# 609 Homework 1

**Enrique Areyan**
**January 31, 2013**

1. Suppose that $a_i = k \cdot b_i$ for all $i$ where $k$ is a constant. Then, CS inequality states:

$$\begin{array}{lcll}
\sum_{i=1}^{N} a_i b_i & \leq & \left(\sum_{i=1}^{N} a_i^2\right)^{1/2} \left(\sum_{i=1}^{N} b_i^2\right)^{1/2} & \text{subsitute } a_i = k \cdot b_i \\
\sum_{i=1}^{N} k \cdot b_i^2 & \leq & \left(\sum_{i=1}^{N} k \cdot b_i^2\right)^{1/2} \left(\sum_{i=1}^{N} k \cdot b_i^2\right)^{1/2} & \text{multiply right-hand side, take constant out} \\
k \cdot \sum_{i=1}^{N} b_i^2 & \leq & k \cdot \sum_{i=1}^{N} b_i^2 & \text{from which we can conclude that} \\
\sum_{i=1}^{N} b_i^2 & = & \sum_{i=1}^{N} b_i^2 & \text{which shows that equality holds. Q.E.D.}
\end{array}$$

Now suppose that the CS inequality is actually an equality, i.e., $\sum_{k=1}^{N} a_k b_k = \left(\sum_{k=1}^{N} a_k^2\right)^{1/2} \left(\sum_{k=1}^{N} b_k^2\right)^{1/2}$.

Then, by the proof given in class, we need only to show that $\frac{a_i}{b_i} = \frac{X_N}{Y_N} \iff \frac{a_i}{b_i} = k$, for $k$ constant. First note that since by hypothesis $X_N \neq 0$ and $Y_N \neq 0$, then we can divide by these quantities.

($\Rightarrow$) Suppose that $\frac{a_i}{b_i} = \frac{X_N}{Y_N}$. Since, both $X_N$ and $Y_N$ are fix numbers, then the ratio $\frac{X_N}{Y_N} = k$ for some constant $k$, which shows the result.

($\Leftarrow$) Suppose that $\frac{a_i}{b_i} = k$. Since by definition $X_N^2 = \sum_{k=1}^{n} a_i^2 =$ (by hypothesis) $\sum_{k=1}^{n} (kb_i)^2 = k^2 \sum_{k=1}^{n} b_i^2 = k^2 Y_n^2$, hence, $X_N^2 = k^2 Y_N^2$, from which it follows that $\frac{X_N}{Y_N} = k = \frac{a_i}{b_i}$.

The case when either all $a_i$ or all $b_i$ are zero is considered by taking the constant $k = 0$. If both all $a_i$ and $b_i$ are zero, then the result holds trivially. Q.E.D.

2. (a)

$$\begin{array}{rcll}
\binom{n}{k} & = & \frac{n!}{(n-k)!k!} & \text{By Pascal's definition of binomial coefficient} \\
& = & \frac{n!}{(n-k)!(k+n-n)!} & \text{Adding and subtracting } n \text{ from } k! \\
& = & \frac{n!}{(n-k)!(n-(n-k))!} & \text{Rearranging } k+n-n = n-(n-k) \\
& = & \binom{n}{n-k} & \text{By Pascal's definition of binomial coefficient}
\end{array}$$

Hence, this shows that $\binom{n}{k} = \binom{n}{n-k}$. Q.E.D.

(b)

$$
\begin{aligned}
\binom{n-1}{k}+\binom{n-1}{k-1} &= \binom{n-1}{n-1-k}+\binom{n-1}{k-1} && \text{By identity previously showed}\\
&= \tfrac{(n-1)!}{(n-1-(n-k-1))!(n-k-1)!}+\tfrac{(n-1)!}{(n-1-(k-1))!(k-1)!} && \text{By Pascal's def. of binomial coef.}\\
&= \tfrac{(n-1)!}{(n-1-n+k+1))!(n-k-1)!}+\tfrac{(n-1)!}{(n-1-k+1))!(k-1)!} && \text{Rearranging denominators}\\
&= \frac{(n-1)!}{k!(n-k-1)!}+\frac{(n-1)!}{(n-k)!(k-1)!} && \text{Rearranging denominators}\\
&= \frac{(n-k)(n-1)!+k(n-1)!}{(n-k)!k!} && \text{Summing fractions}\\
&= \frac{(n-1)!((n-k)+k)}{(n-k)!k!} && \text{Common factor } (n-1)!\\
&= \frac{n(n-1)!}{(n-k)!k!} && \text{By definition of } n!\\
&= \frac{n!}{(n-k)!k!} && \text{By Pascal's def. of binomial coef.}\\
&= \binom{n}{k} && \text{Q.E.D}
\end{aligned}
$$

(1.11) Prove that $\sum\limits_{x\in Y} d(x) = \sum\limits_{A\in F} |Y\cap A|$, for any $Y \subseteq X$

**Proof:** Let $Y \subseteq X$. To prove the equality, let us count in two ways the number of ones in the 0-1 matrix $M' = (m_{x,A,Y})$, where $M'$ is constructed as follow:

(i) The number of rows is $|Y|$. Each row is labeled by points $x \in Y$.

