

# Kullback-Leibler 情報量と Sanov の定理

黒木玄

2016 年 6 月 16 日作成\*

<http://www.math.tohoku.ac.jp/~kuroki/LaTeX/20160616KullbackLeibler.pdf>

## 目次

0	はじめに	2
1	多項分布から Kullback-Leibler 情報量へ	4
1.1	母集団分布が $q_i$ の多項分布	4
1.2	サンプルサイズを大きくしたときの多項分布の漸近挙動	5
1.3	Kullback-Leibler 情報量と相対エントロピーの定義	5
1.4	Kullback-Leibler 情報量の基本性質	6
1.5	二項分布の場合の計算例	7
1.6	max-plus 代数への極限や Laplace の方法との関係	8
1.7	区分求積法による高校レベルの計算で KL 情報量を出す方法	9

\*最新版は下記 URL からダウンロードできる。飽きるまで継続的に更新と訂正を続ける予定である。6 月 16 日 Ver.0.1(10 頁)。数時間かけて 10 頁ほど書いた。6 月 17 日 Ver.0.2(16 頁)。区分求積法による高校レベルの方法に関する付録 1.7 と多項分布の場合の Sanov の定理の厳密に証明するための第 3 節を追加した。そこで紹介した証明は階乗に関する Stirling の公式さえ使わない極めて初等的な証明である。6 月 18 日 Ver.0.2.1。小さな追加と訂正。6 月 18 日 Ver.0.3(22 頁)。Sanov の定理からカノニカル分布の導出について説明した第 4 節を追加した。たくさんのケアレスミスを訂正した。6 月 18 日 Ver.0.3.1。第 4.3 節の誤植を訂正。6 月 19 日 Ver.0.4(23 頁)。例 4.3 の説明の仕方を変更した。他にも細かな訂正。相対 Rényi エントロピーの定義だけに触れた注意 7.2 を追加した。6 月 21 日 Ver.0.5(26 頁)。注意 4.1 に「時間を巻き戻してギャンブルをやり直す話」との関係を追記した。この文書は注意 4.1 から読み始めると読み易いかもしれない。相対 Tsallis エントロピーの定義だけに触れた注意 7.3 を追加した。6 月 22 日 Ver.0.6(30 頁)。タイトルを「KL 情報量の解説」から「KL 情報量と Sanov の定理」に変更した。注意 7.3 などを別の部分節に分離し、内容も増やした。さらにその脚注に相対 Tsallis エントロピーの定義の必然性を理解できていないことを正直に書いた。細かな手直し。「加法性」に関する注意 7.5 を追加した。6 月 23 日 Ver.0.7(32 頁)。相対エントロピーが多項分布の漸近挙動を記述しているのと同じように相対 Tsallis エントロピーで漸近挙動が記述される多項分布のある拡張の構成に関する第 7.5 節を追加した。6 月 24 日 Ver.0.8(36 頁)。KL 情報量が「距離」のような性質を持っていることを意味する不等式を扱った第 5 節を追加した。相対 Rényi エントロピーと相対 Tsallis エントロピー関係の説明を第 7 節に分離した。このノートには後で Cramér の定理の解説も追加する予定。Cramér の定理の上からの評価は自明であり、下からの評価はカノニカル分布に関する大数の弱法則から導かれる。7 月 5 日 Ver.0.9(39 頁)。lim sup と lim inf に関する簡単な解説(第 8 節)を追加した。7 月 6 日 Ver.0.10(40 頁)。相対 Tsallis エントロピーと相性のよい第 7.5 節とは異なる多項分布の拡張に関する第 7.6 節を追加した。7 月 7 日(七夕)Ver.0.11(41 頁)。相対 Rényi エントロピーと相対 Tsallis エントロピーの負値性に関する注意 7.4 を追加した。KL 情報量の記号を  $D[p|q]$  からより標準的な  $D(p||q)$  に書き変えた。置換し忘れがまだ残っている可能性が高い。7 月 7 日 Ver.0.12(48 頁)。Cramér の定理について解説した第 6 節を追加した。7 月 10 日 Ver.0.13(49 頁)。Cramér の定理のガンマ分布への適用例の解説(第 6.4 節)をより詳しくした。補題 6.2 の証明の誤りを訂正した。

<b>2</b>	<b>条件付き大数の法則から Boltzmann 因子へ</b>	<b>9</b>
2.1	問題の設定	10
2.2	Boltzmann 因子の導出	10
2.3	母分布が連続型の場合から連続型の指数型分布族が得られること	12
2.4	標準正規分布の導出例	14
<b>3</b>	<b>多項分布の場合の Sanov の定理</b>	<b>14</b>
3.1	Sanov の定理の主張	14
3.2	Sanov の定理の証明の準備	16
3.3	Sanov の定理の証明	18
<b>4</b>	<b>Sanov の定理を使ったカノニカル分布の導出</b>	<b>20</b>
4.1	分配関数とエネルギーの期待値	20
4.2	条件付き確率分布のカノニカル分布への収束	22
4.3	まとめと二項分布もカノニカル分布の例になっていること	25
<b>5</b>	<b>付録: Kullback-Leibler 情報量に関する不等式</b>	<b>27</b>
5.1	準備: Jensen の不等式	27
5.2	対数和不等式とその応用	28
5.3	Kullback-Leibler 情報量で $L^1$ 距離を上からおさえられこと	29
5.4	Pithagorian theorem	30
<b>6</b>	<b>付録: Cramér の定理</b>	<b>31</b>
6.1	Cramér の定理の設定と主張	31
6.2	Cramér の定理の証明	33
6.3	カノニカル分布の相対エントロピーとの関係	37
6.4	ガンマ分布の場合の例	37
<b>7</b>	<b>付録: 他の種類のエントロピーについて</b>	<b>39</b>
7.1	自由エネルギーや Massieu 関数との関係	39
7.2	相対 Rényi エントロピー	40
7.3	相対 Tsallis エントロピー	41
7.4	加法性 (示量性) について	44
7.5	相対 Tsallis エントロピーを漸近挙動に含む多項分布の拡張 (1)	45
7.6	相対 Tsallis エントロピーを漸近挙動に含む多項分布の拡張 (2)	47
<b>8</b>	<b>付録: 上極限と下極限に関する簡単な解説</b>	<b>48</b>
8.1	上極限と下極限の定義	48
8.2	上極限と下極限の使い方	49

## 0 はじめに

このノートは次のノートの続編である:

「ガンマ分布の中心極限定理と Stirling の公式」というタイトルの雑多なノート

<http://www.math.tohoku.ac.jp/~kuroki/LaTeX/20160501StirlingFormula.pdf>

このノートで使用する Stirling の公式についてはそのノートを見て欲しい。この雑多なノートは「タイトルにいつわりあり」の雑多な内容のノートになっている。

このノートの目標は Kullback-Leibler 情報量 (相対エントロピーの  $-1$  倍) および Boltzmann 因子  $\exp(-\sum_{\nu} \beta_{\nu} f_{\nu}(k))$  で記述されるカノニカル分布が必然的に出て来る理由を説明することである<sup>1</sup>。最初の方では直観的な説明を重視し、数学的に厳密な議論は行なわない。第 3, 4 節において可能な範囲内で数学的に厳密な証明を行なう。

以下の文献などを参考にした。

## 参考文献

- [1] Csiszar, Imre. A simple proof of Sanov's theorem. Bull Braz Math Soc, New Series 37(4), 453–459, 2006.  
<http://www.emis.ams.org/journals/em/docs/boletim/vol374/v37-4-a2-2006.pdf>
- [2] Cover, M. Thomas and Thomas, Joy A. Elements of Information Theory. Second Edition, John Wiley & Sons, Inc., 2006, xxiii+748 pages. ([Google で検索](#))
- [3] Dembo, Amir and Zeitouni, Ofer. Large Deviations Techniques and Applications. Stochastic Modelling and Applied Probability (formerly: Applications of Mathematics), 38, Second Edition, Springer, 1998, 396 pages. ([Google で検索](#))
- [4] Ellis, Richard, S. The theory of large deviations and applications to statistical mechanics. Lecture notes for École de Physique Les Houches, August 5–8, 2008, 123 pages.  
<http://people.math.umass.edu/~rsellis/pdf-files/Les-Houches-lectures.pdf>
- [5] Sanov, I. N. On the probability of large deviations of random variables. English translation of Matematicheskii Sbornik, 42(84):1, pp. 11–44. Institute of Statistics Mimeograph Series No. 192, March, 1958.  
[http://www.stat.ncsu.edu/information/library/mimeo.archive/ISMS\\_1958\\_192.pdf](http://www.stat.ncsu.edu/information/library/mimeo.archive/ISMS_1958_192.pdf)
- [6] Suyari, Hiroki. Mathematical structure derived from the  $q$ -multinomial coefficient in Tsallis statistics. [arXiv:cond-mat/0401546](https://arxiv.org/abs/cond-mat/0401546)

---

<sup>1</sup>インターネット上での日本語による検索結果を眺めたところ、Kullback-Leibler 情報量 (相対エントロピーの  $-1$  倍) について「2つの確率分布の“距離”を表わす量」「2つの確率分布の違いを表わす量」のように説明しただけですませているものが目立ち、Kullback-Leibler 情報量が自然に出て来るシンプルな理由を十分に説明しているものを見付けることができなかつたのでこの解説ノートを書くことにした。Kullback-Leibler 情報量が必然的に出て来る理由は多項分布の  $n \rightarrow \infty$  での漸近挙動に Kullback-Leibler 情報量が自然に出て来るからである。そのことから、 $n \rightarrow \infty$  のときの経験分布の挙動を Kullback-Leibler 情報量で記述可能になる。その結果の数学的に厳密な定式化は Sanov の定理と呼ばれている。この解説ノートを書いたもう一つの理由は、Boltzmann 因子、カノニカル分布が出て来る理由を多項分布の  $n \rightarrow \infty$  での漸近挙動 (もしくは Sanov の定理) に基づいて分かり易く説明している日本語の解説をインターネット上に見付けることができなかつたことである。この解説ノートでは Boltzmann 因子  $e^{-\beta E_i}$  が出て来る理由も詳しく説明する。

- [7] Suyari, Hiroki and Scarfone, Antonio Maria.  $\alpha$ -divergence derived as the generalized rate function in Tsallis statistics. 信学技報, vol. 114, no. 138, IT2014-16, pp. 25–30, 2014 年 7 月. <http://www.ieice.org/ken/paper/201407178BPp/>
- [8] 田崎晴明. 統計力学 I, II. 新物理学シリーズ, 培風館 (2008/12), 合計 525 ページ.  
<https://www.amazon.co.jp/dp/4563024376>  
<https://www.amazon.co.jp/dp/4563024384>
- [9] Tim van Erven and Peter Harremoës. Rényi divergence and Kullback-Leibler divergence. [arXiv:1206.2459](https://arxiv.org/abs/1206.2459)
- [10] Ramon van Handel. Lecture 3: Sanov's theorem. Stochastic Analytic Seminar (Princeton University), Blog Article, 10 October 2013.  
<https://blogs.princeton.edu/sas/2013/10/10/lecture-3-sanovs-theorem/>
- [11] Vasicek, Oldrich Alfonso. A conditional law of large numbers. Ann. Probab., Volume 8, Number 1 (1980), 142–147.  
<http://projecteuclid.org/euclid.aop/1176994830>

## 1 多項分布から Kullback-Leibler 情報量へ

多項分布に Stirling の公式を単純に代入するだけで自然かつ容易に Kullback-Leibler 情報量 (もしくはその  $-1$  倍の相対エントロピー) が現われることを説明したい。

### 1.1 母集団分布が $q_i$ の多項分布

$q_i \geq 0$ ,  $\sum_{i=1}^r q_i = 1$  とする. 1 回の独立試行で状態  $i$  が確率  $q_i$  で得られる状況を考える.  $q = (q_1, \dots, q_r)$  を母集団分布と呼ぶことにする. そのような試行を  $n$  回繰り返したとき, 状態  $i$  が生じた回数を  $k_i$  と書く ( $k_i$  は確率変数である). そのとき状態  $i$  が生じた割合  $k_i/n$  (これを経験分布と呼ぶことにする) が  $n \rightarrow \infty$  でどのように振る舞うかを調べよう.

これは, サイコロ (歪んでいてもよい) を  $n$  回ふったときの  $i$  の目が出た割合の分布 (経験分布) が  $n \rightarrow \infty$  でどのように振る舞うかを調べる問題だと言ってよい.

大数の法則によって  $n \rightarrow \infty$  で  $k_i/n \rightarrow q_i$  となるが, 後で条件付き確率を考えたいので母集団分布から離れた分布が経験分布として現われる確率がどのように減衰するかを知りたい. 第 2 節では条件付き確率を考えることによって Boltzmann 因子が得られることを説明する.

我々はこれから母集団分布  $q = (q_1, \dots, q_r)$  を任意に固定し, 経験分布  $(k_1/n, \dots, k_r/n)$  の確率分布を考え, その  $n \rightarrow \infty$  での様子を調べることになる.

$n$  回の独立試行で状態  $i$  が  $k_i$  回得られる確率は,  $\sum_{i=1}^r k_i = n$  のとき

$$\frac{n!}{k_1! \cdots k_r!} q_1^{k_1} \cdots q_r^{k_r} \quad (*)$$

になり, 他のとき 0 になる (多項分布).

$p_i \geq 0$ ,  $\sum_{i=1}^r p_i = 1$  と仮定する.  $n$  回の独立試行で状態  $i$  が得られた割合  $k_i/n$  がほぼ  $p_i$  になるとき, 経験分布はほぼ  $p_i$  になるということにする.

## 1.2 サンプルサイズを大きくしたときの多項分布の漸近挙動

$n \rightarrow \infty$  のとき経験分布がほぼ  $p_i$  になる確率がどのように振る舞うかを知りたい. そこで  $n \rightarrow \infty$  のとき,  $k_i$  たちが

$$k_i = np_i + O(\log n) = np_i \left( 1 + O\left(\frac{\log n}{n}\right) \right) \quad (**)$$

を満たしていると仮定し, 上の確率 (\*) がどのように振る舞うかを調べよう. この仮定のもとで  $\log(k_i/n) = \log p_i + O((\log n)/n)$  が成立することに注意せよ<sup>2</sup>.

Stirling の公式と  $\sum_{i=1}^r k_i = n$  より

$$\log n! = n \log n - n + O(\log n) = \sum_{i=1}^r k_i \log n - \sum_{i=1}^r k_i + O(\log n),$$

$$\log k_i! = k_i \log k_i - k_i + O(\log k_i) = k_i \log k_i - k_i + O(\log n),$$

$$\log q_i^{k_i} = k_i \log q_i.$$

これらを上の確率 (\*) の対数に代入すると  $k_i$  の項はキャンセルする. さらに (\*\*) を代入すると次が得られる:

$$\begin{aligned} \log \left( \frac{n!}{k_1! \cdots k_r!} q_1^{k_1} \cdots q_r^{k_r} \right) &= -n \sum_{i=1}^r \frac{k_i}{n} \left( \log \frac{k_i}{n} - \log q_i \right) + O(\log n) \\ &= -n \sum_{i=1}^r p_i (\log p_i - \log q_i) + O(\log n) \\ &= -n \sum_{i=1}^r p_i \log \frac{p_i}{q_i} + O(\log n). \end{aligned}$$

同様の計算を区分求積法を用いた高校レベルの計算で実行することもできる (第 1.7 節).

## 1.3 Kullback-Leibler 情報量と相対エントロピーの定義

第 1.2 節の結果は

$$D(p||q) = \sum_{i=1}^r p_i \log \frac{p_i}{q_i}$$

とおくと次のように書き直される:

$$\log \left( \frac{n!}{k_1! \cdots k_r!} q_1^{k_1} \cdots q_r^{k_r} \right) = -nD(p||q) + O(\log n).$$

左辺は経験分布  $k_i/n$  がほぼ  $p_i$  になる確率の対数を意味していることに注意せよ.  $D(p||q)$  を **Kullback-Leibler 情報量** (カルバック・ライブラー情報量) もしくは **Kullback-Leibler divergence** と呼ぶ. Kullback-Leibler 情報量の  $-1$  倍

$$S(p||q) = -D(p||q) = - \sum_{i=1}^r p_i \log \frac{p_i}{q_i}$$

<sup>2</sup>Taylor 展開  $\log(1+x) = x - x^2/2 + x^3/3 - x^4/4 + \cdots$  より.

を相対エントロピーと呼ぶことにする. 相対エントロピーは本質的に  $n$  が大きなときの「母集団分布が  $q_i$  のとき経験分布がほぼ  $p_i$  となる確率の対数の  $n$  分の 1」である.

対数を取る前の公式は次の通り:

$$(n \text{ 回の独立試行で経験分布がほぼ } p_i \text{ になる確率}) = \exp(-nD(p||q) + O(\log n)).$$

もしも  $D(p||q) > 0$  ならば,  $n$  を十分に大きくすれば  $O(\log n)$  の項は  $nD(p||q)$  の項と比較して無視できる量になるので, この確率は  $\exp(-nD(p||q))$  の部分でほぼ決まっていると考えてよい.

## 1.4 Kullback-Leibler 情報量の基本性質

Kullback-Leibler 情報量  $D(p||q) = \sum_{i=1}^r p_i \log(p_i/q_i)$  は函数  $f(x) = x \log x$  を用いて,  $D(p||q) = \sum_{i=1}^r f(p_i/q_i) q_i$  と表わされるので,  $D(p||q)$  の  $p = (p_1, \dots, p_r)$  の函数としての性質を調べるためには函数  $f(x) = x \log x$  の性質を調べればよい.  $f'(x) = \log x + 1$ ,  $f''(x) = 1/x > 0$  なので函数  $f(x)$  は下に狭義凸である. ゆえに函数  $f(x)$  はその接線の函数で下から押さえられる. 特に  $f(x) \geq f(1) + f'(1)(x-1) = x-1$  (等号の成立と  $x=1$  は同値). ゆえに

$$D(p||q) = \sum_{i=1}^r f\left(\frac{p_i}{q_i}\right) q_i \geq \sum_{i=1}^r \left(\frac{p_i}{q_i} - 1\right) q_i = 0,$$

等号の成立は  $p_i = q_i$  ( $i = 1, \dots, r$ ) と同値.

さらに  $f(x)$  が下に狭義凸であることより,  $D(p||q)$  も  $p$  の函数として下に狭義凸であることもわかる.

このように Kullback-Leibler 情報量の値は 0 以上になり, 最小値 0 が実現することと分布  $p_i$  が母集団分布  $q_i$  に等しくなることは同値である. ゆえに, 分布  $p_i$  が母集団分布  $q_i$  に等しくないとき,  $D(p||q) > 0$  となるので, 経験分布がほぼ  $p_i$  になる確率は  $n \rightarrow \infty$  で  $n$  について指数函数的に 0 に収束する. したがって,  $n \rightarrow \infty$  で経験分布  $k_i/n$  は母集団分布  $q_i$  に近づく. これは大数の法則の成立を意味している.

