Mathematical
Inequalities
& Applications
Volume 14, Number 2 (2011), 439–444

ORDER MATTERS WHEN CHOOSING SETS

WARREN B. MOORS AND JULIA C. NOVAK

(*Communicated by N. Elezović*)

Abstract. Given natural numbers t, w and v we show, using high school algebra, that if $1 \leqslant w \leqslant t < v$ then $((v \text{ ch } t) \text{ ch } w) \leqslant ((v \text{ ch } w) \text{ ch } t)$. Here we denote "$n$ choose r" by $(n \text{ ch } r)$.

In this paper we show, using high school algebra, that if $1 < w < t < v$ are natural numbers then

$$\binom{\binom{v}{w}}{t} > \frac{w!(t!)^w}{t!(w!)^t}\binom{\binom{v}{t}}{w}.$$

Our original interest in this inequality arose from the study of incidence structures. Specifically, in regard to the assignment of keys/sub-keys to users in a network in order to ensure that certain specified security conditions are fulfilled (i.e., Key Distribution Patterns). For further information on this see [2, Chapter 4]. However, as this inequality is somewhat natural, not surprisingly, variations on this inequality have been studied before e.g. in [1]. In fact, the special case of our inequality when $w = 2$ and $t = 3$ was considered in [1, Theorem 5].

LEMMA 1. *If $1 \leqslant j \leqslant w < v$ are natural numbers then,*

$$[v(v-1)\cdots(v-w+1) - jw!][v-w+j] \geqslant v(v-1)\cdots(v-w+1)(v-w).$$

Proof. Fix $1 \leqslant j \leqslant w$ then,

$$\begin{aligned}&[v(v-1)\cdots(v-w+1) - jw!][(v-w)+j]\\ &\quad = v(v-1)\cdots(v-w+1)(v-w)\\ &\qquad + \big[jv(v-1)\cdots(v-w+1) - j^2w! - jw!(v-w)\big].\end{aligned}$$

We claim that

$$jv(v-1)\cdots(v-w+1) - j^2w! - jw!(v-w) \geqslant 0.$$

Mathematics subject classification (2010): Primary 05A20; Secondary 05A05, 94A60.
Keywords and phrases: Key distribution patterns, combinatorial inequalities, cryptography.

Paper MIA-14-35

To see this, we simply do more algebra.

$$\begin{aligned} & jv(v-1)\cdots(v-w+1) - j^2 w! - jw!(v-w) \geqslant 0 \\ \iff & jv(v-1)\cdots(v-w+1) \geqslant j^2 w! + jw!(v-w) \\ \iff & \binom{v}{w} \geqslant j + (v-w). \end{aligned}$$

Now, $j+(v-w) \leqslant v$. On the other hand, because $1 \leqslant w < v$, $\binom{v}{w} \geqslant v$. Therefore,

$$[v(v-1)\cdots(v-w+1) - jw!][v-w+j] \geqslant v(v-1)\cdots(v-w+1)(v-w). \quad \square$$

LEMMA 2. *If $1 < w < v$, $1 \leqslant j < v$ and $j, w, v \in \mathbb{N}$ then,*

$$[v(v-1)\cdots(v-w+1) - jw!] \geqslant (v-1)(v-2)\cdots(v-w+1)(v-w) \geqslant (v-w)^w.$$

Proof. To prove this, we again do some algebra.

$$\begin{aligned} & [v(v-1)\cdots(v-w+1) - jw!] - (v-w)(v-1)(v-2)\cdots(v-w+1) \geqslant 0 \\ \iff & -jw! + w(v-1)(v-2)\cdots(v-w+1) \geqslant 0 \\ \iff & (v-1)(v-2)\cdots(v-w+1) \geqslant j(w-1)! \\ \iff & \left[\frac{v-1}{j}\right]\left[\frac{v-2}{w-1}\right]\cdots\left[\frac{v-w+1}{2}\right] \geqslant 1; \end{aligned}$$

which is true since $1 \leqslant j < v$ and $w < v$. $\square$

LEMMA 3. *If $1 \leqslant w < v$ are natural numbers then,*

$$\left[\prod_{j=1}^{w} [v(v-1)\cdots(v-w+1) - jw!]\right][v(v-1)\cdots(v-w+1)] \geqslant [v(v-1)\cdots(v-w)]^w.$$

Proof. This follows directly from Lemma 1 and the fact that:

$$\begin{aligned} & \left[\prod_{j=1}^{w} [v(v-1)\cdots(v-w+1) - jw!]\right][v(v-1)\cdots(v-w+1)] \\ & \quad = \prod_{j=1}^{w} [v(v-1)\cdots(v-w+1) - jw!][v-w+j]. \end{aligned}$$

At last we are ready to prove our inequality which generalises [1, Theorem 5].

