Vectors in $\mathbb{Z}_2^d$

Benjamin Qi

USACO Camp

May 2020

Table of Contents

Number Theory

To write a non-negative integer in **base two** is to write it as a sum of distinct non-negative powers of 2.

Example

Write 13 in base 2.

$$\begin{aligned} 13 &= 8 + 4 + 1 \\ &= 2^3 + 2^2 + 2^0 \\ &= \boxed{1101_2.} \end{aligned}$$

To write a non-negative integer in **base two** is to write it as a sum of distinct non-negative powers of 2.

Example

Write 13 in base 2.

$$\begin{aligned} 13 &= 8 + 4 + 1 \\ &= 2^3 + 2^2 + 2^0 \\ &= \boxed{1101_2.} \end{aligned}$$

Two numbers a and b are **congruent** or **equivalent** modulo k if they have the same remainder when divided by k. This is denoted by $a \equiv b \pmod{k}$. In this presentation, we'll focus on $k = 2$.

XOR

Exclusive-Or (XOR)

For two non-negative integers a and b, the operation a XOR b can be performed as follows:

- Convert both a and b to base 2.
- Add each pair of bits $\pmod 2$.
- Convert the resulting base 2 number back to base 10.

If we denote XOR by $\oplus$, then

$$0 \oplus 0 = 1 \oplus 1 = 0,$$

$$1 \oplus 0 = 0 \oplus 1 = 1.$$

(The OR operation is defined similarly, except 1 OR $1 = 1$.)

XOR

Example

Calculate $5 \oplus 7$. (Express the answer in base 10.)

This is equivalent to

$$\begin{array}{r} (101)_2 \\ \oplus\ (111)_2 \\ \hline (010)_2 \end{array},$$

which is equal to $\boxed{2}$ in base 10.

Another XOR example

Example

Calculate $13 \oplus 25$.

This is equivalent to

$$\begin{array}{r} (01101)_2 \\ \oplus\ (11001)_2 \\ \hline (10100)_2 \end{array},$$

which is equal to $\boxed{20}$ in base 10.

Scalars

Scalars

Scalars are elements of fields, where addition, subtraction, multiplication, division must be defined (ex. rationals, reals).

Scalars

Scalars are elements of fields, where addition, subtraction, multiplication, division must be defined (ex. rationals, reals).

- The integers ($\mathbb{Z}$) do not form a field since the inverses of any nonzero integer aside from -1 and 1 are not integers. For example, the inverse of 2 is $\frac{1}{2}$, which is not an integer.
- However, the integers modulo any prime p do form a field ($\mathbb{Z}_p$) since we can compute modular inverses. For example, the inverse of 2 modulo 7 is 4 since $2 \cdot 4 \equiv 1 \pmod 7$.

Vector Spaces

Vector Space

A **vector space** is a set V on which two operations $+$ and $\cdot$ are defined, called vector addition and scalar multiplication. The elements of V are called **vectors**.

Vector Spaces

Vector Space

A **vector space** is a set V on which two operations $+$ and $\cdot$ are defined, called vector addition and scalar multiplication. The elements of V are called **vectors**.

V must be closed under both of these operations, meaning that $x, y \in V \implies x + y \in V$ and $x \in V \implies c \cdot x \in V$ for any scalar c. Addition should be both associative and commutative while scalar multiplication should be associative and distributive over addition.

Vector Space Examples

Wikipedia

Addition and scalar multiplication are well defined for all of these examples.

- Coordinate spaces
  - Tuples of numbers $(x_1, x_2, \ldots, x_n)$ and scalars c such that $x_i, c \in \mathbb{R}$
  - Component-wise addition and multiplication:

$$(x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n)$$

$$c(x_1, x_2, \ldots, x_n) = (cx_1, cx_2, \ldots, cx_n)$$

  - Also works for any other field (ex. $\mathbb{Z}_2$ instead of $\mathbb{R}$)
- Matrices over some field
- Polynomial vector spaces
  - Operations with vector space of polynomials with real coefficients and degree less than or equal to n: $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ (though the degree doesn't have to be restricted)
- Function spaces
  - Given functions $f(x)$ and $g(x)$ from any set to some field, we can define $(f + g)(x)$ and $(cf)(x)$.