Kullback-Leibler 情報量は母集団分布  $q_i$  のもとで分布  $p_i$  が経験分布としてどれだけ確率的に実現し難いかを表わしている. 異なる分布が実現する確率の比は  $n \rightarrow \infty$  で Kullback-Leibler 情報量の差の  $-n$  倍の指数函数のように振る舞う. ゆえに Kullback-Leibler 情報量がほんの少しでも違っていれば, Kullback-Leibler 情報量がより大きな方の分布は相対的にほとんど生じないということもわかる. ゆえに, ある条件を課して分布  $p_i$  が生じる条件付き確率を考える場合には, 課した条件のもとで Kullback-Leibler 情報量が最小になる分布に経験分布は (条件付き確率の意味で) 近づくことになる (条件付き大数の法則, 条件付き極限定理). この法則を最小 **Kullback-Leibler 情報量の原理** と呼ぶ.  $n$  が非常に大きなとき, ある条件のもとで経験的に実現される分布は課した条件のもとで Kullback-Leibler 情報量が最小の分布になる.

相対エントロピーは Kullback-Leibler 情報量の  $-1$  倍だったので, 条件付きで分布  $p_i$  が経験的に生じる確率を考える場合には課した条件のもとで相対エントロピーが最大になる分布に経験分布が近づくことになる. この言い換えを最大相対エントロピーの原理と呼ぶ.  $n$  が大きなとき, ある条件のもとで経験的に実現される分布は課した条件のもとで相対エントロピーが最大になるような分布である.

補足. 説明の簡素化のために条件  $B$  が成立しているとき条件  $A$  が常に成立していると仮定する. このとき, 条件  $A$  のもとで条件  $B$  が成立する確率 (条件付き確率) は, 条件  $B$  が成立する確率を条件  $A$  が確率で割ったものと定義される. このように条件付き確率は確率の商で定義される. だから, 確率の商が  $n \rightarrow \infty$  でどのように振る舞うかを確認できれば, 条件付き確率がどのように振る舞うかがわかる. 上の議論ではこの考え方を使った.

## 1.5 二項分布の場合の計算例

$r = 2, q_1 = q, q_2 = 1 - q$  の「コイン投げ」(もしくは「丁半博打」) の場合を考える. この場合に多項分布は二項分布になる. このとき,  $p_1 = p, p_2 = 1 - p$  とおくと, Kullback-Leibler 情報量は次のように表わされる:

$$D(p||q) = p \log \frac{p}{q} + (1 - p) \log \frac{1 - p}{1 - q}.$$

これは  $p = q$  で最小値 0 になり,  $p$  が  $q$  から離れれば離れるほど大きくなる. Kullback-Leibler 情報量は分布の経験的な生じ難さを表わす量なので  $q$  から遠い  $p$  ほど経験的に生じ難くなる. しかも  $p$  が経験的に生じる確率は  $n \rightarrow \infty$  で  $\exp(-nD(p||q) + O(\log n))$  と振る舞う. ゆえに, 複数の  $p$  の生じる確率を比較すると,  $D(p||q)$  が相対的に大きな  $p$  が生じる確率は  $n \rightarrow \infty$  で比の意味で相対的に 0 に近づく. 以上を踏まえた上で次の問題について考えよう.

**問題**  $n$  は非常に大きいと仮定する.  $n$  回のコイン投げの結果表が出た割合が  $a$  以上になったとする. このとき表の割合はどの程度になるだろうか?

大数の法則より,  $n \rightarrow \infty$  で表の割合は  $q$  に近づく. ゆえに  $0 \leq a < q$  のとき, 表の割合が  $a$  以上であるという条件は  $n \rightarrow \infty$  で常に実現することになる. だから,  $0 \leq a < q$  のとき, 表の割合が  $a$  以上の場合に制限しても,  $n$  が大きければ表の割合はほぼ  $q$  に等しくなっていると考えられる.

問題は  $q < a \leq 1$  の場合である. そのとき,  $n$  が大きくなればなるほど, 表の割合が  $a$  以上になる確率は 0 に近づく. 上の問題は表の割合が  $a$  以上になる場合に制限したときに表の割合がほぼ  $p$  になる確率 (条件付き確率) がどのように振る舞うかという問題になる. この場合には上で計算した Kullback-Leibler 情報量が役に立つ.  $p \geq a$  という条件のもとでの  $D(p||q)$  の最小値は  $p = a$  で実現される. ゆえに条件付き大数の法則より,  $n \rightarrow \infty$  で経験分布は  $p = a$  に近づく.  $q < a \leq 1$  のとき, 表の割合が  $a$  以上の場合に制限すると,  $n$  が大きければ表の割合はほぼ  $a$  に等しくなっていると考えられる.

以上の結果から以下の公式が成立していることもわかる:

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log \sum_{k/n \geq a} \binom{n}{k} q^k (1 - q)^{n-k} = - \inf_{p \geq a} D(p||q) = \begin{cases} -D(q||q) = 0 & (0 \leq a \leq q), \\ -D(a||q) & (q < a \leq 1). \end{cases}$$

対数を使わない形式でこの公式を書き下すと,

$$\sum_{k/n \geq a} \binom{n}{k} q^k (1 - q)^{n-k} = \exp \left( -n \inf_{p \geq a} D(p||q) + o(n) \right).$$

左辺は表の割合が  $a$  以上になる確率である.  $n \rightarrow \infty$  のとき確率には  $D(p||q)$  が最小になる分布だけが強く効いて来る.

## 1.6 max-plus 代数への極限や Laplace の方法との関係

実数または  $-\infty$  の  $a, b$  に対して演算

$$(a, b) \mapsto \max\{a, b\}, \quad (a, b) \mapsto a + b$$

を考えたもの(半環 (semiring), 半体 (semifield) と呼ばれている)を **max-plus 代数**と呼ぶ。(max-plus 代数は超離散化や **tropical mathematics** や各種正值性を扱う問題などに登場する重要な“代数”である。体は加減剰余が自由にできる“代数”のことであるが、半体は加乗除は自由にできるが引算は自由にできない“代数”のことである。引算が自由にできなくても意味のある面白い数学を作れる。)

大雑把には、 $\max$  は  $0$  以上の実数の足算に対応しており、 $+$  は掛算に対応していて、 $-\infty$  は足算の単位元  $0$  に対応している。その対応は  $\log$  を取って極限を取ることによって与えられる。すなわち、次の公式が成立している:

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log(e^{na} + e^{nb}) = \max\{a, b\}, \quad \lim_{n \rightarrow \infty} \frac{1}{n} \log(e^{na} e^{nb}) = a + b.$$

後者は自明である。前者の公式は次のようにして確かめられる。 $a \geq b$  と仮定すると、 $b - a \leq 0$  となるので、 $e^{n(b-a)}$  は有界になり、

$$\frac{1}{n} \log(e^{an} + e^{nb}) = \frac{1}{n} \log(e^{na} (1 + e^{n(b-a)})) = a + \frac{1}{n} \log(1 + e^{n(b-a)}) \rightarrow a \quad (n \rightarrow \infty)$$

となる。これで前者の公式も示された。

より一般に次が成立している:

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log \sum_{i=1}^r \exp(na_i + O(\log n)) = \max\{a_1, \dots, a_r\}.$$

このように  $\exp(na_i + O(\log n))$  のように振る舞う量の和の対数の  $1/n$  倍では  $n \rightarrow \infty$  のとき最大の  $a_i$  の部分のみが効いて来る。対数を使わない方の公式を書き下すと、

$$\sum_{i=1}^r \exp(na_i + O(\log n)) = \exp(n \max\{a_1, \dots, a_r\} + o(n)) \quad (n \rightarrow \infty).$$

これは積分の場合の Laplace の方法の類似であるとみなされる。

積分の場合は次の通り。適切な設定のもとで次が成立している:

$$\int_{\alpha}^{\beta} \exp\left(-nf(x) + O(\log n)\right) dx = \exp\left(-n \inf_{\alpha \leq x \leq \beta} f(x) + o(n)\right) \quad (n \rightarrow \infty).$$

$f(x)$  が  $\alpha < x = x_0 < \beta$  で一意的な最小値を持ち、 $f''(x_0) > 0$  ならば、

$$\int_{\alpha}^{\beta} e^{-nf(x)} g(x) dx = e^{-nf(x_0)} g(x_0) \sqrt{\frac{2\pi}{nf''(x_0)}} (1 + o(1)) \quad (n \rightarrow \infty).$$

このような漸近挙動の計算の仕方は **Laplace の方法**と呼ばれている。



## 1.7 区分求積法による高校レベルの計算で KL 情報量を出す方法

多項分布の  $n \rightarrow \infty$  での漸近挙動を以下のようにして, 区分求積法を使った高校数学っぽい方法で調べることができる.

$q_i \geq 0, \sum_{i=1}^r q_i = 1$  とし, 非負の整数  $a, b_i$  は  $\sum_{i=1}^r b_i = a$  をみたしているとし,

$$p_i = \frac{b_i}{a} = \frac{Nb_i}{Na}$$

とおく. このとき

$$\lim_{N \rightarrow \infty} \frac{1}{Na} \log \left( \frac{(Na)!}{(Nb_1)! \cdots (Nb_r)!} q_1^{Nb_1} \cdots q_r^{Nb_r} \right) = - \sum_{i=1}^r p_i \log \frac{p_i}{q_i}. \quad (*)$$

この右辺は相対エントロピー (Kullback-Leibler 情報量の  $-1$  倍) である. すなわち

$$\lim_{N \rightarrow \infty} \left( \frac{(Na)!}{(Nb_1)! \cdots (Nb_r)!} q_1^{Nb_1} \cdots q_r^{Nb_r} \right)^{1/(Na)} = \frac{1}{(p_1/q_1)^{p_1} \cdots (p_r/q_r)^{p_r}}.$$

区分求積法でこれを証明してみよう. 公式 (\*) を示せばよい.  $N \rightarrow \infty$  のとき

$$\begin{aligned} & \frac{1}{Na} \log \left( \frac{(Na)!}{(Nb_1)! \cdots (Nb_r)!} q_1^{Nb_1} \cdots q_r^{Nb_r} \right) \\ &= \frac{1}{Na} \left( \sum_{k=1}^{Na} \log k - \sum_{i=1}^r \sum_{k=1}^{Nb_i} \log k + \sum_{i=1}^r Nb_i \log q_i \right) \\ &= \frac{1}{Na} \left( \sum_{k=1}^{Na} \log \frac{k}{Na} - \sum_{i=1}^r \sum_{k=1}^{Nb_i} \log \frac{k}{Na} + \sum_{i=1}^r Nb_i \log q_i \right) \\ &= \frac{1}{Na} \sum_{k=1}^{Na} \log \frac{k}{Na} - \sum_{i=1}^r \frac{1}{Na} \sum_{k=1}^{Nb_i} \log \frac{k}{Na} + \sum_{i=1}^r p_i \log q_i \\ &\rightarrow \int_0^1 \log x \, dx - \sum_{i=1}^r \int_0^{p_i} \log x \, dx + \sum_{i=1}^r p_i \log q_i \\ &= [x \log x - x]_0^1 - \sum_{i=1}^r [x \log x - x]_0^{p_i} + \sum_{i=1}^r p_i \log q_i = - \sum_{i=1}^r p_i \log \frac{p_i}{q_i}. \end{aligned}$$

2つ目の等号で括弧の内側に  $Na \log(Na) - \sum_{i=1}^r Nb_i \log(Na) = 0$  を挿入した. それによって区分求積法を適用できる形に変形できた.

以上の結果は次が成立することを意味している:  $N \rightarrow \infty$  のとき

$$(Na \text{ 回の試行で経験分布が } p_i = b_i/a \text{ になる確率})^{1/(Na)} \rightarrow \frac{1}{(p_1/q_1)^{p_1} \cdots (p_r/q_r)^{p_r}}.$$

## 2 条件付き大数の法則から Boltzmann 因子へ

条件付き大数の法則 (最小 Kullback-Leibler 情報量の原理, 最大相対エントロピーの原理) から Boltzmann 因子で記述される分布が自然に得られることを説明したい.

## 2.1 問題の設定

母集団分布が  $q = (q_1, \dots, q_r)$  の多項分布の設定に戻る.

$n$  回の独立試行によって各々の  $i$  について状態  $i$  が生じた割合  $k_i/n$  がほぼ  $p_i$  に等しいとき, 経験分布がほぼ  $p = (p_1, \dots, p_r)$  に等しくなると言うことにする. その確率について

$$(n \text{ 回で経験分布がほぼ } p \text{ になる確率}) = \exp(-nD(p||q) + O(\log n)) \quad (n \rightarrow \infty)$$

が成立しているのであった.

次の問題を考える: 分布  $p = (p_1, \dots, p_r)$  に  $s$  個の条件

$$\sum_{i=1}^r f_{\nu,i} p_i \approx c_{\nu} \quad (\nu = 1, 2, \dots, s) \quad (*)$$

を課す. ただし,  $\mathbb{R}^r$  のベクトルたち  $(1, 1, \dots, 1), (f_{\nu,1}, \dots, f_{\nu,r})$  ( $\nu = 1, \dots, s$ ) は一次独立であると仮定しておく. 経験分布がこの条件を満たす分布  $p$  にほぼ等しい場合に制限したとき, 経験分布の確率分布は  $n \rightarrow \infty$  でどのように振る舞うか?

たとえば, 状態  $i$  のエネルギーが  $E_i$  の場合に

$$\sum_{i=1}^r E_i p_i \approx U$$

という条件 (すなわちエネルギーの経験的平均値がほぼ  $U$  に等しくなっているという条件) を課したとき, 経験分布が  $n \rightarrow \infty$  でどのように振る舞うか?

たとえば, サイコロを振って  $i$  の目が出たら, 賞金を  $E_i$  ペリカもらえるとき,

$$\sum_{i=1}^r E_i p_i \approx U$$

という条件 (すなわち 1 回あたりの賞金の経験的平均値がほぼ  $U$  ペリカに等しくなっているという条件) を課したとき, 経験分布が  $n \rightarrow \infty$  でどのように振る舞うか?

以上の 2 つの例では  $s = 1$  である. 複数の条件を課せば  $s > 1$  となる.

## 2.2 Boltzmann 因子の導出

条件 (\*) のもとでの経験分布の条件付き確率は  $n \rightarrow \infty$  で, 条件  $\sum_{i=1}^r p_i = 1$  と条件 (\*) のもとで Kullback-Leibler 情報量  $D(p||q) = \sum_{i=1}^r p_i \log(p_i/q_i)$  が最小値になる分布  $p = (p_1, \dots, p_r)$  に集中することになる.

その条件付き最小値問題を解くために Lagrange の未定乗数法を使おう. (Kullback-Leibler 情報量が  $p$  について下に狭義凸な関数であったことを思い出そう.) そのために

$$L = \sum_{i=1}^r p_i \log \frac{p_i}{q_i} + (\lambda - 1) \left( \sum_{i=1}^r p_i - 1 \right) + \sum_{\nu=1}^s \beta_{\nu} \left( \sum_{i=1}^r f_{\nu,i} p_i - c_{\nu} \right)$$

とおく. ここで  $\lambda - 1, \beta_{\nu}$  が未定乗数である. 未定乗数と  $p_i$  で  $L$  を偏微分した結果がすべて 0 になるという方程式

$$0 = \frac{\partial L}{\partial \lambda} = \sum_{i=1}^r p_i - 1, \quad (1)$$

$$0 = \frac{\partial L}{\partial \beta_\nu} = \sum_{i=1}^r f_{\nu,i} p_i - c_\nu \quad (\nu = 1, \dots, s), \quad (2)$$

$$0 = \frac{\partial L}{\partial p_i} = \log \frac{p_i}{q_i} + \lambda + \sum_{\nu=1}^s \beta_\nu f_{\nu,i} \quad (i = 1, \dots, r) \quad (3)$$

を解けばよい. (3) より,

$$p_i = \exp \left( -\lambda - \sum_{\nu=1}^s \beta_\nu f_{\nu,i} \right) q_i$$

これを (1) に代入すると,

$$Z := e^\lambda = \sum_{i=1}^r e^{-\sum_{\nu=1}^s \beta_\nu f_{\nu,i}} q_i, \quad p_i = \frac{1}{Z} e^{-\sum_{\nu=1}^s \beta_\nu f_{\nu,i}} q_i \quad (4)$$

となることがわかる. この  $Z$  は分配函数と呼ばれる. このように  $p_i$  と  $Z = e^\lambda$  は  $\beta_\nu$  たちの函数になっている.  $\beta_\nu$  たちは (4) を (2) に代入することによって決定される.  $\exp(-\sum_{\nu=1}^s \beta_\nu f_{\nu,i})$  を **Boltzmann 因子** と呼ぶことにする. Boltzmann 因子は母集団分布  $q_i$  と条件付きの経験分布  $p_i$  がどれだけ異なるかを記述している. このようにして求められた分布  $p_i$  をカノニカル分布と呼ぶことにする.

条件 (\*) が成立している場合に制限した場合の経験分布は,  $n \rightarrow \infty$  で以上で求めた分布  $p = (p_1, \dots, p_r)$  に近づく (条件付き大数の法則より).  $n$  が巨大ならば経験分布はカノニカル分布の形をしているとしてよい.

たとえば  $s = 1$ ,  $f_{1,i} = E_i$ ,  $c_1 = U$ ,  $\beta_1 = \beta$  のとき,

$$p_i = \frac{1}{Z} e^{-\beta E_i} q_i, \quad Z = \sum_{i=1}^r e^{-\beta E_i} q_i, \quad -\frac{\partial \log Z}{\partial \beta} = \frac{1}{Z} \sum_{i=1}^r E_i e^{-\beta E_i} q_i = U.$$

これらの公式は  $q_i$  たちが互いにすべて等しい場合には統計力学における Boltzmann 因子を用いた確率分布の記述に一致している.

カノニカル分布に対する相対エントロピー  $S(p||q) = -D(p||q) = -\sum_{i=1}^r p_i \log(p_i/q_i)$  の別の表示を求めよう:  $\log(p_i/q_i) = -\sum_{\nu=1}^s \beta_\nu f_{\nu,i} - \log Z$ ,  $\sum_{i=1}^r p_i = 1$ ,  $\sum_{i=1}^r f_{\nu,i} p_i = c_\nu$  なので

$$S(p||q) = \sum_{\nu=1}^s \beta_\nu c_\nu + \log Z.$$

たとえば  $s = 1$ ,  $f_{1,i} = E_i$ ,  $c_1 = U$ ,  $\beta_1 = \beta$  のとき

$$S(p||q) = \beta U + \log Z.$$

自由エネルギー  $F$  を  $F = -\beta^{-1} \log Z$  と定義すると,

$$S(p||q) = \beta(U - F)$$

この公式は, Boltzmann 定数が含まれていない点を除けば, 統計力学を知っている人達にとってお馴染みの公式だろう<sup>3</sup>.

