

PROBABILITY IS EXPECTATION FOUNDED UPON PARTIAL KNOWLEDGE. A PERFECT ACQUAINTANCE WITH ALL THE CIRCUMSTANCES AFFECTING THE OCCURRENCE OF AN EVENT WOULD CHANGE EXPECTATION INTO CERTAINTY, AND LEAVE NETHER ROOM NOR DEMAND FOR A THEORY OF PROBABILITIES.

GEORGE BOOLE

PURE MATHEMATICS IS, IN ITS WAY, THE POETRY OF LOGICAL IDEAS.

ALBERT EINSTEIN

THE MOST PAINFUL THING ABOUT MATHEMATICS IS HOW FAR AWAY YOU ARE FROM BEING ABLE TO USE IT AFTER YOU HAVE LEARNED IT.

JAMES NEWMAN



ALBERTO GONZÁLEZ TREJO

# PROBABILIDAD PROCESOS ALEATORIOS E INFERENCIA

CENTRO DE INVESTIGACIÓN EN COMPUTACIÓN  
INSTITUTO POLITÉCNICO NACIONAL



## *Contents*

*Tarea 1* 11

*Tarea 2* 15

*Tarea 3* 20

*Tarea 4* 22

*Tarea 5* 25

*Tarea 6* 28

*Tarea 7* 30

*Tarea 8* 34

*Tarea 9* 37

*Tarea 10* 39

*Tarea 11* 41

*Tarea 12* 43

*Tarea 13* 47

*Tarea 14* 51

*Tarea 15* 56

*Tarea 16* 58

*Tarea 17* 59

*Tarea 18* 62

*Propuesta Examen* 65

*Bibliography* 72

*Dedicated to those who appreciate Mathematics  
and its beauty*



## *Introducción*

Este pequeño libro de apuntes recopila las tareas, notas y ejercicios tomados en la sesión de Probabilidad, Procesos aleatorios e Inferencia en el Centro de Investigación en Computación del Instituto Politécnico Nacional en la Ciudad de México [2017].



# Tarea 1

LAS NOTAS que se incluyen en esta capítulo constituyen una breve introducción y motivación para el lector relacionadas con la Probabilidad, su estudio y algunas aplicaciones, así como algunas definiciones formales y ejemplos.

## *¿Por qué estudiar Probabilidad?*

Las matemáticas son la lógica de la certidumbre, la probabilidad es la lógica de lo incierto. La probabilidad es extremadamente útil en una gran variedad de campos de estudio debido a que nos provee de herramientas para entender y explicar variaciones, separar ruido de señales y modelar fenómenos complejos <sup>1</sup>. Para dar un pequeño ejemplo de la lista que continuamente sigue creciendo tenemos las siguientes aplicaciones:

- Estadística: La probabilidad es el fundamento y el lenguaje de la estadística, permite muchos métodos poderosos donde se emplean datos para aprender acerca del mundo.
- Física: Einstein dijo una vez: "*Dios no juega a los dados con el Universo*", pero el entendimiento actual de la Física Cuántica implícamente ampliamente probabilidad en su nivel más fundamental.
- Ciencias de la Computación: Los algoritmos aleatorios llevan a cabo elecciones aleatorias mientras son ejecutados, y en muchas aplicaciones importantes son más sencillos y eficientes que cualquier alternativa determinista. La probabilidad también juega un rol esencial en el estudio del desempeño de algoritmos, y es ampliamente empleada en Aprendizaje Máquina e Inteligencia Artificial.

<sup>1</sup> Joseph K. Blitzstein and Jessica Hwang. *Introduction to Probability*. CRC Press, first edition, May 2015

## *¿Qué es la Probabilidad?*

La teoría de la probabilidad es la rama de las matemáticas que estudia los fenómenos que dependen de casos fortuitos, esta clase de fenómenos se conocen como aleatorios. La probabilidad es el estudio de los

<sup>2</sup> Ph.D Hwei P. Hsu. *Probability, Random variables, and Random Processes*. McGraw-Hill, United States of America, 1997

fenómenos puramente aleatorios, es decir, estudia la mayor o menor posibilidad de que ocurra un determinado suceso. En otras palabras, su noción viene de la necesidad de medir o determinar cuantitativamente la certeza o duda de que un suceso dado ocurra o no <sup>2</sup>. Ésta establece una relación entre el número de sucesos favorables y el número total de sucesos posibles.

Existen diferentes interpretaciones de la probabilidad las cuales se listan a continuación:

- Clásica: Está basada en el concepto de resultados igualmente verosímiles, es decir se asume que cada uno de los resultados tiene la misma oportunidad de ocurrir. Se ha definido a lo largo de la historia como la cantidad de formas en que podría ocurrir un evento entre el total de posibles resultados.
- Frecuentista: La probabilidad de un evento es interpretada como la frecuencia relativa con la que se obtendría ese resultado si el proceso se repitiera un gran número de veces, en condiciones similares.
- Subjetiva: Esta interpretación tiene que ver con el grado de conocimiento de la persona sobre el evento y en base a esta experiencia la persona asigna una probabilidad conveniente.
- Geométrica: Se describe la posibilidad de que un punto se encuentre en una parte de un segmento de línea o en algún punto de una región. La probabilidad de que  $X$  esté en el segmento  $PR$  de una línea  $PQ$  se define como:

$$P(PR) = \frac{\text{longitud de } PR}{\text{longitud de } PQ}$$

- Axiomática: Sea  $S$  un ejemplo de espacio muestral y sea  $A$  un evento en  $S$ . La definición axiomática indica que  $P(A)$  del evento  $A$  es un número real asignado a  $A$  el cual satisface los siguientes 3 axiomas:

$$P(A) \geq 0$$

$$P(S) = 1$$

$$P(A \cup B) = P(A) + P(B) \text{ if } A \cap B = \emptyset$$

### *Definiciones*

En la siguiente sección se listan algunas definiciones importantes.

### *Suerte*

Resultado favorable para un suceso poco probable. Un curso o una serie de tales acontecimientos considerados como algo que ocurre por casualidad; oportunidad; destino, fortuna, a menudo, uno de habitual o fortuna característica.

### *Coincidencia*

una coincidencia expresa una semejanza entre dos partes. Un acontecimiento imprevisible, algo inesperado y que tiene un componente poco probable en un experimento que no se puede determinar con exactitud el resultado.

### *Azar*

Es un fenómeno que ocurre cuando existe una serie numérica que no puede obtenerse mediante un algoritmo de manera exacta. En un sistema indeterminista no se puede determinar de antemano cuál será el suceso siguiente.

### *Incertidumbre*

La incertidumbre refiere la duda o perplejidad que se tiene sobre un asunto o cuestión. Un estado por lo general dominado por la duda y que se relaciona con el enfrentamiento de un fenómeno aleatorio.

### *Riesgo*

Se denomina riesgo a la probabilidad de ocurrencia de un evento, típicamente adverso a lo que esperamos o necesitamos de cierto evento determinado.

### *Experimento aleatorio*

En el estudio de la probabilidad, se define como experimento cualquier proceso de observación. Los resultados de una observación son llamados *resultados del experimento*. Un experimento es llamado *experimento aleatorio* si su resultado no puede ser predecido. Ejemplos típicos de experimentos aleatorios son el lanzamiento de un dado, el lanzamiento de una moneda o escoger una carta de un mazo <sup>3</sup>.

<sup>3</sup> Ph.D Hwei P. Hsu. *Probability, Random variables, and Random Processes*. McGraw-Hill, United States of America, 1997

### *Duda*

Escepticismo metódico que anima a considerar escrupulosamente todos los detalles antes de decidirse a expresar un juicio sobre cualquier asunto.

*Fortuna*

Muy asociada con la suerte, representa un resultado favorable o deseado relativamente, de un fenómeno aleatorio cuya probabilidad de que el evento ocurra es menor a la de que ocurra el evento contrario o adverso a lo esperado.

*Oportunidad*

La oportunidad puede referirse a la presencia de un fenómeno aleatorio en la cual se espera ya sea uno y otro resultado.

## *Tarea 2*

LAS NOTAS que se incluyen en esta capítulo conforman la tarea 2, la cual consiste en ejemplos de experimentos deterministas y no deterministas, 2 reseñas de 2 capítulos del libro *The math book*, una breve opinión acerca del capítulo o del libro *The Simpsons and their mathematical secrets* y una reseña del capítulo *Repealing the Law of Averages* del libro *How to cut a cake*.

### *Ejemplos de experimentos deterministas*

Cuando se conoce el resultado del experimento antes de llevarlo a cabo, se dice que se trata de un experimento determinista.

- Lanzar una pelota de *baseball* hacia arriba y saber que subirá durante un determinado intervalo de tiempo pero después caerá.
- Al calentar agua, esta ebullirá cuando alcance los 100 grados celcius.
- Acelerar un cuerpo y saber que la aceleración es directamente proporcional a la fuerza ejercida e inversamente proporcional a la masa de dicho cuerpo.
- Predecir la cantidad de dinero que se tendrá después del transcurso de un lapso de tiempo en una cuenta bancaria conociendo la tasa de interés y el monto inicial.
- Predecir lo que pasará cuando mi novia me invita a ver una película a su casa.
- Conocer el resultado de mi examen departamental final de probabilidad después de estudiar mucho.

### *Ejemplos de experimentos no deterministas*

En un experimento no determinista, es posible repetir el experimento en forma indefinida sin cambiar esencialmente las condiciones y es posible describir el conjunto de todos los resultados posibles del experimento,

sin embargo no es posible conocer el resultado del experimento de antemano.

- Se lanza un dado y se observa el número que aparece en la cara superior.
- Se lanza una moneda cuatro veces y se encuentra el número total de caras obtenidas.
- Se fabrican artículos en una línea de producción y se cuenta el número de artículos defectuosos producidos en un periodo de 24 horas.
- Se lanza un proyectil, después de un tiempo determinado  $t$ , se anotan los tres componentes de la velocidad  $v_x, v_y, v_z$ .
- Medir la resistencia a la tensión de una barra de acero.
- De una urna que contiene sólo esferas negras, se escoge una esfera y se anota su color.

### *Ant Odometer*

El experimento llevado a cabo con la hormiga *Cataglyphis fortis* para verificar la hipótesis que propone que las hormigas poseen un tipo de computadora en su cerebro que les permite calcular el número de pasos y así poder medir distancias y regresar a su nido me parece interesante, ya que al modificar sus patas, sus pasos pueden ser más largos o más cortos, y si las hormigas modificadas que parten desde el nido logran regresar a él exitosamente y las hormigas que son colocadas a mitad de camino no logran llegar al nido, se puede concluir que las hormigas poseen un mecanismo similar a un odómetro. Sin embargo, creo que deben tomarse en cuenta los experimentos que se han llevado a cabo relacionados con las feromonas de las hormigas y el cómo influyen en su comportamiento.

### *Primates count*

Creo que en la naturaleza existen diferentes mecanismos que se fueron perfeccionando a lo largo de la cadena evolutiva, dichos mecanismos permiten que cada especie sea capaz de reconocer patrones, adaptarse y sobrevivir. En mi punto de vista, creo que nuestra capacidad superior de reconocer patrones es lo único que nos separa de los llamados *animales irracionales*. Creo que el mecanismo que tienen los animales mencionados en este capítulo es simplemente de memoria, no se relaciona con alguna etapa cognitiva.



Figure 1: Hormiga del desierto modificada.



Figure 2: Aparentemente los primates tienen un sentido de los números.

### *Cicada-Generated Prime Numbers*

La teoría de la evolución siempre me ha parecido fascinante, el hecho de adaptarse al paso de los años es una idea muy radical y el ir descubriendo el por qué cada especie se comporta de la manera que lo hacen me parece interesante. El ejemplo que se trata en este capítulo nos expone un fenómeno que nos permite imaginarnos cómo las matemáticas pueden ir modelando diversos comportamientos de especies animales, en este caso las cigarras salen del suelo en períodos que corresponden a los números primos 13 y 17. El investigador propone que dicho comportamiento se debe a que de esta manera las cigarras evaden generaciones de depredadores de vida más corta, permitiendo que sobreviva su especie. En mi opinión creo que es posible que dicho comportamiento sea un resultado de la evolución, sin embargo, creo que aún hay muchas cosas por investigar y acotar el fenómeno estudiado, mi pregunta es la misma que propone el autor, *¿Por qué los números 13 y 17?*.



Figure 3: Algunas cigarras emergen del suelo en períodos sincronizados que corresponden usualmente a los números primos 13 y 17.

*How to cut a cake?***PREFACIO**

Ocasionalmente, cuando me siento inusualmente relajado y mi mente comienza a divagar, me pregunto cómo sería el mundo si todos disfrutaran de las matemáticas tanto como yo lo hago.

<sup>4</sup> Ian Stewart. *How to cut a cake and other mathematical conundrums*. OXFORD University Press, first edition, 2006

By Ian Stewart <sup>4</sup>.

*Repealing the Law of Averages*

Según una creencia popular que con frecuencia recibe el nombre de «ley de los promedios», a largo plazo los sucesos aleatorios tienden a nivelarse. Por tanto, ¿debería usted apostar a aquellos números de la lotería que no salen con tanta frecuencia como los demás? La respuesta de la teoría de probabilidades es un rotundo «no». No obstante, sí hay un sentido en el que los sucesos aleatorios realmente se nivelan a largo plazo. Pero eso no le ayudará a ganar la lotería. <sup>5</sup>

<sup>5</sup> Ian Stewart. *How to cut a cake and other mathematical conundrums*. OXFORD University Press, first edition, 2006

Tomando como ejemplo el experimento clásico de lanzar una moneda, podemos decir que la probabilidad de que salga cara es  $\frac{1}{2}$  y la probabilidad de que salga cruz es  $\frac{1}{2}$ . Podemos pensar que si lanzamos la moneda 100 veces, es probable que tengamos un número aproximado de caras y de cruces similar, y mientras mayor sea el número de lanzamientos vamos a aproximarnos cada vez más a un número igual de caras y de cruces. Esta creencia es la llamada «ley de los promedios», la cual es completamente refutable debido a que el experimento de lanzar una moneda  $n$  veces no tiene memoria, es decir, el 2do lanzamiento no depende del 1er lanzamiento y así sucesivamente.

La teoría de los números largos establece que las frecuencias con las cuáles sucede un evento, a la larga, serán muy cercanas a sus probabilidades. Esto nos da pauta para poder definir que un experimento como el mencionado anteriormente, se puede llevar a cabo un gran número de veces y la frecuencia se acercará a la probabilidad de dicho evento.

*The Simpsons and their mathematical secrets*

By Simon Singh <sup>6</sup>.

*The Truth about the Simpsons*

No soy gran fan de esta serie, sin embargo he visto algunos capítulos y ya me había percatado de ciertas peculiaridades referentes a temas científicos e incluso filosóficos. Al enterarme realmente quiénes están detrás de la creación de la serie televisiva más exitosa de todos los

<sup>6</sup> Simon Singh. *The Simpsons and their mathematical secrets*. BLOOMSBURY, 2009

tiempos me queda claro que tengo que ver la serie completa. Me parece de particular interés esa relación de las ciencias (particularmente las matemáticas) con actividades recreativas, permitiendo así una mayor inmersión e interés del público en general hacia dichas áreas.

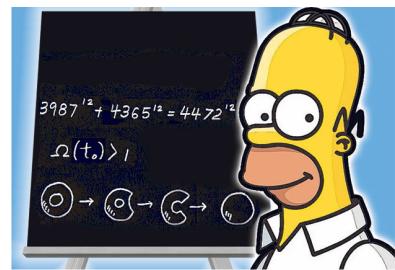


Figure 4: Homero y el Teorema de Fermat

# Tarea 3

LAS NOTAS que se incluyen en esta capítulo conforman la tarea 3, la cual consiste en la definición de espacio muestral y el principio de la Pichonera.

