

Algebraic Methods in Combinatorics

Po-Shen Loh

27 June 2008

1 Warm-up

1. (A result of Bourbaki on finite geometries, from Răzvan) Let X be a finite set, and let \mathcal{F} be a family of distinct proper subsets of X . Suppose that for every pair of distinct elements in X , there is a unique member of \mathcal{F} which contains both elements. Prove that $|\mathcal{F}| \geq |X|$.

Solution: Let $X = [n]$ and $\mathcal{F} = \{A_1, \dots, A_m\}$. We need to show that $n \leq m$. Define the $m \times n$ incidence matrix \mathbf{A} over \mathbb{R} by putting 1 in the i -th row and j -th column if $j \in A_i$. Consider the product $\mathbf{A}^T \mathbf{A}$, which is an $n \times n$ matrix. For $i \neq j$, its entry at (i, j) is precisely 1.

Also, the diagonal entries are strictly larger than 1, because if some element $j \in X$ belongs to only one set $A_k \in \mathcal{F}$, then the condition implies that every element $i \in X$ is also in A_k , contradicting requirement that A_k be **proper**.

Therefore, $\mathbf{A}^T \mathbf{A}$ is nonsingular by Lemma 1, hence $\text{rank}(\mathbf{A}^T \mathbf{A}) = n$. But $\text{rank}(\mathbf{A}^T \mathbf{A}) \leq \text{rank}(\mathbf{A}) \leq m$, so we are done.

2 Combinatorics of sets

We begin with a technical lemma.

Lemma 1 *Let \mathbf{A} be a square matrix over \mathbb{R} , for which all non-diagonal entries are all equal to some $t \geq 0$, and all diagonal entries are strictly greater than t . Then \mathbf{A} is nonsingular.*

Proof. Let \mathbf{J} be the all-ones square matrix, and let $\mathbf{D} = t\mathbf{J} - \mathbf{A}$. Note that \mathbf{D} is nonzero only on the diagonal, and in fact strictly positive there, so it is a positive definite matrix. Also, \mathbf{J} is well-known to be positive semidefinite (easy to verify by hand), so \mathbf{A} is positive definite, hence nonsingular. \square

Now try the following problems. The last two come from *102 Combinatorial Problems*, by T. Andreescu and Z. Feng.

1. (Fisher's inequality) Let $\mathcal{C} = \{A_1, \dots, A_r\}$ be a collection of distinct subsets of $\{1, \dots, n\}$ such that every pairwise intersection $A_i \cap A_j$ ($i \neq j$) has size t , where t is some fixed integer between 1 and n inclusive. Prove that $|\mathcal{C}| \leq n$.

Solution: Consider the $n \times r$ matrix \mathbf{A} , where the i -th column of \mathbf{A} is the characteristic vector of A_i . Then, $\mathbf{A}^T \mathbf{A}$ is a $r \times r$ matrix, all of whose off-diagonal entries are t . We claim that the diagonal entries are all $> t$. Indeed, if there were some $|A_i|$ which were exactly t , then the structure of \mathcal{C} must look like a "flower," with one set A_j of size t , and all other sets fully containing A_j and disjointly partitioning the elements of $[n] \setminus A_j$ among them. Any such construction has size at most $1 + (n - t) \leq n$, so we would already be done.

Therefore, $\mathbf{A}^T \mathbf{A}$ is nonsingular by Lemma 1, hence $\text{rank}(\mathbf{A}^T \mathbf{A}) = r$. But $\text{rank}(\mathbf{A}^T \mathbf{A}) \leq \text{rank}(\mathbf{A}) \leq n$, so we are done.

2. Let A_1, \dots, A_r be a collection of distinct subsets of $\{1, \dots, n\}$ such that all $|A_i|$ are even, and also all $|A_i \cap A_j|$ are even for $i \neq j$. How big can r be, in terms of n ?

Solution: Arbitrarily cluster $[n]$ into pairs, possibly with one element left over. Then take all possible subsets where we never separate the pairs; this gives r up to $2^{\lfloor n/2 \rfloor}$.

But this is also best possible. Suppose that S is the set of characteristic vectors of the sets in the extremal example. The condition translates into S being self-orthogonal. But $S \perp S \Rightarrow \langle S \rangle \perp \langle S \rangle$, so extremality implies that S is in fact an entire linear subspace, which is self-orthogonal (i.e., $S \subset S^\perp$).

