Seewoo Lee
Research Statement

My research centers on number theory, particularly delving into the realms of automorphic forms and the Langlands program, leveraging computational tools to enhance exploration and understanding.

(Relative) Langlands program

Introduced by Robert Langlands, the *Langlands Program* constitutes a comprehensive unification theory in number theory and beyond, seeking to establish connections between two seemingly disparate mathematical domains: *Galois Representations* and *Automorphic Forms.*

In 1846, Évariste Galois delved into the zeros of polynomial equations by examining their *symmetries*, specifically the *Galois groups.* These groups are a fundamental and crucial tool for the study of Diophantine equations. For example, after the discovery of the formulas for cubic and quartic equations by Cardano, it took about 300 more years for Abel and Ruffini to provide a negative answer to the question of the solvability of general polynomial equations of degree at least 5, using Galois theory. One ultimate goal for number theorists is to understand the structure of the *absolute Galois group* $\mathrm{Gal}_{\mathbb{Q}}$, which encodes all possible symmetries for polynomials with rational coefficients. *Galois representations* propose a way to explore the group through the lens of linear algebra.

On the other side of the mathematical spectrum are *automorphic forms* - special functions exhibiting profound internal symmetries. Take *modular forms*, for instance, which are automorphic forms defined on the space of two by two matrices with specific symmetries. They not only encode intricate arithmetic information through *Fourier coefficients* but also play a role in deriving non-trivial formulas in number theory, including the Lagrange's four squares theorem.

The crux of the Langlands program lies in its conjecture that Galois representations and automorphic forms share a profound connection, mediated by entities known as *L-functions.* Evidence of this conjecture can be discovered in Wiles's proof of Fermat's Last Theorem, where the existence of a non-trivial integer solution necessitated the concurrent construction of a Galois representation and an associated modular form with special properties, ultimately making them impossible to exist.

My research delves into the rich world of automorphic forms within the Langlands program, focusing particularly on *the Langlands functorialities* — the relationships between automorphic forms defined on different spaces. Known results for specific pairs of spaces have already yielded significant theorems in number theory, such as the Sato–Tate conjectures [19, 3] or generalized Ramanujan conjectures [34] on the Fourier coefficients of automorphic forms.

Ichino-Ikeda formula for general spin groups - Bessel case

For example, the Gan–Gross–Prasad conjecture [16] proposes an answer to the restriction problem - restricting an automorphic representation on a group to a subgroup - in terms of non-vanishing of the special values of the associated L-functions. Ichino and Ikeda presented a refined version of the conjecture, an equation directly relates period integrals and L-values, and proved certain cases [21]. Building upon the groundwork laid by Liu [32] on the special orthogonal groups ($\mathrm{SO}_2 \times \mathrm{SO}_5$ and $\mathrm{SO}_3 \times \mathrm{SO}_6$) and drawing insights from Emory's work [13] on *general spin groups* ($\mathrm{GSpin}_n \times \mathrm{GSpin}_{n+1}$ for $n = 2, 3, 4$), I am working on the Ichino–Ikeda conjecture for general spin groups, particularly in cases involving general Bessel periods. Furthermore, I'm trying to generalize Furusawa and Morimoto's work on the $\mathrm{SO}_2 \times \mathrm{SO}_{2n+1}$ case and Böcher's conjecture [15] in this direction. My approach involves leveraging exceptional isomorphisms between low-rank general spin groups and other classical groups and reducing the conjecture to the already known cases.

Computational approach in number theory

In the realm of the Langlands Program, dealing with abstract objects like Galois representations and automorphic forms often benefits from grounding these concepts in tangible, computable counterparts. My prior work, exemplified by my undergraduate and master's theses on Maass wave forms and quantum modular forms, provides concrete instances of automorphic forms. By experimenting with examples through MATLAB [22] and SageMath [35], I found an appropriate definition of *Hecke operators* for the spaces of these automorphic forms, which lead to the discovery of novel and non-trivial number-theoretic identities related to roots of unity [26, 27].

Modular forms and optimal sphere packings

Optimal sphere packing problem asks the densest packing of d-dimensional space $\mathbb{R}^d$ with unit balls. The problem is trivial for $d = 1$, and $d = 2$ case is solved by Thue in 1890. The three-dimensional case, known as Kepler's conjecture, was resolved by Thomas Hales based on heavy computer calculations [18]. It took nearly a decade to be formally checked via computer proof assistants HOL Light and Isabelle [17].

