布尔函数的求解问题介绍

XXX, XXX , 2023. 03. 25

汇报内容

密码学背景

布尔函数是密码学的重要研究对象

- 布尔函数广泛用于编码和构造密码算法等
- 评价指标：平衡性、非线性度、代数次数和相关免疫度等

Walsh变换是研究布尔函数性质的重要工具

- Walsh变换是$\mathbb{F}_2$上函数的Fourier变换：$e^{\pi i}+1=0,(-1)^{f(x)}=1-2f(x)$
- Walsh谱包含了布尔函数的所有信息，和真值表互相反演
- Walsh谱和布尔函数的众多评价指标紧密相关，如平衡性，相关免疫度等

相关概念和性质

Definition (*n*元布尔函数)

设$n \geq 1$, 定义n元布尔函数f为$\mathbb{F}_2^n \to \mathbb{F}_2$ 的映射，其中$\mathbb{F}_2^n$为n维线性空间。一般情况下，1维线性空间$\mathbb{F}_2^1$简记为$\mathbb{F}_2$。记$\mathfrak{B}_n$为所有n元布尔函数组成的集合。

Definition (真值表)

设$n \geq 1$，f是n元布尔函数。记整数集$Z_{2^n} = \{0, 1, ..., 2^n - 1\}$，定义$\mathbb{F}_2^n$到$Z_{2^n}$的对应关系为$(x_0, x_1, ..., x_{n-1}) \to \sum_{i=0}^{n-1} x_i 2^{n-1-i}$，并且在此对应关系下，记$2^n$维列向量$\mathbf{f} = (f(0), f(1), ..., f(2^n - 1))$为$f$的真值表。

Definition (Walsh谱)

设$n \geq 1$，f是n元布尔函数。定义$\hat{\mathbf{f}} = (\hat{f}(0), \hat{f}(1), ..., \hat{f}(2^n - 1))$ 为函数f的*Walsh*谱向量, 其中

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

为地址α处的*Walsh*谱值，“$\cdot$”为$\mathbb{F}_2^n$上的内积运算。

为了直观的描述Walsh谱，我们引入哈达玛矩阵和极性化向量两个概念：

Definition (哈达玛矩阵)

设$\mathbf{H}_n$是2^n阶哈达玛矩阵，即$\mathbf{H}_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, $\mathbf{H}_n = \begin{bmatrix} \mathbf{H}_{n-1} & \mathbf{H}_{n-1} \\ \mathbf{H}_{n-1} & -\mathbf{H}_{n-1} \end{bmatrix}$，即$\mathbf{H}_n = \{(-1)^{(i\cdot j)}\}_{(i,j\in\mathbb{F}_2^n)}$.

Definition (极性化向量)

设f为n元布尔函数。定义$(-1)^{\mathbf{f}} = \{(-1)^{f(0)}, (-1)^{f(1)}, ..., (-1)^{f(2^n-1)}\}$为$f$的极性化向量。

由定义可知，n元布尔函数f的Walsh谱可以如下描述

$$\hat{\mathbf{f}} = \mathbf{H}_n(-1)^{\mathbf{f}}$$

即Walsh谱向量本质上是由哈达玛矩阵作用在极性化向量上得到。

计算Walsh谱，若将哈达玛矩阵作为普通矩阵，则大体需要2^{2n}次乘法运算。若考虑哈达玛矩阵的性质，利用蝶形算法（FFT）大体上在$n2^n$的计算量下完成计算：具体代码如下：

```
void FFT(int *f, int nn)//生成walsh谱
{
        for(int i=0; i<(1<<nn); i++) f[i] = 1-2*f[i];

        for(int i = 1;i<nn+1;i++)
        {
                for(int h = 0;h<(1<<(nn-i));h++)
                 {
                        for(int j = 0;j<(1<<(i-1));j++)
                        {
                                int t1 = f[j+h*(1<<i)]+f[j+(1<<(i-1))+h*(1<<i)];
                                int t2 =f[j+h*(1<<i)]-f[j+(1<<(i-1))+h*(1<<i)];
                                f[j+h*(1<<i)] = t1;
                                f[j+(1<<(i-1))+h*(1<<i)] = t2;
                        }
                }
        }
}
```