## *Definición de espacio muestral*

Se define como espacio muestral al conjunto de resultados posibles de un experimento aleatorio y se denota por  $S$ . Un elemento en  $S$  es llamado *punto muestral*. Cada resultado del experimento aleatorio corresponde a un punto muestral <sup>7</sup>.

El espacio muestral puede ser finito, contable infinito o incontable infinito

Por ejemplo, encontrar el espacio muestral del siguiente experimento: *Escoger una carta de una mazo de 52 cartas*. El espacio muestral  $S$  es el conjunto de las 52 cartas.

## *Principio de la Pichonera y aplicaciones*

El principio del palomar, también llamado principio de Dirichlet o principio de las cajas, establece que si  $n$  palomas se distribuyen en  $m$  palomares, y si  $n > m$ , entonces al menos habrá un palomar con más de una paloma.

Si suponemos que lo que se afirma es falso, significa que podemos colocar  $n + 1$  palomas en  $n$  nidos y tener a lo más una paloma por nido. El número total de palomas debe ser la suma de todos los nidos  $j$  de cada paloma  $P_j$  contenida en  $j$ . Por lo tanto

$$\sum_{j=1}^n B_j \leq \sum_{j=1}^n 1$$

$$\sum_{j=1}^n 1 = n * 1$$

Lo cual únicamente se cumple cuando

$$\sum_{j=1}^n B_j \leq \sum_{j=1}^n 1$$

Lo que implica  $n + 1$  palomas, sino a lo más  $n$ . Lo que es contradictorio a lo que se estableció en primera instancia.

**Ejemplo.** Para asegurar que una clase incluye al menos 2 estudiantes los cuales tienen un apellido que comienza con la misma letra del alfabeto inglés, la clase debe tener al menos 27 estudiantes.

## *Tarea 4*

LAS NOTAS que se incluyen en esta capítulo conforman la tarea 4, la cual consiste en una revisión de las técnicas de conteo, combinaciones y permutaciones; así como algunas aplicaciones.

### *Técnicas de conteo*

Suponga que una contraseña de un sistema computacional consiste de seis, siete u ocho caracteres. Cada uno de estos caracteres puede ser un dígito o una letra del alfabeto. Cada contraseña debe contener al menos un dígito, ¿Cuántas contraseñas hay? Las técnicas para responder a esta cuestión se llaman *técnicas de conteo* y se exponen a continuación.

#### *Regla del producto y de la suma*

Si suponemos que un proceso puede ser llevado a cabo mediante 2 tareas. Si hay  $n_1$  formas de realizar la primera tarea y  $n_2$  formas de realizar la segunda tarea, entonces hay  $n_1n_2$  formas de llevar a cabo el proceso, esta es llamada la **regla de la multiplicación**. Ahora bien, la probabilidad de dos o más eventos que ocurren al mismo tiempo y que son mutuamente exclusivos se calcula como la suma de sus probabilidades, la cual es llamada **regla de la suma**.

### *Permutaciones*

Un conjunto ordenado se llama permutación. El número de permutaciones de tamaño  $k$  que se puede formar con los  $n$  individuos u objetos en un grupo es denotado por  $P_{kn}$ . El número de permutaciones se determina utilizando la primera regla de conteo para k-tuplas. La expresión  $P_{3,7}$  puede ser rescrita con la ayuda de notación factorial, entonces

$$P_{kn} = n(n - 1)...(n - (k - 2))(n - (k - 1))$$

Multiplicando y dividiendo ésta por  $(n-k)!$  se obtiene una expresión compacta para el número de permutaciones.

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

### Combinaciones

Las combinaciones son los subconjuntos, donde el orden de selección no es importante, lo que importa es cuáles elementos son seleccionados. El número de permutaciones y el número de combinaciones guardan la siguiente relación:  $\frac{P_{k,n}}{k!}$ . Lo cual nos da como resultado la expresión para calcular el número de combinaciones

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

Nótese que  $\binom{n}{n} = 1$  y  $\binom{n}{0} = 1$  puesto que hay solo una forma de seleccionar un conjunto de  $n$  elementos o de ningún elemento y  $\binom{n}{1} = n$  puesto que existen  $n$  subconjuntos de tamaño 1.

### Problemas de Combinatoria

- ▷ ¿De cuántas formas se pueden permutar las letras en la palabra MISSISSIPPI?
- ▷ ¿Cuántos números telefónicos se pueden formar con 7 dígitos, asumiendo que el primer dígito no puede ser 0 o 1?
- ▷ Fred está planeando con ir a cenar cada noche de la semana, de Lunes a Viernes, cada cena en alguno de sus 10 restaurantes favoritos.
  - a) ¿Cuántas posibilidades hay para los planes de cena de Fred si no quiere cenar en el mismo restaurante dos veces? b) ¿Cuántas posibilidades hay para los planes de cena de Fred si quiere cenar en el mismo restaurante a lo más dos veces?
- ▷ Un torneo de tenis *round-robin* se está llevando a cabo con  $n$  jugadores, esto significa que cada jugador va a jugar en contra de cada uno de los jugadores exactamente una vez. a) ¿Cuántos posibles resultados hay en el torneo? (las listas de los resultados indican quién ganó y perdió cada juego)
- ▷ Para cumplir con los requerimientos para obtener cierto grado, un estudiante puede escoger atender 7 de 20 cursos disponibles, con la restricción de que al menos 1 de los 7 cursos debe ser un curso de estadística. Suponga que 5 de los 20 cursos son de estadística.
  - a) ¿Cuántas opciones hay para tomar los 7 cursos? b) Explicar intuitivamente por qué la respuesta anterior no es  $\binom{5}{1} \cdot \binom{19}{6}$

- ▷ Certo casino usa 10 decks estándar de cartas mezcladas en un gran deck, al cual lo llamaremos *superdeck*. Por lo tanto, el superdeck tiene  $52 \cdot 10 = 520$  cartas, con 10 copias de cada carta. ¿Cuántas manos diferentes de 10 cartas se pueden repartir del superdeck? El orden de las cartas no importa y tampoco importa de cuál deck provienen las cartas seleccionadas. Exprese su respuesta como un coeficiente binomial.
- ▷ ¿De cuántas formas distintas pueden sentarse ocho personas alrededor de una mesa redonda?
- ▷ Quieres ordenar 2 pizzas. Una pizza puede ser chica, mediana, grande o extra grande, con cualquier combinación de 8 guarniciones (es posible no agregar guarniciones o agregar las 8 guarniciones en una sola pizza). ¿Cuántas posibilidades hay para las 2 pizzas?
- ▷ Demostrar
$$\sum_{k=0}^n \binom{n}{k} = 2^n$$
- ▷ Demostrar para todos los enteros positivos  $n$  y  $k$  con  $n \geq k$ 

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$$

## Tarea 5

LAS NOTAS que se incluyen en esta capítulo conforman la tarea 5, la cual consiste en 1 reseña de un capítulo del libro *The math book*, el desarrollo de un árbol empleando *TikZ* y un histograma empleando ROOT.

### Go

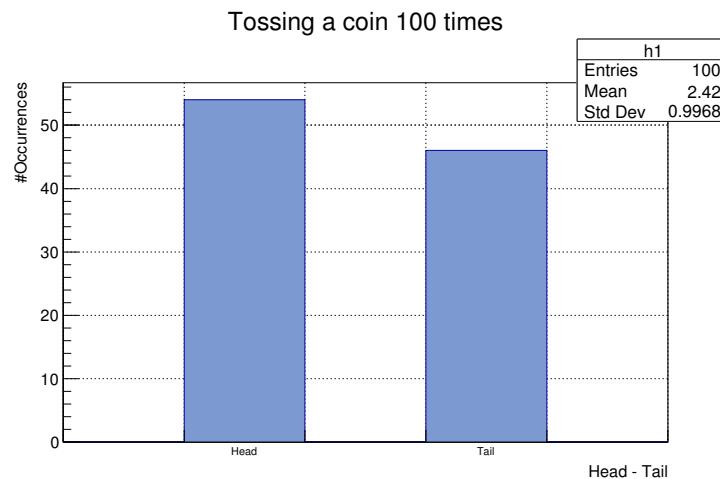
El juego Go es una juego de mesa de dos jugadores que fue creado en China. Consta de un tablero de  $19 \times 19$  casillas y el objetivo del juego es controlar el territorio del enemigo por medio de la captura de sus piedras. Es impresionante el número de movimientos de entrada posibles (32,940) y el número de juegos posibles ( $10^{768}$ ). Actualmente es sabido que una computadora ya pudo vencer a un humano, dicha computadora es *AlphaGo* de Google. Es impresionante como el avance de la Inteligencia Artificial ha sido tal que ha permitido aprender y tomar decisiones de una complejidad de la magnitud de este juego a una computadora.



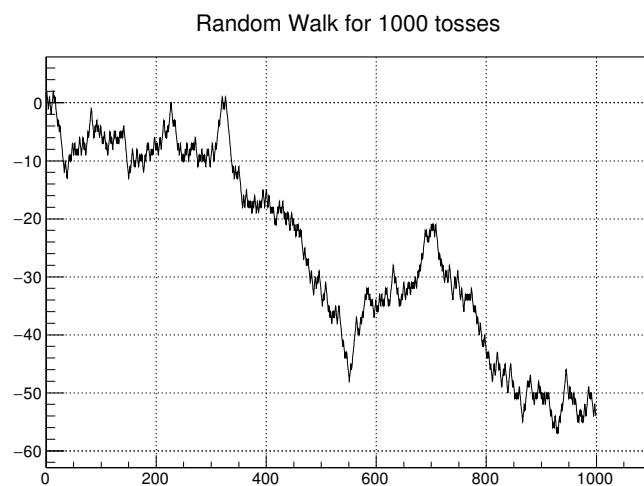
Figure 5: El juego Go es complejo debido a las complejas estrategias y el inmenso número de variantes posibles.

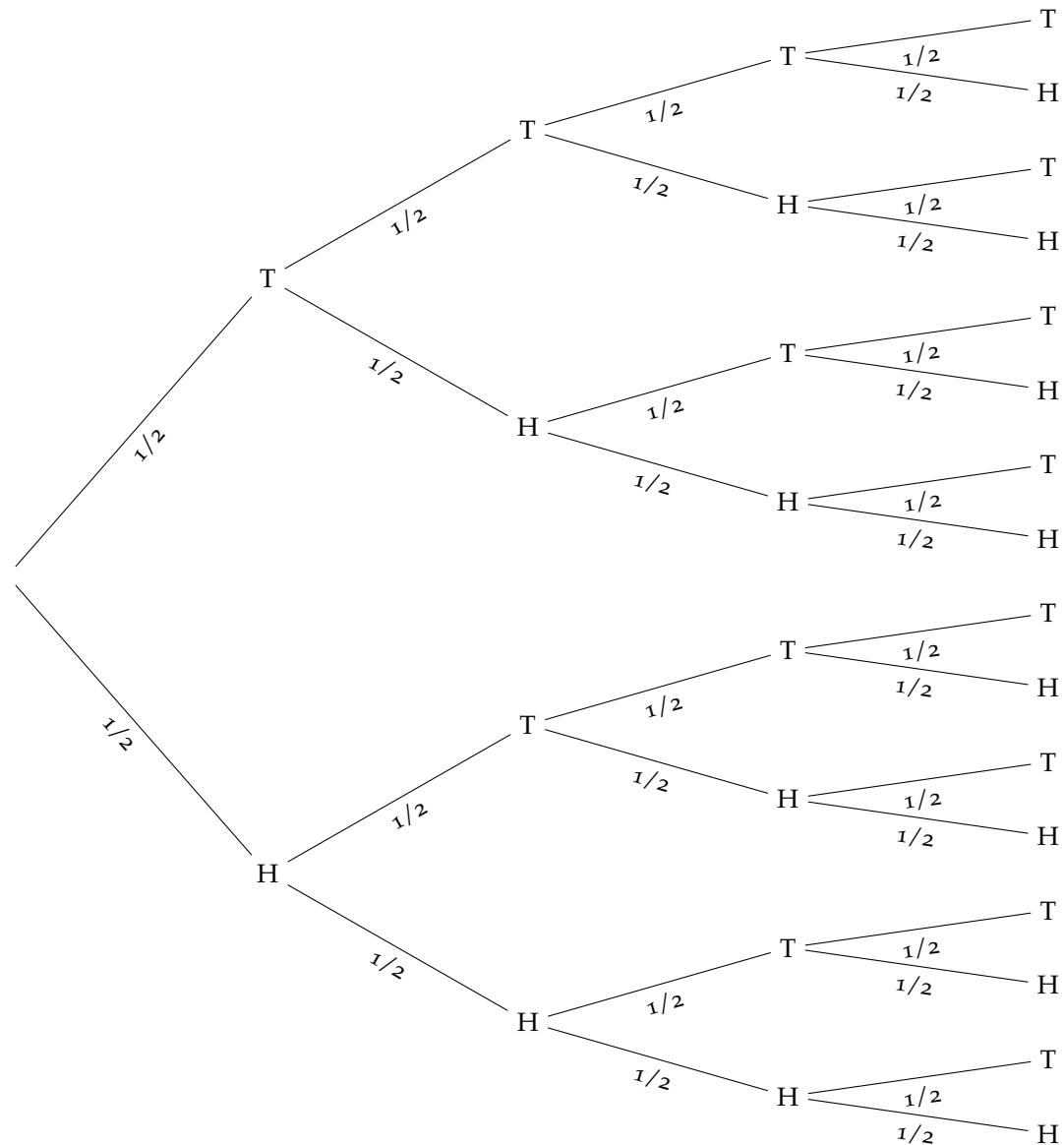
*Árbol de 4 tiradas de una moneda legal*

*Tossing a coin 100 times*



*Random Walk for 1000 Tosses*





## Tarea 6

*Convenio de Suma de Einstein*

$$x'^\mu = a^\mu_v v x^v$$

$$x'^\mu = a_0^\mu x^0 + a_1^\mu x^1 + a_2^\mu x^2 + a_3^\mu x^3$$

$$x'^0 = a_0^0 x^0 + a_1^0 x^1 + a_2^0 x^2 + a_3^0 x^3$$

$$x'^1 = a_0^1 x^0 + a_1^1 x^1 + a_2^1 x^2 + a_3^1 x^3$$

$$x'^2 = a_0^2 x^0 + a_1^2 x^1 + a_2^2 x^2 + a_3^2 x^3$$

$$x'^3 = a_0^3 x^0 + a_1^3 x^1 + a_2^3 x^2 + a_3^3 x^3$$

$$\begin{pmatrix} x'^0 \\ x'^1 \\ x'^2 \\ x'^3 \end{pmatrix} = \begin{pmatrix} a_0^0 & a_1^0 & a_2^0 & a_3^0 \\ a_0^1 & a_1^1 & a_2^1 & a_3^1 \\ a_0^2 & a_1^2 & a_2^2 & a_3^2 \\ a_0^3 & a_1^3 & a_2^3 & a_3^3 \end{pmatrix} \cdot \begin{pmatrix} x^0 \\ x^1 \\ x^2 \\ x^3 \end{pmatrix}$$

*Símbolo de Levi-Civita*

El símbolo de Levi-Civita  $\epsilon_{ijk}$  es un tensor de rango 3 y se define como

$$\epsilon_{ijk} = \begin{cases} 0, & \text{si cualquiera de las dos etiquetas es } 0 \\ 1, & \text{si } i,j,k \text{ es una permutación par de } 1,2,3 \\ -1, & \text{si } i,j,k \text{ es una permutación impar de } 1,2,3 \end{cases}$$

El símbolo de Levi-Civita  $\epsilon_{ijk}$  es antisimétrico en cada par de sus índices. El determinante de una matriz A con elementos  $a_{ij}$  pueden ser escritos en términos de  $\epsilon_{ijk}$  como

