樹莓派, 樹莓派之學習, 樹莓派之教育

時間序列：生成函數《十前》

2017-03-06 | 懸鉤子 | 發表迴響

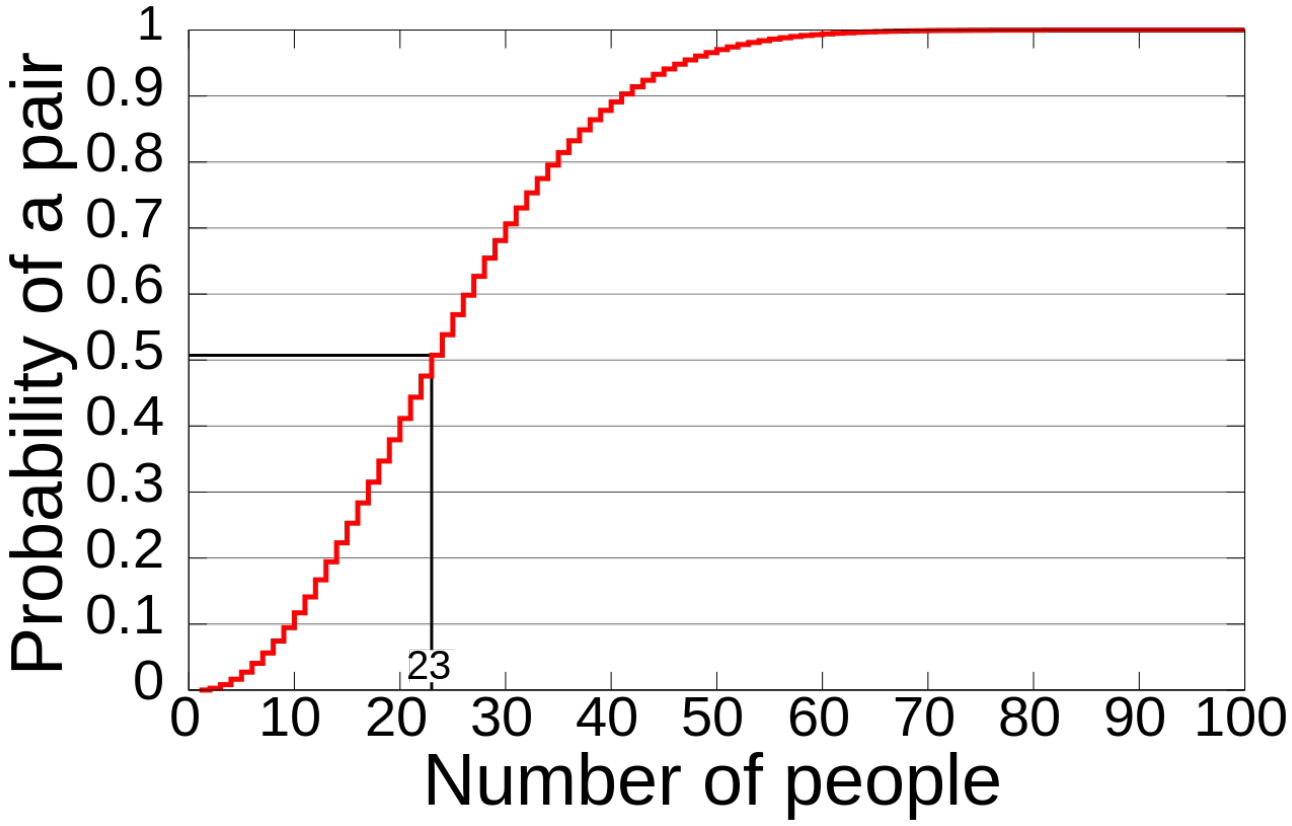
何謂『獨立思考』呢？『直覺』會與『邏輯』衝突嗎？？有個稱作『生日問題』

Birthday problem

In probability theory, the **birthday problem** or **birthday paradox**[nb 1] concerns the probability that, in a set of n randomly chosen people, some pair of them will have the same birthday. By the pigeonhole principle, the probability reaches 100% when the number of people reaches 367 (since there are only 366 possible birthdays, including February 29). However, 99.9% probability is reached with just 70 people, and 50% probability with 23 people. These conclusions are based on the assumption that each day of the year (except February 29) is equally probable for a birthday.