$\mathbb{Z}_2^d$

This is a vector space defined as follows:

- $V = \{0, 1, \ldots, 2^d - 1\}$. Each number stands for an array of d bits.

$\mathbb{Z}_2^d$

This is a vector space defined as follows:

- $V = \{0, 1, \ldots, 2^d - 1\}$. Each number stands for an array of d bits.
- If $x, y \in V$, then $x + y$ is defined to be $x \oplus y$. Note that $x + y \in V$ is satisfied.

$\mathbb{Z}_2^d$

This is a vector space defined as follows:

- $V = \{0, 1, \ldots, 2^d - 1\}$. Each number stands for an array of d bits.
- If $x, y \in V$, then $x + y$ is defined to be $x \oplus y$. Note that $x + y \in V$ is satisfied.
- For any $c \in \mathbb{Z}_2$, let $cx = \overbrace{x + x + \ldots x}^{c \text{ occurences of } x}$. So $cx = 0$ if c is even and $cx = x$ if c is odd.

$\mathbb{Z}_2^d$ is indeed closed under both addition and scalar multiplication.

Span

From now on, we'll do all calculations $\pmod 2$ and substitute $+$ in place of $\oplus$.

Span

From now on, we'll do all calculations $\pmod 2$ and substitute $+$ in place of $\oplus$.

Span

The vector space V **spanned** by a collection of vectors $v_1, v_2, \ldots, v_n$ consists of all vectors x that can be written as a **linear combination** of $v_1, v_2, \ldots, v_n$. In other words, $x = \sum_{i=1}^{n} c_i v_i$ for some choice of scalars $c_i \in \{0, 1\}$.

Span

From now on, we'll do all calculations $\pmod 2$ and substitute $+$ in place of $\oplus$.

Span

The vector space V **spanned** by a collection of vectors $v_1, v_2, \ldots, v_n$ consists of all vectors x that can be written as a **linear combination** of $v_1, v_2, \ldots, v_n$. In other words, $x = \sum_{i=1}^{n} c_i v_i$ for some choice of scalars $c_i \in \{0, 1\}$.

Example

What are $\text{span}(\{3, 5\}), \text{span}(\{3, 5, 6\})$, and $\text{span}(\{\})$?

Answer: Note that $3 \oplus 5 = 6$.

$$\text{span}(\{3, 5\}) = \text{span}(\{3, 5, 6\}) = \{0, 3, 5, 6\}.$$

$$\text{span}(\{\}) = \{0\}.$$

Span

Useful properties:

Firstly, $v_{m+1} \in \text{span}(\{v_1, \ldots, v_m\})$ implies

$$\text{span}(\{v_1, \ldots, v_m, v_{m+1}\}) = \text{span}(\{v_1, \ldots, v_m\}).$$

Span

Useful properties:

Firstly, $v_{m+1} \in \text{span}(\{v_1, \ldots, v_m\})$ implies

$$\text{span}(\{v_1, \ldots, v_m, v_{m+1}\}) = \text{span}(\{v_1, \ldots, v_m\}).$$

Secondly,

$$\text{span}(\{v_1, v_2, \ldots, v_m\}) = \text{span}(\{v_1, v_1 + v_2, \ldots, v_m\}).$$

Basis

Basis

A collection of vectors $v_1, \ldots, v_n$ is a **basis** for a vector space V if $\text{span}(\{v_1, \ldots, v_n\}) = V$ and no nontrivial linear combination of $v_1, \ldots, v_n$ sums to 0 (nontrivial means that you ignore $\sum_{i=1}^{n} 0 \cdot v_i$, which is obviously 0). n is called the **dimension** or **rank** of V (and is the same regardless of the basis chosen, see here). This is denoted by $\dim(V)$ or $\text{rank}(V)$.

Note that 0 should never be in the basis.

Example

If $V = \{0, 3, 5, 6\}$ then $\{3, 5\}$ is a basis for V, but $\{3, 5, 6\}$ is not because $3 + 5 + 6 = 3 \oplus 5 \oplus 6 = 0$. Of course, $\{3, 6\}$ and $\{5, 6\}$ are also bases for V.

