

**ПОСТРОЕНИЕ ЛИНЕЙНЫХ
БАЗИСОВ ВЕКТОРНЫХ
ПРОСТРАНСТВ НАД ПОЛЕМ $GF(2)$**

Головашич С.А.

ХНУРЭ

Элементарные отображения:

- фиксированные
- статически управляемые
- динамически управляемые



Реализация линейного отображения

$$\mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$$

$$Y = A \times X, \quad A = \{\alpha_{i,j}\}, \quad \alpha_{i,j} \in \mathbb{F}_2, \quad i = \overline{1,m}, \quad j = \overline{1,n}$$

$$y_i = \bigoplus_{j=1}^n \alpha_{i,j} \wedge x_j, \quad i = \overline{1,m}$$

$$X = (x_1, \dots, x_n) \in \mathbb{F}_2^n, \quad Y = (y_1, \dots, y_m) \in \mathbb{F}_2^m$$

$$Y = \bigoplus_{j=1}^n T_j \wedge Z_j$$

$$T_j = (\alpha_{1,j}, \dots, \alpha_{m,j}) \in \mathbb{F}_2^m, \quad Z_j = (x_j, \dots, x_j) \in \mathbb{F}_2^m$$

Квадратные матрицы порядка n

Общее количество квадратных матриц:

$$N = 2^{n^2}$$

Количество невырожденных матриц:

$$N_{nsm} = \prod_{i=0}^{n-1} (2^n - 2^i)$$

Количества битов, необходимых для определения всех невырожденных матриц:

$$\lceil \log_2 N_{nsm} \rceil = n^2 - 1$$

Свойства невырожденных матриц

1. Всегда существует разложение: $A = P \times L \times U$

2. Свойства
треугольных
матриц:

$$L_i \times L_j \in \{L_k\}, \quad U_i \times U_j \in \{U_k\}$$

$$L_t \times U_r \notin \{L_k\}, \quad L_t \times U_r \notin \{U_k\},$$

$$\text{где } L_t \neq U_r \neq I$$

$$L_i^{-1} \in \{L_k\}, \quad U_i^{-1} \in \{U_k\}$$

3. Частичное
разложение
уникально:

$$L_1 \times U_1 \neq L_2 \times U_2,$$

$$\text{если } L_1 \neq L_2 \text{ и / или } U_1 \neq U_2$$

Алгоритм формирования 2^{n^2-n} различных базисов

1) интерпритировать “управляющую последовательность” как две треугольные матрицы:

$$C = \{c_k\} \rightarrow L = \{l_{i,j}\}, U = \{u_{i,j}\}; \quad i, j = \overline{0, n-1}, k = \overline{0, n^2 - n}$$

$$l_{i,j} = \begin{cases} 0, & \text{для } i < j \\ 1, & \text{для } i = j \\ c_{i \times (n-1) + j}, & \text{для } i > j \end{cases}, \quad u_{i,j} = \begin{cases} c_{i \times (n-1) + j}, & \text{для } i < j \\ 1, & \text{для } i = j \\ 0, & \text{для } i > j \end{cases}$$

2) выполнить умножение
полученных матриц:

$$B = L \times U$$

Выбор линейного базиса из усеченного пространства

Биекция $F_2^n \rightarrow F_2^n$ может быть задана:

$$h(x) \mapsto g(x) \times h(x) \bmod f(x), \quad (g(x), f(x)) = 1$$

Если $(\alpha_0, \dots, \alpha_{n-1})$ – линейный базис над F_2^n ,

то $(\beta_0, \dots, \beta_{n-1})$ – также линейный базис над F_2^n ,

$$\text{где } \beta_i(x) = g(x) \times \alpha_i(x) \bmod f(x), \quad i = \overline{0, n-1}$$

Если $(\alpha_0, \alpha_1, \dots, \alpha_{n-1}) = (x^0, x^1, \dots, x^{n-1})$, то

$$\beta_i(x) = g(x) \times x^i \bmod f(x), \quad i = \overline{0, n-1}$$

Область применения алгоритмов

Алгоритм 1 - приложения статического формирования линейных преобразований.

Сложность (базовый вариант): $n*(n-1)/2$ операций управляемого XOR n разрядных векторов.

Алгоритм 2 - приложения динамического формирования линейных преобразований.

Сложность: n пар операций SHL и управляемого XOR n разрядных векторов.

Для малых n , программная реализация обоих алгоритмов позволяет параллельно формировать несколько базисов.