(ii) The number of columns is $|F| - b$, where $b = \sum\limits_{A\in F} i$, such that $i = 1$ if $Y \cap A \neq \emptyset$ and 0 otherwise. Each column is labeled by sets $A \in F$ such that $Y \cap A \neq \emptyset$. In other words, we include $A \subseteq F$ as a column if and only if $Y \cap A \neq \emptyset$

(iii) The entry $M' = (m_{x,A,Y}) = 1$ if and only if $x \in A$. Note that $M'$ is the matrix $M$ as defined on the proof of proposition 1.7., but with elements of $Y$ as rows and without the columns in which $A \cap Y = \emptyset$

Observe that $d(x)$ is exactly the number of 1s in the $x$-th row, and $|Y \cap A|$ is the number of 1s in the $A$-th column. Hence, the result follows.

(1.12) First note that the second equality, i.e.,

$$\sum_{A\in F}\sum_{x\in A} d(x) = \sum_{A\in F}\sum_{B\in F} |A\cap B|$$

follows from the proof above (1.11), but restricting our attention to a particular family, i.e., set $B$ in (1.12) would be set $A$ in (1.11); and set $Y$ in (1.11) becomes set $A$ in (1.12). It remains to show the first equality, i.e.,

$$\sum_{x\in X} d(x)^2 = \sum_{A\in F}\sum_{x\in A} d(x)$$

and we would have proven the result, since the final equality, i.e.,

$$\sum_{x\in X} d(x)^2 = \sum_{A\in F}\sum_{B\in F} |A\cap B|$$

follows from transitive property of equality.
So, let us prove the first equality.

Using the double counting principle, let us count in two ways the sum of the squares of the degrees of the vertices in a hypergraph.. The first way is just the definition, i.e., $\sum\limits_{x\in X} d(x)^2$.

The second way is to count, for each set in the family $A \in F$, the degree of its vertices $d(x)$, $x \in A$, i.e., $\sum\limits_{A\in F}\sum\limits_{x\in A} d(x)$. Since the degree of a vertex is just the number of subsets of the family to which it belongs, we will be counting the degree of a vertex $d(x)$ as many times as $x \in A$ for $A \in F$, which is just by definition $d(x)$. Hence, the second count is $\sum\limits_{x\in X} d(x)d(x) = \sum\limits_{A\in F}\sum\limits_{x\in A} d(x) = \sum\limits_{x\in X} d(x)^2$ by the double counting principle.

Q.E.D.

(1.2) Let $k \leq n \in \mathbb{N}$ and let $P(n,k)$ be the product of $k$ consecutive numbers starting in $n$.
We can write $P(n,k) = n\cdot(n-1)\cdots(n-k+1)$. But then,

$$\begin{aligned}
n\cdot(n-1)\cdots(n-k+1) &= n\cdot(n-1)\cdots(n-k+1)\tfrac{(n-k)\cdot(n-k-1)\cdots 1}{(n-k)\cdot(n-k-1)\cdots 1} && \text{Mult. \& div. by the same number.}\\
&= \frac{n!}{(n-k)!}\frac{k!}{k!} && \text{Multiplying \& dividing by } k!\\
&= \binom{n}{k}k! && \text{By def. of binomial coefficient}
\end{aligned}$$

Hence, $P(n,k) = \binom{n}{k}k!$. Since we know that $\binom{n}{k}$ is a natural number for any $k \leq n \in \mathbb{N}$, then we conclude that $k!|P(n,k)$, and in fact $\frac{P(n,k)}{k!} = \binom{n}{k}$. Note that you should pick $n$ to be the biggest number where you want your product to end, and $k$ the number of consecutive numbers you wish to include in the product. For instance, if you want the product $5\cdot 4\cdot 3\cdot 2$, you should pick $P(n=5, k=4)$.

(1.5) Prove that $\sum\limits_{k=1}^{n} k\binom{n}{k} = n2^{n-1}$.

