Electronic Colloquium on Computational Complexity, Report No. 30 (2002)

Inapproximability Results for Equations over Finite Groups

Lars Engebretsen [a,1] Jonas Holmerin [a] Alexander Russell [b]

[a] *Department of Numerical Analysis and Computer Science, Royal Institute of Technology, SE-100 44 Stockholm, SWEDEN*

[b] *Department of Computer Science and Engineering, University of Connecticut, Storrs, CT 06269, USA*

Abstract

An *equation* over a finite group G is an expression of form $w_1 w_2 \ldots w_k = 1_G$, where each w_i is a variable, an inverted variable, or a constant from G; such an equation is *satisfiable* if there is a setting of the variables to values in G so that the equality is realized. We study the problem of simultaneously satisfying a family of equations over a finite group G and show that it is **NP**-hard to approximate the number of simultaneously satisfiable equations to within $|G| - \epsilon$ for any $\epsilon > 0$. This generalizes results of Håstad (2001, J. ACM, 48 (4)), who established similar bounds under the added condition that the group G is Abelian.

Key words: Optimization, Approximation, Groups, Finite groups, Probabilistically Checkable Proofs, NP-hardness

1 Introduction

Many fundamental computational problems can be naturally posed as questions concerning the simultaneous solvability of families of equations over finite groups. This connection has been exploited to achieve a variety of strong inapproximability results for problems such as Max Cut, Max Di-Cut, Exact

Email addresses: `enge@kth.se` (Lars Engebretsen), `joho@kth.se` (Jonas Holmerin), `acr@cse.uconn.edu` (Alexander Russell).

[1] Parts of this research was performed while the author was visiting MIT with support from the Marcus Wallenberg Foundation and the Royal Swedish Academy of Sciences.

ISSN 1433-8092

Satisfiability, and Vertex Cover [8,10,11,15–17,20,26]. A chief technical ingredient in these hardness results is a tight lower bound on the approximability of the problem of simultaneously satisfying equations over a finite *Abelian* group; in this article we extend these results to cover all finite groups.

An *equation* in variables $x_1, \ldots, x_n$ over a group G is an expression of form $w_1 \ldots w_k = 1_G$, where each w_i is either a variable, an inverted variable, or a group constant and 1_G denotes the identity element. A *solution* is an assignment of the variables to values in G that realizes the equality. A collection of equations $\mathcal{E}$ over the same variables induces a natural optimization problem, the problem of determining the maximum number of simultaneously satisfiable equations in $\mathcal{E}$. We let EQ_G denote this optimization problem. The special case where a variable may only appear *once* in each equation is denoted EQ^1_G; when each equation has single occurrences of exactly k variables, the problem is denoted $\mathrm{EQ}^1_G[k]$. Our main theorem asserts that for any finite group G it is $\mathbf{NP}$-hard to approximate $\mathrm{EQ}^1_G[3]$ (and hence EQ^1_G and EQ_G) to within $|G| - \epsilon$ for any $\epsilon > 0$; this is tight.

As mentioned above, EQ_G is tightly related to a variety of familiar optimization problems. When $G = \boldsymbol{Z}_2$, for example, instances of EQ_G where exactly two variables occur in each clause, i.e., $\mathrm{EQ}^1_{\boldsymbol{Z}_2}[2]$, correspond precisely to the familiar optimization problem Max Cut, the problem of determining the largest number of edges which cross some bipartition of an undirected graph. If, for example, $G = S_3$, the (non-Abelian) symmetric group on three letters, then the problem of maximizing the number of bichromatic edges in a three coloring of a given graph can be reduced to EQ_G [14]; other examples are described by Håstad [16] and Zwick [26]. The general problem has also been studied due to applications to the fine structure of $\mathbf{NC}^1$ [3,14] specializing the framework of Barrington *et al.* [4,5]. Finally, the problem naturally gives rise to a number of well-studied combinatorial enumeration problems: see, e.g., [6,13,24] and [23, pp. 110ff.].

If G is Abelian and $\mathcal{E}$ is a collection of equations over G, each of which can individually be satisfied, the trivial randomized approximation algorithm which independently assigns each variable to a uniformly selected value in G satisfies an expected fraction $|G|^{-1}$ of the equations. This algorithm can be efficiently derandomized by the method of conditional expectation [1, §15.1] and it in fact also applies to EQ^1_G for any finite group G. To be more precise, it applies to systems of equations over any finite group G where each equation has the property that there is at least one variable occurring only once in the equation. In 1997, Håstad [16] showed that if $\mathbf{P} \neq \mathbf{NP}$ and G is Abelian, then no polynomial time approximation algorithm can approximate $\mathrm{EQ}^1_G[3]$ to within $|G| - \epsilon$ for any $\epsilon > 0$. The main theorem of this paper shows that this same lower bound holds for all finite groups.

Theorem 1 *For any finite group G and any constant $\epsilon > 0$, it is* ***NP****-hard to approximate* $\mathrm{EQ}^1_G[3]$ *to within* $|G| - \epsilon$.

The paper is organized as follows: After an overview of our contribution in Sec. 2 we briefly describe the representation theory of finite groups and the generalization of the so called *long code* to non-Abelian groups in Sections 3 and 4. The main theorem then appears in Section 5.

2 Overview of our results

A burst of activity focusing on the power of various types of interactive proof systems in the 80s and early 90s culminated in the so called *PCP theorem*, described briefly below. A *probabilistically checkable proof system* (PCP) for a language L consists of a probabilistic polynomial time verifier which, given an input x and oracle access to a purported proof that $x \in L$, probabilistically verifies the validity of the proof. In this paper, we only consider PCPs where the number of random bits used by the verifier is *logarithmic in the input size* and the number of "positions" of the proof examined by the verifier is a *constant*. The verifier is also *nonadaptive* in the sense that the queries may not depend on the values of previously queried positions in the proof. A PCP is said to have *completeness* c and *soundness* s if a correct proof that $x \in L$ is accepted with probability at least c and, when $x \notin L$, no proof is accepted with probability exceeding s.

The PCP theorem [2] asserts the startling fact that any **NP**-language has a PCP with completeness 1 and soundness $1/2$ where the verifier uses logarithmic randomness and examines a constant number of bits of the proof. To prove our inapproximability results for certain families of equations over finite groups we use the PCP theorem to construct, for any finite group G and any positive constants ϵ and δ, a PCP with completeness $1 - \epsilon$ and soundness $|G|^{-1} + \delta$ where the verifier uses logarithmic randomness and examines *three positions* in the proof. Each position in our proof contains a value from G and the verifier tests the validity of the proof by checking a certain linear constraint on the three queried positions.

There is an approximation-preserving reduction from conjunctive normal form Boolean formulas containing exactly three literals per clause (E3-Sat) to E3-Sat formulas where each variable occurs in exactly five clauses [12,18]. Coupling the PCP theorem and this reduction shows that for every language L in **NP**, an arbitrary instance x can be transformed in polynomial time into an E3-Sat formula $\phi_{x,L}$ with the following property: if $x \in L$, then $\phi_{x,L}$ is satisfiable, and if $x \notin L$ then at most a fraction $\mu < 1$ of the clauses can be satisfied. Here μ is a universal constant, independent of the language and the instance.

In his seminal paper [16], Håstad introduced a methodology for proving lower bounds for constraint satisfaction problems. At a high level, the method can be viewed as a simulation of the well-known two-prover one-round (2P1R) protocol for E3-Sat where the verifier sends a variable to one prover and a clause containing that variable to the other prover, accepting if the returned assignments are consistent and satisfy the clause. It follows from Raz's parallel repetition theorem [19] that if the 2P1R protocol is repeated u times in parallel and applied to the formula $\phi_{x,L}$ above then the verifier always accepts an unsatisfiable formula with probability at most c_μ^u where $c_\mu < 1$ is independent of u.

To prove his inapproximability result for equations over finite Abelian groups, Håstad constructed a PCP where the verifier tests a given assignment of variables $x_1, \ldots, x_n$ to group values to determine if it satisfies an equation selected at random from a certain family of equations. As each such equation involves three variables, this can be tested with three oracle queries. He then, in essence, reduced the problem of finding a strategy for the 2P1R protocol for E3-Sat to the problem of finding an assignment which satisfies many of the group equations by showing that if the verifier in the PCP accepts with high probability, there is a strategy for the provers in the 2P1R protocol that makes the verifier of that protocol accept with high probability. The inapproximability result follows since it is known that the verifier in the latter protocol cannot accept an unsatisfiable instance of E3-Sat with high probability.

To adapt Håstad's method to equations over arbitrary finite groups we need to overcome a couple of technical difficulties. The first one regards the coding of the proof in Håstad's proof system. Our second two contributions regard the analysis of the probability that the verifier accepts an incorrect proof. These are surveyed briefly in §2.1 and §2.2, below.

2.1 The non-Abelian long code

To encode the proof, Håstad used a proof with several different tables, each coded with the so called *long code*. For any finite group G, the long G-code of a binary string x of length n consists of the values of all functions from n-bit strings to G evaluated on x. In his proofs, Håstad has to assume that the alleged proofs that the verifier examines have a certain structure. For instance, the positions corresponding to some function f and the function gf for any $g \in G$ must be consistent. This can be enforced by employing certain *access conventions* in the verifier, which we describe in detail later. Our first technical contribution in this paper is to formulate the Fourier transform of the long

G-code for all finite groups G and to prove that certain access conventions, slightly different from those used by Håstad, imply that we can assume that the Fourier coefficients of the alleged proofs examined by our verifier have certain desirable properties.

2.2 Analysis of the verifier

Our main technical contributions are from the part of the analysis where we establish the connection between the proof system that tests a group equation and the 2P1R protocol for E3-Sat. The first step in this analysis is to "arithmetize" the acceptance probability of the former protocol. For the case of an Abelian finite group G, this is straightforward: The acceptance probability can be written as a sum of $|G|$ terms. If the acceptance probability is large, there has to be at least one large term in the sum. Håstad then proceeds by expanding this allegedly large term in its Fourier expansion and then uses the Fourier coefficients to devise a strategy for the provers in the 2P1R game for E3-Sat. Specifically, the probability distribution induced by the Fourier coefficients is used to construct a probabilistic strategy for the provers in the 2P1R game. Roughly speaking, the acceptance probability of the verifier in the 2P1R game is large because some pair of related Fourier coefficients is large.

For non-Abelian groups, the way to arithmetize the test turns out to require a sum of the traces of products of certain matrices given by the representation theory of the group in question. As in Håstad's case, we find that if the acceptance probability of the linear test is large, there has to be one product of matrices with a large trace. Our next step is to expand this matrix product in its Fourier series. Unfortunately, the Fourier expansion of each entry in those matrices contains matrices that could be very large; consequently, the Fourier expansion of the entire trace contains a product of matrices with potentially huge dimension. Thus, the fact that this trace is large does not necessarily mean that the individual entries in the matrices are large and directly using the entries in the matrices to construct the probabilistic strategy for the provers in the 2P1R game does not appear to work. Instead, and this is our first main technical contribution, we prove that the terms in the Fourier expansion corresponding to matrices with large dimension cannot contribute much to the value of the trace. Having done that, we know that the terms corresponding to matrices with reasonably small dimension actually sum up to a significantly large value and we use those terms to construct a strategy for the provers in the 2P1R game; this is our second main technical contribution.

