The intrinsic algebraic structure of sets

1. The vector space of sets

Let X be a finite set, $\mathcal{P}(X)$ the collection of its subsets. For subsets, $A, B \in \mathcal{P}(X)$ define the binary operation *Boolean sum* by:

$$A + B = \{x : x \text{ is an element of exactly one of the set} A \text{ and } B\}.$$

Let $\mathbb{Z}_2$ denote the two element finite field $\{0, 1\}$. For each subset $A \in X$ define scalar multiplication by:

$$0A = \emptyset \text{ and } 1A = A.$$

Theorem 1. *Let X be a finite set. Then $\mathcal{P}(X)$ with Boolean sum and scalar multiplication is a vector space over $\mathbb{Z}_2$ of dimension $|X|$.*

Proof. We must check that for all $A, B, C \in X$ and all $s, t \in \mathbb{Z}_2$:

- $(A + B) + C = A + (B + C)$
- $(A + B) = (B + A)$
- $A + \emptyset = A$
- $A + A = \emptyset$
- $s(A + B) = sA + sB$
- $(st)A = s(tA)$
- $0A = \emptyset$
- $1A = A$

Among these vector space axioms only associativity of addition is not immediate. It follows from the next more general lemma. □

Lemma 1. *Let X be a finite set $\mathcal{P}(X)$ the collection of its subsets. Then Boolean sum is associative and*

$$\sum_{i=1}^{k} A_i = \{x : x \in A_i \textit{ for an odd number of indices}\}.$$

Proof. Clearly the result holds for $k = 0, 1, 2$. Note that $x \notin (A + B)$ if and only if x belongs to an even number of these sets. So, if $x \in (A + B) + C$ and belongs to $(A + B)$ and not C, it belongs to just one of the three sets while, if $x \in (A + B) + C$ and belongs to C and not $(A + B)$, it belongs to C and an even number of set from $\{A, B\}$, just one of the three sets or all three. Similarly, $x \in A + (B + C)$ if an only if x belongs to exactly one of these sets or to all three. Thus $(A+B)+C = \{x : x \text{ belongs to an odd number of the sets } A, B, C\} = A + (B + C)$ and associativity is proved.

Assume that $\sum_{i=1}^{k-1} A_i = \{x : x \in A_i \text{ for an odd number of indices}\}$. it follows that $x \notin \sum_{i=1}^{k} A_i$ if and only if $x \in A_i$ for an even number of

indices. Let $x \in \sum_{i=1}^{k} A_i = (\sum_{i=1}^{k-1} A_i) + A_k$. If $x \in \sum_{i=1}^{k-1} A_i$ but not in A_k, $x \in A_i$ for an odd number of indices; if $x \in A_k$ but not in $\sum_{i=1}^{k-1} A_i$, then $x \in A_i$ for an even number of indices from 1 to $k-1$ and in A_k. The result follows inductively. $\square$

For those that have only studied real vector spaces, we note that the basic results of linear algebra are the same for vector spaces over any field. In fact, the proofs given in any linear algebra course use only the field axioms and hence are valid in the more general setting. The one exception to this statement is with the inner product. We will make appropriate adjustments later when we get to the inner product. For now, we proceed assuming that all of the standard results of linear algebra are valid in this setting.

Of course there are differences. For example, there are only two scalars 0 and 1. This fact actually simplifies some many arguments, even though it appears strange. Since the only scalars are 0 and 1, the only possible linear combinations of the vectors in a collection $\{A_1, A_2 \ldots, A_k\}$ are the sums of subcollections: $A_{j_1} + \cdots + A_{j_h}$. If we index the elements of $X = \{x_1, x_2, \ldots, x_n\}$ and consider the collection of 1-element subsets $\{x_1\}, \{x_2\}, \ldots, \{x_n\}$, we see that $\{x_{j_1}\} + \{x_{j_2}\} + \cdots + \{x_{j_n}\} = \{x_{j_1}, x_{j_2}, \ldots, x_{j_n}\}$. Thus every subset is a linear combination of $\{x_1\}, \{x_2\}, \ldots, \{x_n\}$ and only the trivial linear combination equals $\emptyset$. We conclude:

Lemma 2. *Let X be a set of cardinality n. Then $\dim(\mathcal{P}(X)) = n$ and the collection of 1-element subsets form a basis.*

One easily sees that the 1-dimensional subsets all have the form $\{\emptyset, A\}$, where $A \neq \emptyset$ and that the 2-dimensional subsets all have the form $\{\emptyset, A, B, A+B\}$, where A, B and $\emptyset$ are all distinct. A very important subset is the collection of all even subsets: define $\mathcal{E}(X)$ to be the collection of all even sets (sets of even cardinality) in $\mathcal{P}(X)$.