Basis

Example

In terms of n, how many distinct elements are contained within $\text{span}(\{v_1, \ldots, v_n\})$, if $v_1, \ldots, v_n$ form a basis?

Recall that $\text{span}(\{3, 5\}) = \{0, 3, 5, 6\}$.

Basis

Example

In terms of n, how many distinct elements are contained within $\text{span}(\{v_1, \ldots, v_n\})$, if $v_1, \ldots, v_n$ form a basis?

Recall that $\text{span}(\{3,5\}) = \{0,3,5,6\}$.

Answer: If any x could be written as a linear combination of $\{v_1, v_2, \ldots, v_n\}$ in more than one of the 2^n possible ways, this would contradict the definition of basis. It follows that $|V| = \boxed{2^n.}$

Matrices

Consider any $n \times m$ matrix (n rows, m columns)

$$M = \begin{bmatrix} | & | & \cdots & | \\ v_1 & v_2 & \cdots & v_m \\ | & | & \cdots & | \end{bmatrix}.$$

The v_i are each **column vectors** of dimension n. This represents a **linear transformation** from a vector space of dimension m to a vector space of dimension n.

Matrices

Consider any $n \times m$ matrix (n rows, m columns)

$$M = \begin{bmatrix} | & | & \cdots & | \\ v_1 & v_2 & \cdots & v_m \\ | & | & \cdots & | \end{bmatrix}.$$

The v_i are each **column vectors** of dimension n. This represents a **linear transformation** from a vector space of dimension m to a vector space of dimension n.

So for any column vector x of dimension m,

$$M \cdot x = \sum_{i=1}^{m} v_i x_i$$

is a column vector of dimension n that is a linear combination of the columns of M.

Dimension

Dimension

The **column dimension** of M is equal to

$$\operatorname{cdim}(M) = \dim(\operatorname{span}(\{v_1, v_2, \ldots, v_m\})).$$

Recall that this is the number of linearly independent columns. The **row dimension** can be defined similarly.

Dimension

The **column dimension** of M is equal to

$$\text{cdim}(M) = \dim(\text{span}(\{v_1, v_2, \ldots, v_m\})).$$

Recall that this is the number of linearly independent columns. The **row dimension** can be defined similarly.

Since it can be shown that $\text{cdim}(M) = \text{rdim}(M)$, we can use $\dim(M)$ to refer to both $\text{cdim}(M)$ and $\text{rdim}(M)$. As with vector spaces, this can also be denoted by $\text{rank}(M)$.

Link to Explanations (Optional)

Nullity

Null Space

The **null space** of a matrix M is the set that consists of all column vectors v such that

$$M \cdot v = 0.$$

Note that this set is actually a vector space since

$$M \cdot a = M \cdot b = 0 \implies M \cdot (a + b) = 0$$

$$M \cdot (ca) = c(M \cdot a) = 0$$

The **nullity** of matrix M is the dimension of this set.

Rank-Nullity Theorem

The Rank-Nullity Theorem states that for an $n \times m$ matrix M,

$$\mathrm{rank}(M) + \mathrm{null}(M) = m.$$

For example,

$$\mathrm{rank}\left(\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\right) = 2, \mathrm{null}\left(\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\right) = 0$$

$$\mathrm{rank}\left(\begin{bmatrix}1 & 0 & 0\\0 & 0 & 0\end{bmatrix}\right) = 1, \mathrm{null}\left(\begin{bmatrix}1 & 0 & 0\\0 & 0 & 0\end{bmatrix}\right) = 2$$

We won't prove this (it would require the introduction of additional notation), but you should at least intuitively understand why this is true in the context of linear transformations.

Table of Contents

Programming Note

For all of the following problems, we'll assume that integer values are in the range $[0, 2^{60})$ unless otherwise stated (so that they fit into a `long long`).

XOR Closure

Example

You are given a set of N $(1 \leq N \leq 10^5)$ distinct integer values $x_1, x_2, \ldots, x_N$. Find the minimum number of values that you need to add to the set such that the following will hold true:
For every two integers A and B in the set, $A \oplus B$ is also in the set.

csacademy.com/contest/archive/task/xor-closure/

Extension: Compute the answer for each prefix of $x_1, \ldots, x_N$.

