Sperner's theorem

https://doi.org/10.31713/MCIT.2021.27

Oleksandr Rybak
National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»,
Kyiv, Ukraine

Stepan Tarasenko
National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»,
Kyiv, Ukraine

Abstract — **In the course of this work the analysis of the proofs of the simple case of the Sperner Theorem was carried out, the approaches to the proof of the complicated case were proposed, the partial cases of multisets were considered, the theorem for these partial cases was proved, the generalized theorem was proved for some partial cases. C_n^k (the number of n - element multisets of k - element multiset), developed a small program to graphically show this fact, proved the bimonotonicity of this function. Also, in the course of this work, one of the possible applications of this theorem was considered, namely, the «Procedure for secret distribution», but the applied potential of the theorem does not end there.**

Keywords — **Sperner's theorem; multiset; procedure for secret distribution.**

1. Introduction

Sperner's Theorem:

$M_1,\ldots.,M_k$ – a number of n subsets of a set S = {1, …, n}, we know that $\forall i,j: M_i \not\subset M_j$, so the family of sets $M_1,\ldots.,M_k$ called the anti-chain. Sperner has proven that $k \le C_n^k$, where k is a number of sets in the anti-chain and n is a total number of elements in the set S.

The goal of this work was to prove the Sperner's theorem for the case when the set S could contain elements with a power, so the object S is a multiset.

Sperner's Theoreme multiset case:

The set $S = \{1^{\alpha_1},\ldots.,n^{\alpha_n}\}$ where $\alpha_1,\ldots.,\alpha_n$ – are multiplicity of each element of the multiset and we are constructing the same anti-chain $M_1,\ldots.,M_k$ but each set in the anti-chain could be a multiset. We are stating the same: $k \le C_n^k$.

The way to proof the complicated (multiset) Sperner's theorem based on the Hall's marriage theorem.

Hall's Theorem

In an undirected graph, a matching is a set of disjoint edges. Given a bipartite graph with bipartition A, B, every matching is obviously of size at most |A|. Hall's Theorem gives a nice characterization of when such a matching exists.

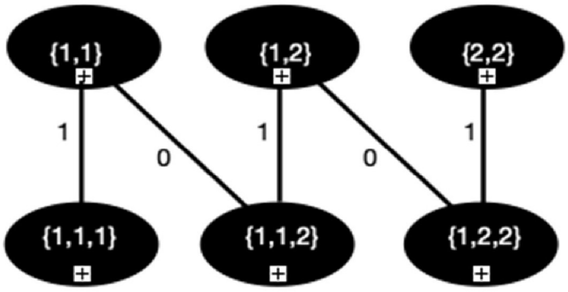
Theorem There is a matching of size A if and only if every set S ⊆ A of vertices is connected to at least |S| vertices in B.

2. Sperner's Theorem partial cases $M = \{a^n, b^m\}$ and $M = \{a_n^2,\ldots..,a_0\}$

Let a graph be constructed in which all multisets of power x are in the upper lobe and power x + 1 are in the lower lobe. The edge is built when the upper multiset is included in the lower. Since in the case of ordinary sets $\overline{deg} = n - t$ and $\underline{deg} = t$. Then in the case of multisets we will weigh the graph by placing the appropriate weights on the edges to obtain a similar result.

Consider a few examples:

Suppose, $M_1,\ldots.,M_k \subseteq \{1,1,1,2,2\}$ and $x = 2$, in the upper lobe of the graph are two-element subsets, in the lower three-element subsets, we are going to construct the graph as follows:

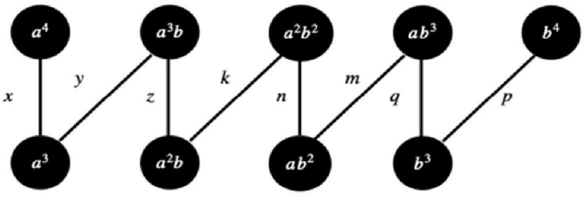


So we made it using the same rule: $\overline{deg} = n - t$ and $\underline{deg} = t$, we are trying to generalize the solution of the non multiset case of Sperner's Theorem on the multiset case.

2.1. Case $M = \{a^n, b^m\}$

In this case we have element a that represented n times in the set M and element b that represented m times in the set M.

The way to proof the partial case was described above, so we are constructing the graph and trying to weight it. Let's start with the case $M = \{a^5, b^4\}$, so the n is 5 and m is 4:



We need to solve the linear equation system that contains eight equations, also we have eight variables, so it is easy to find a solution:

$$\begin{cases} x=4, \\ x+y=5, \\ y+z=4, \\ z+k=5, \\ k+n=4, \\ n+m=5, \\ m+q=4, \\ p=4. \end{cases} \qquad \begin{cases} x=4, \\ y=1, \\ z=3, \\ k=2, \\ n=2, \\ m=4, \\ q=1, \\ p=4. \end{cases}$$