This logic has applications, for example a cryptographic attack called the birthday attack, which uses this probabilistic model to reduce the complexity of finding a collision for a hash function.

The history of the problem is obscure. W. W. Rouse Ball indicated (without citation) that it was first discussed by Harold Davenport.[1] However, Richard von Mises proposed an earlier version of what is considered today to be the birthday problem.[2] The problem was featured by Martin Gardner in his April 1957 “Mathematical Games” column in *Scientific American*.



The computed probability of at least two people sharing a birthday versus the number of people

.....

Calculating the probability

The problem is to compute the approximate probability that, in a group of *n* people, at least two have the same birthday. For simplicity, disregard variations in the distribution, such as leap years, twins, seasonal or weekday variations, and assume that the 365 possible birthdays are equally likely. (Real-life birthday distributions are not uniform, since not all dates are equally likely, but these irregularities have little effect on the analysis.[nb 2])

The goal is to compute $P(A)$, the probability that at least two people in the room have the same birthday. However, it is simpler to calculate $P(A')$, the probability that no two people in the room have the same birthday. Then, because A and A' are the only two possibilities and are also mutually exclusive, $P(A) = 1 - P(A')$.

In deference to widely published solutions concluding that 23 is the minimum number of people necessary to have a *P*(*A*) that is greater than 50%, the following calculation of *P*(*A*) will use 23 people as an example. If one numbers the 23 people from 1 to 23, the event that all 23 people have different birthdays is the same as the event that person 2 does not have the same birthday as person 1, and that person 3 does not have the same birthday as either person 1 or person 2, and so on, and finally that person 23 does not have the same birthday as any of persons 1 through 22. Let these events respectively be called "Event 2", "Event 3", and so on. One may also add an "Event 1", corresponding to the event of person 1 having a birthday, which occurs with probability 1. This conjunction of events may be computed using conditional probability: the probability of Event 2 is 364/365, as person 2 may have any birthday other than the birthday of person 1. Similarly, the probability of Event 3 given that Event 2 occurred is 363/365, as person 3 may have any of the birthdays not already taken by persons 1 and 2. This continues until finally the probability of Event 23 given that all preceding events occurred is 343/365. Finally, the principle of conditional probability implies that *P*(*A*') is equal to the product of these individual probabilities:

$$P(A') = \frac{365}{365} \times \frac{364}{365} \times \frac{363}{365} \times \frac{362}{365} \times \cdots \times \frac{343}{365} \quad (1)$$

The terms of equation (**1**) can be collected to arrive at:

$$P(A') = \left(\frac{1}{365}\right)^{23} \times (365 \times 364 \times 363 \times \cdots \times 343) \quad (2)$$

Evaluating equation (**2**) gives $P(A') \approx 0.492703$

Therefore, $P(A) \approx 1 - 0.492703 = 0.507297$ (50.7297%)

This process can be generalized to a group of *n* people, where *p*(*n*) is the probability of at least

two of the *n* people sharing a birthday. It is easier to first calculate the probability *p*(*n*) that all *n* birthdays are *different*. According to the pigeonhole principle, *p*(*n*) is zero when *n* > 365. When $n \leq 365$:

$$\begin{aligned}\bar{p}(n) &= 1 \times \left(1 - \frac{1}{365}\right) \times \left(1 - \frac{2}{365}\right) \times \cdots \times \left(1 - \frac{n-1}{365}\right) \\ &= \frac{365 \times 364 \times \cdots \times (365 - n + 1)}{365^n} \\ &= \frac{365!}{365^n (365-n)!} = \frac{n! \cdot \binom{365}{n}}{365^n} = \frac{{}_{365}P_n}{365^n}\end{aligned}$$