<sup>3</sup>Boltzmann 定数が 1 になる単位系を採用することもできる.

### 2.3 母分布が連続型の場合から連続型の指数型分布族が得られること

母集団分布が確率密度関数  $q(x)$  で与えられている場合を考えよう. この場合には  $n$  回の独立試行の結果得られる経験分布の確率密度関数がほぼ  $p(x)$  になる確率の対数の  $1/n$  倍は  $n \rightarrow \infty$  で

$$S(p||q) = -D(p||q) = - \int p(x) \log \frac{p(x)}{q(x)} dx$$

に近付くと考えられる. 分布  $p(x)$  に以下の条件を課す:

$$\int f_\nu(x) p(x) dx = c_\nu \quad (\nu = 1, \dots, s).$$

前節と同様にして, この条件のもとで  $D(p||q)$  を最小にする確率密度関数  $p(x)$  を求めると次のようになることがわかる:

$$\begin{aligned} p(x) &= \frac{1}{Z} e^{-\sum_{\nu=1}^s \beta_\nu f_\nu(x)} q(x), \\ Z &= \int e^{-\sum_{\nu=1}^s \beta_\nu f_\nu(x)} q(x) dx, \\ -\frac{\partial \log Z}{\partial \beta_\nu} &= \frac{1}{Z} \int f_\nu(x) e^{-\sum_{\nu=1}^s \beta_\nu f_\nu(x)} q(x) dx = c_\nu. \end{aligned}$$

このようにな形の連続型確率分布の族を連続型の指数型分布族と呼ぶ. 積分が和の場合には離散型の指数型分布族と呼ばれる.

たとえば以下の確率分布はすべて指数型分布族に含まれている.

二項分布:  $0 < \theta < 1$  のとき,  $-\beta = \log \theta - \log(1 - \theta)$  とおくと,  $k = 0, 1, \dots, n$  について

$$p_k = \binom{n}{k} \theta^k (1 - \theta)^{n-k} = \frac{e^{-\beta k} q_k}{Z}, \quad q_k = \binom{n}{k} \frac{1}{2^n}, \quad Z = \frac{1}{2^n (1 - \theta)^n}.$$

この場合と条件付き大数の法則の関係については例 4.3 も参照せよ.

多項分布:  $\theta_i \geq 0$ ,  $\theta_r > 0$ ,  $\sum_{i=1}^r \theta_i = 1$  であるとし,  $-\beta_i = \log \theta_i - \log \theta_r$  とおくと,  $k_1 + \dots + k_r = n$  のとき

$$\begin{aligned} p_{k_1, \dots, k_r} &= \frac{n!}{k_1! \dots k_r!} \theta_1^{k_1} \dots \theta_r^{k_r} = \frac{e^{-\sum_{i=1}^{r-1} \beta_i k_i} q_{k_1, \dots, k_r}}{Z}, \\ q_{k_1, \dots, k_r} &= \frac{n!}{k_1! \dots k_r!} \frac{1}{r^n}, \quad Z = \frac{1}{r^n \theta_r^n} \end{aligned}$$

正規分布:

$$p(x) = \frac{e^{-(x-\mu)^2/(2\sigma^2)}}{\sqrt{2\pi}} = \frac{e^{-(1/(2\sigma^2))x^2 + (\mu/\sigma^2)x}}{Z}, \quad Z = e^{\mu^2/(2\sigma^2)} \sqrt{2\pi\sigma^2}.$$

$\mu = 0$ ,  $\sigma = 1$  の場合については第 2.4 節も参照して欲しい. 正規分布の確率密度関数  $p(x)$  は平均  $\mu$  と分散  $\sigma^2$  を指定したときに, すなわち  $\int_{\mathbb{R}} p(x) dx = 1$ ,

$$\int_{\mathbb{R}} x p(x) dx = \mu, \quad \int_{\mathbb{R}} x^2 p(x) dx = \sigma^2 + \mu^2$$

という条件のもとで、エントロピー

$$S(p) = - \int_{\mathbb{R}} p(x) \log p(x) dx$$

が最大になる  $p(x)$  として特徴付けられる.

**Gamma 分布:**  $x > 0$  において

$$p(x) = \frac{e^{-x/\tau} x^{\alpha-1}}{\tau^\alpha \Gamma(\alpha)} = \frac{e^{-x/\tau + (\alpha-1) \log x}}{Z}, \quad Z = \tau^\alpha \Gamma(\alpha).$$

Gamma 分布の確率密度関数  $p(x)$  は  $\int_{\mathbb{R}} p(x) dx = 1$ ,

$$\int_0^\infty x p(x) dx = c_1, \quad \int_0^\infty (\log x) p(x) dx = c_2$$

という条件のもとでエントロピー

$$S(p(x)) = - \int_0^\infty p(x) \log p(x) dx$$

が最大になる  $p(x)$  として特徴付けられる. 以下も同様である.

**第二種 Beta 分布:**  $x > 0$  において

$$p(x) = \frac{1}{B(\alpha, \beta)} \frac{x^{\alpha-1}}{(1+x)^{\alpha+\beta}} = \frac{e^{(\alpha-1) \log x - (\alpha+\beta) \log(1+x)}}{Z}, \quad Z = B(\alpha, \beta).$$

自由度  $n$  の  $t$  分布を  $1/\sqrt{n}$  でスケールしたもの: 自由度  $n$  の  $t$  分布の確率密度は

$$\rho(t) dt = \frac{1}{c_n} \left( 1 + \frac{t^2}{n} \right)^{-(n+1)/2} dt, \quad c_n = \sqrt{n} B(1/2, n/2) = \frac{\sqrt{n\pi} \Gamma(n/2)}{\Gamma((n+1)/2)}$$

であった.  $p(x) dx = \rho(\sqrt{n} x) d(\sqrt{n} x)$ ,  $\beta = (n+1)/2$  とおくと

$$p(x) = \frac{1}{Z} \frac{1}{(1+x^2)^{(n+1)/2}} = \frac{e^{-\beta \log(1+x^2)}}{Z}, \quad Z = B(1/2, n/2).$$

**第一種 Beta 分布:**  $0 < x < 1$  について

$$p(x) = \frac{x^{\alpha-1} (1-x)^{\beta-1}}{B(\alpha, \beta)} = \frac{e^{(\alpha-1) \log x + (\beta-1) \log(1-x)}}{Z}, \quad Z = B(\alpha, \beta).$$

**Poisson 分布:**

$$p_k = \frac{e^{-\lambda} \lambda^k}{k!} = \frac{e^{-(\log \lambda)k} q_k}{Z}, \quad q_k = \frac{e}{k!}, \quad Z = e^{\lambda+1}.$$

## 2.4 標準正規分布の導出例

例として  $s = 1$ ,  $f_1(x) = x^2$ ,  $c_1 = 1$ ,  $q(x) = 1$  の場合にどうなるかを計算してみよう<sup>4</sup>. この場合に上の結果は,  $n$  回の独立試行の結果得られた  $x^2$  の経験的期待値  $(x_1^2 + \dots + x_n^2)/n$  について

$$\frac{x_1^2 + \dots + x_n^2}{n} = 1$$

という条件を課したとき,  $n \rightarrow \infty$  で  $x$  の経験的分布がどうなるかを求めることに等しい. 上の公式を使うと

$$p(x) = \frac{1}{Z} e^{-\beta x^2}, \quad Z = \int_{\mathbb{R}} e^{-\beta x^2} dx = \sqrt{\pi} \beta^{-1/2}, \quad -\frac{\partial \log Z}{\partial \beta} = \frac{1}{2\beta} = 1.$$

ゆえに  $\beta = 1/2$ ,  $Z = \sqrt{2\pi}$ ,  $p(x) = e^{-x^2/2}/\sqrt{2\pi}$  となる. すなわち  $n \rightarrow \infty$  で得られる分布は標準正規分布になる.

この結果は  $\mathbb{R}^n$  内の半径の 2 乗が  $n$  の原点を中心とする  $n-1$  次元球面上の一様分布の 1 次元部分空間への射影が  $n \rightarrow \infty$  で標準正規分布に収束することを意味している. すなわち次の公式が成立している:

$$\lim_{n \rightarrow \infty} \int_{\sqrt{n} S^{n-1}} f(x_1) \mu_n(dx) = \int_{\mathbb{R}} f(x) \frac{e^{-x^2/2}}{\sqrt{2\pi}} dx.$$

ここで  $\sqrt{n} S^{n-1}$  は原点を中心とする半径  $\sqrt{n}$  の  $n-1$  次元球面

$$\{(x_1, \dots, x_n) \in \mathbb{R}^n \mid x_1^2 + \dots + x_n^2 = n\}$$

を表わし,  $\mu_n$  はその上の一様確率分布であり,  $f(x_1)$  の  $x_1$  は球面上の点  $(x_1, \dots, x_n)$  の射影である. この極限の公式は通常の変数の微積分の計算で直接に確認できる<sup>5</sup>.

以上の計算例を見れば, 指数型分布族に属する他の確率分布がどのような条件を課したときに自然に現われるかも理解できると思う.

## 3 多項分布の場合の Sanov の定理

多項分布の場合の Sanov の定理の主張を明確に述べて厳密に証明しておくことにする. Stirling の公式さえ使わない易しい証明を紹介する. この節の証明はブログ記事 [10] で解説されている証明と本質的に同じものである. そのブログには参考になる解説がたくさんある.

### 3.1 Sanov の定理の主張

有限集合  $\{1, 2, \dots, r\}$  上の確率分布全体の集合を  $\mathcal{P}$  と書く:

$$\mathcal{P} = \{p = (p_1, \dots, p_r) \in \mathbb{R}^r \mid p_1, \dots, p_r \geq 0, p_1 + \dots + p_r = 1\}.$$

<sup>4</sup> $q(x) = 1$  なのでこの場合に  $q(x)$  は確率密度函数にならない. しかし, 以下の計算の結論は正しい.

<sup>5</sup>次の雑多なノートの Maxwell-Boltzmann 則の節にその直接的な計算が書いてある.

$\mathcal{P}$  は  $r-1$  次元の閉単体である. たとえば  $r=3$  のとき  $\mathcal{P}$  は正三角形になる.

確率分布  $q = (q_1, \dots, q_r) \in \mathcal{P}$  を任意に取って固定する. 確率変数  $X_1, X_2, \dots$  は集合  $\{1, 2, \dots, r\}$  に値を持つ確率変数列であり, 独立で同分布  $q = (q_1, \dots, q_r)$  にしたがっていると仮定する.  $q = (q_1, \dots, q_r)$  を母集団分布と呼ぶ.

集合  $A$  に対してその元の個数を  $\#A$  と書き, 条件  $A$  が満たされる確率を  $P(A)$  と書くことにする. (後で条件  $A$  のもとでの  $B$  の条件付き確率を  $P(B|A)$  と書く.)

各々の  $i = 1, \dots, r$  に対して  $X_1, \dots, X_n$  に含まれる  $i$  の個数が  $k_i$  個になる確率は

$$P\left(\#\{k = 1, 2, \dots, n \mid X_k = i\} = k_i \text{ for each } i = 1, \dots, r\right) = \frac{n!}{k_1! \cdots k_r!} q_1^{k_1} \cdots q_r^{k_r}$$

となる. 可能な  $(k_1, \dots, k_r)$  の組合せは  $k_i = 0, 1, \dots, n, k_1 + \cdots + k_r = n$  を満たしていなければいけない. このような  $(k_1, \dots, k_r)$  に対する  $(k_1/n, \dots, k_r/n)$  全体の集合を  $\mathcal{P}_n \subset \mathcal{P}$  と書くことにする:

$$\mathcal{P}_n = \left\{ \left( \frac{k_1}{n}, \dots, \frac{k_r}{n} \right) \mid k_i = 0, 1, \dots, n, k_1 + \cdots + k_r = n \right\}.$$

このとき  $\mathcal{P}_n$  の元の個数は  $(n+1)^r$  以下になる. ( $\#\mathcal{P}_n \leq (n+1)^r$  を後で自由に利用する.)  $X_1, \dots, X_n$  に対応する  $\mathcal{P}_n$  の元  $P_n = (k_1/n, \dots, k_r/n)$  を経験分布と呼ぶ. 経験分布  $P_n$  は  $\mathcal{P}_n$  に値を持つ確率変数である.

確率分布の組  $(p, q) \in \mathcal{P}^2$  の関数  $D(p||q)$  を次のように定める:

$$D(p||q) = \sum_{i=1}^r p_i \log \frac{p_i}{q_i}.$$

$p_i$  や  $q_i$  が 0 になる場合には  $0 \log 0 = 0, -\log 0 = \infty$  という約束のもとで値を定めておく.  $D(p||q)$  を Kullback-Leibler 情報量もしくは Kullback-Leibler ダイバージェンスと呼ぶ.

**定理 3.1** (Sanov). 以上の設定のもとで以下が成立している<sup>6</sup>:

(1)  $A$  が  $\mathcal{P}$  の開部分集合ならば

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \log P(P_n \in A) \geq - \inf_{p \in A} D(p||q).$$

(2)  $A$  が  $\mathcal{P}$  の部分集合ならば<sup>7</sup>

$$\limsup_{n \rightarrow \infty} \frac{1}{n} \log P(P_n \in A) \leq - \inf_{p \in A} D(p||q).$$

(3)  $\mathcal{P}$  の部分集合  $A$  の開核の閉包が  $A$  を含むならば

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log P(P_n \in A) = - \inf_{p \in A} D(p||q).$$

<sup>6</sup> $\liminf, \limsup$  について第 8 節に簡単な解説を書いていた.

<sup>7</sup>我々が扱っている場合には  $A$  は任意の部分集合であっても問題ない. しかし, 無限次元の場合には  $A$  は閉部分集合だと仮定することが重要になるらしい.

このように経験分布の  $n \rightarrow \infty$  での漸近挙動は Kullback-Leibler 情報量  $D(p||q)$  の inf で記述される.  $\square$

例 3.2 (二項分布の場合).  $r = 2$  とし,  $q_1 = q, q_2 = 1 - q, p_1 = p, p_2 = 1 - p$  とおくと,

$$D(p||q) = p \log \frac{p}{q} + (1 - p) \log \frac{1 - p}{1 - q}.$$

これは  $p = q$  のとき最低値 0 になり,  $p$  が  $q$  から離れるとこの値は減少する.

$0 \leq a < b \leq 1$  であるとし,  $A = (a, b) = (a \text{ から } b \text{ までの开区間})$  とおく. このとき

$$P(P_n \in A) = \sum_{a < k/n < b} \binom{n}{k} q^k (1 - q)^{n-k}$$

なので

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log \sum_{a < k/n < b} \binom{n}{k} q^k (1 - q)^{n-k} = - \inf_{a < p < b} D(p||q) = \begin{cases} -D(b||q) & (b < q), \\ -D(q||q) = 0 & (a \leq q \leq b), \\ -D(a||q) & (q < a) \end{cases}$$

となる. これが Sanov の定理の非自明な応用の最も簡単な場合である.  $\square$

### 3.2 Sanov の定理の証明の準備

次の補題が後で Stirling の公式の代わりに使われる.

補題 3.3. 非負の整数  $k, l$  に対して

$$\frac{l!}{k!} \geq k^{l-k}.$$

証明.  $l \geq k$  のとき

$$\frac{l!}{k!} = (k + 1)(k + 2) \cdots l \geq k^{l-k}.$$

$l \leq k$  のとき

$$\frac{l!}{k!} = \frac{1}{(l + 1)(l + 2) \cdots k} \geq \frac{1}{k^{k-l}} = k^{l-k}.$$

これで示すべきことが示された.  $\square$

次の補題が証明できれば Sanov の定理の証明は易しい. 次の補題の証明には Stirling の公式を使わない.

補題 3.4. 任意の  $p \in \mathcal{P}_n$  に対して

$$\frac{1}{(n + 1)^r} e^{-nD(p||q)} \leq P(P_n = p) \leq e^{-nD(p||q)}.$$



証明.  $p = (p_1, \dots, p_r) = (k_1/n, \dots, k_r/n) \in \mathcal{P}_n$  のとき,

$$-nD(p||q) = -\sum_{i=1}^r k_i \log p_i + \sum_{i=1}^r k_i \log q_i,$$

$$e^{-nD(p||q)} = \frac{q_1^{k_1} \cdots q_r^{k_r}}{p_1^{k_1} \cdots p_r^{k_r}}, \quad P(P_n = p) = \frac{n!}{k_1! \cdots k_r!} q_1^{k_1} \cdots q_r^{k_r}.$$

ゆえに, この補題の結論は次と同値である:

$$\frac{1}{(n+1)^r} \leq \frac{n!}{k_1! \cdots k_r!} p_1^{k_1} \cdots p_r^{k_r} \leq 1.$$

上からの評価の方 (右側の不等式) は多項分布の知識より自明である. (多項分布における確率が 1 以下であることを意味しているに過ぎない.) 以下で下からの評価 (左側の不等式) を証明しよう.

$l_i = 0, 1, \dots, n, l_1 + \cdots + l_r = n$  と仮定する. このとき,  $p_i = k_i/n$  なので

$$\frac{n!}{l_1! \cdots l_r!} p_1^{l_1} \cdots p_r^{l_r} \leq \frac{n!}{k_1! \cdots k_r!} p_1^{k_1} \cdots p_r^{k_r} \quad (*)$$

が成立しているはずである. なぜならば多項分布において確率が最大になるのは経験分布 (今の場合は  $l_i/n$ ) が母集団分布 (今の場合は  $p_i = k_i/n$ ) に等しくなるときだからである. 実際, 補題 3.3 より,

$$\frac{\text{(右辺)}}{\text{(左辺)}} = \frac{l_1!}{k_1!} \cdots \frac{l_r!}{k_r!} \cdot k_1^{k_1-l_1} \cdots k_r^{k_r-l_r} \geq k_1^{l_1-k_1} \cdots k_r^{l_r-k_r} \cdot k_1^{k_1-l_1} \cdots k_r^{k_r-l_r} = 1.$$

これで (\*) が証明された. ゆえに, 多項定理より

$$1 = \sum_{l_1+\cdots+l_r=n} \frac{n!}{l_1! \cdots l_r!} p_1^{l_1} \cdots p_r^{l_r} \leq (n+1)^r \frac{n!}{k_1! \cdots k_r!} p_1^{k_1} \cdots p_r^{k_r}$$

両辺を  $(n+1)^r$  で割れば下からの評価が得られる. □

注意 3.5. 以上の結果の一部分は以下のように拡張される.

