1 Basic rank argument

We start with the simplest algebraic technique, the rank argument. The idea is to associate to each object of interest a vector in such a way that the resulting vectors are linearly independent. It then follows that the number of objects does not exceed the dimension of the vector space. We start with three basic applications.

Eventown and Oddtown There was a town, called Eventown, with 100 inhabitants, who loved forming clubs of all sorts. For aesthetic reasons the city planning department had the following three rule pertaining to club-formation:

1. Each club has an even number of members;
2. Any two clubs have even-many members in common;

Since these rules did not prevent creation of infinitely many clubs with the same membership list, as a matter of practical convenience the following rule was adopted.

3. No two clubs can have identical membership.

Despite this restriction, the citizens of the city formed a huge number, 2^{50}, of clubs. They did this by breaking themselves into pairs, and making clubs out of the pairs in all possible ways (including the famous Void Club).

After a while, a group of citizen emerged that condemned such a profusion of club as decadent. They left the town to form a settlement of their own, which they called Oddtown. The new rules for making clubs there were these:

1. Each club has an *odd* number of members;
2. Any two clubs have even-many members in common.

These two rules made the rule 3 redundant, and so it was eliminated. The following theorem provided the guaranteed bound on the number of clubs:

Theorem 1. *Let n be the population of the Oddtown. Then the number of clubs in Oddtown is at most n.*

Proof. Number the inhabitants 1 through n. It is convenient to regard clubs as mere sets of members; let $S_1, \ldots, S_m \subset \{1, 2, \ldots, n\}$ be these sets.

Associate to each C_i a *characteristic vector*, which we shall call v_i. It is a vector of length n, whose coordinates record if the corresponding town inhabitant is a member of C_i. In symbol-speak,

$$v_{i,k} = \begin{cases} 1 & \text{if } k \in S_i \\ 0 & \text{if } k \notin S_i. \end{cases}$$

Let $u \cdot w = \sum_k u_k w_k$ be the standard dot product of vectors. Then $v_i \cdot v_j$ is equal to $|S_i \cap S_j|$. In particular, if we regard v_i and v_j as vectors in $\mathbb{Z}_2^n$, we obtain

$$v_i \cdot v_j = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

A familiar argument implies that the vectors $v_1, \ldots, v_m$ are linearly independent: Indeed, suppose $\sum \lambda_i v_i = 0$. Then taking the dot product with v_j yields $0 = \sum \lambda_i v_i \cdot v_j = \lambda_j$. As j is arbitrary, this implies that there are no non-trivial linear dependencies. □

Equal unions The next theorem illustrates the importance of choosing the right field to work over. The proof below crucially depends on the ordering of $\mathbb{R}$.

Theorem 2. *Suppose $S_1, \ldots, S_m$ are non-empty subsets of an n-element set. Suppose $m \geq m+1$. Then there are disjoint non-empty sets I_1 and I_2 such that*

$$\bigcup_{i \in I_1} S_i = \bigcup_{i \in I_2} S_i. \tag{1}$$

Proof. As in the Oddtown problem, we denote by v_i the characteristic vector of the set S_i. We treat the characteristic vectors as living in $\mathbb{R}^n$. As $m \geq n+1$, the vectors are linearly dependent over $\mathbb{R}$. So, there exist real numbers $\lambda_1, \ldots, \lambda_n$, not all of which are zero, such that

$$\sum_i \lambda_i v_i = 0.$$

Let

$$I_1 = \{i : \lambda_i > 0\},$$
$$I_2 = \{i : \lambda_i < 0\}.$$

We then have

$$\sum_{i \in I_1} \lambda_i v_i = \sum_{i \in I_2} (-\lambda_i) v_i. \tag{2}$$

Let u denote the common value of the two sums in the equation above. As v_i's are non-zero, the vector u is non-zero too. In particular, both I_1 and I_2 are non-empty.