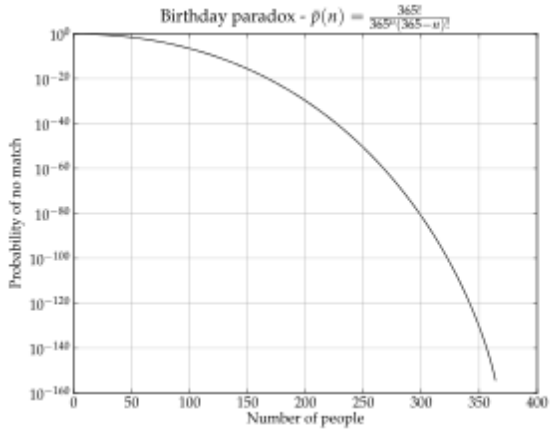
where '!' is the factorial operator, $\binom{365}{n}$ is the binomial coefficient and ${}_k P_r$ denotes permutation.

The equation expresses the fact that the first person has no one to share a birthday, the second person cannot have the same birthday as the first (364/365), the third cannot have the same birthday as either of the first two (363/365), and in general the n^{th} birthday cannot be the same as any of the *n* − 1 preceding birthdays.

The event of at least two of the *n* persons having the same birthday is complementary to all *n* birthdays being different. Therefore, its probability *p*(*n*) is

$$p(n) = 1 - \bar{p}(n).$$

The following table shows the probability for some other values of *n* (this table ignores the existence of leap years, as described above, as well as assuming that each birthday is equally likely):



The probability that no two people share a birthday in a group of *n* people. Note that the vertical scale is logarithmic (each step down is 10^{20} times less likely).

N	***P*(*N*)**
1	0.0%
5	2.7%
10	11.7%
20	41.1%
23	50.7%
30	70.6%
40	89.1%
50	97.0%
60	99.4%
70	99.9%
100	99.99997%
200	99.9999999999999999999999998%
300	$(100 - (6\times10^{-80}))\%$
350	$(100 - (3\times10^{-129}))\%$
365	$(100 - (1.45\times10^{-155}))\%$
366	100%
367	100%

的疑惑誠讓人驚訝，更別說那個『鴿巢原理』

Pigeonhole principle

In mathematics, the **pigeonhole principle** states that if n items are put into m containers, with $n > m$, then at least one container must contain more than one item.[1] This theorem is exemplified in real life by truisms like "there must be at least two left gloves or two right gloves in a group of three gloves". It is an example of a counting argument, and despite seeming intuitive it can be used to demonstrate possibly unexpected results; for example, that two people in London have the same number of hairs on their heads.

The first formalization of the idea is believed to have been made by Peter Gustav Lejeune Dirichlet in 1834 under the name *Schubfachprinzip* ("drawer principle" or "shelf principle"). For this reason it is also commonly called **Dirichlet's box principle** or **Dirichlet's drawer principle**.[2] This should not be confused with **Dirichlet's principle**, a term introduced by Riemann that refers to the minimum principle for harmonic functions.

The principle has several generalizations and can be stated in various ways. In a more quantified version: for natural numbers k and m, if $n = km + 1$ objects are distributed among m sets, then the pigeonhole principle asserts that at least one of the sets will contain at least $k + 1$ objects.[3] For arbitrary n and m this generalizes to $k + 1 = \lfloor (n - 1)/m \rfloor + 1$, where $\lfloor \ldots \rfloor$ is the floor function.

Though the most straightforward application is to finite sets (such as pigeons and boxes), it is also used with infinite sets that cannot be put into one-to-one correspondence. To do so requires the formal statement of the pigeonhole principle, which is *"there does not exist an injective function whose codomain is smaller than its domain"*. Advanced mathematical proofs like Siegel's lemma build upon this more general concept.

Pigeons in holes. Here there are *n* = 10 pigeons in *m* = 9 holes. Since 10 is greater than 9, the pigeonhole principle says that at least one hole has more than one pigeon.

