

5. Generating functions

5.1. Definitions and basic properties

The idea of generating functions comes from analysis and combinatorics. If c_0, c_1, \dots is a sequence of complex numbers then we can define the power series

$$G(s) = \sum_{k=0}^{\infty} c_k \cdot s^k \quad \text{for } s \in \mathbb{C}.$$

We know from analysis that such power series converge for $|s| < R$ where R is the radius of convergence. Analysis further gives that

$$\frac{1}{R} = \limsup_{n \rightarrow \infty} \sqrt[n]{|c_n|}.$$

If $|c_n| \leq 1$ for all n then

$$\frac{1}{R} \leq 1 \Rightarrow R \geq 1.$$

In this chapter we will only look at non-negative integer valued random variables.

○ Definition: Let X be a random variable with values $0, 1, 2, \dots$

We define the generating function of X , denoted by $G_X(s)$ as the power series

$$G_X(s) = \sum_{k=0}^{\infty} P(X=k) \cdot s^k$$

Comments:

(i) The idea is to "pack" up the distribution in a function.

(ii) Since $\sum_{k=0}^{\infty} P(X=k) = 1$.

the power series is dominated by $P(X=k)$ for $|s| \leq 1$ and converges uniformly to a continuous function.

Examples:

(i) if $X \sim \text{Bin}(n, p)$ we have

$$\begin{aligned} G_X(s) &= \sum_{k=0}^n P(X=k) \cdot s^k \\ &= \sum_{k=0}^n \binom{n}{k} p^k q^{n-k} \cdot s^k \\ &= \sum_{k=0}^n \binom{n}{k} (ps)^k q^{n-k} \\ &= (ps + q)^n. \end{aligned}$$

(ii) if $X \sim \text{Po}(\lambda)$ we have

$$\begin{aligned} G_X(s) &= \sum_{k=0}^{\infty} P(X=k) s^k \\ &= \sum_{k=0}^{\infty} \frac{e^{-\lambda} \cdot \lambda^k}{k!} \cdot s^k \\ &= (*) \end{aligned}$$

$$\begin{aligned}
 (*) &= e^{-\lambda} \cdot \sum_{k=0}^{\infty} \frac{(\lambda s)^k}{k!} \\
 &= e^{-\lambda} \cdot e^{\lambda s} \\
 &= e^{-\lambda(1-s)}
 \end{aligned}$$

(iii) Let $X \sim \text{Neg Bin}(m, p)$.

From analysis we have that
for $|x| < 1$

$$(1+x)^a = \sum_{k=0}^{\infty} \binom{a}{k} x^k \quad \text{where}$$

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

The above formula is known as the Newton formula. Replace x by $-x$ and let $a = -r$ for some integer $r > 0$.

We get

$$\begin{aligned}(1-x)^{-r} &= \sum_{k=0}^{\infty} \binom{-r}{k} \cdot (-x)^k \\ &= \sum_{k=0}^{\infty} \frac{(-r)(-r-1)\dots(-r-k+1)}{k!} (-1)^k \cdot x^k \\ &= \sum_{k=0}^{\infty} \frac{r(r+1)\dots(r+k-1)}{k!} \cdot x^k \\ &= \sum_{k=0}^{\infty} \frac{(r-1)! \cdot r(r+1)\dots(r+k-1)}{(r-1)! \cdot k!} x^k \\ &= \sum_{k=0}^{\infty} \frac{(r+k-1)!}{(r-1)! \cdot k!} x^k \\ &= \sum_{k=0}^{\infty} \binom{r+k-1}{r-1} x^k.\end{aligned}$$

We compute

$$\begin{aligned}G_X(s) &= \sum_{k=m}^{\infty} P(X=k) \cdot s^k \\ &= \sum_{k=m}^{\infty} \binom{k-1}{m-1} \cdot p^m \cdot q^{k-m} \cdot s^k \\ &= (*)\end{aligned}$$