Consider $\operatorname{supp} u = \{j : u_{/}= 0\}$. From the left side of (2), we see that $\operatorname{supp} u = \bigcup_{I_1} S_i$. Similarly, the right side yields $\operatorname{supp} u = \bigcup_{I_2} S_i$. Hence, (1) holds. □

We note that the bound is sharp, as seen by sets $\{1\}$, $\{2\}$, $\ldots$, $\{n\}$.

2 Which subspace is it?

Sometimes we construct vectors in some vector space V only to find out that they in fact live in a much smaller space that is a subspace of V. Due to its smaller dimension, that gives a better bound on the number of vectors.

Two-distance sets Consider an equilateral triangle in the plane. Any two of its three vertices lie at the same distance from each other. Same is true for the four vertices of a regular tetrahedron in $\mathbb{R}^3$. In general, in $\mathbb{R}^n$ there exist sets of $n+1$ points that are mutually equidistant. The number $n+1$ is the largest possible; there exist no sets of $n+2$ pairwise equidistant points in $\mathbb{R}^n$ (why?).

As a generalization, call a set $P \subset \mathbb{R}^n$ *two-distance set* if there are numbers r_1 and r_2 such that distance between any pair of points in P is either r_1 or r_2. How many points can a two-distance set have? A crude bound can be obtained from Ramsey's theorem (how?), but linear algebra is more appropriate tool:

Theorem 3. *Let $m_2(n)$ be the maximum cardinality of a two-distance set in $\mathbb{R}^n$. Then*

$$m_2(n) \leq (n+1)(n+4)/2.$$

Proof. Suppose P is a two-distance in $\mathbb{R}^n$. Denote by $\|\cdot\|$ the Euclidean norm on $\mathbb{R}^n$. Let $F(x,y) = \bigl(\|x-y\|^2 - r_1^2\bigr)\bigl(\|x-y\|^2 - r_2^2\bigr)$. By assumption, whenever p, p' are two points in P we have

$$F(p,p') = \begin{cases} r_1^2 r_2^2 & \text{if } p = p', \\ 0 & \text{if } p \neq p'. \end{cases} \tag{3}$$

For each $p \in P$ let $f_p \colon \mathbb{R}^n \to \mathbb{R}$ be the function $f_p(x) = F(x,p)$. Relation (3) implies that the functions $\{f_p\}_{p\in P}$ are linearly independent. Indeed, $\sum \lambda_p f_p = 0$ implies that $0 = \sum \lambda_p f_p(p') = \lambda_{p'} r_1^2 r_2^2$, and so $\lambda_{p'}$ is zero. So, $|P|$ is bounded by the dimension of the space of functions to which f_p's belong. What is that space?

The simplest answer is that f_p's belong to the space polynomials of degree 4 in n variables. The dimension of the latter space is $\binom{n+4}{4}$, and so $m(n) \leq \binom{n+4}{4}$. However, f_p actually belong to a much smaller space. To see that, let us take a closer look at f_p.

The degree-4 component of f_p is $(\sum_i x_i^2)^2$. The degree-3 component of f_p is a linear combination of terms of the form $(\sum_i x_i^2)x_j$. Similar analysis of the lower degree components of f_p shows that f_p is a linear combination of

$$(\sum_i x_i^2)^2, (\sum_i x_i^2)x_j, x_i x_j, x_i, 1.$$

As the preceding list has $1 + n + \binom{n+1}{2} + n + 1 = (n+1)(n+4)/2$ functions on it, it follows that $m_2(n) \leq (n+1)(n+4)/2$, as announced. □

Surprisingly, this bound can strengthened by showing that the functions f_p lie in even smaller space. We will not prove that directly. Instead, we will show that we can add several functions to the family $\{f_p\}_{p\in P}$ such that the resulting collection still belongs to the same vector space as in the preceding proof.

Claim 4. *With the notation of the previous proof, the original functions $\{f_p\}_{p\in P}$ and $n+1$ additional function $x_1,\dots,x_n$ together form a linearly independent set. In particular $m(n)+n+1 \le (n+1)(n+4)/2$.*

Proof. To each point $p\in P$ associate its *projectivization* $\bar{p} = (1, p_1, \dots, p_n)$. Let M be the matrix whose columns are $\bar{p}$ as p runs over P. We can assume that M is of full rank, for otherwise, the set P lies in a proper affine subspace of $\mathbb{R}^n$.

