The Period of a Random Recursive Sequence

Klaus Pommerening

May 1989 – english version May 2020

Summary

This note[1] considers the output of a recursive process of depth[2] 1—that is we consider a finite set, a recurrence formula, and the sequence of its output elements, see Figure 1. Since this sequence can assume only finitely many values it eventually repeats, hence is necessarily cyclic, see Figure 2. Whether we want to use it for the simulation of a random process or for key generation with a stream cipher, in any case the length of the period is of concern. The "classical" approach to pseudorandom or keystream generators aimed at maximum period lengths [2]. This resulted in sequences that pass many statistical tests for randomness—and therefore fit many statistical or simulation purposes—but fail the main cryptographic requirements of being unpredictable and computationally indistinguishable from a "true" random sequence.

This note addresses the question of the distribution of the periods of all such sequences. The main result gives an asymptotic formula for the ecpected value of the period length and shows what to expect for a "random" choice of the recursive process.

1 Periods and Preperiods

Let M be a finite set with $m = \#M$. Since the nature of the elements of M doesn't matter in any way we henceforth often assume without loss of generality that M is the integer interval $M = \{0, 1, \ldots, m-1\}$. We may think of the elements of M as "states" and consider a map ("state transition")[3]

$$s : M \longrightarrow M.$$

For each element ("initial state") $x_0 \in M$ we define a sequence $(x_i)_{i\in\mathbb{N}}$ in M by the recurrence formula $x_i = s(x_{i-1})$ for $i \geq 1$, see Figure 1. The map s is also called the **generating function** of the sequence. Since M is finite this sequence—after a finite preperiod—eventually becomes periodic, see Figure 2. In other words there are smallest integers $\mu \geq 0$ and $\nu \geq 1$ such that $x_{\mu+\nu} = x_\mu$: Take for μ the smallest index such that

[1] an expanded version of a solution for exercise 3.1.12 in [2]

[2] that is each member of the output sequence depends only on its immediate precursor

[3] In other words: we describe a simple finite dynamical system.

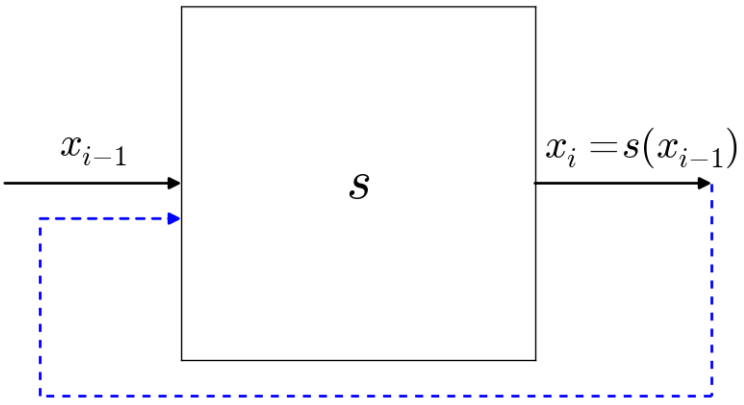

Figure 1: Recursion of depth 1—at each step the output of the process is fed back as input of the next step

the element x_μ reappears somewhere in the sequence, and for $\mu + \nu$ the index where the first repetition occurs. Then also

$$x_{i+\nu} = x_i \quad \text{for } i \geq \mu.$$

Obviously $0 \leq \mu \leq m-1$, $1 \leq \nu \leq m$, $\mu + \nu \leq m$. The values $x_0, \ldots, x_{\mu+\nu-1}$ are all distinct, and the values $x_0, \ldots, x_{\mu-1}$ never reappear in the sequence.

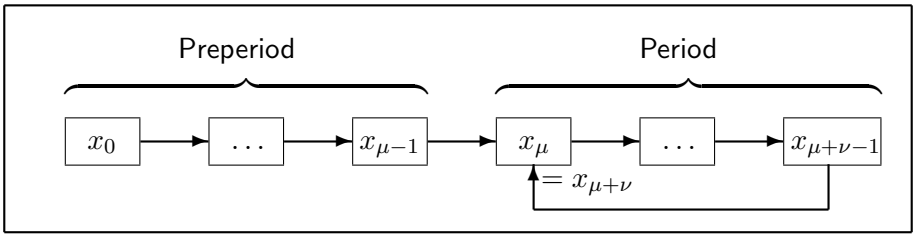

Figure 2: Period and preperiod

Definition μ is called (length of the) **preperiod**, ν, (length of the) **period**, $\lambda = \mu + \nu$, **effective length** of the sequence.

Examples

For examples 2 to 6 we assume that $M = \{0, 1, \ldots, m-1\}$.

1. For $s =$ the identity map of M we have $x_1 = x_0$, hence $\mu = 0$, $\nu = 1$, $\lambda = 1$.
2. For $s(x) = x + 1 \bmod m$ we have $x_m = x_0$, hence $\mu = 0$, $\nu = m$, $\lambda = m$.

3. We slightly modify the previous example, setting $s(m-1) = m-1$. Then we get $\mu = m-1$, $\nu = 1$, $\lambda = m$ (for $x_0 = 0$).

4. With $m = 10$, $s(x) = x^2 \bmod 10$, $x_0 = 3$ we generate the sequence $3, 9, 1, 1, \ldots$ with $\mu = 2$, $\nu = 1$, $\lambda = 3$.

5. For $m = 10$, $s(x) = 7x \bmod 10$, $x_0 = 1$ the sequence becomes $1, 7, 9, 3, 1, 7, 9, 3, \ldots$, hence $\mu = 0, \nu = 4$, $\lambda = 4$.

6. A more general linear recurrence has the generating function $s(x) = ax + b \bmod m$ for integers $a, b \in \mathbb{N}$. This is the classical linear congruence generator (LCG) [2], often used for generating pseudorandom numbers for statistical purposes, especially when its period is about m.

7. Taking for M the finite set $\mathbb{F}_2^n$ of all bitvectors of length n, we define a linear feedback shift register (LFSR) by the generating function:

$$s(t_1, \ldots, t_n) = (t_2, \ldots, t_n, a_1 t_1 + \cdots + a_n t_n)$$

where the coefficients are bits $a_1, \ldots, a_n \in \mathbb{F}_2$. The output sequence[4] has similar good statistical properties as an LCG. This kind of pseudorandom generation is of widespread use for generating "white noise" in engineering [1], especially when its period is 2^n.

2 Formulas for the Probabilities

Let A be a finite set. We use the notation

$$P(B) := \frac{\#B}{\#A} \quad \text{for } B \subseteq A,$$

called the **probability**[5] of B. As basic set[6] in the scenario of Section 1 we consider $A = M^M \times M$ where M^M denotes the set of all maps from M to M. It has $\#(M^M) = m^m$ elements. For $s \in M^M$ and $x \in M$ let $f(s, x)$ be the preperiod and $g(s, x)$ be the period of the sequence $x_0 = x$, $x_1 = s(x_0)$, ... This defines two functions

$$f, g \colon M^M \times M \longrightarrow \mathbb{N}.$$

Remarks

1. The set of all maps $s \colon M \longrightarrow M$, represented by M^M, is in bijective correspondence with the set of all m-tuples $(s_0, \ldots, s_{m-1})$ with $s_0, \ldots, s_{m-1} \in M$.