Lemma 3. *Let X be an n-element set for some positive n. Then $\mathcal{E}(X)$ is an (n-1)-dimensional subspace of $\mathcal{P}(X)$.*

Proof. One easily checks the result to be true if $n = 1$, hence we assume $n > 1$. We have $|A+B| = |A|+|B|-2|A \cap B|$; therefore, the sum of two even sets is an even set. Hence, $\mathcal{E}(X)$ is closed under addition and scalar multiplication (every collection of subsets that include the empty set is closed under scalar multiplication). So, $\mathcal{E}(X)$ is a subspace. To compute its dimension, we construct a basis. Index $X = \{x_0, x_1, \ldots, x_{n-1}\}$ and consider the sets $T_i = \{x_0, x_i\}$ for $i = 1, \ldots, (n-1)$. one easily sees that

$$T_{j_1} + \cdots + T_{j_h} = \begin{cases} \{x_{j_1} + \cdots + x_{j_h}\} \text{ when } h \text{ is even,} \\ \{x_0, x_{j_1} + \cdots + x_{j_h}\} \text{ when } h \text{ is odd.} \end{cases}$$

From this it is easy to see that the T_i form a basis for $\mathcal{E}(X)$. □

Let $\mathcal{S}$ be a subspace of $\mathcal{P}(X)$ and let $\mathcal{M}(\mathcal{S})$ denote the collection of minimal (under set inclusion), non-empty subsets in $\mathcal{S}$. The sets in $\mathcal{M}(\mathcal{S})$ are called the *minimal sets* of $\mathcal{S}$. Whenever the sets in a sum $A_1 + A_2 + \cdots + A_k$ are pairwise disjoint, we call the sum a *disjoint sum* and write $A_1 \oplus A_2 \oplus \cdots \oplus A_k$. When $A \subset B$, $B + A$ consists of B with the elements of A deleted; in this case, it is natural to write $B - A$ for $B + A$. With these definitions we can state a very useful decomposition theorem:

Theorem 2. *Let X be a finite set and $\mathcal{S}$ a subspace of $\mathcal{P}(X)$. Then each $S \in \mathcal{S}$ is the disjoint sum of minimal sets from $\mathcal{M}(\mathcal{S})$.*

Proof. Let $S \in \mathcal{S}$. If $S = \emptyset$, it equals the empty sum which is a disjoint sum; if $S \in \mathcal{M}(\mathcal{S})$, $S = S$ which is also a disjoint sum. Assume then that S is not minimal. Then there exists $M_1 \in \mathcal{M}(\mathcal{S})$ so that $M_1 \subsetneqq S$. It follows that $S = M_1 \oplus (S - M_1)$. Let M_2 be a minimal subset of $S - M_1$. If $M_2 = S - M_1$, then $S = M_1 \oplus M_2$ and we are done. If not, we have $S = M_1 \oplus M_2 \oplus (S - M_1 - M_2)$ and proceed to decompose $S - M_1 - M_2$. This must end in a finite number of steps with $S = M_1 \oplus M_2 \oplus \cdots \oplus M_h$. □

The minimal sets of $\mathcal{E}(X)$ are the 2-element subsets and indeed each even set is the disjoint sum of 2-element sets. Collections of the form $\mathcal{M}(\mathcal{S})$ for some subspace of $\mathcal{P}(X)$ have been studied extensively under another name: binary matroid.