3 Representation theory and the Fourier transform

In this section, we give a short account of the representation theory needed to state and prove our results. For more details, we refer the reader to the excellent accounts by Serre [22] and Terras [25].

The traditional Fourier transform, as appearing in, say, signal processing [9], algorithm design [21], or PCPs [16], focuses on decomposing functions $f\colon G \to \boldsymbol{C}$ defined over an Abelian group G. This "decomposition" proceeds by writing f as a linear combination of *characters* of the group G. Unfortunately, this same procedure cannot work over a non-Abelian group since in this case there are not enough characters to span the space of all functions from G into $\boldsymbol{C}$; the theory of group representations fills this gap, being the natural framework for Fourier analysis over non-Abelian groups and shall be the primary tool utilized in the analysis the "non-Abelian PCPs" introduced in Section 4.

Group representation theory studies realizations of groups as collections of matrices: specifically, a *representation* of a group G associates a matrix with each group element so that the group multiplication operation corresponds to normal matrix multiplication. Such an association gives an embedding of the group into $\mathrm{GL}(V)$, the group of invertible linear operators on a finite dimensional $\boldsymbol{C}$-vector space V. (Note that if V is one-dimensional, then this is exactly the familiar notion of character used in the Fourier analysis over Abelian groups.)

Definition 2 *Let G be a finite group. A* representation *of G is a homomorphism $\gamma\colon G \to \mathrm{GL}(V)$; the dimension of V is denoted by d_γ and called the* dimension of the representation.

Two representations are immediate: the *trivial representation* has dimension 1 and maps everything to 1. The permutation action of a group on itself gives rise to the *left regular representation.* Concretely, let V be a $|G|$-dimensional vector space with an orthogonal basis $B = \{e_g : g \in G\}$ indexed by elements of G. Then the *left regular representation* $\mathrm{reg}\colon G \to \mathrm{GL}(V)$ is given by $\mathrm{reg}(g)\colon e_h \mapsto e_{gh}$; the matrix associated with $\mathrm{reg}(g)$ is simply the permutation matrix given by mapping each element h of G to gh.

If γ is a representation, then for each group element g, $\gamma(g)$ is a linear operator and, as mentioned above, can be identified with a matrix. We denote by $(\gamma(g)_{ij})$ the matrix corresponding to $\gamma(g)$. Two representations γ and θ of G are *isomorphic* if they have the same dimension and there is a change of basis U so that $U\gamma(g)U^{-1} = \theta(g)$ for all g. A representation non-isomorphic to the trivial representation is said to be *nontrivial.*

If $\gamma\colon G \to \mathrm{GL}(V)$ is a representation and $W \subseteq V$ is a subspace of V, we say that W is *invariant* if $\gamma(g)(W) \subseteq W$ for all g. If the only invariant subspaces are $\{0\}$ and V, we say that γ is *irreducible*. Otherwise, γ does have a nontrivial invariant subspace W_0 and notice that by restricting each $\gamma(g)$ to W_0 we obtain a new representation. When this happens, it turns out that there is always another invariant subspace W_1 so that $V = W_0 \oplus W_1$ and in this case we write $\gamma = \gamma_0 \oplus \gamma_1$, where γ_0 and γ_1 are the representations obtained by restricting to W_0 and W_1. This is equivalent to the existence of a basis in which the $\gamma(g)$ are all block diagonal, where the matrix of $\gamma(g)$ consists of $\gamma_0(g)$ on the first block and $\gamma_1(g)$ on the second block. In this way, any representation can be decomposed into a sum of irreducible representations. The matrix entries of irreducible representations of a finite group G are orthogonal with respect to the pairing function

$$\langle f_1 \mid f_2 \rangle_G = \frac{1}{|G|} \sum_{g \in G} f_1(g) f_2(g^{-1}) \tag{1}$$

for functions from G to $\boldsymbol{C}$:

Proposition 3 *Let γ and θ be two non-isomorphic irreducible representations of G. Suppose that they are represented by the matrices (γ_{ij}) and $(\theta_{k\ell})$, respectively. Then $\langle \gamma_{ij} \mid \theta_{k\ell} \rangle_G = 0$ for all i, j, k, l and $d_\gamma \langle \gamma_{ij} \mid \gamma_{k\ell} \rangle_G = \delta_{ik}\delta_{j\ell}$.*

In particular, any nontrivial representation is orthogonal to the trivial representation:

Corollary 4 *Let $\gamma \colon G \to V$ be a nontrivial irreducible representation of G. Then $\sum_{g \in G} \gamma(g) = 0$.*

For a finite group G, there are only a finite number of irreducible representations up to isomorphism; we let $\hat{G}$ denote the set of distinct irreducible representations of G. It is not hard to show that any irreducible representation is isomorphic to a representation where each $\gamma(g)$ is unitary, and we will always work under this assumption.

There is also a natural product of representations, the *tensor product*. We define the tensor product $A \otimes B$ of two matrices $A = (a_{ij})$ and $B = (b_{k\ell})$ to be the matrix indexed by pairs $(i,k);(j,\ell)$ so that $(A \otimes B)_{(i,k);(j,\ell)} = a_{ij} b_{k\ell}$. We will use the so called *inner trace* of a tensor product: For a matrix M indexed by pairs $(i,k);(j,\ell)$ the inner trace, denoted by $\operatorname{Tr} M$, is defined by $(\operatorname{Tr} M)_{ij} = \sum_k M_{(i,k),(j,k)}$. We let tr denote the normal trace. The inner trace is the "opposite" of the tensor product in the sense that $\operatorname{Tr}(A \otimes B) = (\operatorname{tr} B) A$. If γ and θ are representations of G and H, respectively, we define $\gamma \otimes \theta$ to be the representation of $G \times H$ given by $(\gamma \otimes \theta)(g,h) = \gamma(g) \otimes \theta(h)$.

Proposition 5 *Let G and H be finite groups. Then the irreducible representations of $G \times H$ are precisely $\{\gamma \otimes \theta \mid \gamma \in \hat{G}, \theta \in \hat{H}\}$. Furthermore, each of* *these representations is distinct up to isomorphism.*

For a representation γ, the function $g \mapsto \operatorname{tr}\gamma(g)$ is called the *character corresponding to* γ and is denoted by χ_γ. Note that χ_γ takes values in $\boldsymbol{C}$ even if γ has dimension larger than 1. Our principal use of the character comes from the following fact:

Proposition 6 *Let g be an element of G. Then $\sum_{\gamma\in\hat{G}} d_\gamma \chi_\gamma(g) = |G|$ if $g = 1_G$ and $\sum_{\gamma\in\hat{G}} d_\gamma\chi_\gamma(g) = 0$ otherwise.*

3.1 The Fourier transform

We now proceed to describe the Fourier transform of functions from an arbitrary finite group G to $\boldsymbol{C}$. Let f be a function from G to $\boldsymbol{C}$ and γ be an irreducible representation of G. Then

$$\hat{f}_\gamma = \frac{1}{|G|}\sum_{g\in G} f(g)\gamma(g) \tag{2}$$

is the *Fourier coefficient of f at* γ. Moreover, f can be written as a Fourier series

$$f(g) = \sum_{\gamma\in\hat{G}} d_\gamma \operatorname{tr}\left(\hat{f}_\gamma\gamma(g^{-1})\right) \tag{3}$$

In our analysis, we need the following version of Plancherel's equality:

Lemma 7 *Suppose that f is a function from G to $\boldsymbol{C}$. Then*

$$\sum_{\gamma\in\hat{G}}\sum_{1\le i\le d_\gamma}\sum_{1\le j\le d_\gamma} d_\gamma\left|\langle f \mid \gamma_{ij}\rangle_G\right|^2 = \frac{1}{|G|}\sum_{g\in G}|f(g)|^2 \tag{4}$$

if the representations $\gamma\in\hat{G}$ are represented in unitary bases.

PROOF. We expand the expression above using the definition of $\langle\cdot \mid \cdot\rangle_G$:

$$\left|\langle f \mid \gamma_{ij}\rangle_G\right|^2 = \frac{1}{|G|^2}\sum_{g\in G}\sum_{h\in G} f(g)\gamma_{ij}(g^{-1})f^*(h)\left(\gamma_{ij}(h^{-1})\right)^*$$

Since γ is a unitary representation, $\gamma(h^{-1}) = \gamma^{-1}(h) = \gamma^*(h)$, and hence $\gamma_{ij}(h^{-1}) = (\gamma_{ji}(h))^*$. Therefore,

$$\begin{aligned}
&\sum_{\gamma\in\hat{G}} \sum_{1\le i\le d_\gamma} \sum_{1\le j\le d_\gamma} d_\gamma \Big|\langle f \mid \gamma_{ij}\rangle_G\Big|^2 \\
&\qquad = \frac{1}{|G|^2} \sum_{\gamma\in\hat{G}} d_\gamma \sum_{1\le i\le d_\gamma} \sum_{1\le j\le d_\gamma} \sum_{g\in G} \sum_{h\in G} f(g) f^*(h) \gamma_{ij}(g^{-1}) \gamma_{ji}(h) \\
&\qquad\quad = \frac{1}{|G|^2} \sum_{g\in G} \sum_{h\in G} f(g) f^*(h) \sum_{\gamma\in\hat{G}} d_\gamma \operatorname{tr}\Big(\gamma(g^{-1})\gamma(h)\Big) \\
&\qquad\quad = \frac{1}{|G|^2} \sum_{g\in G} \sum_{h\in G} f(g) f^*(h) \sum_{\gamma\in\hat{G}} d_\gamma \operatorname{tr}\Big(\gamma(g^{-1}h)\Big) = \frac{1}{|G|} \sum_{g\in G} |f(g)|^2,
\end{aligned}$$

where the last equality follows from Proposition 6. (See also Serre's account [22, §6.2, Exercise 6.2], which disucsses this in different language.)