[4] Take the leftmost bit of each vector to avoid the duplicatios

[5] Since we deal with finite uniform probability spaces only, this naive definition is adequate.

[6] or probability space

2. The symmetric group $\mathcal{S}_m$, the group of permutations of M, acts on $M^M \times M$ by the rule
$$(s, x) \overset{\sigma}{\mapsto} (\sigma s \sigma^{-1}, \sigma x).$$
For the sequence x_0, $x_1 = s(x_0)$, ... clearly $\sigma x_j = \sigma x_i \iff x_j = x_i$. Therefore the sequence with generating function $\sigma s \sigma^{-1}$ and initial value σx has the same preperiod and period as the sequence with s and x. In other words the functions f, g, and $f + g$ are invariant under $\mathcal{S}_m$.

3. Now we assume that $M = \{0, 1, \ldots, m-1\}$, and let $\tau \in \mathcal{S}_m$ be the shift map $i \mapsto i+1 \bmod m$. Each orbit of the cyclic subgroup $H = \langle \tau \rangle \leq \mathcal{S}_m$ meets $M^M \times \{0\}$ in exactly one point and has size m. These orbits partition $M^M \times M$ into m^m subsets of size m, and
$$\begin{aligned} f(s,0) &= f(\tau s \tau^{-1}, 1) = \ldots = f(\tau^i s \tau^{-i}, i) = \ldots \\ g(s,0) &= g(\tau s \tau^{-1}, 1) = \ldots = g(\tau^i s \tau^{-i}, i) = \ldots \end{aligned}$$
for each generating function $s \in M^M$.

By Remark 3 when calculating probabilities we need only consider sequences with 0 as initial value. The probability of observing the preperiod μ and the period ν is
$$\begin{aligned} P_m(\mu, \nu) &= \frac{1}{m^{m+1}} \cdot \#\{(s, x) \in M^M \times M \mid f(s, x) = \mu,\ g(s, x) = \nu\} \\ &= \frac{1}{m^m} \cdot \#\{s \in M \mid f(s, 0) = \mu,\ g(s, 0) = \nu\}. \end{aligned}$$
The probability of observing the effective length λ is $\sum_{\mu+\nu=\lambda} P_m(\mu, \nu)$. The probability that μ occurs with any period, or that ν occurs with any preperiod is[7]
$$\begin{aligned} P_m(\mu, *) &= \frac{1}{m^m} \cdot \#\{s \in M^M \mid f(s, 0) = \mu\} = \sum_{\nu=1}^{m} P_m(\mu, \nu)\,, \\ P_m(*, \nu) &= \frac{1}{m^m} \cdot \#\{s \in M^M \mid g(s, 0) = \nu\} = \sum_{\mu=0}^{m-1} P_m(\mu, \nu)\,. \end{aligned}$$
Here are some special examples—note that by Remark 1 we may choose the x_i independently from each other:

- $P_m(0, 1) = \frac{1}{m}$ (the probability that $x_1 = x_0$);
- $P_m(0, 2) = (1 - \frac{1}{m}) \cdot \frac{1}{m}$ (the probability that $x_1 \neq x_0$, $x_2 = x_0$);
- $P_m(1, 1) = (1 - \frac{1}{m}) \cdot \frac{1}{m}$ (the probability that $x_1 \neq x_0$, $x_2 = x_1$);
- $P_m(2, 1) = (1 - \frac{1}{m})(1 - \frac{2}{m}) \cdot \frac{1}{m}$ (the probability that $x_1 \neq x_0$, $x_2 \neq x_0, x_1$, and $x_3 = x_2$).

[7] Note that the star is not a wild-card symbol but denotes a summation.

More generally

$$P_m(\mu,\nu) = \frac{1}{m}\cdot\prod_{k=1}^{\mu+\nu-1}(1-\frac{k}{m}),\quad P_m(\mu,*) = \sum_{\nu=1}^{m-\mu}\frac{1}{m}\cdot\prod_{k=1}^{\mu+\nu-1}(1-\frac{k}{m})\,.$$

We use the abbreviation

$$R_m(l) := \prod_{k=1}^{l}(1-\frac{k}{m}),$$

and express P_m by it:

Lemma 1 (i) *$P_m(\mu,\nu) = \frac{1}{m}\cdot R_m(\mu+\nu-1)$, in particular $P_m(\mu,\nu)$ depends only on $\lambda = \mu+\nu$, the effective length.*

(ii) *$P_m(\mu,*) = \frac{1}{m}\cdot\sum_{\nu=1}^{m-\nu} R_m(\mu+\nu-1)$, in particular $P_m(\mu,*)$ is strongly decreasing as a function of μ.*

(iii) *$P_m(*,\nu) = \frac{1}{m}\cdot\sum_{\mu=0}^{m-\nu-1} R_m(\mu+\nu-1)$, in particular $P_m(*,\nu)$ is strongly decreasing as a function of $\nu \geq 1$.*

(iv) *$P_m(\mu,*) = P_m(*,\mu+1)$ for $\mu = 1,\ldots,m-1$.*

(v) *$P_m(\mu,\nu) = P_m(\nu-1,\mu+1)$.*

(vi) *The probability of observing the effective length λ is $p_m(\lambda) = (\lambda/m)\cdot R_m(\lambda-1)$.*

(vii) *$R_m(0) = 1$, $R_m(1) = 1-1/m$, $R_m(j) = (1-j/m)\,R_m(j-1)$ for $j \geq 1$, and $R_m(j) = 0$ for $j \geq m$.*

Proof. (i), (ii), (iii) are direct consequences of the definitions. Formula (iv) follows from (ii) and (ii), and (v) from (i).

For (vi), using (i), we get

$$p_m(\lambda) = \sum_{\mu+\nu=\lambda} P_m(\mu,\nu) = \frac{1}{m}\sum_{\mu+\nu=\lambda} R_m(\mu+\nu-1) = \frac{1}{m}\sum_{\mu+\nu=\lambda} R_m(\lambda-1).$$

The assertion follows since the sum consists of λ identical summands.

The formulas in (vii) are immediate from the definition. $\diamond$

These formulas yield fast algorithms for calculating the distributions of preperiods, periods, and effective lengths, see Appendix A for the algorithms and Appendix B for Python (or SageMath) code. Table 1 shows the results for $m = 20$, Figure 3 shows the corresponding graphic for periods and lengths.

i	0	1	2	3	4	5	6	7	8	9	10
μ	0.265	0.215	0.167	0.124	0.088	0.059	0.037	0.022	0.012	0.006	0.003
ν	0.0	0.265	0.215	0.167	0.124	0.088	0.059	0.037	0.022	0.012	0.006
λ	0.0	0.05	0.095	0.128	0.145	0.145	0.131	0.107	0.079	0.054	0.033

i	11	12	13	14	15	16	17	18	19	20
μ	0.001	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
ν	0.003	0.001	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
λ	0.018	0.009	0.004	0.001	0.0	0.0	0.0	0.0	0.0	0.0

Table 1: Probabilities of preperiods μ, periods ν, and effective lengths λ for $m = 20$