We have the general fact that for any linear subspace, $\dim S^\perp = n - \dim S$. This is because if $d = \dim S$, we can pick a basis v_1, \dots, v_d of S , and write them as the rows of a matrix \mathbf{A} . Then, the kernel of \mathbf{A} is precisely S^\perp , but any kernel has dimension equal to n minus the dimension of the row space (d).

Therefore, $S \subset S^\perp$ implies that $\dim S \leq \dim S^\perp = n - \dim S$, which forces $\dim S \leq \lfloor n/2 \rfloor$, so we are done.

3. What happens in the previous problem if we instead require that all $|A_i|$ are odd? We still maintain that all $|A_i \cap A_j|$ are even for $i \neq j$.

Solution: Answer: $r \leq n$. Work over \mathbb{F}_2 . The characteristic vectors v_i of the A_i are orthonormal¹, so they are linearly independent: given any dependence relation of the form $\sum c_i v_i = \mathbf{0}$, we can dot product both sides with v_k and conclude that $c_k = 0$. Thus, there can only be $\leq n$ of them.

ALTERNATE: Let \mathbf{A} be the $n \times r$ matrix where the columns are the characteristic vectors of the A_i . Then $\mathbf{A}^T \mathbf{A}$ equals the $r \times r$ identity matrix, which is of course of full rank r . Thus $r = \text{rank}(\mathbf{A}^T \mathbf{A}) \leq \text{rank}(\mathbf{A}) \leq n$.

4. Prove that if all codegrees² in a simple graph on n vertices are odd, then n is also odd.

Solution: First we show that all degrees are even. Let v be an arbitrary vertex. All vertices $w \in N(v)$ have odd codegree with v , which means they all have odd degree in the graph induced by $N(v)$. Since the number of odd-degree vertices in any graph must always be even, we immediately find that $|N(v)|$ is even, as desired.

Let A be the adjacency matrix. Then $A^T A = J - I$. But consider right-multiplying by $\mathbf{1}$. $A\mathbf{1} = \mathbf{0} \Rightarrow A^T A\mathbf{1} = \mathbf{0}$ and $I\mathbf{1} = \mathbf{1}$, so we need to have $J\mathbf{1} = \mathbf{1}$, which implies that n is odd.

ALTERNATE ENDING: Now, let $S = \{\mathbf{1}, v_1, \dots, v_n\}$ be the set of $n + 1$ vectors in \mathbb{F}_2^n where $\mathbf{1}$ is the all-ones vector and v_i is the characteristic vector of the neighborhood of the i -th vertex. There must be some nontrivial linear dependence $b\mathbf{1} + \sum_i a_i v_i = \mathbf{0}$. But note that if we take the inner product of this equation with v_k , we obtain $\sum_{i \neq k} a_i = 0$ because $\mathbf{1} \cdot v_k = 0 = v_k \cdot v_k$ and $v_i \cdot v_k = 1$ for $i \neq k$. Hence all the a_i are equal. Yet if they are all zero, then b is also forced to be zero, contradicting the nontriviality of this linear combination. Therefore, all a_i are 1, and the equation $\sum_{i \neq k} a_i = 0$ forces $n - 1$ to be even, and n to be odd.

5. (Introductory Problem 38) 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.

Solution: Let A be adjacency matrix. Suppose for contradiction that every pair of people has an odd number of common friends. Then over \mathbb{F}_2 , we have $A^T A = J - I$, where J is the all-ones matrix and I is the identity. Since all degrees even, $A\mathbf{1} = \mathbf{0}$. Hence $A^T A\mathbf{1} = \mathbf{0}$. But $J\mathbf{1} = \mathbf{0}$ because J is a $2n \times 2n$ matrix, and $I\mathbf{1} = \mathbf{1}$. Thus we have $\mathbf{0} = A^T A\mathbf{1} = (J - I)\mathbf{1} = \mathbf{1}$, contradiction.

6. (Advanced Problem 49) A set T is called *even* if it has an even number of elements. Let n be a positive even integer, and let S_1, \dots, S_n be even subsets of the set $\{1, \dots, n\}$. Prove that there exist some $i \neq j$ such that $S_i \cap S_j$ is even.