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \sum_{i=1}^3 \sum_{j=1}^3 \sum_{k=1}^3 \epsilon_{ijk} a_{1i} a_{2j} a_{3k} = \epsilon_{ijk} a_{1i} a_{2j} a_{3k}$$

Note la notación compacta donde la sumatoria sobre las direcciones espaciales es removida. Notar que el símbolo de *Levi-Civita* puede por lo tanto ser expresado como el determinante, o triple producto mezclado, o cualquiera de los vectores unitarios  $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$  del marco de referencia ortogonal dirigido y normalizado.

$$\epsilon_{ijk} = \det(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k) = \mathbf{e}_i \cdot (\mathbf{e}_j \times \mathbf{e}_k)$$

Ahora podemos definir por analogía a la definición del determinante un tipo adicional de producto, el vector producto o simplemente producto cruz

$$\mathbf{a} \times \mathbf{b} = \det \begin{vmatrix} \mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix} = \epsilon_{ijk} \mathbf{e}_i a_j b_k$$

O para cada coordenada

$$(\mathbf{a} \times \mathbf{b})_i = \epsilon_{ijk} a_j b_k$$

## Tarea 7

### Data Encryption Standard (DES)

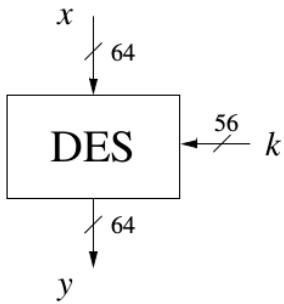


Figure 6: DES block cipher

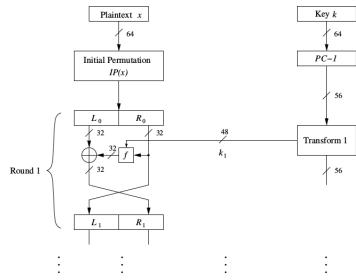


Figure 7: Primer bloque del DES

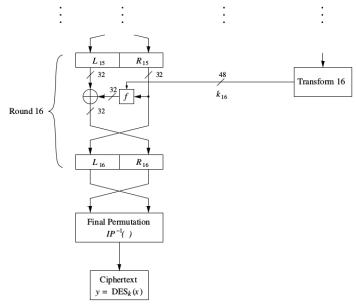


Figure 8: Segundo bloque del DES

El *Data Encryption Standard* ha sido hasta ahora el cifrador a bloques más popular de los últimos 30 años. A pesar de que actualmente no se considera seguro en contra de ataques específicos debido a que el espacio de llave es muy pequeño, se sigue empleando en aplicaciones comerciales. DES es un cifrador que encripta bloques de longitud de 64 bits con una llave de 56 bits de tamaño.

DES es un cifrador simétrico, lo que significa que la misma llave se emplea para cifrar y decifrar. DES es, como virtualmente todos los cifradores a bloques, un algoritmo iterativo. Por cada bloque de texto plano, el cifrado se realiza en 16 rondas las cuales llevan a cabo las mismas operaciones. Los bloques que componen el DES son las permutaciones inicial y final, las rondas del DES con su núcleo, la función  $f$  y el generador de llaves.

El cifrador DES está basado en una red *Feistel*, lo cual permite que las operaciones de cifrado y decifrado sean casi las mismas. El decifrado requiere únicamente un cálculo de llaves inverso, lo cual representa una ventaja en sus implementaciones en hardware y software. Después de una permutación inicial  $IP$  de 64 bits de texto plano, este bloque se divide en dos partes,  $L_0$  y  $R_0$ . Estos segmentos de 32 bits son la entrada a la red de Feistel, la cual consiste en 16 rondas.

La parte derecha  $R_i$  es la entrada de la función  $f$ . A la salida de la función  $f$  se le aplica una operación  $XOR$  denotada por el símbolo  $\oplus$  con la parte izquierda  $L_i$ . Finalmente, la parte derecha e izquierda son intercambiadas. Este proceso se repite en cada ronda y puede ser expresado como

$$L_i = R_{i-1}, \quad R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$$

Después de la ronda número 16, los segmentos de 32 bits  $L_{16}$  y  $R_{16}$  se intercambian nuevamente, y por último se aplica la permutación final  $IP^{-1}$ . Como la notación sugiere, la permutación final es el inverso de la permutación inicial. En cada ronda, una llave  $k_i$  se deriva de la llave principal de 56 bits usando un generador de llaves.

## Advanced Encryption Standard (AES)

El AES es el cifrador simétrico más empleado actualmente en sistemas comerciales e incluso en aplicaciones gubernamentales. A la fecha, no hay otros ataques contra el AES más que fuerza bruta. El cifrador AES es casi idéntico al cifrador *Rijndael*. El tamaño del bloque y de la llave del cifrador *Rijndael* varía entre 128, 192 y 256 bits, mientras que el AES únicamente emplea bloques de 128 bits. El número de rondas del AES está en función de la longitud de la llave. AES cifra todos los 128 bits en una iteración ya que a diferencia del DES, no se basa en una estructura *Feistel*. AES se compone de capas, cada capa manipula los 128 bits del camino de datos, también conocido como el estado del algoritmo. Hay únicamente 3 tipos diferentes de capas, cada ronda, con excepción de la primera, consiste en cada una de las 3 capas.

A continuación se describe brevemente cada una de las 3 capas:

- ▷ **Key Addition Layer** Una llave de ronda de 128 bits, o subllave, la cual ha sido calculada de la llave principal en la planificación de llaves.
- ▷ **Byte Substitution Layer (S-Box)** Cada elemento del estado actual del algoritmo es no-linealmente transformado empleando *lookup tables* con propiedades matemáticas especiales. Esta capa introduce *confusión* a los datos, por lo tanto se asegura que los cambios en los bits de estado individuales se propaguen rápidamente a través del camino de datos.
- ▷ **Diffusion Layer** Esta capa provee *difusión* sobre todos los bits de estado. Consiste en dos subcapas, las cuales llevan a cabo las siguientes operaciones lineales, la subcapa *ShiftRows* permuta los datos a nivel de bytes y la subcapa *MixColumn* es una operación matricial la cual mezcla bloques de 4 bytes.

## The RSA Cryptosystem

El esquema de cifrado RSA algunas veces referido como el algoritmo *Rivest-Shamir-Adleman*, es actualmente es esquema de cifrado asimétrico más empleado, a pesar de que las curvas elípticas y los algoritmos discretos están ganando terreno. El algoritmo RSA fue patentado en Estados Unidos en el año 2000. Existen muchas aplicaciones para RSA, pero se emplea principalmente para cifrado de datos pequeños, especialmente para transporte de llaves y para firmas digitales.

RSA se emplea típicamente junto con un cifrador simétrico como el AES, donde el cifrador simétrico cifra toda la información y RSA únicamente cifra la llave. El cifrado y decifrado se lleva a cabo en el

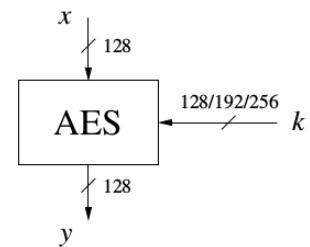


Figure 9: Parámetros de entrada y salida del AES

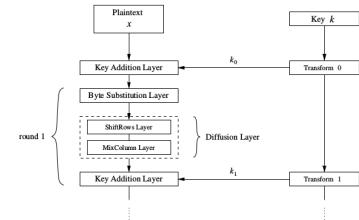


Figure 10: Primer bloque del AES

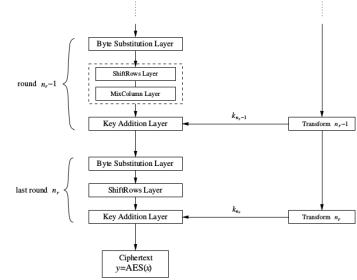


Figure 11: Primer bloque del AES

anillo  $\mathbb{Z}_n$  y los cálculos modulares juegan un rol central. RSA cifra texto plano  $x$ , donde se considera a la cadena de bits  $x$  como un elemento en  $\mathbb{Z}_n = 0, 1, \dots, n, -1$ . Como consecuencia el valor binario del texto plano  $x$  debe ser menor a  $n$ . El cifrado con la llave pública y el decifrado con la llave privada se muestran a continuación

**RSA Encryption** Dada la llave pública  $key(n, e) = k_{pub}$  y el texto plano  $x$ , la función de cifrado es

$$y = e_{k_{pub}} \equiv x^e \text{ mod } n \text{ donde } x, y \in \mathbb{Z}_n$$

**RSA Decryption** Dada la llave privada  $key d = k_{pr}$  y el texto cifrado  $y$ , la función de decifrado es

$$x = d_{k_{pr}}(y) \equiv y^d \text{ mod } n \text{ donde } x, y \in \mathbb{Z}_n$$

En la práctica,  $x, y, nyd$  son números muy largos, usualmente de 1024 bits de longitud o más. El valor  $e$  es algunas veces referido como *exponente de cifrado o exponente público*, y la llave privada  $d$  es algunas veces llamada *exponente de decifrado o exponente privado*.<sup>8</sup>

### La Máquina Enigma

En 1925 la armada alemana adquirió varias muestras de la comercialmente producida máquina de cifrado llamada *ENIGMA*, manufacturada por *Chiffriermaschinen Aktiengesellschaft*, después de algunas modificaciones, la armada adoptó la máquina para darle uso extenso. El corazón de la máquina *ENIGMA* era mecánico y constaba de varios rotores conectados entre sí. Cada rotor es un disco circular plano con 26 contactos eléctricos en cada cara, uno por cada letra del alfabeto. Cada contacto de una cara está conectado a un contacto diferente de la cara contraria.<sup>9</sup> Por ejemplo, en un rotor en particular, el contacto número 1 de una cara puede estar conectado con el contacto número 14 en la otra cara y el contacto número 5 de una cara con el número 22 de la otra. Cada uno de los 5 rotores proporcionados con la máquina *ENIGMA* estaba cableado de una forma diferente y los rotores utilizados por el ejército alemán poseían un cableado distinto al de los modelos comerciales.

<sup>8</sup> Christof Paar and Jan Pelzl. *Understanding Cryptography, a textbook for Students and Practitioners*. Springer, 2010

<sup>9</sup> David P. Mowry. *German Cipher Machines of World War II*. National Security Agency, 2014



Figure 12: Máquina ENIGMA Militar Estándar

# Tarea 8

## Ejemplos de Notación Indical

$$\mathbf{A} = \mathbf{B}, \leftrightarrow \begin{bmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{bmatrix} = \begin{bmatrix} B_{11} & B_{12} & B_{13} \\ B_{21} & B_{22} & B_{23} \\ B_{31} & B_{32} & B_{33} \end{bmatrix}$$

<sup>10</sup> Considerando un espacio  $n$ -dimensional con coordenadas  $x_1, x_2, \dots, x_n$ . Se define el gradiente de una función  $f(x_1, x_2, \dots, x_n)$ ,

$$(\nabla f)_\mu := \frac{\partial f}{\partial x_\mu}$$

Tomando la función  $f(x_1, x_2, \dots, x_n)$  y el gradiente  $\omega'_\alpha = \frac{\partial f}{\partial x'_\alpha}$

Esto nos lleva (empleando la regla de la cadena) a lo siguiente

$$\frac{\partial f}{\partial x'_1} = \frac{\partial f}{\partial x_1} \frac{\partial x_1}{\partial x'_1} + \frac{\partial f}{\partial x_2} \frac{\partial x_2}{\partial x'_1} + \dots + \frac{\partial f}{\partial x_n} \frac{\partial x_n}{\partial x'_1}$$

Esto es,

$$\frac{\partial f}{\partial x'_\mu} = \left( \frac{\partial x_\nu}{\partial x'_\mu} \right) \frac{\partial f}{\partial x_\nu},$$

$$\omega'_\mu = \left( \frac{\partial x_\nu}{\partial x'_\mu} \right) \omega_\nu$$

## Definición de Conjunto Producto para $A$ conjuntos

Sean  $A$  y  $B$  dos conjuntos. El *Conjunto Producto* de  $A$  y  $B$  denotado por  $A \times B$ , consiste en todos los pares ordenados  $(a, b)$  donde  $a \in A$  y  $b \in B$ :

$$A \times B = (a, b) : a \in A, b \in B$$

El concepto de conjunto producto se extiende para cualquier número finito de conjuntos en forma natural. El conjunto producto de los

<sup>10</sup> Kees Dullemond and Kasper Peeters.  
Introduction to tensor calculus, 2010

conjuntos  $A_1, A_2, \dots, A_m$ , escrito como  $A_1 \times A_2 \times \cdots \times A_m$ , es el conjunto de todas las  $m$ -tuplas ordenadas  $(a_1, a_2, \dots, a_m)$  donde  $a_i \in A_i$  para cada  $i$ .

### *Cardinalidad del conjunto potencia*

La cardinalidad del conjunto potencia de un conjunto finito  $A$  es  $2$  elevado al cardinal de  $A$ :

$$|P(A)| = 2^{|A|}$$

Es posible deducir esta relación mediante los coeficientes binomiales. Si el conjunto  $A$  tiene  $n$  elementos, el número de subconjuntos con  $k$  elementos es igual al número combinatorio  $C(n, k)$ . Un subconjunto de  $A$  puede tener 0 elementos como mínimo, y  $n$  como máximo, y por lo tanto:

$$|P(A)| = \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{k} = 2^n = 2^{|A|}$$

## Tarea 9

### Oveja Dolly

La oveja Dolly, el primer mamífero clonado en el mundo, fue reprimida el 14 de febrero de este año. Ella sufría de un virus que le causó un tumor en el pulmón. Esto ha dado lugar a una nueva ronda de debate acerca de la clonación, en particular sobre los problemas de envejecimiento de los animales clonados. Los científicos se han preocupado por los animales clonados ya que estos podrían heredar la edad de su donante de células, siendo de este modo un nacimiento viejo y por lo tanto el clon morirá prematuramente. Los *telómeros* son las unidades que se encuentran al final de todos los cromosomas.

En el proceso de transferencia nuclear, una célula somática, con la longitud del telómero acortado, se transfiere a un ovocito enucleado y se activa para iniciar el desarrollo del embrión. Una pregunta directa es la siguiente, ¿están los telómeros acortados de las células del donante restaurados en toda su longitud en los animales producidos por transferencia nuclear? Era una preocupación de que si los telómeros acortados de hecho fueron heredados por los animales clonados.

Lo que ha sucedido con la oveja Dolly es que ella se clonó a partir de una célula de una oveja adulta, cuyas células ya se habían dividido un cierto número de veces, y por lo tanto sus telomeros se habían acortado en igual proporción. Al clonarse las células adultas de la madre retrocedió su reloj biológico volviendo a ser pluripotencial, pero en el proceso sus telomeros persistieron cortos. Lo probable es entonces que Dolly viva el tiempo que le queda de telomeros para que las células continúen dividiéndose. Pero como ésta lo recibió más corto, posiblemente muera. La parte buena de la noticia es que esto va a desestimar las iniciativas para clonar un ser humano. Nadie va a querer clonarse si ya al nacer su expectativa de vida va a ser corta.



Figure 13: El doctor Ian Wilmut posa con el cuerpo disecado de Dolly en el Museo Real de Edimburgo.

## Codones

La información genética, contenida en el ARNm, se escribe con cuatro letras, que corresponden a las bases nitrogenadas del ARNm(A,C,G,U), pero van agrupadas de tres en tres. Cada grupo de tres es llamado *codón* y su función es codificar un aminoácido o un símbolo de puntuación. El orgánulo celular que sintetiza las proteínas a partir de aminoácidos con la información contenida en el ARNm, leyendo los codones, es el ribosoma.