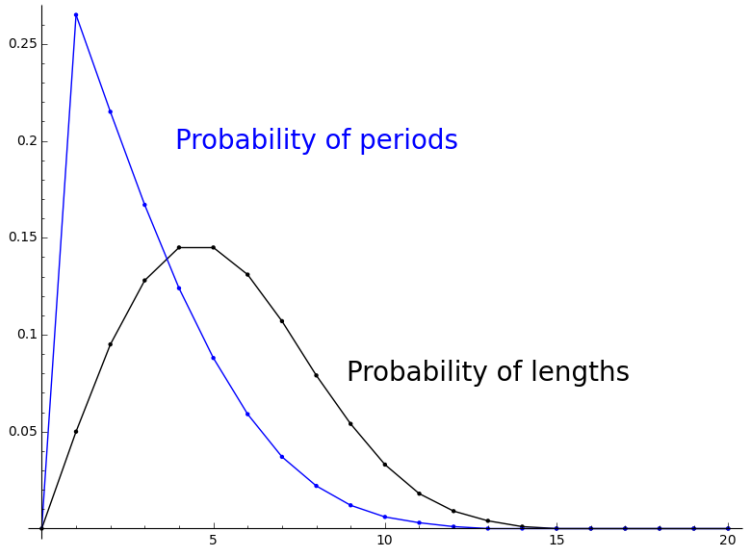

Figure 3: Distribution of periods ν, and effective lengths λ for $m = 20$

3 The Expected Value of Period and Preperiod

How large is the expected value of the period, preperiod, and effective length of a recursion of depth 1 when we choose the generating function s and the initial value x at random?

In general let A be a finite set and $\Phi\colon A \longrightarrow \mathbb{R}$ be a real valued function. Then the weighted sum

$$E(\Phi) := \frac{1}{\#A} \sum_{x \in A} \Phi(x) = \sum_{r \in \mathbb{R}} r \cdot P(\Phi^{-1}(r))$$

is called the **expected value** (or mean value) of Φ.

Our goal is determining the expected values of the functions f, g, and $f+g$ from Section 2, that is the expected values of preperiod, period, and effective length of the recursive sequences with arbitrarily chosen generating functions $s\colon M \longrightarrow M$ and initial values $x \in M$. By definition we have

$$\begin{aligned} E(f) &= \sum_{\mu \in \mathbb{N}} \mu \cdot P(f^{-1}(\mu)) = \sum_{\mu=0}^{m-1} \mu \cdot P_m(\mu, *), \\ E(g) &= \sum_{\nu \in \mathbb{N}} \nu \cdot P(g^{-1}(\nu)) = \sum_{\nu=1}^{m} \nu \cdot P_m(*, \nu), \\ E(f+g) &= E(f) + E(g). \end{aligned}$$

We try to calculate the expected value of g using a common summation trick, see Figure 4:

$$\begin{aligned} E(g) &= \sum_{\nu=1}^{m} \nu \cdot P_m(*,\nu) \;=\; \frac{1}{m} \cdot \sum_{\nu=1}^{m} \sum_{\mu=0}^{m-\nu} \nu \cdot R_m(\mu+\nu-1) \\ &= \frac{1}{m} \cdot \sum_{\rho=1}^{m} \sum_{\nu=1}^{\rho} \nu \cdot R_m(\rho-1) \;=\; \frac{1}{m} \cdot \sum_{\rho=1}^{m} \frac{\rho\,(\rho+1)}{2} \cdot R_m(\rho-1) \\ &= \sum_{\rho=1}^{m} \frac{\rho+1}{2} \cdot \underbrace{\frac{\rho}{m} \cdot R_m(\rho-1)}_{R_m(\rho-1)-R_m(\rho)} \\ &= R_m(0) + \sum_{\rho=2}^{m} \frac{\rho+1}{2} \cdot R_m(\rho-1) - \sum_{\rho=1}^{m-1} \frac{\rho+1}{2} \cdot R_m(\rho) - \underbrace{\frac{m+1}{2} \cdot R_m(m)}_{0} \\ &= 1 + \sum_{j=1}^{m-1} \frac{j+2}{2} \cdot R_m(j) - \sum_{j=1}^{m-1} \frac{j+1}{2} \cdot R_m(j) \;=\; 1 + \sum_{j=1}^{m-1} \frac{1}{2} \cdot R_m(j) \\ &= \frac{1}{2} + \sum_{j=0}^{m-1} \frac{1}{2} \cdot R_m(j) \;=\; \frac{Q(m)+1}{2}\,, \end{aligned}$$

with the function

$$Q(m) := \sum_{j=0}^{m-1} R_m(j). \tag{1}$$

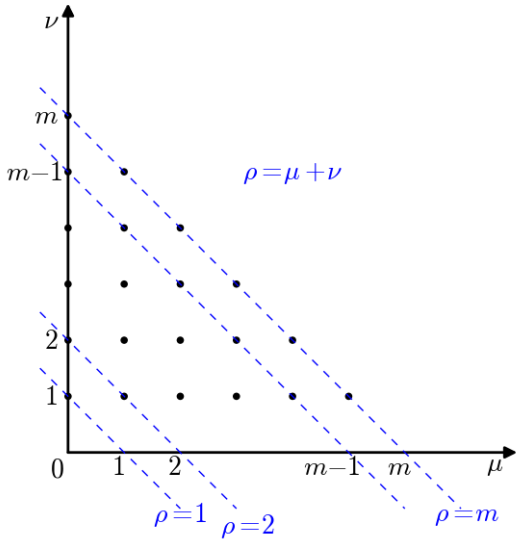

Figure 4: A common summation trick

Along similar lines we also could attack the expected value of f. However a simpler approach is to use the symmetry $P_m(\mu,*) = P_m(*,\mu+1)$ from Lemma 1 (iv), hence

$$\begin{aligned} E(f) &= \sum_{\mu=0}^{m-1} \mu P_m(\mu,*) = \sum_{\mu=0}^{m-1} \mu P_m(*,\mu+1) = \sum_{\rho=1}^{m} (\rho-1)\cdot P_m(*,\rho) \\ &= \sum_{\rho=1}^{m} \rho P_m(*,\rho) - \sum_{\rho=1}^{m} P_m(*,\rho) = \frac{Q(m)+1}{2} - 1 \\ &= \frac{Q(m)-1}{2}. \end{aligned}$$

Finally the effective length of the sequence $x_0, x_1, \ldots$ is the sum of preperiod and period. Therefore its expected value is $Q(m)$. In summary we have proved:

Proposition 1 *Let M be a finite set of $m = \#M$ elements. Then the expected value of the periods of the recursive sequences in M is $\frac{Q(m)+1}{2}$. The expected value of the preperiods is $\frac{Q(m)-1}{2}$. The expected value of the effective lengths is $Q(m)$.*

Although Proposition 1 looks mathematically elegant—it is only a minor reformulation of our problem, not a satisfying solution. We want to know more about the function Q. Fortunately already RAMANUJAN analyzed its asymptotic behaviour.