**Proof:** To prove this identity we can count in two ways the set $P = \{(x,M) : x \in M \subseteq \{1,...,n\}\}$.

<u>First count</u>: We can partition the set $P$ by considering pairs in which $|M| = 1,2,...,n$. Note that since there is nothing in the empty set, we do not need to count the pairs where $|M| = 0$.
How many pairs are there such that $|M| = 1$? By definition, there are $\binom{n}{1}$ 1-element subsets of $\{1,2,...,n\}$. By the product rule there are $1\cdot\binom{n}{1}$ many pairs.
How many pairs are there such that $|M| = 2$? By definition, there are $\binom{n}{2}$ 2-element subsets of $\{1,2,...,n\}$. By the product rule there are $2\cdot\binom{n}{2}$ many pairs.
In general, how many pairs are there such that $|M| = i$, for $1 \leq i \leq n$?. By definition, there are $\binom{n}{i}$ $i$-element subsets of $\{1,2,...,n\}$. By the product rule there are $i\cdot\binom{n}{i}$ many pairs.
We want all possible pairs so we need to take the sum, i.e.,

$$|P| = \sum_{k=1}^{n} k\binom{n}{k}$$

<u>Second count:</u> Let $P' = \{(x,M) : x \in \{1,...,n\} \wedge M \subseteq \{1,...,n\}\}$, i.e., the set of pairs with no restrictions.
Since any element is either a member of $M \subseteq \{1,2,...,n\}$ or not, we know that $|P'| = 2|P|$. To count the cardinality of $|P'|$, just use the product rule to count the number of elements $n$ followed by the number of possible subsets of $\{1,2,...,n\}$ which we know to be $2^n$. Therefore, $|P'| = n\cdot 2^n \Rightarrow |P| = \frac{n\cdot 2^n}{2}$, i.e.,

$$|P| = n\cdot 2^{n-1}$$

By the double counting principle, the first and second count must agree. Hence, $\sum\limits_{k=1}^{n} k\binom{n}{k} = n\cdot 2^{n-1}$

(1.9) To prove the Cauchy-Vandermonde identity we can apply the double counting principle. We will count the number of $k$-element subsets a set with $p+q$ elements.

<u>First count</u>: By definition, we know that a set of $p+q$ elements has $\binom{p+q}{k}$ number of $k$-element subsets.

Second count: Partition the set of $p+q$ into sets of $p$ and $q$ elements respectively. To count the number of $k$-element subsets of a set with $p+q$ elements, we can first count the number of $i$-element subsets of the set with $p$ elements, where $0 \leq i \leq k$. By definition there are these many choices $\binom{p}{i}$ for each $i$. Now we need to select elements of the set with $q$ elements. To complete a subset of $k$ elements, we need to select $k-i$ elements of the $q$ set. There are this many choices $\binom{q}{k-i}$. Finally, by the product rule, we can form subsets of $k$-elements out of the initial $p+q$ set by taking the product $\binom{p}{i}\binom{q}{k-i}$. So, for each $i$, this product is the number of $i$-elements subsets of a set with $p+q$ elements. Hence, to count the total number we just take the sum: $\sum_{i=0}^{k} \binom{p}{i}\binom{q}{k-i}$.

By the double counting principle, the first and second count must agree. Hence, $\binom{p+q}{k} = \sum_{i=0}^{k} \binom{p}{i}\binom{q}{k-i}$

(1.10)

$$\begin{aligned}
\binom{2n}{n} &= \binom{n+n}{n} && \text{Since } 2n = n+n \\
&= \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-k} && \text{By Cauchy-Vandermonde identity} \\
&= \sum_{k=0}^{n} \binom{n}{k}\binom{n}{n-(n-k)} && \text{Since } \binom{n}{k} = \binom{n}{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k}\binom{n}{k} && \text{Algebraic manipulation, taking product} \\
&= \sum_{k=0}^{n} \binom{n}{k}^2 && \text{Which shows the result. Q.E.D.}
\end{aligned}$$

(1.12) Two different proofs:

Algebraic:

$$\begin{aligned}
\binom{n}{k}\binom{k}{l} &= \frac{n!}{(n-k)!k!}\frac{k!}{(k-l)!l!} && \text{Pascal definition of binomial coefficient} \\
&= \frac{n!}{(n-k)!}\frac{1}{(k-l)!l!}\frac{(n-l)!}{(n-l)!} && \text{Canceling } k! \text{ and mult. and div. by } (n-l)! \\
&= \frac{n!}{(n-l)!l!}\frac{(n-l)!}{(n-k)!(k-l)!} && \text{Rearranging denominator} \\
&= \frac{n!}{(n-l)!l!}\frac{(n-l)!}{(n-l-k+l)!(k-l)!} && \text{Adding and subtracting } l \text{ in 1st factor of 2nd denominator} \\
&= \binom{n}{l}\binom{n-l}{k-l} && \text{Pascal definition of binomial coefficient}
\end{aligned}$$

Double Counting: Count in two ways the number of pairs $(L, K)$ of subsets of $\{1, ..., n\}$ such that $L \subseteq K, |L| = l, |K| = k$.