$$(*) = \sum_{l=0}^{\infty} \binom{m+l-1}{m-1} p^m \cdot q^l s^{m+l}$$

$$= p^m \cdot s^m \cdot \sum_{l=0}^{\infty} \binom{m+l-1}{m-1} s^l \cdot q^l$$

$$= \frac{p^m \cdot s^m}{(1-qs)^m}$$

$$= \left(\frac{ps}{1-qs} \right)^m$$

(iv) The computation in previous example gives

$$(1-x)^{-a} = \sum_{k=0}^{\infty} \frac{(a)_k}{k!} \cdot x^k \quad |x| < 1.$$

Let X have the Po'lya distribution

$$P(X=k) = \frac{\beta^a (a)_k}{k! (1+\beta)^{a+k}}$$

We have

$$\begin{aligned}G_X(s) &= \sum_{k=0}^{\infty} P(X=k) \cdot s^k \\&= \sum_{k=0}^{\infty} \frac{\beta^a (a)_k}{k! (1+\beta)^{a+k}} \cdot s^k \\&= \sum_{k=0}^{\infty} \frac{\beta^a (a)_k}{k! (1+\beta)^a} \left(\frac{s}{1+\beta}\right)^k \\&= \frac{\beta^a}{(1+\beta)^a} \cdot \left(1 - \frac{s}{1+\beta}\right)^{-a} \\&= \left(\frac{\beta}{1+\beta-s}\right)^a\end{aligned}$$

Theorem 5.1: Let X be a nonnegative integer valued random variable and let $G_X(s)$ be its generating function.

Then $G_X(s)$ uniquely determines the distribution of X .

Proof: Since $G_X(s)$ converges for $|s| < 1$ we have

$$G_X^{(n)}(0) = n! P(X=n).$$

Theorem 6.2: Let X be an integer valued random variable with generating function $G_X(s)$.

(i)

$$E(X) = \lim_{s \uparrow 1} G_X'(s)$$

(ii)

$$E[X(X-1)\dots(X-m+1)]$$

$$= \lim_{s \uparrow 1} G_X^{(m)}(s)$$

Proof: Let $\varepsilon > 0$ and assume first that $E(X) < \infty$.

There is a N_ε such that for $n \geq N_\varepsilon$ we have $\sum_{k=n}^{\infty} k P(X=k) < \varepsilon$.

This means that

$$E(X) - \sum_{k=0}^{N_\varepsilon-1} k P(X=k) < \varepsilon.$$

Since all the coefficients in the power series are non-negative we

have that for $s \in (0, 1)$

$$\sum_{k=0}^{N_\varepsilon-1} k P(X=k) s^{k-1} \leq G'_X(s) \leq E(X).$$

As $s \uparrow 1$ we have

$$\sum_{k=0}^{N_\varepsilon-1} k P(X=k) \leq \lim_{s \uparrow 1} G'_X(s) \leq E(X)$$

The limit exists because $G_X(s)$ is nondecreasing on $(0, 1)$. But the above means that

$$E(X) - \varepsilon \leq \lim_{s \uparrow 1} G'_X(s) \leq E(X)$$

for all $\varepsilon > 0$.

If $E(X) = \infty$ we have that

$$\lim_{\lambda \uparrow 1} G_X'(\lambda) \geq \sum_{k=1}^N k P(X=k)$$

for any finite N . This implies

that $\lim_{\lambda \uparrow 1} G_X'(\lambda) = \infty$.

(ii) The proof is similar.

Theorem 5.3: Let X, Y be independent.

Then

$$G_{X+Y}(\lambda) = G_X(\lambda) \cdot G_Y(\lambda)$$

Proof: We can write

$$E(\lambda^X) = \sum_{k=0}^{\infty} \lambda^k \cdot P(X=k) = G_X(\lambda)$$

Then

$$\begin{aligned} E(\lambda^{X+Y}) &= E(\lambda^X \cdot \lambda^Y) \\ &\stackrel{\text{indp}}{=} E(\lambda^X) \cdot E(\lambda^Y) \end{aligned}$$

$$= G_X(s) \cdot G_Y(s)$$

Comment: This is the most important property of generating functions.

By extension we have for

○ independent X_1, X_2, \dots, X_r

$$G_{X_1 + X_2 + \dots + X_r}(s) = G_{X_1}(s) \cdot G_{X_2}(s) \cdots G_{X_r}(s)$$

Examples:

○ (i) X, Y independent $X \sim \text{Bin}(m, p)$ and $Y \sim \text{Bin}(n, p)$. We have

$$\begin{aligned} G_{X+Y}(s) &= G_X(s) \cdot G_Y(s) \\ &= (ps + q)^m \cdot (ps + q)^n \\ &= (ps + q)^{m+n} \end{aligned}$$

This last function is the generating function of the Bin $(m+n, p)$ distribution. It follows, by uniqueness, $X+Y \sim \text{Bin}(m+n, p)$.