4 Parenthesis: Ramanujan's Q Function

We slightly rewrite the formulas for R_n and Q:

$$\begin{aligned} R_n(l) &= \prod_{k=1}^{l}(1-\frac{k}{n}) = \prod_{k=1}^{l}\frac{n-k}{n} = \frac{(n-1)\cdots(n-l)}{n^l} \\ &= \frac{n!}{(n-l-1)!\cdot n^{l+1}}, \end{aligned}$$

$$\begin{aligned} Q(n) &= \sum_{l=0}^{n-1} R_n(l) = \sum_{l=1}^{n} R_n(l-1) = \sum_{l=1}^{n}\frac{n!}{(n-l)!\cdot n^l} \\ &= \frac{n!}{n^n}\cdot\sum_{l=1}^{n}\frac{n^{n-l}}{(n-l)!} = \frac{n!}{n^n}\cdot\sum_{k=0}^{n-1}\frac{n^k}{k!}. \end{aligned}$$

The Taylor formula with Cauchy's form of the remainder for a function[8] f is

$$f(x) = \sum_{k=0}^{n-1}\frac{f^{(k)}(0)}{k!}\cdot x^k + \frac{1}{(n-1)!}\cdot\int_{t=0}^{x} t^{n-1}f^{(n)}(x-t)dt.$$

We apply it to the exponential function $f(x) = e^x$ using $f^{(n)}(x) = e^x$. The remainder becomes

$$\frac{e^x}{(n-1)!}\cdot\int_{t=0}^{x} t^{n-1}e^{-t}dt = \frac{e^x}{(n-1)!}\cdot\gamma(n,x)$$

with the **incomplete gamma function**[9] γ. Hence e^n decomposes as

$$e^n = \sum_{k=0}^{n-1}\frac{n^k}{k!} + \frac{e^n}{(n-1)!}\cdot\gamma(n,n) = \frac{n^n}{n!}Q(n) + T(n),$$

where the remainder has the form

$$T(n) = e^n\cdot\frac{\gamma(n,n)}{\Gamma(n)}.$$

We have proved:

Proposition 2 *The function Q defined by* (1) *satisfies*

$$Q(n) = \frac{n!}{n^n}\,e^n\cdot\left(1-\frac{\gamma(n,n)}{\Gamma(n)}\right) \quad \textit{for } n\geq 1.$$

To turn Proposition 2 into a useful result for Q we need results on the gamma function that we derive in Section 7 below after two more parentheses.

[8] defined around 0 and n times differentiable

[9] The "complete" gamma function Γ arises from γ by the limit $x\to\infty$. It has the special values $\Gamma(n) = (n-1)!$.

5 Parenthesis: The Stirling Formula

Proposition 3 *For all natural numbers $n \geq 1$ we have*

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \cdot e^{r_n}$$

where the error term r_n is bounded by

$$\frac{1}{12n+1} \leq r_n \leq \frac{1}{12n}$$

Proof. We consider the sequence

$$a_n = \frac{n!}{(\frac{n}{e})^n \cdot \sqrt{n}}$$

and show that it decreases monotonically; because all of its members are positive, we then know that it converges.

Dividing two consecutive terms we get

$$\frac{a_n}{a_{n+1}} = \frac{n!(\frac{n+1}{e})^{n+1} \cdot \sqrt{n+1}}{(\frac{n}{e})^n \cdot \sqrt{n} \cdot (n+1)!} = \frac{1}{e} \cdot (\frac{n+1}{n})^{n+1/2},$$

$$\log \frac{a_n}{a_{n+1}} = -1 + (n+\frac{1}{2}) \cdot \log \frac{n+1}{n}.$$

Lemma 3 below immediately gives

$$0 < \frac{1}{12} \cdot (\frac{1}{n+\frac{1}{12}} - \frac{1}{n+\frac{1}{12}+1}) < \log \frac{a_n}{a_{n+1}} < \frac{1}{12} \cdot (\frac{1}{n} - \frac{1}{n+1}).$$

From the left inequality we conclude $a_n > a_{n+1}$ as claimed.

Now let $a = \lim_{n\to\infty} a_n$. Then $a \geq 0$ and by telescoping

$$\frac{1}{12} \cdot (\frac{1}{n+\frac{1}{12}} - \frac{1}{n+\frac{1}{12}+k}) < \log \frac{a_n}{a_{n+k}} < \frac{1}{12} \cdot (\frac{1}{n} - \frac{1}{n+k}).$$

For $k \to \infty$ we get

$$\frac{1}{12n+1} \leq \log \frac{a_n}{a} \leq \frac{1}{12n},$$

$$e^{\frac{1}{12n+1}} \leq \frac{a_n}{a} \leq e^{\frac{1}{12n}}.$$

To complete the proof of the theorem we have to show that $a = \sqrt{2\pi}$.

From Wallis' product formula, see Lemma 4 below, and using $k! = a_k k^{k+1/2}/e^k$, we get

$$\sqrt{\pi} = \lim_{n\to\infty} \frac{a_n^2 \cdot n^{2n+1} \cdot 2^{2n} \cdot e^{2n}}{e^{2n} \cdot a_{2n} \cdot (2n)^{2n+1/2} \cdot \sqrt{n+1/2}}$$

$$= a \cdot \lim_{n\to\infty} \frac{\sqrt{n}}{\sqrt{2}\cdot\sqrt{n+1/2}} = \frac{a}{\sqrt{2}}.$$

Therefore $a = \sqrt{2\pi}$. $\diamond$

Lemma 2 *For* $0 < x < 1$

$$\frac{3x}{3-x^2} < \frac{1}{2}\log\frac{1+x}{1-x} < x\cdot\left(1+\frac{1}{3}\cdot\frac{x^2}{1-x^2}\right).$$

Proof. For $|x| < 1$ we have the well-known power series expansion

$$\frac{1}{2}\log\frac{1+x}{1-x} = x + \frac{x^3}{3} + \frac{x^5}{5} + \ldots = \sum_{\nu=1}^{\infty}\frac{x^{2\nu-1}}{2\nu-1}.$$

For $0 < x < 1$ we get the upper bound

$$\frac{1}{2}\log\frac{1+x}{1-x} < x + \frac{x^3}{3} + \frac{x^5}{3}\cdots = x + \sum_{\nu=2}^{\infty}\frac{x^{2\nu-1}}{3} = x + \frac{x^3}{3}\left(1+x^2+x^4+\cdots\right)$$

$$= x + \frac{x^3}{3}\cdot\frac{1}{1-x^2} = x\cdot\left(1+\frac{1}{3}\cdot\frac{x^2}{1-x^2}\right).$$

For the lower bound we use

$$\frac{1}{2}\log\frac{1+x}{1-x} > x + \frac{x^3}{3} + \frac{x^5}{9}\cdots = \sum_{\nu=1}^{\infty}\frac{x^{2\nu-1}}{3^{\nu-1}} = x\cdot\sum_{\nu=0}^{\infty}\frac{x^{2\nu}}{3^{\nu}} = x\cdot\frac{1}{1-\frac{x^2}{3}}.$$

$\diamond$

Lemma 3 *For* $n \in \mathbb{N}_1$

$$2 + \frac{1}{6}\cdot\left(\frac{1}{n+\frac{1}{12}} - \frac{1}{n+\frac{1}{12}+1}\right) < (2n+1)\cdot\log\frac{n+1}{n} < 2 + \frac{1}{6}\cdot\left(\frac{1}{n} - \frac{1}{n+1}\right)$$

Proof. In Lemma 2 we substitute $x = \frac{1}{2n+1}$. Then

$$\frac{1+x}{1-x} = \frac{1+\frac{1}{2n+1}}{1-\frac{1}{2n+1}} = \frac{2n+2}{2n} = \frac{n+1}{n}.$$

