KU-STAR Research Internship

Tejas Anand

IIT Delhi
Kyoto University

June 3, 2024

Presentation Overview

Overview
- About me
- Research Topic at Kyoto University
- Essential things for Kyoto University for research
- Future Research Interests
- Thank You

About me

- JEE Advanced 2021 AIR 119
- Incoming 4th year CS Student (Integrated Dual Degree) at IIT Delhi
- Previously worked as a research intern at the Algorithms, Biology Structure Lab at INRIA, Cote d'Azur, Nice France.
- Working with Professor Kohei Suenaga and Atsushi Igarashi on extending approximation algorithms for model counting to integers and lists.
- Hobbies include playing the piano, table tennis and relaxing.

Research Topic at Kyoto University

Approximating the number of **equivalence classes** of a given relation.

Research Topic at Kyoto University

Approximating the number of **equivalence classes** of a given relation.

And how does it help?

Research Topic at Kyoto University

Approximating the number of **equivalence classes** of a given relation.

And how does it help?

Well, It helps in quantifying the sensitive **information leaked** by a computer program as **entropy**.

A question for the audience

Example: How many equivalence classes does the following relation have, where x, y are 32 bit integers ?

$$x \sim y \Leftrightarrow x \equiv y \equiv 0 \mod 8 \textbf{ or } x = y \tag{1}$$

A question for the audience

Example: How many equivalence classes does the following relation have, where x, y are 32 bit integers ?

$$x \sim y \Leftrightarrow x \equiv y \equiv 0 \mod 8 \textbf{ or } x = y \tag{1}$$

Answer: $7 \cdot 2^{29} + 1$. All of the multiples of 8 form 1 equivalence class, and the remaining $7/8^{ths}$ of the total 2^{32} integers form singleton equivalence classes of their own.

A question for the audience

Example: How many equivalence classes does the following relation have, where x, y are 32 bit integers ?

$$x \sim y \Leftrightarrow x \equiv y \equiv 0 \mod 8 \textbf{ or } x = y \tag{1}$$

Answer: $7 \cdot 2^{29} + 1$. All of the multiples of 8 form 1 equivalence class, and the remaining $7/8^{ths}$ of the total 2^{32} integers form singleton equivalence classes of their own.

$$(x \equiv y \equiv 0 \mod 8) \vee (x = y) \rightarrow \boxed{\textbf{Our Algorithm}} \rightsquigarrow 7 \cdot 2^{29}$$

Research Topic at Kyoto University

- Model counting is the problem of counting the number of solutions to a given set of constraints.
- The problem of Model Counting (#SAT) is #P-complete.
- Therefore, we work with an (ϵ, δ) approximation algorithm $\mathcal{A}$, whose output n over a problem instance $\mathcal{F}$ satisfies,

$$\Pr[\mathrm{n} \leftarrow \mathcal{A}(\mathcal{F}) : \frac{\#\mathcal{F}}{1+\epsilon} \leq \mathrm{n} \leq \#\mathcal{F}(1+\epsilon)] \geq 1 - \delta$$

- In simple words, it gives a good enough number with high probability, for small values of ϵ and δ.
- For instance, we might want to count the number of equivalence classes of the given relation

$$x \sim y \Leftrightarrow x \equiv y \equiv 0 \mod 8 \vee x = y \tag{2}$$

Research Topic at Kyoto University

- Recently, a scalable approximation algorithm for model counting over boolean constraints was propsed by Chakraborty et al.
- We want to generalize this algorithm to simple arithmetic constraints like modulo, addition, subtraction, etc. over integers (finite fields like Z_n) and lists, using SMT solvers (SAT modulo theory) like Z3.
- This has applications in computer security, it would be the main ingredient to quantify the sensitive information leaked by a computer programme.

Essential things at Kyoto University for research

- One of the most important things for me that Kyoto University offers is the peaceful and serene environment, which in my opinion is essential for research.
- I would also like to thank my Advisors Professor Kohei Suenaga and Atsushi Igarashi for hosting me and providing me with a wonderful topic to work on.

Future Research Interests

- Haven't yet decided on a specific area of research as of now.
- For now, I would like to explore more by taking courses in different areas of computer science like verification, ML, systems etc.
- This internship would be really helpful in helping me explore approximation algorithms.

Thank You

Thank You for your Attention!