46 Шифрмашина

Задача. Шифрмашина работает с двоичной лентой, в начале которой записано входное слово длины n, а затем идут нули. Машина зашифровывает входное слово, возвращая результат на его месте. Шифрмашина может выполнять две операции:

1) менять местами любые два символа ленты;

2) применять к первым m символам ленты фиксированную подстановку S.

Ко всем входным словам применяется одна и та же последовательность операций. Эта последовательность (программа шифрмашины) определяется преобразованием зашифрования — биекцией на словах длины n. При каких условиях на S с помощью шифрмашины можно реализовать любую биекцию?

Решение. Необходимо и достаточно, чтобы $S(00\ldots0) \neq 00\ldots0$ и чтобы подстановка S не была аффинной.

Первое условие позволяет получить на ленте единицу. Второе условие означает, что некоторая из координатных функций $f(x_1, x_2, \ldots, x_m)$ подстановки S не является аффинной. Подставляя вместо определенных $m-2$ переменных f определенные значения, можно сузить f до произведения $x_i x_j$. Подобным образом можно получить и сумму $x_i + x_j$.

С учетом возможности перестановки символов ленты, в качестве x_i, x_j могут выступать любые входные переменные. Таким образом, шифрмашина может вычислять любые полиномиальные выражения от входов и, следовательно, реализовывать любые биекции. □