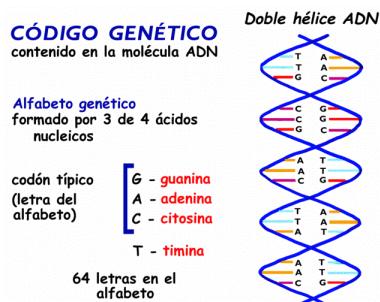


Figure 14: Código Genético

Cada aminoácido está codificado por un codón o varios codones. En total hay 64 codones que codifican para 20 aminoácidos y 3 señales de parada de la traducción. Esto hace que el código sea redundante, lo que se denomina *código generado*, y que haya varios codones diferentes que codifican para un sólo aminoácido.

## Telómeros

Los telómeros son estructuras cromatínicas especializadas que se encuentran localizadas en los extremos de los cromosomas eucariontes. Tanto el ADN como las proteínas que los constituyen presentan características singulares que los diferencian del resto de los cromosomas. Parecen estar implicados en numerosas funciones celulares, especialmente las relacionadas con el control de la duración de la vida de diferentes estirpes celulares. Estas estructuras se replican durante el ciclo celular gracias a la acción de enzimas denominadas telomerasas, que están formadas por proteínas y ARN y presentan un mecanismo peculiar. Recientemente se ha estudiado el comportamiento de las telomerasas en las células cancerosas y sus posibles aplicaciones diagnósticas y terapéuticas.

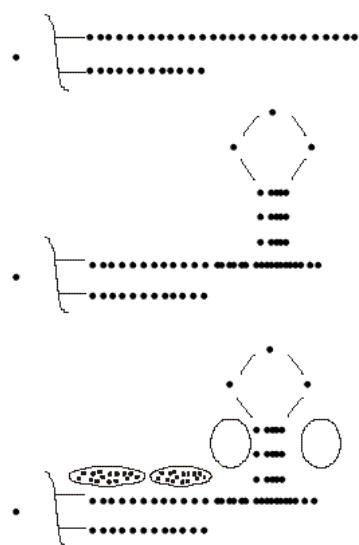


Figure 15: Representación esquemática de la estructura de los telómeros

En casi todos los eucariontes estudiados, el ADN telomérico (ADNt) consiste en repeticiones en tandem de pequeñas secuencias nucleotídicas con una distribución asimétrica de los pares G : C, pues las G se acumulan en una de las hebras (hebra G) y se encuentran agrupadas. La hebra G está orientada de 5' a 3' hacia el extremo del telómero y forma el extremo 3' del ADN cromosómico. En la zona más externa no está apareada formando un segmento final monofibrilar con una longitud que varía según la especie.

# Tarea 10

## Decaimiento radioactivo

El decaimiento radioactivo es un proceso en el que un núcleo inestable se transforma en uno más estable, emitiendo partículas y/o fotones y liberando energía durante el proceso. Una sustancia que experimenta este fenómeno espontáneamente se denomina sustancia radioactiva. Pueden emitir tres tipos de radiación, Radiación  $\alpha$ , Radiación  $\beta$  y Radiación  $\gamma$ .

Los procesos de desintegración nuclear son estadísticos. La desintegración de todos los núcleos de una cierta masa no se suceden a intervalos iguales de tiempo sino que obedecen a las leyes estadísticas. En base a ésto es posible determinar la velocidad a la que ocurre un proceso de decaimiento en una muestra radioactiva, la cual es proporcional al número de núcleos radioactivos presentes. Si  $N$  es la cantidad de núcleos radioactivos presentes en la muestra en algún instante, entonces la razón de cambio de  $N$  es

$$\frac{dN}{dt} = -\lambda * N$$

donde  $\lambda$  se denomina **constante de decaimiento**.

La constante de decaimiento es la probabilidad de que un núcleo decaiga en un instante de tiempo y el tiempo de vida promedio  $\tau$  es el promedio del tiempo de vida de todos los núcleos radioactivos en una muestra. Se define como

$$\tau = \frac{1}{\lambda}$$

## El problema de Monty Hall

El problema de **Monty Hall** es un problema matemático de probabilidad basado en el concurso televisivo estadounidense *Let's Make a Deal*, famoso entre 1963 y 1986. Su nombre proviene del presentador, Monty Hall.

En este concurso, el concursante escoge una puerta entre tres, y su premio consiste en lo que se encuentra detrás. Una de ellas oculta

un coche, y tras las otras dos hay una cabra. Sin embargo, antes de abrirla, el presentador, que sabe donde se encuentra el premio. abre una de las otras dos puertas y muestra que detrás de ella hay una cabra. Ahora tiene el concursante una última oportunidad de cambiar la puerta escogida. *¿Debe el concursante mantener su elección original o escoger la otra puerta? ¿Hay alguna referencia?*

### *Falacia del apostador*

La falacia del apostador, también conocida como la falacia de Monte Carlo, es la creencia errónea de que, si algo pasa más frecuente de lo normal durante cierto periodo, esto pasará menos frecuente en el futuro. Se cree erróneamente que los sucesos pasados afectan a los futuros en lo relativo a actividades aleatorias, como es el caso de muchos juegos de azar. Puede comprender las siguientes ideas equivocadas:

- ▷ Un suceso aleatorio tiene más probabilidad de ocurrir porque no ha ocurrido durante cierto periodo.
- ▷ Un suceso aleatorio tiene menos probabilidad de ocurrir porque ha ocurrido durante cierto periodo.
- ▷ Un suceso aleatorio tiene más probabilidad de ocurrir si no ocurrió recientemente.
- ▷ Un suceso aleatorio tiene menos probabilidad de ocurrir si ocurrió recientemente.

Las anteriores son ideas equívocas que surgen cotidianamente en razonamientos sobre probabilidades, muchos de los cuales se han estudiado con gran profundidad.

## Tarea 11

### Criterios de divisibilidad

*Criterio de divisibilidad entre 3.* Para saber si un número es divisible entre 3, se tiene que comprobar que la suma de todos sus dígitos es 3 o múltiplo de 3. Por ejemplo: 1098.

$$1098 : 1 + 0 + 9 + 8 = 18$$

$$1 + 8 = 9$$

*Criterio de divisibilidad entre 11.* Primero se identifica cuáles son las cifras que ocupan las posiciones pares y las que ocupan las posiciones impares. Por ejemplo, para 5863 tenemos

$$\text{Par. } 5 \text{ y } 6. \text{ Sumando : } 5 + 6 = 11$$

$$\text{Impar. } 8 \text{ y } 3. \text{ Sumando : } 8 + 3 = 11$$

Tenemos  $11 - 11 = 0$  por lo tanto 5863 es divisible entre 11.

### El juego de la vida

El juego de la vida es un autómata celular diseñado por el matemático británico John Horton Conway en 1970. Desde un punto de vista teórico, es interesante porque es equivalente a una máquina universal de Turing, es decir, todo lo que se puede computar algorítmicamente se puede computar en el juego de la vida.

El juego de la vida es en realidad un juego de cero jugadores, lo que quiere decir que su evolución está determinada por el estado inicial y no necesita ninguna entrada de datos posterior. El "tablero de juego" es una malla formada por cuadrados ("células") que se extiende por el infinito en todas las direcciones. Cada célula tiene 8 células vecinas, que son las que están próximas a ella, incluidas las diagonales. Las células tienen dos estados: están "vivas" o "muertas". El estado de la malla evoluciona a lo largo de unidades de tiempo discretas(turnos). El estado de todas las células se tiene en cuenta para calcular el estado de las mismas al turno siguiente. Todas las células se actualizan simultáneamente. Las transiciones dependen del número de células vecinas vivas:

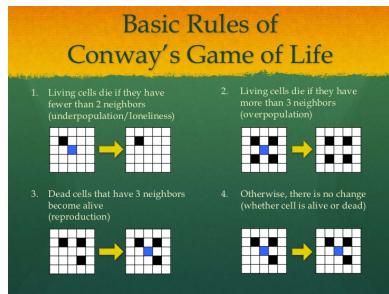


Figure 16: Reglas básicas del Juego de la Vida.

▷ Una célula muerta con exactamente 3 células vecinas vivas "nace" (al turno siguiente estará viva).

▷ Una célula viva con 2 o 3 células vecinas vivas sigue viva, en otro caso muere o permanece muerta (por "soledad" o "superpoblación").

Existen numerosos tipos de patrones que pueden tener lugar en el juego de la vida.

▷ Osciladores. Los osciladores son patrones que son predecesores de si mismos. En otras palabras, son patrones que tras un número finito de generaciones vuelven a su estado inicial. El número de generaciones determina el período del oscilador.

▷ Vidas estáticas. Las vidas estáticas son patrones que no cambian de una generación a la siguiente. Las vidas estáticas se pueden considerar como osciladores de período 1. En general se asume que las vidas estáticas son finitas y no vacías. Se las puede dividir en vidas estáticas *estáticas* y *pseudo* vidas estáticas. Las vidas estáticas estás son aquellas cuyas partes no son estáticas por sí mismas.

▷ Naves espaciales. Las naves espaciales son patrones que reaparecen en otra posición tras completar su período. Esto es, son patrones que tras un número finito de generaciones vuelven a su estado original pero en una ubicación diferente.

## Cuaterniones

Los cuaterniones son números de 4 dimensiones, creados por el matemático Irlandés William Hamilton. Los cuaterniones son empleados para describir la dinámica del movimiento en 3 dimensiones y aplicados en campos como los gráficos por computadora, realidad virtual, programación de videojuegos, procesamiento de señales, robótica, bioinformática y estudios de la geometría del espacio.

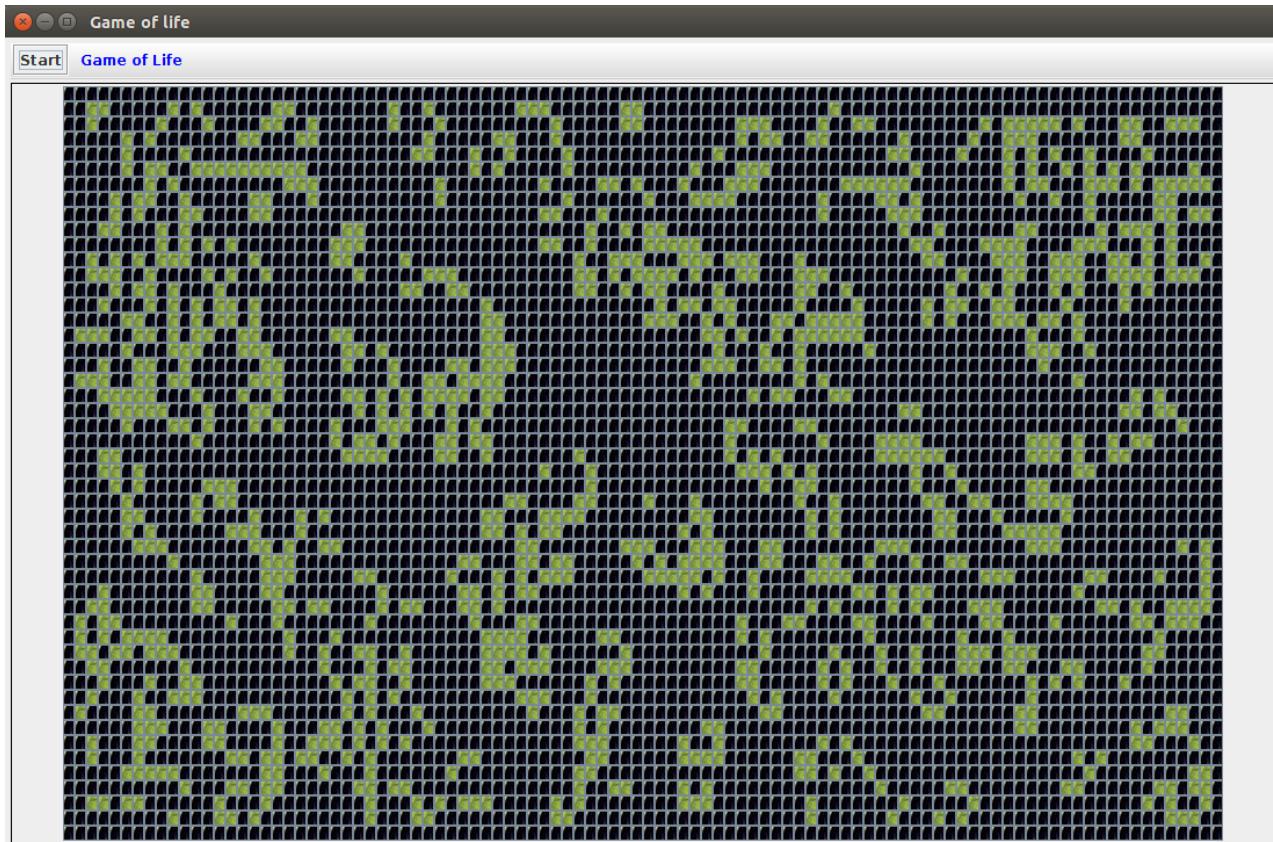


Figure 17: Juego de la vida

Los cuaterniones pueden ser representados en 4 dimensiones por  $Q = a_0 + a_1i + a_2j + a_3k$  donde  $i, j$  y  $k$  son vectores unitarios en 3 direcciones ortogonales, y son perpendiculares al eje de los números reales. Para sumar o multiplicar dos cuaterniones, se deben tratar como polinomios en  $i, j$  y  $k$ , pero se deben usar las siguientes reglas para los productos:  $i^2 = j^2 = k^2 = -1; ij = -ji = k; jk = -kj = i$  y  $ki = -ik = j$ .

### Logaritmos

El matemático escocés John Napier es el famoso inventor de los logaritmos, publicados en su libro llamado *A Description of the Marvelous Rule of Logarithms*. Este método ha contribuido a incontables avances en la ciencia e ingeniería permitiendo llevar a cabo cálculos complicados de una forma más simple. Un logaritmo de base  $b$  de un número  $x$  es expresado como  $\log_b(x)$  y es igual al exponente  $y$  que satisface  $x = b^y$ .

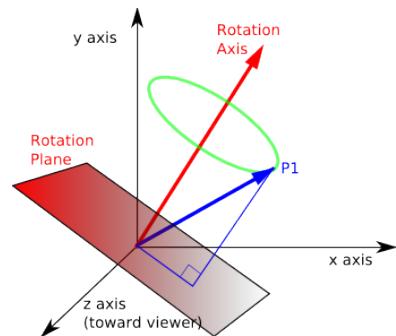


Figure 18: Representación de un cuaternion.

Por ejemplo, si  $3^5 = 3 \times 3 \times 3 \times 3 \times 3 = 243$ , podemos decir que el logaritmo de 243 (base 3) es 5. En la actualidad muchas cantidades científicas son expresadas como logaritmos de otras cantidades. Por ejemplo, la escala *pH* en Química, la unidad *bel* en acústica y la escala *Ritcher* usada para medir la intensidad de los terremotos.

## Tarea 12

### Congruencia de Zeller

La congruencia de Zeller es un algoritmo ideado por Julius Christian Johannes Zeller para calcular el día de la semana de cualquier fecha del calendario. Para el calendario gregoriano la congruencia de Zeller es

$$h = \left( q + \left( \frac{(m+1)26}{10} \right) + K + \left( \frac{K}{4} \right) + \left( \frac{J}{4} \right) + 5J \right)_{mod7}$$

donde

h es el día de la semana (0 = sábado, 1 = domingo, 2 = lunes, ...)

q es el día del mes

m es el mes

J es la centuria (año entre 100)

K el año de la centuria (año mod 100)

Enero y Febrero se cuentan como meses 13 y 14 del año anterior. Por ejemplo, el 2 de Enero del 2013, es m=13, año=2012.