$f(n)$  は  $f(0) = 0$  を満たす非負の整数  $n$  の単調増加関数であるとし,

$$f(n)! = f(1)f(2)\cdots f(n), \quad f(0)! = 1$$

と定める. これを  $f$  階乗と呼ぶことにする. このとき非負の整数  $k, l$  に対して,

$$\frac{f(l)!}{f(k)!} \geq f(k)^{l-k}.$$

実際,  $l \geq k$  のとき

$$\frac{f(l)!}{f(k)!} = f(k+1)f(k+2)\cdots f(l) \geq f(k)^{l-k}$$

となり,  $l \leq k$  のとき

$$\frac{l!}{k!} = \frac{1}{f(l+1)f(l+2)\cdots f(k)} \geq \frac{1}{f(k)^{k-l}} = f(k)^{l-k}.$$

$k_i \in \mathbb{Z}_{\geq 0}$   $p_i = f(k_i)/f(n)$  とおくと,  $l_i \in \mathbb{Z}_{\geq 0}$  のとき,

$$\frac{f(n)!}{f(l_1)! \cdots f(l_r)!} p_1^{l_1} \cdots p_r^{l_r} \leq \frac{f(n)!}{f(l_1)! \cdots k_r!} p_1^{k_1} \cdots p_r^{k_r}.$$

なぜならば

$$\begin{aligned} \frac{(\text{右辺})}{(\text{左辺})} &= \frac{f(l_1)! \cdots f(l_r)!}{f(k_1)! \cdots f(k_r)!} \cdot f(k_1)^{k_1-l_1} \cdots f(k_r)^{k_r-l_r} \\ &\geq f(k_1)^{l_1-k_1} \cdots f(k_r)^{l_r-k_r} \cdot f(k_1)^{k_1-l_1} \cdots f(k_r)^{k_r-l_r} = 1. \end{aligned}$$

$f(n)$  が特別な場合にはこの類似をさらにたどることができると思われる.  $\square$

### 3.3 Sanov の定理の証明

**定理 3.1** の証明. 下からの評価 (1) を示そう.  $A$  は有限集合  $\{1, 2, \dots, r\}$  上の確率分布全体の空間  $\mathcal{P}$  (これは  $r-1$  次元単体になる) の開部分集合であるとする.  $\bigcup_{n=1}^{\infty} \mathcal{P}_n = \mathcal{P} \cap \mathbb{Q}^r$  は  $\mathcal{P}$  の中で稠密である.  $A$  は  $\mathcal{P}$  の開部分集合なので分布列  $p_n \in \mathcal{P}_n \cap A$  で

$$\lim_{n \rightarrow \infty} D(p_n \| q) = \inf_{p \in A} D(p \| q)$$

をみたすものを取れる. 以上の状況で

$$P(P_n \in A) = \sum_{p \in \mathcal{P}_n \cap A} P(P_n = p) \geq P(P_n = p_n) \geq \frac{1}{(n+1)^r} e^{-nD(p_n \| q)}.$$

最後の不等号で補題 3.4 の下からの評価を使った. これより

$$\frac{1}{n} \log P(P_n \in A) \geq -D(p_n \| q) - \frac{r}{n} \log(n+1)$$

となることがわかる. したがって,  $n \rightarrow \infty$  とすることによって,

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \log P(P_n \in A) \geq -\inf_{p \in A} D(p \| q).$$

これで (1) が証明された.

上からの評価 (2) を示そう.  $A$  は有限集合  $\{1, 2, \dots, r\}$  上の確率分布全体の空間  $\mathcal{P}$  の任意の部分集合であるとする. このとき

$$P(P_n \in A) = \sum_{p \in \mathcal{P}_n \cap A} P(P_n = p) \leq \sum_{p \in \mathcal{P}_n \cap A} e^{-nD(p \| q)} \leq (n+1)^r e^{-n \inf_{p \in A} D(p \| q)}.$$

最初の不等号で補題 3.4 の上からの評価を使った. これより

$$\frac{1}{n} \log P(P_n \in A) \leq -\inf_{p \in A} D(p \| q) + \frac{r}{n} \log(n+1)$$

となることがわかる. したがって,  $n \rightarrow \infty$  とすることによって,

$$\limsup_{n \rightarrow \infty} \frac{1}{n} \log P(P_n \in A) \leq -\inf_{p \in A} D(p \| q).$$

これで (2) が証明された。

(3) を示そう。  $A$  の開核を  $B$  と書き、  $B$  の閉包を  $C$  と書き、  $A \subset C$  と仮定する。  
 $B \subset A \subset C$  より  $-\inf_{p \in B} D(p||q) \leq -\inf_{p \in A} D(p||q) \leq -\inf_{p \in C} D(p||q)$ 。  $C$  が  $B$  の閉包であること  $D(p||q)$  が  $p$  の連続関数であることより、  $-\inf_{p \in C} D(p||q) = -\inf_{p \in B} D(p||q)$ 。  
ゆえに  $-\inf_{p \in B} D(p||q) = -\inf_{p \in A} D(p||q) = -\inf_{p \in C} D(p||q)$ 。 したがって (1), (2) から (3) が導かれる。

これで定理 3.1 が証明された。 □

**注意 3.6.** 以上の証明では階乗に関する Stirling の近似公式を使っていない。 証明で本質的に使った事柄は次の二つだけである。

(1) 上からの評価のために次の事実を使った:

$p_i \geq 0, p_1 + \dots + p_r = 1$  のとき

$$\frac{n!}{k_1! \dots k_r!} p_1^{k_1} \dots p_r^{k_r} \leq 1 \quad (k_i \in \mathbb{Z}_{\geq 0}, k_1 + \dots + k_r = n).$$

これは多項分布において「確率は 1 以下であること」を意味している。 それを意味する不等式は、左辺を  $k_i$  たちを動かして足し上げた結果が多項定理より 1 になること

$$\sum_{k_1 + \dots + k_r = n} \frac{n!}{k_1! \dots k_r!} p_1^{k_1} \dots p_r^{k_r} = (p_1 + \dots + p_r)^n = 1$$

から、ただちに得られる。

(2) 下からの評価のために次の事実を使った:

$k_i \in \mathbb{Z}_{\geq 0}, k_1 + \dots + k_r = n, p_i = k_i/n$  のとき、

$$\frac{n!}{l_1! \dots l_r!} p_1^{l_1} \dots p_r^{l_r} \leq \frac{n!}{k_1! \dots k_r!} p_1^{k_1} \dots p_r^{k_r} \quad (l_i \in \mathbb{Z}_{\geq 0}, l_1 + \dots + l_r = n)$$

これは多項分布において「確率が最大になるのは分布が母集団分布に等しくなるときであること」を意味している。 その不等式は次の易しい不等式 ( $k, l$  の大小関係によらずに成立している) からただちに得られる:

$$\frac{l!}{k!} \geq k^{l-k} \quad (k, l \in \mathbb{Z}_{\geq 0}).$$

実際、この不等式を使うと、  $p_i = k_i/n$  より

$$\frac{\text{(右辺)}}{\text{(左辺)}} = \frac{l_1!}{k_1!} \dots \frac{l_r!}{k_r!} \frac{k_1^{k_1}}{k_1^{l_1}} \dots \frac{k_r^{k_r}}{k_r^{l_r}} \geq k_1^{l_1-k_1} \dots k_r^{l_r-k_r} \cdot k_1^{k_1-l_1} \dots k_r^{k_r-l_r} = 1.$$

以上の 2 つの結果は多項分布について知っていれば当然知っているはずの事柄である。 たったそれだけの事実から多項分布版の Sanov の定理は証明されるのである。

補題 3.4 の証明を逆にたどって Kullback-Leibler 情報量が出て来るところまでの議論を繰り返そう。

$k_i \in \mathbb{Z}_{\geq 0}, k_1 + \dots + k_r = n, p_i = k_i/n$  と仮定する。 上の (2) を  $l_i$  達について足し上げることによって

$$1 = \sum_{l_1 + \dots + l_r = n} \frac{n!}{l_1! \dots l_r!} p_1^{l_1} \dots p_r^{l_r} \leq (n+1)^r \frac{n!}{k_1! \dots k_r!} p_1^{k_1} \dots p_r^{k_r}.$$

これらの両辺を  $(n+1)^r$  で割って得られる不等式と上の (1) を合わせると

$$\frac{1}{(n+1)^r} \leq \frac{n!}{k_1! \cdots k_r!} p_1^{k_1} \cdots p_r^{k_r} \leq 1$$

を得る.  $q_i \in \mathbb{Z}_{\geq 0}$ ,  $q_1 + \cdots + q_r = 1$  であるとし, この不等式全体を  $p_1^{k_1} \cdots p_r^{k_r}$  で割って,  $q_1^{k_1} \cdots q_r^{k_r}$  をかけると

$$\frac{1}{(n+1)^r} \frac{q_1^{k_1} \cdots q_r^{k_r}}{p_1^{k_1} \cdots p_r^{k_r}} \leq \frac{n!}{k_1! \cdots k_r!} q_1^{k_1} \cdots q_r^{k_r} \leq \frac{q_1^{k_1} \cdots q_r^{k_r}}{p_1^{k_1} \cdots p_r^{k_r}}.$$

$k_i = np_i$  より, この時点ですでに Kullback-Leibler 情報量

$$D(p||q) = \sum_{i=1}^r p_i \log \frac{p_i}{q_i}$$

が見えている:

$$\log \frac{q_1^{k_1} \cdots q_r^{k_r}}{p_1^{k_1} \cdots p_r^{k_r}} = \log \left( \left( \frac{q_1}{p_1} \right)^{p_1} \cdots \left( \frac{q_r}{p_r} \right)^{p_r} \right)^n = -nD(p||q).$$

したがって

$$\frac{1}{(n+1)^r} e^{-nD(p||q)} \leq \frac{n!}{k_1! \cdots k_r!} q_1^{k_1} \cdots q_r^{k_r} \leq e^{-nD(p||q)}.$$

この不等式が補題 3.4 の結論であった. そしてこの不等式を用いて多項分布の  $n \rightarrow \infty$  の様子を調べればただちに Sanov の定理 (定理 3.1) が得られるのであった.  $\square$

## 4 Sanov の定理を使ったカノニカル分布の導出

第 3 節の記号をそのまま引き継ぐ. たとえば  $\mathcal{P}$  は有限集合  $\{1, 2, \dots, r\}$  上の確率分布  $p = (p_1, \dots, p_r)$  全体の集合であるとし, 母集団分布  $q = (q_1, \dots, q_r) \in \mathcal{P}$  を任意に取って固定する.  $n$  回の独立試行の結果, 状態  $i$  が生じた回数を  $k_i$  と書くと, 状態  $i$  の生じた割合は  $k_i/n$  である. 経験分布  $P_n = (k_1/n, \dots, k_r/n)$  は  $\mathcal{P}$  に値を持つ確率変数になる<sup>8</sup>.

### 4.1 分配関数とエネルギーの期待値

$E = (E_1, \dots, E_r) \in \mathbb{R}^r$  であるとし,

$$E_1 = \cdots = E_a < E_{a+1} \leq \cdots \leq E_{r-b} < E_{r-b+1} = \cdots = E_r$$

かつ  $q_1, q_r > 0$  であると仮定しておく (あとで分配関数の対数凸性を保証するための仮定).  $E_i$  たちを状態  $i$  のエネルギーと呼ぶ<sup>9</sup>.  $\beta \in \mathbb{R}$  に対して分布  $p(\beta) = (p_1(\beta), \dots, p_r(\beta)) \in \mathcal{P}$  と関数  $Z(\beta)$  を

$$p_i(\beta) = \frac{e^{-\beta E_i} q_i}{Z(\beta)}, \quad Z(\beta) = \sum_{i=1}^r e^{-\beta E_i} q_i,$$

<sup>8</sup>サイコロの目のように試行ごとに値が確率的に変化する変数を確率変数と呼ぶ. 経験分布  $P_n$  の値は  $n$  回の独立試行をやり直すごとに確率的に変化するので,  $P_n$  は確率変数だとみなされる.

<sup>9</sup>ギャンブルが好きな人はエネルギーをサイコロで  $i$  の目が出たときにもらえる賞金だと思ってよい.

によって定める. さらに函数  $U(\beta) = \langle E \rangle_\beta$  を

$$U(\beta) = \langle E \rangle_\beta = \sum_{i=1}^r E_i p_i(\beta) = -\frac{\partial}{\partial \beta} \log Z(\beta)$$

と定める.  $\beta$  を逆温度と呼び,  $e^{-\beta E_i}$  を **Boltzmann** 因子と呼び,  $p(\beta)$  をカノニカル分布と呼び, 函数  $Z(\beta)$  を分配函数と呼び, 函数  $U(\beta)$  をエネルギーの期待値と呼ぶ.

$\log Z(\beta)$  は  $\beta$  に関する下に狭義凸な函数である. なぜならば

$$\left( \frac{\partial}{\partial \beta} \right)^2 \log Z(\beta) = \frac{Z''(\beta)Z(\beta) - Z'(\beta)^2}{Z(\beta)^2}$$

であり,  $a_i = e^{-\beta E_i} q_i \geq 0$  とおくと, 最初の方の仮定から  $a_1, a_r > 0$  かつ  $E_1 < E_r$  なので

$$\begin{aligned} Z''(\beta)Z(\beta) - Z'(\beta)^2 &= \sum_{i,j} E_i^2 a_i a_j - \sum_{i,j} E_i a_i E_j a_j \\ &= \frac{1}{2} \sum_{i,j} (E_i^2 + E_j^2) a_i a_j - \frac{1}{2} \sum_{i,j} 2E_i E_j a_i a_j = \frac{1}{2} \sum_{i,j} (E_i - E_j)^2 a_i a_j > 0 \end{aligned}$$

となり, ゆえに

$$\left( \frac{\partial}{\partial \beta} \right)^2 \log Z(\beta) > 0$$

となるからである. したがって, エネルギーの期待値

$$U(\beta) = -\frac{\partial}{\partial \beta} \log Z(\beta)$$

は  $\beta$  の狭義単調減少函数である.

次に  $U(\beta)$  の値の様子を調べよう. まず  $p(0) = q$  より

$$U(0) = \sum_{i=1}^r E_i q_i.$$

次に  $\beta \rightarrow \infty$  のとき

$$U(\beta) = \frac{\sum_i E_i e^{-\beta E_i} q_i}{\sum_i e^{-\beta E_i} q_i} = \frac{e^{-\beta E_1} \sum_i E_i e^{-\beta(E_i - E_1)} q_i}{e^{-\beta E_1} \sum_i e^{-\beta(E_i - E_1)} q_i} \rightarrow \frac{e^{-\beta E_1} \sum_{i=1}^a E_i q_i}{e^{-\beta E_1} \sum_{i=1}^a q_i} = E_1.$$

最後に  $\beta \rightarrow -\infty$  のとき

$$U(\beta) = \frac{\sum_i E_i e^{-\beta E_i} q_i}{\sum_i e^{-\beta E_i} q_i} = \frac{e^{-\beta E_r} \sum_i E_i e^{\beta(E_r - E_i)} q_i}{e^{-\beta E_r} \sum_i e^{\beta(E_r - E_i)} q_i} \rightarrow \frac{e^{-\beta E_r} \sum_{i=r-b+1}^r E_i q_i}{e^{-\beta E_r} \sum_{i=r-b+1}^r q_i} = E_r.$$

以上によって,  $E_r \geq U \geq E_1$  と  $-\infty \leq \beta \leq \infty$  は  $U = U(\beta)$  によって一対一に対応していることがわかる.

## 4.2 条件付き確率分布のカノニカル分布への収束

経験分布  $p = (p_1, \dots, p_r) \in \mathcal{P}$  について, 条件  $\sum_{i=1}^r E_i p_i \approx U(\beta)$  のもとで,  $n \rightarrow \infty$  のとき条件付き確率分布がカノニカル分布  $p(\beta)$  に収束することを示したい.

以下では, 数学的に厳密な取り扱いをするために, 条件  $\sum_{i=1}^r E_i p_i \approx U(\beta)$  の代わりに, 任意に  $a > 0$  を取って以下のように条件を課す:

- $\beta \geq 0$  のとき, 条件  $U(\beta) - a \leq \sum_{i=1}^r E_i p_i \leq U(\beta)$  を課す.
- $\beta \leq 0$  のとき, 条件  $U(\beta) \leq \sum_{i=1}^r E_i p_i \leq U(\beta) + a$  を課す.

後で  $a > 0$  の取り方は議論の本質に無関係であることがわかる. この条件のもとでの条件付き確率を考えるために  $\{1, 2, \dots, r\}$  上の確率分布全体の集合  $\mathcal{P}$  の部分集合  $A$  を

$$A = \begin{cases} \{p \in \mathcal{P} \mid U(\beta) - a \leq \sum_{i=1}^r E_i p_i \leq U(\beta)\} & (\beta \geq 0), \\ \{p \in \mathcal{P} \mid U(\beta) \leq \sum_{i=1}^r E_i p_i \leq U(\beta) + a\} & (\beta \leq 0) \end{cases}$$

と定める. 条件  $P_n \in A$  のもとでの条件付き確率

$$P(P_n \in B \mid P_n \in A) = \frac{P(P_n \in A \cap B)}{P(P_n \in A)} \quad (B \subset \mathcal{P})$$

が  $n \rightarrow \infty$  でカノニカル分布  $p(\beta)$  に集中することを Sanov の定理 (定理 3.1) を使って証明したい. そのために, 任意に  $\varepsilon > 0$  を取って,  $\mathcal{P}$  の部分集合  $B$  を次のように定める:

$$B = \{p \in \mathcal{P} \mid \|p - p(\beta)\| < \varepsilon\}.$$

ここで  $\|\cdot\|$  は Euclid ノルムである.  $B$  は  $p(\beta)$  の  $\varepsilon$  開近傍である. 以上の設定のもとで,  $n \rightarrow \infty$  で条件付き確率分布がカノニカル分布  $p(\beta)$  に集中することを意味する

$$P(P_n \in B \mid P_n \in A) \rightarrow 1 \quad (n \rightarrow \infty) \quad (*)$$

を示すことが以下の目標である.