We next introduce two very important vector space over $\mathbb{Z}_2$; they are both associated with graphs. Let $\Gamma = (V, E)$ be a connected graph (no loops). The first space associated with Γ is called the *bond space* or *cocycle space* of Γ. For each vertex $v \in V$, define B_v, the *vertex cocycle* of v, to be the set of edges with v as an end point. The bond space of Γ, $\mathcal{B}(\Gamma)$ is then the subspace of $\mathcal{P}(E)$ spanned by the vertex cocycles. One easily checks that for any subset of vertices, $U \subset V$:

$$\sum_{v \in U} B_v = \{e \in E : e \text{ has one endpoint in } U \text{ the other in } (V - U)\}$$

It follows that $\sum_{v \in V} B_v = \emptyset$. So the collection of vertex cycles is not an independent set of vectors and hence not a basis. However, since the graph is connected, $\sum_{v \in U} B_v \neq \emptyset$ whenever U is a proper subset: there must be at least one edge connecting some vertex in U with some vertex in $V - U$. Hence, any collection of $|V| - 1$ vertex cocycles will

be independent and, as a maximal independent set of a spanning set, a basis. So $\dim \mathcal{B}(\Gamma) = |V| - 1$.

The second space associated with the connected graph $\Gamma = (V, E)$ is called the *cycle space* of Γ and is denoted by $\mathcal{C}(\Gamma)$:

$$\mathcal{C}(\Gamma) = \{C \subset E : |C \cap B_v| \text{ is even for each } v \in V\}.$$

It is a simple exercise, left to the reader, to show that $\mathcal{M}(\mathcal{C}(\Gamma))$ is the collection of elementary cycles of Γ, i.e. the edge sets of the elementary circuits of Γ. (Our convention is that a circuit is a sub graph consisting of edges and vertices while a cycle is edge set of a circuit.) In view of Theorem **??**, $\mathcal{C}(\Gamma)$ is frequently defined as the collection of all disjoint sums of elementary cycles of Γ.

We may construct a basis for $\mathcal{C}(\Gamma)$ as follows. Let $\Phi = (V, T)$ be a spanning tree for Γ and index $E - T = \{e_1, \ldots, e_m\}$, where $m = |E| - |V| + 1$. For each $e_i \in E - T$, the subgraph $(V, T \cup \{e_i\})$ contains a unique cycle C_i and, of course, that cycle contains e_i but no other edge from $E - T$. Since $\{e_{j_1}, \ldots, e_{j_h}\} \subset C_{j_1} + \cdots + C_{j_h}$ for each non empty sum of these cycles, $\{C_1, \ldots, C_m\}$ is an independent collection. To see that these cycles span, let C be any element of $\mathcal{C}(\Gamma)$. Since T contains no cycles, $\{e_{j_1}, \ldots, e_{j_h}\} = C \cap (E_T)$ is not empty. Now note that $C + C_{j_1} + \cdots + C_{j_h}$ is in $\mathcal{C}(\Gamma)$ and is contained entirely in T. Hence, $C + C_{j_1} + \cdots + C_{j_h} = \emptyset$ and $C = C_{j_1} + \cdots + C_{j_h}$. So $\{C_1, \ldots, C_m\}$ is a basis for $\mathcal{C}(\Gamma)$ and $\dim(\mathcal{C}(\Gamma)) = |E| - |V| + 1$. We summarize these results in the next theorem.

Theorem 3. *Let $\Gamma = (V, E)$ be a connected graph. Then the bond space, $\mathcal{B}(\Gamma)$, is a subspace of $\mathcal{P}(E)$ of dimension $|V| - 1$ and the cycle space, $\mathcal{C}(\Gamma)$, is a subspace of $\mathcal{P}(E)$ of dimension $|E| - |V| + 1$.*

2. THE INNER PRODUCT

While the basic results about vector spaces are the same over every field, this is not true when it comes to inner products. Most student first encounter with an inner product is in a course on real vector spaces and here the properties of the reals are used. The inner product is usually defined as follows: for all vectors v and w, $v \cdot w$ is scalar (real number) satisfying the following conditions.

- *symmetric,* $v \cdot w = w \cdot v$, for all vectors v and w;
- *bilinear,* $v \cdot (\alpha u + \beta w) = \alpha v \cdot u + \beta v \cdot w$, for all vectors u, v and w and all scalars α and β;
- *positive definite,* $v \cdot v > 0$ for all non-zero vectors v.