¹Strictly speaking, this is not true, because there is no positive definite inner product over \mathbb{F}_2 . However, if one carries out the typical proof that orthonormality implies linear independence, it still works with the mod-2 dot product.

²The *codegree* of a pair of vertices is the number of vertices that are adjacent to both of them.

Solution: Let A be $n \times n$ matrix over \mathbb{F}_2 with columns that are the characteristic vectors of the S_i . Then $A^T A = J - I$. A is singular because $A^T \mathbf{1} = 0$, so $\det A^T A = (\det A)^2 = 0$. However, $\det(J - I)$ is precisely the parity of D_n , the number of derangements of $[n]$. It remains to prove that for even n , D_n is odd. But this follows from the well-known recursion $D_n = (n - 1)(D_{n-1} + D_{n-2})$, which can be verified by looking at where the element n is permuted to.

3 Solution spaces

Suppose we have a system of equations over some field \mathbb{F} , e.g.

$$\begin{aligned} 3x_1 + x_2 - 8x_3 &= 1 \\ 9x_1 - x_2 - x_3 &= 2 \end{aligned}$$

The set of ordered triples (x_1, x_2, x_3) that solve the system is precisely the set of 3-element vectors $\mathbf{x} \in \mathbb{F}^3$ that solve the matrix equation

$$\mathbf{A}\mathbf{x} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \text{ where } \mathbf{A} = \begin{bmatrix} 3 & 1 & -8 \\ 9 & -1 & -1 \end{bmatrix}.$$

When \mathbf{A} is an $m \times n$ matrix and \mathbf{y} is an m -element vector, the solution set of $\mathbf{A}\mathbf{x} = \mathbf{y}$ is closely related to the following concept.

Definition 1 A nonempty subset S of the vector space \mathbb{F}^n is called a **linear subspace** if it is closed under both scalar multiplication and vector addition. (i.e., $\mathbf{x} \in S, c \in \mathbb{F} \Rightarrow c \cdot \mathbf{x} \in S$, and $\mathbf{x}, \mathbf{y} \in S \Rightarrow \mathbf{x} + \mathbf{y} \in S$.)

When the right hand side (\mathbf{y}) consists of all zeros, $\mathbf{A}\mathbf{x} = \mathbf{0}$ is called a *homogeneous system*, and it is easy to prove the following theorem straight from the above definition. **Check it.**

Theorem 1 (Homogeneous systems) Let \mathbf{A} be an $m \times n$ matrix over any field \mathbb{F} , and let $\mathbf{0}$ be the m -element all-zero vector. Then the solution set of the system $\mathbf{A}\mathbf{x} = \mathbf{0}$ is a linear subspace of \mathbb{F}^n .

It is also easy to generalize this result to inhomogeneous systems.

Theorem 2 (General systems) Let \mathbf{A} be an $m \times n$ matrix over any field \mathbb{F} , and let \mathbf{y} be an m -element vector in \mathbb{F}^m . Then the solution set of the system $\mathbf{A}\mathbf{x} = \mathbf{y}$ is either:

- empty, or
- has the form $\mathbf{x}_0 + S$, where \mathbf{x}_0 is a single n -element vector which solves $\mathbf{A}\mathbf{x}_0 = \mathbf{y}$, and S is the linear subspace of \mathbb{F}^n which is the solution set of the matrix equation $\mathbf{A}\mathbf{x} = \mathbf{0}$.

Linear subspaces have very restrictive properties.

Definition 2 Let S be a linear subspace of \mathbb{F}^n , and let $B = \{\mathbf{v}_1, \dots, \mathbf{v}_t\}$ be a set of vectors in S .

- If there are no nontrivial³ linear combinations $\sum_i c_i \cdot \mathbf{v}_i$ that equal $\mathbf{0}$ (with $c_i \in \mathbb{F}$), then we say that B is **linearly independent**.
- If every vector $\mathbf{x} \in S$ can be expressed as a linear combination $\sum_i c_i \cdot \mathbf{v}_i = \mathbf{x}$ with all $c_i \in \mathbb{F}$, then we say that B **spans** S .
- If B has both of the above properties, then we say that B is a **basis** of S . Note that a basis need not be unique (in fact, it never is).