This yields the upper bound

$$\frac{1}{2}\cdot\log\frac{n+1}{n} < \frac{1}{2n+1}\cdot\left(1+\frac{1}{3}\cdot\frac{1}{4n^2+4n}\right) = \frac{1}{2n+1}\cdot\left(1+\frac{1}{12}\cdot\frac{1}{n(n+1)}\right),$$

as claimed. At the lower bound we get

$$\frac{1}{2}\cdot\log\frac{n+1}{n} > \frac{3(2n+1)}{3(2n+1)^2-1},$$

whence

$$(2n+1)\cdot\log\frac{n+1}{n} > \frac{6(2n+1)^2}{3(2n+1)^2-1} = 2+\frac{2}{3(2n+1)^2-1} = 2+\frac{2}{12n^2+12n+2}\,.$$

The lower bound we aim at evaluates to

$$2+\frac{1}{6}\cdot\left(\frac{1}{n+\frac{1}{12}}-\frac{1}{n+\frac{1}{12}+1}\right) = 2+2\cdot\left(\frac{1}{12n+1}-\frac{1}{12n+13}\right)$$

$$= 2+2\cdot\frac{12}{(12n+1)(12n+13)} = 2+2\cdot\frac{12}{12\cdot 12n^2+14\cdot 12n+13} = 2+2\cdot\frac{2}{12n^2+14n+\frac{13}{12}}$$

which is clearly smaller for $n \geq 1$. $\diamond$

Lemma 4 (Product formula of Wallis**)**

$$\sqrt{\pi} = \lim_{n\to\infty}\frac{2^{2n}\cdot(n!)^2}{(2n)!\cdot\sqrt{n+1/2}}.$$

Proof. Starting with the product expansion of the sine function,

$$\sin(\pi x) = \pi x\cdot\prod_{k=1}^{\infty}(1-\frac{x^2}{k^2}),$$

and substituting $x = 1/2$, we get

$$1 = \frac{\pi}{2}\cdot\prod_{k=1}^{\infty}\frac{4k^2-1}{4k^2},$$

$$\frac{\pi}{2} = \prod_{k=1}^{\infty}\frac{(2k)^4}{(2k-1)2k\cdot 2k(2k+1)} = \lim_{n\to\infty}\frac{2^{4n}\cdot(n!)^4}{((2n)!)^2(2n+1)},$$

and this immediately yields the assertion. $\diamond$

Corollary 1 *For all natural numbers* $n \geq 1$

$$\frac{n!\,e^n}{n^n} = \sqrt{2\pi n}\cdot u_n$$

where the error term u_n is bounded by

$$1 + \frac{1}{13n} < u_n < 1 + \frac{1}{11n}.$$

For[10] $n \to \infty$

$$\frac{n!\, e^n}{n^n} = \sqrt{2\pi n} + \mathrm{O}\left(\frac{1}{\sqrt{n}}\right).$$

Proof. We use the inequality $e^x > 1 + x$ for all real $x \neq 0$. For $0 < x < 1$ we therefore have $1 - x \leq e^{-x}$, whence $e^x \leq \frac{1}{1-x} = 1 + \frac{1}{\frac{1}{x}-1}$. Therefore

$$\frac{n!\, e^n}{n^n} < \sqrt{2\pi n} \cdot \left(1 + \frac{1}{12n-1}\right) \leq \sqrt{2\pi n} \cdot \left(1 + \frac{1}{11n}\right).$$

For the lower bound we have

$$\frac{n!\, e^n}{n^n} > \sqrt{2\pi n} \cdot \left(1 + \frac{1}{12n+1}\right) \geq \sqrt{2\pi n} \cdot \left(1 + \frac{1}{13n}\right).$$

◇

Corollary 2 *For all natural numbers $n \geq 1$*

$$\frac{n^n}{n!\, e^n} = \frac{1}{\sqrt{2\pi n}} \cdot v_n$$

where the error term v_n is bounded by

$$1 - \frac{1}{12n} < v_n < 1 - \frac{1}{14n},$$

in particular $v_n = 1 + \varepsilon_n$ where $\varepsilon_n = \mathrm{O}(\frac{1}{n})$ for $n \to \infty$.

Proof. The lower bound is immediate from $1 - x \leq e^{-x}$. For the upper bound we use $e^{-x} < \frac{1}{1+x} = 1 - \frac{1}{\frac{1}{x}+1}$, and get

$$\frac{n^n}{n!\, e^n} < \frac{1}{\sqrt{2\pi n}} \cdot \left(1 - \frac{1}{12n+2}\right) \leq \frac{1}{\sqrt{2\pi n}} \cdot \left(1 - \frac{1}{14n}\right).$$

◇

The narrow error bounds of the Stirling formula in Proposition 3 are due to Robbins, see [4].

[10] Here is an exact algebraic interpretation of asymptotic O-statements for $n \to \infty$: Consider the ring R of all real-valued functions $\mathbb{N} \longrightarrow \mathbb{R}$. For $h \in R$ the set of all functions that "are" $\mathrm{O}(h)$ is closed under addition and under multiplication by bounded functions. Interpret $\mathrm{O}(h)$ as this set, then it is a weak form of an ideal. Instead of $f = g + \mathrm{O}(h)$ we should write $f - g \in \mathrm{O}(h)$.

6 Parenthesis: Some Bits of Calculus

Lemma 5 (Gaussian integral)

$$\int_{-\infty}^{\infty} e^{-x^2/2}\,dx = \sqrt{2\pi}\,.$$

Proof. There are several tricks for evaluating this integral I—the most elegant of them might be the following: Interpret the square

$$I^2 = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-s^2/2}e^{-t^2/2}\,ds\,dt$$

as an area integral and transform it to polar coordinates $s = r\cos\varphi$, $t = r\sin\varphi$. The Jacobi matrix of this transformation is

$$\begin{pmatrix} \cos\varphi & -r\sin\varphi \\ \sin\varphi & -r\cos\varphi \end{pmatrix},$$

hence the Jacobi determinant is r, and thus

$$I^2 = \int_0^{\infty}\int_0^{2\pi} e^{-r^2/2} r\,dr\,d\varphi = 2\pi\cdot\int_0^{\infty} e^{-u}du = 2\pi.$$

We conclude that $I = \sqrt{2\pi}$. $\diamond$

In the following we perform the operations of taking square roots, and of reverting and inverting power series by using indeterminate coefficients and equating coefficients[11]. For future tricky integral substitutions we'll need some auxiliary functions, see Figure 5:

Lemma 6 *Let the function $f\colon]-1,\infty[\longrightarrow \mathbb{R}$ be defined by*

$$f(u) = u - \ln(1+u).$$

Then $f(0) = 0$, $f'(u) = u/(u+1)$, and f is strictly increasing in the interval $[\,0,\infty[$. For $-1 < u < 1$ the function f is represented by the power series

$$f(u) = \frac{1}{2}\,u^2 - \frac{1}{3}\,u^3 + \frac{1}{4}\,u^4 \pm \ldots = \sum_{i=2}^{\infty} \frac{(-1)^i}{i}\,u^i$$

Proof. Elementary calculus. $\diamond$

Corollary 3 *Let $g = f^{-1}$ be the inverse function in the interval $[\,0,\infty[$, in other words,*

$$u = g(x) \Longleftrightarrow x = f(u).$$

Then g satisfies the differential equation $g' = 1 + 1/g$ in $]0,\infty[$.