Thoughts?

XOR Closure

Example

You are given a set of N ($1 \leq N \leq 10^5$) distinct integer values $x_1, x_2, \ldots, x_N$. Find the minimum number of values that you need to add to the set such that the following will hold true:
For every two integers A and B in the set, $A \oplus B$ is also in the set.

csacademy.com/contest/archive/task/xor-closure/

Extension: Compute the answer for each prefix of $x_1, \ldots, x_N$.

Thoughts?

Solution: Let $X = \{x_1, x_2, \ldots, x_N\}$. We need to compute $\dim(\text{span}(X))$. Then the answer will be $2^{\dim(\text{span}(X))} - N$.

XOR Closure

It suffices to add the integers of X one by one.

- If $x_{i+1} \in \text{span}(x_1, x_2, \ldots, x_i)$, then adding it will leave the span unchanged.
- Otherwise, the size of the basis increases by one (and the number of elements in the span of the basis is multiplied by two).

XOR Closure

It suffices to add the integers of X one by one.

- If $x_{i+1} \in \text{span}(x_1, x_2, \ldots, x_i)$, then adding it will leave the span unchanged.
- Otherwise, the size of the basis increases by one (and the number of elements in the span of the basis is multiplied by two).

Question 1

How can you quickly test whether $x_{i+1} \in \text{span}(x_1, \ldots, x_i)$? Obviously, going through all 2^i possible linear combinations of $x_1, \ldots, x_i$ is not sufficient.

XOR Closure

For a positive integer x, let $msb(x)$ be the index of the **m**ost **s**ignificant **b**it in x (one less than the length of x when written in base 2).

Example

$$msb(4) = msb(7) = 2$$

$$msb(3) = 1, msb(1) = 0$$

XOR Closure

For a positive integer x, let $msb(x)$ be the index of the **m**ost **s**ignificant **b**it in x (one less than the length of x when written in base 2).

Example

$$msb(4) = msb(7) = 2$$

$$msb(3) = 1, msb(1) = 0$$

Easier Version: Suppose that we have a basis $\{v_1, v_2, \ldots, v_n\}$ of $x_1, x_2, \ldots, x_i$ such that $msb(v_1) > msb(v_2) > \cdots > msb(v_n)$. Can you easily test whether a vector a is in $\text{span}(\{v_1, \ldots, v_n\})$?

XOR Closure

Example

Is it true that $20 \in \text{span}(\{26, 15, 3, 1\})$?

$$
\begin{aligned}
26 &= 11010_2 \\
15 &= 01111_2 \\
3 &= 00011_2 \\
1 &= 00001_2 \\
20 &= 10100_2
\end{aligned}
$$

XOR Closure

Example

Is it true that $20 \in \text{span}(\{26, 15, 3, 1\})$?

$$\begin{aligned} 26 &= 11010_2 \\ 15 &= 01111_2 \\ 3 &= 00011_2 \\ 1 &= 00001_2 \\ 20 &= 10100_2 \end{aligned}$$

Can verify that $20 = 26 \oplus 15 \oplus 1$.

XOR Closure

Example

Is it true that $20 \in \text{span}(\{26, 15, 3, 1\})$?

$$\begin{aligned} 26 &= 11010_2 \\ 15 &= 01111_2 \\ 3 &= 00011_2 \\ 1 &= 00001_2 \\ 20 &= 10100_2 \end{aligned}$$

Can verify that $20 = 26 \oplus 15 \oplus 1$.

XOR Closure

Solution: Let $A = a$. Iterate over all i from $1 \ldots n$. If $A + v_i < A$, replace A with $A + v_i$. If $A = 0$ at the end of this process, then $a \in \text{span}(\{v_1, \ldots, v_n\})$.

Note

More generally, this allows us compute the minimum value of $a + v$ over all $v \in \text{span}(\{v_1, \ldots, v_n\})$.