Estas fórmulas se basan en la observación de que el día de la semana progresó de una manera predecible basada en cada subparte de esa fecha. Cada término de la fórmula se usa para calcular el desplazamiento necesario para obtener el día correcto de la semana. Para el calendario gregoriano, las partes de la fórmula se entienden de la siguiente forma

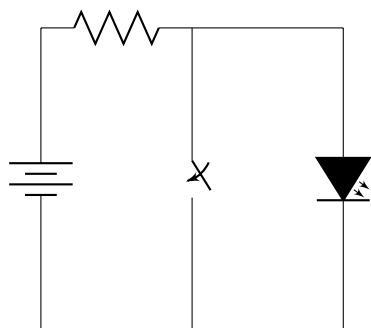
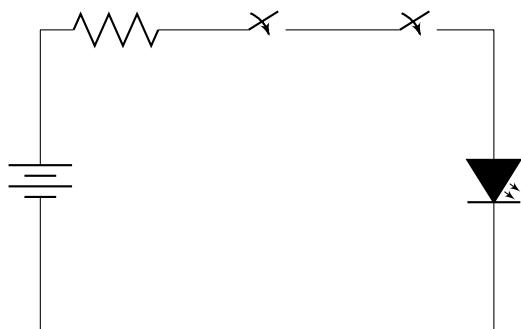
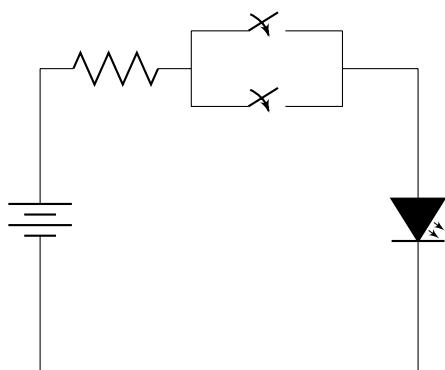
- ▷ **q** representa la progresión del día de la semana basada en el día del mes, dado que cada día sucesivo resulta en un desplazamiento adicional de 1 en el día de la semana.
- ▷ **K** representa la progresión del día de la semana basada en el año. Suponiendo que cada año tiene 365 días, la misma fecha de cada año sucesivo será desplazada por un valor de  $365 \bmod 7 = 1$ .
- ▷ Como hay 366 días en cada año bisiesto, esto se toma en cuenta añadiendo un día adicional al valor de desplazamiento del día de la semana. Esto se logra añadiendo  $\left( \frac{K}{4} \right)$  al desplazamiento. Este término se calcula como un resultado entero. Cualquier resto que pueda haber es descartado.

- ▷ Usando una lógica similar, se puede calcular la progresión del día de la semana para cada centuria observando que hay 36524 días en una centuria normal, y 36525 en cada centuria divisible por 400. Dado que  $36525 \bmod 7 = 6$  y  $36524 \bmod 7 = 5$ , el término  $\left(\frac{l}{4}\right) + 5J$  refleja esto.
  
  
  
  
  
  
- ▷ El término  $\left(\frac{(m+1)26}{10}\right)$  se puede explicar de la siguiente manera. Zeller observó que, al iniciar cada año el 1 de marzo, el día de la semana de cada mes sucesivo progresaba multiplicando el mes por un valor constante y descartando el resto fraccional.
  
  
  
  
  
  
- ▷ La función global  $\bmod 7$ , normaliza el resultado para que se encuentre en el intervalo de 0 a 6, lo que da como resultado el índice del día de la semana correcto para la fecha analizada.

### *Comportamiento agresivo en autómatas inteligentes*

Investigación hecha por la empresa *Google* relacionada con Inteligencia Artificial ha mostrado ser la prueba conclusiva en el ámbito del comportamiento animal referente al desarrollo evolutivo de las actitudes, pues a través de su motor de Inteligencia Artificial *Deep Mind*, se observó la formación de una actitud aprendida a partir de las condiciones de la simulación, donde la escasez de recurso y la necesidad de competencia desarrolló **agresividad**.

Durante la investigación, el equipo de *Google* ejecutó 40 millones de vueltas de un juego de computadora simple de *recolección de frutas*, pidiendo a dos agentes de *Deep Mind* que compitieran entre sí para reunir tantas manzanas virtuales como les fuera posible. Ellos encontraron que las cosas iban sin problemas, siempre y cuando hubiese suficientes manzanas para los dos, pero tan pronto como las manzanas comenzaron a *disminuir*, los dos agentes se tornaron agresivos, usando rayos láser para golpearse mutuamente y robar todas las manzanas.

*Compuertas lógicas con circuitos**NOT**AND**OR**Combinaciones con repetición**Problema de los caramelos*

¿De qué manera se pueden repartir 4 caramelos a 5 niños?

Este problema puede ser reconstruido a partir de un multiconjunto de combinación con repetición, donde a cada niño se le asignará una letra, A, B, C, D y E. Por el principio de biyección, el número de formas en que se pueden repartir los caramelos es igual al número de series de 5 letras (sin tomar en cuenta el orden) A,B,C,D,E. Pero cada una de ellas corresponde a un multiconjunto con 4 elementos, por lo que el número total de formas de repartir los caramelos es  $\binom{5}{4}$ . Debido a que queremos dividir 4 caramelos sin etiqueta entre 5 grupos (niños), colocamos 4 objetos en línea e insertamos 4 separadores para dividirlos en 5 secciones. Si representamos los caramelos con asteriscos y los separadores con barras, los ejemplos serían

$$AAAA \rightarrow * * * * / / /$$

$$ABCD \rightarrow * / * / * / *$$

$$AABB \rightarrow * * / * * / /$$

$$ABCE \rightarrow * / * / * / *$$

(1)

De esta manera, el número de formas a repartir corresponde al número de símbolos, de los cuales 4 son asteriscos y 4 barras. Este es el número de formas de elegir 4 objetos de un conjunto con 8 y por lo tanto el número de ordenamiento es

$$\binom{n}{k} = \binom{5}{4} = \binom{n+k-1}{k} =$$

$$\frac{(n+k-1)!}{k!(n-1)!} = \frac{(5+4-1)!}{4!(5-1)!} = 840$$

# Tarea 13

## Probabilidad Condicional

### Ejemplo 1

Consideremos la diferencia que existe entre el elegir al azar un artículo de un lote con o sin sustitución. Supongamos que un lote tiene la siguiente composición: 80 artículos sin defectos y 20 defectuosos. Supóngase que elegimos dos artículos: a) con sustitución y b) sin sustitución. Definamos los eventos siguientes:

$$A = \{\text{el primer artículo es defectuoso}\},$$

$$B = \{\text{el segundo artículo es defectuoso}\}.$$

Si escogemos con sustitución,  $P(A) = P(B) = \frac{20}{100} = \frac{1}{5}$ . Cada vez que elegimos, en el lote hay 20 artículos defectuosos de un total de 100. Sin embargo, si elegimos *sin* sustitución, los resultados no son totalmente inmediatos. Todavía es verdad que  $P(A) = \frac{1}{5}$ . Pero, ¿cuál es el valor de  $P(B)$ ? Es evidente que con el propósito de calcular  $P(B)$  deberíamos conocer la composición del lote *cuando se escoge el segundo artículo*. En otras palabras, deberíamos saber si el evento  $A$  ocurrió o no. Por lo tanto, sean  $A$  y  $B$  dos eventos asociados con un experimento  $\epsilon$ , sea  $P(B|A)$  la *probabilidad condicional* del evento  $B$ , *dado* que  $A$  ha ocurrido. Por lo tanto tenemos que si  $A$  ha ocurrido, al sacar por segunda vez, solo quedan 99 artículos, de los cuales 19 son defectuosos, entonces  $P(B|A) = \frac{19}{99}$ .

### Ejemplo 2

Se lanzan dos dados normales y se anotan los resultados  $(x_1, x_2)$ , donde  $x_i$  es el resultado del  $i$ -ésimo dado,  $i = 1, 2$ . Por tanto, el espacio muestral  $S$  se puede representar por el siguiente arreglo de 36 resultados

igualmente posibles:

$$S = \begin{pmatrix} (1,1) & (1,2) & \dots & (1,6) \\ (2,1) & (2,2) & \dots & (2,6) \\ \vdots & \vdots & \vdots & \vdots \\ (6,1) & (6,2) & \dots & (6,6) \end{pmatrix}$$

Consideremos los dos eventos siguientes:

$$A = \{(x_1, x_2) \mid x_1 + x_2 = 10\},$$

$$B = \{(x_1, x_2) \mid x_1 > x_2 = 10\}.$$

Tenemos  $A = (5,5), (4,6), (6,4)$  y  $B = (2,1), (3,1), (3,2), \dots, (6,5)$ . Por tanto,  $P(A) = \frac{3}{36}$  y  $P(B) = \frac{15}{36}$ . Además,  $P(B|A) = \frac{1}{3}$ , ya que el espacio muestral es ahora A (que son 3 resultados), y sólo uno de ellos es consistente con el evento B. De manera semejante, se puede calcular  $P(A|B) = \frac{1}{15}$ . Finalmente, calculando  $P(A \cap B)$  tenemos que el evento  $A \cap B$  ocurre si y sólo si la suma de los dos dados es diez y el primer dado indica un valor mayor que el segundo. Solamente hay un resultado y, por tanto,  $P(A \cap B) = \frac{1}{36}$

### Ejemplo 3

Una caja contiene 4 tubos malos y 6 buenos. Se sacan dos *a la vez*. Se prueba uno de ellos y se encuentra que es bueno. ¿Cuál es la probabilidad de que el otro también sea bueno?

Consideremos los eventos siguientes

$$A = \{\text{El tubo es bueno}\}$$

$$B = \{\text{El otro tubo es bueno}\}$$

Podemos notar que dado que ya se sacó un tubo que es bueno, la probabilidad de que el otro tubo sea bueno, es decir,  $P(B|A)$  se define como la cantidad de tubos buenos restantes entre la cantidad de tubos restantes, por lo tanto tenemos  $P(B|A) = \frac{5}{9}$ .

### Ejemplo 4

Veinte artículos, 12 de los cuales son defectuosos y 8 no defectuosos, se inspeccionan uno después de otro. Si esos artículos se escogen al azar, ¿cuál es la probabilidad de que

- a) los dos primeros artículos inspeccionados sean defectuosos?
- b) los dos primeros artículos inspeccionados *no* sean defectuosos?

- c) entre los dos primeros artículos inspeccionados haya uno defectuoso y uno no defectuoso?

Consideremos los eventos siguientes

$$A = \{\text{El primer artículo es defectuoso}\}$$

$$B = \{\text{El segundo artículo es defectuoso}\}$$

$$A \cap B = \{\text{Los 2 primeros artículos son defectuosos}\}$$

Para el inciso *a*) tenemos  $P(B|A) = \frac{P(A \cap B)}{P(A)}$ ; pero lo que nos interesa es la probabilidad de  $P(A \cap B)$  por lo tanto, despejando tenemos  $P(A \cap B) = P(B|A)P(A)$ . Tenemos que  $P(A) = \frac{12}{20}$  ya que existen 12 artículos defectuosos y en total son 20 artículos.  $P(B|A) = \frac{11}{19}$  ya que existen 11 artículos defectuosos restantes (dado que ya se escogió un artículo defectuoso) y restan 19 artículos en total. Por tanto tenemos que  $P(A \cap B) = P(B|A)P(A) = (\frac{12}{20})(\frac{11}{19}) = \frac{33}{95}$ .

Para el inciso *b*) consideremos los eventos siguientes

$$A = \{\text{El primer artículo no es defectuoso}\}$$

$$B = \{\text{El segundo artículo no es defectuoso}\}$$

$$A \cap B = \{\text{Los 2 primeros artículos no son defectuosos}\}$$

Tenemos que  $P(A) = \frac{8}{20}$  ya que existen 8 artículos no defectuosos y en total son 20 artículos.  $P(B|A) = \frac{7}{19}$  ya que existen 7 artículos no defectuosos restantes (dado que ya se escogió un artículo no defectuoso) y restan 19 artículos en total. Por tanto tenemos que  $P(A \cap B) = P(B|A)P(A) = (\frac{7}{19})(\frac{8}{20}) = \frac{14}{95}$ .

Para el inciso *c*) consideremos los eventos siguientes

$$A = \{\text{El primer artículo es defectuoso}\}$$

$$B = \{\text{El segundo artículo no es defectuoso}\}$$

$$C = \{\text{El primer artículo no es defectuoso}\}$$

$$D = \{\text{El segundo artículo es defectuoso}\}$$

$$(A \cap B) \cup (C \cap D) = \{\text{Entre los dos primeros artículos inspeccionados hay uno defectuoso y uno no defectuoso}\}$$

Tenemos que  $P(A) = \frac{12}{20}$  ya que existen 12 artículos defectuosos y en total son 20 artículos.  $P(B|A) = \frac{8}{19}$  ya que existen 8 artículos no defectuosos y restan 19 artículos en total. Por tanto tenemos que  $P(A \cap B) = P(B|A)P(A) = (\frac{8}{19})(\frac{12}{20}) = \frac{24}{95}$ . Tenemos que  $P(C) = \frac{8}{20}$  ya que existen 8 artículos no defectuosos y en total son 20 artículos.  $P(D|C) = \frac{12}{19}$  ya que existen 12 artículos defectuosos y restan 19 artículos en total.

Por tanto tenemos que  $P(A \cap B) = P(B|A)P(A) = (\frac{8}{20})(\frac{12}{19}) = \frac{24}{95}$ . Por último tenemos que  $P((A \cap B) \cup (C \cap D)) = P(A \cap B) + P(C \cap D) = \frac{24}{95} + \frac{25}{95} = \frac{48}{95}$ .

### Ejemplo 5

Supóngase que tenemos 2 urnas, 1 y 2, cada una con dos cajones. La urna 1 tiene una moneda de oro en un cajón y una de plata en el otro, mientras que la urna 2 tiene una moneda de oro en cada uno de los cajones. Se escoge una urna al azar, y de ésta se escoge un cajón al azar. La moneda que se encontró en este cajón es de oro. ¿Cuál es la probabilidad de que la moneda provenga de la urna 2?

Consideremos los eventos siguientes

$$A = \{\text{La moneda es de oro}\}$$

$$B = \{\text{La moneda proviene de la urna 2}\}$$

La probabilidad de que la moneda sea de oro es  $P(A) = \frac{3}{4}$  debido a que hay 4 monedas en total y 3 de esas monedas son de oro. La probabilidad de que la moneda sea de oro y provenga de la urna 2 es  $P(A \cap B) = \frac{1}{2}$  debido a que la probabilidad de escoger una moneda de la urna 2 es  $\frac{1}{2}$  y la probabilidad de que esa moneda sea de oro es 1, por lo tanto de acuerdo a la *regla de multiplicación*, se multiplican las probabilidades y tenemos como resultado  $\frac{1}{2}$ . Por último, la probabilidad de que una moneda provenga de la urna 2 dado que es una moneda de oro, la denotamos como  $P(B|A) = \frac{P(A \cap B)}{P(A)} = \frac{\frac{1}{2}}{\frac{3}{4}} = \frac{2}{3}$ .

### Ejemplo 6

Se selecciona una carta al azar de un mazo previamente barajeado. Encontrar la probabilidad de que dicha carta sea un as dado que se sabe que es una carta negra.

Consideremos los eventos siguientes

$$A = \{\text{La carta es un as}\}$$

$$B = \{\text{La carta es negra}\}$$

Hay 2 ases negros y 26 cartas negras, por lo tanto la probabilidad de que la carta sea un as negro es  $\frac{2}{26} = \frac{1}{13}$ .