Our vector space of subsets has a natural "inner product." We define the *inner product* of A and B by $A \cdot B = |A \cap B|_{(mod\ 2)}$, that is $A \cdot B$ is

0 when $|A \cap B|$ is even and 1 when $|A \cap B|$ is odd. This inner product is obviously symmetric. Is it bilinear? Yes:

$$A \cap (B + C) = (A \cap B) + (A \cap C);$$
$$|A \cap (B + C)| = |(A \cap B) + (A \cap C)|$$
$$= |(A \cap B)| + |(A \cap C)| - 2|(A \cap B \cap C)|;$$
$$|A \cap (B + C)|_{(mod\ 2)} = |(A \cap B)|_{(mod\ 2)} + |(A \cap C)|_{(mod\ 2)}.$$

The addition in this last line is the addition in $\mathbb{Z}_2$ and so it may be reread as

$$A \cdot (B + C) = (A \cdot B) + (A \cdot C).$$

Our inner product is not positive definite. Even if we introduce the order $1 > 0$, $A \cdot A = 0$ for every set of even cardinality. We will discuss the condition that replaces positive definite later; for now we investigate this *symmetric bilinear form,* as it is usually called. As before, any thing we proved about the inner product in our linear algebra course that did not use the positive definite condition is valid for our inner product.

First of all, the definition that two vectors are orthogonal if their inner product is 0, still makes sense. We write $A \perp B$ whenever $A \cdot B = 0$; we write $A \perp \mathcal{B}$ whenever $A \perp B$, for every $B \in \mathcal{B}$; we write $\mathcal{A} \perp \mathcal{B}$ whenever $A \perp B$, for every $A \in \mathcal{A}$ and $B \in \mathcal{B}$ and we write $\mathcal{B}^{\perp}$ for $\{A : A \perp B, \text{ for all } B \in \mathcal{B}\}$. The basic properties of orthogonality do not require the positive definite condition or a substitute. Hence, their proofs are the same as in a basic linear algebra course. We list the important ones in the next lemma.

Lemma 4. *Let $A_1, \ldots A_k, B \in \mathcal{P}(X)$, let $\mathcal{B}$ be a subset of mathcal$P(X)$ and let $\mathcal{S}$ be a subspace of $\mathcal{P}(X)$. Then:*

(i) *$B \perp A_i$, for all i, if and only if $B \perp \langle A_1, \ldots A_k \rangle$ (the subspace spanned by the A_i).*
(ii) *$\mathcal{B}^{\perp}$ is a subspace of $\mathcal{P}(X)$.*
(iii) *$\mathcal{S} \subseteq (\mathcal{S}^{\perp})^{\perp}$.*

For an arbitrary subspace and an arbitrary symmetric bilinear form, equality need not hold in part (iii) of this lemma. Equality does hold for all subspaces with our inner product. But we will need a substitute for positive definite to prove it. We will also need this substitute to prove the next important result.

Theorem 4. *Let X be an n-element set and let $\mathcal{S}$ be a subspace of $\mathcal{P}(X)$. Then* $\dim(\mathcal{S}) + \dim(\mathcal{S}^{\perp}) = n$.

We will defer the proof of this result to the next section and continue assuming it to be valid. Applying the theorem to $\mathcal{S}^{\perp}$, we conclude that $\mathcal{S}$ and $(\mathcal{S}^{\perp})^{\perp}$ have the same dimension, giving:

Corollary 1. *Let X be an n-element set and let $\mathcal{S}$ be a subspace of $\mathcal{P}(X)$. Then $\mathcal{S} = (\mathcal{S}^\perp)^\perp$.*

Now let's return to our examples. By the definition of $\mathcal{C}(\Gamma)$ and Lemma **??** (ii), $\mathcal{C}(\Gamma) = \mathcal{B}(\Gamma)^\perp$. And then, $\mathcal{C}(\Gamma)^\perp = (\mathcal{B}(\Gamma)^\perp)^\perp = \mathcal{B}(\Gamma)$. Back to basic set theory, we have the following interesting result:

Theorem 5. *Let X be an n-element set and let $\mathcal{S}$ be a subspace of $\mathcal{P}(X)$. Then:*

(i) $\{\emptyset, X\}^\perp = \mathcal{E}(X)$;
(ii) $\mathcal{S} \subseteq \mathcal{E}(X)$ *if and only if* $X \in \mathcal{S}$.

