第六届（2021）全国高校密码数学挑战赛

赛题二

一、赛题名称

Z_2^n上非空子集线性不等式完全刻画问题

二、赛题描述

2.1 基础知识

设 n 为正整数，$Z_2 = \{0,1\}$，$Z_2^n = Z_2 \times Z_2 \times \cdots \times Z_2$为所有分量均在$Z_2$上取值的所有 n 元组组成的集合。

对任意给定集合Z_2^n的非空子集 A，我们总可以用一组整系数线性不等式 L **完全刻画**，也就是说，该线性不等式组在限制变元取值为 0 和 1 时其解所构成的集合恰好等于 A。

例如，n=3, A={(000),(101),(011),(110)}。我们可以构造一组线性不等式组 L:

$$\begin{cases} x_1 + x_2 \geq x_3 \\ x_1 + x_3 \geq x_2 \\ x_2 + x_3 \geq x_1 \\ x_1 + x_2 + x_3 \leq 2 \end{cases},$$

其由 4 个不等式组成。容易验证，上述线性不等式组 L 关于(x_3,x_2,x_1)的解集恰好为 A。

2.2 问题描述

给定Z_2^n上的非空子集A，求一组整系数线性不等式L，使得该线

性不等式组在Z_2^n上的解集恰好等于A且要求L中不等式个数尽可能少。

2.3 成绩评判标准

本赛题包含 8 道小题，每道小题给定的子集分别存储在一个文本文件中，并采用统一格式命名为 q_i_n=a.txt，其中 i 表示小题的序号，a 表示 n 的取值，相关参数设置见表 1。例如 q_1_n=6.txt，表示第 1 道小题，n 等于 6。文件中指定子集包含的每个元素均采用十六进制表示，高位在左边，低位在右边。对于指定的 n，有效数据为从低位开始往高位截取 n 个比特，例如元素 3b，写成二进制比特 00111011，如果 n=6，则对应的变元(x_6,x_5,x_4,x_3,x_2,x_1)取值为(111011)。

表 1 每道小题的参数设置

小题序号	n	元素个数
1	6	29
2	8	97
3	10	317
4	12	2017
5	14	6361
6	16	32386
7	20	491144
8	24	8115092

假设有 m 名选手参赛，第i名选手对第j道小题得到$l_{i,j}$个线性不等式。如果选手不做小题，或者其给出的线性不等式的解集错误，不等于指定的子集，则该小题得 0 分；否则，恰好等于给定的子集时，该选手第j道小题得分为

$$Score_{i,j} = \delta_j c_j / l_{i,j},$$

这里

$$c_j = \min\{l_{1,j}, l_{2,j}, \dots, l_{m,j}, r_j\},$$

其中，δ_j为第j道小题的权重分值，r_j为第j道小题不等式个数的参考值，它们的取值见表 2。这里特别说明的是，**参赛选手给出的线性不等式组中不能包含除主变元外的其他任何中间变元(即哑变元(dummy variable))，否则该题记 0 分**。

表 2 每道小题权重分值δ_j和不等式个数参考值r_j的取值

小题序号j	δ_j	r_j
1	100	8
2	200	16
3	200	30
4	200	180
5	400	800
6	600	2300
7	800	36000
8	1000	576000

选手i的总成绩为

$$Score_i = \sum_{j=1}^{8} Score_{i,j}.$$

本赛题需提交一份 word 说明文件，源程序代码以及记录每道小题答案的文本文件。其中，word 文件要求详细说明所采用的方法，源代码运行环境，以及每道小题求解的线性不等式的个数等，如果直接使用了他人方法，则需注明引用来源，如果提出新方法，需详细说明，可酌情加分；记录每道小题答案的文本文件要求统一命名为 q_i_l=a.txt，其中 i 表示小题序号，a 表示文件中包含的线性不等式的

个数，a 为十进制表示的整数，高位在左边，低位在右边。文本文件格式要求如下:

1) 每行文本包含一个线性不等式，因此文本总行数等于线性不等式的总个数;

2) 对每个线性不等式 $a_1x_1 + a_2x_2+\ldots+a_nx_n+b \geq 0$,约定用 n+1 个整数存储，文本格式如下:

$$a_1, a_2, \ldots, a_n, b$$

例如，n=6，线性不等式为 $2x_1 - x_2 + x_6 - 5 \geq 0$，则存储该线性不等式的文本数据如下:

2, -1, 0, 0, 0, 1, -5

三、密码学背景及相关问题的研究进展

整数线性规划（Integer Linear Programming, ILP）是在某些线性约束条件下求目标函数的最大值或最小值的一类问题。一个具体的 ILP 问题可以描述如下:

给定正整数n、实数矩阵A、实数向量b和实数$c_1, c_2, \ldots, c_n$，寻找满足条件$Ax \leq b$且使得目标函数$\sum_{i=1}^{n} c_i x_i$达到最大或最小的n维整数向量x。

近些年，ILP 问题被广泛应用于密码学分析中，已经成为对称密码自动化分析的一种强大工具。

差分分析和线性分析是两种最常用且非常有效的对称密码分析方法。研究人员已经将 ILP 问题与差分分析和线性分析等相结合，发

展出一套自动化寻找对称密码差分迹和线性迹的工具。在基于 ILP 模型的密码分析中，一个核心的数学问题就是，对密码算法核心部件的密码属性进行线性不等式刻画，给出它们之间的约束条件，然后利用 Gurobi，Cplex 等软件进行求解。上述问题可以抽象为Z_2^n上非空子集线性不等式完全刻画问题。针对该问题，当前主要求解方法可参考文献[1]和[2]。虽然利用 Gurobi 等软件求解 ILP 问题的效率与变元和不等式个数的关系尚不能准确刻画，但一般来说，变元和不等式个数显著减少时，求解效率往往会更高。因此我们要求该问题中求得的线性不等式组 L 中包含的线性不等式个数尽可能的少。

四、参考文献

[1] Yu Sasaki and Yosuke Todo. New algorithm for modeling s-box in MILP based differential and division trail search. In Farshim P., Simion E. (eds) Innovative Security Solutions for Information Technology and Communications. SecITC 2017. Lecture Notes in Computer Science, vol 10543, pages 150–165. Springer, Cham, 2017.

[2] Daniel Coggia and Christina Boura. Efficient milp modelings for sboxes and linear layers of SPN ciphers. IACR Transactions on Symmetric Cryptology, 2020, Issue 3:327–361, 2020.