Por otra parte tenemos que la probabilidad de que una carta sea negra es  $P(B) = \frac{26}{52}$ . Y la probabilidad de que la carta sea un as y sea negra es  $P(A \cap B) = \frac{2}{52}$ . Por lo tanto, tenemos  $P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{\frac{2}{52}}{\frac{26}{52}} = \frac{1}{13}$

*Ejemplo 7*

Se toman 2 cartas aleatoriamente de un mazo previamente barajeado, una tras otra sin reemplazo. Sea  $A$  el evento de sacar una carta de corazones, y sea  $B$  el evento de que la segunda carta sea roja. Encontrar  $P(A|B)$  y  $P(B|A)$ .

De acuerdo a la definición clásica de probabilidad y la regla de multiplicación tenemos  $P(A \cap B) = \frac{13 \cdot 25}{52 \cdot 51} = \frac{25}{204}$   
 $P(B) = \frac{26 \cdot 51}{52 \cdot 51} = \frac{1}{2}$ ,  $P(A) = \frac{1}{4}$ , por lo tanto tenemos

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{25/204}{1/2} = \frac{25}{102}$$

$$P(B|A) = \frac{P(B \cap A)}{P(A)} = \frac{25/204}{1/4} = \frac{25}{51}$$

## *Tarea 14*

### *El hombre anumérico*

El anumerismo y todos los errores relacionados con el mal uso de los números, esparcido por los medios de comunicación, políticos y cualquier persona común y corriente, es un mal que puede ser tomado como ventaja, con la intención de dirigir a la sociedad o lucrar con la ignorancia. Temas que van desde porcentajes, mal manejo de las nociones de probabilidad y el poder contar, son tópicos merecedores de nuestra atención, debido al gran impacto que tiene en la vida diaria y sobre todo, en lo común de su uso.

En lo personal, creo que el anumerismo es un mal que debe ser combatido, ya que la mayoría de las personas, muchas veces no importando su nivel académico, son incapaces de reconocer algunas situaciones donde son engañadas. Creo que el mal viene desde la percepción de las matemáticas como una asignatura complicada y por ende, muchas personas perciben estos temas como *imposibles* de entender para personas común y corrientes. Sin embargo, es de suma importancia tener un manejo de ciertos conceptos básicos de probabilidad y estadística, principalmente por la importancia que ésta rama de las matemáticas tiene en nuestra vida cotidiana.

### *La falacia del fiscal*

Supongamos que se ha cometido un asesinato y que el autor ha dejado algún tipo de evidencia en la escena del crimen como, por ejemplo, una mancha de sangre en la alfombra. Supongamos que, atendiendo a ciertos marcadores bioquímicos, la sangre encontrada en la escena del crimen es tal que sólo la de una de cada 1000 personas coincide con ella. Tenemos un sospechoso X cuya sangre coincide con la encontrada en la escena del crimen, quién es acusado del asesinato y llevado juicio. El fiscal, durante el juicio, asegura lo siguiente:

*La probabilidad de que la sangre de un inocente coincida con la de la escena*

*del crimen es de 1 entre 1000. La sangre de X coincide con la de la escena del crimen. Entonces, la probabilidad de que sea inocente es de 0.001, es decir, es culpable con probabilidad de 0.999.*

Pero esta aseveración, que puede sonar convincente e influir decisivamente en un juez o un jurado es, sencillamente, falsa. Veamos por qué. Imaginemos que la población de posibles autores del crimen es de 100000 personas y que hay 100 personas cuya sangre coincide con la de la escena del crimen, uno de ellos es el asesino. **Si no hay otra evidencia en contra de X aparte de la coincidencia de la sangre**, resulta que X tiene la misma probabilidad que los otros 99 de ser el asesino, luego su probabilidad de ser inocente sería 0.99 en vez de 0.001. ¿Cómo se explica esta discrepancia? La explicación de la falacia presentada por el fiscal se basa en una simple confusión con respecto a probabilidades condicionales. Llamemos  $H$  a la hipótesis "X es inocente". Naturalmente, será cierta o falsa, aunque no lo sabemos.

La incertidumbre que tenemos respecto de esta hipótesis se expresa mediante la probabilidad  $P(H)$ , que es la probabilidad "*a priori*" de que X sea inocente. Sea  $E$  la evidencia "*la sangre de X coincide con la de la escena del crimen*". Lo que en realidad nos interesa conocer es  $P(H|E)$ , es decir, la probabilidad de que X sea inocente, conociendo la evidencia de que su sangre coincide con la de la alfombra. Y ésta es la probabilidad que el fiscal calcula incorrectamente como 0.001. Porque 0.001 es, en realidad,  $P(E|H)$ , es decir, la probabilidad de que la sangre de X coincida con la de la alfombra, si en realidad es inocente. Así que lo que ha pasado es que el fiscal ha confundido  $P(H|E)$  con  $P(E|H)$ , y ha calculado la segunda cuando pensaba que estaba calculando la primera.

## Tarea 15

### Experimento de Mendel

Gregor Johann Mendel fue un monje agustino católico y naturalista quien formuló, por medio de trabajos que llevó a cabo con diferentes variedades del guisante, las hoy llamadas *Leyes de Mendel* que dieron origen a la herencia genética. Los primeros trabajos en genética fueron realizados por Mendel. Inicialmente efectuó cruces de semillas, las cuales se particularizaron por salir de diferentes estilos y algunas de su misma forma. Mendel publicó sus experimentos con guisantes en 1865 y 1866. Los principales motivos por los que Mendel eligió el guisante como material de trabajo fueron los siguientes

- ▷ Los guisantes eran baratos y fáciles de obtener en el mercado
- ▷ Ocupaban poco espacio y tenían un tiempo de generación relativamente corto.
- ▷ Producían muchos descendientes.
- ▷ Existían variedades diferentes que mostraban distinto color, forma, tamaño, etc. Por lo tanto, presentaban variedad genética.
- ▷ Es una especie *autógama*, se autopoliniza, de manera que el polen de las anteras de una flor cae sobre el estigma de la misma flor.
- ▷ Era sencillo llevar a cabo cruzamientos entre distintas variedades a voluntad.



Figure 19: Experimento de Mendel

Según Mendel realizaba siempre el mismo esquema de cruzamientos: cruzaba dos variedades o líneas puras que diferían en uno o varios caracteres, obtenía la 1<sup>a</sup> generación filial ( $F_1$ ), seguidamente autofecundaba (Ä) los híbridos de la 1<sup>a</sup> generación filial ( $F_1$ ) y obtenía la 2<sup>da</sup> generación filial ( $F_2$ ) y, por último, autofecundaba (Ä) las plantas de la 2<sup>da</sup> generación filial ( $F_2$ ) y conseguía la 3<sup>ra</sup> generación filial ( $F_3$ ). El cruzamiento inicial lo llevaba a cabo en las dos direcciones posibles, es decir, en un caso utilizaba como donador de polen al  $MP_2$  y en el otro al  $MP_1$ , realizó cruzamientos recíprocos:  $FP_1 \times MP_2$  y  $FP_2 \times MP_1$ .

# Tarea 16

## Inversión en tecnologías de Cómputo

Tomando cuenta foco principal de la investigación el futuro del *Hardware* para *Machine Learning* debido a su relevancia, tenemos lo siguiente.

Los algoritmos de *Machine Learning* casi siempre consisten de operaciones matriciales y tensoriales. Estos cálculos se benefician grandemente del cómputo paralelo, lo que nos lleva al entrenamiento de modelos en tarjetas gráficas. La progresión natural del *Hardware* computacional es el siguiente

1. Central Processing Unit (CPU)
2. Graphics Processing Unit (GPU)
3. Field Programmable Gate Array (FPGA)
4. Application-Specific Integrated Circuit (ASIC)

En cada paso de la progresión anterior existe una mejora muy grande en desempeño, el desempeño puede ser medido de las siguientes formas

- ▷ Capacidad Computacional (*throughput*)
- ▷ Eficiencia Energética (cálculos por *Joule*)
- ▷ Eficiencia de Costos (*throughput* por dólar)

Para llevar a cabo la comparación, consideremos la tarea de *mining cryptocurrencies*, la cual un poder computacional considerable a cambio de ganancia financiera. Desde la introducción de *Bitcoin* en 2009, la industria del *crypto-mining* evolucionó del uso de CPUs a GPUs, de GPUs a FPGAs y finalmente de FPGAs a sistemas ASIC.

### Cómputo de Propósito General (CPUvsGPU)

Antes del 2001 el cómputo de propósito general se llevaba a cabo con CPUs y los GPUs eran empleados únicamente para procesar gráficos.

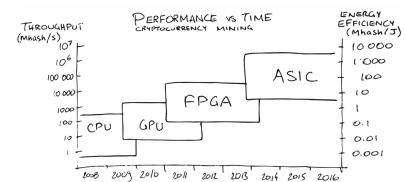


Figure 20: Aproximación de desempeño relativa a un CPU por unidad computacional

El cómputo de propósito general en tarjetas gráficas comenzó a ser práctico cuando los científicos computacionales desarrollaron multiplicación de matrices y las técnicas de factorización para que fueran más rápidas y eficientes. Desde ese momento se ha hecho un gran esfuerzo en la creación de lenguajes de programación para permitir cómputo de propósito general en GPUs, incluyendo *CUDA* y *OpenCL*. De cualquier manera, los GPUs consumen energía notable.

#### *Hardware Especializado: FPGA*

*Field Programmable Gate Arrays(FPGA)* son circuitos integrados cuyos bloques lógicos pueden ser programados y reconfigurados empleando lenguajes de descripción de hardware (HDL). En el caso de la *cryptocurrency*, las tarjetas FPGA marcaron la transición del *mining* a *Hardware* especializado.

Actualmente se hacen esfuerzos para implementar modelos de *Machine Learning* empleando FPGAs. Por ejemplo, la compañía *Altera* implementó unos casos de eso de *AlexNet Convolutional Neural Network* usada para clasificar imágenes.

A finales del 2012, la empresa *Microsoft* comenzó a probar los procesadores basados en FPGAs para su motor de búsqueda *Bing*. Actualmente los FPGAs únicamente empatan a los GPUs en *throughput*, sin embargo consumen menos energía para la misma carga de trabajo, por ende es más factible emplearlos en sistemas de bajo consumo como los autos autónomos.

#### *ASICs*

*Cryptocurrency mining* ha continuado su evolución a hardware especializado y los ASICs se convirtieron rápidamente en la única opción competitiva. La misma tendencia ha comenzado en *Machine Learning*. En Mayo del 2016, ingenieros de *Google* anunciaron que habían creado un ASIC especializado en *Machine Learning* llamado *Tensor Processing Unit(TPU)*. Los servidores TPU corren su propio *RankBrain system*, *StreetView* e incluso el sistema *AlphaGo* que venció al campeón del mundo, Lee Sedol.

#### *Futuro*

Aparentemente la demanda por *Deep Learning* y *Statistical Inference* está dirigiendo la industria del *Hardware* hacia un *Hardware* especializado en *Machine Learning*. Actualmente Google lidera con sus ASICs, sus competidores más cercanos usan FPGAs, y el resto de nosotros

seguimos calentando nuestros hogares con GPUs. Los siguientes pasos de esta evolución de Hardware incluyen nuevos materiales, cómputo biológico y cómputo cuántico.

### *Inversión*

Con la información mostrada en esta sección, la inversión que haría es la siguiente

1. 50% Investigación y Desarrollo en las tecnologías emergentes
2. 20% FPGAs
3. 10% ASICs
4. 5% GPUs
5. 5% CPUs
6. 10% Infraestructura (Redes)

### *Root Mean Square*

En estadística y sus aplicaciones, el valor cuadrático medio (*Root Mean Square RMS*) es una medida estadística de la magnitud de una cantidad variable. Puede calcularse para una serie de valores discretos o para una función matemática de variable continua. El nombre deriva del hecho de que es la raíz cuadrada de la media aritmética de los cuadrados de los valores. Algunas veces la variable toma valores positivos y negativos, como ocurre, por ejemplo, con los errores de media. En tal caso se puede estar interesado en obtener un promedio que no recoja los efectos del signo. Este problema se resuelve, mediante la denominada media cuadrática. Consiste en elevar al cuadrado todas las observaciones, en obtener después su media aritmética y en extraer, finalmente, la raíz cuadrada de dicha media para volver a la unidad de medida original.

La media cuadrática para una colección de  $N$  valores  $\{X_1, X_2, \dots, X_N\}$  de una variable discreta  $X$ , está dada por la fórmula

$$X_{RMS} = \sqrt{\frac{1}{N} \sum_{i=1}^N x_i^2} = \sqrt{\frac{x_1^2 + x_2^2 + \dots + x_N^2}{N}}$$

Para una función de variable continua  $f(t)$  definida sobre el intervalo  $T_1 \leq t \leq T_2$  está dada por la expresión

$$x_{rms} = \sqrt{\frac{1}{T_2 - T_1} \int_{T_1}^{T_2} [f(t)]^2 dt}$$

## Tarea 17

### Eigenvalores y Eigenvectores

Considere una matriz  $\mathbf{A} \in \mathbb{R}^{n \times n}$  dada por

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{bmatrix} \quad (2)$$

**Definición: Eigenvalor y Eigenvector.** Un vector  $\vec{b} \in \mathbb{R}^n$ , tal que  $\vec{b} \neq \vec{0}$ , se dice que es un **eigenvector, vector propio o vector característico**, de la matriz  $\mathbf{A}$  si y sólo si

$$\mathbf{A}\vec{b} = \lambda\vec{b}, \text{ donde } \lambda \in \mathbb{C} \quad (3)$$

Además se dice que el escalar  $\lambda$  es el **eigenvalor, valor propio o valor característico** de la matriz  $\mathbf{A}$  asociado al eigenvector  $\vec{b}$  de manera recíproca, se dice que  $\vec{b}$  es un eigenvector de  $\mathbf{A}$  asociado al eigenvalor  $\lambda$ . Debe notarse que, aún cuando la matriz  $\mathbf{A}$  es real, los eigenvalores asociados a la matriz pueden ser números complejos.

**Teorema I.** El conjunto de todos los eigenvectores  $\vec{b}$  asociados al eigenvalor  $\lambda$  constituyen un subespacio vectorial de  $\mathbb{R}^n$ , conocido como el **eigenespacio** asociado al eigenvalor  $\lambda$ .

Considere

$$\mathbf{A}\vec{b} = \lambda\vec{b}, \text{ o } \mathbf{A}\vec{b} = \mathbf{I}_n\lambda\vec{b}, \text{ o } [\mathbf{A} - \lambda\mathbf{I}_n]\vec{b} = \vec{0} \quad (4)$$

donde  $\mathbf{I}_n$  es la matriz identidad de orden  $n$ . Puesto que, por definición,  $\vec{b} \neq \vec{0}$ , la única posibilidad para que la ecuación (3) se satisfaga es que, la matriz  $[\mathbf{A} - \lambda\mathbf{I}_n]$  sea singular y que  $\vec{b}$  sea un elemento del espacio nulo o kernel de la matriz. Una condición necesaria y suficiente para que la matriz  $[\mathbf{A} - \lambda\mathbf{I}_n]$  sea singular es que su determinante sea cero; es decir

$$p(\lambda) = |\mathbf{A} - \lambda\mathbf{I}_n| = 0 \quad (5)$$

Expandiendo el determinante de la ecuación anterior se obtiene una ecuación polinomial real de  $n$ -ésimo orden en  $\lambda$ . Esta ecuación se denomina la **ecuación característica** de la matriz  $\mathbf{A}$ . Las raíces de la ecuación característica son los eigenvalores de la matriz y los vectores que satisfacen la ecuación (3) son los eigenvectores asociados a los eigenvalores respectivos.

*Método directo de determinación de los eigenvalores y eigenvectores de una matriz*

1. Determine la ecuación característica de la matriz, es decir determine

$$p(\lambda) = |\mathbf{A} - \lambda \mathbf{I}_n| = 0$$

2. Encuentre las  $n$  raíces de la ecuación característica. Estas raíces son los eigenvalores de la matriz.

3. Para cada uno de los eigenvalores determine el subespacio solución de la ecuación

$$[\mathbf{A} - \lambda \mathbf{I}_n] \vec{b} = \vec{0}$$

Estos subespacios solución constituyen el eigenespacio asociado al eigenvalor  $\lambda$ .