(ii) Let X, Y be independent and

$$P(X=k) = \frac{\beta^a (a)_k}{k! (1+\beta)^{a+k}}, \quad k=0,1,\dots$$

$$P(Y=l) = \frac{\beta^b (b)_l}{l! (1+\beta)^{b+l}}, \quad l=0,1,\dots$$

We have

$$\begin{aligned} G_{X+Y}(s) &= G_X(s) \cdot G_Y(s) \\ &= \left(\frac{\beta}{1+\beta-s} \right)^a \cdot \left(\frac{\beta}{1+\beta-s} \right)^b \\ &= \left(\frac{\beta}{1+\beta-s} \right)^{a+b} \end{aligned}$$

Conclusion:

$$P(X+Y=k) = \frac{\beta^{a+b} (a+b)_k}{k! (1+\beta)^{a+b}}, \quad k=0, 1, \dots$$

Comment: We have computed the distribution of $x+y$ before but the above is much more elegant.

(iii) Suppose X_1, X_2, \dots, X_r are independent and $X_i \sim \text{Geom}(p)$. We have

$$\begin{aligned} G_{X_i}(s) &= \sum_{i=0}^{\infty} s^i \cdot 2^{i-1} \cdot p \\ &= ps \sum_{i=0}^{\infty} (2s)^i \\ &= \frac{ps}{1-2s} \end{aligned}$$

It follows

$$G_{X_1 + \dots + X_r}(s) = \left(\frac{ps}{1-2s} \right)^r$$

Conclusion: $X_1 + \dots + X_r \sim \text{Neg Bin}(r, p)$.

5.2. Branching processes

In applications of probability we often calculate sums of a random number of random variables. Let X_1, X_2, \dots be random variables and N an integer valued nonnegative random variable. We need to define $X_1 + X_2 + \dots + X_N$. Formally we define

$$X = \sum_{k=1}^{\infty} X_k \cdot \mathbb{1}(N \geq k)$$

Comment: For a fixed $\omega \in \Omega$ we have $N(\omega) < \infty$ and so the sum is finite because only a finitely many terms are $\neq 0$.

We will write

$$X = X_1 + X_2 + \dots + X_N.$$

Theorem 5.4 : Let N, X_1, X_2, \dots be independent, X_1, X_2, \dots equally distributed non-negative integer valued random variables and N non-negative integer valued. Let $X = X_1 + X_2 + \dots + X_N$. Then

$$G_X(s) = G_N(G_{X_1}(s)).$$

Proof: We use the formula for the total expectation.

$$\begin{aligned}
 G_X(s) &= E(s^X) \\
 &= \sum_{k=0}^{\infty} E(s^X | N=k) P(N=k) \\
 &= \sum_{k=0}^{\infty} E(s^{X_1 + \dots + X_k} | N=k) P(N=k) \\
 &\stackrel{\text{indep}}{=} \sum_{k=0}^{\infty} E(s^{X_1 + \dots + X_k}) P(N=k) \\
 &= (*)
 \end{aligned}$$

$$\begin{aligned}
 \phi(x) &= \sum_{k=0}^{\infty} [G_{X_1}(s)]^k \cdot P(N=k) \\
 &= G_N(G_{X_1}(s)).
 \end{aligned}$$

Example : A hen lays N eggs. A chick hatches from each egg with probability p independent of all other eggs. Suppose $N \sim \text{Po}(\lambda)$. What is the distribution of the number of chicks? In mathematical notation we are asking about the distribution of $I_1 + I_2 + \dots + I_N$ where I_1, I_2, \dots are independent with $I_k \sim \text{Bernoulli}(p)$ and independent of N . We have

$$G_X(s) = G_N(G_{X_1}(s)).$$

$$\begin{aligned}
 G_{I_1}(s) &= s^0 P(I_1=0) + s^1 \cdot P(I_1=1) \\
 &= q + ps
 \end{aligned}$$

