Problem 4. Column functions

Dung Le Quoc

Ngày 22 tháng 10 năm 2023

1 Problem

Xét 2^n các hàm boolean vector phân biệt và là song ánh $G_i : \mathbb{F}_2^n \to \mathbb{F}_2^n$ với $i = 1, 2, \ldots, 2^n$.

Với $n = 2^m, m \geq 5$ ta định nghĩa ma trận M kích thước $2^n \times n2^n$ như sau.

Hàng thứ i, $i = 1, 2, \ldots, 2^n$, tạo bởi việc nối các giá trị $G_i(0, 0, \ldots, 0, 0)$, $G_i(0, 0, \ldots, 0, 1)$, ..., $G_i(1, 1, \ldots, 1, 1)$.

Mỗi cột của ma trận M có thể xem như một hàm boolean n biến, ta gọi đó là *column function*. Như vậy có $n2^n$ column function theo ma trận M.

Khi $m \geq 5$, giả thuyết đặt ra là, với mọi cách tạo ma trận M như vậy, ta có thể tìm $2^{n/2}$ column function $f_1, f_2, \ldots, f_{2^{n/2}}$ thỏa mãn hai điều kiện sau:

- với mọi vector $\boldsymbol{x} \in \mathbb{F}_2^n$ ta có
$$f(f_1(\boldsymbol{x}), f_2(\boldsymbol{x}), \ldots, f_{2^{n/2}}(\boldsymbol{x})) = 0$$
- với mọi vector $\boldsymbol{y} \in \mathbb{F}_2^{2^{n/2}}$ thì giá trị $f(\boldsymbol{y})$ được tính với không quá $2^{n/2}$ toán tử cộng và nhân modulo 2.

2 Solution

Mình sẽ chứng minh rằng nếu một bộ 2^n các hàm G_i thỏa mãn giả thuyết đề bài thì ta có thể sinh ra các hàm G_i' cũng thỏa mãn hai tính chất trên. Mục tiêu của cách chứng minh này là, với một bộ 2^n ban đầu thỏa mãn, ta sẽ sinh ra tất cả tổ hợp 2^n hàm bất kì trong số $(2^n)!$ song ánh và mỗi tổ hợp đó đều thỏa mãn giả thuyết.

Đầu tiên, với mọi $n = 2^m$, luôn tồn tại 2^n hàm G_i thỏa mãn hai tính chất trên.

Chứng minh. Xét tập các song ánh

$$\begin{aligned}
G_1 &= (0, 1, \ldots, 2^n - 2, 2^n - 1),\\
G_2 &= (1, 2, \ldots, 2^n - 1, 0),\\
G_3 &= (2, 3, \ldots, 0, 1),\\
\cdots &= \cdots,\\
G_{2^n-1} &= (2^n - 2, 2^n - 1, \ldots, 2^n - 4, 2^n - 3),\\
G_{2^n} &= (2^n - 1, 0, \ldots, 2^n - 3, 2^n - 2)
\end{aligned}$$

Theo đó, trong ma trận M, cột 1 là bit đầu của các số $0, 1, 2, \ldots, 2^n - 2, 2^n - 1$, nói cách khác là

$$\underbrace{0, 0, \ldots, 0, 0}_{2^n/2}, \underbrace{1, 1, \ldots, 1, 1}_{2^n/2}$$

Cột thứ $1 + n$ là bit đầu của các số $1, 2, 3, \ldots, 2^n - 1, 0$, nói cách khác là

$$\underbrace{0, 0, \ldots, 0, 0}_{2^n/2-1}, \underbrace{1, 1, \ldots, 1, 1}_{2^n/2}, 0$$

Cột thứ $1 + 2n$ là bit đầu của các số $2, 3, 4, \ldots, 0, 1$, nói cách khác là

$$\underbrace{0, 0, \ldots, 0, 0}_{2^n/2-2}, \underbrace{1, 1, \ldots, 1, 1}_{2^n/2}, 0, 0$$

Cột thứ $1 + (2^n/2)n$ là bit đầu của các số $2^n/2, 2^n/2 + 1, \ldots, 2^n/2 - 2, 2^n/2 - 1$, nói cách khác là

$$\underbrace{1, 1, \ldots, 1, 1}_{2^n/2}, \underbrace{0, 0, \ldots, 0, 0}_{2^n/2}$$

Cột thứ $1 + (2^n/2 + 1)n$ là bit đầu của các số $2^n/2 + 1, 2^n/2 + 2, \ldots, 2^n/2 - 1, 2^n/2$, nói cách khác là

$$\underbrace{1, 1, \ldots, 1, 1}_{2^n/2-1}, \underbrace{0, 0, \ldots, 0, 0}_{2^n/2}, 1$$

