第八届（2023）全国高校密码数学挑战赛

赛题三

一、赛题名称：布尔函数的求解问题

二、赛题描述

2.1 符号说明

二元域$\mathbb{F}_2$：是由元素 0，1 按照异或运算“$\oplus$”和乘法运算“$\times$”构成的域：$0\oplus 0=0, 0\oplus 1=1, 1\oplus 0=1, 1\oplus 1=0, 0\times 0=0$，$0\times 1=0$，$1\times 0=0$，$1\times 1=1$；

n维线性空间$\mathbb{F}_2^n$：$\mathbb{F}_2^n=\{(x_0,x_1,\dots,x_{n-1})|x_i\in\mathbb{F}_2, 0\le i\le n-1\}$为$\mathbb{F}_2$上的$n$维线性空间，其中$n\ge 1$为正整数；

$\mathbb{F}_2^n$上的内积运算“$\cdot$”：$x\cdot y=\bigoplus_{i=0}^{n-1}x_i\times y_i$，其中$x,y\in\mathbb{F}_2^n$。

2.2 基础知识

定义n元布尔函数f为$\mathbb{F}_2^n$到$\mathbb{F}_2$的映射，记$\mathfrak{B}_n$为所有n元布尔函数组成的集合。定义$\mathbb{F}_2^n$到整数集合$\mathrm{Z}_{2^n}=\{0,1,\dots,2^n-1\}$上的一个双射运算为：

$$c=(c_0,c_1,\dots,c_{n-1})\to\sum_{i=0}^{n-1}c_i2^{n-1-i},$$

则在此对应下，$\mathbb{F}_2^n$上的每个向量都可以表示为集合Z_{2^n}中的一个整数。

对于任意$f\in\mathfrak{B}_n$，我们可以将f的取值排列成2^n维的列向量：

$$\{f(0),f(1),\dots,f(2^n-1)\},$$

记为f的真值表向量。进一步，定义f的 Walsh 谱向量为：

$$\hat{\boldsymbol{f}}=\{\hat{f}(0),\hat{f}(1),\dots,\hat{f}(2^n-1)\}$$

其中

$$\hat{f}(\alpha)=\sum_{x\in\mathbb{F}_2^n}(-1)^{\alpha\cdot x\oplus f(x)}\ ,\ \alpha\in\mathbb{F}_2^n$$

我们称列向量行号α为地址，对应取值$\hat{f}(\alpha)$为该地址的 Walsh 谱值。

2.3 问题描述

设n为正整数，给定由若干个地址和对应 Walsh 谱值所组成二元对构成的集合$\{(i_j,\gamma_{i_j})\}_{0\le j\le m-1}$，其中$0<m<2^n$，要求参赛者尽可能多的求取出集合

$$\{f\in\mathfrak{B}_n\mid\hat{f}(i_j)=\gamma_{i_j},0\le j\le m-1\}$$

中的元素，即布尔函数的真值表向量。

变元n有 7 种不同规模，分别为 13、14、15、16、17、18 和 19。在不同规模下，m有两种取值，因此共 14 道题目。

附件文件包含 7 份题目数据文件（分别放在 13、14、15、16、17、18 和 19 文件夹下，每个文件夹下各两份）、数据格式说明文件、5 元函数的示例文件和参考文献。

2.4 成绩评判标准

针对每个小题，要求给出计算结果，并简述求解原理（包括给出求解思路、建立问题转化模型和分析可解性等）、求解方案（包括给出算法和实现方案、分析复杂度和优化程序等）和实现效率（包括计算平台、计算需要的时间和空间等）。

每个小题求解结果的文件应包括如下参数：解得个数和各函数的真值表。格式约定：第 0 行给出所求得函数的总个数，第一行给出第一个布尔函数的完整真值表，此后每个函数各占一行，从第二个函数

开始仅给出与第一个函数真值表不同的坐标即可。文件命名和题目文件相同即可。

参赛者所求取满足条件的布尔函数的个数越多，得分越高。将每个选手的14个题的解的个数求和，最大值记为max，最小值记为min，令 z=(max-min)/100。若某选手的求解总数为 A，则$\left\lceil\frac{A-min}{Z}\right\rceil$为该选手的得分，其中$\lceil\cdot\rceil$表示向上取整。

理论部分注重求解原理、技术和方法创新以及算法理论的完善性等，鼓励思考分析随机条件下影响解个数的指标因素和建立合理的模型评估解个数的分布情况等开放性问题，满分为 100 分；

最终得分中计算得分和理论得分各占 50%。引用前人方法的必须给出明确引用，否则报告内容作废。

三、密码学背景及相关问题的研究进展

布尔函数是密码学的重要研究对象，在设计序列密码、分组密码散列函数和随机数发生器中扮演着重要的角色，研究布尔函数的密码学性质是密码学中最活跃的研究领域。Walsh 谱是研究布尔函数密码学性质的重要工具。布尔函数的许多性质都可以利用 Walsh 谱表示或反映，如布尔函数的平衡性、线性结构、最佳线性逼近、非线性度、Bent 性、扩散特性、相关免疫性和代数结构等。

Walsh 谱和布尔函数的密码学性质紧密相关。在已知 Walsh 谱的若干元素的条件下，研究布尔函数的计数和构造问题具有重要意义。一方面，研究该问题有理论意义，指导和帮助理解 Walsh 谱的密码学性质；另一方面，研究该问题有实际应用价值，比如可以帮助设计者

在密码算法设计中快速地选择出合适的布尔函数和在密码算法安全性评估中建立科学严谨的分析模型等。

四、参考文献

1．Thomas Cusick, Pantelimon Stanica，Cryptographic Boolean Functions and Applications，Academic Press（2009）

2. Gilbert Strang，Introduction to Applied Mathematics, Wellesley-Cambridge Press(1986)

3. Yishay Mansour，Learning Boolean Functions via the Fourier Transform Theoretical，Advances in Neural Computation and Learning (1994)