Let $\Gamma = (V, E)$ be a graph. We note that Γ is bipartite if and only if the vertices can be partitioned into two cells so that all edges have one endpoint in each cell, i.e. if and only if the entire edge set E is a bond. On the other hand, $\mathcal{C}(\Gamma) \subseteq \mathcal{E}(E)$ if and only if each cycle has even length. Hence:

Corollary 2. *$\Gamma = (V, E)$ be a graph, then Γ is bipartite if and only if each circuit has even length.*

It is a simple exercise to show that a connected graph Γ admits an euler circuit if and only if E is a cycle. On the other hand $\mathcal{B}(\Gamma) \subseteq \mathcal{E}(E)$ if and only if each vertex degree is even. Hence:

Corollary 3. *$\Gamma = (V, E)$ be a connected graph, then Γ admits an euler cycle if and only if each vertex has even degree.*

So, these two of the oldest theorems of graph theory are both specializations of the same basic theorem in the vector space of sets! Of course these results can and should be proved directly. The algebra simply adds insight to the relationship between them. However, no nonalgebraic proof is known for the following result:

Theorem 6. *Let X be an n-element set and let $A_1, \ldots, A_m$ be odd subsets of X with pair wise even intersections. Then $m \leq n$.*

Proof. Suppose that $\sum_{i=1}^m \alpha_i A_i = \emptyset$ for scalars $\alpha_i \in \mathbb{Z}_2$. Note that $A_j \cdot A_i = \begin{cases} 1 & j = i \\ 0 & j \neq i \end{cases}$ Taking the inner product of both sides with A_j, we have: $\alpha_j = \sum_{i=1}^m \alpha_i A_j \cdot A_i = A_j \cdot \emptyset = 0$, for all $j = 1, \ldots, m$. Hence, $\{A_1, \ldots, A_m\}$ is an independent set and $m \leq n$. □

3. PROVING $\dim(\mathcal{S}) + \dim(\mathcal{S}^\perp) = n$

Arbitrary symmetric bilinear forms may admit "troublesome vectors" of two possible types: vectors orthogonal to themselves and vectors orthogonal to all other vectors. A vector v that is orthogonal to

every vector in the space is called a *null vector*. Clearly, the only null vector in the familiar inner product space over the reals is the zero vector. Also, the familiar inner product space over the reals admits no non-zero *self-orthogonal vector*. However, non-zero self-orthogonal vectors may exist for an arbitrary symmetric bilinear form. All even sets are self-orthogonal in the vector space of sets. There are many other important examples. Subspaces of the vector space of n-tuples over a finite field are studied extensively in Coding Theory. There they are called linear codes and the orthogonal complement of a linear code, frequently called the dual code, is another linear code. The dimension theorem relates the dimensions of these two codes in spite of the fact that there may well exist self-orthogonal "code words." An example of a symmetric bilinear form over the reals that admits self-orthogonal vectors is Minkowski space, the vector space of special relativity. The real 4-tuple $\vec{p}_i = (t_i, x_i, y_i, z_i)$ represents the time space coordinates of a position in Minkowski space. The inner product for Minkowski space is defined by $\vec{p}_i \cdot \vec{p}_j = (t_i, x_i, y_i, z_i) \cdot (t_j, x_j, y_j, z_j) = t_i t_j - x_i x_j - y_i y_j - z_i z_j$. We interpret this inner product as follows: think of yourself as being at the origin of this vector space and each vector $\vec{p} = (t, x, y, z)$ with $t > 0$ as a position you might occupy at some later time. If $\vec{p} \cdot \vec{p} = 0$, you would have to move at the speed of light to occupy position $\vec{p}$; if $\vec{p} \cdot \vec{p} > 0$, you would have to move at a speed greater than the speed of light to occupy position $\vec{p}$; if $\vec{p} \cdot \vec{p} < 0$, you could get to position $\vec{p}$ by moving at a speed less than the speed of light. In this example too, the dimension theorem holds.

In the presents of non-zero null vectors the dimension theorem is false. Whereas the presents of non-zero self-orthogonal vectors simply prevent one from extending the traditional proof of the dimension theorem to the general case. To give a generalizable proof that could be included in any first year linear algebra course, we simply work around these troublesome vectors. We need just one "new" lemma to prove this dimension theorem.

