Xor Problem

Semchankau Aliaksei (Neodym)
Moscow Institute of Physics and Technology

December 20, 2015

1 Problem

I've been asked by this question lots of times, so I'm going to give an explicite answer on it. Formal statement of problem: set of n numbers $x_1, x_2, ..., x_n$ and number x is given, how many subsets $y_1, ..., y_m$ of this set exist, such that $y_1 \oplus y_2 \oplus ... \oplus y_m = x$?

2 Solution

As we know, $x \oplus 0 = x$, that's why we can reformulate problem as follows: how many sets $a_1, a_2, ..., a_n$ (each a_i is either 0 or 1) exist, such that $a_1x_1 \oplus a_2x_2 \oplus ... \oplus a_nx_n = x$?

Let's rewrite every x_i and x as binary vectors (each integer has binary representation). Problem will go like this:

$$\begin{pmatrix} a_1x_{1,1} \\ a_1x_{1,2} \\ ... \\ a_1x_{1,32} \end{pmatrix} + \begin{pmatrix} a_2x_{2,1} \\ a_2x_{2,2} \\ ... \\ a_2x_{2,32} \end{pmatrix} + ... + \begin{pmatrix} a_nx_{n,1} \\ a_nx_{n,2} \\ ... \\ a_nx_{n,32} \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ ... \\ x_{32} \end{pmatrix}$$

So, now our problem rewrited as system of equations, where $x_{i,j}$ and x_i are known, but a_i are variables:

$$\begin{cases} a_1x_{1,1} + a_2x_{2,1} + ... + a_nx_{n,1} = x1 \\ a_1x_{1,2} + a_2x_{2,2} + ... + a_nx_{n,2} = x2 \\ ... \\ a_1x_{1,32} + a_2x_{2,32} + ... + a_nx_{n,32} = x32 \end{cases}$$

It can be written in terms of matrix multiplication (google it, if you don't know this term) like this:

$$\begin{pmatrix} x_{1,1} & x_{2,1} & ... & x_{n,1} \\ x_{1,2} & x_{2,2} & ... & x_{n,2} \\ ... & .... & .... & ... \\ x_{1,32} & x_{2,32} & ... & x_{n,32} \end{pmatrix} \times \begin{pmatrix} a_1 \\ a_2 \\ ... \\ a_{32} \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ ... \\ x_{32} \end{pmatrix}$$

Of course, we make all calculations modulo 2 ($1 + 1 = 0$) One can see, that this system is equivalent to system:

$$\begin{pmatrix} x_{1,1} & x_{2,1} & ... & x_{n,1} \\ x_{1,2} - x_{1,1} & x_{2,2} - x_{2,1} & ... & x_{n,2} - x_{n,1} \\ ... & ... & ... & ... \\ x_{1,32} & x_{2,32} & ... & x_{n,32} \end{pmatrix} \times \begin{pmatrix} a_1 \\ a_2 \\ ... \\ a_{32} \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 - x1 \\ ... \\ x_{32} \end{pmatrix}$$

Also, it's equivalent to system:

$$\begin{pmatrix} x_{1,2} & x_{2,2} & ... & x_{n,2} \\ x_{1,1} & x_{2,1} & ... & x_{n,1} \\ ... & ... & ... & ... \\ x_{1,32} & x_{2,32} & ... & x_{n,32} \end{pmatrix} \times \begin{pmatrix} a_1 \\ a_2 \\ ... \\ a_{32} \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 \\ ... \\ x_{32} \end{pmatrix}$$

So, we can make linear transformations with rows of this matrix (substruct one row from another row, and switch rows). After that we use Gaussian algorithm (you can google it too): it means, that we're trying to make all cells placed under main diagonal of matrix be filled by zeros.

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

Lets make transformations with first matrix:

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \rightarrow$$

switch first and second row:

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \rightarrow$$

subtract first row from third row:

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \rightarrow$$

first column is fine at this moment. Let's fill second column with zeroes. Subtract second row from first row:

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \rightarrow$$

subtract second row from third row:

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \rightarrow$$

rank of matrix is a number of cells on main diagonal, which remained filled by 1's after Gaussian algorithm (it can be proved, that rank does not depend on algorithm you used). In this problem, rank is equal 2. Actually, our system of equations looks like this now:

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$$

or: $\begin{cases} b_1 + b_3 = y_1 \\ b_2 + b_3 = y_2 \\ 0 = y_3 \end{cases}$

if y_3 is not equal 0, than system is clearly unsolvable, and problem has no solution (number of subsets is equal 0). Otherwise, we get, that b_3 is independent variable (because third cell on main diagonal of matrix is filled with zero), but b_1 and b_2 are dependent variables — $b_1 = y_1 - b_3, b_2 = y_2 - b_3$.

Actually, it follows, that count of independent variables is $n - rank$, where n is number of variables (in our case it means number of columns). Obviously, number of solutions for system of equations is equal to number of ways to fill independent variables with 0 and 1, so, the answer for problem is 2^{n-rank}, q.e.d.