3.2 The Fourier transform of matrix-valued functions

We also need to use the Fourier transform on functions $f\colon G \to \mathrm{End}(V)$, where $\mathrm{End}(V)$ is the set of linear maps from the vector space V to itself; we here identify $\mathrm{End}(V)$ with the space of all $\dim V \times \dim V$ matrices over $\boldsymbol{C}$. Although we have not found any treatment of such transforms in the literature, it is straightforward to generalize the concepts from the previous section to matrix-valued functions. For a representation γ of G, we define

$$\hat{f}_\gamma = \frac{1}{|G|} \sum_{g\in G} f(g) \otimes \gamma(g). \tag{5}$$

Treating the $f(g)$ as matrices, this is nothing more than the component-wise Fourier transform of the function f. The reason for grouping them together into these tensor products is the following: Let $f, h\colon G \to \mathrm{End}(V)$ be two such functions, and define their convolution as

$$(f * h)(g) = \frac{1}{|G|} \sum_{t\in G} f(t) h(t^{-1}g),$$

this product being the ring product in $\mathrm{End}(V)$ (that is, function composition). Then it turns out that $(\widehat{f * h})_\gamma = \hat{f}_\gamma \hat{h}_\gamma$, this product being matrix multiplication:

$$
\begin{aligned}
(\widehat{f * h})_\gamma &= \frac{1}{|G|} \sum_{g \in G} (f * h)(g) \otimes \gamma(g) \\
&= \frac{1}{|G|^2} \sum_{g \in G} \sum_{t \in G} \Big(f(t) h(t^{-1} g) \Big) \otimes \gamma(t t^{-1} g) \\
&= \frac{1}{|G|^2} \sum_{g \in G} \sum_{t \in G} \Big(f(t) \otimes \gamma(t) \Big) \Big(h(t^{-1} g) \otimes \gamma(t^{-1} g) \Big) \\
&= \hat{f}_\gamma \hat{h}_\gamma .
\end{aligned}
$$

In this case, the Fourier series is

$$
f(g) = \sum_{\gamma \in \hat{G}} d_\gamma \operatorname{Tr}\Big(\hat{f}_\gamma \Big(\boldsymbol{I} \otimes \gamma(g^{-1}) \Big) \Big) \tag{6}
$$

where $\operatorname{Tr} M$ is the inner trace. This also gives rise to a Plancherel equality: for two functions $f, h \colon G \to \operatorname{End}(V)$,

$$
\frac{1}{|G|} \sum_{g \in G} f(g) h(g^{-1}) = (f * h)(1_G) = \sum_{\gamma \in \hat{G}} d_\gamma \operatorname{Tr}(\hat{f}_\gamma \hat{h}_\gamma). \tag{7}
$$

As we noted above, the representations of a finite group can always be expressed in a unitary basis. When a function from a finite group G to $\operatorname{End}(V)$ behaves like a unitary matrix in a certain sense and the representations of G are expressed in a unitary basis, the Fourier coefficients are Hermitian. This turns out to be important in our analysis.

Definition 8 *Let G be a finite group, V be a finite-dimensional vector space, and f be a function from G to* $\operatorname{End}(V)$*. Then f is* skew-symmetric *if $f(g^{-1}) = f^*(g)$ for all $f \in G$.*

Lemma 9 *Let G be a finite group, V be a finite-dimensional vector space, and f be a skew-symmetric function from G to* $\operatorname{End}(V)$*. Then $\hat{f}_\gamma$ is Hermitian if γ is expressed in a unitary basis.*

PROOF. Recall that a matrix M is Hermitian if $M = M^*$. By equation (5),

$$
\begin{aligned}
\hat{f}_\gamma = \frac{1}{|G|} \sum_{g \in G} f(g) \otimes \gamma(g) &= \frac{1}{2|G|} \sum_{g \in G} \Big(f(g) \otimes \gamma(g) + f(g^{-1}) \otimes \gamma(g^{-1}) \Big) \\
&= \frac{1}{2|G|} \sum_{g \in G} \Big(f(g) \otimes \gamma(g) + f^*(g) \otimes \gamma^*(g) \Big),
\end{aligned}
$$

where the last equality follows since f is skew-symmetric and γ is expressed in a unitary basis. Now, $f(g) \otimes \gamma(g) + f^*(g) \otimes \gamma^*(g)$ is clearly Hermitian, and since a sum of Hermitian matrices is Hermitian, $\hat{f}_\gamma$ is Hermitian.

4 The non-Abelian long code and its Fourier transform

The long code was introduced by Bellare, Goldreich and Sudan [7] and adapted by Håstad [16] to prove approximability bounds for linear equations over Abelian groups. In this section, we once more generalize the long code for use in our proof system, that must work for all finite groups.

Let K be a finite set and denote by G^K the set of all functions from K to G. The *long G-code* of some $x \in K$ is the function A_x from G^K to G such that $A_x(f) = f(x)$. The proof in our PCP consists of several separate tables, each of which is a purported long code. In the analysis of the soundness of the verifier, we study the Fourier transform of such purported long codes composed with a representation of G, i.e., the Fourier transform of functions from G^K to $\mathrm{End}(V)$, where V is the underlying vector space of a representation ρ.

4.1 Folding

We first note that the concept of *folding* that has been used extensively for ordinary long codes extends to the long G-code.

Definition 10 *Let G be a finite group, $\gamma \in \hat{G}$ be arbitrary, V be the space corresponding to γ, K be a finite set, and A be a function from G^K to $\mathrm{End}(V)$. Then A is* γ-homogeneous *if $A(gf) = \gamma(g)A(f)$ for all $f \in K$.*

In the above definition, gf is interpreted in the obvious way: it is the function defined by $x \mapsto gf(x)$.

Lemma 11 *Let G be a finite group, γ be an arbitrary nontrivial representation of G, V be the space corresponding to γ, K be a finite set, and A be a γ-homogeneous function from G^K to $\mathrm{End}(V)$. Then $\hat{A}_\rho = 0$ when ρ is the trivial representation of G^K.*

PROOF. Since $\rho(f) = 1$ for all f when ρ is the trivial representation, (5) immediately yields

$$\begin{aligned}\hat{A}_\rho = \frac{1}{|G|^{|K|}} \sum_{f \in G^K} A(f) = \frac{1}{|G|^{|K|+1}} \sum_{g \in G} \sum_{f \in G^K} A(gf) \\ = \frac{1}{|G|^{|K|+1}} \sum_{f \in G^K} \left(\sum_{g \in G} \gamma(g) \right) A(f) = 0,\end{aligned}$$

where the last equality follows from Corollary 4.

By employing a certain access convention in the verifier, we can ensure that tables correspond to γ-homogeneous functions.

Definition 12 *Let G be a finite group, K be a finite set, and A be a function from G^K to G. Partition G^K into equivalence classes by the relation $\equiv$, where $f \equiv h$ if there is $g \in G$ such that $f = gh$. (The function f is given by $f(w) = gh(w)$.). Write $[f]$ for the equivalence class of f. Define A_G, A* left-folded over G *by choosing a representative for each equivalence class and defining $A_G(h) = gA(f)$, if $h = gf$ and f is the chosen representative for $[h]$.*

Lemma 13 *Let G be a finite group, K be a finite set, and A be a function from G^K to G. Then $\gamma \circ A_G$ is γ-homogeneous for every $\gamma \in \hat{G}$.*

PROOF. Note that $A_G(gf) = gA_G(f)$ for all $g \in G$ and all $f \in G^K$. Hence $(\gamma \circ A_G)(gf) = \gamma(g)(\gamma \circ A_G)(f)$.

It turns out that our analysis only requires some of the tables in the proof to be folded, while the other tables must be skew-symmetric functions as per Definition 8. Again, this can be accomplished by proper access conventions in the verifier.

Definition 14 *Let G be a finite group, K be a finite set, and A be a function from G^K to G. Partition G^K into equivalence classes by the relation $\equiv$, where $f \equiv g$ if $f = g$ or $f = g^{-1}$. Write $[f]$ for the equivalence class of f. Define A_{inv}, A* folded over inverse *by choosing a representative from each equivalence class and defining $A_{\text{inv}}(f) = 1_G$ if $f = f^{-1}$, $A_{\text{inv}}(f) = A(f)$ if f is the representative for $[f]$, and $A_{\text{inv}}(f) = A(f)^{-1}$ if f^{-1} is the representative for $[f]$.*

Lemma 15 *Let G be a finite group, K be a finite set, and A be a function from G^K to G. Then $\gamma \circ A_{\text{inv}}$ is skew-symmetric for every unitary $\gamma \in \hat{G}$.*

PROOF. Note that $A_{\text{inv}}(f^{-1}) = (A_{\text{inv}}(f))^{-1}$ for all f. Hence $(\gamma \circ A_{\text{inv}})(f^{-1}) = \gamma^{-1}(A_{\text{inv}}(f)) = ((\gamma \circ A_{\text{inv}})(f))^*$.

4.2 Projection

To state the final long G-code property that we need, we have to develop a more precise and detailed description of the Fourier transform. Since we can represent a function $f : K \to G$ by a table containing $f(x)$ for every $x \in K$, we can identify G^K with $G^{|K|}$. In order to reason about the Fourier transform of a function from G^K to $\text{End}(V)$, we need an understanding of the irreducible representations of powers of G. It follows from Proposition 5 that the irreducible representations of G^K are precisely those representations obtained by taking tensor products of $|K|$ irreducible representations of G: when $\rho_x \in \hat{G}$ for each $x \in K$ this is the representation given by

$$\rho = \bigotimes_{x \in K} \rho_x \qquad \text{where} \qquad \rho(f) = \bigotimes_{x \in K} \rho_x(f(x)).$$

We treat the tensor product of two matrices as a matrix indexed by pairs. Analogously, we treat the tensor product of $|K|$ matrices as a matrix indexed by $|K|$-tuples. In order to reason about single entries in the tensor product that forms a representation $\rho = \bigotimes_{x \in K} \rho_x$ we define the *set of indices* $\iota(\rho)$. An element $i \in \iota(\rho)$ is a vector indexed by elements of K so that for all $x \in K, 1 \le i_x \le d_{\rho_x}$; we refer to such an element i as an *index*. Then for two indices $i, j \in \iota(\rho)$ we define

$$\rho_{ij}(f) = \prod_{x \in G^K} \Big(\rho_x\big(f(x)\big)\Big)_{i_x, j_x}.$$

We also define the *size* $|\rho|$ of an irreducible representation ρ of G^K to be the number of $x \in K$ such that ρ_x is nontrivial.

The verifier in our PCP checks positions in tables corresponding to two related long codes. The precise details of how these tables are related is described below; for now it is enough to know that the tables correspond to functions from $F = G^K$ to G and from $H = G^L$ to G, respectively, where there is an onto function $\pi \colon L \to K$. There is a natural way to transform an $f \in F$ into a function in H by composing it with π; we denote this function by $f \circ \pi$. The projection π can also be used to transform the components of a representation $\rho \in \hat{H}$ into a function on F. For $i, j \in \iota(\rho)$ the components ρ_{ij} are functions from H to $\boldsymbol{C}$. We denote the new, associated, function by $\rho^\pi_{ij} \colon F \to \boldsymbol{C}$; it is defined by the map $f \mapsto \rho_{ij}(f \circ \pi)$. Using our definition of the index sets,

$$\rho^\pi_{ij}(f) = \rho_{ij}(f \circ \pi) = \prod_{x \in K} \prod_{y \in \pi^{-1}(x)} \Big(\rho_y\big(f(x)\big)\Big)_{i_y, j_y}.$$

We are now ready to formulate the following projection lemma:

Lemma 16 *Let K and L be finite sets and $\pi \colon L \to K$ be an onto function. Let $F = G^K$ and $H = G^L$. Define the relation $\sim$ on $\hat{F} \times \hat{H}$ so that for $\tau \in \hat{F}$ and $\rho \in \hat{H}$, $\tau \sim \rho$ if for all $x \in K$ such that τ_x is nontrivial, there is some $y \in \pi^{-1}(x)$ such that ρ_y is nontrivial. Then*

(1) $\tau \sim \rho \implies |\tau| \le |\rho|$.
(2) $\tau \not\sim \rho \implies \forall i, j \in \iota(\rho), \forall k, \ell \in \iota(\tau), \Big(\langle \rho^\pi_{ij} \mid \tau_{k\ell} \rangle_F = 0\Big)$.