Cột thứ $1 + (2^n/2 + 2)n$ là bit đầu của các số $2^n/2 + 2, 2^n/2 + 3, \ldots, 2^n/2, 2^n/2 + 1$, nói cách khác là

$$\underbrace{1, 1, \ldots, 1, 1}_{2^n/2-2}, \underbrace{0, 0, \ldots, 0, 0}_{2^n/2}, 1, 1$$

Theo đó, ta bắt cặp cột 1 và cột $1 + (2^n/2)n$ (các bit của chúng đối nhau), tương tự là cột $1 + n$ với cột $1 + (2^n/2 + 1)n$, cột $1 + 2n$ với cột $1 + (2^n/2 + 2)n$, ..., cột $1 + (2^{n/2} - 1)n$ và cột $1 + (2^n/2 + 2^{n/2} - 1)n$.

Với các cột như vậy ta định nghĩa hàm $f(x_1, \ldots, x_{2^{n/2}}) = x_1 \cdot x_2 \cdots x_n$. Ta thấy rằng x_i luôn là đối của bit $x_{i+2^{n/2}/2}$ nên giá trị hàm f luôn luôn bằng 0. Thêm nữa, do có $2^{n/2}$ hạng tử nên có $2^{n/2} - 1$ phép nhân cần thiết để tính giá trị hàm f.

Như vậy ta đã chứng minh được rằng với mọi n ta luôn chọn được 2^n hàm boolean vector thỏa mãn hai tính chất. □

Tiếp theo, với mỗi đoạn n bit của G_1, ứng với $G_1(0, 0, \ldots, 0, 0)$, $G_1(0, 0, \ldots, 0, 1)$, ..., $G_1(1, 1, \ldots, 1, 0)$ và $G_1(1, 1, \ldots, 1, 1)$, ta sẽ biến đổi theo general linear group. Nghĩa là

$$G_1(\boldsymbol{x}) \to G_1(\boldsymbol{x}) \cdot A \oplus \boldsymbol{b}$$

với A là ma trận thuộc GL (ma trận có định thức bằng 1), và $\boldsymbol{b}$ là vector thuộc $\mathbb{F}_2^n$.

Ở bên trên khi chọn các hàm boolean vector G_i, ta xét các cột 1, 2, ..., $1 + (2^{n/2} - 1)n$, tương ứng (đối bit) là cột $1 + (2^n/2)n$, $1 + (2^n/2 + 1)$, ..., $1 + (2^n/2 + 2^{n/2} - 1)n$. Tương ứng bây giờ ta chỉ cần xem xét bit đầu của $G_1(\boldsymbol{x}) \cdot A \oplus \boldsymbol{b}$ là đủ.

Ta chọn cột 1 và cột $1+(2^n/2)n$ là để các bit đối nhau. Nếu xét cột 1 là bit đầu của vector $\boldsymbol{x} = G_1(0, 0, \ldots, 0, 0) \in \mathbb{F}_2^n$, thì cột $(1 + (2^n/2)n)$ là bit đầu của vector $\boldsymbol{x'} = G_1(0, 0, \ldots, 0, 0) \oplus (1, 0, \ldots, 0, 0) = \boldsymbol{x} \oplus (1, 0, \ldots, 0, 0)$.

Đặt $A = (a_1^T, a_2^T, \ldots, a_n^T)$ với a_i^T là các cột của ma trận A, và $\boldsymbol{b} = (b_1, b_2, \ldots, b_n)$ thì bit đầu sau khi biến đổi $\boldsymbol{x} \cdot A \oplus \boldsymbol{b}$ là $\langle G_1(\boldsymbol{x}), a_1^T \rangle \oplus b_1$.

Tương tự, bit đầu của $\boldsymbol{x'} \cdot A \oplus \boldsymbol{b}$ là $\langle \boldsymbol{x'}, a_1^T \rangle \oplus b_1$.

Ta có

$$\langle \boldsymbol{x'}, a_1^T \rangle \oplus b_1 = \langle \boldsymbol{x} \oplus (1, 0, \ldots, 0, 0), a_1^T \rangle \oplus b_1 = \langle \boldsymbol{x}, a_1^T \rangle \oplus \langle (1, 0, \ldots, 0, 0), a_1^T \rangle \oplus b_1$$

Tương đương với $\langle \boldsymbol{x'}, a_1^T \rangle \oplus \langle \boldsymbol{x}, a_1^T \rangle = \langle (1, 0, \ldots, 0, 0), a_1^T \rangle \oplus b_1$. Gọi a là bit đầu tiên của a_1^T. Như vậy $\boldsymbol{x}$ và $\boldsymbol{x'}$ có bit đầu trái dấu nhau qua tích vô hướng với a_1^T nếu $a = 0, b_1 = 1$ hoặc $a_1 = 1, b_1 = 0$.