Theorem 3 Every linear subspace S of \mathbb{F}^n has a basis. Furthermore, every basis of S has the same cardinality. This cardinality is called the **dimension** of S .

³Nontrivial means that $(c_1, \dots, c_t) \neq (0, \dots, 0)$.

The above theorem is not trivial (though not hard) to prove, so the reader should instead **establish the following useful corollary**.

Corollary 1 *Let \mathbb{F} be a finite field, and let S be a d -dimensional subspace of \mathbb{F}^n . Then the cardinality of S must be precisely $|\mathbb{F}|^d$. In particular, every matrix equation $\mathbf{Ax} = \mathbf{y}$ over \mathbb{F} has either zero solutions, or exactly $|\mathbb{F}|^d$ solutions for some integer $d \geq 0$.*

Now try these problems.

1. (Răzvan and Titu's *Putnam and Beyond*, #238) We have n coins of unknown masses and a balance. We are allowed to place some of the coins on one side of the balance and an equal number of coins on the other side. After thus distributing the coins, the balance gives a comparison of the total mass of each side, either by indicating that the two masses are equal or by indicating that a particular side is the more massive of the two. Show that at least $n - 1$ such comparisons are required to determine whether all of the coins are of equal mass.

Solution: Suppose there was a sequence of $n - 2$ comparisons, after which the operator was able to conclude that the coins were all of equal mass. Note that since we are required to put an equal number of coins on each side, the operator could only conclude that all masses were equal if every weighing was an equality. Therefore, if we let $\{x_i\}$ be the masses of the coins, the operator must have seen a sequence of $n - 2$ equations of the form $x_1 + x_5 + x_7 = x_2 + x_8 + x_9$. However, this has a 2-dimensional solution space. Therefore, it is impossible to conclude that the coins all must have equal weight, because that corresponds to the conclusion that the system has solution space spanned by the vector of all ones.

2. (USAMO 2008/6). At a certain mathematical conference, every pair of mathematicians are either friends or strangers. At mealtime, every participant eats in one of two large dining rooms. Each mathematician insists upon eating in a room which contains an even number of his or her friends. We need to prove that the number of ways that the mathematicians may be split between the two rooms is a power of two (i.e., is of the form 2^k for some positive integer k). **Reduce the problem to showing that there exists at least 1 way to do this.**

Solution: Let there be n vertices in the graph, called $\{1, 2, \dots, n\}$. Represent a partition as a vector (x_1, x_2, \dots, x_n) over the finite field \mathbb{F}_2 , where the value of x_i (which is either 0 or 1) tells whether it is in V_0 or V_1 , respectively. The even-degree condition boils down to the following system of equations.

For each vertex i :

- if its degree in G is even, write down the equation: $\sum_{j \sim i} x_j = 0$;
- if its degree in G is odd, write down the equation: $x_i + \sum_{j \sim i} x_j = 1$.

(Here, " $j \sim i$ " means that vertices j and i were adjacent in G .)

One can verify that a partition is valid IFF its corresponding vector satisfies the above system of n equations. So, if there is just at least 1 valid partition at all, then linear algebra tells us that the number of solutions is some 2^k , since all nonempty subspaces of \mathbb{F}_2^n have cardinality a power of 2.

Remark. The Gallai Cycle-Cocycle Partition Theorem (c.f. Exercise 1.35 in *Graph Theory* by R. Diestel) states that

The vertex set of any graph can be partitioned into two (possibly empty) sets such that each set induces a subgraph with all degrees even.

This precisely implies that there is at least one way to split the mathematicians, completing the solution to USAMO 2008/6. We will prove this theorem in the next section.

4 But how do I know the solution space is nonempty?

Unfortunately, one of the possibilities in Theorem 2 is that there are no solutions at all. There is a clean way to verify that a solution exists when the finite field is \mathbb{F}_2 . Luckily, that is essentially the only field that arises in Olympiad combinatorics problems!

Theorem 4 Let \mathbf{A} be an $m \times n$ matrix over \mathbb{F}_2 , and let $\mathbf{1}$ be the m -element all-ones vector in \mathbb{F}_2^m . Then the matrix equation $\mathbf{Ax} = \mathbf{1}$ has **no** solution if and only if:

- There is an odd number of row vectors in \mathbf{A} whose sum (over \mathbb{F}_2) is the zero vector.