We have found a way to weight the graph for the set $M=\{a^5,b^4\}$, so it is easy to generalize

$$\begin{cases} x=y+z=k+n=m+q+p+s_1, \\ x+y=k+z=n+m=p+q=s_2. \end{cases}$$

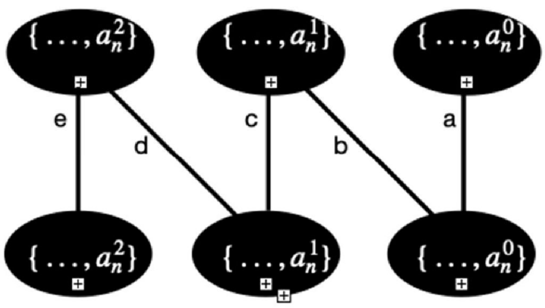
this solution $\forall M=\{a^n,b^m\}$. s_1, s_2 are sums that flows in up and down lobes.

$$5s_1=4s_2.$$

We can take s_1 any, other values will be proportional. We will make the same system in case of incomplete saturation of a graph.

2.2. Case $M=\{a_n^2,\ldots\ldots,a_0\}$

In this case we have element a_n represented two times in the set M and the rest of elements of the set are represented one time.

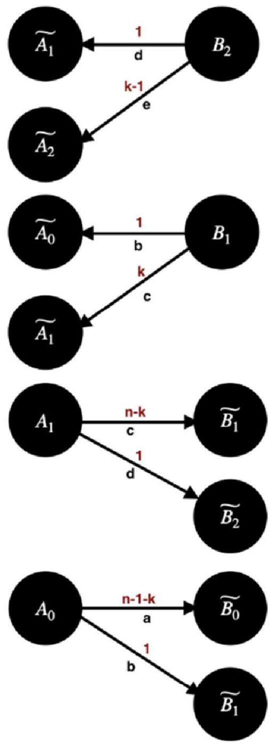


In order to proof the theorem for this case we need to weight the graph:

In the upper lobe of the graph $(k+1)$ – element subsets, in the lower lobe k – element subsets a,b,c,d,e – the weights of the edges between the corresponding types of subsets.

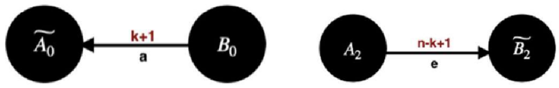
Let A_i – k subset of i-th type (i=0, 1, 2), where type – a_n the number contained in A_i. Find how many $(k+1)$ – subsets of type 0, 1, 2 contain this A_i. (All calculations for this subparagraph are omitted only the results are shown).

We need to weight the following subsets, where each node not a simple set but a family of subsets:

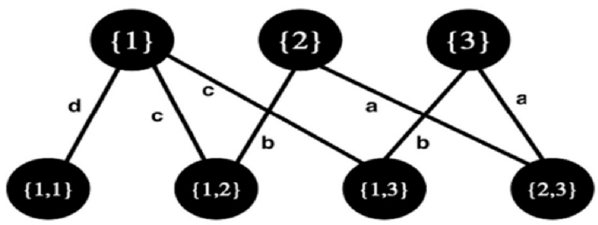


By solving the system of linear equations we have found an explicit way of weighting a graph. Let's try to use the formulas to weight the graph for the following case and consider a few examples:

Let $M=\{1,1,2,3\}$, weight the graph, describing the transition from single-element submultiples to double-element ones, in our case $n=3$ (The power of the set M,



while counting only unique elements) and we are going to weight the graph by transition from one element subsets to two element subsets so the $k=1$:



We have found an explicit formulas to weight the graph, to simplify the formula let's designate:

$$m=n^2-nk+k^2$$

Explicit formulas to calculate weights:

$$\begin{cases} m = n^2 - nk + k^2 = 7, \\ a = m + n - k = 9, \\ c = m - n + 1 = 3, \\ e = m + k = 8, \\ b = n^2 + nk + n = 15, \\ d = 2n^2 - nk + n = 18. \end{cases}$$

we have the following

$$\begin{cases} 18 = d = c + b = a + a, \\ 24 = d + c + c = a + b. \end{cases}$$

So the calculations formulas for the weights is are correct.

3. Conclusion

The proof of the Sperner's Theorem for the partial cases $M = \{a_n^2, \ldots.., a_0\}$ and $M = \{a^n, b^m\}$ could help to build mathematical objects that are based on multiset theory and be sure that for the following partial cases the Sperner's Theorem is working and the number of anti-chains are $k \leq C_n^k$. We have considered in the introduction that one of the interesting applications of this theorem is «Procedure for secret distribution». This is a cryptographic problem to distribute the secret between a number of people or other entities, this theorem could help to make this secret distribution if the the «secret» has multidimensional nature.

References

[1] Kapitonova Yu. V., Krivoy SL, Letichevsky A. A. Lectures on discrete mathematics. SPb. : BHV-Petersburg, 2004 . 624 p.
[2] Lipsky V. Combinatorics for programmers. M., 1988. 200 p.
[3] Doug Wiedemann A computation of the eighth Dedekind number. Order. 1991. T. 8. Вып. 1. C. 5–6.
[4] Kleitman D., Markowsky G. On Dedekind's problem: the number of isotone Boolean functions. II. Transactions of the American Mathematical Society. 1975. T. 213. C. 373–390.