Lemma 5. *Let $\mathcal{V}$ be and n-dimensional vector space with a symmetric bilinear form and let $\mathcal{S}$ and $\mathcal{T}$ be subspaces of $\mathcal{V}$.*

(i) *If $\dim(\mathcal{S}) > \dim(\mathcal{T})$, then $\mathcal{S}$ contains a nonzero vector that is orthogonal to every vector in $\mathcal{T}$.*

(ii) *If $\mathcal{S}$ contains no nonzero vector orthogonal to every vector in $\mathcal{T}$ and $\mathcal{T}$ contains no nonzero vector orthogonal to every vector in $\mathcal{S}$, then $\dim(\mathcal{S}) = \dim(\mathcal{T})$*

Proof. Let $b_1, \ldots, b_k$ be a basis for $\mathcal{S}$ and $d_1, \ldots, d_h$ a basis for $\mathcal{T}$, where $k > h$. Consider the h-tuples $t_i = (b_i \cdot d_1, \ldots, b_i \cdot d_h)$, for $i = 1, \ldots, k$.

If $t_i = (0, \ldots, 0)$, b_i is the vector we seek. Assume then that the t_i are a set of k nonzero vectors in $\mathbb{R}^h$. Since $k > h$, $\{t_1 \ldots, t_k\}$ is dependent and $\sum_{i=1}^{k} \alpha_i t_i = (0, \ldots, 0)$, for some set of scalars $\alpha_1 \ldots, \alpha_k$, not all of which are zero. But then $v = \sum_{i=1}^{k} \alpha_i b_i$ is a nonzero vector of $\mathcal{S}$ and one easily sees that

$$(v \cdot d_1, \ldots, v \cdot d_h) = \sum_{i=1}^{k} \alpha_i t_i = (0 \ldots, 0).$$

Thus $v \perp d_j$, for $j = 1 \ldots h$, and v is a nonzero vector of $\mathcal{S}$ orthogonal to every vector in $\mathcal{T}$. Part (i) is proved and Part (ii) follows from it. □

Theorem 7. *Let $\mathcal{V}$ be a finite dimensional vector space with a symmetric bilinear form and let $\mathcal{S}$ be a subspace that contains no non-zero null vector. Then*

$$\dim(\mathcal{S}) + \dim(\mathcal{S}^{\perp}) = \dim(\mathcal{V}).$$

Proof. Let $b_1, \ldots, b_k$ be a basis for $\mathcal{S}^{\perp}$, let $b_1, \ldots, b_n$ be an extension of that basis for $\mathcal{S}^{\perp}$ to a basis for $\mathcal{V}$ and let $\mathcal{T}$ be the subspace spanned by $b_{k+1}, \ldots, b_n$. Clearly, $\dim(\mathcal{T}) + \dim(\mathcal{S}^{\perp}) = \dim(\mathcal{V})$ and we need only show that $\dim(\mathcal{S}) = \dim(\mathcal{T})$.

Suppose that $v \in \mathcal{T}$ is orthogonal to every vector in $\mathcal{S}$. Then $v \in \mathcal{S}^{\perp} \cap \mathcal{T}$ and, therefore, must be the zero vector. Suppose that $v \in \mathcal{S}$ is orthogonal to every vector in $\mathcal{T}$. Then $v \perp b_i$, for all i. Thus v is a null vector in $\mathcal{S}$ and, by hypothesis, must be the zero vector. The result now follows by Part (ii) of Lemma **??**. □

A symmetric bilinear form on a vector space $\mathcal{V}$ is said to be *non-singular* if $\mathcal{V}$ has no non-zero null vectors and the term *inner product* is frequently used for a symmetric, non-singular bilinear form. In this sense, all of our examples the vector space of sets, codes and Minkowski space, are supplied with an inner product. And, using this definition of inner product, we have:

Theorem 8. *Let $\mathcal{V}$ be a finite dimensional vector space with an inner product and let $\mathcal{S}$ be any subspace. Then*

$$\dim(\mathcal{S}) + \dim(\mathcal{S}^{\perp}) = \dim(\mathcal{V}).$$