Міністерство освіти і науки України
Сумський державний університет
Наукове товариство студентів, аспірантів,
докторантів і молодих вчених СумДУ

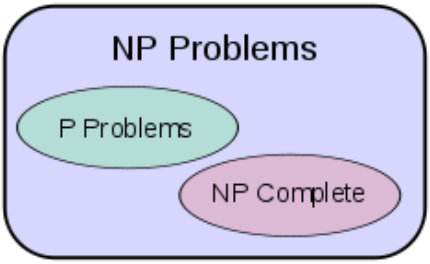
ПЕРШИЙ КРОК У НАУКУ

Матеріали
IX студентської конференції
(Суми, 25 лютого 2018 року)

Суми
Сумський державний університет
2018

РІВНІСТЬ КЛАСІВ P І NP

Перехрестюк П.О., *студентка*; СумДУ, гр. ІН-72

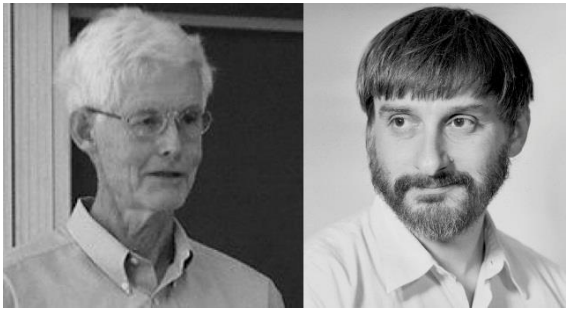


Питання про рівність класів P і NP займає центральне місце в сучасній теоретичній і практичній інформатиці серед задач з теорії алгоритмів. Це також одна з семи невирішених задач тисячоліття, розв'язання якої триває вже більше трьох десятиліть. І якщо ця рівність підтвердиться науково, це буде означати, що швидкість вирішення складних задач у будь-яких областях збільшиться у багато разів, ніж це є зараз.

Так у чому ж полягає проблема P=NP? Якщо позитивну відповідь на якесь питання можна швидко перевірити за поліноміальний час (зміна часу виконання алгоритму не залежить від об'єму даних) то чи правда, що відповідь на це питання можна так само швидко знайти (за поліноміальний час і використовуючи поліноміальну пам'ять)? Або, чи дійсно перевірка результату розв'язання задачі може бути складнішою за її рішення? Важливість питання P vs NP пов'язана з успішними теоріями криптографії на основі NP-повноти і її складності, а також приголомшливих практичних наслідків конструктивного доказу P=NP.

Теорія NP-повноти бере свої корені в теорії обчислювання, яка з'явилася в роботах Тьюринга, Геделя та інших в 30-х роках минулого століття. Так, алгоритми рішення P vs NP задач почали шукати найрізноманітніші вчені. На початку 1970-х років виникла необхідність у швидкому алгоритмі вирішення задач типу P та NP, адже з його допомогою можна було б набагато швидше розв'язати будь-яку іншу задачу такого типу. Це, майже одночасно, зрозуміли

вчені Стівен Кук і Леонід Левін. Саме вони зробили великий внесок у



розкриття цієї проблеми та поширення її в маси. На даний момент отримано безліч цікавих результатів, так чи інакше пов'язаних з P vs NP, але неможна сказати, що досягнуто якийсь прогрес. Наприклад, 6 серпня 2010 року індійський математик, співробітник дослідницької лабораторії в Пало-Альто Віней Деолалікар виклав свій доказ нерівності P і NP. Це викликало небачений резонанс серед його колег – вчені почали масово читати та обговорювати статтю. На жаль, майже всі спеціалісти одразу знайшли недоліки в доказі і вже через тиждень математичне співтовариство дійшло висновку, що з поставленим завданням Деолалікар не впорався. Час від часу, з'являються роботи про доказ або спростування цієї проблеми, але поки що нічого з цього не підтвердилося.

Проблема P vs NP важлива насамперед для сучасної криптографії. Якщо виявиться, що P=NP – ми матимемо можливість побудувати швидкі алгоритми для завдань з класу NP, і багато типів шифрування відразу стануть застарілими, оскільки кожен матиме швидкий алгоритм, який зможе обійти захист. Також алгоритми для вирішення завдань з типу NP використовуються при відновленні частково пошкоджених файлів, розкладанні числа на прості множники в криптографії, оптимізації маршрутів для перевезення товарів різного типу в логістиці та багато іншого.

1. Иэн Стюарт. Величайшие математические задачи. — М.: Альпина нон-фикшн, 2015. — 460 с.
2. Borwein, J. and Bailey, D. Mathematics by Experiment: Plausible Reasoning in the 21st Century. Wellesley, MA: A K Peters, pp. 4-5, 2003.
3. S. Aaronson. Is P versus NP formally independent? Bulletin of the EATCS, (81), October 2003.

Керівник: Шуда І.О, *доцент* каф. МА і МО