



Problem 8. «Bijections for ciphers»

A mapping $F : \{0, 1\}^n \rightarrow \{0, 1\}^n$, $F = (f_1, \dots, f_n)$, is such that all coordinate Boolean functions f_i , $i = 1, \dots, n$, depend on k variables, $k \leq n$. Each function f_i is defined as follows: by a Boolean function g_i in k variables and an integer vector m_i of length k , containing the indices of the essential variables.

Example: Let $n = 3$, $k = 2$, $g_1 = g_2 = g_3 = x_1x_2$, $m_1 = (2, 3)$, $m_2 = (1, 3)$, $m_3 = (1, 2)$; then $f_1 = x_2x_3$, $f_2 = x_1x_3$, $f_3 = x_1x_2$, and the mapping F is given by the table:

x_1	x_2	x_3	F
0	0	0	000
0	0	1	000
0	1	0	000
0	1	1	100
1	0	0	000
1	0	1	010
1	1	0	001
1	1	1	111

A problem. Formulate conditions (necessary; sufficient; both) on the functions g_i and vectors m_i under which the mapping F is a bijection (an one-to-one function).

A requirement: It should be not necessary to construct the truth table for F while checking the conditions.