THEOREM 1. *If $1 < w < t < v$ are natural numbers then* $\binom{\binom{v}{w}}{t} > \dfrac{w!(t!)^w}{t!(w!)^t}\binom{\binom{v}{t}}{w}$.

Proof. Suppose that $1 < w < t < v$ are natural numbers then

$$\begin{aligned}
\binom{\binom{v}{w}}{t} &= \frac{1}{t!}\left[\prod_{j=0}^{t-1}\frac{[v(v-1)\cdots(v-w+1)-jw!]}{w!}\right] \\
&\geqslant \frac{1}{t!(w!)^t}\left[\prod_{j=0}^{w}[v(v-1)\cdots(v-w+1)-jw!]\right][(v-w)^w]^{t-w-1} \quad \text{by Lemma 2} \\
&= \frac{1}{t!(w!)^t}\left[v(v-1)\cdots(v-w+1)\prod_{j=1}^{w}[v(v-1)\cdots(v-w+1)-jw!]\right][(v-w)^{t-w-1}]^w \\
&\geqslant \frac{1}{t!(w!)^t}\Big([v(v-1)\cdots(v-w)]^w\cdot[(v-w)^{t-w-1}]^w\Big) \quad \text{by Lemma 3} \\
&= \frac{1}{t!(w!)^t}\Big([v(v-1)\cdots(v-w)(v-w)^{t-w-1}]^w\Big) \\
&\geqslant \frac{1}{t!(w!)^t}\Big([v(v-1)\cdots(v-w)\cdots(v-t+1)]^w\Big) \\
&> \frac{w!(t!)^w}{t!(w!)^t}\left[\frac{1}{w!}\prod_{j=0}^{w-1}\frac{[v(v-1)\cdots(v-t+1)-jt!]}{t!}\right] \\
&= \frac{w!(t!)^w}{t!(w!)^t}\binom{\binom{v}{t}}{w}. \quad \square
\end{aligned}$$

PROPOSITION 1. *If $1 < w < t$ are natural numbers then*

$$\lim_{v\to\infty}\frac{\binom{\binom{v}{w}}{t}}{\binom{\binom{v}{t}}{w}} = \frac{w!(t!)^w}{t!(w!)^t}.$$

Proof. Define $P:\mathbb{R}\to\mathbb{R}$ and $Q:\mathbb{R}\to\mathbb{R}$ by, $P(x) := \prod_{j=0}^{t-1}[(x(x-1)\cdots(x-w+1)-jw!]$ and $Q(x) := \prod_{j=0}^{w-1}[(x(x-1)\cdots(x-t+1)-jt!]$. Then P and Q are monic polynomials of degree wt. Therefore, $\lim_{x\to\infty}\dfrac{P(x)}{Q(x)} = 1$. It now follows that,

$$\lim_{v\to\infty}\frac{\binom{\binom{v}{w}}{t}}{\binom{\binom{v}{t}}{w}} = \lim_{v\to\infty}\frac{\frac{1}{t!(w!)^t}P(v)}{\frac{1}{w!(t!)^w}Q(v)} = \frac{w!(t!)^w}{t!(w!)^t}\cdot\lim_{v\to\infty}\frac{P(v)}{Q(v)} = \frac{w!(t!)^w}{t!(w!)^t}. \quad \square$$

Together Proposition 1 and Theorem 1 yield the fact that for any natural numbers $1 \leqslant w \leqslant t$

$$\inf_{v\in\{t+1,t+2,\ldots\}}\frac{\binom{\binom{v}{w}}{t}}{\binom{\binom{v}{t}}{w}} = \frac{w!(t!)^w}{t!(w!)^t}.$$

To understand this inequality better we need the following crude estimate.

