SUMMER CAMP 2015 TRAINING: VECTOR SPACES OVER $\mathbb{Z}/2\mathbb{Z}$

1. Definitions and Examples

Let's jump right in! Suppose V is some set with a binary operation which we're gonna write as $+$. We say V is a *vector space over* $\mathbb{Z}/2\mathbb{Z}$ if the following conditions hold:

(1) There is a zero element in V. That is, there is an element of V - which we shall always write as 0 - such that for all other $v \in V$, we have $0 + v = v + 0 = v$.
(2) The operation is commutative. That is, $a + b = b + a$ for any a, b in V.
(3) The operation is associative. That is, $a + (b + c) = (a + b) + c$ For any a, b, c in V.
(4) Doubling yields 0. That is, $a + a = 0$ for every a in V.

Basically, the conditions are that addition works like you expect, and also that twice an element always gives 0. Here are a bunch of examples:

(1) The simplest example is $V = \mathbb{Z}/2\mathbb{Z}$, with the usual addition!
(2) More generally, for any positive integer n, we can write $V = \mathbb{Z}/2\mathbb{Z}^n$. Specifically, V consists of strings $(a_1, \ldots, a_n)$ where each a_i is an element of $\mathbb{Z}frm{-}e\mathbb{Z}$ and addition is done entry by entry. That is, $(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$. The zero element is the string $(0, 0, \ldots, 0)$. As we shall see a bit later, this is basically the most general example.
(3) Let n be a positive integer. We can take V to be the powerset of $\{1, 2, \ldots, n\}$. That is, the set of all such subsets, where addition is defined via the XOR operation. That is,

$$A + B = (A \backslash A \cap B) \cup (B \backslash A \cap B).$$

Prove to yourself that this defines a vector space over $\mathbb{Z}/2\mathbb{Z}$, with the empty set as the zero element!

2. Bases and Linear independence

We say that a subset $\{v_1, \ldots, v_m\}$ of V is *linearly independent* if no non-empty subset of them adds to 0. We say that $\{v_1, \ldots, v_m\}$ is a *basis* if it is a maximal linearly independent set. The following lemma is extremely useful:

Theorem 2.1. *Let V be a finite vector space, and suppose that $B = \{v_1, \ldots, v_n\}$ is a basis. Then every element of V can be written as a unique way as a sum of distinct elements of B. In particular, $|V| = 2^n$, and thus all bases have the same size. Finally, a set $C = \{w_1, \ldots, w_n\}$ is a basis of V if every vector in V can be written as a sum of elements of C.*

Proof. Let w be an element of V. If $w \in B$ then w can clearly be written as $w = v_1$, so suppose this is not the case. Now, $\{w, v_1, \ldots, v_n\}$ cannot be linearly independent since $\{v_1, \ldots, v_n\}$ is a maximal linearly independent set by definition. Thus, there is a non-empty subset C of $\{w, v_1, \ldots, v_n\}$ that sums to 0. Now, C must contain w, or else we would have $C \subset B$ and this is a contradiction. So we can write $0 = w + \sum_{i \in I} v_i$ for some set I. However, adding w to both sides gives $w = \sum_{i \in I} v_i$, and so every element of V can be written as a sum of distinct elements of V.

To prove uniqueness, suppose that I, J are distinct subsets of B such that

$$\sum_{i \in I} v_i = w = \sum_{i \in J} v_j.$$

Adding $\sum_{i \in I} v_i$ to both sides, we see that $0 = \sum_{k \in \mathrm{XOR}(I,J)} v_k$. Since I and J are distinct, this contradicts the fact that B is a linearly independent sets.

For the last claim, we have already shown that if C is a basis then every element can be written as a sum of elements of C. For the opposite claim, note that there are 2^n subsets of C, and 2^n elements of V, and thus each element has a unique representation as a sum of elements of C. Thus, there can be no non-empty subset of C which sums to 0, and so C is a linearly independent set, and hence a basis since it has n elements.

