-way machines. In *International Symposium on Mathematical Foundations of Computer Science*, pages 33–45. Springer, 1981.

12 Alex Gamburd, Dmitry Jakobson, and Peter Sarnak. Spectra of elements in the group ring of su (2). *Journal of the European Mathematical Society*, 1(1):51–85, 1999.

13 Albert G Greenberg and Alan Weiss. A lower bound for probabilistic algorithms for finite state machines. *Journal of Computer and System Sciences*, 33(1):88–105, 1986.

14 Lov K Grover. A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-Eighth Annual ACM Symposium of Theory of Computing*, pages 212–219, 1996.

15 Aram W Harrow, Avinatan Hassidim, and Seth Lloyd. Quantum algorithm for linear systems of equations. *Physical review letters*, 103(15):150502, 2009.

16 Thomas Herbst. On a subclass of context-free groups. *RAIRO-Theoretical Informatics and Applications-Informatique Théorique et Applications*, 25(3):255–272, 1991.

17 Derek F Holt, Matthew D Owens, and Richard M Thomas. Groups and semigroups with a one-counter word problem. *Journal of the Australian Mathematical Society*, 85(2):197–209, 2008.

18 Derek F Holt, Sarah Rees, Claas E Röver, and Richard M Thomas. Groups with context-free co-word problem. *Journal of the London Mathematical Society*, 71(3):643–657, 2005.

19 Emmanuel Kowalski. *An introduction to the representation theory of groups*, volume 155. American Mathematical Society, 2014.

20 Richard J Lipton and Yechezkel Zalcstein. Word problems solvable in logspace. *Journal of the ACM (JACM)*, 24(3):522–526, 1977.

21 Clara Löh. *Geometric group theory*. Springer, 2017.

22 Cristopher Moore and James P Crutchfield. Quantum automata and quantum grammars. *Theoretical Computer Science*, 237(1-2):275–306, 2000.

23 David E Muller and Paul E Schupp. Groups, the theory of ends, and context-free languages. *Journal of Computer and System Sciences*, 26(3):295–310, 1983.

24 Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

25 Michael O Rabin. Probabilistic automata. *Information and control*, 6(3):230–245, 1963.

26 Michael O Rabin and Dana Scott. Finite automata and their decision problems. *IBM journal of research and development*, 3(2):114–125, 1959.

27 Zachary Remscrim. Lower bounds on the running time of two-way quantum finite automata and sublogarithmic space quantum turing machines. *Electronic Colloquium on Computational Complexity (ECCC)*, 26:182, 2019. URL: `https://eccc.weizmann.ac.il/report/2019/182`.

28 Zachary Remscrim. The power of a single qubit: Two-way quantum/classical finite automata and the word problem for linear groups. *Electronic Colloquium on Computational Complexity (ECCC)*, 26:107, 2019. URL: `https://eccc.weizmann.ac.il/report/2019/107`.

29 AC Say and Abuzer Yakaryilmaz. Magic coins are useful for small-space quantum machines. *Quantum Information & Computation*, 17(11-12):1027–1043, 2017.

30 Wolfgang M Schmidt. Simultaneous approximation to algebraic numbers by rationals. *Acta Mathematica*, 125(1):189–201, 1970.

31 Peter W Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

32 John Stallings. A finitely presented group whose 3-dimensional integral homology is not finitely generated. *American Journal of Mathematics*, 85(4):541–543, 1963.

33 Andreas Thom. Convergent sequences in discrete groups. *Canadian Mathematical Bulletin*, 56(2):424–433, 2013.

34 John Watrous. On the complexity of simulating space-bounded quantum computations. *Computational Complexity*, 12(1-2):48–84, 2003.

35 John Watrous. *The theory of quantum information*. Cambridge University Press, 2018.

36 Abuzer Yakaryilmaz and AC Cem Say. Languages recognized by nondeterministic quantum finite automata. *Quantum Information & Computation*, 10(9):747–770, 2010.

37 Abuzer Yakaryilmaz and AC Cem Say. Succinctness of two-way probabilistic and quantum finite automata. *Discrete Mathematics and Theoretical Computer Science*, 12(4):19–40, 2010.