MAT235: Discussion 6

1 Generating functions

1.1 Probability generating function

Probability generating functions of r.v. X is defined as

$$G_X(s) = E(s^X).$$

and

$$P(X = k) = G^{(k)}(0)$$

. **Theorem**: If X and Y are independent, then $G_{X+Y}(s) = G_X(s)G_Y(s)$.

Theorem: If $X_1, X_2, \cdots$ is a sequence of independent identically distributed random variables with common generating function $G_X(s)$ and $N \geq 0$ is a random variable independent of X_i and has generating function G_N, then $S = X_1 + \cdots + X_N$ has generating function given by:

$$G_S(s) = G_N(G_X(s)).$$

Proof. Use the property of conditional expectation to find that

$$\begin{aligned} G_S(s) = E(s^S) = E(E(s^S|N)) &= \sum_n E(s^S|N = n)P(N = n) \\ &= \sum_n E(s^{X_1+\cdots+X_n})P(N = n) \\ &= \sum_n E(s^{X_1}) \cdots E(s^{X_n})P(N = n) \\ &= \sum_n G_X(s)^n P(N = n) = G_N(G_X(s)). \end{aligned}$$

Example (Branching process): let $Z_0 = 1$, and Z_n be the number of members of the n-th generation. Each member can independently produce family members of the next generation according to a same discrete distribution. We are interested in the random sequence $Z_0, Z_1, \cdots$ of generation sizes. Let $G_n(s) = E(s^{Z_n})$ be the generating function of Z_n.

Lemma: It is the case that $G_{m+n}(s) = G_m(G_n(s)) = G_n(G_m(s))$, and thus $G_n(s) = G(G(\cdots(G(s))\cdots))$ is the n-fold iterate of G.
Proof. Each member of the $(m + n)$-th generation has a unique ancestor in the m-th generation.

$$Z_{m+n} = X_1 + \cdots + X_{Z_m}$$

where X_i is the number of family members of the i-th individual from the m-th generation. By assumptions of the branching process, X_i's are independent and identically distributed with generating function $G_{X_1}(s) = G_n(s)$. Thus

$$G_{m+n}(s) = G_m(G_n(s))$$

according to the previous theorem. Iterate this relation to obtain

$$G_n(s) = G(G(\cdots(G(s))\cdots)).$$

We are interested in the event of ultimate extinction $\{\text{ultimate extinction}\} = \cup_n \{Z_n = 0\}$. Let $A_n = \{Z_n = 0\}$, then $A_n \subseteq A_{n+1}$. Let $E(Z_1) = \mu$.

Theorem: As $n \to \infty, P(Z_n = 0) \to P(\text{ultimate extinction}) = p$, where p is the smallest non-negative root of $s = G(s)$. Also, $p = 1$ if $\mu < 1$, and $p = 1$ if $\mu > 1$. If $\mu = 1$, then $p = 1$ as long as the family-size distribution has strictly positive variance.
Proof. Let $p_n = P(Z_n = 0)$. Then,

$$p_n = G_n(0) = G(G_{n-1}(0)) = G(p_{n-1}).$$

By continuity of probability we know that $p_n \uparrow p$, and the continuity of G guarantees that $p = G(p)$. If α is any non-negative root of the equation $s = G(s)$, then $p \leq \alpha$. Notice that G is non-decreasing on $[0, 1]$ and so

$$p_1 = G(0) \leq G(\alpha) = \alpha.$$

Similarly,

$$p_2 = G(p_1) \leq G(\alpha) = \alpha$$

and hence by induction, $p_n \leq \alpha$ for all n, implying $p \leq \alpha$. Thus p is the smallest non-negative root of the equation $s = G(s)$.
Now we can verify G is a convex function on $[0, 1]$. Since $G''(s) \geq 0$ if $s \geq 0$. Since $G(0) = p_0 > 0$, $G(1) = 1$ and G is convex, the smallest root of $s = G(s)$ is $\alpha = 1$ if $G'(1) = \mu < 1$ and is $\alpha < 1$ if $G'(1) = \mu > 1$.

1.2 Moment generating function

Probability generating functions of r.v. X is defined as

$$M_X(t) = G_X(e^t) = E(e^{tX}).$$

and

$$E(X^k) = M^{(k)}(0).$$

Example: For standard normal random variable it is to show that the moment generating function is $e^{-\frac{t^2}{2}}$ by integration using completing the square. Then using the moment generating function, it is to show that $E(X^{2k-1}) = 0$ and $E(X^{2k}) = 1 \cdot 3 \cdots (2k-1)$ for $k = 1, 2, \cdots$.

Try to find the moment generating functions of other common distributions.

2 Law of large numbers

Example (independent but not identically distributed case): Consider the number of cycles in a random permutation of n numbers, where a cycle is defined as a group of numbers that permutes within themselves.

Let Z_n denotes the number of cycles in a permutation of n numbers, then $Z_{n+1} = Z_n + X_{n+1}$, where X_{n+1} is independent of Z_n and is distributed as $Bernoulli(\frac{1}{n+1})$. Since whether the last number starts a new cycle is independent of the existing cycles. Therefore we have,

$$E(Z_n) = \sum_{k=1}^{n} \frac{1}{k} \sim \log n,$$
$$Var(Z_n) = \sum_{k=1}^{n} \frac{k-1}{k^2} \sim \log n.$$

By Chebyshev's inequality

$$P(|Z_n - \log n| > (\log n)^{\frac{1}{2}+\epsilon}) = \frac{1}{(\log n)^{2\epsilon}} \to 0 \text{ as } n \to \infty.$$

Therefore $\frac{Z_n}{\log n} \to 1$ in probability.

Example (identical but not independent distributed case): Consider the matching problem talked before, where n letters are randomly put into n envelopes, what is number of correct matches and what is its limit behavior.