Study Plan

Applicant's name: Yihan Zhang

Major: Computational complexity, quantum computing.

Proposed Topic: My research interest mainly lies in quantum computing, computational complexity and algorithm design and analysis, all of which are significant topics in theoretical computer science. I am also interested in combinatorial number theory with strong computer science techniques, in particular, problems connected with Van der Waerden's theorem and Szemerédi's theorem.

Potential Advisor: Shengyu Zhang (Theory, Computer Science and Engineering)

1 Computational complexity and quantum computing

1.1 Introduction to Graph Isomorphism Problem

Recently, László Babai[1] from University of Chicago posted a digest of a series of talks and claimed that he found an algorithm to solve Graph Isomorphism Problem (GI) in quasi-polynomial time, which might be the most significant breakthrough in recent decade in theoretical computer science. Its an interesting topic and worth of further research.

To commence with, I will first introduce P and NP. We claim that a problem is in P if it can be solved by Deterministic Turing Machine in polynomial time. And we claim that a problem is in NP if it can be verified by Deterministic Turing Machine in polynomial time. To determine whether P is equal to NP or not is a major open problem in theoretical computer science. And Graph Isomorphism Problem has strong connections to P/NP problem. As the name implies, GI asks us to determine whether two finite graphs are isomorphic.

1.2 Relations of GI with computational complexity and quantum computing

What does it mean if $P = NP$? Briefly speaking, it means we can solve a problem if we can judge its answer, which seems amazing. The most common way to show that two sets are different is to find an element which lies in set A but doesnt lie in set B. In computational complexity, those elements are defined to be NP-intermediate (NPI) problems. They lies in NP but doesnt lie in P.

Therefore, Graph Isomorphism Problem is significant because its one of two candidates of NPI problems. The other one is Factoring Problem. The existence of NPI problems leads to a claim that $P \neq NP$. And obtaining a quasi-polynomial time algorithm means that GI is either more likely to get into P or more likely to stay outside of P forever, if someone shows that the time complexity of Babais algorithm is a strict lower bound.

Famous theoretical computer scientist Scott Aaronson from MIT made some comments regarding Babais result on his blog[2], which might lead us to a deeper understanding of Babais work. He mentioned that the problem solved by Babai is actually String Isomorphism Problem (Given two string on a finite set and several permutations as generators of a group G, the problem asks: can we find a permutation σ in G such that $\sigma(x) = y$?)

Moreover, GI also has strong connections to quantum computing. GI is a special case of Hidden Subgroup Problem (HSP) in quantum computing. HSP is described as: given a group G and a function $f : G \to \{0, 1\}^n$, find a subgroup H of G such that $f(x) = f(y)$ if and only if $x - y \in H$, where x and y are 0-1 strings. In terms of graph theory, an isomorphism between two graphs is a permutation, and S_n is a hidden subgroup. In fact, many scientists tried to bring GI into BQP class, which is to say, find a polynomial algorithm for GI on quantum computer. But they all failed.

1.3 Why I am competent for related topics

Clearly, many problems remain open and more related questions can be posed regarding this topic. I intend to access these topics step by step from fundamental and special cases. As is known to us, theoretical computer science has strong connections to mathematics and many mathematical techniques are involved in theoretical computer science research. I believe I have a solid foundation of mathematics comparing with other undergraduates who major in computer science and technology. Specially, I am familiar with algebra and group representation, which are commonly used in quantum computing. Also, I have taken, currently am taking courses or learn by myself many mathematics courses to support my theory research, including partial differential equations, algebra, group representation theory, algebraic topology, functional analysis, etc. Compared with general specializations in computer engineering, the key distinction lies in the level of formality and rigor necessary to call something a proof. I never stop training myself be rigorous which is essential in theory research.

Moreover, I received systematic computer science and engineering education and grasp many technologies to implement algorithm and form or verify conjectures according to a large scale of calculation. Although it cannot substitute a rigorous proof, I can easily obtain intuition or determine whether a result is likely to be true or not, which will facilitate my theory research.