PROOF. The first implication follows directly from the definition of the relation $\sim$. To prove the second implication, assume that $\tau \not\sim \rho$; then there is some $x' \in K$ such that $\tau_{x'}$ is nontrivial but ρ_y is trivial for all $y \in \pi^{-1}(x')$. Recall that we can write

$$\rho_{ij}^{\pi}(f) = \prod_{x \in K} \prod_{y \in \pi^{-1}(x)} \Big(\rho_y\big(f(x)\big)\Big)_{i_y, j_y} \qquad \text{and} \qquad \tau_{k\ell}(f) = \prod_{x \in K} \Big(\tau_x\big(f(x)\big)\Big)_{k_x, \ell_x}$$

by our definition of the index sets; hence

$$\begin{aligned}
\langle \rho_{ij}^{\pi} \mid \tau_{k\ell} \rangle_F &= \frac{1}{|F|} \sum_{f \in F} \left(\prod_{x \in K} \prod_{y \in \pi^{-1}(x)} \Big(\rho_y\big(f(x)\big)\Big)_{i_y, j_y} \right) \left(\prod_{x \in K} \Big(\tau_x\big(f^{-1}(x)\big)\Big)_{k_x, \ell_x} \right) \\
&= \frac{1}{|F|} \sum_{f \in F} \prod_{x \in K} \Big(\tau_x\big(f^{-1}(x)\big)\Big)_{k_x, \ell_x} \prod_{y \in \pi^{-1}(x)} \Big(\rho_y\big(f(x)\big)\Big)_{i_y, j_y} \\
&= \prod_{x \in K} \left(\frac{1}{|G|} \sum_{g \in G} \Big(\tau_x(g^{-1})\Big)_{k_x, \ell_x} \prod_{y \in \pi^{-1}(x)} \Big(\rho_y(g)\Big)_{i_y, j_y} \right)
\end{aligned}$$

where the last equality holds since a sum over all functions $f \in F$ can be viewed as $|K|$ nested sums over the possible values of $f(x)$ for $x \in K$. We can then change the sums of a product into a product of $|K|$ sums, i.e., a product of sums over all $g \in G$.

Since ρ_y is trivial for all $y \in \pi^{-1}(x')$, the factor corresponding to x' in the above product is

$$\frac{1}{|G|} \sum_{g \in G} \Big(\tau_{x'}(g^{-1})\Big)_{k_{x'}, \ell_{x'}} = 0,$$

where the equality follows from Proposition 3.

5 The main result

In his paper [16], Håstad introduced a methodology for proving lower bounds for constraint satisfaction problems. At a high level, the method can be viewed as a simulation of the well-known two-prover one-round (2P1R) protocol for E3-Sat where the verifier sends a clause to one prover and a variable contained in that clause to the other prover, accepting if the returned assignments are consistent and satisfy the clause.

5.1 The two-prover one-round protocol

The starting point for our PCPs will be the standard 2P1R protocol for **NP** which we will now describe.

Definition 17 *We define the decision problem* μ-gap E3-Sat(5)*. A Boolean formula* ϕ *in conjunctive normal form is* μ-promised *if either* ϕ *is satisfiable or no more than a* μ*-fraction of the clauses of* ϕ *are simultaneously satisfiable.* μ-gap E3-Sat(5) *is the problem of determining satisfiability of a* μ*-promised Boolean formula, where each clause contains exactly three literals and each literal occurs exactly five times.*

Recall that it is possible to reduce any problem in **NP** to an instance of μ-gap E3-Sat(5) [2,12,18]. This gives rise to a natural 2P1R protocol consisting of two provers, P_1 and P_2, and one verifier. Given an instance, i.e., an E3-Sat formula ϕ, the verifier picks a clause C and variable x in C uniformly at random from the instance and sends C to P_1 and x to P_2. It then receives an assignment to the variables in C from P_1 and an assignment to x from P_2, and accepts if these assignments are consistent and satisfy C. If the provers are honest, the verifier always accepts with probability 1 when ϕ is satisfiable, i.e., the proof system has *completeness* 1, or *perfect completeness.* It can be shown that the provers can fool the verifier with probability at most $(2+\mu)/3$ when ϕ is not satisfiable, i.e., that the above proof system has *soundness* $(2+\mu)/3$.

The soundness can be lowered to $((2+\mu)/3)^u$ by repeating the protocol u times independently, but it is also possible to construct a one-round proof system with lower soundness by repeating u times in parallel as follows: The verifier picks u clauses $(C_1, \dots, C_u)$ uniformly at random from the instance. For each C_i, it also picks a variable x_i from C_i uniformly at random. The verifier then sends $(C_1, \dots, C_u)$ to P_1 and $(x_1, \dots, x_u)$ to P_2. It receives an assignment to the variables in $(C_1, \dots, C_u)$ from P_1 and an assignment to $(x_1, \dots, x_u)$ from P_2, and accepts if these assignments are consistent and satisfy $C_1 \wedge \cdots \wedge C_u$. As above, the completeness of this proof system is 1, and it can be shown [19] that the soundness is at most c_μ^u, where $c_\mu < 1$ is some constant depending on μ but not on u or the size of the instance.

5.2 The protocol

The proof in our PCP contains a purported encoding of a pair of strategies for the provers in the above u-parallel game. For a multiset U of variables, we denote by $\{-1,1\}^U$ the set of all assignments to the variables in U; for a multiset W of clauses, we denote by SAT^W the set of all satisfying assignments to the clauses in W. When x is an assignment to all the variables in an instance and V is a multiset of variables or a multiset of clauses, we denote by $x|_V$ the assignment to the variables in V. If V is a multiset of clauses $x|_V$ is therefore an assignment to the variables that constitute the clauses in V.

Definition 18 *A* Standard Written G-Proof with parameter u *for a for-*

Input: A formula ϕ and oracle access to a Standard Written G-Proof with parameter u.

(1) Select uniformly at random a multiset $W = \{C_{i_1}, \dots, C_{i_u}\}$ of u clauses.
(2) Construct a multiset U by choosing a variable uniformly at random from each C_{i_k}.
(3) Let π be the function that creates an assignment in $\{-1,1\}^U$ from an assignment in SAT^W.
(4) Select uniformly at random $f\colon \{-1,1\}^U \to G$.
(5) Select uniformly at random $h\colon \mathrm{SAT}^W \to G$.
(6) Choose $e\colon \mathrm{SAT}^W \to G$, such that, independently for each $y \in \mathrm{SAT}^W$,
    (a) With probability $1-\epsilon$, $e(y) = 1_G$.
    (b) With probability ϵ, $e(y)$ is chosen uniformly at random from G.
(7) If $A_{U,G}(f)A_{W,\mathrm{inv}}(h)A_{W,\mathrm{inv}}(h^{-1}(f \circ \pi)^{-1}e) = 1_G$ then accept, else reject.

Fig. 1. The above PCP is parameterized by the positive integer u and the positive real ϵ and tests if a μ-gap E3-Sat(5) formula ϕ is satisfiable by querying three positions in a Standard Written G-Proof with parameter u.

mula ϕ consists of a table $A_U\colon G^{\{-1,1\}^U} \to G$ for each multiset U of u variables from ϕ and a table $A_W\colon G^{\mathrm{SAT}^W} \to G$ for each multiset W of u clauses from ϕ.

Definition 19 *A Standard Written G-Proof with parameter u is a* correct proof for a formula ϕ *if there is an assignment x, satisfying ϕ, such that A_V is the long G-code of $x|_V$ for any multiset V containing either u variables from ϕ or u clauses from ϕ.*

The protocol itself is similar to that used by Håstad [16] to prove inapproximability of equations over Abelian group; the only difference is in the coding of the proof. The tables corresponding to sets of variables are left-folded over G and the tables corresponding to sets of clauses are folded over inverse. The verifier is given in Figure 1. The completeness is straightforward:

Lemma 20 *The verifier in Figure 1 has completeness at least $1-(1-|G|^{-1})\epsilon$.*

PROOF. Let x be a correctly encoded proof of an assignment satisfying ϕ. Then, by the definition of the long G-code,

$$A_{U,G}(f)A_{W,\mathrm{inv}}(h)A_{W,\mathrm{inv}}(h^{-1}(f \circ \pi)^{-1}e) \\ = f(x|_U)h(x|_W)h^{-1}(x|_W)f^{-1}(x|_U)e(x|_W) = e(x|_W).$$

Considering how e is selected by the verifier, $e(x|_W) = 1_G$ with probability $1 - (1 - |G|^{-1})\epsilon$ and hence the verifier accepts a correctly encoded proof of a satisfying assignment with probability $1 - (1 - |G|^{-1})\epsilon$.

5.3 Analysis of the soundness

The analysis follows the now standard approach. We assume that the verifier accepts a proof corresponding to an unsatisfiable formula with probability $|G|^{-1} + \delta$ and prove that it is then possible to construct strategies for the provers in the 2P1R game that make the verifier of that game accept with high probability. Since it is known that this cannot be the case, there cannot exist a proof corresponding to an unsatisfiable formula that the PCP verifier accepts with probability $|G|^{-1} + \delta$.

To this end, we first apply Proposition 6 to arrive at an expression for the acceptance probability. Since

$$|G|^{-1} \sum_{\gamma \in \hat{G}} d_\gamma \chi_\gamma(A_{U,G}(f) A_{W,\text{inv}}(h) A_{W,\text{inv}}(h^{-1}(f \circ \pi)^{-1} e))$$

is an indicator of the event that the verifier accepts, the acceptance probability can be written as:

$$|G|^{-1} \sum_{\gamma \in \hat{G}} d_\gamma \,\mathrm{E}_{f,h,e,U,W}\left[\chi_\gamma\Big(A_{U,G}(f) A_{W,\text{inv}}(h) A_{W,\text{inv}}\big(h^{-1}(f \circ \pi)^{-1} e\big)\Big)\right].$$

Since the term corresponding to the trivial representation in the above sum is exactly 1, the assumption that the verifier in Figure 1 accepts with probability $|G|^{-1} + \delta$ implies that there must be some non-trivial irreducible representation γ of G such that

$$\left|\mathrm{E}_{f,h,e,U,W}\left[\chi_\gamma\Big(A_{U,G}(f) A_{W,\text{inv}}(h) A_{W,\text{inv}}\big(h^{-1}(f \circ \pi)^{-1} e\big)\Big)\right]\right| > d_\gamma \delta. \qquad (8)$$

We now proceed by applying Fourier-inversion to $A_{U,G}$ and $A_{W,\text{inv}}$. More precisely, we first apply Fourier-inversion to $A_{W,\text{inv}}$, resulting in:

Lemma 21 *Suppose that the verifier in Figure 1 accepts with probability $|G|^{-1} + \delta$. Then there exists a nontrivial representation γ of G such that*

$$\left|\mathrm{E}_{f,U,W}\left[\mathrm{tr}\left(A(f) \sum_{\rho \in \hat{H}} d_\rho (1-\epsilon)^{|\rho|} \,\mathrm{Tr}\Big(\hat{B}_\rho^2\big(\boldsymbol{I}_{d_\gamma} \otimes \rho(f \circ \pi)\big)\Big)\right)\right]\right| > d_\gamma \delta.$$

where $A = \gamma \circ A_{U,G}$, $H = G^{\mathrm{SAT}^W}$ and $B = \gamma \circ A_{W,\text{inv}}$.

