Pontificia Universidad Católica de Chile
Escuela de Ingeniería
Departamento de Ciencias de la Computación

Ayudante: Nicholas Mc-Donnell
Email: namcdonnell@uc.cl

Ayudantía 03

Combinatoria y Probabilidad

IIC3253 – Criptografía

Fecha: 2021-04-07

1. Combinatoria

La combinatoria es el área de las Matemáticas que principalmente trata como contar cosas, hay varios resultados útiles para este curso, varios de los cuales estarán en está ayudantía.

1.1. Notación Básica

Definición 1.1 (Cardinalidad)**.** Dado un conjunto A se denota $|A|$ a su cardinalidad. Para conjuntos finitos $|A|$ es un número natural (entero mayor o igual a cero).

1.2. Teoremas Básicos

No se presentará demostración de los siguientes teoremas.

Teorema 1.1 (Biyección)**.** *Dados dos conjuntos A y B, existe $f : A \to B$ biyectiva si y solo si $|A| = |B|$.*

Teorema 1.2 (Exclusión/Inclusión)**.** *Dado dos conjuntos finitos A y B, se tiene que*

$$|A \cup B| = |A| + |B| - |A \cap B| .$$

Teorema 1.3 (Principio Múltiplicativo)**.** *Dado dos conjuntos finitos A y B, se tiene que*

$$|A \times B| = |A| \cdot |B|$$

Teorema 1.4 (Principio de la División)**.** *Dado dos conjuntos finitos A, B y una función $f : A \to B$ tal que para todo $y \in B$ su preimagén cumple que $|f^-1\{y\}| = d$, entonces se tiene que*

$$|B| = \frac{|A|}{d}$$

Teorema 1.5 (Principio de Palomar)**.** *Dado dos conjuntos no vacíos A y B tales que $|A| > |B|$, no existe una función inyectiva de A a B, equivalentemente para toda función $f : A \to B$ existen dos elementos distintos $x, y \in A$ tales que $f(x) = f(y)$.*

Teorema 1.6 (Inducción)**.** *Dado alguna proposición $P(n)$ sobre un número natural n, sí se tiene que $P(0) \wedge (\forall n \in \mathbb{N} P(n) \implies P(n+1))$, entonces se tiene que $\forall n \in \mathbb{N} P(n)$.*

1.3. Permutaciones

Definición 1.2 (Permutación)**.** Dado un conjunto A el conjunto de permutaciones S_A consiste en las biyecciones de A en si mismo.

Nota. *Para efectos del curso, solo se considera permutaciones donde A es un conjunto finito, más aún, en general se asume que $A = \{0,1\}^n$ para algún n, o sea, el conjunto de binary strings de largo n. Pero para está ayudantía solo se asume que A es finito, salvo que se diga lo contrario.*

Teorema 1.7. *Si $|A| = n$, entonces $|S_A| = n!$*

Demostración. Se usa inducción:

$n = 1$ Como $|A| = 1$, la única función biyectiva de A en si misma es la identidad, por lo que $|S_A| = 1$.

$n \implies n+1$ Dado $|A| = n+1$, se escribe $A = A' \cup \{a\}$ donde $|A'| = n$, toda permutación π en $S_{A'}$ se puede extender de dos formas a una permutación en S_A, fijando a (i.e. $\pi(a) = a$) y no fijando a (i.e. $\pi(a) \neq a$). El primer caso nos da $|S_{A'}|$ permutaciones, que por hipótesis inductiva son $n!$. El segundo caso nos da $|A'| \cdot |S_{A'}|$, ya que $\pi(a)$ tiene que ser un elemento de A'[1], por lo que por hipotesis inductiva son $n \cdot n!$. Juntando ambos casos nos da $|S_A| = n! + n \cdot n! = (n+1)n! = (n+1)!$.

□

Nota. *Se denota S_n a las permutaciones sobre el conjunto $\{1, \ldots, n\}$, y se nota que todo resultado sobre S_n se extiende naturalmente a S_A cuando $|A| = n$.*

[1]Para extender en este caso se toma el elemento $b \in A'$ tal que $pi(b) = pi(a)$, y se redefine $\pi(b) = a$.

Teorema 1.8. *El conjunto* $S_{n,k} = \{\pi \in S_n : \forall i \leq k\, \pi(i) = i\}$ *tiene* $(n-k)!$ *elementos. Y de forma más general dados* $a_1, \ldots, a_k \in \{1, \ldots, n\}$ *se tiene que* $|\{\pi \in S_n : \forall i \leq k\, \pi(i) = a_i\}| = (n-k)!$.

Demostración. Se toma $f : S_{n-k} \to S_{n,k}$ donde $f(\pi)$ cumple que $\forall i, j \leq n-k\ \pi(i) = j$ si y solo si $f(\pi)(i+k) = j+k$, y $\forall i \leq k\, f(\pi)(i) = i$. Se nota que f es biyección, por lo que $|S_{n,k}| = |S_{n-k}| = (n-k)!$.

La segunda parte del teorema de una extensión natural de la demostración anterior. □

1.4. Variación

Definición 1.3 (Variación)**.** Se denota $P(n,k)$ a la cardinalidad de $f : A \to B \mid f$ inyectiva, donde $|A| = k$, $|B| = n$ y $k \leq n$.