2 Combinatorial number theory with strong computer science techniques

2.1 Overview of combinatorial number theory

In combinatorial number theory, many conjectures are motivated by Van der Waerden's and Szemerédi's theorem and more related questions can be posed. Although these problems have been discussed for a long time since their formulation, many of them still remain open, and some of them even seem far from clear. I intend to access these topics step by step from fundamental and special cases. My main resource for posing, history and progress of problems is the serial papers *Problems and results on combinatorial number theory I[3], II[4], II'[5] and III[6]* by Erdös P.

In particular, I will adopt computer techniques in research. For one thing, it will partly solve a problem. For another, results can be verified step by step on machine automatically, during which underlying error will be reported. To be specific, I want to computationally verify my results' validity and obtain empirical data to have a refined understanding of my hypothesis. If the hypothesis is true, computational method will give me actual examples; otherwise, it will produce a counterexample. The latter case is pretty significant when construction of counterexample is sophisticated and lacking in regularity, in other words, it can hardly be engineered by combining known facts. In such cases, I will turn to computer to find counterexamples and analyse why they occur. Then I will revise my hypothesis until things go well in every corner.

2.2 Background of Van der Waerden's theorem and Szemerédi's theorem and related topics

To make it more self contained, Van der Waerden's theorem and Szemerédi's theorem are shown below:

Theorem 1 (Van der Waerden's theorem[7]). *$\forall r, k \in \mathbb{Z}^+$, $\exists N$, s.t. if integers $\{1, 2, \ldots, N\}$ are coloured, each with one of r different colors, then there are $\geq k$ integers in arithmetic progression all of the same color. The least such N is the Van der Waerden number(function) $W(r, k)$.*

Note 1 ([11]). *In terms of hypergraph, we can sate the above theorem by considering the hypergraph whose vertices are the integers and whose edges are the k term arithmetic progressions. This hypergraph has chromatic number $+\infty$.*

Theorem 2 (Szemerédi's theorem[8]). *$\forall \delta > 0, k \in \mathbb{Z}^+$, $\exists N$, s.t. every subset A of set $\{1, 2, \ldots, N\}$ of size $\geq \delta N$ contains an arithmetic progression of length k.*

Note 2 ([8]). *In terms of density[9], the above theorem can be stated as follows: any subset of $\{1, 2, \ldots, N\}$ with positive upper density contains infinite arithmetic progressions of length*

k for all positive integers k. Here, a subset A of $\{1, 2, \ldots, N\}$ is said to have positive upper density iff.

$$\overline{d}(A) = \limsup_{n \to +\infty} \frac{|A \cap \{1, 2, \ldots, N\}|}{n} > 0.$$

Note 3 ([8])**.** *If we define function $r_k(N)$ as the the size of the largest subset of $\{1, 2, \ldots, N\}$ without an arithmetic progression of length k, the above theorem can be stated as*

$$r_k(N) = o(N).$$

We will come to this later.

2.2.1 Conjectures related to $f(n)$

Van der Waerden[12] proved that: there is an $f(n)$ so that if we divide integers $1 \leq t \leq f(n)$ into two classes, at least one of them contains an arithmetic progression of n terms. Then mathematicians want to establish satisfactory upper and lower bound for $f(n)$. Paul Erdös conjectured that:

$$\lim_{n \to +\infty} f(n)^{\frac{1}{n}} = +\infty. \tag{1}$$

But considering the difficulty of (1), Erdös later gave an easier version: let $\frac{1}{2}n < u \leq n$, let $f(u, n)$ be the smallest integer s.t. if we divide integers $1 \leq t \leq f(u, n)$ into two classes, there is always an arithmetic progression of n terms, in which one of the classes has $\geq u$ terms. However, we still know little about $f(u, n)$. We can get

$$f(u, n) > (1 + c(\varepsilon))^n \quad \text{for } u > \frac{n}{2}(1 + \varepsilon) \tag{2}$$

by probability method. But more interesting and challenging problems can be posed. It is reasonable to begin by determining or estimate $f(u, n)$ for u and n which are fixed or conform to some special condition. Van der Waerden[12] even extend $f(n)$ to more than two variables in his original paper which proved Van der Waerden's theorem. This is of course further more difficult to evaluate.