PROOF. Since the verifier in Figure 1 accepts with probability $|G|^{-1}+\delta$ there exists a nontrivial representation γ of G such that the inequality (8) holds; we now fix that γ and select a basis such that it is unitary. We proceed by expanding the expectation in (8) in a Fourier series. To shorten the notation, we introduce the shorthands $A = \gamma \circ A_{U,G}$ and $B = \gamma \circ A_{W,\mathrm{inv}}$. We now consider the expression

$$\operatorname{tr} \mathrm{E}\Big[A(f)B(h)B(h^{-1}(f\circ\pi)^{-1}e)\Big] = \operatorname{tr} \mathrm{E}_{f,U,W}\Big[A(f)\, \mathrm{E}_{h,e}\Big[B(h)B(h^{-1}(f\circ\pi)^{-1}e)\Big]\Big] \tag{9}$$

which is exactly the expectation in (8). We expand the inner expectation in its Fourier series. Since $\mathrm{E}_{h,e}[B(h)B(h^{-1}(f\circ\pi)^{-1}e)] = \mathrm{E}_e[(B*B)((f\circ\pi)^{-1}e)]$, this is immediate:

$$\mathrm{E}_e[(B*B)((f\circ\pi)^{-1}e)] = \sum_{\rho\in\hat{H}} d_\rho \operatorname{Tr}\Big(\hat{B}_\rho^2\Big(\boldsymbol{I}_{d_\gamma} \otimes \Big(\rho(f\circ\pi)\, \mathrm{E}_e[\rho(e^{-1})]\Big)\Big)\Big).$$

To compute $\mathrm{E}_e[\rho(e^{-1})]$, note that

$$\mathrm{E}_e[\rho(e^{-1})] = \mathrm{E}_e\Bigg[\bigotimes_{y\in\mathrm{SAT}^W}\Big(\rho_y\Big(e(y)^{-1}\Big)\Big)\Bigg] = \bigotimes_{y\in\mathrm{SAT}^W} \mathrm{E}_{e(y)}\Big[\rho_y\Big(e(y)^{-1}\Big)\Big],$$

where the second equality follows since $e(y)$ is selected independently for every y. Now, $\mathrm{E}_{e(y)}[\rho_y(e(y)^{-1})] = \boldsymbol{I}_{d_{\rho_y}}$ if ρ_y is trivial; otherwise

$$\mathrm{E}_{e(y)}\Big[\rho_y\Big(e(y)^{-1}\Big)\Big] = (1-\epsilon)\rho_y(1_G) + \mathrm{E}_{g\in G}[\rho_y(g)] = (1-\epsilon)\boldsymbol{I}_{d_{\rho_y}},$$

where the last equality follows from Corollary 4. Hence $\mathrm{E}_e[\rho(e^{-1})] = (1-\epsilon)^{|\rho|}\boldsymbol{I}_{d_\rho}$; when this is substituted into the above expression, (9) becomes

$$\operatorname{tr} \mathrm{E}\Big[A(f)B(h)B(h^{-1}(f\circ\pi)^{-1}e)\Big] = \mathrm{E}_f\Bigg[\operatorname{tr}\Bigg(A(f)\sum_{\rho\in\hat{H}} d_\rho(1-\epsilon)^{|\rho|}\operatorname{Tr}\Big(\hat{B}_\rho^2\Big(\boldsymbol{I}_{d_\gamma}\otimes\rho(f\circ\pi)\Big)\Big)\Bigg)\Bigg]. \tag{10}$$

We then prove that, for every fixed f, many terms in the resulting sum are very small. Specifically, we prove that there is a constant c such that the terms corresponding to ρ with $|\rho| > c$ contribute at most $d_\gamma\delta/2$.

Lemma 22 *Let G be a finite group, V be a d_γ-dimensional vector space, $A(f) \in \mathrm{End}(V)$ be unitary, H be a power of G, and $B\colon H \to \mathrm{End}(V)$ be skew-symmetric. Then*

$$\Bigg|\operatorname{tr}\Bigg(A(f)\sum_{\substack{\rho\in\hat{H}\\|\rho|>c}} d_\rho(1-\epsilon)^{|\rho|}\operatorname{Tr}\Big(\hat{B}_\rho^2\Big(\boldsymbol{I}_{d_\gamma}\otimes\rho(f\circ\pi)\Big)\Big)\Bigg)\Bigg| \le d_\gamma(1-\epsilon)^c \tag{11}$$

for any positive real ϵ and any positive integer $c > 0$.

Corollary 23 *Suppose that the verifier in Figure 1 accepts with probability $|G|^{-1} + \delta$. Then, for any unitary $\gamma \in \hat{G}$,*

$$\left|\mathrm{E}_{f,U,W}\left[\mathrm{tr}\left(A(f) \sum_{\substack{\rho \in \hat{H} \\ |\rho| \geq c}} d_\rho (1-\epsilon)^{|\rho|} \operatorname{Tr}\left(\hat{B}_\rho^2\left(\boldsymbol{I}_{d_\gamma} \otimes \rho(f \circ \pi)\right)\right)\right)\right]\right| < \frac{d_\gamma \delta}{2}$$

where $A = \gamma \circ A_{U,G}$, $H = G^{\mathrm{SAT}^W}$ and $B = \gamma \circ A_{W,\mathrm{inv}}$; provided that $c > \lceil (\log \delta - 1)/\log(1-\epsilon) \rceil$.

PROOF of Lemma 22. Let T be a unitary matrix that diagonalizes $A(f)$, i.e., such that $A(f) = T^*(f)D(f)T(f)$. Such a T always exists since A is unitary and therefore unitarily diagonalizable. Then the left-hand side of (11) can be rewritten as

$$\left|\mathrm{tr}\left(T^* D T \sum_{\substack{\rho \in \hat{H} \\ |\rho| > c}} d_\rho (1-\epsilon)^{|\rho|} \operatorname{Tr}\left(\hat{B}_\rho^2\left(\boldsymbol{I}_{d_\gamma} \otimes \rho(f \circ \pi)\right)\right) T^* T\right)\right|$$

By Lemma 31 and Corollary 33 from Appendix A, this is equal to

$$\left|\mathrm{tr}\left(D \sum_{\substack{\rho \in \hat{H} \\ |\rho| > c}} d_\rho (1-\epsilon)^{|\rho|} \operatorname{Tr}\left((T \otimes \boldsymbol{I}_{d_\rho})\hat{B}_\rho^2 (T \otimes \boldsymbol{I}_{d_\rho})^*\left(\boldsymbol{I}_{d_\gamma} \otimes \rho(f \circ \pi)\right)\right)\right)\right|$$

According to Corollary 30 in Appendix A, $(T \otimes \boldsymbol{I}_{d_\rho})\hat{B}_\rho^2 (T \otimes \boldsymbol{I}_{d_\rho})^* = \hat{C}_\rho^2$ where $\hat{C}_\rho$ are the Fourier coefficients for the function B expressed in the basis that diagonalizes $A(f)$, i.e., for the function $C = TBT^*$. Therefore, we have to bound the magnitude of

$$\mathrm{tr}\left(D \sum_{\substack{\rho \in \hat{H} \\ |\rho| > c}} d_\rho (1-\epsilon)^{|\rho|} \operatorname{Tr}(\hat{C}_\rho^2 U_\rho)\right)$$

where D is a diagonal matrix, and U_ρ are unitary matrices. First note that $\mathrm{tr}(\sum_{\rho \in \hat{H}} d_\rho \operatorname{Tr}(\hat{C}_\rho^2)) = d_\gamma$, since $\sum_{\rho \in \hat{H}} d_\rho \operatorname{Tr}(\hat{C}_\rho^2) = (C * C)(1_G) = \boldsymbol{I}_{d_\gamma}$, where the last equality follows since C has the property that $C(g^{-1}) = C(g)^{-1}$. By Lemma 27 in Appendix A this implies that

$$\mathrm{tr}\left(\sum_{\substack{\rho \in \hat{H} \\ |\rho| > c}} d_\rho (1-\epsilon)^{|\rho|} \operatorname{Tr}(\hat{C}_\rho^2)\right) \leq (1-\epsilon)^c d_\gamma.$$

Note that, since B is skew-symmetric, $\hat{B}_\rho$ is Hermitian by Lemma 9 from Appendix A and thus both $\hat{B}_\rho^2$ and $\hat{C}_\rho^2$ are positive semidefinite matrices. Therefore, Lemma 28 in Appendix A establishes that

$$\left|\operatorname{tr}\left(D \sum_{\substack{\rho\in\hat{H}\\|\rho|>c}} d_\rho(1-\epsilon)^{|\rho|} \operatorname{Tr}(\hat{C}_\rho^2 U_\rho)\right)\right| \leq (1-\epsilon)^c d_\gamma.$$

which completes the proof.

While we bound the terms corresponding to ρ with $|\rho| \geq c$ by a purely algebraic argument, we bound the terms corresponding to ρ with $|\rho| < c$ by using them to devise a strategy for the provers in the 2P1R game for μ-gap E3-Sat(5). Since this strategy has a success probability that is independent of u, the number of repetitions in the 2P1R game, we can then select u in such a way that also the terms corresponding to ρ with $|\rho| < c$ have to be upper bounded by $d_\gamma\delta/2$.

Lemma 24 *Suppose that for any nontrivial $\gamma \in \hat{G}$,*

$$\left|\mathrm{E}_{f,U,W}\left[\operatorname{tr}\left(A(f) \sum_{\substack{\rho\in\hat{H}\\|\rho|<c}} d_\rho(1-\epsilon)^{|\rho|} \operatorname{Tr}\left(\hat{B}_\rho^2\left(\boldsymbol{I}_{d_\gamma} \otimes \rho(f\circ\pi)\right)\right)\right)\right]\right| \geq \eta \qquad (12)$$

where $A\colon G^{\{-1,1\}^U} \to \mathrm{End}(V)$ and $B\colon G^{\mathrm{SAT}^W} \to \mathrm{End}(V)$ are unitary functions known to both provers in the 2P1R game from §5.1, V is the vector space corresponding to γ, and $H = G^{\mathrm{SAT}^W}$. Then there is a strategy for the provers in the 2P1R protocol with success probability at least $\eta^2 c^{-1}|G|^{-c} d_\gamma^{-6}$.