We have

$$\begin{aligned}G_X(s) &= G_N(p+qs) \\ &= e^{-\lambda(1-p-qs)} \\ &= e^{-\lambda(p-qs)} \\ &= e^{-\lambda p(1-s)}\end{aligned}$$

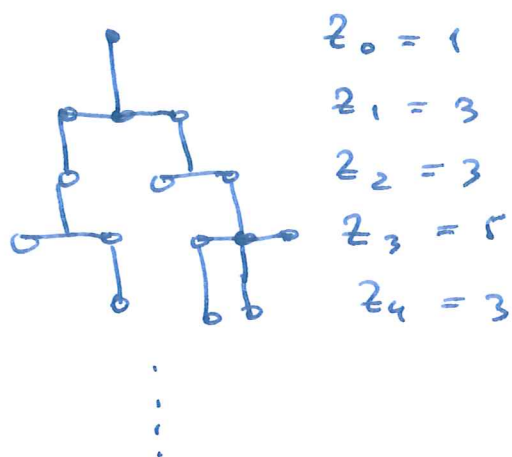
This last function is the generating function of the $P(\lambda p)$ distribution so $X \sim Po(\lambda p)$.

Branching processes

In 1874 Sir Francis Galton (1822-1911) asked the following question:
suppose you take an English aristocrat. He will have a random number of sons. His sons will have a random number of sons, ...

The problem is to determine the probability that the family tree will die out.

Figure: A possible family tree



The problem was solved by Galton and Watson in 1875 (F. Galton, H.W.

Watson, *Proceedings of the Royal Society*, (1875)

On the probability of the extinction of families, *Journal of the Royal Anthropological Institute* 4, (1875) 138-144) using generating functions.

To solve the problem mathematically we need a few additional assumptions:

- (i) Generations are simultaneous.
- (ii) Each individual has sons independently of all the others.
- (iii) The random number of sons has the same distribution for all individuals.

The above assumptions imply the following mathematical formulation:

Let $\{\xi_{n,k}\}_{n \geq 1, k \geq 1}$ be independent, equally distributed non-negative integer valued random variables with generating function G .

We define

$$Z_0 = 1 \quad \text{and recursively}$$

$$Z_{n+1} = \xi_{n+1,1} + \xi_{n+1,2} + \dots + \xi_{n+1,Z_n}$$

The sequence Z_0, Z_1, \dots of random variables is called the branching process.

The above means that Z_u
individuals in the u -th generation
have randomly many offspring.

The random variable Z_u depends
on $\xi_{m,k}$ for $m \leq u$ so it is
independent of

$$\xi_{u+1,1}, \xi_{u+1,2}, \dots$$

Denote $G_u(s) = G_{Z_u}(s)$. By
Theorem 5.4 we have

$$G_{u+1}(s) = G_u(G(s)).$$

By definition $G_1(s) = G(s)$ and
by the above recursion

$$G_2(s) = G_1(G(s)) = (G \circ G)(s)$$

$$G_3(s) = G_2(G(s)) = (G \circ G \circ G)(s)$$

\vdots

$$G_u(s) = (G \circ G \circ \dots \circ G)(s).$$

Since composition is associative we have

$$G_{n+1}(s) = G(G_n(s))$$

Let $A = \{ \text{the family tree dies out} \}$.

The family tree dies out if one of the generations is empty so

$$A = \bigcup_{n=1}^{\infty} \{z_n = 0\}.$$

But $\{z_1 = 0\} \subseteq \{z_2 = 0\} \subseteq \dots$

In the first chapter we proved that for $A_1 \subseteq A_2 \subseteq \dots$ we have

$$P\left(\bigcup_{n=1}^{\infty} A_n\right) = \lim_{n \rightarrow \infty} P(A_n).$$

Denote $\eta = P(A)$. We have

$$\eta = P(A) = \lim_{n \rightarrow \infty} P(z_n = 0).$$

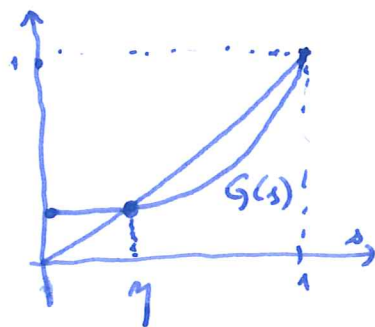
But $P(z_n = 0) = G_n(0)$.