XOR Closure

Example

Is it true that $9 \in \text{span}(\{26, 15, 3, 1\})$?

$$\begin{aligned} 26 &= 11010_2 \\ 15 &= 01111_2 \\ 3 &= 00011_2 \\ 1 &= 00001_2 \\ 9 &= 01001_2 \end{aligned}$$

XOR Closure

Example

Is it true that $9 \in \text{span}(\{26, 15, 3, 1\})$?

$$\begin{aligned} 26 &= 11010_2 \\ 15 &= 01111_2 \\ 3 &= 00011_2 \\ 1 &= 00001_2 \\ 9 &= 01001_2 \end{aligned}$$

The minimum possible XOR of 9 with some subset is

$$9 \oplus 15 \oplus 3 \oplus 1 = 4 = 100_2.$$

Example

Is it true that $9 \in \text{span}(\{26, 15, 3, 1\})$?

If we add it to the basis and maintain the sorted order, then it looks like this:

$$
\begin{aligned}
26 &= 11010_2 \\
15 &= 01111_2 \\
4 &= 00100_2 \\
3 &= 00011_2 \\
1 &= 00001_2
\end{aligned}
$$

The most significant bits are still in decreasing order!

XOR Closure

Recap:

Go through all elements $a \in X$ in any order. For each a, calculate A, which is the minimum value of $a + v$ over all v in the span of the elements that precede a.

XOR Closure

Recap:

Go through all elements $a \in X$ in any order. For each a, calculate A, which is the minimum value of $a + v$ over all v in the span of the elements that precede a.

- If a is already in the span of the elements that precede it, then $A = 0$, continue.
- Otherwise, add A to the basis while maintaining the decreasing msb condition. This is how **Gaussian elimination** is used to convert a matrix into **row echelon form** (meaning that as you go down the rows, the leftmost one always moves to the right).

XOR Closure

C++ Code:

```
typedef long long ll; // represents ints in [0,2^{60})
vector<ll> basis; // list of basis elements, initially empty
for (ll a: X) { // go through elements in any order
    ll A = a;
    for (ll b: basis) A = min(A,A^b);
    if (A) { // add A to basis
        int ind = 0;
        while (ind < basis.size()
            && basis[ind] > A) ind ++;
        basis.insert(begin(basis)+ind,A);
        // preserve decreasing property
    }
}
```

Example (Again)

Example

Is it true that $9 \in \text{span}(\{26, 15, 3, 1\})$?

- Let $a = A = 9$.
- $A \oplus 26 = 19 > A$, A doesn't change.
- $A \oplus 15 = 6 < A$, set $A = 6$.
- $A \oplus 3 = 5 < A$, set $A = 5$.
- $A \oplus 1 = 4 < A$, set $A = 4$.

Then we can insert A into the basis, making it $\{26, 15, 4, 3, 1\}$.

Power Grid

Hopefully, the next few problems should be easier now that we've worked through one. If you're confused, please let me know.

Power Grid

Hopefully, the next few problems should be easier now that we've worked through one. If you're confused, please let me know.

Example

A power grid consists of stations labelled $0 \ldots 2^K - 1$. You are given a list of integers $X = \{x_1, \ldots, x_M\}$ such that an edge connects stations i and j iff $i \oplus j \in X$. Compute the number of connected components in this graph.
www.codechef.com/COOK106A/problems/XORCMPNT

Power Grid

Hopefully, the next few problems should be easier now that we've worked through one. If you're confused, please let me know.

Example

A power grid consists of stations labelled $0 \ldots 2^K - 1$. You are given a list of integers $X = \{x_1, \ldots, x_M\}$ such that an edge connects stations i and j iff $i \oplus j \in X$. Compute the number of connected components in this graph.
www.codechef.com/COOK106A/problems/XORCMPNT

Hint: The answer depends only on K and $\dim(X)$.

Hopefully, the next few problems should be easier now that we've worked through one. If you're confused, please let me know.

Example

A power grid consists of stations labelled $0 \ldots 2^K - 1$. You are given a list of integers $X = \{x_1, \ldots, x_M\}$ such that an edge connects stations i and j iff $i \oplus j \in X$. Compute the number of connected components in this graph.
www.codechef.com/COOK106A/problems/XORCMPNT

Hint: The answer depends only on K and $\dim(X)$.