Corollary 25 *Let $A_{U,G}$ and $A_{W,\mathrm{inv}}$ be the tables in a Standard Written G-Proof with parameter u corresponding to an unsatisfiable formula. Then, for any unitary $\gamma \in \hat{G}$,*

$$\left|\mathrm{E}_{f,U,W}\left[\operatorname{tr}\left(A(f) \sum_{\substack{\rho\in\hat{H}\\|\rho|<c}} d_\rho(1-\epsilon)^{|\rho|} \operatorname{Tr}\left(\hat{B}_\rho^2\left(\boldsymbol{I}_{d_\gamma} \otimes \rho(f\circ\pi)\right)\right)\right)\right]\right| < \frac{d_\gamma\delta}{2} \qquad (13)$$

where $A = \gamma \circ A_{U,G}$, $H = G^{\mathrm{SAT}^W}$ and $B = \gamma \circ A_{W,\mathrm{inv}}$; provided that $u > \lceil (2\log\delta^{-1} + \log c + c\log|G| + 4\log d_\gamma + 2)/\log c_\mu^{-1}\rceil$ where c_μ is the constant from §5.1.

PROOF of Lemma 24. Expand $A(f)$ using Fourier inversion (6). Then the left hand side of (12) becomes

$$\left|\mathrm{E}_{U,W,f}\left[\mathrm{tr}\left(\sum_{\tau\in\hat{F}}\sum_{\substack{\rho\in\hat{H}\\|\rho|<c}} d_\tau d_\rho \,\mathrm{Tr}\Big(\hat{A}_\tau\big(\boldsymbol{I}_{d_\gamma}\otimes\tau(f^{-1})\big)\Big)\,\mathrm{Tr}\Big(\hat{B}_\rho^2\big(\boldsymbol{I}_{d_\gamma}\otimes\rho(f\circ\pi)\big)\Big)\right)\right]\right|$$

If this expression is larger than η, then there must be some index t such that

$$\frac{\eta}{d_\gamma}\le\left|\mathrm{E}_{U,W,f}\left[\left(\sum_{\tau\in\hat{F}}\sum_{\substack{\rho\in\hat{H}\\|\rho|<c}} d_\tau d_\rho \,\mathrm{Tr}\Big(\hat{A}_\tau\big(\boldsymbol{I}_{d_\gamma}\otimes\tau(f^{-1})\big)\Big)\,\mathrm{Tr}\Big(\hat{B}_\rho^2\big(\boldsymbol{I}_{d_\gamma}\otimes\rho(f\circ\pi)\big)\Big)\right)_{tt}\right]\right| \tag{14}$$

We now fix this value of t. By our notation for the index sets $\iota(\tau)$ and $\iota(\rho)$ and the "projected" representation ρ^π_{op} from §4.2,

$$\begin{aligned}
\left(\mathrm{Tr}\Big(\hat{A}_\tau\big(\boldsymbol{I}_{d_\gamma}\otimes\tau(f^{-1})\big)\Big)\right)_{tk} &= \sum_{m,n\in\iota(\tau)}\big(\hat{A}_\tau\big)_{tn,km}\tau_{mn}(f^{-1}),\ \text{and}\\
\left(\mathrm{Tr}\Big(\hat{B}_\rho^2\big(\boldsymbol{I}_{d_\gamma}\otimes\rho(f\circ\pi)\big)\Big)\right)_{kt} &= \sum_{o,p\in\iota(\rho)}\big(\hat{B}_\rho^2\big)_{ko,tp}\rho^\pi_{op}(f)\\
&= \sum_{o,p\in\iota(\rho)}\sum_{\substack{q\in\iota(\rho)\\1\le r\le d_\gamma}}(\hat{B}_\rho)_{ko,rq}(\hat{B}_\rho)_{rq,tp}\rho^\pi_{op}(f).
\end{aligned}$$

Inserting these expressions into the right hand side of (14), we have

$$\frac{\eta}{d_\gamma}\le\left|\sum_{\substack{1\le k\le d_\gamma\\1\le r\le d_\gamma}}\mathrm{E}_{U,W}\left[\sum_{\tau\in\hat{F}}\sum_{\substack{\rho\in\hat{H}\\|\rho|<c}}\sum_{\substack{m,n\in\iota(\tau)\\o,p,q\in\iota(\rho)}} (\hat{A}_\tau)_{tn,km}(\hat{B}_\rho)_{ko,rq}(\hat{B}_\rho)_{rq,tp}\,\mathrm{E}_f\Big[\tau_{mn}(f^{-1})\rho^\pi_{po}(f)\;\Big|\;U,W\Big]\right]\right|. \tag{15}$$

Focus now on the innermost expectation

$$\mathrm{E}_f\Big[\tau_{mn}(f^{-1})\rho^\pi_{po}(f)\;\Big|\;U,W\Big]=\langle\rho^\pi_{po}\mid\tau_{mn}\rangle_F.$$

By Lemma 16, this is zero unless $\tau\sim\rho$, where $\sim$ is the relation defined in Lemma 16. Hence (15) becomes

$$\frac{\eta}{d_\gamma}\le\left|\sum_{\substack{1\le k\le d_\gamma\\1\le r\le d_\gamma}}\mathrm{E}_{U,W}\left[\sum_{\substack{\rho\in\hat{H}\\|\rho|<c}}\sum_{\substack{\tau\in\hat{F}\\\tau\sim\rho}}\sum_{\substack{m,n\in\iota(\tau)\\o,p,q\in\iota(\rho)}} d_\tau d_\rho(\hat{A}_\tau)_{tn,km}(\hat{B}_\rho)_{ko,rq}(\hat{B}_\rho)_{rq,tp}\langle\rho^\pi_{po}\mid\tau_{mn}\rangle_F\right]\right|. \tag{16}$$

We now apply Cauchy-Schwartz to simplify the above expression further:

$$\begin{aligned}\frac{\eta^2}{d_\gamma^4} &\le \sum_{\substack{1\le k\le d_\gamma\\1\le r\le d_\gamma}} \mathrm{E}_{U,W}\left[\left|\sum_{\substack{\rho\in\hat H\\|\rho|<c}}\sum_{\substack{\tau\in\hat F\\\tau\sim\rho}}\sum_{\substack{m,n\in\iota(\tau)\\o,p,q\in\iota(\rho)}}\right.\right.\\ &\qquad\left.\left. d_\tau d_\rho (\hat A_\tau)_{tn,km}(\hat B_\rho)_{ko,rq}(\hat B_\rho)_{rq,tp}\langle\rho^\pi_{po}\mid\tau_{mn}\rangle_F\right|^2\right]\\ &\le \sum_{\substack{1\le k\le d_\gamma\\1\le r\le d_\gamma}} \mathrm{E}_{U,W}\left[\left(\sum_{\substack{\rho\in\hat H\\|\rho|<c}}\sum_{\substack{\tau\in\hat F\\\tau\sim\rho}}\sum_{\substack{m,n\in\iota(\tau)\\o,p,q\in\iota(\rho)}} d_\tau d_\rho\left|(\hat A_\tau)_{tn,km}\right|^2\left|(\hat B_\rho)_{ko,rq}\right|^2\right)\right.\\ &\qquad\left.\left(\sum_{\substack{\rho\in\hat H\\|\rho|<c}}\sum_{\substack{\tau\in\hat F\\\tau\sim\rho}}\sum_{\substack{m,n\in\iota(\tau)\\o,p,q\in\iota(\rho)}} d_\tau d_\rho\left|(\hat B_\rho)_{rq,tp}\right|^2\left|\langle\rho^\pi_{po}\mid\tau_{mn}\rangle_F\right|^2\right)\right]\end{aligned}\tag{17}$$

We proceed by bounding the second factor above, i.e.,

$$\begin{aligned}&\sum_{\substack{\rho\in\hat H\\|\rho|<c}}\sum_{\substack{\tau\in\hat F\\\tau\sim\rho}}\sum_{\substack{m,n\in\iota(\tau)\\o,p,q\in\iota(\rho)}} d_\tau d_\rho\left|(\hat B_\rho)_{rq,tp}\right|^2\left|\langle\rho^\pi_{po}\mid\tau_{mn}\rangle_F\right|^2\\ &\qquad= \sum_{\substack{\rho\in\hat H\\|\rho|<c}}\sum_{p,q\in\iota(\rho)} d_\rho\left|(\hat B_\rho)_{rq,tp}\right|^2\left(\sum_{\substack{\tau\in\hat F\\\tau\sim\rho}}\sum_{\substack{m,n\in\iota(\tau)\\o\in\iota(\rho)}} d_\tau\left|\langle\rho^\pi_{po}\mid\tau_{mn}\rangle_F\right|^2\right).\end{aligned}\tag{18}$$

By equation (4) in Lemma 7,

$$\sum_{\tau\in\hat F}\sum_{\substack{m,n\in\iota(\tau)\\o\in\iota(\rho)}} d_\tau\left|\langle\rho^\pi_{po}\mid\tau_{nm}\rangle_F\right|^2 = \frac{1}{|F|}\sum_{f\in F}\sum_{o\in\iota(\rho)}|\rho_{po}(f\circ\pi)|^2 = 1,$$

where the last equality follows since ρ is written in a unitary basis and the inner sum is therefore exactly one for every f. Regarding the rest of (18), note that $(\hat B_\rho)_{rq,tp} = |H|^{-1}\sum_{h\in H} B_{rt}(h)\rho_{qp}(h) = \langle B_{rt}\mid\rho^{-1}_{pq}\rangle_H$; another application of Lemma 7 therefore shows that

$$\sum_{\rho\in\hat H}\sum_{p,q\in\iota(\rho)} d_\rho\left|(\hat B_\rho)_{rq,tp}\right|^2 = \sum_{\rho\in\hat H}\sum_{p,q\in\iota(\rho)} d_\rho\left|\langle B_{rt}\mid\rho^{-1}_{pq}\rangle_H\right|^2 = \frac{1}{|H|}\sum_{h\in H}|B_{rt}(h)|^2 \le 1,$$

where the inequality follows since B is unitary and therefore has entries with at most unit magnitude. Using the above bounds in (17) transforms that bound into

$$\frac{\eta^2}{d_\gamma^4} \le \sum_{\substack{1\le k\le d_\gamma\\ 1\le r\le d_\gamma}} \mathrm{E}_{U,W}\left[\sum_{\substack{\tau\in\hat{F}\\ \tau\sim\rho}}\sum_{\substack{\rho\in\hat{H}\\ |\rho|<c}}\sum_{\substack{m,n\in\iota(\tau)\\ o,p,q\in\iota(\rho)}} d_\tau d_\rho \left|(\hat{A}_\tau)_{tn,km}\right|^2 \left|(\hat{B}_\rho)_{ko,rq}\right|^2\right]$$

$$\le |G|^c \sum_{\substack{1\le k\le d_\gamma\\ 1\le r\le d_\gamma}} \mathrm{E}_{U,W}\left[\sum_{\substack{\tau\in\hat{F}\\ \tau\sim\rho}}\sum_{\substack{\rho\in\hat{H}\\ |\rho|<c}}\sum_{\substack{m,n\in\iota(\tau)\\ o,q\in\iota(\rho)}} d_\tau d_\rho \left|(\hat{A}_\tau)_{tn,km}\right|^2 \left|(\hat{B}_\rho)_{ko,rq}\right|^2\right]$$

where the second inequality follows by summing over p in the innermost sum. To conclude, there must be some $k, r \in \{1, \ldots, d_\gamma\}$ such that

$$\mathrm{E}_{U,W}\left[\sum_{\substack{\rho\in\hat{H}\\ |\rho|<c}}\sum_{\substack{\tau\in\hat{F}\\ \tau\sim\rho}}\sum_{\substack{m,n\in\iota(\tau)\\ o,q\in\iota(\rho)}} d_\tau d_\rho \left|(\hat{A}_\tau)_{tn,km}\right|^2 \left|(\hat{B}_\rho)_{ko,rq}\right|^2\right] \ge \frac{\eta^2}{|G|^c d_\gamma^6}. \tag{19}$$

We now describe the strategies for the provers in the 2P1R protocol. The index t is independent of U and W and can be calculated by the provers in advance. Also the values of k and r mentioned above can be calculated in advance.