[11] This leads to confusing formulas, if we strive for exact estimates. Therefore we are content with O-statements.

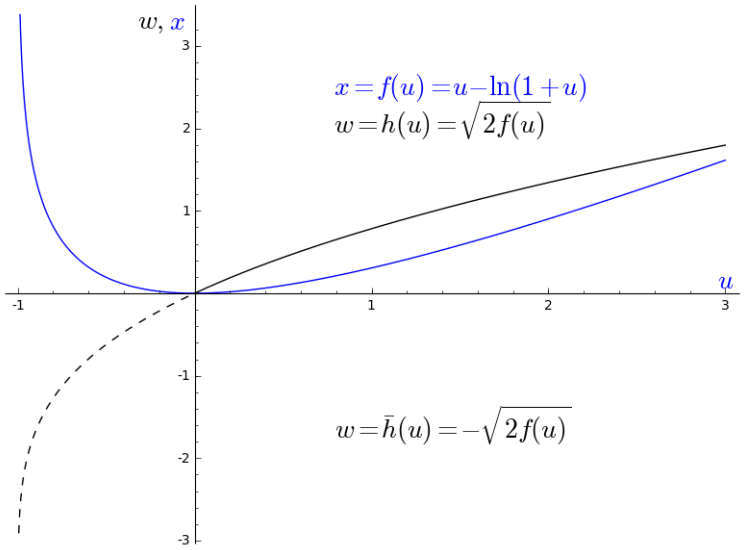

Figure 5: The auxiliary function f

Proof. For $u = g(x)$ we conclude by the inverse function theorem and Lemma 6 that $g'(x) = (u+1)/u = 1 + 1/u$. $\diamond$

Lemma 7 *There is an analytic function $h :]-1, \infty[\longrightarrow \mathbb{R}$ with $h^2 = 2f$. It is strictly increasing, has $h'(0) = 1$, and*

$$h(u) = \begin{cases} \sqrt{2f(u)} & \text{for } u \geq 0, \\ -\sqrt{2f(u)} & \text{for } u \leq 0, \end{cases} \tag{2}$$

see Figure 5. Its power series expansion around 0 is[12]

$$h(u) = u \cdot \left(1 - \frac{1}{3}\,u + \alpha(u)\right)$$

where α is a power series with terms $a_i u^i$, $i \geq 2$, $a_i \in \mathbb{R}$, in other words, $\alpha(u)$ is a $\mathrm{O}(u^2)$ for $u \to 0$.

Proof. If h exists, then it has a power series expansion

$$h(u) = a_1 u + a_2 u^2 + a_3 u^3 + \ldots$$

around 0. We compare the coefficients in

$$u^2 - \frac{2}{3}\,u^3 \pm \ldots = 2\,f(u) = h(u)^2 = a_1^2\,u^2 + 2\,a_1 a_2\,u^3 + \ldots$$

[12] Complex analysis immediately tells us that the convergence radius is 1.

and get a unique solution beginning with $a_1 = 1$, $a_2 = -1/3$.

For $h =$ this power series we have $h(0) = 0$ and $h'(0) = a_1 = 1$. Thus h is positive for small $u \geq 0$, and negative for $u < 0$ near 0. Therefore the square roots have to be taken such that Equation (2) holds. Finally h is strictly increasing in $[\,0, \infty[$ because f is, and in $]-1, 0\,]$ because f is strictly decreasing in this interval. $\diamond$

Lemma 8 *Let $j = h^{-1} \colon \mathbb{R} \longrightarrow]-1, \infty[$ be the inverse function. Then*

$$j(w) = w \cdot \left(1 + \frac{1}{3}\, w + \beta(w)\right) \quad \textit{for small } w > 0,$$

where β is a power series with terms $b_i w^i$, $i \geq 2$, $b_i \in \mathbb{R}$, in other words, β is a $\mathrm{O}(w^2)$.

Proof. Since j is analytic, and $j(0) = 0$, it has a power series expansion

$$j(w) = b_1 w + b_2 w^2 + \ldots$$

around 0. We compare the coefficients in

$$w = h(j(w)) = j(w) - \frac{1}{3}\, j(w)^2 + \ldots = b_1 w + (b_2 - \frac{1}{3}\, b_1^2)\, w^2 + \ldots$$

and get $b_1 = 1$, $b_2 = b_1^2/3 = 1/3$. $\diamond$

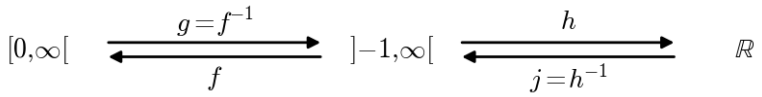

Figure 6: The auxiliary functions f, g, h, j

The diagram in Figure 6 gives some orientation with all these functions and inverse functions.

Corollary 4 *For small $w > 0$*

$$\frac{1}{j(w)} = \frac{1}{w} \cdot \left(1 - \frac{1}{3}\, w + \gamma(w)\right)$$

where γ is a power series with terms $c_i w^i$, $i \geq 2$, $c_i \in \mathbb{R}$, in other words, γ is a $\mathrm{O}(w^2)$.

Proof. Since $j(w)/w$ is analytic, so is $w/j(w)$, and it has a power series expansion $w/j(w) = \sum c_i w^i$ around 0. We compare the coefficients in

$$1 = \frac{j(w)}{w} \cdot \frac{w}{j(w)} = \left(1 + \frac{1}{3}\, w + \ldots\right) \cdot (c_0 + c_1 w + \ldots)$$

and get $c_0 = 1$, $c_1 = -1/3$. $\diamond$

Lemma 9 *For the inverse function $g = f^{-1}$ in $[0,\infty[$ there are constants $c > 0$ and $r > 0$ such that*

$$1 + \frac{1}{g(x)} = \frac{1}{\sqrt{2x}} + \frac{2}{3} + \delta(x) \quad \textit{for } 0 < x < \infty,$$

with $|\delta(x)| \le c\sqrt{x}$ for $0 < x < r$. In other words: $\delta(x)$ is a $\mathrm{O}(x^{1/2})$ for $x \to 0$.

Proof. Since f takes only values ≥ 0 in $[0,\infty[$ we have

$$h \circ g(x) = \sqrt{2\, f \circ g(x)} = \sqrt{2x}$$

for $x \ge 0$. Applying $h = g^{-1}$ yields $g(x) = j(\sqrt{2x})$, hence

$$1 + \frac{1}{g(x)} = 1 + \frac{1}{j(\sqrt{2x})} = 1 + \frac{1}{\sqrt{2x}} \left(1 - \frac{1}{3}\sqrt{2x} + \gamma(2x)\right)$$

for small $x > 0$. $\diamond$

7 Parenthesis: The Gamma Function

We need some simple properties of the gamma function. It is defined by

$$\Gamma(x) = \int_0^\infty e^{-t} t^{x-1}\, dt \quad \text{for } x > 0.$$

Proposition 4 (i) $\Gamma(1) = 1$.

(ii) $\Gamma(x+1) = x \cdot \Gamma(x)$.

(iii) $\Gamma(n) = (n-1)!$ *for each natural number* $n \ge 1$.

(iv) $\Gamma(\frac{1}{2}) = \sqrt{\pi}$.

Proof. (i) immediate.