Consider a linear dependence

$$\sum_p \lambda_p f_p + \sum_{j=0}^{n} \tau_j x_j = 0. \tag{4}$$

As all f_p's have the same degree-4 homogeneous part, it follows that

$$\sum_{p\in P} \lambda_p = 0. \tag{5}$$

Similarly, since the degree-3 part is $-4\big(\sum x_i^2\big)\sum_p \lambda_p x_j p_j$, it follows that

$$\sum_{p\in P} \lambda_p p_j = 0, \qquad \text{for all } j = 1,\dots,n. \tag{6}$$

We can write (5) and (6) together as

$$M\vec{\lambda} = 0.$$

Applying (4) to a point $q\in P$ yields $r_1^2 r_2^2 \lambda_q + \sum_{j=0}^{n} \tau_j q_j = 0$, which is equivalent to

$$r_1^2 r_2^2 \vec{\lambda} + \vec{\tau} M = 0$$

Multiplying by matrix M^T on the right (or equivalently multiplying q_i and summing over q) yields

$$\vec{\tau} M M^T = 0$$

Since M is of full rank, MM^T is nonsingular, implying $\vec{\tau} = 0$. The rest follows from the preceding proof. □

Equal unions and intersections In preceding section we showed that among $n+1$ sets one can find two families with the same union. Since complement turns unions into intersections, $n+1$ sets also suffice if desire two families with same intersections. The next result surprisingly shows that we need only one more set to ensure that both conditions hold simultaneously.

Theorem 5. *Suppose $S_1, \dots, S_m$ are non-empty subsets of an n-element set. Suppose $m \geq m+1$. Then there are disjoint non-empty sets I_1 and I_2 such that*

$$\bigcup_{i \in I_1} S_i = \bigcup_{i \in I_2} S_i,$$
$$\bigcap_{i \in I_1} S_i = \bigcap_{i \in I_2} S_i.$$

Proof. By de Morgan's laws, the second condition condition is equivalent to $\bigcap_{i \in I_1} \bar{S}_i = \bigcap_{i \in I_2} \bar{S}_i$. Let v_i be the characteristic vector of S_i, and let u_i be the characteristic vector of $\bar{S}_i$. By the same argument from the proof of Theorem 2 it suffices to find real numbers, not all of which are zero, $\lambda_1, \dots, \lambda_n$ such that

$$\begin{aligned} \sum_i \lambda_i v_i &= 0, \\ \sum_i \lambda_i u_i &= 0. \end{aligned} \tag{7}$$

It is easy to find such λ_i's if $m \geq 2n+1$. Indeed, let $w_i = (v_i, u_i)$. The vector w_i is an element of $\mathbb{R}^n \times \mathbb{R}^n$, and can be thought of as a simply the concatenation of the vectors v_i and u_i. If $m \geq 2n+1$, then the vectors $w_1, \dots, w_m$ are linearly dependent, and so there exist non-trivial coefficients λ_i such that $\sum_i \lambda_i w_i = 0$. The latter equation is equivalent to (7).

To bring down the dimension of the ambient space, we note that all of w_i are contained in $V = \{(v, w) \in \mathbb{R}^n \times \mathbb{R}^n : v_1 + w_1 = \cdots = v_n + w_n = 1\}$. The set V is not a vector space, it is an affine subspace of dimension n. It is however contained in the vector space $\{(v, w) \in \mathbb{R}^n \times \mathbb{R}^n : v_1 + w_1 = \cdots = v_n + w_n\}$ of dimension $n+1$. As every set $n+2$ vectors in this space are linearly dependent, and the rest of the proof proceeds as before. $\square$

It is also possible to prove the same result using the projectivization. One notes that the vectors $\bar{v}_i$ are linearly dependent, and then uses that $u_i = \vec{1} - v_i$ to argue that in (7) the first equation implies the second.