A surprising bridge emerges between the 8 and 24-dimensional sphere packing problem and number theory. Cohn and Elikies introduced the *linear programming bound* [9], which suggests that identifying specific "magic functions" holds the key to optimal sphere packing in these dimensions. However, constructing these functions, requiring control over both the function and its Fourier transform, is challenging due to the uncertainty principle. Maryna Viazovska used modular forms from number theory to construct a magic function for dimension 8 [36], and the 24-dimensional case was soon resolved using similar methods [10].

To prove these two cases, the authors [36, 10] relied on numerical approximations and extensive computer assisted computations to establish desired inequalities between modular forms. However, it is natural to ask if there is a more general and conceptual proof for these inequalities. While a more straightforward proof exists for the case of dimension 8 by Dan Romik [33], I found *algebraic* proofs for both of the dimensions 8 and 24 cases that circumvents reliance on numerical calculations or approximations [28]. Notably, I develop a theory of *positive* and *completely positive* quasimodular forms, and use the theory to study the *magic modular forms* appear in the optimal sphere packing. Especially, I found an interesting connection with Kaneko and Koike's *extremal quasimodular forms* [24], which are conjectured to have nonnegative Fourier coefficients. The proofs are based on a simple observation on the monotonicity of quotients of two forms to compare. The main inegredients are the differential equations satisfied by the modular forms. This also opens a new possibility to generalize Viazovska's construction to the dimensions other than 8 and 24, based on the construction of Fourier eigenfunctions by Feigenbaum, Grabner, and Hinder [14]. Especially, it would imply a new upper bound for the uncertainty principle [4] in specific dimensions. Also, as a byproduct, I proved Kaneko–Koike's conjecture on the positivity of Fourier coefficients of extremal forms in the case of depth 1.

Again, the above results are hinted a lot from experiments with many examples through SageMath. Especially, once I plot the quotient of two modular forms (Figure xxx), it becomes clear that what I should try to prove (monotonicity and limit), which turned out to be true.

Maass wave forms, Quantum modular forms, and Hecke operators

In [8], Cohen construct the first explicit example of maass wave form, based on one of the Ramanujan's q-series. Its coefficients are certain Hecke character of the real quadratic field $\mathbb{Q}(\sqrt{6})$, and Cohen conjectured that the Maass wave form is an eigenform for suitable Hecke operators. However, the usual Hecke operator is not the right candidate since the multiplier system (Nebentypus) of Cohn's Maass wave form does not come from Dirichlet characters. In my undergraduate and master's thesis, I propose the correct definition of Hecke operator that works for more general multiplier systems, including Cohn's Maass wave form, and prove that the Maass wave form is indeed eigenform under the operators [26, 27]. Also, one can associate *quantum modular forms* to the Maass wave form as a period integral (following [30, 37]), and I proved that this map is Hecke-equivariant. As a corollary, this gives a nontrivial identities on ceratin p-th root of unities and p-th coefficient of the Maass wave form for primes p. Same argument also worked for Li–Ngo–Rhoades' Maass wave form [31].

Other projects

My interest is not restricted to number theory. I'm interested in various subjects, including

- formalization of mathematics,
- discrete geometry,
- homomorphic encryption.

Formalization of Polynomial Fermat's Last Theorem

Conway–Soifer Conjecture - homothetic case

Consider an equilateral triangle of side length $n + \varepsilon$ for an integer $n \geq 1$ and a sufficiently small $\varepsilon > 0$. What is the minimum number of unit equilateral triangles needed to cover the whole triangle? It is easy to see that at least $n^2 + 1$ triangles are required, by considering area. Conway and Soifer give two different ways to cover the large triangle with $n^2 + 2$ unit triangles [11], and conjectured that this is the minimum number of triangles required.

With Jineon Baek, we proved that the conjecture is true *if we restrict our attention to homothetic triangles*, i.e. assuming all the sides of the unit equilateral triangles are parallel to the large triangle ($\triangle$ or $\bigtriangledown$) [2]. In fact, we proved the following general statement.

Theorem (Baek-Lee)**.** *Call a triangle a horizontal triangle of base b and height h, if it has a side of length b parallel to the x-axis, and the height h measured in the direction of y-axis. Then $n^2 + 1$ horizontal triangles of base b and height h cannot cover a horizontal triangle of base nb and height $> nh$.*

The proof is elementary, and we also determined the largest possible ε such that an equilateral triangle of side length $n + \varepsilon$ can be covered by $n^2 + 2$ or $n^2 + 3$ homothetic unit equilateral triangles ($\varepsilon = 1/(n + 1)$ and $\varepsilon = 1/n$, respectively).