Theorem 5.5 : The probability η satisfies the equation $\eta = G(\eta)$ and is the smallest solution of the above equation on $[0, 1]$.

Comments :

- (i) If $\eta = G(\eta)$ we say that η is a fixed point of G .
- (ii) Since $G(1) = 1$ there is always at least one fixed point on $[0, 1]$. The set of fixed points is compact so it contains a smallest point.

Figure :



Proof : $G(s)$ is continuous on $[0, 1]$.

So we have

$$\begin{aligned}\eta &= \lim_{n \rightarrow \infty} G_{n+1}(0) = \lim_{n \rightarrow \infty} G(G_n(0)) \\ &= G\left(\lim_{n \rightarrow \infty} G_n(0)\right) = G(\eta).\end{aligned}$$

So η is a fixed point. To

prove that η is the smallest

fixed point let $\bar{\eta}$ be a fixed point on $[0,1]$. We have

$$0 \leq \bar{\eta}$$

Since G is nondecreasing on $[0,1]$ it follows

$$G(0) \leq G(\bar{\eta}) = \bar{\eta}$$

$$G(G(0)) \leq G(\bar{\eta}) = \bar{\eta}$$

\vdots

$$(G \circ \dots \circ G)(0) = G_n(0) \leq \bar{\eta}$$

So

$$\lim_{n \rightarrow \infty} G_n(0) = \eta \leq \bar{\eta}.$$

This means that any fixed point \bar{y} is $\geq y$ which proves the theorem.

Example: Suppose every individual has 0, 1, 2, 3 sons with probability $1/4$ each. This means that

$$G(s) = \frac{1 + s + s^2 + s^3}{4}$$

We need all solutions of

$$G(s) = s \Leftrightarrow 1 - 3s + s^2 + s^3 = 0$$

We know that $s = 1$ is a solution so we can factor

$$1 - 3s + s^2 + s^3 = (s-1)(s^2 + 2s - 1)$$

The solutions are

$$s = 1$$

$$s = -1 + \sqrt{2}$$

$$s = -1 - \sqrt{2}$$

The smallest

fixed point

on $[0, 1]$ is $-1 + \sqrt{2}$

$$\approx 0.4142.$$

Example: Suppose $G(s) = \frac{p}{1-q^s}$.

What is $G_n(s)$?

$$\begin{aligned}G_2(s) &= G(G(s)) \\&= \frac{p}{1-q \cdot \frac{p}{1-q^s}} \\&= \frac{p(1-q^s)}{1-pq-q^s}\end{aligned}$$

$$\begin{aligned}G_3(s) &= \frac{p}{1-q \cdot \frac{p(1-q^s)}{1-pq-q^s}} \\&= \frac{p(1-pq-q^s)}{1-pq-q^s-pq(1-q^s)} \\&= \frac{p(1-pq-q^s)}{1-2pq-q(1-pq^s)}\end{aligned}$$

We see that

$$G_n(s) = \frac{a_n - b_n s}{c_n - d_n s}$$

$$G_{n+1}(s) = \frac{a_n - b_n \cdot \frac{p}{1-q^s}}{c_n - d_n \cdot \frac{p}{1-q^s}}$$

Multiplying out we get

$$a_{n+1} = a_n - p \cdot b_n$$

$$b_{n+1} = q a_n$$

We have $f_0(x) = 1 \Rightarrow a_0 = 0, b_0 = -1$

Write in matrix form

$$\begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & -p \\ q & 0 \end{pmatrix} \begin{pmatrix} a_n \\ b_n \end{pmatrix}.$$

Iteration gives

$$\begin{aligned} \begin{pmatrix} a_n \\ b_n \end{pmatrix} &= \begin{pmatrix} 1 & -p \\ q & 0 \end{pmatrix}^n \begin{pmatrix} a_0 \\ b_0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -p \\ q & 0 \end{pmatrix}^n \begin{pmatrix} 0 \\ -1 \end{pmatrix} \end{aligned}$$

We need to find the power of the matrix. Suppose $p \neq q$.