Again, because of the very difficulty to determine upper bound for $f(n)$, Turán and Erdös[13] conjectured that every sequence of positive upper density contains arbitrarily long arithmetic progressions. Or, equivalently, let $r_k(n)$ be the smallest integer s.t. if $1 \leq a_1 < \ldots < a_{r_k(n)} \leq n$, then $(a_i)_{i=1}^{r_k(n)}$ contains an arithmetic progression of k terms. Then the above conjecture can be sated as

$$r_k(n) = o(n). \tag{3}$$

Szemerédi[14] proved this which is known as the glamorous Szemerédi theorem. Here I want to mention that Fürstenberg[15] later proved the theorem using ergodic theory and topological dynamics, which is a stunningly amazement in the area of combinatorial number theory. Similarly, obtaining asymptotic bound for $r_k(n)$ is still a hard task. Szemerédi remarked that we don't even know whether it's true that

$$\frac{r_k(n)}{r_{k+1}(n)} \to 0 \quad (n \to +\infty). \tag{4}$$

2.2.2 Other problems related to Van der Waerden's and Szemerédi's theorem

Let $A(n, k)$ be the largest integer s.t. if we divide integers $1 \leq t \leq n$ into two classes, there are $\geq A(n, k)$ k-term arithmetic progressions all whose terms are in the same class. Then the result

$$A(n, k) > c(k)n^2 \tag{5}$$

can be obtained by applying Van der Waerden's theorem, and

$$A(n, k) < \frac{n^2}{2(k-1)2^{k-1}}(1 + o(1)) \tag{6}$$

follows from some probability method.

Let $f_k(n, \alpha)$ be the largest integer s.t. every set of αn integers $\leq n$ contains $\geq f_k(n, \alpha)$ arithmetic progressions of k terms. Then the result

$$f_k(n, \alpha) > c(\alpha, k)n^2 \tag{7}$$

can be obtained by applying Szemerédi's theorem.

It's also a challenge to obtain an asymptotic bound for $A(n, k)$ and $f_k(n, \alpha)$.

2.3 Planned Study

To commence, as student who majors in Computer Science and Technology during undergraduate time, I have to show the interaction between number theory and computer science. It's twofold: firstly, a computer science student can use computers to form conjectures or obtain intuition regarding unsolved conjectures based on patterns coming from running a large scale of calculations; secondly, it's also a common technique to divide a conjecture into several cases and prove by reduction by hand that the core part is true for sufficiently large integers, then resort to computers to knock off corner cases.

Basically, I will use computer science skills to search for regularities in congruences and identities for proposed conjectures. Then it will be easier to apply techniques from the field of modular forms, analytics, ergodic theory, topological dynamics etc. During this process, generating functions will certainly play a significant role. For many combinatorial objects, generating functions turn out to have certain symmetries when looked at as functions. In other words, when viewed algebraically, one can get deep understanding of combinatorial objects using knowledge of group, fields and stuffs with nice symmetries; when viewed from an analytical point, one will usually get familiar with functions by evaluate their analytical qualities. Using the two techniques allows one to move knowledge from one side to the other. According to W. T. Gowers[10], combinatorial number theory lies on the interface of additive number theory, harmonic analysis and combinatorics where neither algebraic method nor analytical method, such as Riemann zeta function $\zeta(s)$ plays a central role. As shown in section 2.2, it's hard to say which field of knowledge would get involved in this the area of combinatorial number theory. When Fürstenberg first introduced ergodic theory and topological dynamics into combinatorial number theory, one cannot immediately evaluate influence and prospective of such invasion, just as the application of analytics to combinatorial number theory. In fact, time witnessed the formulation of a new specialization called analytical number theory after the application of analytics. Nowadays ergodic theory and topological dynamics also seem to become most powerful tools in number theory research which are worth of further development.

Combinatorial number theory also involves determining some function(finding certain identities) and evaluating upper and lower bound for it(building satisfactory inequalities). The basic motivation for this process is counting objects. Here counting is a generalized concept, possibly delineating some quality of certain set which has certain known relation with other different types of sets.