PROPOSITION 2. *If $1 \leqslant w \leqslant t$ are natural numbers then*

$$\frac{w!(t!)^w}{t!(w!)^t} \geqslant \left(\frac{w+1}{2}\right)^{(t-w)} \geqslant 1.$$

Proof. We need only consider the case when $1 < w < t$.

$$\frac{w!(t!)^w}{t!(w!)^t} = \frac{(t!)^{(w-1)}}{(w!)^{(t-1)}} = \frac{(t!)^{(w-1)}}{(w!)^{(t-w)}(w!)^{(w-1)}} = \frac{[t(t-1)\cdots(w+1)]^{(w-1)}}{(w!)^{(t-w)}}$$
$$= \underbrace{\left(\frac{t^{(w-1)}}{w!}\right)\left(\frac{(t-1)^{(w-1)}}{w!}\right)\cdots\left(\frac{(w+1)^{(w-1)}}{w!}\right)}_{(t-w)-\text{factors}}.$$

Now, $\dfrac{j^{(w-1)}}{w!} \geqslant \dfrac{w+1}{2}$ for all $(w+1) \leqslant j$ since,

$$\frac{j^{(w-1)}}{w!} = \underbrace{\left(\frac{j}{w}\right)\left(\frac{j}{w-1}\right)\cdots\left(\frac{j}{3}\right)\left(\frac{j}{2}\right)}_{(w-1)-\text{times}}$$
$$\geqslant \underbrace{\left(\frac{j}{w}\right)\left(\frac{j}{w-1}\right)\cdots\left(\frac{j}{3}\right)\left(\frac{w+1}{2}\right)}_{(w-1)-\text{factors}} \geqslant \frac{w+1}{2}. \quad \square$$

Given a natural number $v > 1$ and natural numbers $a_1, a_2, \ldots, a_n$ smaller than v we may inductively define the following notation. $N_v(a_1) := \binom{v}{a_1}$. If $N_v(a_1, a_2, \ldots, a_k)$ has been defined for $1 \leqslant k < n$ then we define $N_v(a_1, a_2, \ldots, a_{k+1}) := \binom{N_v(a_1, a_2, \ldots, a_k)}{a_{k+1}}$.

With this notation we may state the following generalisation of the previous theorem.

COROLLARY 1. *Given natural numbers $a_1 \leqslant a_2 \leqslant \cdots \leqslant a_n < v$,*

$$N_v(a_1, a_2, \ldots, a_n) = \max\{N_v(a_{\pi(1)}, a_{\pi(2)}, \ldots, a_{\pi(n)}) : \pi \textit{ is a permutation of the set } \{1, 2, \ldots, n\}\}.$$

Proof. Let S_n denote the set of all permutations on $\{1, 2, \ldots, n\}$ and let $\sigma \in S_n$ be chosen so that

$$N_v(a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(n)}) = \max_{\pi \in S_n} N_v(a_{\pi(1)}, a_{\pi(2)}, \ldots, a_{\pi(n)}).$$

If $a_{\sigma(j)} = 1$ for some $1 < j \leqslant n$ then

$$N_v(a_{\sigma(1)}, \ldots, a_{\sigma(j-1)}, a_{\sigma(j)}, \ldots, a_{\sigma(n)}) = N_v(a_{\sigma(1)}, \ldots, a_{\sigma(j)}, a_{\sigma(j-1)}, \ldots, a_{\sigma(n)}).$$

Hence, if for some $1 \leqslant k \leqslant n$, $a_j = 1$ for all $1 \leqslant j \leqslant k$ then we may assume without loss of generality that $a_{\sigma(j)} = 1$ for all $1 \leqslant j \leqslant k$. That is, we can shuffle all the 1's to the front of the queue without altering the value of $N_v(a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(n)})$.

Thus, in this case, we have that $1 = a_j = a_{\sigma(j)}$ for all $1 \leqslant j \leqslant k$ and so

$$\begin{aligned} &N_v(a_1, a_2, \ldots, a_k, a_{k+1}, \ldots, a_n) < N_v(a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(k)}, a_{\sigma(k+1)}, \ldots, a_{\sigma(n)}) \\ \iff &N_v(a_{k+1}, a_{k+2}, \ldots, a_n) < N_v(a_{\sigma(k+1)}, a_{\sigma(k+2)}, \ldots, a_{\sigma(n)}). \end{aligned}$$

In this way, we see that we can restrict our attention to the case where $1 < a_1 \leqslant a_2 \leqslant \cdots \leqslant a_n < v$.

Next we show that $a_{\sigma(i)} \leqslant a_{\sigma(i+1)}$ for all $1 \leqslant i < n$. So let us suppose, in order to obtain a contradiction that for some $1 \leqslant j < n$, $a_{\sigma(j)} > a_{\sigma(j+1)}$. We consider 3 cases (mainly for notational reasons):

(i) $j = 1$; (ii) $1 < j = n-1$ and (iii) $1 < j < n-1$.