□

The number n in the theorem is called the *dimension* of V. As a corollary, it follows that for each positive integer n, there is a 'unique' vector space of size 2^n. Moreover, all non-zero vectors 'look the same' inside this vector space! In fact, we prove the following stronger fact:

Corollary 2.2. *Let V, W be vector spaces over $\mathbb{Z}/2\mathbb{Z}$ of size 2^n with bases $B = \{v_1, \ldots, v_n\}$ and $C = \{w_1, \ldots, w_n\}$ respectively. Then there is a bijection $\phi : V \to W$ such that for all $a, b \in V$ we have $\phi(a + b) = \phi(a) + \phi(b)$, and $\phi(v_i) = w_i$ for $1 \leq i \leq n$. In other words, V with basis B looks exactly like W with basis C.*

Proof. We define ϕ as follows. By Theorem 2.1, for each element $v \in V$, we can write $v = \sum_{i \in I} v_i$ for a unique subset I of $\{1, 2, \ldots, n\}$. We define $\phi(w) = \sum_{i \in I} w_i$. We leave it as an exercise to prove that ϕ has the required properties.

□

This corollary an conceptually be very helpful, as you can be sure that there is nothing special about a particular vector space, or even a particular

choice of vector. They all look exactly the same! We give an example problem that can be done with vector spaces.:

Example Problem: Let G be a finite directed graph. Each vertex of G may be colored either white or black. Initially all vertices are colored white. We may preform the operation of picking a vertex v of G and flipping the color of all vertices w such that there is an edge from v to w. Prove that the following are equivalent:

(1) Through a sequence of operations, we may achieve any possible coloring of G.
(2) There is no non-empty subset S of vertices of G, such that applying our operation to each element of S keeps every vertex colored white.

Proof. We define a vector space V over $\mathbb{Z}/2\mathbb{Z}$ as follows: the elements of V are the subsets of the vertices of G, with the XOR operation being addition. Now, to each possible coloring of G, we may associate an element of V by taking the set of black vertices. Moreover, for each vertex v of g, we may define an element e_v of V by taking the subset of all vertices w of G such that there is an edge from v to w.

Now that we have this setup, we can see that applying our operation to each element of a subset S of G, amounts to changing the coloring by adding the vector $\sum_{v\in S} e_v$ to it. Thus, letting $B = \{e_v\}_{v\in V}$, condition (1) says that every element of V can be written as a sum of elements of B, and condition (2) is saying no non-empty subset of B sums to 0. By Theorem 2.1, both conditions are equivalent to B being a basis.

□

2.1. **Exercises.**

(1) If $B = \{v_1, \ldots, v_m\}$ is a linearly independent set of V, prove that there are 2^m elements of V that can be written as a sum of elements of B.
(2) Let B be an independent set of V as above. For $v \in V\backslash B$, prove that $B\cup v$ is a linearly independent if and only if v cannot be written as a sum of elements of B.
(3) Let V be a finite vector space of size dimension n. Let $v_1, \ldots, v_n$ be n vectors of V picked at random uniformly from V. Let p_n be the probability that $\{v_1, \ldots, v_n\}$ forms a basis of V. Find an exact formula for p_n (Warning: This will be a long product, and not simplify further!) and prove that $p_n > 1/8$.[1]
(4) Let V be a vector space of dimension n, and let S be the set of all bases of V. Let v be a non-zero element of V.What is the probability that an arbitrary element of S will contain v?

[1]This is extremely surprising to me! No matter how large n is, you've always got a good choice of just randomly picking a basis.

3. Subspaces and homomorphisms

If V is a vector space, we say that a subset $W \subset V$ is a *subspace* of V if W contains 0 and is closed under addition. That is, for any 2 elements w_1, w_2 of W, $w_1 + w_2$ is also in W. It is clear that in this case, W is also a vector space. For example, for any non-zero element $v \in V$, the subset $W = \{0, v\}$ is a subspace of V.

