第二届（2017）全国高校密码数学挑战赛
赛题一

一、赛题名称：布尔函数方程的求解问题

二、赛题描述：

2.1 基本概念：

布尔函数是密码学中重要的研究对象, Walsh谱是研究布尔函数密码学性质的重要工具.

设$\mathbb{F}_2 = \{0, 1\}$, 按模2加运算"$\oplus$"和乘运算"$\cdot$"构成一个域. 设$k \geq 1$, 记

$$\mathbb{F}_2^k = \{(a_0, \cdots, a_{k-1}) \mid a_i \in \mathbb{F}_2, 0 \leq i \leq k-1\}$$

为$\mathbb{F}_2$上的k维线性空间, 称映射$f : \mathbb{F}_2^k \to \mathbb{F}_2$是$k$元布尔函数.

$\mathbb{F}_2^k$中向量与集合$\{0, 1, \cdots, 2^k-1\}$的元素存在自然的一一对应, $c = (c_0, \cdots, c_{k-1}) \mapsto \sum_{i=0}^{k-1} c_i 2^i$. 在此对应下, 可以把$k$元布尔函数$f$的函数值列成一个$2^k$维的列向量, 记为

$$f(\mathbb{F}_2^k) \triangleq \begin{pmatrix} f(0) \\ f(1) \\ \vdots \\ f(2^k-1) \end{pmatrix} \in \mathbb{F}_2^{2^k},$$

称为函数f的真值表向量.

对$\mathbb{F}_2^k$中的任一向量c, k元布尔函数$f(x)$在c点的Walsh谱值定义为

$$w_f(c) = \frac{1}{2^k} \sum_{x \in \mathbb{F}_2^k} (-1)^{f(x) \oplus c \cdot x},$$

其中$x=(x_0,x_1,\cdots,x_{k-1})\in\mathbb{F}_2^k$, $c\cdot x=\oplus_{i=0}^{k-1}c_ix_i$是$c$与$x$的内积.

2.2 问题描述:

设k,n是正整数, $m=2^k$, 给定$\mathbb{F}_2$上的$m\times n$阶列满秩矩阵A, m维向量b, 及k维向量$\alpha,\beta,\gamma,\delta$, 且$\alpha\oplus\beta\oplus\gamma\oplus\delta=\mathbf{0}$,其中$\mathbf{0}$为$k$维向量. 设$f$是未知的$k$元布尔函数, x是$\mathbb{F}_2^n$中的未知向量, 满足下述方程组

$$\begin{cases} Ax\oplus f(\mathbb{F}_2^k)=b, \\ w_f(\alpha)=w_f(\beta)=\frac{1}{8}, \\ w_f(\gamma)=w_f(\delta)=-\frac{1}{8}. \end{cases}$$

令参数$k=12,m=4096,n=90$, 对给定的$A,b,\alpha,\beta,\gamma,\delta$(见附件), 求解$x$和$f$:

2.3 评分标准：

(1) 给出求解原理（在给定参数规模下的非穷举方式求解思路, 问题转化模型, 可解性原理, 解的唯一性等问题）；

(2) 设计求解方案（给出算法及实现方案,分析复杂度及可行性,算法优化比较等）；

(3) 解出答案；

(4) 讨论一般参数$(k,m=2^k,n)$条件下方程组解的唯一性问题。

四、参考文献

[1] 李超，屈龙江等,《密码函数的安全性指标分析》, 科学出版社.