Proof. The “if” direction is obvious, because the sum of the equations corresponding to those special row vectors would yield $\mathbf{0}$ on the LHS, while the RHS would be $\mathbf{1}$, because the sum of an odd number of 1’s is 1.

For the “only if” direction, suppose that the bulleted condition is **not** fulfilled; we will show that there is a solution. Apply Gaussian Elimination, reducing the matrix $[\mathbf{A}, \mathbf{1}]$ to row-reduced-echelon form. Note that this process replaces every row by a linear combination of the original rows. However, over \mathbb{F}_2 , linear combinations are simply sums of selected rows, because the only scalars are $\{0, 1\}$. By our assumption, this process will **never** create a row that looks like $[0, \dots, 0, 1]$, which is the only obstruction to the existence of a solution. Therefore, a solution exists. \square

To familiarize yourself with the proof of the previous theorem, **follow the same argument to prove the following slight generalization.**

Theorem 5 Let \mathbf{A} be an $m \times n$ matrix over \mathbb{F}_2 , and let \mathbf{y} be an m -element vector in \mathbb{F}_2^m . Then the matrix equation $\mathbf{Ax} = \mathbf{y}$ has **no** solution if and only if:

- There is a collection of row vectors in \mathbf{A} , an odd number of which have corresponding entries in \mathbf{y} that are 1’s, whose sum (over \mathbb{F}_2) is the zero vector.

Now try these problems.

1. (Iran 1997/4) Let A be a matrix of zeroes and ones which is symmetric ($A_{ij} = A_{ji}$ for all i, j) such that $A_{ii} = 1$ for all i . Show that there exists a subset of the rows whose sum is a vector all of whose components are odd.

Solution: Let a selection correspond to a vector \mathbf{x} over \mathbb{F}_2 . A valid selection is a solution of $\mathbf{A}^T \mathbf{x} = \mathbf{1}$, which is the same as $\mathbf{Ax} = \mathbf{1}$ since \mathbf{A} is symmetric. Consider an odd collection of rows, say indexed by $\{r_1, \dots, r_t\}$. Create the t -vertex graph G with adjacency matrix corresponding to the indices $\{r_1, \dots, r_t\}$, but not putting loops on each vertex (as would have been required since all $A_{ii} = 1$).

We need to show that the sum of this odd collection of rows is nonzero. But suppose it is zero. Then, since each $A_{r_i r_i} = 1$, the graph G must have all degrees odd. However, G also has an odd number of vertices, which is impossible! Therefore, Theorem 4 ensures that there is a solution.

2. (*Odd-parity covers*, by Sutner) Suppose that each of the vertices of a simple graph is equipped with an indicator light and a button. Each vertex’s button simultaneously toggles the states of all of its neighbors, as well as its own state. Initially, all lights are off. Prove that it is possible to turn on all of the lights.

Solution: This is exactly the previous problem, where A is the adjacency matrix plus the identity matrix.

3. (Does not use linear algebra) Show that the previous exercise implies the Gallai Cycle-Cocycle Partition Theorem, stated at the end of the previous section. **Hint: for every vertex v of even degree, attach a brand new vertex v' which is adjacent only to it.**

Solution: Now all degrees are odd, hence all sets $N(v) \cup \{v\}$ are even, and so if X is an odd-parity cover, then X^c is also an odd-parity cover. Immediately, we have that all degrees within each X and X^c are even, but there are extra vertices, so we need to show that deleting the extra vertices keeps all degrees even.

But every special pair $\{v, v'\}$ as introduced above must be separated by any odd-parity cover, because v' has degree exactly 1. Therefore, if we restrict both of X and X^c to the original vertex set (simply discarding the new vertices v'), all degrees will still be even.

- (Russia 1997/40) An $n \times n \times n$ cube is divided into unit cubes. We are given a closed non-self-intersecting polygon (in space), each of whose sides joins the centers of two unit cubes sharing a common face. The faces of unit cubes which intersect the polygon are said to be distinguished. Prove that the edges of the unit cubes may be colored in two colors so that each distinguished face has an odd number of edges of each color, while each nondistinguished face has an even number of edges of each color.

