Research Statement

Srivatsa Srinivas

1 Introduction

I am a PhD student of Professor Alireza Salehi-Golsefidy at the University of California, San Diego. My research interests lie in the applications of Probability and Information Theory towards the study of finite groups and number theory. This document will surmise the works that I completed during my PhD, works that are on the way and theorems which can be possibly proved in the future using the ideas that I have helped develop. The papers that I have co-authored are cited in red.

2 Definitions

In order to fluently convey the ideas of my articles, I believe that it would be best to create a vocabulary which can concisely explain the ideas that pervade them.

1. Given a set S and a non-negative valued measure μ on S we define $L^2(S,\mu)$ to be the set of measurable functions $f : S \to \mathbb{C}$ such that $\int_S |f|^2 \, d\mu < \infty$. We note that $L^2(S,\mu)$ forms an inner product space with inner product

$$\langle f, g\rangle = \int_S f\bar{g} \, d\mu$$

We define the 2-norm of a function $f \in L^2(S,\mu)$ to be

$$\|f\|_2^2 := \langle f, f\rangle = \int_S |f|^2 \, d\mu$$

Given a measure space (S,μ) and a function $f : S \to T$, we can endow T with a measure $f[\mu]$ defined by

$$f[\mu](A) := \mu(f^{-1}(A))$$

2. If G is a compact group, we define $L^2(G) := L^2(G,\mu_G)$ where μ_G is the Haar probability measure on G. We define the subspace,

$$L^2(G)^\circ := \{f \mid f \in L^2(G), \langle f, 1\rangle = 0\}$$

3. Let G be a compact group and let μ, ν be Borel probability measures on G. We can define a new Borel probability measure $\mu * \nu$ on G as

$$\int_G f(x) \, d(\mu * \nu)(x) := \int_G \int_G f(yz) \, d\mu(y) d\nu(z)$$

where f is any Borel measurable function. We say that μ is *symmetric* if for all Borel sets $E \subset G$ we have that $\mu(E) = \mu(E^{-1})$. Given a finite subset $S \subset G$ we define

$$\mu_S(x) := \begin{cases} \frac{1}{|S|} \text{ if } x \in S \\ 0 \text{ else} \end{cases}$$

4. Let μ be a symmetric Borel measure on a compact group G. We define an operator $T_\mu : L^2(G) \to L^2(G)$ by

$$(T_\mu(f))(x) = \int_G f(xz^{-1}) d\mu(z)$$

and note that T_μ restricts to an operator on $L^2(G)^\circ$. We define

$$|\lambda|(\mu) := \sup_{\substack{f \in L^2(G)^\circ \\ \|f\|_2 = 1}} \|T_\mu(f)\|_2$$

The above value is referred to as the *spectral gap* (or $1 - x$, where x is the *spectral gap*) of the measure μ.

5. Let G be a group that left acts measurably on a space a measure space (S, ν). We let $\cdot$ denote the group action. Given a probability measure μ on G and a $g \in L^2(S, \nu)$, we define $\mu \boxtimes \nu \in L^2(S, \nu)$ as

$$(\mu \boxtimes g)(x) := \int_G g(y^{-1} \cdot x) \, d\mu(y)$$

If S is a finite set, we assume that ν is the non-normalized counting measure on S.

3 Main Research Interests

3.1 Published Work

3.1.1 Random walks on group extensions in the single scale setting

We note that $SL_2(\mathbb{F}_p) \ltimes \mathbb{F}_p^n$ is the group defined by the following multiplication

$$(A, v) \cdot (B, w) = (AB, Aw + v)$$

We note that the projection $\pi_p : SL_2(\mathbb{F}_p) \ltimes \mathbb{F}_p^n$ given by

$$(A, v) \mapsto A$$

is a homomorphism. In the paper [LV16b] Lindenstrauss and Varju prove the following result

