12.9 偏った硬貨から公平な判定を

ワークシート

問題

STEP I 2019、問 11

先に進む前に、まず問題を読んでおこう。問題は、OCR が配布している 2019 年の STEP 過去問一式（zip ファイル）のうち、STEP I の問題用紙にある：

www.ocr.org.uk/Images/696590-2019-past-papers.zip

ヒント

まずは自力で問題に取り組んでみよう。行き詰まったら、ヒントを**一つずつ**読み、そのたびに問題に戻ること。**手を止めて、やってみよう**と記したヒントが重要な段階である。各ヒントの後には計算用の余白がある。

> **考えてみよう**　1 回のラウンドで決定が下される確率はいくらか。決定が下されない確率はどうか。$2pq$ がとりうる最大の値はいくらか。

段階 1　第 n 回での決着

扱う内容：小問 (i)、第 n 回

> **考えてみよう**　1 回の試行で、硬貨の表裏が一致する確率（probability）はいくらか。第 n 回で決着するには、$n-1$ 回続けて不一致となり、その次に一致する必要がある。

段階 2 第 n 回までの決着

扱う内容：小問 (i)、第 n 回まで

> **手を止めて、やってみよう** 最初の n 回で決着しない確率はいくらか。$pq = p(1-p)$ はどこまで大きくなり得るか。

段階 3　3 人の場合

扱う内容：小問 (ii)

考えてみよう　第 1 回は、3 枚の硬貨がすべて一致したときに決着する。そうでない場合、多数派が表であれば、少数の 1 枚を表に変える。このとき第 2 回では何が必要か。多数派が裏の場合はどうか。

手を止めて、やってみよう　$p+q=1$ と $p^3+q^3=(p+q)^3-3pq(p+q)$ を用いて、すべてを $s=pq$ で表せ。

背後にある数学

フォン・ノイマンのトリック

この問題の手順は速いが偏り（bias）がある。フォン・ノイマンの手順は公平である：2 回投げ、HT か TH なら決定し、HH か TT なら繰り返す。各試行が成功する確率は $2pq$ なので、平均して $\frac{1}{2pq}$ 回の試行を要し、硬貨が大きく偏っているときには時間がかかる（図 12.9.1）。この問題の手順は 1 ラウンドあたり確率 $p^2+q^2\geq\frac{1}{2}$ で決定を下すが、$p>\frac{1}{2}$ のときにはその答えがホテルに偏る。

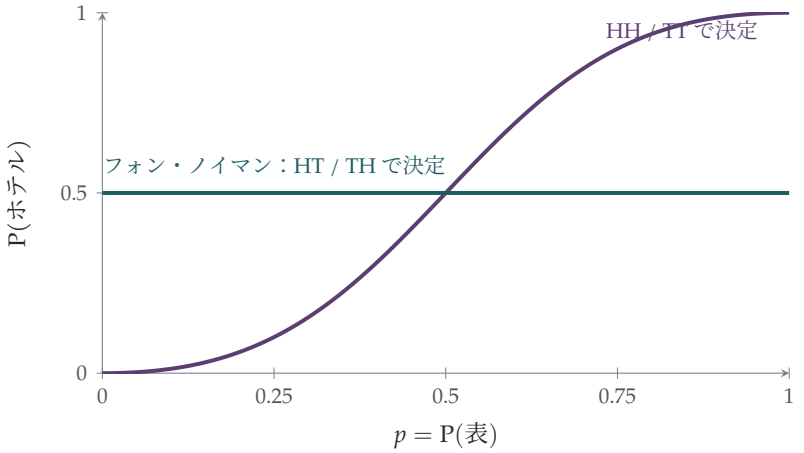

図 12.9.1　硬貨の偏りに対する、ホテルが選ばれる確率。硬貨の結果が一致したときに決定する方法（プラム色）は速いが、出やすい面に有利になる。フォン・ノイマンの手順（ティール色）はすべての p に対して厳密に公平であるが、その代償として、硬貨が大きく偏っているときには時間がかかる。

ランダムネスの抽出

フォン・ノイマンのトリックは、最初の**乱数抽出器**（randomness extractor）である。これは不完全なランダムネスを完全なランダムネスに変える手順である。この方法は無駄が多い（2 回投げるごとに得られる公平なビットは高々 1 つで、1 つも得られないことも多い）。より優れた方法では、捨てられた HH や TT の組を再利用して、硬貨がもつランダムネスのほぼすべてを抽出する。このランダムネスの量は、1 回の投げあたり $-p\log_2 p - q\log_2 q$ ビットという**エントロピー**（entropy）で測られる。抽出器は、コンピュータのハードウェア乱数生成器で用いられている。ハードウェア乱数生成器は、予測不可能だが偏りのある物理的なノイズを集め、それを暗号のために偏りのないビットに変換しなければならないのである。

フォン・ノイマンと乱数

フォン・ノイマンは、1951 年の論文 “Various techniques used in connection with random digits”（乱数に関連して用いられるさまざまな技法）でこのトリックを述べた。この論文が書かれたのは、彼と同僚たちが核兵器の設計のために、最初期のコンピュータ・シミュレーションのいくつか（「モンテカルロ法（Monte Carlo method）」）を実行していた時期である。同じ論文の中で、彼は算術によって乱数を生成することについて、有名な言葉を残している：「算術的な方法で乱数を作り出そうと考える者は、言うまでもなく罪の状態にある。」

次の一歩

1. **ラウンド数の期待値。**小問 (i) の手順とフォン・ノイマンの手順のそれぞれについて、ラウンド数の期待値（expected value）を求めよ。どのような p に対して、フォン・ノイマンの手順のほうが遅くなるか。

2. **公平な三者択一。**偏りのある硬貨を用いて、3 つの選択肢のうち 1 つを、それぞれちょうど確率 $\frac{1}{3}$ で選ぶ手順を考案せよ。

3. **公平な硬貨から偏ったさいころを。**公平な硬貨を用いて、表が出る確率がちょうど $\frac{1}{3}$ である硬貨を模擬する手順を考案せよ。投げる回数の期待値はいくらか。

4. **再び 3 人の場合。**小問 (ii) において、3 人がホテルに行く確率を p の関数として求めよ。$p = \frac{1}{2}$ のとき、この手順は公平か。

さらに学ぶために

- **John von Neumann, “Various techniques used in connection with random digits”**, *National Bureau of Standards Applied Mathematics Series* 12 (1951). 短く、有名な論文である。
- **Donald Knuth, *The Art of Computer Programming*, Vol. 2** (Addison-Wesley)。第 3 章で乱数を扱っている。
- **Michael Mitzenmacher & Eli Upfal, *Probability and Computing*** (Cambridge University Press)。ランダムネスの抽出とエントロピーを扱っている。

詳しい解説付きの解答は第 12.9 節にある：

https://beyondstep.keithmcnulty.org/ja/ch12/von-neumann.html

毎週 1 問の STEP の問題を丁寧に解き明かす The STEP Up。メールで無料配信中：keithmcnulty.substack.com