Upon receiving W, P_1 first picks $\rho \in \hat{H}$ with probability proportional to $\sum_{o,q\in\iota(\rho)} d_\rho |(\hat{B}_\rho)_{ko,rq}|^2$. This is a well-defined procedure since

$$\sum_{\rho\in\hat{H}}\sum_{o,q\in\iota(\rho)} d_\rho\left|(\hat{B}_\rho)_{ko,rq}\right|^2 = \frac{1}{|H|}\sum_{h\in H}|B_{kr}(h)|^2 \le 1.$$

Having selected ρ, P_1 then returns a random y such that ρ_y is nontrivial. If no such y exists—this happens only if ρ is trivial—P_1 gives up.

Upon receiving U, P_2 picks $\tau \in \hat{F}$ with probability $\sum_{n,m\in\iota(\tau)} d_\tau |(\hat{A}_\tau)_{tn,km}|^2$. This is a well-defined procedure since

$$\sum_{\rho\in\hat{F}}\sum_{n,m\in\iota(\tau)} d_\tau\left|(\hat{A}_\tau)_{tn,km}\right|^2 = \frac{1}{|F|}\sum_{f\in F}|A_{tk}(f)|^2 \le 1.$$

Then P_2 picks a random x such that τ_x is nontrivial and returns this x as its answers. This is always possible since $\hat{A}_\tau$ is nonzero only for nontrivial τ by Lemma 11.

To analyze the success rate of this strategy, suppose that P_1 picks ρ and P_2 picks τ such that $\tau \sim \rho$. If P_2 returns x', then there must be some $y' \in \pi^{-1}(x')$ such that $\rho_{y'}$ is nontrivial. The probability of P_1 picking this y' is at least

$|\rho|^{-1}$. Hence the probability of success is at least

$$\mathrm{E}_{U,W}\Bigg[\sum_{\substack{\rho\in\hat{H}\\|\rho|<c}}\sum_{\substack{\tau\in\hat{F}\\\tau\sim\rho}}\sum_{\substack{m,n\in\iota(\tau)\\o,q\in\iota(\rho)}}\frac{d_\tau d_\rho\left|(\hat{A}_\tau)_{tn,km}\right|^2\left|(\hat{B}_\rho)_{ko,rq}\right|^2}{|\rho|}\Bigg]\geq\frac{\eta^2}{c|G|^c d_\gamma^6}$$

where the inequality follows from the bound (19).

Finally, we put together these two parts and establish the soundness of the verifier.

Lemma 26 *For any constants $\delta > 0$ and $\epsilon > 0$, there is a choice of the parameters c and u such that the soundness of the PCP in Fig. 1 is at most $|G|^{-1}+\delta$.*

PROOF. Suppose for contradiction that ϕ is not satisfiable and there is a proof which the verifier accepts with probability $|G|^{-1}+\delta$. By Lemma 21, for this proof, there is a nontrivial irreducible representation γ of G such that

$$\left|\mathrm{E}_{f,U,W}\Bigg[\mathrm{tr}\bigg(A(f)\sum_{\rho\in\hat{H}}d_\rho(1-\epsilon)^{|\rho|}\,\mathrm{Tr}\Big(\hat{B}_\rho^2\big(\boldsymbol{I}_{d_\gamma}\otimes\rho(f\circ\pi)\big)\Big)\bigg)\Bigg]\right|>d_\gamma\delta.$$

where $A=\gamma\circ A_{U,G}$, $H=G^{\mathrm{SAT}^W}$ and $B=\gamma\circ A_{W,\mathrm{inv}}$. However, by selecting constants $c>\lceil(\log\delta-1)/\log(1-\epsilon)\rceil$ and $u>\lceil(2\log\delta^{-1}+\log c+c\log|G|+4\log d_\gamma+2)/\log c_\mu^{-1}\rceil$, Corollaries 23 and 25 show that

$$\left|\mathrm{E}_{f,U,W}\Bigg[\mathrm{tr}\bigg(A(f)\sum_{\substack{\rho\in\hat{H}\\|\rho|\geq c}}d_\rho(1-\epsilon)^{|\rho|}\,\mathrm{Tr}\Big(\hat{B}_\rho^2\big(\boldsymbol{I}_{d_\gamma}\otimes\rho(f\circ\pi)\big)\Big)\bigg)\Bigg]\right|<\frac{d_\gamma\delta}{2},$$

$$\left|\mathrm{E}_{f,U,W}\Bigg[\mathrm{tr}\bigg(A(f)\sum_{\substack{\rho\in\hat{H}\\|\rho|<c}}d_\rho(1-\epsilon)^{|\rho|}\,\mathrm{Tr}\Big(\hat{B}_\rho^2\big(\boldsymbol{I}_{d_\gamma}\otimes\rho(f\circ\pi)\big)\Big)\bigg)\Bigg]\right|<\frac{d_\gamma\delta}{2},$$

which is a contradiction.

5.4 Hardness of approximating $\mathrm{EQ}_G^1[3]$

We now apply this PCP to obtain hardness results for approximating systems of equations over G.

PROOF of Theorem 1. By Lemma 20 and Lemma 26 for any constants $\epsilon > 0$ and $\delta > 0$ it is possible to choose the parameters of the verifier in

Figure 1 such that it is **NP**-hard to distinguish between the case that there is a proof which the verifier accepts with probability $1 - \epsilon$, and the case that there is no proof which is accepted with probability more than $|G|^{-1} + \delta$.

Now we create a system of equations in the obvious way; the variables corresponds to the positions in the proofs, and we add an equation for each random string corresponding to the test made for this random string. One may think that these would always be on the form $xyz = 1_G$, but this is not the case due to folding over G and over inverse, and in general an equation is of the form $gxy^iz^j = 1_G$, where g is a group constant and $i, j \in \{1, -1\}$. There is also a technicality in that there is a small probability that $h = h^{-1}(f \circ \pi)^{-1}e$ in the protocol, and thus a variable can occur more than once. But since this happens with probability $o(1)$, such equations may be omitted from the instance. Hence we may construct instances of $\mathrm{EQ}^1_G[3]$ in which it is hard to distinguish between the case that $1 - \epsilon$ of all equations are satisfiable, and the case that at most $|G|^{-1} + \delta$ of all equations are satisfiable, which completes the proof.

6 Open questions

An interesting question is that of *satisfiable instances*. Some problems, such as E3-Sat, retain their inapproximability properties even when restricted to satisfiable instances. This is not the case for $\mathrm{EQ}^1_G[k]$ when G is a finite Abelian group, since if such a system is satisfiable a solution may be found essentially by Gaussian elimination. However, when G is non-Abelian, deciding whether a system of equations over G is satisfiable is **NP**-complete [14], so it seems reasonable that the problem over non-Abelian groups retains some hardness of approximation for satisfiable instances. However, the following simple argument shows that we can not hope, even for the non-Abelian groups, for a lower bound of $|G|^{-1} + \delta$: Given an instance σ of $\mathrm{EQ}^1_G[k]$ over some non-Abelian group G, we construct an instance σ' over $\mathrm{EQ}^1_H[k]$, where $H = G/G'$ and G' is the commutator subgroup of G, i.e., the subgroup generated by the elements $\{g^{-1}h^{-1}gh : g, h \in G\}$. The instance σ' is the same as σ, except that all group constants are replaced by their equivalence class in G/G'. Now since H is an Abelian group, we can solve over H. The solution is an assignment of cosets to the variables. We then construct a random solution of x by for each variable choosing a random element in the corresponding coset. Now the value of the left hand side of each equation will be uniformly distributed in the coset of the right hand side, and thus we will satisfy an expected fraction $|G'|^{-1}$ of all equations.

7 Acknowledgments

We would like to thank Johan Håstad for useful discussions and Volker Diekert for valuable comments on a preliminary version of this paper.

A Identities from linear and multilinear algebra

This appendix contains some identities and bounds that are needed in the proof of Lemma 22. They all follow in a straightforward manner from standard linear and multilinear algebra.

Lemma 27 *Let S_ρ be a family of positive semidefinite matrices and d_ρ and n_ρ be positive integers. Then*

$$\sum_{\rho:n_\rho>c} d_\rho(1-\epsilon)^{n_\rho} \operatorname{tr} S_\rho \le (1-\epsilon)^c \sum_\rho d_\rho \operatorname{tr} S_\rho.$$

PROOF. Since the S_ρ is positive semidefinite $\sum_{\rho:n_\rho>c} d_\rho(1-\epsilon)^{n_\rho} \operatorname{tr} S_\rho$ is a sum of non-negative numbers and thus non-negative. Therefore

$$\sum_{\rho:n_\rho>c} d_\rho(1-\epsilon)^{n_\rho} \operatorname{tr} S_\rho \le (1-\epsilon)^c \sum_{\rho:n_\rho>c} d_\rho \operatorname{tr} S_\rho \le (1-\epsilon)^c \sum_\rho d_\rho \operatorname{tr} S_\rho.$$

Lemma 28 *Let D be a diagonal $n \times n$ matrix, $\{S_\rho\}$ be a family of positive semidefinite matrices that are tensor products of $n \times n$ matrices and $k \times k$ matrices, $\{U_\rho\}$ be a family of unitary matrices, that are tensor products of $n \times n$ matrices and $k \times k$ matrices, and d_ρ and n_ρ be positive integers. Then*

$$\left|\operatorname{tr}\left(D \sum_{\rho:n_\rho>c} d_\rho(1-\epsilon)^{n_\rho} \operatorname{Tr}(S_\rho U_\rho)\right)\right| \le \sum_{\rho:n_\rho>c} d_\rho(1-\epsilon)^{n_\rho} \operatorname{tr}(S_\rho),$$

where the inner trace is with respect to the tensor products forming S_ρ and U_ρ.