Theorem 1 ([LV16b, Theorem 1])**.** *Let $n \in \mathbb{N}, n > 1$. There exist universal constants K_1, K_2 such that if p is a prime and $p > K_1$, μ is a symmetric probability measure on $SL_2(\mathbb{F}_p) \ltimes \mathbb{F}_p^n$ with α defined to be*

$$\alpha := \max_{v \in \mathbb{F}_p^n} \|\mu \boxtimes \delta_v\|_2$$

Then we have that

$$-\log|\lambda|(\mu) \geq \frac{1}{K_2} \min\left\{ \frac{-\log|\lambda|(\pi_p[\mu])}{\min\{-\log(\alpha^{1/2} - \alpha), 100\}}, -\log\alpha \right\}$$

This theorem is significant because it states that modulo some exceptional cases for small primes, the spectral gap of a measure on $SL_2(\mathbb{F}_p) \ltimes \mathbb{F}_p^n$ depends log-linearly on the spectral gap of the measure obtained on projecting by π_p and the degree to which it fixes a vector in $\mathbb{F}_p^n$ (quantified by α). The above proof exploited the fact that $\mathbb{F}_p^n$ was an abelian group. Therefore, the next logical step would be to formulate a version of the above theorem for $SL_2(\mathbb{F}_p) \times SL_2(\mathbb{F}_p)$. We first define $\pi_{L,p}, \pi_{R,p} : SL_2(\mathbb{F}_p) \times SL_2(\mathbb{F}_p) \to SL_2(\mathbb{F}_p)$ as

$$\pi_{L,p}(x,y) := x, \pi_{R,p}(x,y) := y$$

Question 1. *Does there exist a constant K_1 such that if $p > K_1$, S is a symmetric generating set of $SL_2(\mathbb{F}_p) \times SL_2(\mathbb{F}_p)$, $\lambda_L := |\lambda|(\pi_{L,p}[\mu_S]), \lambda_R := |\lambda|(\pi_{R,p}[\mu_S])$ then*

$$-\log|\lambda|(\mu_S) \gg_{\lambda_L,\lambda_R,|S|} 1$$

In order to state the theorem that Prof. Golsefidy and I proved, which positively answers the above question, we must first define an action of $SL_2(\mathbb{F}_p) \times SL_2(\mathbb{F}_p)$ on the group of automorphisms of $SL_2(\mathbb{F}_p)$. Given an element $(x,y) \in SL_2(\mathbb{F}_p) \times SL_2(\mathbb{F}_p)$ and an automorphism $\phi : \mathrm{Aut}(SL_2(\mathbb{F}_p))$ we define

$$(x,y) \cdot \phi := c_x \circ \phi \circ c_y^{-1}$$

where c_a is the automorphism given by conjugation by a. We can now present our theorem

Theorem 2 ([GS21, Theorem 1])**.** *There exist universal constants K_1, K_2 such that if p is a prime and $p > K_1$, μ is a symmetric probability measure on $SL_2(\mathbb{F}_p) \times SL_2(\mathbb{F}_p)$ with α defined to be*

$$\alpha := \max_{\phi \in \mathrm{Aut}(SL_2(\mathbb{F}_p))} \|\mu \boxtimes \delta_\phi\|_2$$

Then we have that

$$-\log|\lambda|(\mu) \geq \frac{1}{K_2} \min\left\{ \frac{-\log|\lambda|(\pi_{L,p}[\mu])}{\min\{-\log(\alpha^{1/2}-\alpha), 100\}}, \frac{-\log|\lambda|(\pi_{R,p}[\mu])}{\min\{-\log(\alpha^{1/2}-\alpha), 100\}}, -\log\alpha \right\}$$

Our solution to the problem was respected by the group actions community, leading to its publication in *Journal of the European Mathematical Society*. The ideas of this work were further extended to give us the following result

Theorem 3 ([GS22, Weaker version of Theorem D])**.** *Let $\mathbb{G}$ be an algebraic group that is perfect over $\mathbb{Z}$, i.e. $\mathbb{G} = \mathbb{H} \ltimes \mathbb{U}$, where $\mathbb{H}, \mathbb{U}$ are algebraic groups defined over $\mathbb{Z}$ with $\mathbb{H}$ being semi-simple and $\mathbb{U}$ being unipotent. Suppose that $\mathbb{H} = \prod_{j=1}^{l} \mathbb{H}_j$. Then there exists a universal constant K_1 such that if $(F_i)_{1 \leq i \leq k}$ are finite fields with characteristic greater than K_1 and μ is a symmetric probability measure on $G = \mathbb{G}(\prod_{i=1}^{k} F_i)$ whose support generates G, on definining*