Solution: One equation per face. Look for solution over \mathbb{F}_2 . Turns out that linear combination of rows amounts to taking a cycle-sum of elementary 4-loops. If we have 2 loops in sum, their sum is a loop, and its winding number (mod 2) around the special polygon is the sum of the winding numbers of the summands.

Odd number of distinguished rows in linear combination means that winding number should be odd, therefore cannot have linear combination of zero!

5 More linear algebra problems

- (IMO Shortlist 1998/C2, but standard result) Suppose we have an $m \times n$ rectangular array of real numbers, with the property that every row sum and every column sum is an integer. Prove that it is possible to round up or down each entry to obtain an array of integers with each row and column sum the same as it was before.

Solution: Given an instance of this problem, assume that we have done as many roundings as possible to reduce the number of non-integers. Suppose there are still some non-integers left. Ignore all rows that already are completely integers, and also for columns. WLOG, we are left with an $m \times n$ matrix where each row/column still has ≥ 1 (hence ≥ 2) non-integers.

Write $m + n$ equations for the sums of the rows and columns, using unknowns for the non-integers. At least 2 unknowns per row/column, so at least $\max(2m, 2n) \geq m + n$ unknowns. But there is 1 trivial dependence between the $m + n$ equations: by double-counting, sum of all m row equations equals sum of all n column equations.

So we have more unknowns than equations, hence a nontrivial linear space of solutions (there was at least one solution by the given configuration). So we may “push” the solution so that one entry hits the next integer, contradicting minimality.

- (Răzvan and Titu’s *Putnam and Beyond*, #247) There are given $2n + 1$ real numbers, $n \geq 1$, with the property that whenever one of them is removed, the remaining $2n$ can be split into two sets of n elements that have the same sum of elements. Prove that all the numbers are equal.
- (Alon-Spencer, exercise 2.3) Recall that we proved the following result of Erdős in my Probabilistic Methods lecture:

A set S is called sum-free if there is no triple of (not necessarily distinct) elements $x, y, z \in S$ satisfying $x + y = z$. Then every set A of nonzero integers contains a subset $S \subset A$ of size $|S| > |A|/3$ which is sum-free.

Now prove the generalization of the above result in which the elements of A are allowed to be nonzero **real numbers**.

Solution: We reduce to the integer result, but noting that our previous proof could be trivially generalized to multisets. Let our given set A be $\{x_1, \dots, x_n\}$. Some of these satisfy relations, e.g., $x_i + x_j = x_k$. Collect all of these relations and write them down as a system of equations. Clearly, this system has a nontrivial solution over \mathbb{R} , because it was given as A !

But the system has only rational coefficients, so if we forget that the x_i mean anything, there will also be a solution over \mathbb{Q} , and in fact all in \mathbb{Z} by clearing the denominators. Let A' be the new set corresponding

to those final values x'_i , and apply the integer result to A' . If we end up keeping $x'_{i_1}, \dots, x'_{i_r}$, then we define $S = \{x_{i_1}, \dots, x_{i_r}\}$.

A The language of linear algebra

- The *rank* of a matrix is its the number of linearly independent columns. This is always equal to the number of linearly independent rows. **Fact:** the rank of the product of two matrices is \leq the rank of either matrix, because the columns of the product \mathbf{AB} are linear combinations of the columns of \mathbf{A} , hence column space can only shrink, etc.
- A square matrix \mathbf{A} is *singular* if the equation $\mathbf{Ax} = \mathbf{0}$ has a nontrivial solution. Otherwise, it is *nonsingular*.
- A set of vectors is *orthogonal* if their pairwise dot products are zero. **Fact:** if the vectors also have nonzero dot product with themselves, then the collection is linearly independent.
- A square matrix \mathbf{A} is *positive semidefnite* if $\mathbf{x}^T \mathbf{Ax}$ is ≥ 0 for all vectors \mathbf{x} . If in addition we also know that the only way to get $= 0$ above is by using the $\mathbf{0}$ vector for \mathbf{x} , then we say that \mathbf{A} is *positive definite*. **Fact:** every positive definite matrix is nonsingular, because if we have some $\mathbf{x} \neq \mathbf{0}$ with $\mathbf{Ax} = \mathbf{0}$, then of course $\mathbf{x}^T \mathbf{Ax} = 0$, contradicting *positive* definiteness.