Kullback-Leibler 情報量  $D(p||q)$  の定義を  $\mathcal{P}$  の部分集合  $C$  に

$$D(C||q) = \inf_{p \in C} D(p||q)$$

と拡張しておく. Sanov の定理より,  $\mathcal{P}$  の部分集合  $C$  の開核の閉包が  $C$  を含むとき

$$P(P_n \in C) = \exp(-nD(C||q) + o(n)).$$

上で定めた  $\mathcal{P}$  の部分集合  $A, B, A \cap B$  の開核の閉包はそれぞれ  $A, B, A \cap B$  を含む. さらに  $B$  の  $A$  での補集合  $B' = A \setminus B$  も同様である. ゆえに

$$P(P_n \in B' \mid P_n \in A) = \frac{P(P_n \in B')}{P(P_n \in A)} = \exp(-n(D(B'||q) - D(A||q)) + o(n)).$$

これが  $n \rightarrow \infty$  で 0 に収束することと目標である (\*) は同値である.

もしも条件  $p \in A$  のもとで  $p = p(\beta)$  が  $D(p||q)$  が唯一の最小点になるならば,  $B' = A \setminus B$  の閉包に  $p(\beta)$  が含まれないことより,  $D(B'||q) > D(A||q) = D(p(\beta)||q)$  となり,  $n \rightarrow \infty$  で  $P(P_n \in B' | P_n \in A) \rightarrow 0$  となることがわかる.

$D(p||q)$  は  $p$  の関数として下に狭義凸であり,  $A$  は  $\mathcal{P}$  の凸部分集合なので, 条件  $p \in A$  のもとでの  $D(p||q)$  が  $p = p(\beta)$  で最小になるならば,  $p = p(\beta)$  は唯一の最小点になる. ゆえに条件  $p \in A$  のもとで  $D(p||q)$  が  $p = p(\beta)$  で最小になることを示せば (\*) の証明が終了する. 以下でそのことを証明しよう.

カノニカル分布  $p(\beta)$  は

$$\sum_{i=1}^r E_i p_i(\beta) = U(\beta)$$

を満たしているので,  $p(\beta) \in A$  である. さらに<sup>10</sup>

$$\begin{aligned} D(p(\beta)||q) &= \sum_{i=1}^r p_i(\beta) \log \frac{p_i(\beta)}{q_i} = \sum_{i=1}^r p_i(\beta) \log \frac{e^{-\beta E_i}}{Z(\beta)} \\ &= \sum_{i=1}^r p_i(\beta) (-\beta E_i - \log Z(\beta)) = -\beta U(\beta) - \log Z(\beta). \end{aligned} \quad (\%)$$

これが条件  $p \in A$  のもとでの  $D(p||q)$  の最小値であることを示したい. すなわち  $p \in A$  のとき  $D(p||q) \geq D(p(\beta)||q)$  となることを示したい.

$p \in A$  と仮定する. このとき,  $A$  の定義より,  $\beta \geq 0$  のとき  $\sum_{i=1}^r E_i p_i \leq U(\beta)$  となり,  $\beta \leq 0$  のとき  $\sum_{i=1}^r E_i p_i \geq U(\beta)$  となるので,  $\beta$  の符号によらずに

$$\beta \sum_{i=1}^r E_i p_i \leq \beta U(\beta). \quad (\#)$$

が成立している. 第 4.1 節の計算より,  $\beta > 0$  と  $U(\beta) < \sum_{i=1}^r E_i q_i$  は同値であり,  $\beta < 0$  と  $U(\beta) > \sum_{i=1}^r E_i q_i$  は同値である. 集合  $A$  を定義するとき用いた  $a > 0$  は以下の議論には関係しない.

Kullback-Leibler 情報量  $D(p||q)$  は以下のように変形される:

$$\begin{aligned} D(p||q) &= \sum_{i=1}^r p_i \log \frac{p_i}{q_i} = \sum_{i=1}^r p_i \log \left( \frac{p_i}{p_i(\beta)} \frac{p_i(\beta)}{q_i} \right) = \sum_{i=1}^r p_i \log \frac{p_i}{p_i(\beta)} + \sum_{i=1}^r p_i \log \frac{p_i(\beta)}{q_i} \\ &= D(p||p(\beta)) + \sum_{i=1}^r p_i \log \frac{e^{-\beta E_i}}{Z(\beta)} = D(p||p(\beta)) + \sum_{i=1}^r p_i (-\beta E_i - \log Z(\beta)) \\ &= D(p||p(\beta)) - \beta \sum_{i=1}^r E_i p_i - \log Z(\beta). \end{aligned}$$

ゆえに, 不等式 (#) とカノニカル分布の Kullback-Leibler 情報量  $D(p(\beta)||q)$  の表示 (%) と Kullback-Leibler 情報量が常に 0 以上であることより,

$$D(p||q) \geq D(p||p(\beta)) - \beta U(\beta) - \log Z(\beta) = D(p||p(\beta)) + D(p(\beta)||q) \geq D(p(\beta)||q).$$

これで条件  $p \in A$  のもとで  $D(p||q)$  は  $p = p(\beta)$  で最小になることがわかった. 目標の (\*) が証明された.

<sup>10</sup>相対エントロピー  $S(p||q) = -D(p||q)$  を用いて公式を書き直すと  $S(p||q) = \beta U(\beta) + \log Z(\beta)$  になる. この手の公式は統計力学を知っている人達にはお馴染みのものだろう.

注意 4.1 (不等式 (#) について). 以上の議論は本質的に不等式 (#) の仮定だけにに基づく.

統計力学の文脈では  $\beta$  は絶対温度の Boltzmann 定数倍の逆数を意味する. その場合には  $\beta > 0$  となるので不等式 (#) は

$$(\text{エネルギーの平均値}) = \sum_{i=1}^r E_i p_i \leq U(\beta)$$

を意味する. この型の条件でカノニカル分布が特徴付けられることについては田崎 [8] の第 9-2-1 節 (p.319) も参照せよ.

カノニカル分布が経験的に自然に得られることを示すためには,  $\sum_{i=1}^r E_i p_i \approx U(\beta)$  という強い条件を仮定する必要はなく, 不等式 (#) を仮定するだけでよい. この点についてもう少し詳しくコメントしておく.

第 4.1 節で計算した通り,  $U(0)$  は母集団分布でのエネルギーの期待値  $\sum_{i=1}^r E_i q_i$  になる. そして  $\beta > 0$  を大きくすると  $U(\beta)$  は最小エネルギー準位  $\min\{E_1, \dots, E_r\}$  に近付き,  $\beta < 0$  を小さくすると  $U(\beta)$  は最大エネルギー準位  $\max\{E_1, \dots, E_r\}$  に近づく.  $\beta = \infty$  で状態は最小エネルギー状態 (基底状態) にはりつくようになり,  $\beta = -\infty$  で状態は最大エネルギー状態にはりつくようになる.

統計力学において  $\beta$  は絶対温度の逆数であり,  $\beta = \infty$  は絶対零度に対応し,  $\beta = 0$  は絶対温度無限大に対応している. 我々が扱っている場合には  $\beta$  は負にもなりえる. その場合には対応する絶対温度も負の値になる. 絶対温度の高さを逆温度  $\beta$  の低さで測ることにすれば, 負の絶対温度は絶対温度無限大よりも高温であるとみなされる.

我々が扱っているのは次のような状況であると考えられる.

$r$  種類の目が出るルーレットを回して,  $i$  の目が出たら賞金を  $E_i$  ペリカもらえるゲームを考える. ( $E_i < 0$  の場合には  $|E_i|$  ペリカ支払うことにすればギャンブルになる.)  $i$  の目が出る確率は  $q_i$  であるとする. そのようなゲーム 1 回あたりの賞金の期待値は  $U_0 = \sum_{i=1}^r E_i q_i$  になる. 大数の法則よりそのようなゲームをたくさん繰り返せば 1 回あたりの賞金の平均値は  $U_0$  に近づく.

まず  $U > U_0$  であると仮定する. ゲームをたくさん繰り返して (回数は  $n$  回とする). ゲーム 1 回あたりの賞金の平均値が  $U$  未満で終わったならば, 時間を巻き戻して何度でも  $n$  回分のゲームをやり直せると仮定する. そのようにしてゲーム 1 回あたりの賞金の平均値がゲーム自体の期待値である  $U_0$  より大きい  $U$  以上になったら時間を巻き戻すのを止める. このとき,  $n$  回のゲーム中  $i$  の目が出た割合  $p_i$  は ( $n$  が大きなとき) どのような値になる可能性が高いだろうか?

ゲーム 1 回あたりの賞金の平均値が  $U_0$  から離れれば離れるほどそのような状況が生じる確率は下がるので, ゲーム 1 回あたりの賞金の平均値はほぼ  $U$  (すなわち  $U$  よりほんの少し大きな数値) になってしまう可能性が高いだろう.

そのときの  $i$  の目が出た割合  $p_i$  を計算すると,  $U$  が定める  $\beta$  に対応するカノニカル分布  $p_i(\beta)$  に近くなる可能性が高いというのがこの節において数学的にきちんと証明したことである.

この場合には  $U > U_0$  なので  $\beta < 0$  となる. すなわち必要ならば時間を巻き戻すことによって, ゲーム自体の賞金期待値よりも高い賞金を求めると, 対応する絶対温度は負の値になってしまうと解釈される.

絶対温度が正の値の状況を作り出すには,  $U < U_0$  であると仮定し, 必要ならば時間を巻き戻して, ゲーム 1 回あたりの賞金の平均値が  $U$  以下になるようにすればよい. そのと



き, ゲーム 1 回あたりの賞金の平均値が  $U_0$  から離れば離れるほどそのような状況が生じる確率は下がるので, ゲーム 1 回あたりの賞金の平均値はほぼ  $U$  になる可能性が高く,  $i$  の目が出た割合は  $U$  に対応するカノニカル分布  $p_i(\beta)$  に近くなる可能性が高い. この場合には  $U < U_0$  なので  $\beta > 0$  となり, 絶対温度は正の値になる.

つまり, 時間を巻き戻して, ゲーム自体の期待値よりも低い賞金を得るようにすると絶対温度は正の値になるとされるのである.

以上の説明を読めばカノニカル分布の導出で使った不等式 (#) の向きがどのように自然であるかがわかると思う. 上の議論と第 1.5 節の最後の方の極限の計算と比較してみよ. 第 1.5 節では「丁半博打」のケースを扱っていると考えられる.  $\square$

### 4.3 まとめと二項分布もカノニカル分布の例になっていること

以上の結果は次のようにまとめられる.

**定理 4.2** (条件付き大数の弱法則, 条件付き極限定理). 母集団分布は  $q = (q_1, \dots, q_r) \in \mathcal{P}$  であるとする.  $X_1, X_2, \dots$  は独立で同分布  $q$  にしたがう  $\{1, 2, \dots, r\}$  に値を持つ確率変数列であるとする.  $X_1, X_2, \dots, X_n$  の中に含まれる  $i$  の個数を  $k_i$  と書き,  $P_n = (k_1/n, \dots, k_r/n)$  とおく.  $P_n$  は分布の集合  $\mathcal{P}$  に値を持つ確率変数になる.  $E_i \in \mathbb{R}$  は第 4.1 節の通りとする.  $E_1 < U < E_r$  であるとし,  $\beta \in \mathbb{R}$ ,  $p(\beta) = (p_1(\beta), \dots, p_r(\beta)) \in \mathcal{P}$ ,  $Z(\beta)$  を以下の条件で定める:

$$p_i(\beta) = \frac{e^{-\beta E_i} q_i}{Z(\beta)}, \quad Z(\beta) = \sum_{i=1}^r e^{-\beta E_i} q_i, \quad -\frac{\partial}{\partial \beta} \log Z(\beta) = \sum_{i=1}^r E_i p_i(\beta) = U.$$

$p(\beta)$  をカノニカル分布と呼ぶ.  $0 < a \leq \infty$  とし, 分布の集合  $A_U \subset \mathcal{P}$  を

$$A_U = \begin{cases} \{p \in \mathcal{P} \mid U - a \leq \sum_{i=1}^r E_i p_i \leq U\} & (\beta \geq 0), \\ \{p \in \mathcal{P} \mid U \leq \sum_{i=1}^r E_i p_i \leq U + a\} & (\beta \leq 0) \end{cases}$$

と定める. このとき  $\sum_{i=1}^r E_i p_i(\beta) = U$  なので  $p(\beta) \in A_U$  である. 任意に  $\varepsilon > 0$  を取り,  $p(\beta)$  の  $A_U$  における  $\varepsilon$  開近傍を  $B_\varepsilon(p(\beta))$  と書く. このとき,  $n \rightarrow \infty$  で

$$P(P_n \in B_\varepsilon(p(\beta)) \mid P_n \in A_U) = \frac{P(P_n \in B_\varepsilon(p(\beta)))}{P(P_n \in A_U)} \rightarrow 1.$$

すなわち経験分布  $P_n$  は  $n \rightarrow \infty$  でカノニカル分布  $p(\beta)$  に(確率)収束する.  $\square$

**例 4.3.** 確率  $\theta$  に対応する一般の二項分布が確率  $1/2$  の二項分布を母集団分布とする場合のカノニカル分布として自然に現われることを説明しよう. この例は母集団分布が一様分布でない場合のカノニカル分布の簡単な例になっている.

有限集合  $\{0, 1, \dots, r\}$  に値を持つ確率変数  $X$  は確率  $1/2$  に対応する対称な二項分布にしたがうと仮定する:

$$P(X = i) = \binom{r}{i} \frac{1}{2^r} \quad (i = 0, 1, \dots, r).$$

$X_1, X_2, \dots$  は独立で  $X$  と同じ分布を持つ確率変数の列であるとする.  $X_1, X_2, \dots, X_n$  の中に含まれる  $i$  の個数を  $k_i$  と書き,  $P_n = (k_0/n, k_1/n, \dots, k_r/n)$  とおくと,  $P_n$  は  $\{0, 1, \dots, r\}$

上の確率分布に値を持つ確率変数になる。大数の法則より、何も条件を付けずに  $n \rightarrow \infty$  とすると、 $P_n$  は対称な二項分布に近づく。

$E_i = i$  の場合にカノニカル分布が何になるかを計算してみよう。そのとき、分配関数は二項定理より

$$Z(\beta) = \sum_{i=0}^r e^{-\beta E_i} q_i = \sum_{i=0}^r \binom{r}{i} \left(\frac{e^{-\beta}}{2}\right)^i \left(\frac{1}{2}\right)^{r-i} = \frac{(e^{-\beta} + 1)^r}{2^r}$$

となるので、カノニカル分布は

$$p_i(\beta) = \frac{e^{-\beta E_i} q_i}{Z(\beta)} = \binom{r}{i} \frac{e^{-\beta i}}{(e^{-\beta} + 1)^r} = \binom{r}{i} \left(\frac{e^{-\beta}}{e^{-\beta} + 1}\right)^i \left(\frac{1}{e^{-\beta} + 1}\right)^{r-i}$$

と二項分布になる。つまり、

$$p_i(\beta) = \binom{r}{i} \theta^i (1 - \theta)^{r-i}, \quad \theta = \frac{e^{-\beta}}{e^{-\beta} + 1}.$$

このとき、

$$-Z'(\beta) = \frac{r e^{-\beta} (e^{-\beta} + 1)^{r-1}}{2^r}$$

なので、“エネルギーの期待値”は

$$U(\beta) = -\frac{\partial}{\partial \beta} Z(\beta) = \frac{-Z'(\beta)}{Z(\beta)} = \frac{r e^{-\beta}}{e^{-\beta} + 1} = r\theta$$

と確率  $\theta$  に対応する二項分布における  $i$  の期待値になる。

確率  $1/2$  に対応する対称な二項分布についてはコイン投げの状況を想像すると分かり易いだろう。コインを投げたとき表になる確率が  $1/2$  である状況を考える。そのようなコインを  $r$  回投げて表の出た回数  $i$  と表が出た割合  $i/r$  を記録する行為を  $n$  回繰り返したとしよう。ただし  $n$  は非常に大きいとする。記録には表の出た回数  $i$  と表が出た割合  $i/r$  がそれぞれ  $n$  個ずつ記録されている。その記録を見ると次が成立していたとする<sup>11</sup>:

$$(\text{表の出た割合 } i/r \text{ の平均値}) = \sum_{i=0}^r \frac{i}{r} p_i \approx \theta. \quad (*)$$

このとき  $p_i = k_i/n$  たちはどのような値になっている可能性が高いだろうか?

「経験分布  $p = (p_0, p_1, \dots, p_r)$  は確率  $\theta$  に対応する二項分布にほぼ等しくなっている可能性が高い」というのが、定理 4.2 をすぐ上の計算に適用したときの結論になる。

上で計算したカノニカル分布  $p(\beta)$  (確率  $\theta$  に対応する二項分布) は、定理 4.2 より、

$$(\text{表が出た回数 } i \text{ の期待値}) = \sum_{i=0}^r i p_i = \sum_{i=0}^r E_i p_i \approx U(\beta) = r\theta$$

を満たす分布  $p = (p_0, p_1, \dots, p_r)$  に制限した場合の経験分布  $P_n$  が  $n \rightarrow \infty$  で近づく先になっている。この条件は上の (\*) と同値である。表の出る割合が  $\theta$  になるという条件で制限を付ければ確率  $\theta$  に対応する二項分布が経験分布として自然に現われる。

<sup>11</sup>大数の(弱)法則より、 $\theta$  が  $1/2$  から離れている確率は  $n \rightarrow \infty$  で 0 に近づく。ここではそのような稀なケースが生じた場合を想定している。

**結論.** 表の出る確率が  $1/2$  の公平なコインを  $r$  回投げて表の出た回数を数えることをたくさん繰り返し,  $r$  回中表の出た回数が大量に記録されたリストを作ったとする. そのときもしもその記録において  $r$  回中表の出た割合の平均値が  $\theta$  になっているならば<sup>12</sup>, そのリストにはあたかも「表の出る確率が  $\theta$  の二項分布の記録が残っている」かのように見えてしまうことになる.  $\square$

**注意 4.4.** 例 4.3 の議論を一般化するとほぼ自明に以下のようなことが成立していることがわかる. 母集団分布  $q_i$  は最初から  $E_i$  に関するカノニカル分布の形をしていると仮定する:

$$q_i = \frac{e^{-\beta_0 E_i} q_{0,i}}{Z_0}, \quad Z_0 = \sum_{i=1}^r e^{-\beta_0 E_i} q_{i,0}.$$

ここで  $q_{0,i} \geq 0$ ,  $\sum_{i=1}^r q_{0,i} = 1$ ,  $E_1, \dots, E_r \in \mathbb{R}$  の最大値  $E_1$  と最大値  $E_r$  は異なり,  $q_1, q_r > 0$  であると仮定する. このとき, この母集団分布と  $E_i$  たちに対応するカノニカル分布  $p(\beta)$  も母集団分布と同じ形のカノニカル分布になる:

$$p_i(\beta) = \frac{e^{-(\beta_0+\beta)E_i} q_{0,i}}{Z_0 Z(\beta)}, \quad Z_0 Z(\beta) = Z_0 \sum_{i=1}^r e^{-\beta E_i} q_i = \sum_{i=1}^r e^{-(\beta_0+\beta)E_i} q_{0,i}.$$

二項分布は離散型の指数型分布族に含まれているので例 4.3 のようなことが成立するのである. 他の指数型分布族に含まれる確率分布についても同様のことが成立する.  $\square$

## 5 付録: Kullback-Leibler 情報量に関する不等式

Cover-Thomas [2] は情報理論に関する有名な教科書である. 情報量とエントロピー一般に関する詳しい解説を読みたい人はその本を参照すればよい. 以下では主にこの教科書を参照しながら, Kullback-Leibler 情報量が「距離」のような性質を持っていることを意味する不等式を扱う.