关于哈达玛矩阵，有如下性质：

- 对称性：$(\mathbf{H}_n)^T = \mathbf{H}_n$，$T$表示矩阵的转置操作
- 正交性：$\mathbf{H}_n\mathbf{H}_n = 2^n\mathbf{I}_n$，$\mathbf{I}_n$表示$2^n$阶单位矩阵

由此可以得到Walsh谱的如下性质：

- 反演公式：$(-1)^{\mathbf{f}} = \frac{1}{2^n}\mathbf{H}_n\hat{\mathbf{f}}$
- 一阶恒等式：$(-1)^{f(0)} = \frac{1}{2^n}\sum_{\alpha\in\mathbb{F}_2^n}\hat{f}(\alpha)$
- 二阶恒等式：$\sum_{\alpha\in\mathbb{F}_2^n}\hat{f}^2(\alpha) = 2^{2n}$
- 保范性：$\sum_{\alpha\in\mathbb{F}_2^n}(\hat{f}(\alpha)-\hat{g}(\alpha))^2 = 2^{n+2}\sum_{x\in\mathbb{F}_2^n}(f(x)-g(x))^2$

问题描述

问题：

- 给出2^n长列向量中m个元素的值，$\{\gamma_{i_j}\}_{0\le i_0<i_1<,,,<i_{m-1}\le 2^n-1}$，其中$m<2^n$
- 要求尽可能多的给出集合$\{f\in\mathfrak{B}_n|\hat{f}(i_j)=\gamma_{i_j},0\le j\le m-1\}$中的元素

其中，数据文件见附件，其中n共有7种：13，14，15，16，17，18和19，并且每个n个取值下都有两份数据。

变元规模(n)	已知谱点数	比例
13	4405	0.538
	4701	0.574
14	7709	0.470
	7986	0.487
15	17609	0.538
	18713	0.571
16	30756	0.469
	31955	0.488
17	55716	0.425
	58991	0.450
18	119757	0.457
	123044	0.469
19	281177	0.536
	363009	0.692

例子：

示例：5元布尔函数 10111110000111010001100001000111 的Walsh谱为

0,4,0,-4,8,4,8,-4,0,-12,0,-4,-8,4,8,-4,-8,-4,0,-4,0,-4,8,-4,-8,-4,0,12,0,-4,-8,-4,

给出16个点的谱值如下：

0,0 3,-4 4,8 7,-4 9,-12 10,0 13,4 14,8 17,-4 18,0 21,-4 22,8 24,-8 27,12 28,0 31,-4