$$\alpha := \min_{x \in G} \mu(x)$$

$$H_{i,j} = \mathbb{H}_j(F_i)$$

and noting that that there are homomorphisms, $\pi_{i,j} : G \to H_{i,j}$ we have that

$$-\log|\lambda|(\mu) \gg \min_{i,j}\{-\log|\lambda|(\pi_{i,j}[\mu])\}$$

where the implied constants in the $\gg$ depend on $\alpha, \dim\mathbb{G}, k$ and the maximum power of the prime appearing in the F_i.

The full version of the above result has the following implications for the field; spectral gap results for perfect algebraic groups in the "single scale" setting only depend upon spectral gap results for simple algebraic groups. It is set for publication in the *Transactions of the AMS*.

3.2 Completed Ideas being typed

The following results will be published during my tenure as a postdoc at your institution

3.2.1 Random walks on group extensions in the multi scale setting

The works from the previous section deal with the "single scale" setting. The work that Professor Golsefidy and I have since completed and is in the progress of being typed deal with the "multi scale" setting. Transferring the ideas of Theorem 3 from the single scale setting to the multi scale setting was not trivial and requires a lot of supplementary theorems. We hope to finish typing up a result that encompasses the following theorem within a year and a half

Theorem 4 (Proposed corollary)**.** *Let $\mathbb{G}$ be an algebraic group that is perfect over $\mathbb{Z}$, i.e. $\mathbb{G} = \mathbb{H} \ltimes \mathbb{U}$, where $\mathbb{H}, \mathbb{U}$ are algebraic groups defined over $\mathbb{Z}$ with $\mathbb{H}$ being semi-simple and $\mathbb{U}$ being unipotent. Suppose that $\mathbb{H} = \prod_{j=1}^{l} \mathbb{H}_j$. Define $G_n := \mathbb{G}(\mathbb{Z}/n\mathbb{Z})$ and $H_{j,n} = \mathbb{H}_j(\mathbb{Z}/n\mathbb{Z})$. Note that there are projections $\pi_{i,j} : G_n \to H_{j,n}$. Then there exists a universal constant K_1 such that if $n \in \mathbb{N}, n > K_1$, μ is a symmetric probability measure on G_n whose support generates G_n,*

$$\alpha := \min_{x \in G} \mu(x)$$

and λ is an eigenvalue of an irreducible representation of G_n that does not factor through an irreducible representation of any G_q where $q \mid n$ then,

$$-\log \lambda \gg \min_{j} \{-\log |\lambda|(\pi_{j,n}[\mu])\}$$

where the implied constants in the $\gg$ depend on $\dim \mathbb{G}$ *and α.*

The above result would have a great impact on the "spectral gap community" for it states the following mantra; Spectral gap results on perfect algebraic groups in the number theoretical setting only depend on spectral gap results for simple algebraic groups. We hope that the full version of the above theorem, combined with recent advances in the field for spectral gap results on simple algebraic groups, will help prove the Super-Approximation conjecture [Gol19, Page 2].

3.3 Ideas that I want to work on in the future

3.3.1 Random walks on group extensions in the Archimedean setting

The paper which contains Theorem 1 was an offshoot of a more significant result obtained by Lindenstrauss and Varju in [LV16a]. The paper [LV16a] deals with the group $SO_n(\mathbb{R}) \ltimes \mathbb{R}^n$. Therfore, it might be fruitful to explore analogues of our non-archimedean results in the archimedan setting. Applying ideas from the proof of Theorem 4 one could hope to secure the following the result

Theorem 5. *Let S be a finite symmetric generating set on $SO_3(\mathbb{R}) \times SO_3(\mathbb{R})$ whose support generates $SO_3(\mathbb{R}) \times SO_3(\mathbb{R})$. Then we have that*

$$-\log |\lambda|(\mu) \gg_{|S|} \min\{-\log |\lambda|(\pi_L[\mu]), -\log |\lambda|(\pi_R[\mu])\}$$