### 5.1 準備: Jensen の不等式

関数  $f(X)$  を数  $E[f(X)]$  に対応させる汎関数  $E[\cdot]$  は以下の条件を満たしていると仮定する:

1. 線形性: 関数  $f(X), g(X)$  と数  $\alpha, \beta$  に対して,  

$$E[\alpha f(X) + \beta g(X)] = \alpha E[f(X)] + \beta E[g(X)].$$
2. 短調性: 常に  $f(X) \geq g(X)$  ならば  $E[f(X)] \geq E[g(X)]$ .
3. 規格化条件:  $E[1] = 1$ .

規格化条件と短調性より, 数  $\alpha$  に対して  $E[\alpha] = \alpha$  となることがわかる. このような  $E[\cdot]$  を期待値汎関数と呼ぶ. たとえば  $p_i \geq 0$ ,  $\sum_{i=1}^r p_i = 1$  のとき,  $E[f(X)] = \sum_{i=1}^r f(x_i) p_i$  は期待値汎関数である. 他にも  $\rho(x) \geq 0$ ,  $\int_a^b \rho(x) dx = 1$  のとき,  $E[f(X)] = \int_a^b f(x) \rho(x) dx$  も期待値汎関数である.

このとき以下の不等式が成立している (**Jensen の不等式**):

<sup>12</sup> $\theta$  が  $1/2$  から離れると,  $n$  が大きなきそのようなりリストが得られる確率はほぼ 0 になるが, そのような稀な状況が生じてしまった場合についても考えている.

- $f(X)$  が上に凸ならば  $E[f(X)] \leq f(E[X])$ .
- $f(X)$  が下に凸ならば  $E[f(X)] \geq f(E[X])$ .

以下で前者のみを証明しよう. 後者は  $-f(X)$  に前者を適用すれば得られる.

前者の証明. 函数  $f(X)$  は上に凸であると仮定し,  $\mu = E[X]$  とおく. このとき上に凸な函数  $f(X)$  の  $X = \mu$  での“接線”を  $a(X - \mu) + f(\mu)$  と書くと,

$$f(X) \leq a(X - \mu) + f(\mu)$$

となるので,

$$E[f(X)] \leq E[a(X - \mu) + f(\mu)] = a(E[X] - \mu) + f(\mu) = f(E[X]).$$

2つ目の等号で期待値汎函数の短調性を使い, 2つ目の等号でその線形性と規格化条件を使った<sup>13</sup>. □

**注意 5.1.** 上の証明から,  $f(X)$  が上に狭義凸ならば,  $X$  の分布が  $\mu = E[f(X)]$  に集中していない限り (ほとんど確実に  $f(X) = \mu$  が成立していない限り), 等号を含まない強い不等式が成立していることがわかる. □

## 5.2 対数和不等式とその応用

次の不等式はたとえば [2], p.31, Theorem 2.7.1 (Log sum inequality) に書いてある.

対数和不等式 0 以上の  $a_i, b_i$  に対して,

$$\sum_{i=1}^n a_i \log \frac{a_i}{b_i} \geq A \log \frac{A}{B}, \quad A = \sum_{i=1}^n a_i, \quad B = \sum_{i=1}^n b_i.$$

等号の成立と  $a_i/b_i$  が互いにすべて等しいことは同値である. いつものように  $0 \log 0 = 0$ ,  $a \log(a/0) = \infty$  と約束しておく.

**証明.**  $a_i > 0, b_i > 0$  の場合のみを証明すれば十分である. (一般の場合はその場合の極限として証明される.)  $f(x) = x \log x$  とおくと,  $f'(x) = \log x + 1$ ,  $f''(x) = 1/x$  なので  $f(x)$  は  $x > 0$  で下に狭義凸である. これに Jensen の不等式を適用しよう. そのために  $p_i = b_i/B$  とおく. このとき

$$\begin{aligned} \frac{1}{B} \sum_{i=1}^n a_i \log \frac{a_i}{b_i} &= \sum_{i=1}^n \frac{b_i}{B} \frac{a_i}{b_i} \log \frac{a_i}{b_i} = \sum_{i=1}^n p_i f\left(\frac{a_i}{b_i}\right) \\ &\geq f\left(\sum_{i=1}^n p_i \frac{a_i}{b_i}\right) = f\left(\sum_{i=1}^n \frac{b_i}{B} \frac{a_i}{b_i}\right) = f\left(\frac{A}{B}\right) = \frac{A}{B} \log \frac{A}{B}. \end{aligned}$$

$f(x)$  の狭義凸性より, 等号が成立することと  $a_i/b_i$  が互いにすべて等しいことが同値であることもわかる. □

<sup>13</sup>  $E[f(X)] = \sum_{i=1}^r f(x_i)p_i$  の場合の Jensen の不等式は  $r$  に関する数学的帰納法で証明することもできるが, 期待値汎函数の公理だけを使って証明する方が不等式が成立する理由が分かりやすいと思う.

この不等式を使えば特に  $p_i, q_i$  が非負でそれぞれの総和が 1 のとき

$$D(p||q) = \sum_{i=1}^r p_i \log \frac{p_i}{q_i} \geq 1 \log \frac{1}{1} = 0$$

が得られる (Kullback-Leibler 情報量の非負性). さらに, 集合  $\{1, 2, \dots, r\}$  の分割

$$\{1, 2, \dots, r\} = A_1 \sqcup \dots \sqcup A_s$$

に対して,  $\{A_1, \dots, A_s\}$  上の確率分布  $P = (P_1, \dots, P_s), Q_j = (Q_1, \dots, Q_s)$  を

$$P_j = \sum_{i \in A_j} p_i, \quad Q_j = \sum_{i \in A_j} q_i$$

と定めると, 対数和不等式より

$$D(p||q) = \sum_{j=1}^s \sum_{i \in A_j} p_i \log \frac{p_i}{q_i} \geq \sum_{j=1}^s P_j \log \frac{P_j}{Q_j} = D(P||Q).$$

要するに, 細部の情報を忘れると Kullback-Leibler 情報量は小さくなる.

### 5.3 Kullback-Leibler 情報量で $L^1$ 距離を上からおさえられこと

集合  $\{1, 2, \dots, r\}$  上の確率分布  $p = (p_1, \dots, p_r), q = (q_1, \dots, q_r)$  のあいだの  $L^1$  距離  $\|p - q\|_{L^1}$  を

$$\|p - q\|_{L^1} = \sum_{i=1}^r |p_i - q_i|$$

と定める. 確率分布  $p$  に関する確率を

$$p(A) = \sum_{i \in A} p_i \quad (A \subset \{1, 2, \dots, r\})$$

と書くと,

$$\|p - q\|_{L^1} = 2(p(A) - q(A)), \quad A = \{i \in \{1, 2, \dots, r\} \mid p_i \geq q_i\}. \quad (\#)$$

なぜならば

$$\begin{aligned} \|p - q\|_{L^1} &= \sum_{i \in A} (p_i - q_i) + \sum_{i \in A^c} (q_i - p_i) = p(A) - q(A) + q(A^c) - p(A^c) \\ &= p(A) - q(A) + (1 - q(A)) - (1 - p(A)) = 2(p(A) - q(A)). \end{aligned}$$

以上の記号を以下においてそのまま用いる.

KL 情報量で  $L^1$  距離を上からおさえられること:

$$D(p||q) \geq \frac{1}{2} \|p - q\|_{L^1}^2. \quad (*)$$

この不等式を証明したい.

$r = 2$  の場合の (\*) の証明.  $0 < a < 1, 0 < b < 1$  のとき

$$a \log \frac{a}{b} + (1-a) \log \frac{1-a}{1-b} \geq 2(a-b)^2$$

となることを示せばよい. そのために左辺から右辺を引いた結果を  $f(b)$  と書く:

$$f(b) = a \log \frac{a}{b} + (1-a) \log \frac{1-a}{1-b} - 2(a-b)^2.$$

このとき

$$f'(b) = -\frac{a}{b} + \frac{1-a}{1-b} - 4(b-a) = (b-a) \left( \frac{1}{b(1-b)} - 4 \right).$$

$b(1-a) \leq 1/4$  より,  $1/(b(1-b)) - 4 \geq 0$  となる. ゆえに  $f(b)$  の符号は  $b-a$  の符号に等しい. すなわち  $f(b)$  は  $b < a$  で単調減少し,  $b > a$  で単調増加する. したがって  $f(b) = 0$  なので  $f(b) \geq 0$  となることがわかる.  $\square$

一般の場合の (\*) の証明. 集合  $A$  は (#) の通りであるとし, 集合  $\{1, 2, \dots, r\}$  の分割  $\{A, A^c\}$  上の確率分布  $P = (a, 1-a)$ ,  $Q = (b, 1-b)$  を  $a = p(A)$ ,  $b = q(A)$  と定める. このとき細部の情報を忘れると Kullback-Leibler 情報量が小さくなること (第 5.2 節) より

$$D(p||q) \geq D(p||q) \geq 2(a-b)^2 = 2(p(A) - q(B))^2 = \frac{1}{2} \|p - q\|_{L^1}^2.$$

ここで2つ目の不等号で上で証明した  $r = 2$  の場合の結果を使い, 最後に (#) を使った.  $\square$

## 5.4 Pithagorian theorem

$\mathcal{P} = \{p = (p_1, \dots, p_r) \in \mathbb{R}_{\geq 0}^r \mid p_1 + \dots + p_r = 1\}$  とおき,  $\mathcal{P}$  を集合  $\{1, 2, \dots, r\}$  上の確率分布全体の集合とみなす.  $\mathcal{P}$  は  $r-1$  次元単体である.

次の不等式は [2], p.367, Theorem 11.6.1 にある.

**Pythagorian theorem**  $E$  は  $\mathcal{P}$  の凸閉部分集合であるとし,  $q \in \mathcal{P} \setminus E$  であるとする.  $p^* = (p_1^*, \dots, p_r^*) \in E$  は  $D(p||q)$  を  $E$  上で最小化する  $p$  であるとする:

$$D(p^*||q) = \min_{p \in E} D(p||q).$$

このとき

$$D(p||q) \geq D(p||p^*) + D(p^*||q) \quad (p \in E).$$

この不等式と Kullback-Leibler 情報量の非負性より,  $D(p||q) \rightarrow D(p^*||q)$  ならば  $p \rightarrow p^*$  となることが導かれる.

証明. (pythagorean theorem の証明)  $p^*$  と  $p$  を通る直線上の Kullback-Leibler 情報量の値の  $p^*$  における微係数を見ればこの不等式が証明される.

$t \in \mathbb{R}$  に対して

$$p(t) = (p_1(t), \dots, p_r(t)) = tp + (1-t)p^*, \quad p_i(t) = tp_i + (1-t)p_i^*,$$

$$f(t) = D(p(t)||q) = \sum_{i=1}^r (tp_i + (1-t)p_i^*) \log \frac{tp_i + (1-t)p_i^*}{q_i}$$

とおく. このとき

$$f'(t) = \sum_{i=1}^r \left( (p_i - p_i^*) \log \frac{tp_i + (1-t)p_i^*}{q_i} + (p_i - p_i^*) \right)$$

$$= \sum_{i=1}^r (p_i - p_i^*) \log \frac{tp_i + (1-t)p_i^*}{q_i}.$$

2つ目の等号で  $\sum_{i=1}^r p_i = \sum_{i=1}^r p_i^* = 1$  となることを使った.

$p(0) = p^* \in E$ ,  $p(1) = p \in E$  であり,  $E$  は凸だったので  $p(t) \in E$  ( $0 \leq t \leq 1$ ).  $p^*$  は  $D(p||q)$  を  $E$  上で最小化する  $p$  だったので,  $f'(0) \geq 0$  となる. ゆえに

$$0 \leq f'(0) = \sum_{i=1}^r (p_i - p_i^*) \log \frac{p_i^*}{q_i} = \sum_{i=1}^r p_i \log \left( \frac{p_i p_i^*}{q_i p_i} \right) - \sum_{i=1}^r p_i^* \log \frac{p_i^*}{q_i}$$

$$= \sum_{i=1}^r p_i \log \frac{p_i}{q_i} - \sum_{i=1}^r p_i \log \frac{p_i}{p_i^*} - \sum_{i=1}^r p_i^* \log \frac{p_i^*}{q_i} = D(p||q) - D(p||p^*) - D(p^*||q).$$

これで示したい不等式が示された. □

## 6 付録: Cramér の定理

完璧に論理的に厳密な解説をするつもりはないので厳密な証明に興味がある人は注意して欲しい. 目標は統計力学の formulation との対応を明瞭になるようなスタイルで Cramér の定理の証明の概略を説明することである.

### 6.1 Cramér の定理の設定と主張

$H$  は平均値を持つ確率変数であるとし, その平均値を

$$U_0 = E[H]$$

と書く.  $H$  のモーメント母関数<sup>14</sup>:

$$Z(\beta) = E[e^{-\beta H}].$$

<sup>14</sup>確率論の教科書では, 通常, 確率変数  $H$  のモーメント母関数を  $M(t) = E[e^{tH}]$  と定義するが, ここでは統計力学との対応を見易くするために  $t = -\beta$  とおき, 統計力学における分配関数と同じ記号  $Z(\beta)$  をモーメント母関数に割り振った.

は正の幅を持つ区間上で有限の値を持つと仮定する.  $U(\beta)$  を次のように定める:

$$U(\beta) = \frac{E[He^{-\beta H}]}{Z(\beta)} = -\frac{\partial}{\partial \beta} \log Z(\beta).$$

$H_1, H_2$  独立な確率変数達で  $H$  と同じ分布にしたがうならば,  $Z(\beta)$  が有限になる開区間において,

$$\begin{aligned} \left(\frac{\partial}{\partial \beta}\right)^2 \log Z(\beta) &= -\frac{\partial}{\partial \beta} U(\beta) = \frac{Z''(\beta)Z(\beta) - Z'(\beta)^2}{Z(\beta)^2}, \\ Z''(\beta)Z(\beta) - Z'(\beta)^2 &= \frac{1}{2}E[(H_1 - H_2)^2 e^{-\beta(H_1+H_2)}] \geq 0 \end{aligned}$$

となるので,  $\log Z(\beta)$  は下に凸な函数になり,  $U(\beta)$  は単調減少函数になる. 特に,  $U(0) = U_0 = E[H]$  となり,  $\beta \geq 0$  のとき  $U(\beta) \leq U_0$  となり,  $\beta \leq 0$  のとき  $U(\beta) \geq U_0$  となる.

$\log Z(\beta)$  の Legendre 変換  $S(u)$  とその  $-1$  倍  $D(u)$  を次のように定める:

$$\begin{aligned} S(u) &= \inf_{\beta \in \mathbb{R}} (\beta u + \log Z(\beta)), \\ D(u) &= -S(u) = \sup_{\beta \in \mathbb{R}} (-\beta u - \log Z(\beta)) \quad (u \in \mathbb{R}). \end{aligned}$$

$S(u)$  は  $u$  に関する一次函数 (特に下に凸な函数) の族の各点ごとの下限で定義された函数なので,  $S(u)$  は上に凸な函数になる.  $0u - \log Z(0) = 0$  なので

$$S(u) \leq 0, \quad D(u) \geq 0 \quad (u \in \mathbb{R})$$

となる. さらに  $Z(\beta)$  が有限な開区間において,

$$\frac{\partial}{\partial \beta} (\beta u + \log Z(\beta)) = u - U(\beta)$$

なので,  $U(\beta) = u$  となる  $\beta = \beta(u)$  が存在するならば,

$$S(u) = \beta(u)u + \log Z(\beta(u)), \quad S(U(\beta)) = \beta U(\beta) + \log Z(\beta)$$

となる. 簡単のためこのような  $\beta = \beta(u)$  が常にとれると仮定する. これらの公式より  $S(u)$  はカノニカル分布の相対エントロピーに対応し,  $D(u) = -S(u)$  はカノニカル分布の **Kullback-Leibler 情報量** に対応することがわかる. 特に

$$S(U(0)) = 0, \quad D(U(0)) = 0$$

となるので,  $S(u)$  は  $u = U(0) = E[H]$  で最大値 0 になり,  $D(u)$  は同点で最小値 0 になる.  $S(u)$  (もしくは  $D(u)$ ) は  $u \geq U(0) = E[H]$  で単調減少 (もしくは単調増加) し,  $u \leq U(0) = E[H]$  で単調増加 (もしくは単調減少) する.

$U(\beta)$  は単調減少函数なので,  $u \leq U(0) = E[H]$  のとき  $\beta(u) \geq 0$  となり,  $u \geq U(0) = E[H]$  のとき  $\beta(u) \leq 0$  となる. ゆえに次が成立している:

$$S(u) = \begin{cases} \inf_{\beta \geq 0} (\beta u + \log Z(\beta)) & (u \leq U(0) = E[H]), \\ \inf_{\beta \leq 0} (\beta u + \log Z(\beta)) & (u \geq U(0) = E[H]). \end{cases} \quad (\#)$$

$D(u)$  についても同様の表示が存在する.  $u$  が  $H$  の平均値  $U(0) = E[H]$  以上と以下の場合で上限もしくは下限を取る範囲  $\beta$  の範囲を半分に制限できる.