It is also sometimes useful to consider maps between vector spaces over $\mathbb{Z}/2\mathbb{Z}$. Let V_1, V_2 be two vector spaces over $\mathbb{Z}/2\mathbb{Z}$. A map $f : V_1 \to V_2$ is called a *homomorphism* if $f(0) = 0$ and f respects addition. That is, for any v, w in V_1, $f(v + w) = f(v) + f(w)$. For example, we can take $V_1 = V_2 = \mathbb{Z}/2\mathbb{Z}^2$, and we can define $f(a_1, a_2) = (a_1 + a_2, 0)$.

Given a map f, we may build subspaces of V_1 and V_2 as follows. We define the *kernel* of f — written $\ker f$ — to be the subspace of V_1 consisting of all elements v such that $f(v) = 0$. We define the *image* of f — written $\mathrm{im} f$— to be the subspace of V_2 consisting of all elements w in V_2 such that there exists an element $v \in V_1$ with $f(v) = w$. **Exercise: Prove that** $\ker f$ **and** $\mathrm{im} f$ **are subspaces!**

The following fact is extremely important, as it relates these two fundamental quantities:

Theorem 3.1. *Let $f : V_1 \to V_2$ be a homomorphism between vector spaces over $\mathbb{Z}/2\mathbb{Z}$, and suppose that V_1 is finite. Then*

$$|\mathrm{im} f| \times |\ker f| = |V_1|.$$

Proof. It is clear that $|V_1| = \sum_{w \in \mathrm{im} f} |f^{-1}(w)|$ so it suffices to show that $|f^{-1}(w)| = |f^{-1}(0)|$ for each $w \in \mathrm{im} f$ (recall that $f^{-1}(0) = \ker f$).

So let $w \in \mathrm{im} f$ and fix $v_0 \in V_1$ so that $f(v_0) = w$. We have a map $F : f^{-1}(w) \to \ker f$ given by $F(v) = v + v_0$. Indeed, if $f(v) = w$, then $f(v + v_0) = f(v) + f(v_0) = w + w = 0$. Moreover, the map $f^{-1}(w) \to \ker f$ given by $v \to v + v_0$ is an inverse. Thus, F is a bijection and so we're done. □

Try the following exercises, they'll show you how one can use the above theorem to great effect!

3.1. exercises.

(1) Let V_1, V_2 be finite vector spaces over $\mathbb{Z}/2\mathbb{Z}$ of dimensions m_1, m_2 respectively. Show that the number of homomorphisms from V_1 to V_2 is $2^{m_1 m_2}$. **Hint: Show that a homomorphism is determined by what happens to a basis**.

(2) Let V be a vector space over $\mathbb{Z}/2\mathbb{Z}$, and $w, v_1, \ldots, v_n$ be elements of V. Prove that the number of subsets $I \subset \{1, 2, \ldots, n\}$ such that $w = \sum_{i \in I} v_i$ is[2] a power of 2

[2]Whenever you see a graph theory problem that asks you to prove something is a power of 2, there is a 50% chance that this is where its coming from!

(3) Let $f : V_1 \to V_2$ be a homomorphism of finite vector spaces over $\mathbb{Z}/2\mathbb{Z}$ of the same dimension, and let $B = \{v_1, \ldots, v_n\}$ be a basis of V_1. Prove that $f(B) = \{f(v_1), \ldots, f(v_n)\}$ is a basis of V_2 if and only if f is a bijection.