3.3.2 Uniform spectral gaps

Given a compact group G, we define $|\lambda|(G,k)$ as

$$|\lambda|(G,k) := \sup_{|S|=k, \langle S\rangle = G} |\lambda| \left(\frac{\mu_S + \mu_{S^{-1}}}{2} \right)$$

If G is a finite group then by definition, $|\lambda|(G,k) < 1$. Therefore, questions of interest pertaining $|\lambda|(G,k)$ either involve a family of finite groups or infinite compact groups. Using a result of Gamburd and Brueillard [BG10] one can show the following

Theorem 6 (Folklore Result)**.** *There exists a sequence of primes* $(p_i)_{i\in I} \subset \text{Primes}$ *such that on defining*

$$G := \prod_{i\in I} SL_2(\mathbb{F}_{p_i})$$

for all $k > 1 \in \mathbb{N}$ *we have that*

$$|\lambda|(G,k) < 1$$

This result is interesting because it states that every generating set of the above group generates the group quickly. One can now ask a more detailed question

Question 2. *Does there exist a prime* $p \in \text{Primes}$ *and a* $k \in \mathbb{N}$ *such that*

$$|\lambda|(SL_2(\mathbb{Z}_p), k) < 1$$

This question is very interesting to me, and although I have had some thoughts and ideas on how to attack this problem, as of now they are insufficient. During my postdoc, I would like to work on this problem and try to create a roadmap towards solving this problem.

4 Miscellaneous research interests

4.1 Using SMT solvers to answer questions in pure math

SMT (Satisfiable Modulo Theory) solvers are computer programs that determine the satisfiability of tractable first order logic statements. They are used in the verification of protocols, programs and constructing puzzles. These solvers have immediate application to questions in pure mathematics which can be broken down into combinatorial or integer inequality problems which are easy to state but too difficult to work out by hand. In a blog post (in progress, to be completed before applications) I have proved the following result of Schinzel from 1962, shoving the arduous part of the paper in to a Haskell program that uses SMT solvers.

Theorem 7 ([Sch62])**.** *If* $\xi \in \mathbb{C}$ *is such that there exists an arithmetic progression of length* 4*, i.e. a set of the form*

$$\{a, a+d, a+2d, a+3d\}$$

which is a subset of $\{\xi^i \mid i \in \mathbb{Z}\}$ *then we must have that* $|\xi| = 1$*.*

I would like to devote some time during my postdoc towards studying the integration of SMT solvers to theorem proving assistants such as Lean4, and possibly contribute to projects such as `lean-auto`.

References

[BG10] Emmanuel Breuillard and Alex Gamburd. "Strong Uniform Expansion in $SL(2,p)$". In: *Geometric and Functional Analysis* 20 (2010), pp. 1201–1209.

[Gol19] Alireza Salehi Golsefidy. "Super-Approximation, II: the p-adic case and the case of bounded powers of squrae-free integers". In: *Journal of the European Mathematical Society* 21.7 (2019), pp. 2163–2232. DOI: 10.4171/JEMS/883.

[GS21] Alireza Salehi Golsefidy and Srivatsa Srinivas. "Random walks on direct product of groups". In: *Accepted to be published in JEMS* (2021).

[GS22] Alireza Salehi Golsefidy and Srivatsa Srinivas. "Random walks on Group Extensions". In: *Accepted to be published in Transactions of the AMS* (2022).

[LV16a] Elon Lindenstrauss and Péter P. Varjú. "Random walks in the group of Euclidean isometries and self-similar measures". In: *Duke Mathematical Journal* 165.6 (2016), pp. 1061–1127. DOI: 10.1215/00127094-3167490. URL: https://doi.org/10.1215/00127094-3167490.

[LV16b] Elon Lindenstrauss and Péter P. Varjú. "Spectral gap in the group of affine transformations over prime fields". en. In: *Annales de la Faculté des sciences de Toulouse : Mathématiques* Ser. 6, 25.5 (2016), pp. 969–993. DOI: 10.5802/afst.1518. URL: https://afst.centre-mersenne.org/articles/10.5802/afst.1518/.

[Sch62] Andrzej Schinzel. "Solution d'un problème de K. Zarankiewicz sur les suites de puissances consécutives de nombres irrationnels". FRA. In: *Colloquium Mathematicum* 9.2 (1962), pp. 291–296.