Тези до семінару
«Алгоритми розв'язання лінійних обмежень у кільцях лишків та їх застосування»

Кривий С.Л.

Алгоритми, які автор виносить на семінар, відносяться до однієї з областей сучасних досліджень, яка називається «**Constraint Programming** (CP)» (**Програмування з обмеженнями**). Цю область відносять до математичних основ штучного інтелекту і вона активно розвивається зв'язку з тим, що її методи застосовуються в задачах планування, логістики, побудови пруверів, біоінформатики тощо.

Основна проблема, яку розв'язують в області CP – це проблема Constraint Satisfaction Problem (CSP). Розв'язання CSP – це пошук моделі, на якій всі обмеження виконуються.

Розглядаються алгоритми розв'язання систем лінійних Діофантових обмежень типу рівностей (однорідні/неоднорідні) та заперечення відношення рівності в кільці лишків за модулем $\boldsymbol{m}$:

$$S = \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1n}x_n \;\; R \;\; b_1, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2n}x_n \;\; R \;\; b_2, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \;\; \ldots \quad (\text{mod m}) \\ L_q(x) = a_{q1}x_1 + \ldots + a_{qn}x_n \;\; R \;\; b_q, \end{cases}$$

де $R=\{=,\neq\}$, а коефіцієнти $b_i, a_{ij} \in Z_m$ і пошук розв'язків ведеться в кільці Z_m.

Показано, що пропоновані алгоритми мають поліноміальну складність для всіх обмежень. Проблема розв'язання такого типу обмежень зводиться до розв'язання одного лінійного порівняння.

Робота алгоритмів ілюструється прикладами та графіками. Обговорюються області застосування розроблених алгоритмів та короткий огляд інших підходів до розв'язання CSP для лінійних обмежень. Описується застосування отриманих результатів у криптографії