### *Caminata al azar*

Supongamos una partícula que se mueve en una dirección, con una probabilidad  $p$  para la derecha y  $q = 1 - p$  para la izquierda. Sabemos que  $p + q = 1$ , y debido a que los eventos son disjuntos, es posible aplicar el principio básico del conteo, lo que nos da como resultado

$$ppppp \dots pqqqqq \dots q = p^{n_1} q^{n_2}$$

donde  $n_1$  y  $n_2$  son el número de pasos a cada lado.

Si se consideran los resultados posibles para 4 movimientos de una partícula, cuando  $p = 0.5$ , se genera un árbol binario donde el número total de pasos dados es  $N = n_1 + n_2$ , que representa la profundidad del árbol binario. Al asociar un resultado a la posición final de la partícula de la forma:  $x = ml$  donde  $m$  es la posición final unitaria tras  $N$  pasos,  $l$  la longitud de los pasos,  $x$  la posición final en el plano unidimensional.

Sabemos que  $-N \leq m \leq N$  y  $m = n_1 - n_2$ . El número de maneras diferentes en el que la partícula puede terminar en  $m$  es representado por

$$N(m) = \frac{N!}{n_1! n_2!}$$

La probabilidad individual de las posiciones  $m$  que se repiten más que otras se puede calcular con la siguiente ecuación

$$W(m) = \frac{N!}{n_1!n_2!} p^{n_1} q^{n_2}$$

Multiplicando la probabilidad previamente calculada para cada caso de pasos  $n_1$  y  $n_2$ , y la cantidad de permutaciones que resulta en  $m$ . Si deseamos conocer la probabilidad de  $m$  es necesario convertir todas nuestras variables de la forma

$$m = n_1 - n_2 = n_1 - (N - n_1) = 2n_1 - N$$

$$n_1 = \frac{(m + N)}{2}$$

$$n_2 = \frac{(m - N)}{2}$$

Sustituyendo se obtiene

$$P(m) = \frac{N!}{\left(\frac{m+N}{2}\right)! \left(\frac{m-N}{2}\right)!} p^{\left(\frac{m+N}{2}\right)} q^{\left(\frac{m-N}{2}\right)}$$

# *Propuesta Examen*

1. ¿De cuántas formas se pueden permutar las letras en la palabra MISSISSIPPI?

$$M = 1, S = 4, I = 4, P = 2$$

$$\frac{11!}{1!4!4!2!}$$

2. Probar el siguiente teorema

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$$

Tenemos  $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r} = \frac{n!}{(r-1)!(n-r+1)!} + \frac{n!}{r!(n-r)!}$ .

Para obtener el mismo denominador en ambas fracciones, multiplicamos la primera fracción por  $\frac{r}{r}$  y la segunda fracción por  $\frac{n-r+1}{n-r+1}$ . Por lo tanto tenemos,

$$\begin{aligned} \binom{n}{r-1} + \binom{n}{r} &= \frac{rn!}{r(r-1)!(n-r+1)!} + \frac{(n-r+1)n!}{r!(n-r+1)(n-r)!} \\ &= \frac{rn!}{r!(n-r+1)!} + \frac{(n-r+1)n!}{r!(n-r+1)!} \\ &= \frac{rn! + (n-r+1)n!}{r!(n-r+1)!} = \frac{[r + (n-r+1)]n!}{r!(n-r+1)!} \\ &= \frac{(n+1)n!}{r!(n-r+1)!} = \frac{(n+1)!}{r!(n-r+1)!} = \binom{n+1}{r} \end{aligned}$$

3. ¿Cuántos números de cuatro cifras pueden formarse con los dígitos 0,1,2,3,...,9 si (a) los números pueden repetirse, (b) si los números no pueden repetirse, (c) si el último número ha de ser cero y los números no pueden repetirse?

(a) La primer cifra puede ser cualquiera menos 0. La segunda, tercera y cuarta pueden ser cualquiera de las 10. Entonces  $9 * 10 * 10 * 10 = 9000$  son los números que pueden formarse.

- (b) La primera puede ser cualquiera menos o. La segunda puede ser cualquiera entre 9 (no puede ser la que ocupó el primer puesto). La tercera puede ser cualquiera entre 8 (no pueden ser ninguna de las que ocupan los dos primeros puestos). La cuarta puede ser cualquiera entre 7 (no pueden ser ninguna de las que ocupan los tres primeros puestos). Entonces  $9 * 9 * 8 * 7 = 4536$  son los números que pueden formarse.
- (c) La primera cifra puede elegirse entre 9, la segunda entre 8 y la tercera entre 7. Entonces  $9 * 8 * 7 = 504$  son los números que pueden formarse.

4. Hallar el valor de  $50!$ .

Para una  $n$  muy grande,  $n! \sqrt{2\pi n} n^n e^{-n}$ . Por tanto

$$50! \sqrt{2\pi(50)} 50^{50} e^{-50} \equiv N$$

Para evaluar  $N$  utilizamos logaritmos de base 10. Así

$$\begin{aligned} \log_{10} N &= \log_{10} (\sqrt{100\pi} 50^{50} e^{-50}) \\ &= \frac{1}{2} \log_{10} 100 + \frac{1}{2} \log_{10} \pi + 50 \log_{10} 50 - 50 \log_{10} e \\ &= \frac{1}{2} \log_{10} 100 + \frac{1}{2} \log_{10} 3.1416 + 50 \log_{10} 50 - 50 \log_{10} 2.718 \\ &= \frac{1}{2}(2) + \frac{1}{2}(0.4972) + 50(1.6990) - 50(0.4343) = 64.4836 \end{aligned}$$

de donde  $N = 3.04 \times 10^{64}$ , un número que tiene 65 dígitos.

5. Una pareja tiene 2 hijos. Encontrar la probabilidad  $p$  de que ambos hijos sean niños si (i) sabemos que el hijo más joven es niño, (ii) sabemos que al menos uno de los hijos es niño. El espacio muestral para el sexo de los dos hijos es  $S = bb, bg, gb, gg$  con probabilidad de  $\frac{1}{4}$  para cada punto. (En este problema la secuencia de cada punto corresponde a la secuencia de nacimientos).

- (i) El espacio muestral reducido consiste de dos elementos,  $\{bb, gb\}$ ; por lo tanto  $p = \frac{1}{2}$ .
- (ii) El espacio muestral reducido consiste de tres elementos,  $\{bb, bg, gb\}$ ; por lo tanto  $p = \frac{1}{3}$ .

6. Dos dígitos son seleccionados aleatoriamente del 1 al 9. Si la suma es par, encontrar la probabilidad  $p$  de que ambos números sean impares. La suma es par si ambos números son pares o si ambos números son impares. Hay 4 números pares (2, 4, 6, 8); por lo tanto hay  $\binom{4}{2} = 6$  formas de escoger dos números pares. Hay 5 números impares (1, 3, 5, 7, 9); por lo tanto hay  $\binom{5}{2} = 10$  formas de escoger dos números impares.

En consecuencia tenemos  $6 + 10 = 16$  formas de escoger dos números tales que su suma es par, dado que 10 de estas formas ocurren cuando ambos números son impares,  $p = \frac{10}{16} = \frac{5}{8}$ .

7. 3 máquinas A,B y C producen respectivamente 60%, 30% y 10% del total de objetos de una fábrica. El porcentaje de salida defectuosa de estas máquinas es respectivamente 2%, 3% y 4%. Un objeto es seleccionado aleatoriamente y se encuentra que está defectuoso. Encontrar la probabilidad de que el objeto fue producido por la máquina C.

Sea  $X = \{\text{objetos defectuosos}\}$  Buscamos  $P(C|X)$ , la probabilidad de que un objeto sea producido por la máquina C dado que está defectuoso. Por el teorema de Bayes tenemos

$$\begin{aligned} P(C|X) &= \frac{P(C)P(X|C)}{P(A)P(X|A) + P(B)P(X|B) + P(C)P(X|C)} \\ &= \frac{(.10)(.04)}{(.60)(.02) + (.30)(.03) + (.10)(.04)} = \frac{4}{25} \end{aligned}$$

8. En el IPN, 4% de los hombres y 1% de las mujeres son más altas que 6 pies. Además, 60% de los estudiantes son mujeres. Si seleccionamos un estudiante aleatoriamente y resulta que es más alto que 6 pies, ¿cuál es la probabilidad de que el estudiante sea una mujer?

Sea  $A = \{\text{número de estudiantes más altos que 6 pies}\}$ . Buscamos  $P(W|A)$ , la probabilidad de que el estudiante es mujer dado que el estudiante es más alto que 6 pies. Por el teorema de Bayes tenemos

$$P(W|A) = \frac{P(W)P(A|W)}{P(W)P(A|W) + P(M)P(A|M)} = \frac{(.60)(.01)}{(.60)(.01) + (.40)(.04)} = \frac{3}{11}$$

9. Una moneda cargada tal que  $P(H) = \frac{3}{4}$  y  $P(T) = \frac{1}{4}$  se lanza 3 veces. Sea  $X$  la variable aleatoria que denota la cadena más larga de caras obtenidas. Encontrar la distribución, esperanza, varianza y desviación estándar de  $X$ . La variable aleatoria  $X$  es definida en el espacio muestra  $S = \{HHH, HHT, HTH, HTT, THH, THT, TTH, TTT\}$ . Los puntos en  $S$  tienen las siguientes probabilidades

$$\begin{aligned} P(HHH) &= \frac{3}{4} * \frac{3}{4} * \frac{3}{4} = \frac{27}{64} \\ P(HHT) &= \frac{3}{4} * \frac{3}{4} * \frac{1}{4} = \frac{9}{64} \\ P(HTH) &= \frac{3}{4} * \frac{1}{4} * \frac{3}{4} = \frac{9}{64} \\ P(HTT) &= \frac{3}{4} * \frac{1}{4} * \frac{1}{4} = \frac{3}{64} \\ P(THH) &= \frac{1}{4} * \frac{3}{4} * \frac{3}{4} = \frac{9}{64} \\ P(THT) &= \frac{1}{4} * \frac{3}{4} * \frac{1}{4} = \frac{3}{64} \\ P(TTH) &= \frac{1}{4} * \frac{1}{4} * \frac{3}{4} = \frac{3}{64} \end{aligned}$$

$$P(TTT) = \frac{1}{4} * \frac{1}{4} * \frac{1}{4} = \frac{1}{64}$$

Dado que  $X$  denota la cadena más larga de caras obtenidas

$$X(TTT) = 0$$

$$X(HTT) = 1$$

$$X(HTH) = 1$$

$$X(THT) = 1$$

$$X(TTH) = 1$$

$$X(HHT) = 2$$

$$X(THH) = 2$$

$$X(HHH) = 3$$

Por lo tanto, tenemos que el conjunto imagen de  $X$  es  $X(S) = \{0, 1, 2, 3\}$ . La probabilidad  $f(x_i)$  de cada número  $x_i$  en  $X(S)$  es obtenida sumando las probabilidades de los puntos en  $S$  cuya imagen es  $x_i$ .

$$f(0) = P(TTT) = \frac{1}{64}$$

$$f(1) = P(HTT) + P(HTH) + P(THT) + P(TTH) = \frac{18}{64}$$

$$f(2) = P(HHT) + P(THH) = \frac{18}{64}$$

$$f(3) = P(HHH) = \frac{27}{64}$$

En consecuencia, la distribución de  $X$  es la siguiente

$x_i$	0	1	2	3
$f(x_i)$	$\frac{1}{64}$	$\frac{18}{64}$	$\frac{18}{64}$	$\frac{27}{64}$

Tenemos

$$\mu = E(X) = 0 \cdot \frac{1}{64} + 1 \cdot \frac{18}{64} + 2 \cdot \frac{18}{64} + 3 \cdot \frac{27}{64} = \frac{135}{64} = 2.1$$

$$E(X^2) = 0 \cdot \frac{1}{64} + 1 \cdot \frac{18}{64} + 4 \cdot \frac{18}{64} + 9 \cdot \frac{27}{64} = \frac{333}{64} = 5.2$$

$$\sigma^2 = \text{Var}(X) = E(X^2) - \mu^2 = 5.2 - (2.1)^2 = .8$$

$$\sigma = \sqrt{.8} = .9$$

10. Una moneda justa es lanzada 3 veces. Sea  $X$  la variable aleatoria que denota 0 o 1 dependiendo si sale cara o cruz en el primer lanzamiento,

y sea  $Y$  la variable aleatoria que denota el número de caras que salen. Determinar (i) las distribuciones de  $X$  y  $Y$ , (ii) la distribución conjunta  $h$  de  $X$  y  $Y$ .

- (i) El espacio muestra  $S$  consiste de los siguientes 8 puntos, cada uno con probabilidad  $\frac{1}{8}$

$$S = \{HHH, HHT, HTH, HTT, THH, THT, TTH, TTT\}$$

Tenemos

$$X(HHH) = 0, X(HHT) = 0, X(HTH) = 0, X(HTT) = 0,$$

$$X(THH) = 1, X(THT) = 1, X(TTH) = 1, X(TTT) = 1$$

Y por otra parte

$$Y(HHH) = 3$$

$$Y(HHT) = 2$$

$$Y(HTH) = 2$$

$$Y(THH) = 2$$

$$Y(HTT) = 1$$

$$Y(THT) = 1$$

$$Y(TTH) = 1$$

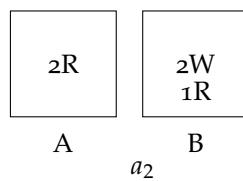
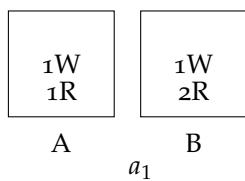
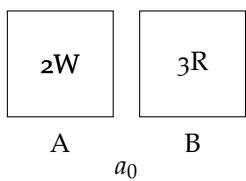
$$Y(TTT) = 0$$

Tenemos que las distribuciones de probabilidad de  $X$  y  $Y$  son

$x_i$	0	1
$f(x_i)$	$\frac{1}{2}$	$\frac{1}{2}$

$y_i$	0	1	2	3
$g(y_i)$	$\frac{1}{8}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{1}{8}$

11. Hay 2 canicas blancas en una urna A y hay 3 canicas rojas en una urna B. En cada paso del proceso una canica es seleccionada de cada urna y las dos canicas seleccionadas son intercambiadas. Sea el estado  $a_i$  del sistema el número  $i$  de canicas rojas en la urna A. (i) Encontrar la matriz de transición  $P$ . (ii) ¿Cuál es la probabilidad de que se encuentren 2 canicas rojas en la urna A después de 3 pasos? (iii) A largo plazo, ¿cuál es la probabilidad de que se encuentren 2 canicas rojas en la urna A?



(i) Si el sistema se encuentra en el estado  $a_0$ , se debe seleccionar una canica de cada urna e intercambiarlas, por lo tanto, la primer fila de la matriz de transición es  $(0, 1, 0)$ . Ahora supongamos que el sistema se encuentra en el estado  $a_1$ . Este se puede mover al estado  $a_0$  si y solo si se selecciona una canica roja de la urna A y una canica blanca de la urna B, la probabilidad de que eso suceda es  $\frac{1}{2} \cdot \frac{1}{3} = \frac{1}{6}$ . Por lo tanto  $p_{10} = \frac{1}{6}$ . El sistema se puede mover del estado  $a_1$  al estado  $a_2$  si y solo si se selecciona una canica blanca de la urna A y una canica roja de la urna B; la probabilidad de que esto suceda es de  $\frac{1}{2} \cdot \frac{2}{3} = \frac{1}{3}$ . Por lo tanto  $p_{12} = \frac{1}{3}$ . Por último, la probabilidad de que el sistema permanezca en el estado  $a_1$  es  $p_{11} = 1 - \frac{1}{6} - \frac{1}{3} = \frac{1}{2}$ . En consecuencia la segunda fila de la matriz de transición es  $(\frac{1}{6}, \frac{1}{2}, \frac{1}{3})$ .