We can check by multiplication that

$$\begin{aligned} \underbrace{\begin{pmatrix} p & 1 \\ q & 1 \end{pmatrix}}_A \begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix} \underbrace{\begin{pmatrix} \frac{1}{p-q} & -\frac{1}{p-q} \\ -\frac{q}{p-q} & \frac{p}{p-q} \end{pmatrix}}_{A^{-1}} \\ = \begin{pmatrix} 1 & -p \\ q & 0 \end{pmatrix} \end{aligned}$$

We have diagonalized the matrix

$\begin{pmatrix} 1 & -p \\ \ell & 0 \end{pmatrix}$. This means

$$\begin{aligned} \begin{pmatrix} 1 & -p \\ \ell & 0 \end{pmatrix}^n &= \begin{pmatrix} p & 1 \\ \ell & 1 \end{pmatrix} \begin{pmatrix} p^n & 0 \\ 0 & \ell^n \end{pmatrix} \begin{pmatrix} 1 & -1 \\ -\ell & p \end{pmatrix} \cdot \frac{1}{p-\ell} \\ &= \begin{pmatrix} p^{n+1} - \ell^{n+1} & -p^{n+1} + p\ell^n \\ \ell p^n - \ell^{n+1} & -\ell p^n + p\ell^n \end{pmatrix} \cdot \frac{1}{p-\ell} \end{aligned}$$

We find:

$$\begin{aligned} \begin{pmatrix} 1 & -p \\ \ell & 0 \end{pmatrix}^n \begin{pmatrix} 0 \\ -1 \end{pmatrix} &= \\ &= \frac{1}{p-\ell} \begin{pmatrix} p(\ell^n - p^n) \\ \ell \ell (p^{n-1} - \ell^{n-1}) \end{pmatrix} = \begin{pmatrix} a_n \\ b_n \end{pmatrix} \end{aligned}$$

For c_n, d_n the procedure is the same except that $\begin{pmatrix} c_0 \\ d_0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

and

$$\begin{pmatrix} c_n \\ d_n \end{pmatrix} = \begin{pmatrix} p^{n+1} - \ell^{n+1} \\ \ell (p^n - \ell^n) \end{pmatrix} \cdot \frac{1}{p-\ell}$$

Finally,

$$G_n(s) = \frac{p(p^n - q^n) - qs(p^{n-1} - q^{n-1})}{p^{n+1} - q^{n+1} - qs(p^n - q^n)}$$

We find

$$\begin{aligned} P(z_n = 0) &= G_n(0) \\ &= \frac{p(p^n - q^n)}{p^{n+1} - q^{n+1}} \end{aligned}$$

We get: if $p > q$, then

$$\lim_{n \rightarrow \infty} P(z_n = 0) = 1$$

if $p < q$

$$\lim_{n \rightarrow \infty} P(z_n = 0) = \frac{p}{q} < 1.$$

Comment: The fixed points

satisfy $\frac{p}{1-qs} = s \Rightarrow$

$$qs^2 - s + p = (s-1)(qs-p) = 0 \Rightarrow$$

There is a fixed point in $(0,1)$ other than $\frac{1}{2}$ if $p < q$.

Comment : For $p = q = \frac{1}{2}$ we get

$$G_n(s) = \frac{n - (n-1)s}{n+1 - ns}$$

and

$$G_n(0) = \frac{n}{n+1} \rightarrow 1, \text{ as } n \rightarrow \infty.$$

Theorem 5.6: Let z_0, z_1, z_2, \dots be a branching process. Let $\mu = E(z_1)$.

- (i) If $\mu < 1$ then $\eta = 1$.
- (ii) If $\mu > 1$ then $\eta \in (0, 1)$.
- (iii) If $\mu = 1$ and $G(s) \neq s$ then $\eta = 1$.

Comment: The case $G(s) = s$ is

uninteresting.

The proof of the theorem has more to do with analysis than probability.

Proof: Note that $\mu = \lim_{s \uparrow 1} G'(s)$.

The function $G'(s)$ is nondecreasing

on $(0, 1)$.

(i) If $\mu < 1$, then $G'(s) \leq \mu < 1$ for all $s \in (0, 1)$. If $G(\bar{\eta}) = \bar{\eta}$

for $\bar{\eta} \in (0, 1)$ then by

Lagrange theorem

$$\begin{aligned} G(1) - G(\bar{\eta}) &= G'(\xi)(1 - \bar{\eta}) \quad \text{for } \xi \in (\bar{\eta}, 1). \\ \text{"} & \\ 1 - \bar{\eta} & \end{aligned}$$

But $G'(\xi) < 1$. So we have a contradiction.