真叫人瞋目結舌耶！果然『尸乂ㄨ數』能夠『解題』耶！！要講得或不得實有『思路』哉？？！！寫此『偶然』似乎『必然』之事也 ！！ ？？

依據鴿巢原理， n < 365 個人生日全不相同的機率為：

$$\bar{p}(n) = 1 \cdot \left(1 - \frac{1}{365}\right) \cdot \left(1 - \frac{2}{365}\right) \cdots \left(1 - \frac{n-1}{365}\right) = \frac{365}{365} \cdot \frac{364}{365} \cdot \frac{363}{365} \cdot \frac{362}{365} \cdots \frac{365-n+1}{365}$$

由 $e^{-x},\ x \leq 1$ 展開的泰勒級數

$= 1 - x + (\frac{x^2}{2!} - \frac{x^3}{3!}) + \cdots + (\frac{x^{2n}}{2n!} - \frac{x^{2n+1}}{(2n+1)!}) + \cdots$

可知

$e^{-x} > 1 - x$ 。

所以

$\bar{p}(n) < e^{\frac{-1}{365}} \cdot e^{\frac{-2}{365}} \cdots e^{\frac{-(n-1)}{365}} = e^{\frac{-n(n-1)}{730}}$ 。

當 $n \geq 23$ 時，$e^{\frac{-n(n-1)}{730}} < \frac{1}{2}$，得到了此神奇數字『二十三』之推導。這或許就是 Halmos 先生追求的『理解』之『意義』吧。

Halmos寫道：

這個推導是基於一些數學系學生必須掌握的重要工具。生日問題曾經是一個絕妙的例子，用來演示純思維是如何勝過機械計算：一兩分鐘就可以寫出這些不等式，而乘法運算則需要更多時間，並更易出錯，無論使用的工具是一隻鉛筆還是一台老式電腦。計算器不能提供的是理解力，或數學才能，或產生更高級、普適化理論的堅實基礎。[1]

如是者在重要論述定理前，總會思之再三乎☆

Functions of independent random variables

Probability generating functions are particularly useful for dealing with functions of independent random variables. For example:

- If $X_1, X_2, \ldots, X_n$ is a sequence of independent (and not necessarily identically distributed) random variables, and

$$S_n = \sum_{i=1}^{n} a_i X_i,$$

where the a_i are constants, then the probability generating function is given by

$$G_{S_n}(z) = \mathbf{E}(z^{S_n}) = \mathbf{E}(z^{\sum_{i=1}^{n} a_i X_i,}) = G_{X_1}(z^{a_1}) G_{X_2}(z^{a_2}) \cdots G_{X_n}(z^{a_n}).$$

For example, if

$$S_n = \sum_{i=1}^{n} X_i,$$

then the probability generating function, $G_{S_n}(z)$, is given by

$$G_{S_n}(z) = G_{X_1}(z) G_{X_2}(z) \cdots G_{X_n}(z).$$

It also follows that the probability generating function of the difference of two independent random variables $S = X_1 - X_2$ is

$$G_S(z) = G_{X_1}(z) G_{X_2}(1/z).$$

- Suppose that N is also an independent, discrete random variable taking values on the non-negative integers, with probability generating function G_N. If the $X_1, X_2, \ldots, X_N$ are independent *and* identically distributed with common probability generating function G_X, then

$$G_{S_N}(z) = G_N(G_X(z)).$$

This can be seen, using the law of total expectation, as follows:

$$G_{S_N}(z) = \mathbf{E}(z^{S_N}) = \mathbf{E}(z^{\sum_{i=1}^{N} X_i}) = \mathbf{E}\left(\mathbf{E}(z^{\sum_{i=1}^{N} X_i} | N)\right) = \mathbf{E}\left((G_X(z))^N\right) = G_N(G_X(z)).$$

This last fact is useful in the study of Galton–Watson processes.

- Suppose again that N is also an independent, discrete random variable taking values on the non-negative integers, with probability generating function G_N and probability density $f_i = \mathbf{Pr}\{N = i\}$. If the $X_1, X_2, \ldots, X_N$ are independent, but *not* identically distributed random variables, where G_{X_i} denotes the probability generating function of X_i, then

$$G_{S_N}(z) = \sum_{i \geq 1} f_i \prod_{k=1}^{i} G_{X_i}(z).$$

For identically distributed X_i this simplifies to the identity stated before. The general case is sometimes useful to obtain a decomposition of S_N by means of generating functions.