First count: By definition there are $\binom{n}{k}$ many possible $k$-elements subsets of the set $\{1, 2, ..., n\}$. Also, by definition, there are $\binom{k}{l}$ many possible $l$-elements subsets of the set $\{1, 2, ..., k\}$. By the product rule, there are $\binom{n}{k}\binom{l}{l}$ pairs $(L, K)$ with the given conditions.

Second count: By definition there are $\binom{n}{l}$ many possible $l$-elements subsets of the set $\{1, 2, ..., n\}$. We have already selected $l$ elements we wish to include as the first member of the pair, therefore, we need to subtract

$l$ from $n$ and choose $(k-l)$-elements subsets to complete the pair, i.e., $\binom{n-l}{k-l}$. Finally, by the product rule, there are $\binom{n}{k}\binom{n-l}{k-l}$ pairs $(L,K)$ with the given conditions.

From the Double counting principle it follows that the first and second count must agree, hence,

$$\binom{n}{k}\binom{k}{l} = \binom{n}{l}\binom{n-l}{k-l}$$

(1.14) Let $p$ be a prime number.

(i) Let $1 \le k < p$. By definition: $\binom{p}{k} = \frac{p!}{(p-k)!k!} = \frac{p(p-1)\cdots(p-k+1)}{k!} \Rightarrow \binom{p}{k}k! = p(p-1)\cdots(p-k+1)$.
Let $(p-1)\cdots(p-k+1) = r$. Then we can write more compactly: $\binom{p}{k}k! = p\cdot r$ where $r \in \mathbb{N}$.
In particular, this means that $p|\binom{p}{k}k!$. Since $p$ is a prime, by Euclid's Lemma we have that $p|\binom{p}{k}$ or $p|k!$

Claim: it is not possible that $p|k!$. Proof: By definition $k! = k(k-1)\cdots 1$. Since $p$ is a prime, by Euclid's lemma it would have to divide some $i$ for $1 \le i \le k$. But this is impossible! Suppose that indeed there exists $i$ such that $p|i$ for $0 < i < p$. Then $i = p\cdot q$, for some $q \in \mathbb{N}$. Then $i > p$, a contradiction. Hence, $p$ does not divide $k!$.

Since $p$ does not divide $k!$ then it must be the case that $p|\binom{p}{k} \iff \binom{p}{k} \equiv 0 \pmod{p}$. Q.E.D.

(ii) Let $1 \le k \le n < p$. By definition: $\binom{n}{k} = \frac{n!}{(n-k)!k!} = \frac{n(n-1)\cdots(n-k+1)}{k!} \Rightarrow \binom{n}{k}k! = n(n-1)\cdots(n-k+1)$.
Divide both sides of the last identity by $p$:

$$\frac{\binom{n}{k}k!}{p} = \frac{n(n-1)\cdots(n-k+1)}{p}$$

To assert that $p|\binom{n}{k}k!$ is equivalent to assert that $p|n(n-1)\cdots(n-k+1)$. By Euclid's lemma, if $p|n(n-1)\cdots(n-k+1)$ then $p|(n-i)$ for some $0 \le i \le k+1$. But it is not the case that $p|(n-i)$ since $p > n-i$ for $0 \le i \le k+1$, since by hypothesis $k$ is at least 1 and $n < p$. Therefore $p \nmid n(n-1)\cdots(n-k+1) \iff p \nmid \binom{n}{k}k!$. Finally, since the converse of Euclid's lemma is also true, we can conclude that $p \nmid k!$ and $p \nmid \binom{n}{k} \iff \binom{n}{k} \not\equiv 0 (\text{mod } p)$

(1.15) Proof by induction. Let $S(n)$ be the following statement: $n^p \equiv p \pmod{p}$, where $p$ is a prime number.
We want to show that $S(n)$ is true for all $n \in \mathbb{N}$.

Base case: $S(1) : 1^p = 1 \equiv 1 \pmod{p}$, so base case holds true.

Inductive Step: Suppose that $S(n)$ is true. We want to show that $S(n+1)$ is true, i.e., we want to prove that $(n+1)^p \stackrel{?}{=} n+1 \pmod{p}$.

We begin by considering:

$$\begin{aligned}
(n+1)^p &= \sum_{k=0}^{p}\binom{p}{k}n^{p-k}1^k && \text{By binomial Theorem}\\
&= n^p + \sum_{k=1}^{p-1}\binom{p}{k}n^{p-k}1^k + 1 && \text{Factoring out the first and last element of the sum}\\
&\equiv n^p + 0 + 1 \pmod{p} && \text{By previous exercise (1.15(i)) since } 1 \le k < p\\
&= n^p + 1 && \text{Working the sum}\\
&\equiv n + 1 \pmod{p} && \text{By Inductive Hypothesis. Q.E.D}
\end{aligned}$$