A combinatorial proof of Fisher's Inequality

Rogers Mathew*[1] and Tapas Kumar Mishra[2]

[1] *Department of Computer Science and Engineering, Indian Institute of Technology, Hyderabad*
rogers@iith.ac.in
[2] *Department of Computer Science and Engineering, National Institute of Technology, Rourkela*
mishrat@nitrkl.ac.in

Abstract

In this note, we give a simple, counting based proof of Fisher's Inequality that does not use any tools from linear algebra.

1 Introduction

Let k be a positive integer and let $\mathcal{A}$ be a family of subsets of $[n]$. Fisher's Inequality states that if the cardinality of the intersection of every pair of distinct sets in $\mathcal{A}$ is k, then $|\mathcal{A}| \leq n$. R. A. Fisher [Fisher, 1940] while studying Balanced Incomplete Block Designs (BIBDs) proved that the number of points never exceeds the number of blocks. R.C. Bose [Bose, 1949] proved the Fisher's inequality when all the sets in the family $\mathcal{A}$ are of the same size. In [De Bruijn and Erdös, 1948], it was shown that a maximal family of subsets of $[n]$ that has exactly one common element among every pair of distinct sets has cardinality at most n. The first proof of the general form of the Fisher's Inequality was given by K. N. Majumdar [Majumdar, 1953] using linear algebraic methods. László Babai in [Babai, 1987] remarked that it would be challenging to obtain a proof of Fisher's Inequality that does not rely on tools from linear algebra. D. R. Woodall [Woodall, 1997] took up the challenge and gave the first fully combinatorial proof of the inequality. Below, we give a simple, alternate proof of the inequality that does not rely on tools from linear algebra.

Theorem 1. *(Fisher's Inequality) Let k be a positive integer and let $\mathcal{A} = \{A_1, \ldots, A_m\}$ be a family of subsets of $U = \{e_1, \ldots, e_n\}$. If $|A_i \cap A_j| = k$ for each $1 \leq i < j \leq m$, then $m \leq n$.*

Proof. It is safe to assume that all the sets in $\mathcal{A}$ are of size more than k. (Otherwise, let $A \in \mathcal{A}$ be a set of size exactly k. Then, the set $\{B \setminus A | B \in \mathcal{A} \setminus \{A\}\}$ partitions the elements of $[n]$ not present in A: this leads to $m \leq n - k + 1$.) For the sake of contradiction, assume that $m \geq n + 1$. Let $x_{i,j}$, $1 \leq i \leq m$, $1 \leq j \leq n$, be mn variables with

$$x_{i,j} = \begin{cases} 1, & \text{if } j \in A_i \\ 0, & \text{otherwise.} \end{cases}$$

*This author was supported by a grant from the Science and Engineering Research Board, Department of Science and Technology, Govt. of India (project number: MTR/2019/000550).

Let $s > m^n$ be an integer. Consider a function $f : [m] \to [s]$. Let

$$\begin{aligned}
f(1)x_{1,1} + f(2)x_{2,1} + \cdots + f(m)x_{m,1} =& c_1 && \text{(corresponding to element } e_1\text{)} \\
&\vdots \\
f(1)x_{1,n} + f(2)x_{2,n} + \cdots + f(m)x_{m,n} =& c_n && \text{(corresponding to element } e_n\text{)}
\end{aligned} \tag{1}$$

We define a *profile* of the function f corresponding to the family $\mathcal{A}$ as the n-tuple $(c_1, c_2, \ldots, c_n)$. Note that the number of distinct functions from $[m]$ to $[s]$ is s^m and the number of distinct profiles is at most $(ms)^n$. Since the number of profiles is strictly less than the total number of functions from $[m]$ to $[s]$, by pigeonhole principle, it follows that there are two distinct functions f_1, f_2 that yield the same profile. Let $\tau = f_1 - f_2$. Since f_1 and f_2 are distinct, τ is not the zero function. From the set of Equations (1), it follows that

$$\begin{aligned}
\tau(1)x_{1,1} + \tau(2)x_{2,1} + \cdots + \tau(m)x_{m,1} =& 0 && \text{(Equation } (b_1)\text{)} \\
&\vdots \\
\tau(1)x_{1,n} + \tau(2)x_{2,n} + \cdots + \tau(m)x_{m,n} =& 0 && \text{(Equation } (b_n)\text{)}
\end{aligned}$$