Encrypted transfer learning with homomorphic encryption

While I was working at CryptoLab as a Research Engineer during my alternative military service, I developed privacy-preserving machine learning library called `HEaaN.SDK` [1] based on CKKS homomorphic encryption (HE) scheme [5]. In theory, one can compute arbitrary arithmetic circuit over encrypted real and complex numbers (with small errors) using CKKS scheme, and one might think implementing machine learning algorithms with HE is not hard. However, encrypted computations over ciphertexts are much slower than over plaintexts, and naive implementations could be highly impractical. Hence we need to re-design the algorithm in *HE-friendly* way, which is usually a nontrivial research problem. In particular, I found that there were no HE-based training algorithms for *multiclass* classification tasks at the moment, and most of the previous works are only applicable for binary classifications with small number of features.

To implement such an HE-based multiclass classification algorithm, we need 1) efficient encrypted softmax computation with large input, and 2) efficient large encrypted matrix multiplication. Both problems were resolved in HETAL (efficient **H**omomorphic **E**ncryption based **Tra**nsfer **L**earning) [29]. For the softmax computation, we found that homomorphic comparison [6] can be used to normalize inputs (subtract maximum value), then homomorphic domain extension [7] let us to cover wider range of inputs with much smaller errors, compared to the previous works [23, 25, 20]. To perform efficient encrypted matrix multiplications, we implement two types of multiplications $AB^\intercal$ and $A^\intercal B$ separately, which allow us to avoid transpose operation. Tiling and complex packing techniques are used to reduce the number of rotations required substantially, which result matrix multiplication algorithms that are 1.8 to 323 times faster than the previous algorithms [12, 23]. As a result, we were able to fine-tune commonly used vision and language models within an hour with a single A40 GPU on five benchmark datasets, which shows HE-based encrypted fine-tuning is indeed practical.

References

[1] HEaaN.SDK. `https://www.heaan.it/docs/stat/python/`.

[2] Jineon Baek and Seewoo Lee. n^2+1 unit equilateral triangles cannot cover an equilateral triangle of side $> n$ if all triangles have parallel sides, 2024.

[3] Tom Barnet-Lamb, David Geraghty, Michael Harris, and Richard Taylor. A family of calabi–yau varieties and potential automorphy ii. *Publications of the Research Institute for Mathematical Sciences*, 47(1):29–98, 2011.

[4] Jean Bourgain, Laurent Clozel, and Jean-Pierre Kahane. Principe d'heisenberg et fonctions positives. In *Annales de l'institut Fourier*, volume 60, pages 1215–1232, 2010.

[5] Jung Hee Cheon, Andrey Kim, Miran Kim, and Yongsoo Song. Homomorphic encryption for arithmetic of approximate numbers. In *Advances in Cryptology–ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I 23*, pages 409–437. Springer, 2017.

[6] Jung Hee Cheon, Dongwoo Kim, and Duhyeong Kim. Efficient homomorphic comparison methods with optimal complexity. In *Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part II 26*, pages 221–256. Springer, 2020.

[7] Jung Hee Cheon, Wootae Kim, and Jai Hyun Park. Efficient homomorphic evaluation on large intervals. *IEEE Transactions on Information Forensics and Security*, 17:2553–2568, 2022.

[8] Henri Cohen. q-identities for maass waveforms. *Inventiones mathematicae*, 91(3):409–422, 1988.

[9] Henry Cohn and Noam Elkies. New upper bounds on sphere packings i. *Annals of mathematics*, pages 689–714, 2003.

[10] Henry Cohn, Abhinav Kumar, Stephen Miller, Danylo Radchenko, and Maryna Viazovska. The sphere packing problem in dimension 24. *Annals of Mathematics*, 185(3):1017–1033, 2017.

[11] JH Conway and Alexander Soifer. Covering a triangle with triangles, 2005.

[12] Eric Crockett. A low-depth homomorphic circuit for logistic regression model training. *Cryptology ePrint Archive*, 2020.

[13] Melissa Emory. On the global Gan–Gross–Prasad conjecture for general spin groups. *Pacific Journal of Mathematics*, 306(1):115–151, 2020.