Por último supongamos que el sistema se encuentra en el estado  $a_2$ . Una canica roja debe ser seleccionada de la urna A. Por otra parte, si una canica roja es seleccionada de la urna B, con probabilidad  $\frac{1}{3}$ , el sistema permanece en el estado  $a_2$ ; y si una canica blanca es seleccionada de la urna B, con probabilidad  $\frac{2}{3}$ , el sistema se mueve al estado  $a_1$ . Notar que el sistema nunca se puede mover del estado  $a_2$  al estado  $a_0$ . Por lo tanto, la tercer fila de la matriz de transición es  $(0, \frac{2}{3}, \frac{1}{3})$ . Entonces la matriz de transición es

$$P = \begin{matrix} & a_0 & a_1 & a_2 \\ a_0 & 0 & 1 & 0 \\ a_1 & \frac{1}{6} & \frac{1}{2} & \frac{1}{3} \\ a_2 & 0 & \frac{2}{3} & \frac{1}{3} \end{matrix}$$

(ii) El sistema empieza en el estado  $a_0$ , es decir,  $p^{(0)} = (1, 0, 0)$ . Por lo tanto

$$p^{(1)} = p^{(0)}P = (0, 1, 0)$$

$$p^{(2)} = p^{(1)}P = \left(\frac{1}{6}, \frac{1}{2}, \frac{1}{3}\right)$$

$$p^{(3)} = p^{(2)}P = \left(\frac{1}{12}, \frac{23}{36}, \frac{5}{18}\right)$$

Por lo tanto, la probabilidad de que se encuentren 2 canicas rojas en la urna A después de 3 pasos es  $\frac{5}{18}$ .

(iii) Buscamos el único vector de probabilidad fijo  $t$  de la matriz de transición  $P$ . Primero buscamos cualquier vector fijo  $u = (x, y, z)$

$$(x, y, z) \begin{pmatrix} 0 & 1 & 0 \\ \frac{1}{6} & \frac{1}{2} & \frac{1}{3} \\ 0 & \frac{2}{3} & \frac{1}{3} \end{pmatrix} = (x, y, z) \quad \text{o} \quad \begin{cases} \frac{1}{6}y = x \\ x + \frac{1}{2}y + \frac{2}{3}z = y \\ \frac{1}{3}y + \frac{1}{3}z = z \end{cases}$$

Sea  $x = 1$ . Sustituyendo en la primera ecuación, obtenemos  $y = 6$  y sustituyendo en la tercera ecuación tenemos  $z = 3$ . Por lo tanto  $u = (1, 6, 3)$ . Multiplicando  $u$  por  $\frac{1}{1+6+3} = \frac{1}{10}$  obtenemos el único vector de probabilidad fijo  $t = (.1, .6, .3)$ . Por lo tanto, a largo plazo, 30% del tiempo encontraremos 2 canicas rojas en la urna A.

12. Supongamos que existen dos fábricas de bombillas en el mercado. Las bombillas de la fábrica X funcionan alrededor de 5000 horas en el 99% de los casos, mientras que las bombillas de la fábrica Y funcionan alrededor de 5000 horas el 95% de los casos. Se sabe que la fábrica X provee el 60% del total de bombillas disponibles. ¿Cuál es la probabilidad de que el foco comprado funcione más de 5000 horas?

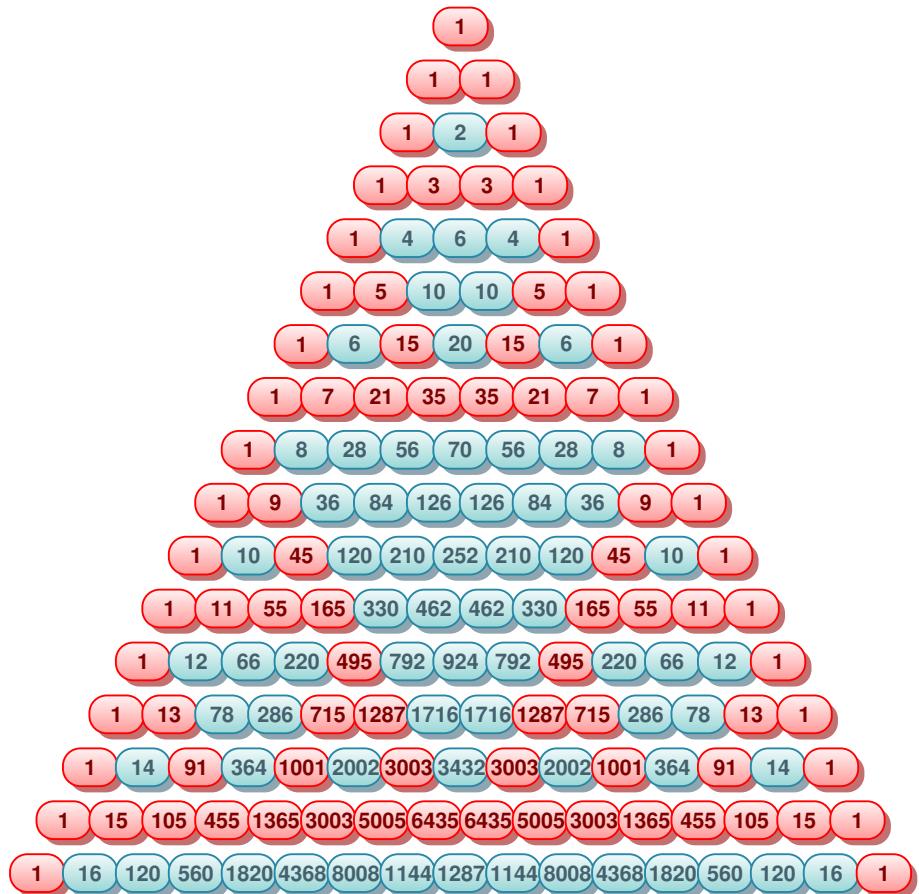
- ▷  $P(B_x) = \frac{6}{10}$ , la bombilla fue hecha por la fábrica X.
- ▷  $P(B_y) = \frac{4}{10}$ , la bombilla fue hecha por la fábrica Y.
- ▷  $P(A|B_x) = \frac{99}{100}$ , la bombilla hecha por X funcionará alrededor de 5000 horas.
- ▷  $P(A|B_y) = \frac{95}{100}$ , la bombilla hecha por Y funcionará alrededor de 5000 horas.

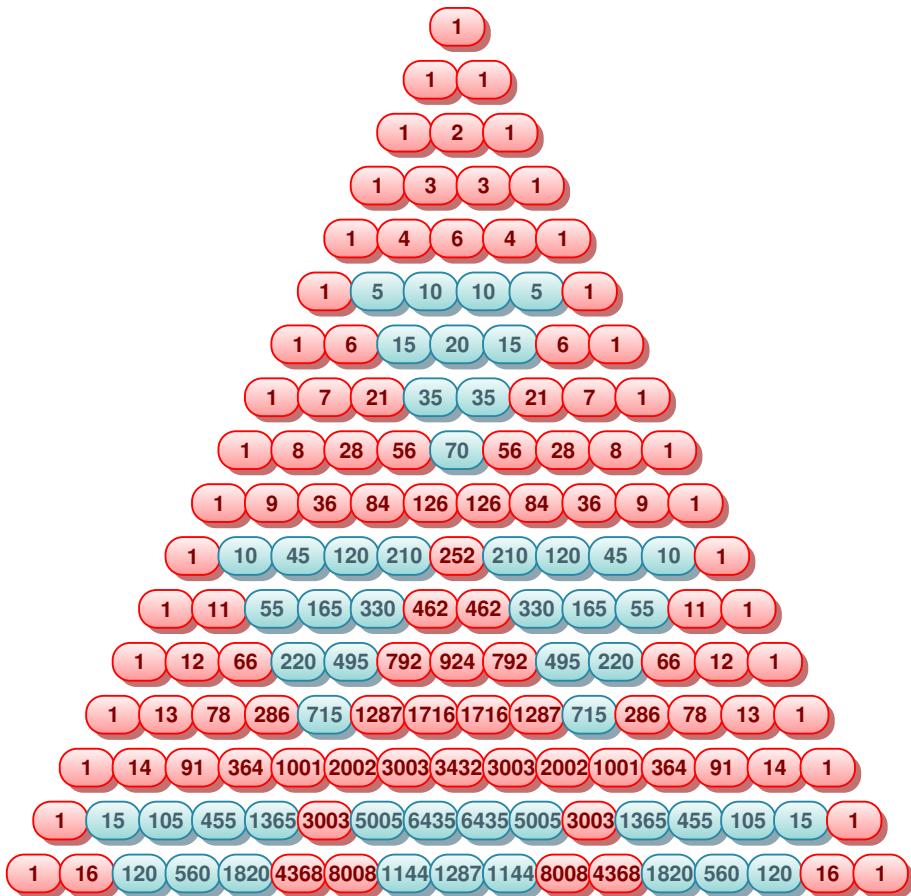
Aplicando la ley de la probabilidad total tenemos

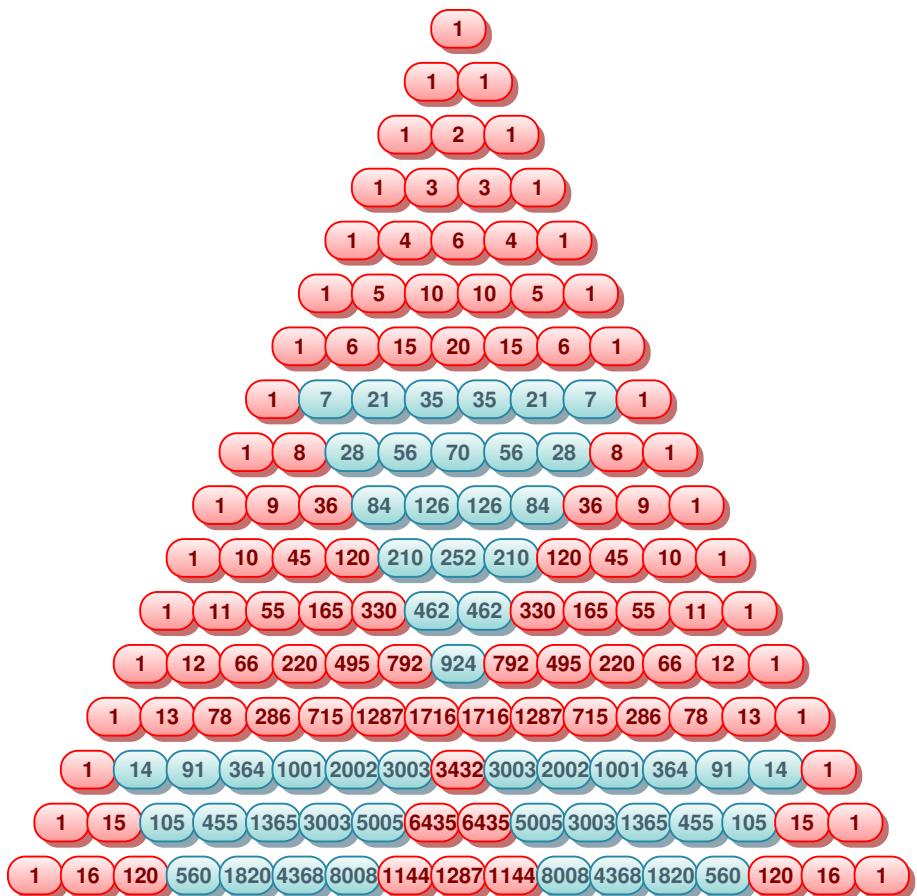
$$\begin{aligned} P(A) &= P(A|B_x) \cdot P(B_x) + P(A|B_y) \cdot P(B_y) \\ &= \frac{99}{100} \cdot \frac{6}{10} + \frac{95}{100} \cdot \frac{4}{10} = \frac{974}{1000} \end{aligned}$$

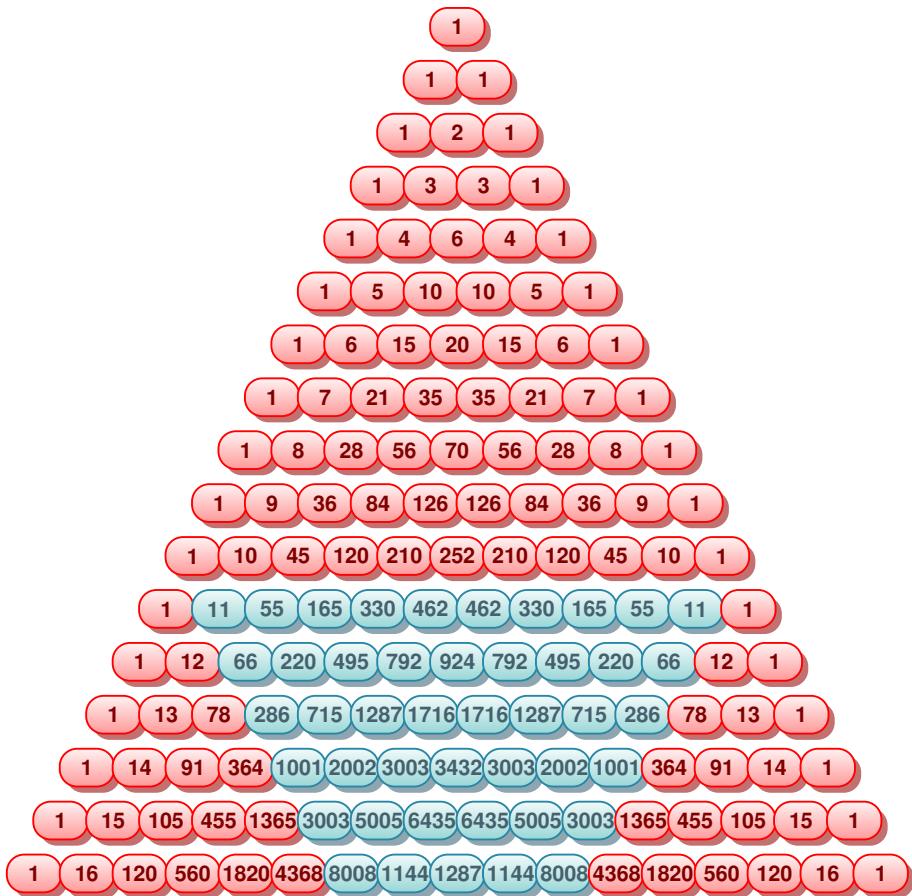
Por lo tanto la probabilidad de que cualquier bombilla funcione más de 5000 horas es del 97.4%

Triángulo de Pascal  $n=16$ , factores de  
3,5,7 y 11









## Bibliography

Joseph K. Blitzstein and Jessica Hwang. *Introduction to Probability*. CRC Press, first edition, May 2015.

Kees Dullemond and Kasper Peeters. Introduction to tensor calculus, 2010.

Ph.D Hwei P. Hsu. *Probability, Random variables, and Random Processes*. McGraw-Hill, United States of America, 1997.

David P. Mowry. *German Cipher Machines of Wolrd War II*. National Security Agency, 2014.

Christof Paar and Jan Pelzl. *Understanding Cryptography, a textbook for Students and Practitioners*. Springer, 2010.

Simon Singh. *The Simpsons and their mathematical secrets*. BLOOMSBURY, 2009.

Ian Stewart. *How to cut a cake and other mathematical conundrums*. OXFORD University Press, first edition, 2006.