Teorema 1.9. *Dado* $n, k \in \mathbb{N}$ *tales que* $k \leq n$ *se tiene que*

$$P(n,k) = \frac{n!}{(n-k)!}$$

Demostración. Se usa inducción sobre k. Para el caso $k = 0$, solo hay una función inyectiva (la función con dominio vacío). Para el caso inductivo, se tiene A de cardinalidad $k+1$, sea $a_0 \in A$, entonces una función inyectiva de A a B se construye eligiendo una imagén $b_0 \in B$ para a_0, y eligiendo una función inyectiva de $A \setminus \{a_0\}$ a $B \setminus \{b_0\}$. Hay n formas de elegir b_0, y como $|A \setminus \{a_0\}| = k-1$ y $|B \setminus \{b_0\}| = n-1$, por hipótesis inductiva hay $\frac{(n-1)!}{((n-1)-(k-1))!}$ formas de elegir una función inyectiva, se tiene lo pedido. □

Corolario. *Dado* S *un conjunto finito, con* $|S| = n$*. La cantidad de formas de elegir* k *elementos de* S *sin repeticiones es* $\frac{n!}{(n-k)!}$.

Demostración. Elegir k elementos de S sin repeticiones es equivalente a elegir un función inyectiva desde $\{1, \ldots, k\}$ a S, por lo que por el teorema anterior se tiene lo pedido. □

1.5. Combinación

Definición 1.4 (Combinación)**.** Se denota $C(n,k) = \binom{n}{k}$ a la cardinalidad de $\{S \subseteq A : |S| = k\}$ donde $|A| = n$. De forma más coloquial "de cuantas formas se pueden elegir k elementos de n". Se nota que $\binom{n}{0} = \binom{n}{n} = 1$.

Teorema 1.10. *Dado* $n, k \in \mathbb{N}$ *tales que* $1 \leq k \leq n$*, se tiene que*

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \text{ y } \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Demostración. Dado un conjunto A de cardinalidad n, se quiere elegir un subconjunto S de cardinalidad k, este conjunto de puede construir de la siguiente forma, tomas un elemento $a_0 \in A$ y lo agregas, así queda el problema de elegir un subconjunto de cardinalidad $k-1$ del conjunto $A \setminus \{a_0\}$, o no lo agregas y tienes que elegir un subconjunto de cardinalidad k del conjunto $A \setminus \{a_0\}$. Con lo que se tiene que $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Se nota que $P(n,k) = C(n,k) \cdot P(k,k)$, en otras palabras elegir k elementos de n sin repetición es lo mismo que elegir un subconjunto de cardinalidad k y ordenarlo de alguna forma. Por lo tanto $\binom{n}{k} = C(n,k) = \frac{P(n,k)}{P(k,k)} = \frac{n!}{(n-k)!} \cdot \frac{1}{k!} = \frac{n!}{k!(n-k)!}$. □

2. Probabilidad

La probabilidad es el área de las Matemáticas que principalmente trata de cuantificar númericamente cuan probable es un evento, o cuan probable una proposición es verdad.

Nota. *Para efectos del curso se verá una versión limitada de probabilidad, específicamente probabilidad finita, donde se tomarán dos conjuntos finitos $A \subseteq B$, donde A es un evento en el universo B. Una consecuencia de eso es que $P(A) = \frac{|A|}{|B|}$.*

2.1. Notación

Definición 2.1. Se denota $\underset{s \leftarrow B}{P}(A(s))$ a la probabilidad del evento $A(s)$ que depende de un s elegido con alguna distribución de B.

2.2. Teoremas y Definiciones Básicas

No se presentará demostración de los siguientes teoremas.

Definición 2.2 (Eventos Independientes)**.** Se dice que dos eventos A y B son independientes si y solo si $P(A \cap B) = P(A) \cdot P(B)$.

Definición 2.3 (Eventos Mutuamente Excluyentes)**.** Se dice que dos eventos A y B son mutuamente excluyentes si y solo si $P(A \cap B) = 0$.

Teorema 2.1. *Dado dos eventos A y B se tiene queda*

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

Definición 2.4 (Probabilidad Condicional)**.** Dado dos eventos A y B se denota $P(A \mid B)$ a la probabilidad de que pase el evento A dado que pasa el evento B. Más aún $P(A \mid B) = \frac{P(A \cup B)}{P(B)}$.

Teorema 2.2 (Bayes)**.** *Se tiene que*

$$P(A \mid B) = \frac{P(B \mid A) \cdot P(A)}{P(B)}$$

2.3. Problemas

Teorema 2.3. *Dado $w_1, \ldots, w_k \in A$ y $w'_1, \ldots, w'_k \in A$, tal que $i \neq j \implies (w_i \neq w_j) \wedge (w'_i \neq w'_j)$, donde $k \leq |A| = n$. Se tiene que*

$$\underset{\pi \leftarrow S_A}{P}(\forall i \, \pi(w_i) = w'_i) = \frac{(n-k)!}{n!}$$

Demostración. Sea $B = \{\pi \in S_A \mid \forall i \, \pi(w_i) = w'_i\}$, por teorema 1.8 $|B| = (n-k)!$, por lo que se tiene lo pedido. □

Corolario. *La probabilidad de que una permutación fije k elementos es $\frac{1}{k!}$.*