Case (i) If $j = 1$ then by Theorem 1, $N_v(a_{\sigma(1)}, a_{\sigma(2)}) < N_v(a_{\sigma(2)}, a_{\sigma(1)})$ and so

$$N_v(a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)}, \ldots, a_{\sigma(n)}) < N_v(a_{\sigma(2)}, a_{\sigma(1)}, a_{\sigma(3)}, \ldots, a_{\sigma(n)});$$

which contradicts the maximality of $N_v(a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(n)})$.

Case (ii) If $1 < j = n-1$, let $v^* := N_v(a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(j-1)})$. Then,

$$\begin{aligned} N_v(a_{\sigma(1)}, \ldots, a_{\sigma(j-1)}, a_{\sigma(j)}, a_{\sigma(n)}) &= N_{v^*}(a_{\sigma(j)}, a_{\sigma(n)}) < N_{v^*}(a_{\sigma(n)}, a_{\sigma(j)}) \text{ by Theorem 1} \\ &= N_v(a_{\sigma(1)}, \ldots, a_{\sigma(j-1)}, a_{\sigma(n)}, a_{\sigma(j)}); \end{aligned}$$

which again contradicts the maximality of $N_v(a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(n)})$.

Case (iii) If $2 \leqslant j < n-1$, let $v^* := N_v(a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(j-1)})$. Then,

$$\begin{aligned} N_v(a_{\sigma(1)}, \ldots, a_{\sigma(j-1)}, a_{\sigma(j)}, a_{\sigma(j+1)}) &= N_{v^*}(a_{\sigma(j)}, a_{\sigma(j+1)}) < N_{v^*}(a_{\sigma(j+1)}, a_{\sigma(j)}) \\ &\qquad \text{by Theorem 1} \\ &= N_v(a_{\sigma(1)}, \ldots, a_{\sigma(j-1)}, a_{\sigma(j+1)}, a_{\sigma(j)}) \end{aligned}$$

and so $N_v(a_{\sigma(1)}, \ldots, a_{\sigma(j)}, a_{\sigma(j+1)}, \ldots, a_{\sigma(n)}) < N_v(a_{\sigma(1)}, \ldots, a_{\sigma(j+1)}, a_{\sigma(j)}, \ldots, a_{\sigma(n)})$; which as before, contradicts the maximality of $N_v(a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(n)})$. Hence, $a_{\sigma(i)} \leqslant a_{\sigma(i+1)}$ for all $1 \leqslant i < n$.

Now, since both $(a_i : 1 \leqslant i \leqslant n)$ and $(a_{\sigma(i)} : 1 \leqslant i \leqslant n)$ are non-decreasing and re-arrangements of each other, it follows that $a_i = a_{\sigma(i)}$ for all $1 \leqslant i \leqslant n$. Therefore,

$$N_v(a_1, a_2, \ldots, a_n) = N_v(a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(n)}) = \max_{\pi \in S_n} N_v(a_{\pi(1)}, a_{\pi(2)}, \ldots, a_{\pi(n)}). \quad \square$$

From the proof of the Corollary we see that if $1 < a_1 < a_2 < \cdots < a_n < v$ then

$$N_v(a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(n)}) = \max_{\pi \in S_n} N_v(a_{\pi(1)}, a_{\pi(2)}, \ldots, a_{\pi(n)})$$

if, and only if, σ is the identity mapping.

QUESTION 1. Is there a simple combinatorial proof of Theorem 1?

REFERENCES

[1] SOLOMON W. GOLOMB, *Iterated Binomial Coefficients*, Amer. Math. Monthly, **87** (1980), 719–727.
[2] JULIA C. NOVAK, *Generalised Key Distribution Patterns*, PhD Thesis, Royal Holloway, University of London, (in preparation).

(Received April 27, 2009)

Warren B. Moors
Department of Mathematics
The University of Auckland
Private Bag 92019
Auckland 1142
New Zealand
e-mail: moors@math.auckland.ac.nz
URL: http://www.math.auckland.ac.nz/∼moors/

Julia C. Novak
Department of Mathematics
The University of Auckland
Private Bag 92019
Auckland 1142
New Zealand
e-mail: novakj@math.auckland.ac.nz
URL: http://www.math.auckland.ac.nz/∼jnov002/