(ii) By partial integration we conclude

$$\Gamma(x+1) = \int_0^\infty e^{-t} t^x\, dt = x \cdot \int_0^\infty e^{-t} t^{x-1}\, dt = x \cdot \Gamma(x).$$

(iii) follows from (i) and (ii) by induction.

(iv) The substitution $t = s^2/2$ leads to

$$\Gamma(\frac{1}{2}) = \int_0^\infty \frac{e^{-t}}{\sqrt{t}}\, dt = \sqrt{2} \cdot \int_0^\infty e^{-s^2/2}\, ds = \frac{1}{\sqrt{2}} \cdot \int_{-\infty}^\infty e^{-s^2/2}\, ds,$$

and this integral evaluates to $\sqrt{\pi}$ by Lemma 5. $\diamond$

Proposition 5 (RAMANUJAN) *For $n \to \infty$ we have*

$$\frac{\gamma(n,n)}{\Gamma(n)} = \frac{1}{2} + \frac{1}{3\sqrt{2\pi n}} + \mathrm{O}(\frac{1}{n})\,.$$

Proof. By partial integration we get

$$\begin{aligned}\frac{\gamma(n,n)}{\Gamma(n)} &= \frac{1}{(n-1)!}\cdot\int_0^n e^{-t}t^{n-1}\,dt = \frac{n^n}{n!e^n} + \frac{1}{n!}\cdot\int_0^n e^{-t}t^n\,dt \\ &= \frac{n^n}{n!e^n} + \underbrace{\frac{1}{n!}\cdot\int_0^\infty e^{-t}t^n\,dt}_{=1 \text{ by Prop. 4 (iii)}} - \underbrace{\frac{1}{n!}\cdot\int_n^\infty e^{-t}t^n\,dt}_{=:I_n}\,.\end{aligned}$$

In the integral I_n we substitute $t = n + nu = n\,(1+u)$:

$$I_n = \frac{n^n}{n!e^n}\cdot\underbrace{n\cdot\int_0^\infty e^{-nu}(1+u)^n\,du}_{=:J_n}\,.$$

In summary we get

$$\frac{\gamma(n,n)}{\Gamma(n)} = 1 + \frac{n^n}{n!e^n}\cdot(1-J_n)\,.$$

In the integral J_n we substitute $x = u - \ln(1+u) = f(u)$ from Lemma 6—this is a strictly increasing function of u in $[0,\infty[$ which takes the value 0 at $x = 0$, and

$$\frac{dx}{du} = 1 - \frac{1}{1+u} = \frac{u}{u+1}\,,\quad \frac{du}{dx} = 1 + \frac{1}{u} = 1 + \frac{1}{g(x)}\,.$$

This yields

$$\begin{aligned}J_n &= n\cdot\int_0^\infty e^{-n\,(u-\ln(1+u))}\,du = n\cdot\int_0^\infty e^{-nx}\,\left(1+\frac{1}{g(x)}\right)\,dx \\ &= n\cdot\int_0^\infty e^{-nx}\,\left(\frac{1}{\sqrt{2}}\,x^{-\frac{1}{2}} + \frac{2}{3} + \delta(x)\right)\,dx\end{aligned}$$

with help of Lemma 9. Thus the evaluation of the integral J_n leads to integrals of types

$$n\cdot\int_0^\infty e^{-nx}x^a\,dx$$

where $a > -1$. Substituting $t = nx$, thus $n\,dx = dt$, by the definition of Γ

$$n\cdot\int_0^\infty e^{-nx}x^a\,dx = \frac{1}{n^a}\cdot\int_0^\infty e^{-t}t^a\,dt = \frac{\Gamma(a+1)}{n^a}\,.$$

In summary we have

$$J_n = \frac{1}{\sqrt{2}}\cdot\Gamma(\frac{1}{2})\cdot n^{-1/2} + \frac{2}{3} + R_n \;=\; \sqrt{\frac{\pi}{2}}\cdot\sqrt{n} + \frac{2}{3} + R_n\,.$$

The remainder R_n decomposes as

$$R_n = n \cdot \int_0^\infty e^{-nx}\delta(x)\,dx = \underbrace{n \cdot \int_0^r e^{-nx}\delta(x)\,dx}_{R_n(r)} + \underbrace{n \cdot \int_r^\infty e^{-nx}\delta(x)\,dx}_{S_n(r)}$$

where the first summand is bounded by

$$|R_n(r)| \le c \cdot \frac{\Gamma(\frac{3}{2})}{n^{\frac{1}{2}}}.$$

For the second summand we use that for $x > 0$

$$\delta(x) = 1 + \frac{1}{g(x)} - \frac{1}{\sqrt{2x}} - \frac{2}{3},$$

yielding a decomposition

$$\begin{aligned} S_n(r) &= n \cdot \int_r^\infty e^{-nx}\delta(x)\,dx \\ &= \underbrace{n \cdot \int_r^\infty e^{-nx}\left(1 + \frac{1}{g(x)}\right)\,dx}_{A_n(r)} - \underbrace{n \cdot \int_r^\infty e^{-nx}\frac{1}{\sqrt{2x}}\,dx}_{B_n(r)} - \underbrace{\frac{2n}{3} \cdot \int_r^\infty e^{-nx}\,dx}_{C_n(r)} \end{aligned}$$

For $A_n(r)$ we use that $r \le x \le g(x)$ and get

$$0 \le A_n(r) \le n \cdot \int_r^\infty e^{-nx}\left(1 + \frac{1}{r}\right)\,dx \le \left(1 + \frac{1}{r}\right) \cdot e^{-nr}.$$

Estimating $B_n(r)$ and $C_n(r)$ is even simpler:

$$0 \le B_n(r) \le \frac{n}{\sqrt{2}} \cdot \int_r^\infty e^{-nx}\frac{1}{\sqrt{r}}\,dx \le \frac{1}{\sqrt{2r}} \cdot e^{-nr},$$

$$C_n(r) = \frac{2n}{3} \cdot \int_r^\infty e^{-nx}\,dx = \frac{2}{3} \cdot e^{-nr}.$$

Putting the snippets together yields

$$-\left(\frac{1}{\sqrt{2r}} + \frac{2}{3}\right) \cdot e^{-nr} \le S_n(r) \le \left(1 + \frac{1}{r}\right) \cdot e^{-nr}.$$

For large n (depending on r) we get $|S_n(r)| \le 1/n$. And so

$$\left|J_n - \sqrt{\frac{\pi}{2}} \cdot \sqrt{n} - \frac{2}{3}\right| = |R_n| = |R_n(r) + S_n(r)| \le c \cdot \frac{\Gamma(\frac{3}{2})}{\sqrt{n}} + \frac{1}{n} \le \frac{d}{\sqrt{n}}$$

for large n with a constant $d > 0$. Using this bound and Corollary 2 of the Stirling formula, Proposition 3, we get

$$\frac{\gamma(n,n)}{\Gamma(n)} \;=\; 1 + \frac{n^n}{n!e^n} \cdot (1 - J_n) \;=\; 1 + \frac{1}{\sqrt{2\pi n}}\,\left(1 + \mathrm{O}(\frac{1}{n})\right) \cdot (-\sqrt{\frac{\pi n}{2}} + \frac{1}{3} + \mathrm{O}(\frac{1}{\sqrt{n}}))$$

$$= 1 - \frac{1}{2} + \frac{1}{3\sqrt{2\pi n}} + \mathrm{O}(\frac{1}{n}) \,,$$

as claimed. $\diamond$

Applying Ramanujan's asymptotic formula, Proposition 5, to the function Q as given by Proposition 2, and using Corollary 1 of Stirling's formula, Proposition 3, we get:

$$\begin{aligned} Q(n) &= \frac{n!e^n}{n^n} \cdot \left(1 - \frac{\gamma(n,n)}{\Gamma(n)}\right) \\ &= \left(\sqrt{2\pi n} + \mathrm{O}\left(\frac{1}{\sqrt{n}}\right)\right) \cdot \left(\frac{1}{2} - \frac{1}{3\sqrt{2\pi n}} + \mathrm{O}\left(\frac{1}{n}\right)\right) \\ &= \sqrt{\frac{\pi}{2}} \cdot \sqrt{n} - \frac{1}{3} + \mathrm{O}\left(\frac{1}{\sqrt{n}}\right). \end{aligned}$$