4. Dot Product

Consider the vector space $\mathbb{Z}/2\mathbb{Z}^n$, and let $v = (a_1, \ldots, a_n), w = (b_1, \ldots, b_n)$ be two elements of it. We define the *dot product* $v \cdot w$ as

$$v \cdot w = \sum_{i=1}^{n} a_i b_i.$$

It is easy to see that $v \cdot w = w \cdot v$ and that $(v_1 + v_2) \cdot w = v_1 \cdot w + v_2 \cdot w$. Dot product in this context behaves pretty similarly to the dot product you're used to from geometry, except there is no cosine law, and you can definitely have $v \cdot v = 0$. Here is a common example of how dot product can come up in a problem: Let G be a finite graph. Label the vertices of G by $\{1, 2\, dots n\}$. To the i'th vertex of v associate the vector v_i of $\mathbb{Z}/2\mathbb{Z}^n$ by setting the i'th entry of v_i to be 0, and for $i \neq j$ the j'th entry of v_i is 1 if and only if i and j are neighbors. Then for $i \neq j$, notice that $v_i \cdot v_j$ is 0 if and only if i and j have an even number of neighbors in common,and $v_i \cdot v_i$ is 0 if and only if v_i has an even number of friends.

We've only defined dot products on $\mathbb{Z}/2\mathbb{Z}^n$, but recall that we showed that every vector space is secretly this one in disguise! Dot products can be useful for proving things are linearly independent.

Lemma 4.1. *Let $B = \{v_1, \ldots, v_m\}$ be a subset of $\mathbb{Z}/2\mathbb{Z}^n$. Assume that for all $i \neq j$, $v_i \cdot v_i = 1$ and $v_i \cdot v_j = 0$. Then B is a linearly independent set.*

Proof. Suppose that a linear combination of elements of B is 0. Then its dot product with each of v_i is 0. The proof follows easily from here (in other words, I'm lazy and so its an exercise!)

□

4.1. Exercises.

(1) For $i = 1, \ldots, n$ let e_i be the element of $\mathbb{Z}/2\mathbb{Z}^n$ with a 1 in the i'th place and 0 elsewhere. Let $f_i = e_i + e_{i+1}$ where we take $e_{n+1} = e_1$. Prove that $B = \{f_1, \ldots, f_n\}$ is NOT a basis of $\mathbb{Z}/2\mathbb{Z}^n$. Let W be the subspace consisting of all elements that can be written as a sum of all the elements in a subset of B. Can you describe B succinctly using a dot product?

(2) Let $B = \{v_1, \ldots, v_n\}$ be a basis of $\mathbb{Z}/2\mathbb{Z}^n$. Let V be the set of all homomorphisms from $\mathbb{Z}/2\mathbb{Z}^n$ to $\mathbb{Z}/2$. Notice that V is naturally a vector space over $\mathbb{Z}/2\mathbb{Z}$. Let v_i^* be the homomorphism given by $v_i^*(v) = v_i \cdot v$. Prove that v_i^* is a basis for V.

5. Determinant

If you know about matrices, determinant is a familiar creature to you. If not, then over $\mathbb{F}_2$ it turns out one can talk about it in a really easy an explicit way! Namely, for $i = 1, 2, \ldots, n$ let e_i be the element of $\mathbb{Z}/2\mathbb{Z}^n$ with a 1 in the i'th place and zeroes elsewhere. Now let $B = \{v_1, \ldots, v_n\}$ be a subset of V. Then the determinant of B, written $\det B$, is defined as follows:

$$\det B = \sum_{\pi} \prod_{i=1}^{n} v_i \cdot e_{\pi(i)}$$

where the sum is over all permutations π of $\{1, \ldots, n\}$. This looks messy, but its actually quite clean! Namely, let v_1' be some other vector of V, and write $B' = \{v_1', v_2, v_3, \ldots, v_n\}$ and $B'' = \{v_1 + v_1', v_2, v_3, \ldots, v_n\}$. Then it is easy to see that $\det B + \det B' = \det B''$! The key property is the following:

Theorem 5.1. *$B = \{v_1, \ldots, v_n\}$ is a basis if and only if $\det B = 1$.*

Proof. Sketch: The key is that if any 2 vectors of B are the same, the determinant of B is clearly 0.