**定理 6.1** (Cramér の定理). 以上の設定のもとで,  $H_1, H_2, \dots$  は独立同分布な確率変数列であり,  $H$  と同じ分布にしたがうと仮定する. このとき以下が成立している:

(1)  $F$  が  $\mathbb{R}$  の閉部分集合ならば

$$\limsup_{n \rightarrow \infty} \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \in F \right) \leq \sup_{u \in F} S(u) = - \inf_{u \in F} D(u).$$

(2)  $G$  が  $\mathbb{R}$  の開部分集合ならば

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \in G \right) \geq \sup_{u \in G} S(u) = - \inf_{u \in G} D(u).$$

(3)  $A$  が  $\mathbb{R}$  の部分集合であり,  $A$  の開核  $G$  の閉包  $F$  が  $A$  を含み,  $\sup_{u \in G} S(u) = \sup_{u \in F} S(u)$  が成立しているならば

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \in A \right) = \sup_{u \in A} S(u) = - \inf_{u \in A} D(u).$$

このように, 標本平均  $(H_1 + \dots + H_n)/n$  が集合  $A$  に含まれる確率の  $n \rightarrow \infty$  での漸近挙動はカノニカル分布の相対エントロピーに対応する量  $S(u)$  (もしくはカノニカル分布の Kullback-Leibler 情報量に対応する量  $D(u)$ ) の  $A$  における上限 (もしくは下限) で記述される.  $\square$

## 6.2 Cramér の定理の証明

**補題 6.2** (Cramé の定理の本質的部分). 第 6.1 節の設定のもとで以下が成立している.

(1)  $u$  が  $H$  の平均値  $U(0) = E[H]$  以上と以下の場合において, それぞれ

$$\begin{aligned} \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \geq u \right) &\leq S(u) & (u \geq U(0) = E[H]), \\ \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \leq u \right) &\leq S(u) & (u \leq U(0) = E[H]). \end{aligned}$$

この結果を適用するとき,  $u \geq U(0) = E[H]$  で  $S(u)$  は単調減少し,  $u \leq U(0) = E[H]$  で  $S(u)$  は単調増加することに注意せよ.

(2) 任意の  $\delta > 0$  に対して

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \in (u - \delta, u + \delta) \right) \geq S(u).$$

(1) の上からの評価は特別なアイデア抜きに容易に証明される. (2) の下からの評価は“カノニカル分布に関する大数の弱法則”を使って証明される.  $\square$

証明. (1) の上からの評価を証明しよう. まず,  $u \leq U(0) = E[H]$  と仮定する.  $H_1 + \dots + H_n \leq nu$  のとき 1 で他のとき 0 になる函数を  $1_{H_1 + \dots + H_n \leq nu}$  と書くと,  $\beta \geq 0$  のとき

$$\begin{aligned} P\left(\frac{1}{n} \sum_{k=1}^n H_k \leq u\right) &= E[1_{H_1 + \dots + H_n \leq nu}] \\ &\leq E[1_{H_1 + \dots + H_n \leq nu} e^{-\beta(H_1 + \dots + H_n - nu)}] \\ &\leq E[e^{-\beta(H_1 + \dots + H_n - nu)}] \\ &= e^{n\beta u} Z(\beta)^n = e^{n(\beta u + \log Z(\beta))}. \end{aligned}$$

ゆえに  $u \leq U(0) = E[H]$ ,  $\beta \geq 0$  のとき

$$\frac{1}{n} \log P\left(\frac{1}{n} \sum_{k=1}^n H_k \leq u\right) \leq \beta u + \log Z(\beta).$$

したがって第 6.1 節の (#) より

$$\frac{1}{n} \log P\left(\frac{1}{n} \sum_{k=1}^n H_k \leq u\right) \leq \inf_{\beta \geq 0} (\beta u + \log Z(\beta)) = S(u).$$

次に,  $u \geq U(0) = E[H]$  と仮定して, 上と同様の議論を行なう.  $H_1 + \dots + H_n \geq nu$  のとき 1 で他のとき 0 になる函数を  $1_{H_1 + \dots + H_n \geq nu}$  と書くと,  $\beta \leq 0$  のとき

$$\begin{aligned} P\left(\frac{1}{n} \sum_{k=1}^n H_k \geq u\right) &= E[1_{H_1 + \dots + H_n \geq nu}] \\ &\leq E[1_{H_1 + \dots + H_n \geq nu} e^{-\beta(H_1 + \dots + H_n - nu)}] \\ &\leq E[e^{-\beta(H_1 + \dots + H_n - nu)}] \\ &= e^{n\beta u} Z(\beta)^n = e^{n(\beta u + \log Z(\beta))}. \end{aligned}$$

ゆえに  $u \geq U(0) = E[H]$ ,  $\beta \leq 0$  のとき

$$\frac{1}{n} \log P\left(\frac{1}{n} \sum_{k=1}^n H_k \geq u\right) \leq \beta u + \log Z(\beta).$$

したがって第 6.1 節の (#) より

$$\frac{1}{n} \log P\left(\frac{1}{n} \sum_{k=1}^n H_k \geq u\right) \leq \inf_{\beta \leq 0} (\beta u + \log Z(\beta)) = S(u).$$

これで (1) の上からの評価が証明された.

(2) の下からの評価を証明しよう. (2) は “カノニカル分布に関する大数の弱法則” から導かれる. 確率変数  $H$  の確率分布は  $\mathbb{R}$  上の確率測度  $\mu$  が定める確率分布にしたがっているとする. 確率測度  $\mu_\beta$  を

$$\mu_\beta(dx) = \frac{e^{-\beta x} \mu(dx)}{Z(\beta)}$$

と定め、この確率測度の定める確率分布をカノニカル分布と呼ぶことにする。カノニカル分布に関する期待値と確率をそれぞれ  $E_\beta[\cdot]$ ,  $P_\beta(\cdot)$  と書く。確率変数  $H$  のカノニカル分布に関する平均は

$$E_\beta[H] = \frac{E[He^{-\beta H}]}{Z(\beta)} = U(\beta)$$

になる。以下では  $u = U(\beta)$ ,  $\delta > 0$  と仮定する。このとき  $S(u)$  の定義より、

$$S(u) = \beta u + \log Z(\beta).$$

$\delta$  以下の任意の  $\varepsilon > 0$  を取る。カノニカル分布に関する大数の弱法則より

$$\lim_{n \rightarrow \infty} P_\beta \left( \frac{1}{n} \sum_{k=1}^n H_k \in (u - \varepsilon, u + \varepsilon) \right) = 1.$$

そして、カノニカル分布での確率と母集団分布での確率のあいだに以下の関係がある：

$$\begin{aligned} P_\beta \left( \frac{1}{n} \sum_{k=1}^n H_k \in (u - \varepsilon, u + \varepsilon) \right) &= \frac{E[1_{H_1 + \dots + H_n \in (nu - n\varepsilon, nu + n\varepsilon)} e^{-\beta(H_1 + \dots + H_n)}]}{Z(\beta)^n} \\ &\leq Z(\beta)^{-n} E[1_{H_1 + \dots + H_n \in (nu - n\varepsilon, nu + n\varepsilon)} e^{-n\beta u + n|\beta|\varepsilon}] \\ &= e^{-n(\beta u + \log Z(\beta) - |\beta|\varepsilon)} P \left( \frac{1}{n} \sum_{k=1}^n H_k \in (u - \varepsilon, u + \varepsilon) \right) \\ &\leq e^{-n(\beta u + \log Z(\beta) - |\beta|\delta)} P \left( \frac{1}{n} \sum_{k=1}^n H_k \in (u - \delta, u + \delta) \right). \end{aligned}$$

以上の結果を合わせると

$$P \left( \frac{1}{n} \sum_{k=1}^n H_k \in (u - \delta, u + \delta) \right) \geq e^{n(\beta u + \log Z(\beta) - |\beta|\varepsilon)} (1 + o(1)) \quad (n \rightarrow \infty).$$

ゆえに両辺の対数の  $1/n$  倍の  $n \rightarrow \infty$  での極限を取ることによって次を得る：

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \in (u - \delta, u + \delta) \right) \geq \beta u + \log Z(\beta) - |\beta|\varepsilon = S(u) - |\beta|\varepsilon.$$

$\varepsilon > 0$  はいくらでも小さくできるので、

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \in (u - \delta, u + \delta) \right) \geq S(u).$$

これで (2) も示された。 □

**定理 6.1** の証明. (1) の上からの評価を証明しよう。  $F$  は  $\mathbb{R}$  の閉部分集合であるとし、

$$F_+ = \{u \in F \mid u \geq U(0) = E[H]\}, \quad F_- = \{u \in F \mid u \leq U(0) = E[H]\}$$

とおく。これらも  $\mathbb{R}$  の閉部分集合なので、 $F_-$  の最大値  $u_-$  と  $F_+$  の最小値  $u_+$  が存在する。 $S(u)$  は  $u \geq U(0) = E[H]$  で単調減少し、 $u \leq U(0) = E[H]$  で単調増加するので

$$\sup_{u \in F_+} S(u) = S(u_+), \quad \sup_{u \in F_-} S(u) = S(u_-), \quad \sup_{u \in F} S(u) = \max\{S(u_+), S(u_-)\}.$$

ゆえに補題 6.2 (1) より,

$$\begin{aligned} \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \in F_+ \right) &\leq \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \geq u_+ \right) \leq S(u_+), \\ \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \in F_- \right) &\leq \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \leq u_- \right) \leq S(u_-), \\ P \left( \frac{1}{n} \sum_{k=1}^n H_k \in F \right) &\leq e^{nS(u_+)} + e^{nS(u_-)} \leq 2e^{n \sup_{u \in F} S(u)}. \end{aligned}$$

ゆえに

$$\limsup_{n \rightarrow \infty} \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \in F \right) \leq \sup_{u \in F} S(u).$$

これで (1) が示された.

(2) の下からの評価を証明しよう.  $G$  は  $\mathbb{R}$  の開部分集合であると仮定する. 任意に  $\varepsilon > 0$  を取ると, ある  $u \in G$  で

$$S(v) \geq \sup_{u \in G} S(u) - \varepsilon$$

を満たすものが存在する.  $G$  は開部分集合なので, ある  $\delta > 0$  で  $(v - \delta, v + \delta) \subset G$  を満たすものを取れる. このとき, 補題 6.2 (2) より

$$\begin{aligned} \liminf_{n \rightarrow \infty} \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \in G \right) &\geq \liminf_{n \rightarrow \infty} \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \in (v - \delta, v + \delta) \right) \\ &\geq S(v) \geq \sup_{u \in G} S(u) - \varepsilon. \end{aligned}$$

したがって

$$\liminf_{n \rightarrow \infty} \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \in G \right) \geq \sup_{u \in G} S(u).$$

これで (2) も示された.

最後に (3) を示そう.  $A$  は  $\mathbb{R}$  の部分集合であるとし,  $A$  の開核を  $G$  と書き,  $G$  の閉包を  $F$  と書く.  $A \subset F$  と仮定する. このとき  $G \subset A \subset F$  なので

$$\begin{aligned} \sup_{u \in G} S(u) &\leq \liminf_{n \rightarrow \infty} \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \in G \right) \leq \liminf_{n \rightarrow \infty} \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \in A \right) \\ &\leq \limsup_{n \rightarrow \infty} \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \in A \right) \leq \limsup_{n \rightarrow \infty} \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \in F \right) \leq \sup_{u \in F} S(u), \\ \sup_{u \in G} S(u) &\leq \sup_{u \in A} S(u) \leq \sup_{u \in F} S(u). \end{aligned}$$

ゆえに  $\sup_{u \in G} S(u) = \sup_{u \in F} S(u)$  ならば

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log P \left( \frac{1}{n} \sum_{k=1}^n H_k \in A \right) = \sup_{u \in A} S(u).$$

これで示すべきことがすべて示された. □

### 6.3 カノニカル分布の相対エントロピーとの関係

$q = (q_1, \dots, q_r)$  は有限集合  $\{1, \dots, r\}$  上の確率分布であるとする:

$$q_i \geq 0, \quad q_1 + \dots + q_r = 1.$$

確率変数  $H$  すなわち有限集合  $\{1, \dots, r\}$  上の関数  $H(i) = E_i \in \mathbb{R}$  を考える. このとき

$$Z(\beta) = E[e^{-\beta H}] = \sum_{i=1}^r e^{-\beta E_i} q_i.$$

カノニカル分布  $p(\beta) = (p_1(\beta), \dots, p_r(\beta))$  は

$$p_i(\beta) = \frac{e^{-\beta E_i} q_i}{Z(\beta)}$$

と定義され,

$$U(\beta) = E_\beta[H] = \sum_{i=1}^r E_i p_i(\beta) = \frac{1}{Z(\beta)} \sum_{i=1}^r E_i e^{-\beta E_i} q_i.$$

ゆえに

$$\begin{aligned} S(U(\beta)) &= \beta U(\beta) + \log Z(\beta) = -(-\beta U(\beta) - \log Z(\beta)) \\ &= -\sum_{i=1}^r p_i(\beta)(-\beta E_i - \log Z(\beta)) = -\sum_{i=1}^r p_i(\beta) \log \frac{p_i(\beta)}{q_i} = S(p(\beta) \| q). \end{aligned}$$

すなわち,  $\log Z(\beta)$  の Legendre 変換で定義された  $S(u)$  に  $u = U(\beta)$  を代入した結果はカノニカル分布の相対エントロピーに一致する.

### 6.4 ガンマ分布の場合の例

確率変数  $H$  が形状  $\alpha > 0$ , スケール  $\tau > 0$  のガンマ分布にしたがうとは

$$E[f(H)] = \frac{1}{\Gamma(\alpha)\tau^\alpha} \int_0^\infty f(x) e^{-x/\tau} x^{\alpha-1} dx$$

が成立することである. このとき  $\beta > -1/\tau$  ならば

$$\begin{aligned} Z(\beta) &= E[e^{-\beta H}] = \frac{1}{\Gamma(\alpha)\tau^\alpha} \int_0^\infty e^{-(1+\tau\beta)x/\tau} x^{\alpha-1} dx = \frac{1}{(1+\tau\beta)^\alpha}, \\ U(\beta) &= \frac{(1+\tau\beta)^\alpha}{\Gamma(\alpha)\tau^\alpha} \int_0^\infty e^{-(1+\tau\beta)x/\tau} x^\alpha dx = \frac{(1+\tau\beta)^\alpha \Gamma(\alpha+1)\tau^{\alpha+1}}{\Gamma(\alpha)\tau^\alpha (1+\tau\beta)^{\alpha+1}} = \frac{\tau\alpha}{1+\tau\beta} > 0. \end{aligned}$$

ここでよく使われる次の公式を使った<sup>15</sup>:

$$\int_0^\infty e^{-cx} x^{s-1} dx = \frac{\Gamma(s)}{c^s} \quad (s, c > 0).$$

<sup>15</sup>使った公式はガンマ関数の定義から置換積分によって容易に示される.  $U(\beta)$  に関する公式は  $U(\beta) = -(\partial/\partial\beta) \log Z(\beta)$  を使えばより簡単に得られる.

ゆえに

$$\begin{aligned} S(U(\beta)) &= \beta U(\beta) + \log Z(\beta) = \frac{\tau\alpha\beta}{1+\tau\beta} - \alpha \log(1+\tau\beta) \\ &= \alpha - \frac{\alpha}{1+\tau\beta} - \alpha \log(1+\tau\beta). \end{aligned}$$

これに  $U(\beta) = u > 0$  と

$$1 + \tau\beta = \frac{\tau\alpha}{u}, \quad \beta = \frac{\alpha}{u} - \frac{1}{\tau}$$

を代入すると,

$$S(u) = \alpha - \frac{u}{\tau} - \alpha \log \frac{\tau\alpha}{u} = \alpha - \alpha \log \alpha - \left( \frac{u}{\tau} - \alpha \log \frac{u}{\tau} \right).$$

$S(u)$  は  $u = U(0) = \tau\alpha$  で最大値 0 になる.

$H_1, H_2, \dots$  が独立同分布な確率変数列で各々が  $H$  と同じ形状  $\alpha$ , スケール  $\tau$  のガンマ分布にしたがうとき, ガンマ分布の再生性より<sup>16</sup>,  $H_1 + \dots + H_n$  は形状  $n\alpha$ , スケール  $\tau$  のガンマ分布にしたがうので,

$$E \left[ f \left( \frac{1}{n} \sum_{k=1}^n H_k \right) \right] = \frac{1}{\Gamma(n\alpha)\tau^{n\alpha}} \int_0^\infty f \left( \frac{y}{n} \right) e^{-y/\tau} y^{n\alpha-1} dy.$$

ゆえに  $0 \leq a < b$  のとき

$$P \left( a < \frac{1}{n} \sum_{k=1}^n H_k < b \right) = \frac{1}{\Gamma(n\alpha)\tau^{n\alpha}} \int_{na}^{nb} e^{-y/\tau} y^{n\alpha-1} dy = \frac{n^{n\alpha}}{\Gamma(n\alpha)} \int_{a/\tau}^{b/\tau} e^{-nx} x^{n\alpha-1} dx.$$

2つ目の等号で  $y = n\tau x$  とおいた. Cramér の定理より,

$$\lim_{n \rightarrow \infty} \left( \frac{1}{n} \log \frac{n^{n\alpha}}{\Gamma(n\alpha)} \int_{a/\tau}^{b/\tau} e^{-nx} x^{n\alpha-1} dx \right) = \sup_{a < u < b} S(u) = \begin{cases} S(b) & (b/\tau < \alpha), \\ 0 & (a/\tau \leq \alpha \leq b/\tau), \\ S(a) & (\alpha < a/\tau). \end{cases}$$

<sup>16</sup>  $H_1 + \dots + H_n$  のモーメント母関数は  $H$  のモーメント母関数の  $n$  乗  $Z(\beta)^n = (1 + \tau\beta)^{-n\alpha}$  に等しい. これは形状  $n\alpha$ , スケール  $\tau$  のガンマ分布のモーメント母関数に一致する. このことから  $H_1 + \dots + H_n$  が形状  $n\alpha$ , スケール  $\tau$  のガンマ分布にしたがうことがわかる. 直接的な計算によってもそのことを示せる.  $H, K$  は独立な確率変数であり, それぞれ形状  $\alpha, \beta$ , スケール  $\tau$  のガンマ分布にしたがうならば

$$\begin{aligned} E[f(H+K)] &= \frac{1}{\Gamma(\alpha)\Gamma(\beta)\tau^{\alpha+\beta}} \int_0^\infty \left( \int_0^\infty f(x+y) e^{-(x+y)/\tau} x^{\alpha-1} y^{\beta-1} dy \right) dx \\ &= \frac{1}{\Gamma(\alpha)\Gamma(\beta)\tau^{\alpha+\beta}} \int_0^\infty \left( \int_x^\infty f(t) e^{-t/\tau} x^{\alpha-1} (t-x)^{\beta-1} dt \right) dx \\ &= \frac{1}{\Gamma(\alpha)\Gamma(\beta)\tau^{\alpha+\beta}} \int_0^\infty f(t) e^{-t/\tau} \left( \int_0^y x^{\alpha-1} (t-x)^{\beta-1} dx \right) dy \\ &= \frac{1}{\Gamma(\alpha)\Gamma(\beta)\tau^{\alpha+\beta}} \int_0^\infty f(t) e^{-t/\tau} \left( \int_0^1 t^{\alpha-1} u^{\alpha-1} t^{\beta-1} (1-u)^{\beta-1} t du \right) dy \\ &= \frac{B(\alpha, \beta)}{\Gamma(\alpha)\Gamma(\beta)\tau^{\alpha+\beta}} \int_0^\infty f(t) e^{-t/\tau} t^{\alpha+\beta-1} dt \\ &= \frac{1}{\Gamma(\alpha+\beta)\tau^{\alpha+\beta}} \int_0^\infty f(t) e^{-t/\tau} t^{\alpha+\beta-1} dt \end{aligned}$$

2つ目の等号で  $y = t - x$  とおいて  $y$  から  $t$  に積分変数を置換し, 4つ目の等号で  $x = tu$  とおいて  $x$  から  $u$  に積分変数を変換した. これより  $H + K$  が形状  $\alpha + \beta$ , スケール  $\tau$  のガンマ分布にしたがうことがわかる. ガンマ分布は形状について再生性を持つと言う.