Corollary 5 *For $n \to \infty$ we have*

$$Q(n) = \sqrt{\frac{\pi}{2}} \cdot \sqrt{n} - \frac{1}{3} + \mathrm{O}\left(\frac{1}{\sqrt{n}}\right) .$$

For a single concrete n such a O-statement has no meaning. Nevertheless numerical experiments show that the approximation is quite exact: From $n = 4$ on the first decimal place is correct, from $n = 950$ on even the second. And the error term decreases in absolute value for $n \to \infty$.

8 The Main Result

Let us apply this result to the recursive sequences of Proposition 1:

Theorem 1 *Let M be a finite set of $m = \#M$ elements. Up to a summand of type $\mathrm{O}(1/\sqrt{m})$ the expected value for the periods of the recursive sequences in M is*

$$\sqrt{\frac{\pi}{8}} \cdot \sqrt{m} + \frac{1}{3},$$

the expected value for the preperiods is

$$\sqrt{\frac{\pi}{8}} \cdot \sqrt{m} - \frac{2}{3},$$

ans the expected value for the number of different elements is

$$\sqrt{\frac{\pi}{2}} \cdot \sqrt{m} - \frac{1}{3}.$$

The expected values for preperiod and period are about $\sqrt{\pi/8} \cdot \sqrt{m} \approx 0.63 \cdot \sqrt{m}$, and the expected number of different elements is about $\sqrt{\pi/2} \cdot \sqrt{m} \approx 1.25 \cdot \sqrt{m}$.

As a consequence we might informally conclude: For the "classical" pseudorandom generators that aim at the maximum possible period length (about m) a modification will probably lead to a much shorter period length and significantly fewer different output elements—but maybe to better cryptographic strength, and so also to better pseudorandom properties, at the cost of squaring the size of the base set M, or doubling the bitsize of the objects under consideration.

By the way the subject of this note may be interpreted as "random mappings of finite sets". For a comprehensive treatment see the book [3].

A Explicit Determination of the Distributions

The formulas in Lemma 1 yield an efficient algorithm for calculating the distributions of the preperiods, periods, and effective lengths of recursive sequences of recursion depth 1. In this appendix we specify this explicitly. However for explicit calculations we prefer integers as far as possible. Therefore we deal with frequencies instead of probabilities (= relative frequencies). Thus we consider

$$F_m(\mu,\nu) = \#\{(s,x) \mid f(s,x) = \mu, g(s,x) = \nu\} = m^{m+1}\, P_m(\mu,\nu) = m^m\, R_m(\mu+\nu-1).$$

The corresponding integer version of R_m is

$$\hat{R}_m(l) = \prod_{k=1}^{l} (m-k) = m^l\, R_m(l).$$

Using this the frequencies are given by

$$F_m(\mu,\nu) = m^m \cdot R_m(\mu+\nu-1) = m^{m+1-\mu-\nu} \cdot \hat{R}_m(\mu+\nu-1), \tag{3}$$

$$F_m(\mu,*) = \sum_{\nu=1}^{m-\mu} F_m(\mu,\nu) = \sum_{\nu=1}^{m-\mu} m^{m+1-\mu-\nu} \cdot \hat{R}_m(\mu+\nu-1), \tag{4}$$

$$F_m(*,\nu) = \sum_{\mu=0}^{m-\nu} F_m(\mu,\nu) = \sum_{\mu=0}^{m-\nu} m^{m+1-\mu-\nu} \cdot \hat{R}_m(\mu+\nu-1), \tag{5}$$

$$\varphi_m(\lambda) = \sum_{\mu+\nu=\lambda} F_m(\mu,\nu) = m^{m+1-\lambda} \cdot \lambda\, \hat{R}_m(\lambda-1), \tag{6}$$

where $\varphi_m(\lambda)$ denotes the number of all sequences of effective length λ, compare Lemma 1 (vi).

For the algorithmic determination of these frequencies we first calculate the value table of $\hat{R}_m$ by the recurrence

$$\hat{R}_m(0) := 1, \quad \hat{R}_m(l) = (m-l) \cdot \hat{R}_m(l-1) \quad \text{for } \; l = 1, \ldots, m.$$

Note that $\hat{R}_m(l) := 0$ for $l \geq m$.

Then we calculate the frequencies $F_m(\mu, *)$ of the preperiods μ by Formula (4), the frequencies $F_m(*, \nu)$ of the periods ν by Formula (5), and the frequencies $\varphi_m(\lambda)$ of the lengths λ by Formula (6).

B Python Code

```
import sys
m = int(sys.argv[1])
mm = m**(m+1)

### Part 0: The auxiliary function Rhat -
###         calculate the list [Rhat[0], ..., Rhat[m]].

Rhat = [1]
for l in range(1,m):
  Rhat.append((m-l)*Rhat[l-1])

### Part 1: The frequency and probability of preperiod mu.

Fmu = []     # list of frequencies
for mu in range(0,m+1):
  sum = 0
  for nu in range(1,m+1-mu):
    sum += m**(m+1-mu-nu) * Rhat[mu+nu-1]
  Fmu.append(sum)
pmu = []     # list of probabilities
for mu in range(0,m+1):
  pmu.append(round(Fmu[mu]/mm,3))
print(pmu)

### Part 2: The frequency and probability of period nu.

Fnu = [0]     # list of frequencies
for nu in range(1,m+1):
  Fnu.append(Fmu[nu-1])
pnu = []     # list of probabilities
for nu in range(0,m+1):
  pnu.append(round(Fnu[nu]/mm,3))
print(pnu)
```

```
### Part 3: The frequency and probability of effective length lambda.

Lm = [0]     # list of frequencies
for l in range(1,m+1):
  Lm.append(m**(m+1-l) * l * Rhat[l-1])
plm = []     # list of probabilities
for l in range(0,m+1):
  plm.append(round(Lm[l]/mm,3))
print(plm)
```

References

[1] Solomon W. Golomb, *Shift Register Sequences*. Revised Edition: Aegean Park Press, Laguna Hills 1982.

[2] D. Knuth: *The Art of Computer Programming*, Vol. 2. Addison-Wesley, Reading 1981 (2nd Ed.).

[3] V. F. Kolchin: *Random Mappings.* Springer-Verlag, Berlin usw. 1986.

[4] H. Robbins: A remark on Stirling's formula. Amer. Math. Monthly 62 (1955), 26–29.