PROOF. Since D is diagonal, the left expression above can be rewritten as

$$\left|\sum_i D_{ii}\left(\sum_{\rho:n_\rho>c} d_\rho(1-\epsilon)^{n_\rho}\Big(\operatorname{Tr}(S_\rho U_\rho)\Big)_{ii}\right)\right| \le \sum_i \left|\sum_{\rho:n_\rho>c} d_\rho(1-\epsilon)^{n_\rho}\Big(\operatorname{Tr}(S_\rho U_\rho)\Big)_{ii}\right|$$

where the inequality follows since D is unitary and diagonal and thus has diagonal entries with unit magnitude. Since Lemma 34 tells us that $|(\operatorname{Tr} S_\rho U_\rho)_{ii}| \le (\operatorname{Tr} S_\rho)_{ii}$ we are done.

Lemma 29 *Let H be a finite group and let B be a function from H to* $\mathrm{End}(V)$ *in some basis. Let $C(h) = TB(h)T^*$ where T is a unitary matrix. Then $\hat{C}_\rho = (T \otimes \boldsymbol{I})\hat{B}_\rho(T \otimes \boldsymbol{I})^*$.*

Corollary 30 *Let $B(g)$ be a function from H to* $\mathrm{End}(V)$ *in some basis. Let $C(h) = TB(h)T^*$ where T is a unitary matrix. Then $\hat{C}^2_\rho = (T \otimes \boldsymbol{I})\hat{B}^2_\rho(T \otimes \boldsymbol{I})^*$.*

PROOF of Lemma 29. By definition, $\hat{B}_\rho = |H|^{-1} \sum_{h \in H} B(h) \otimes \rho(h)$, and

$$\hat{C}_\rho = |H|^{-1} \sum_{h \in H} C(h) \otimes \rho(h) = |H|^{-1} \sum_{H \in H} (TB(h)T^*) \otimes \rho(h).$$

By a repeated application of the rule $(AB) \otimes (CD) = (A \otimes C)(B \otimes D)$, we can rewrite the last summand as $(TB(g)T^*) \otimes \rho(g) = (TB(g)T^*) \otimes (\boldsymbol{I}\rho(g)\boldsymbol{I}) = (T \otimes \boldsymbol{I})((B(g)T^*) \otimes (\rho(g)\boldsymbol{I})) = (T \otimes \boldsymbol{I})(B(g) \otimes \rho(g))(T^* \otimes \boldsymbol{I})$, which implies that

$$\hat{C}_\rho = \sum_{g \in G} (T \otimes \boldsymbol{I})(B(g) \otimes \rho(g))(T^* \otimes \boldsymbol{I}) = (T \otimes \boldsymbol{I})\hat{B}_\rho(T^* \otimes \boldsymbol{I}).$$

Since $T^* \otimes \boldsymbol{I} = (T \otimes \boldsymbol{I})^*$, the proof is completed.

Lemma 31 *Let A and C be $n \times n$ matrices and B be a tensor product of an $n \times n$ matrix and a $k \times k$ matrix. Then $A(\mathrm{Tr}\, B)C = \mathrm{Tr}((A \otimes \boldsymbol{I}_k)B(C \otimes \boldsymbol{I}_k))$.*

PROOF. Suppose that $B = B_1 \otimes B_2$. Then $(A \otimes \boldsymbol{I}_k)B(C \otimes \boldsymbol{I}_k) = (AB_1 \otimes B_2)(C \otimes I) = AB_1C \otimes B_2$ and hence $\mathrm{Tr}((A \otimes \boldsymbol{I}_k)B(C \otimes \boldsymbol{I}_k)) = (\mathrm{tr}\, B_2)AB_1C = A(\mathrm{Tr}\, B)C$.

Lemma 32 *Let A_1 and A_2 be $n \times n$ matrices and B_1 and B_2 be $k \times k$ matrices. If $A_1A_2 = A_2A_1$ and $B_1B_2 = B_2B_1$, then $(A_1 \otimes B_1)(A_2 \otimes B_2) = (A_2 \otimes B_2)(A_1 \otimes B_1)$.*

Corollary 33 *Let A be an $n \times n$ matrix and B be a $k \times k$ matrix. Then $(A \otimes \boldsymbol{I}_k)(\boldsymbol{I}_n \otimes B) = (\boldsymbol{I}_n \otimes B)(A \otimes \boldsymbol{I}_k)$.*

PROOF of Lemma 32. $(A_1 \otimes B_1)(A_2 \otimes B_2) = (A_1A_2) \otimes (B_1B_2) = (A_2A_1) \otimes (B_2B_1) = (A_2 \otimes B_2)(A_1 \otimes B_1)$.

Lemma 34 *Let A be a positive semidefinite matrix and U be a unitary matrix. Then $|\,\mathrm{tr}(AU)| \leq \mathrm{tr}\, A$.*

PROOF. Since A is positive semidefinite, it can be written as VDV^* where V is a unitary matrix and D is a diagonal matrix with non-negative entries on the diagonal. Since the trace is invariant under similarity transforms, $\operatorname{tr} A = \sum_i D_{ii}$. Let us now rewrite

$$\operatorname{tr}(AU) = \operatorname{tr}(VDV^*U) = \operatorname{tr}(VDV^*UVV^*) = \operatorname{tr}(VDWV^*) = \operatorname{tr}(DW)$$

where $W = V^*UV$ is a product of unitary matrices and therefore unitary. Since a unitary matrix cannot contain entries of absolute value grater than one,

$$|\operatorname{tr}(AU)| = \left|\sum_i D_{ii}W_{ii}\right| \leq \sum_i |D_{ii}W_{ii}| \leq \sum_i D_{ii} = \operatorname{tr} A.$$

References

[1] N. Alon, A. Spencer, The Probabilistic Method, 2nd edition, John Wiley & Sons, 2000.

[2] S. Arora, C. Lund, R. Motwani, M. Sudan, M. Szegedy, Proof verification and the hardness of approximation problems, Journal of the ACM 45 (3) (1998) 501–555.

[3] D. A. M. Barrington, P. McKenzie, C. Moore, P. Tesson, D. Thérien, Equation satisfiability and program satisfiability for finite monoids, in: Proceedings of the 25th Annual Symposium on Mathematical Foundations of Computer Science, Bratislava, Slovak Republic, 2000, pp. 172–181.

[4] D. A. M. Barrington, H. Straubing, D. Thérien, Non-uniform automata over groups, Information and Computation 89 (2) (1990) 109–132.

[5] D. A. M. Barrington, D. Thérien, Finite monoids and the fine structure of NC^1, Journal of the ACM 35 (4) (1988) 941–952.

[6] F. Bédard, A. Goupil, The poset of conjugacy classes and decomposition of products in the symmetric group, Canadian Mathematical Bulletin 35 (2) (1992) 152–160.

[7] M. Bellare, O. Goldreich, M. Sudan, Free bits, PCPs and non-approximability—towards tight results, SIAM Journal on Computing 27 (3) (1998) 804–915.

[8] I. Dinur, S. Safra, The importance of being biased, in: Proceedings of the 34th Annual ACM Symposium on Theory of Computing, Montréal, Quebéc, Canada, 2002, pp. 33–42.

[9] H. Dym, H. P. McKean, Fourier Series and Integrals, Vol. 14 of Probability and Mathematical Statistics, Academic Press, 1972.

[10] L. Engebretsen, The non-approximability of non-Boolean predicates, in: M. Goemans, K. Jansen, J. D. P. Rolim, L. Trevisan (Eds.), Proceedings of 5th International Workshop on Randomization and Approximation Techniques in Computer Science, Vol. 2129 of Lecture Notes in Computer Science, Springer-Verlag, Berkeley, California, USA, 2001, pp. 241–248.

[11] L. Engebretsen, J. Holmerin, Clique is hard to approximate within $n^{1-o(1)}$, in: U. Montanari, J. D. P. Rolim, E. Welzl (Eds.), Proceedings of 27th International Colloquium on Automata, Languages and Programming, Vol. 1853 of Lecture Notes in Computer Science, Springer-Verlag, Geneva, 2000, pp. 2–12.

[12] U. Feige, A threshold of $\ln n$ for approximating set cover, Journal of the ACM 45 (4) (1998) 634–652.

[13] H. Finkelstein, K. I. Mandelberg, On solutions of "equations in symmetric groups", Journal of Combinatorial Theory, Series A 25 (2) (1978) 142–152.

[14] M. Goldmann, A. Russell, The computational complexity of solving systems of equations over finite groups, in: Proceedings of the Fourteenth Annual IEEE Conference on Computational Complexity, Atlanta, Georgia, 1999, pp. 80–86.

[15] V. Guruswami, J. Håstad, M. Sudan, Hardness of approximate hypergraph coloring, in: 41st Annual Symposium on Foundations of Computer Science, IEEE, Redondo Beach, California, 2000, pp. 149–158.

[16] J. Håstad, Some optimal inapproximability results, Journal of the ACM 48 (4) (2001) 798–859.

[17] S. Khot, Improved inapproximability results for maxclique, chromatic number and approximate graph coloring, in: 42nd Annual Symposium on Foundations of Computer Science, IEEE, Las Vegas, Nevada, 2001, pp. 600–609.

[18] C. H. Papadimitriou, M. Yannakakis, Optimization, approximation, and complexity classes, Journal of Computer and System Sciences 43 (3) (1991) 425–440.

[19] R. Raz, A parallel repetition theorem, SIAM Journal on Computing 27 (3) (1998) 763–803.

[20] A. Samorodnitsky, L. Trevisan, A PCP characterization of NP with optimal amortized query complexity, in: Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, Portland, Oregon, 2000, pp. 191–199.

[21] A. Schönhage, V. Strassen, Schnelle Multiplikation großer Zahlen, Computing 7 (1971) 281–292.

[22] J.-P. Serre, Linear Representations of Finite Groups, Vol. 42 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1977.

[23] R. P. Stanley, Enumerative Combinatorics, Volume 2, Vol. 62 of Cambridge Studies in Advances Mathematics, Cambridge University Press, Cambridge, 1999.

[24] S. P. Strunkov, K teorii uravnenij na konečnyh gruppah, Izvestiâ Rossijskoj Akademii Nauk, Seriâ Matematičeskaâ 59 (6) (1995) 171–180, English translation: On the theory of equations in finite groups. Izvestiya: Mathematics, 59(6):1273–1282, 1995.

[25] A. Terras, Fourier Analysis on Finite Groups and Applications, Vol. 43 of London Mathematical Society student texts, Cambridge University Press, Cambridge, 1999.

[26] U. Zwick, Approximation algorithms for constraint satisfaction programs involving at most three variables per constraint, in: Proceedings of the Ninth Annual ACM-SIAM Symposium on Discrete Algorithms, San Francisco, California, 1998, pp. 201–210.

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'