There is another thing I want to explain. As is known to all, finding valuable problems to work on is perhaps the hardest part of mathematics research. Personally speaking, I intend to begin from existing unsolved problems or conjectures. For one thing, those problems are formulated by previous mathematicians, which means they have certain meaningful background. For another, there have been some progress regarding many of them, which means I can adopt some classical methods or ideas rather than do everything from scratch.

To be specific, procedures of research are shown below.

1. Formulate a hypothesis regarding a conjecture by beginning with some intuition about what might be true.

2. Test the hypothesis with as many cases as possible using computers, either programming languages or symbolic computation software. As a student who has received systematic education of computer science, I am capable of choosing examples which are both good enough to indicate main characteristics of the core case and to cover enough corner cases. Moreover, knowledge of algorithm and data structure also allows me to design efficient algorithms. Finally, engineering techniques, such as parallel computing, will lend support to implementing these algorithms so that computers can run a large scale of data in tolerable time with reasonable memory, in other word, I can get results without much cost.

3. If guess from step 1 doesn't work out for all cases, revise hypothesis based on step 2 (either generalize the hypothesis, i.e. weaken condition of it, or classify correct cases in original hypothesis, i.e. restrict conclusion of it). Return to step 2 to check again. So on and so forth until I'm sure that it's true, i.e. step 1 works out for all cases checked in step 2. Finally, the most important step, prove in precise mathematical manner that my hypothesis holds in general. Usually methods like induction and generating functions are applied. But sometimes techniques out of expectation might be needed as shown in section 2.2.

References

[1] László Babai: Talks, Nov 10-Dec 1, 2015. In *László Babai's homepage of University of Chicago* from http://people.cs.uchicago.edu/~laci/quasipoly.html.

[2] G. Phi. Fo. Fum. In *Scott Aaronson's blog* http://www.scottaaronson.com/blog/?p=2521

[3] Erdös, P. (1973). Problems and results on combinatorial number theory I. In *A survey of combinatorial theory (Proc. Internat. Sympos., Colorado State Univ., Fort Collins, Colo., 1971)* (pp. 117-138).

[4] Erdös, P. (1974). Problems and results on combinatorial number theory II. In *Journées Arithmétiques de Bordeaux* (pp. 295-310).

[5] Erdös, P. (1977). Problems and results on combinatorial number theory II'. In *J. Indian Math. Soc.* (pp. 285-298).

[6] Erdös, P. (1977). Problems and results on combinatorial number theory III. In *Number Theory Day* (pp. 43-72). Springer Berlin Heidelberg.

[7] Van der Waerden's theorem. (2015, October 28). In *Wikipedia, The Free Encyclopedia.* Retrieved 04:38, October 29, 2015, from https://en.wikipedia.org/w/index.php?title=Van_der_Waerden%27s_theorem&oldid=646964802

[8] Szemerédi's theorem. (2015, September 30). In *Wikipedia, The Free Encyclopedia.* Retrieved 04:52, October 29, 2015, from https://en.wikipedia.org/w/index.php?title=Szemer%C3%A9di%27s_theorem&oldid=683519170

[9] Natural density. (2015, October 13). In *Wikipedia, The Free Encyclopedia.* Retrieved 04:55, October 29, 2015, from https://en.wikipedia.org/w/index.php?title=Natural_density&oldid=685623708

[10] Gowers, W. T. (2001). Some unsolved problems in additive/combinatorial number theory. *preprint.*

[11] Erdös, P. (1980). A survey of problems in combinatorial number theory. *Ann. Discrete Math, 6*, 89-115.

[12] Van der Waerden, B. L. (1927). Beweis einer baudetschen vermutung. *Nieuw Arch. Wisk, 15*(2), 212-216.

[13] Erdös, P.; Turán, P. (1936). On some sequences of integers. *Journal of the London Mathematical Society, 11*(4), 261-264.

[14] Szemerédi, E. (1975). On sets of integers containing no k elements in arithmetic progression. *Acta Arith, 27*(2), 199-245.

[15] Fürstenberg, H. (1977). Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions. *Journal d'Analyse Mathmatique, 31*(1), 204-256.