(ii) If $\mu > 1$ there is a $\delta > 0$ such that $G'(s) > 1$ for $s \in (1-\delta, 1)$. By Lagrange for $s \in (1-\delta, 1)$ we have

$$G(1) - G(s) = G'(\xi)(1-s) \geq (1-s)$$

for $\xi \in (s, 1)$. This implies

$$1 - G(s) > 1 - s \Rightarrow G(s) < s.$$

On the other hand $G(0) \geq 0$.

For $s \in (1-\delta, 0)$ we have that

$$F(0) = G(0) - 0 \geq 0$$

$$F(s) = G(s) - s < 0.$$

There must be a zero of F on $(0, s) \subset (0, 1) \Rightarrow \eta \in (0, 1)$.

(iii) If $g(s) \neq 1$ then either $g(s) = 1$
in which case $\eta = 1$ or g is
strictly convex on $(0, 1)$, or
 $g'(s)$ is strictly increasing on $(0, 1)$.

If $g(\bar{\eta}) = \bar{\eta}$ for some $\bar{\eta} \in (0, 1)$
this would imply

$$\begin{aligned} g(1) - g(\bar{\eta}) &= 1 - \bar{\eta} \\ &= g'(\xi)(1 - \bar{\eta}) \end{aligned}$$

for some $\xi \in (\bar{\eta}, 1)$. This means

$g'(\xi) = 1$. But $g'(s)$ is strictly
increasing meaning $\lim_{s \rightarrow 1} g'(s) > 1$.

A contradiction.

Paujer recursion

If $X = X_1 + X_2 + \dots + X_N$ we know that

$$G_X(s) = G_N(G_{X_1}(s)).$$

In principle we get $P(X=k)$

by expanding the right side into

power series. But this is often difficult and recursive formulae are needed. This problem is often dealt with in insurance.

Definition: The random variable N is of Paujer class if

$$P(N=u) = \left(a + \frac{b}{u}\right) P(N=u-1)$$

for $u = 1, 2, \dots$

Examples: (i) Take $a = 0$ and $b > 0$.

$$\text{We get } P(N=u) = \frac{b}{u} P(N=1) \Rightarrow$$

$$P(N=u) = e^{-b} \cdot \frac{b^u}{u!} \Rightarrow N \sim Po(b).$$

(ii) Suppose $N \sim \text{Bin}(M, p)$. We have
compu test

$$\frac{P(N=u)}{P(N=u-1)} = \frac{M-u+1}{u} \cdot \frac{p}{q}$$

$$= \left(-\frac{p}{q} + \frac{(M+1)p}{q \cdot u} \right)$$

We take $a = -\frac{p}{q}$, $b = \frac{(M+1)p}{q}$

We see that $P(N=M+1) = 0$.

We compute

$$P(N=1) = \left(-\frac{p}{q} + \frac{(M+1)p}{q} \right) P(N=0)$$

$$= \frac{p}{q} M \cdot P(N=0)$$

$$P(N=2) = \left(-\frac{p}{q} + \frac{(M+1)p}{2q} \right) P(N=1)$$

$$= \frac{p}{q} \left(-1 + \frac{M+1}{2} \right) P(N=1)$$

$$= \frac{p}{q} \cdot \frac{M-1}{2} \cdot \frac{p}{q} \cdot \frac{M}{1}$$

Continuing we get

$$P(N=u) = \left(\frac{p}{z}\right)^u \cdot \frac{M(M-1)\cdots(M-u+1)}{u!} P(N=0)$$
$$= \left(\frac{p}{z}\right)^u \binom{M}{u} \cdot P(N=0)$$

Because all probabilities must add to 1 we have

$$\left(1 + \frac{p}{z}\right)^M P(N=0) = 1 \Rightarrow$$

$$P(N=0) = z^{-M}$$

or

$$P(N=u) = \binom{M}{u} p^u z^{M-u}$$

Conclusion: N is in the Poisson class.