[14] Ahram S Feigenbaum, Peter J Grabner, and Douglas P Hardin. Eigenfunctions of the fourier transform with specified zeros. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 171, pages 329–367. Cambridge University Press, 2021.

[15] Masaaki Furusawa and Kazuki Morimoto. Refined global gross–prasad conjecture on special bessel periods and böcherer's conjecture. *Journal of the European Mathematical Society*, 23(4):1295–1331, 2020.

[16] Wee Teck Gan, Benedict H Gross, and Dipendra Prasad. Symplectic local root numbers, central critical L-values, and restriction problems in the representation theory of classical groups. *Astérisque*, pages No–pp, 2011.

[17] Thomas Hales, Mark Adams, Gertrud Bauer, Tat Dat Dang, John Harrison, Hoang Le Truong, Cezary Kaliszyk, Victor Magron, Sean McLaughlin, Tat Thang Nguyen, et al. A formal proof of the kepler conjecture. In *Forum of mathematics, Pi*, volume 5, page e2. Cambridge University Press, 2017.

[18] Thomas C Hales. A proof of the kepler conjecture. *Annals of mathematics*, pages 1065–1185, 2005.

[19] Michael Harris, Nick Shepherd-Barron, and Richard Taylor. A family of calabi-yau varieties and potential automorphy. *Annals of Mathematics*, pages 779–813, 2010.

[20] Seungwan Hong, Jai Hyun Park, Wonhee Cho, Hyeongmin Choe, and Jung Hee Cheon. Secure tumor classification by shallow neural network using homomorphic encryption. *BMC genomics*, 23(1):284, 2022.

[21] Atsushi Ichino and Tamutsu Ikeda. On the periods of automorphic forms on special orthogonal groups and the gross–prasad conjecture. *Geometric and Functional Analysis*, 19:1378–1425, 2010.

[22] The MathWorks Inc. MATLAB, 2022.

[23] Chao Jin, Mohamed Ragab, and Khin Mi Mi Aung. Secure transfer learning for machine fault diagnosis under different operating conditions. In *International Conference on Provable Security*, pages 278–297. Springer, 2020.

[24] Masanobu Kaneko and Masao Koike. On extremal quasimodular forms. *Kyushu Journal of Mathematics*, 60(2):457–470, 2006.

[25] Joon-Woo Lee, HyungChul Kang, Yongwoo Lee, Woosuk Choi, Jieun Eom, Maxim Deryabin, Eunsang Lee, Junghyun Lee, Donghoon Yoo, Young-Sik Kim, et al. Privacy-preserving machine learning with fully homomorphic encryption for deep neural network. *iEEE Access*, 10:30039–30054, 2022.

[26] Seewoo Lee. Quantum modular forms and hecke operators. *Research in Number Theory*, 4(2):18, 2018.

[27] Seewoo Lee. Maass wave forms, quantum modular forms and hecke operators. *Research in the Mathematical Sciences*, 6(1):7, 2019.

[28] Seewoo Lee. Algebraic proof of modular form inequalities for optimal sphere packings. *In preparation*, 2024.

[29] Seewoo Lee, Garam Lee, Jung Woo Kim, Junbum Shin, and Mun-Kyu Lee. HETAL: Efficient privacy-preserving transfer learning with homomorphic encryption. In *International Conference on Machine Learning*, pages 19010–19035. PMLR, 2023.

[30] John Lewis and Don Zagier. Period functions for maass wave forms. i. *Annals of Mathematics*, 153(1):191–258, 2001.

[31] Yingkun Li, Hieu T Ngo, and Robert C Rhoades. Renormalization and quantum modular forms, part i: Maass wave forms. *arXiv preprint arXiv:1311.3043*, 2013.

[32] Yifeng Liu. Refined global gan–gross–prasad conjecture for bessel periods. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2016(717):133–194, 2016.

[33] Dan Romik. On Viazovska's modular form inequalities. *Proceedings of the National Academy of Sciences*, 120(43):e2304891120, 2023.

[34] Peter Sarnak. Notes on the generalized ramanujan conjectures. *Harmonic analysis, the trace formula, and Shimura varieties*, 4:659–685, 2005.

[35] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.8)*, 2023. `https://www.sagemath.org`.

[36] Maryna Viazovska. The sphere packing problem in dimension 8. *Annals of mathematics*, pages 991–1015, 2017.

[37] Don Zagier. Quantum modular forms. *Quanta of maths*, 11:659–675, 2010.