Next, If B is a basis, then we can transform B into the basis $\{e_1, \ldots, e_n\}$ by adding late vectors to earlier ones and rearranging.

If B is not a basis, then we can reduce to the case where v_1 is a sum of other vectors in B.

Exercise:Fill in the details to this proof!!

□

6. Problems

(1) The vertices of a regular n-gon are initially marked with one of the signs $+$ or $-$. A move consists in choosing three consecutive vertices and changing the signs from the vertices , from $+$ to $-$ and from $-$ to $+$.
   (a) Prove that if $n = 2015$ then for any initial configuration of signs, there exists a sequence of moves such that we'll arrive at a configuration with only $+$ signs.
   (b) Prove that if $n = 2016$, then there exists an initial configuration of signs such that no matter how we make the moves we'll never arrive at a configuration with only $+$ signs.

(2) In how many ways can one place a 1 or a -1 in an $n \times n$ grid such that the product of the entries in each row and each column is -1?

(3) On a finite graph, every vertex may be colored either black or white. Initially, every vertex is black. It is allowable to pick a vertex and to change the color of it as well as all of its neighbours.
   (a) Is it always possible to change the color of every vertex from black to white by a sequence of operations of this type?
   (b) Prove that the number of reachable states from the position where all the lamps are black is a power of 2.

(4) G is a graph with n elements. For every pair of vertices in G, there are an even number of vertices sharing edges with both of them. Prove that n is odd.
(5) There are $2n$ people at a party. Each person has an even number of friends at the party. (Here, friendship is a mutual relationship.) Prove that there are two people who have an even number of common friends at the party.
(6) A bunch of mathematicians are at a conference, and some of them are friends. Prove that one may divide them into 2 rooms, so that in each room everyone has an even number of friends, and that the number of ways of doing this is a power of 2.
(7) Alice and Bob play a game. Alice going first, they alternate picking subsets of $\{0, 1, \ldots, 0\}$. After 1024 moves when all subsets have been chosen, a player loses if they contain a single subset such that each of the ten digits occurs on an even number of their remaining subsets. Otherwise a draw is declared.
    (a) Prove that Alice has either $0, 1, 1023$ or 1024 winning moves.
    (b) Find all the winning moves for Alice.
(8) Let $A_1, \ldots, A_r$ be a collection of distinct subsets of $\{1, 2, \ldots, n\}$ such that any A_i has an odd number of elements, and any intersection $A_i \cap A_j$ has an even number of elements. Determine the maximum possible size of r.
(9) Let $S_1, \ldots, S_n$ be subsets of $\{1, 2, \ldots, n\}$ each containing an even number of elements. Prove that there exists i, j such that $|S_i \cap S_j|$ is even.
(10) A contest with n question was taken by m contestants. Each question was worth a certain (positive) number of points, and no partial credits were given. After all the papers have been graded, it was noticed that by reassigning the scores of the questions, any desired ranking of the contestants could be achieved. What is the largest possible value of m (in terms of n)? **This isn't really a fair question. It uses vector spaces, but not over $\mathbb{Z}/2\mathbb{Z}$!**
(11) Let S be an $2^n - 1 \times 2^n - 1$ grid of squares. Two cells are considered neighbours if they share an edge. Determine the number of ways to write 1 or -1 in each square such that for each cell, the product of the values in the neighbours of that cell equals the value of the cell.
(12) There are 2007 senators in a senate. Each senator has enemies within the senate. Prove that there is a non-empty subset K of senators such that for every senator in the senate, the number of enemies of that senator in the set K is an even number.
(13) A round robin tournament is played among n teams. A team gains 0 points from a loss, 2 points from a win, and 1 point from a draw. For each non-empty subset S of the teams, there exists a team (possibly in S) which gained an odd number of points from games agains S. Prove that n is even.