Theorem 5.7: For $|s| < 1$ the generating function of N satisfies

$$(1-as)G_N'(s) = (a+b)G_N(s).$$

Proof: From the recursion equation we have

$$P(N=u) \cdot s^u = \left(a + \frac{b}{u}\right) P(N=u-1) \cdot s^{u-1}.$$

Sum both sides over $u = 1, 2, \dots$

We get

$$G_N(s) - G_N(0)$$

$$= a \sum_{n=1}^{\infty} P(N=n-1) s^{n-1}$$

$$+ b \cdot \sum_{n=1}^{\infty} \frac{s^{n-1}}{n} P(N=n-1)$$

$$= as G_N(s) + b \sum_{n=0}^{\infty} \left(\int_0^1 u^n du \right) P(N=n)$$

$$= as G_N(s) + b \int_0^1 \left(\sum_{n=0}^{\infty} u^n P(N=n) \right) du$$

$$= as G_N(s) + b \int_0^1 G_N(u) du.$$

It is legitimate to interchange summation and integration because the sum converges uniformly on $[0, 1]$.

Take derivatives to get

$$G'_N(s) = a G_N(s) + as G'_N(s) + b G_N(s).$$

Rearranging gives the equation.

If $X = X_1 + X_2 + \dots + X_N$ where X_1, X_2 are independent equally distributed we get

$$G_X(s) = G_N(G_{X_1}(s))$$

Taking derivatives we get

$$G'_X(s) = G'_N(G_{X_1}(s)) \cdot G'_{X_1}(s)$$

Multiply both sides by

$$1 - aG_{X_1}(G_{X_1}(s))$$

and use Theorem 5.7. We get

$$\begin{aligned} G'_X(s) (1 - a G_{X_1}(s)) \\ = (a+b) G_X(s) G'_{X_1}(s) \end{aligned}$$

Denote $P(N=n) = p_n$ for $n=0, 1, \dots$

Denote $P(X=r) = g_r$ and

$P(X_1=k) = f_k$ for $k=0, 1, \dots$

We have that $X=0$ if either
 $N=0$ or $N>0$ and $X_1+\dots+X_N=0$.

It follows

$$P(X=0) = P(N=0) + \sum_{n=1}^{\infty} P(N=n) \cdot f_0^n$$

$$= G_N(f_0)$$

In our notation

$$P(X=0) = g_0 = G_N(f_0).$$

From Analysis we know that

$$\left(\sum_{k=0}^{\infty} a_k x^k \right) \left(\sum_{k=0}^{\infty} b_k x^k \right) = \sum_{k=0}^{\infty} c_k x^k$$

with

$$c_k = \sum_{i=0}^k a_i b_{k-i}.$$

Comment: This is called the Cauchy product of power series.

In the formulae connecting the generating functions

Equate coefficients for x^n .

$$h: (n+1)g_{n+1} = a \sum_{k=0}^n f_k \cdot (n+1-k)g_{n+1-k}$$

$$\begin{aligned} r: (a+b) \sum_{k=0}^n (k+1) f_{k+1} \cdot g_{n-k} \\ = (a+b) \sum_{k=1}^{n+1} k f_k \cdot g_{n-k+1} \end{aligned}$$

Rearranging we get

$$(n+1)g_{n+1} - a f_0 (n+1)g_{n+1}$$

$$= a \sum_{k=1}^n f_k (n+1-k) g_{n+1-k} +$$

$$(a+b) \sum_{k=0}^n (k+1) f_{k+1} g_{n-k}$$

$$= a \sum_{k=1}^n f_k (n+1-k) g_{n+1-k}$$

$$+ (a+b) \sum_{k=1}^{n+1} k f_k \cdot g_{n+1-k}$$

$$= a \cdot \sum_{k=1}^{n+1} f_k (n+1-k) g_{n+1-k}$$

$$+ (a+b) \sum_{k=1}^{n+1} k f_k g_{n+1-k}$$

Divide by $(n+1)(1-af_0)$ to get

$$g_{n+1} = \frac{1}{1-af_0} \sum_{k=1}^{n+1} \left(a + \frac{bk}{n+1} \right) f_k g_{n+1-k}$$

Theorem 5.8 (Paujer recursion)

We have

$$g_{n+1} = \frac{1}{1-af_0} \sum_{k=1}^{n+1} \left(a + \frac{bk}{n+1} \right) f_k g_{n+1-k}$$