Solution: Every power station is in the same connected component as $2^{\dim(X)}$ others. The answer will be $\frac{2^K}{2^{\dim(X)}} = 2^{K-\dim(X)}$.

Square Subsets

Example

Given an array a ($|a| \leq 10^5$) find the number of different ways to select a non-empty subset of elements from it in such a way that their product is equal to a square of some integer. Two ways are considered different if sets of indexes of elements chosen by these ways are different. All elements of a are in the range $[1, 70]$.
Since the answer can be very large, you should find the answer modulo $10^9 + 7$.

codeforces.com/contest/895/problem/C

Square Subsets

Example

Given an array a ($|a| \leq 10^5$) find the number of different ways to select a non-empty subset of elements from it in such a way that their product is equal to a square of some integer. Two ways are considered different if sets of indexes of elements chosen by these ways are different. All elements of a are in the range $[1, 70]$.
Since the answer can be very large, you should find the answer modulo $10^9 + 7$.

codeforces.com/contest/895/problem/C

Solution: For each number in a, we only need to consider the primes that divide it an odd number of times. Since there are only 19 primes in $[1, 70]$, each number corresponds to a vector in $\mathbb{Z}_2^{19}$ and multiplying two numbers corresponds to an xor operation. A square corresponds to the 0 vector.

Square Subsets

The process of choosing a subset can be represented by the following linear transformation:

$$f(v) = f(v_1, v_2, \ldots, v_{|a|}) = \bigoplus_{i=1}^{|a|} (v_i \cdot a_i),$$

where $v_i = 1$ if a_i is included in the subset and $v_i = 0$ otherwise. This can be represented by a $19 \times |a|$ matrix:

$$f(v) = \begin{bmatrix} a_{1,0} & a_{2,0} & \cdots & a_{|a|,0} \\ a_{1,1} & a_{2,1} & \cdots & a_{|a|,1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1,18} & a_{2,18} & \cdots & a_{|a|,18} \end{bmatrix} \cdot \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_{|a|} \end{bmatrix}$$

Our goal is to find the number of nontrivial elements in the null space of this matrix (so 2 to the power of the nullity minus one).

Square Subsets

Let $b = \text{basis}(a)$, which we can compute in the same way as the previous problem. Then $|b|$ is the rank of f.

Square Subsets

Let $b = \text{basis}(a)$, which we can compute in the same way as the previous problem. Then $|b|$ is the rank of f.

By the rank-nullity theorem, $|a| - |b|$ is the nullity of f, which is exactly what we want! Specifically, each of the $2^{|b|}$ elements of $\text{span}(a)$ (including 0) are attained by $2^{|a|-|b|}$ values of v.

Example

Given $a = \{3, 5\}$, $|a| - |b| = 0$, and each of $0, 3, 5, 6$ can be written as a distinct linear combination of elements in a.
Given $a = \{3, 5, 6\}$, $|a| - |b| = 1$, and each of $0, 3, 5, 6$ can be written as two different linear combinations of elements in a.

Let $b = \text{basis}(a)$, which we can compute in the same way as the previous problem. Then $|b|$ is the rank of f.

By the rank-nullity theorem, $|a| - |b|$ is the nullity of f, which is exactly what we want! Specifically, each of the $2^{|b|}$ elements of span(a) (including 0) are attained by $2^{|a|-|b|}$ values of v.

Example

Given $a = \{3, 5\}$, $|a| - |b| = 0$, and each of $0, 3, 5, 6$ can be written as a distinct linear combination of elements in a.
Given $a = \{3, 5, 6\}$, $|a| - |b| = 1$, and each of $0, 3, 5, 6$ can be written as two different linear combinations of elements in a.

Recap: The answer is $2^{|a|-|b|} - 1$, where one is subtracted for the empty set. Of course, slower solutions involving factors such as $70 \cdot 2^{19}$ also work due to the low constraints.

Table of Contents

Conclusion

These slides will be posted here:

sites.google.com/view/phsmathteam/resources/materials

Hope you learned something interesting!

CF Blog about XOR: codeforces.com/blog/entry/68953

(used for some of the initial definitions)