Adding the LHS and RHS of Equations (b_1) to (b_n), we get

$$\tau(1)|A_1| + \tau_2|A_2| + \cdots + \tau(m)|A_m| = 0. \tag{2}$$

Let $A_1 = \{e_{i_1}, e_{i_2}, \ldots, e_{i_r}\}$. Adding the LHS and RHS of the Equations $(b_{i_1}), \ldots, (b_{i_r})$, we get

$$\begin{aligned}
&\tau(1)|A_1| + \tau(2)|A_1 \cap A_2| + \cdots + \tau(m)|A_1 \cap A_m| = 0 \\
\implies &\tau(1)|A_1| + k(\tau(2) + \cdots + \tau(m)) = 0
\end{aligned} \tag{3}$$

Writing similar equations corresponding to each set A_i in $\mathcal{A}$, we get m equations as follows.

$$\begin{aligned}
&\tau(1)|A_1| + k(\tau(2) + \cdots + \tau(m)) = 0 \\
&\tau(2)|A_2| + k(\tau(1) + \tau(3) + \cdots + \tau(m)) = 0 \\
&\vdots \\
&\tau(m)|A_m| + k(\tau(1) + \cdots + \tau(m-1)) = 0
\end{aligned} \tag{4}$$

Adding the LHS and RHS of every equation in (4), we get

$$\begin{aligned}
&\tau(1)|A_1| + \tau_2|A_2| + \cdots + \tau(m)|A_m| + k(m-1)(\tau(1) + \cdots + \tau(m)) = 0 \\
\implies &\tau(1) + \cdots + \tau(m) = 0 \text{ (Using Equation 2).}
\end{aligned} \tag{5}$$

Since τ is not the zero function, without loss of generality, assume that $\tau(1) \neq 0$. From Equation 3, it follows that

$$\begin{aligned}
&\tau(1)|A_1| + k(\tau(2) + \cdots + \tau(m)) = 0 \\
\implies &\tau(1)|A_1| + k(-\tau(1)) = 0 \text{ (From Equation 5)} \\
\implies &\tau(1)(|A_1| - k) = 0.
\end{aligned} \tag{6}$$

This is a contradiction as $|A_1| > k$ and $\tau(1) \neq 0$. So, our assumption that $m \geq n + 1$ is false. $\square$

2 Concluding remarks

The pigeonholing argument used to show that there exists a non-trivial solution to the homogeneous system of linear equations (b_1) to (b_n) whose coefficients are either 0 or 1 can be extended to any homogeneous system of n linear equations on m $(> n)$ variables whose coefficients are integers by taking an appropriately large s (Siegel's Lemma [Siegel, 1929]). Hence, a similar pigeonholing argument can be used to give a proof, that does not rely on 'tricks' of linear algebra, of other theorems in combinatorics that use a homogeneous system of linear equations like the Beck-Fiala Theorem [Beck and Fiala, 1981], Beck-Spencer Theorem [Beck and Spencer, 1983], etc. In [Vishwanathan, 2013], a counting based proof of the Graham-Pollak Theorem is given using similar ideas.

References

[Babai, 1987] Babai, L. (1987). On the nonuniform fisher inequality. *Discrete mathematics*, 66(3):303–307.

[Beck and Fiala, 1981] Beck, J. and Fiala, T. (1981). integer-making theorems. *Discrete Applied Mathematics*, 3(1):1–8.

[Beck and Spencer, 1983] Beck, J. and Spencer, J. (1983). Balancing matrices with line shifts. *Combinatorica*, 3(3-4):299–304.

[Bose, 1949] Bose, R. C. (1949). A note on fisher's inequality for balanced incomplete block designs. *The Annals of Mathematical Statistics*, 20(4):619–620.

[De Bruijn and Erdös, 1948] De Bruijn, N. G. and Erdös, P. (1948). On a combinatorial problem. *Proceedings of the Section of Sciences of the Koninklijke Nederlandse Akademie van Wetenschappen te Amsterdam*, 51(10):1277–1279.

[Fisher, 1940] Fisher, R. A. (1940). An examination of the different possible solutions of a problem in incomplete blocks. *Annals of Human Genetics*, 10(1):52–75.

[Majumdar, 1953] Majumdar, K. N. (1953). On some theorems in combinatorics relating to incomplete block designs. *The Annals of Mathematical Statistics*, 24(3):377–389.

[Siegel, 1929] Siegel, C. L. (1929). *Über einige Anwendungen diophantischer Approximationen*. Akad. de Gruyter in Komm.

[Vishwanathan, 2013] Vishwanathan, S. (2013). A counting proof of the graham-pollak theorem. *Discret. Math.*, 313(6):765–766.

[Woodall, 1997] Woodall, D. R. (1997). A note on fisher's inequality. *Journal of Combinatorial Theory, Series A*, 77(1):171 –176.