则可以得到如下 64个布尔函数 在上述16个点具有相同的谱值：（布尔函数真值表 16个谱点值 完整Walsh谱）

00101110000000001100110111010111	0,0	3,-4	4,8	7,-4	9,-12	10,0	13,4	14,8	17,-4	18,0	21,-4	22,8	24,-8	27,12	28,0	31,-4
00101110000001011001100111010111	0,0	3,-4	4,8	7,-4	9,-12	10,0	13,4	14,8	17,-4	18,0	21,-4	22,8	24,-8	27,12	28,0	31,-4
00101110000010011001101011010111	0,0	3,-4	4,8	7,-4	9,-12	10,0	13,4	14,8	17,-4	18,0	21,-4	22,8	24,-8	27,12	28,0	31,-4
00101110000011011001100011010111	0,0	3,-4	4,8	7,-4	9,-12	10,0	13,4	14,8	17,-4	18,0	21,-4	22,8	24,-8	27,12	28,0	31,-4
00101110000100010001101111010111	0,0	3,-4	4,8	7,-4	9,-12	10,0	13,4	14,8	17,-4	18,0	21,-4	22,8	24,-8	27,12	28,0	31,-4
00101110000101010001100111010111	0,0	3,-4	4,8	7,-4	9,-12	10,0	13,4	14,8	17,-4	18,0	21,-4	22,8	24,-8	27,12	28,0	31,-4
00101110000110010001101011010111	0,0	3,-4	4,8	7,-4	9,-12	10,0	13,4	14,8	17,-4	18,0	21,-4	22,8	24,-8	27,12	28,0	31,-4
00101110000111010001100011010111	0,0	3,-4	4,8	7,-4	9,-12	10,0	13,4	14,8	17,-4	18,0	21,-4	22,8	24,-8	27,12	28,0	31,-4
00101110100000001100010111010111	0,0	3,-4	4,8	7,-4	9,-12	10,0	13,4	14,8	17,-4	18,0	21,-4	22,8	24,-8	27,12	28,0	31,-4
00101110100001011000100111010111	0,0	3,-4	4,8	7,-4	9,-12	10,0	13,4	14,8	17,-4	18,0	21,-4	22,8	24,-8	27,12	28,0	31,-4
00101110100010011000101011010111	0,0	3,-4	4,8	7,-4	9,-12	10,0	13,4	14,8	17,-4	18,0	21,-4	22,8	24,-8	27,12	28,0	31,-4
00101110100011011000100011010111	0,0	3,-4	4,8	7,-4	9,-12	10,0	13,4	14,8	17,-4	18,0	21,-4	22,8	24,-8	27,12	28,0	31,-4
00101110100100010000101111010111	0,0	3,-4	4,8	7,-4	9,-12	10,0	13,4	14,8	17,-4	18,0	21,-4	22,8	24,-8	27,12	28,0	31,-4
00101110100101010000100111010111	0,0	3,-4	4,8	7,-4	9,-12	10,0	13,4	14,8	17,-4	18,0	21,-4	22,8	24,-8	27,12	28,0	31,-4
00101110100110010000101011010111	0,0	3,-4	4,8	7,-4	9,-12	10,0	13,4	14,8	17,-4	18,0	21,-4	22,8	24,-8	27,12	28,0	31,-4
00101110100111010000100011010111	0,0	3,-4	4,8	7,-4	9,-12	10,0	13,4	14,8	17,-4	18,0	21,-4	22,8	24,-8	27,12	28,0	31,-4
00111110000000001100110111010111	0,0	3,-4	4,8	7,-4	9,-12	10,0	13,4	14,8	17,-4	18,0	21,-4	22,8	24,-8	27,12	28,0	31,-4

成绩评判标准

综合得分：

- 综合得分包括计算得分和理论得分，各占一半
- 计算得分：按照参数选手求得解的排名计算得分
- 理论得分：求解原理、求解步骤和实现效率
- 提交文档：报告和解列表文档，其中解列表文档按照赛题格式命名和存放

理论部分可以思考如下开放性问题：

- 随机选取一个布尔函数和其Waslh谱中的一个谱值，试分析解的个数
- 随机选取一个布尔函数和其Waslh谱中的两个谱值，试分析解的个数
- 随机选取一个布尔函数，试分析解的个数和已知谱点数的关系
- 试分析解集合中各解之间有什么关系

一般的求解方法

遍历$\mathfrak{B}_n$：

- 利用快速Walsh变换求解f的Walsh 谱$\hat{f}$
- 判断$f \in \{f \in \mathfrak{B}_n | \hat{f}(i_j) = \gamma_{i_j}, 0 \leq j \leq m-1\}$?
- 复杂度：$2^{2^n} \times n2^n \times m^2$

解线性方程组:

- 线性方程组包括：2^n个未知数$\{-1,1\}^{2^n}$和m个方程
- 利用高斯消元法求解，计算量为$2^n \times m^2$。(环上的？还是域上的？)

近似计算法:(保范性)

- 将未知谱点值设为0，做逆哈达玛变换，得到近似极性化向量
- 根据近似极性化向量得到近似真值表
- 修改真值表的部分取值，得到满足条件的布尔函数

Thank You.