Stirling の公式より  $-\log \Gamma(n\alpha) = -n\alpha \log n + n(\alpha - \alpha \log \alpha) + o(n)$  なので, これは次の公式と同値である ( $A = a/\tau, B = b/\tau$ ):

$$\begin{aligned} & \lim_{n \rightarrow \infty} \frac{1}{n} \log \left( \int_A^B e^{-nx} x^{n\alpha-1} dx \right) \\ &= \sup_{a/\tau < x < b/\tau} (\alpha \log x - x) = \begin{cases} \alpha \log B - B & (B < \alpha), \\ \alpha \log \alpha - \alpha & (A \leq \alpha \leq B), \\ \alpha \log A - A & (\alpha < A). \end{cases} \end{aligned}$$

この公式は

$$e^{-nx} x^{n\alpha-1} = \exp(n(\alpha \log x - x) + o(n))$$

に Laplace の方法を適用することによって直接に示される.

## 7 付録: 他の種類のエントロピーについて

### 7.1 自由エネルギーや Massieu 函数との関係

**注意 7.1** (モーメント母函数とキュムラント母函数). 確率分布  $q_i$  のもとで確率変数  $X : i \mapsto X_i$  のモーメント母函数  $M_X(t)$  は

$$M_X(t) = \sum_{i=1}^r e^{tX_i} q_i$$

と定義される. これは  $X = E, t = -\beta$  のとき分配函数

$$Z(\beta) = \sum_{i=1}^r e^{-\beta E_i} q_i$$

に一致する. 確率論の教科書に書いてあるモーメント母函数 (積率母函数) は分配函数と本質的に同じものだと思ってよい. 確率論の教科書によればモーメント母函数の対数

$$K_X(t) = \log M_X(t)$$

は確率変数  $X$  のキュムラント母函数 (cumulant generating function) と呼ばれている. 自由エネルギーの定義

$$F(\beta) = -\frac{1}{\beta} \log Z(\beta)$$

は本質的にキュムラント母函数の定義に一致している. より正確には逆温度  $\beta$  で割る前の

$$\mathcal{F}(\beta) = \log Z(\beta) \quad (\text{より正確には右辺はその Boltzmann 定数倍})$$

の方がキュムラント母函数の直接の対応物になる. こちらの  $\mathcal{F}(\beta)$  は **Massieu 函数** と呼ばれている.  $\square$

## 7.2 相対 Rényi エントロピー

注意 7.2 (相対 Rényi エントロピー). 2つの確率分布  $p = (p_1, \dots, p_r)$ ,  $q = (q_1, \dots, q_r)$  に対して, 相対 Rényi エントロピー  $S_\beta(p||q)$  が

$$S_\beta(p||q) = -\frac{1}{\beta-1} \log \sum_{i=1}^r \left(\frac{p_i}{q_i}\right)^\beta q_i = -\frac{1}{\beta-1} \log \sum_{i=1}^r p_i^\beta q_i^{1-\beta}$$

と定義される. これの  $\beta-1$  倍を  $\beta$  で微分すると

$$\frac{\partial}{\partial \beta} ((\beta-1)S_\beta(p||q)) = -\frac{\sum_{i=1}^r p_i^\beta q_i^{1-\beta} \log(p_i/q_i)}{\sum_{i=1}^r p_i^\beta q_i^{1-\beta}}$$

なので, さらに  $\beta=1$  とすると,

$$\left. \frac{\partial}{\partial \beta} \right|_{\beta=1} ((\beta-1)S_\beta(p||q)) = -\sum_{i=1}^r p_i \log \frac{p_i}{q_i} = S(p||q)$$

と相対エントロピーが出て来る. ゆえに

$$S_1(p||q) := \lim_{\beta \rightarrow 1} S_\beta(p||q) = S(p||q).$$

相対 Rényi エントロピーは相対エントロピーのワンパラメータ変形になっていると考えられる.  $q_i = 1$  の場合の Rényi エントロピーの定義を知っていれば相対 Rényi エントロピーの定義は誰でも容易に思い付くと思われる.

相対 Rényi エントロピーの定義は分配関数

$$Z(\beta; p, q) = \sum_{i=1}^r \left(\frac{p_i}{q_i}\right)^\beta q_i = \sum_{i=1}^r e^{-\beta E_i} q_i, \quad E_i = -\log \frac{p_i}{q_i}$$

に付随する自由エネルギー  $F(\beta; p, q)$  と Massieu 関数  $\mathcal{F}(\beta; p, q)$  の定義

$$\begin{aligned} F(\beta; p, q) &= -\beta^{-1} \log Z(\beta; p, q), \\ \mathcal{F}(\beta; p, q) &= \log Z(\beta; p, q) \quad (\text{Boltzmann 定数倍は略}) \end{aligned}$$

と本質的に同じである:

$$(\beta-1)S_\beta(p||q) = \beta F(\beta; p, q) = -\mathcal{F}(\beta; p, q) = -\log Z(\beta; p, q).$$

Rényi divergence (相対 Rényi エントロピーの  $-1$  倍) の基本性質のまとめが [9] にある.

$(\beta-1)S_\beta(p||q) = -\log Z(\beta; p, q)$  は  $\beta$  の函数として上に凸である:

$$\left(\frac{\partial}{\partial \beta}\right)^2 (-\log Z(\beta; p, q)) = -\frac{\sum_{i,j=1}^r (E_i - E_j)^2 e^{-\beta(E_i+E_j)} q_i q_j}{2Z(\beta)^2} \leq 0$$

(等号成立は  $p_i = q_i$  ( $i = 1, \dots, r$ ) と同値).

そして,  $(\beta-1)S_\beta(p||q) = -\log Z(\beta; p, q)$  の  $\beta=1$  での値が  $-\log Z(1; p, q) = -\log 1 = 0$  であることと,  $(\beta-1)S_\beta(p||q) = -\log Z(\beta; p, q)$  の  $\beta=1$  での微係数が相対エントロピー  $S(p||q)$  に等しいという上の計算結果より,

$$(\beta-1)S_\beta(p||q) \leq (\beta-1)S(p||q).$$

右辺は左辺の接線の式である. □



### 7.3 相対 Tsallis エントロピー

**注意 7.3** (相対 Tsallis エントロピー). 確率分布  $p = (p_1, \dots, p_r), q = (q_1, \dots, q_r)$  に対して,  $Z(\beta; p, q)$  を次のように定める:

$$Z(\beta; p, q) = \sum_{i=1}^r e^{-\beta E_i} q_i = \sum_{i=1}^r \left( \frac{p_i}{q_i} \right)^\beta q_i = \sum_{i=1}^r p_i^\beta q_i^{1-\beta}, \quad E_i = -\log \frac{p_i}{q_i}.$$

各  $E_i$  は 2 つの確率分布  $p$  と  $q$  の各  $i$  ごとの違いを表わしている. カノニカル分布  $p(\beta) = (p_1(\beta), \dots, p_r(\beta))$  を

$$p_i(\beta) = \frac{e^{-\beta E_i} q_i}{Z(\beta; p, q)} = \frac{p_i^\beta q_i^{1-\beta}}{Z(\beta; p, q)}$$

と定めると, 逆温度  $\beta$  は  $q_i = p_i(0)$  と  $p_i = p_i(1)$  を補間するパラメーターになっている. このとき, 相対 Rényi エントロピー  $S_\beta(p||q)$  は

$$S_\beta(p||q) = \frac{\log Z(\beta; p, q)}{1 - \beta} = \frac{1}{1 - \beta} \log \sum_{i=1}^r p_i^\beta q_i^{1-\beta}$$

と表わされ, 相対エントロピー  $S(p||q)$  は

$$S(p||q) = - \left. \frac{\partial}{\partial \beta} \right|_{\beta=1} \log Z(\beta; p, q) = - \left. \frac{\partial}{\partial \beta} \right|_{\beta=1} Z(\beta; p, q) = - \sum_{i=1}^r p_i \log \frac{p_i}{q_i}$$

と表わされる. 2 つ目の等号で  $Z(1; p, q) = 1$  を使った.

次の演算を  $x$  に関する  $q$  差分作用素と呼ぶ:

$$D_{x,q} f(x) = \frac{f(x) - f(qx)}{(1-q)x}.$$

$q \rightarrow 1$  で  $q$  差分  $D_{x,q} f(x)$  は微分  $\partial f(x)/\partial x$  に収束する.

上の相対エントロピーの式の  $\log Z(\beta; p, q)$  ではなく  $Z(\beta; p, q)$  を用いた表示における  $\beta$  に関する微分を  $q$  差分で置き換えることによって<sup>17</sup>, 相対 Tsallis エントロピーが次のように定義される<sup>18</sup> ( $q$  差分の  $q$  を次の式では  $\alpha$  と書く):

$$T_\alpha(p||q) = - D_{\beta,\alpha} \Big|_{\beta=1} Z(\beta; p, q) = - \frac{Z(1; p, q) - Z(\alpha; p, q)}{1 - \alpha} = - \frac{1 - \sum_{i=1}^r p_i^\alpha q_i^{1-\alpha}}{1 - \alpha}.$$

$\alpha \rightarrow 1$  で  $\alpha$  差分は通常の微分に収束するので, 相対 Tsallis エントロピーは相対エントロピーに収束する. そのことは

$$T_\alpha(p||q) = - \sum_{i=1}^r \frac{(p_i/q_i) - (p_i/q_i)^\alpha}{1 - \alpha} q_i, \quad \lim_{\alpha \rightarrow 1} \frac{x - x^\alpha}{1 - \alpha} = \left. \frac{\partial}{\partial \alpha} \right|_{\alpha=1} x^\alpha = x \log x.$$

<sup>17</sup>筆者は 2016 年 6 月 22 日の段階でその必然性をまったく理解できていない.

<sup>18</sup>筆者は (相対)Tsallis エントロピーの定義の必然性をまったく理解していない. (相対)Rényi エントロピーは本質的に分配函数の対数 (自由エネルギー, Massieu 函数) なのでそのようなものを考えることの必然性を納得できるが, (相対)Tsallis エントロピーについてはよくわからない.

より, 直接にも確かめられる. 相対 Tsallis エントロピーは相対エントロピーの定義における  $x \log x$  を  $(x - x^\alpha)/(1 - \alpha)$  で置き換えたものだと言える. 相対 Tsallis エントロピーを相対 Rényi エントロピーで次のように表わすこともできる:

$$T_\beta(p||q) = \frac{Z(\beta; p, q) - 1}{1 - \beta} = \frac{\exp((1 - \beta)S_\beta(p||q)) - 1}{1 - \beta}.$$

逆に相対 Rényi エントロピーを相対 Tsallis エントロピーによって

$$S_\beta(p||q) = \frac{\log Z(\beta; p, q)}{1 - \beta} = \frac{\log(1 + (1 - \beta)T_\beta(p||q))}{1 - \beta}$$

と表わすこともできる. 相対 Tsallis エントロピーと相対 Rényi エントロピーの違いは  $x - 1$  と  $\log x = \log(1 + (x - 1))$  の違いであると考えられる.

以上のように, 相対エントロピー, 相対 Rényi エントロピー, 相対 Tsallis エントロピーはどれも分配関数  $Z(\beta; p, q)$  からの派生物である.  $\square$

**注意** (相対 Tsallis エントロピーと相対 Rényi エントロピーの関係). 相対 Tsallis エントロピー  $T_\beta(p||q)$  と相対 Rényi エントロピー  $S_\beta(p||q)$  はどちらも

$$Z_\beta(p||q) = \sum_{i=1}^r p_i^\beta q_i^{1-\beta}$$

を用いて

$$T_\beta(p||q) = -\frac{Z_\beta(p||q) - 1}{\beta - 1}, \quad S_\beta(p||q) = -\frac{\log Z_\beta(p||q)}{\beta - 1}.$$

と表わされる.  $\beta > 1$  (もしくは  $\beta < 1$ ) の場合はどちらも  $Z_\beta(p||q)$  の単調減少函数 (もしくは単調増加函数) なので, それらを最大化することは  $Z_\beta(p||q)$  を最小化 (もしくは最大化) することと同値になる. さらに

$$e_{\beta-1}(x) = (1 + (\beta - 1)x)^{1/(\beta-1)}, \quad \ell_{\beta-1}(x) = \frac{x^{\beta-1} - 1}{\beta - 1}$$

が互いに相手の逆函数になることより,

$$Z_\beta(p||q)^{1/(\beta-1)} = e_{\beta-1}(-T_\beta(p||q)) = \exp(-S_\beta(p||q)).$$

この意味で相対 Tsallis エントロピーと相対 Rényi エントロピーの違いはちょうど  $e_{\beta-1}(x)$  と  $\exp(x)$  の違いになっている. もちろん, この事実は最初から

$$T_\beta(p||q) = -\ell_{\beta-1}(Z_\beta(p||q)^{1/(\beta-1)}), \quad S_\beta(p||q) = -\log(Z_\beta(p||q)^{1/(\beta-1)})$$

と書いておけば自明なのであるが.  $\square$

**注意 7.4** (負値性).  $p_i, q_i \geq 0$ ,  $\sum_{i=1}^r p_i = \sum_{i=1}^r q_i = 1$  であるとし,  $\beta > 0$  であると仮定する. 相対エントロピー, 相対 Rényi エントロピー, 相対 Tsallis エントロピーはそれぞれ

$$S(p||q) = -\sum_{i=1}^r p_i \log \frac{p_i}{q_i}$$

$$S_\beta(p||q) = -\frac{1}{\beta-1} \log \sum_{i=1}^r p_i^\beta q_i^{1-\beta},$$

$$T_\beta(p||q) = -\frac{\sum_{i=1}^r p_i^\beta q_i^{1-\beta} - 1}{\beta-1}$$

と定義されたのであった.  $\ell_{\beta-1}(x)$  を

$$\ell_{\beta-1}(x) = \frac{x^{\beta-1} - 1}{\beta-1}$$

と定めると, 相対 Tsallis エントロピーは

$$T_\beta(p||q) = -\sum_{i=1}^r p_i \ell_{\beta-1} \left( \frac{p_i}{q_i} \right)$$

と表わされる.  $S(p||q)$ ,  $S_\beta(p||q)$ ,  $T_\beta(p||q)$  がすべて 0 以下であることを示そう.

**相対エントロピー**  $f(x) = x \log x$  とおくと,  $f'(x) = \log x + 1$ ,  $f''(x) = 1/x$  より  $f(x)$  は下に凸な関数であり,  $f(1) = 0$ ,  $f'(1) = 1$  より,  $f(x) \geq x - 1$  となる. ゆえに

$$S(p||q) = -\sum_{i=1}^r f \left( \frac{p_i}{q_i} \right) q_i \leq -\sum_{i=1}^r \left( \frac{p_i}{q_i} - 1 \right) q_i = 0.$$

**相対 Tsallis エントロピー**  $g(x) = x \ell_{\beta-1}(x)$  とおくと,  $g'(x) = \ell_{\beta-1}(x) + x^{\beta-1}$ ,  $g''(x) = \beta x^{\beta-2}$  と  $\beta > 1$  より,  $g(x)$  は下に凸な関数であり,  $g(1) = 0$ ,  $g'(1) = 1$  より,  $g(x) \geq x - 1$  となる. ゆえに

$$T_\beta(p||q) = -\sum_{i=1}^r g \left( \frac{p_i}{q_i} \right) q_i \leq -\sum_{i=1}^r \left( \frac{p_i}{q_i} - 1 \right) q_i = 0. \quad (7.1)$$

**相対 Rényi エントロピー**  $\beta > 1$  という仮定より,  $S_\beta(p||q) \leq 0$  を示すためには

$$\sum_{i=1}^r p_i^\beta q_i^{1-\beta} = \sum_{i=1}^r \left( \frac{p_i}{q_i} \right)^\beta q_i \geq 1$$

を示せばよい.  $h(x) = x^\beta$  とおくと,  $h'(x) = \beta x^{\beta-1}$ ,  $h''(x) = \beta(\beta-1)x^{\beta-2}$  と  $\beta > 1$  より,  $h(x)$  は下に凸な関数であり,  $h(1) = 1$ ,  $h'(1) = \beta$  より  $h(x) \geq 1 + \beta(x-1)$  となる. ゆえに

$$\sum_{i=1}^r \left( \frac{p_i}{q_i} \right)^\beta q_i \geq \sum_{i=1}^r \left( 1 + \beta \left( \frac{p_i}{q_i} - 1 \right) \right) q_i = 1$$

これで示すべきことがすべて示された. 以上の議論において Jensen の不等式を使えばほんの少しだけ近道できる.  $\square$

## 7.4 加法性 (示量性) について

**注意 7.5** (加法性について).  $\nu = 1, 2$  に対する有限集合  $R_\nu = \{1, 2, \dots, r_\nu\}$  上の確率分布  $p_\nu = (p_{\nu,1}, \dots, p_{\nu,r_\nu})$ ,  $q_\nu = (q_{\nu,1}, \dots, q_{\nu,r_\nu})$  に対して, 相対エントロピーと相対 Rényi エントロピーは

$$S(p_\nu || q_\nu) = - \sum_{i=1}^{r_\nu} p_{\nu,i} \log \frac{p_{\nu,i}}{q_{\nu,i}},$$

$$S_\beta(p_\nu || q_\nu) = \frac{\log Z_\beta(p_\nu || q_\nu)}{1 - \beta}, \quad Z_\beta(p_\nu || q_\nu) = \sum_{i=1}^{r_\nu} p_{\nu,i}^\beta q_{\nu,i}^{1-\beta}$$

となる. 直積集合  $R_1 \times R_2 = \{(i, j) \mid i \in R_1, j \in R_2\}$  上の確率分布が  $(i, j) \mapsto p_{1,i} p_{2,j}$ ,  $(i, j) \mapsto q_{1,i} q_{2,j}$  によって定義される. この直積集合上の確率分布の組に対する相対エントロピーと相対 Rényi エントロピーの定義を書き下すと次のようになる:

$$S(p_1, p_2 || q_1, q_2) = - \sum_{i,j} p_{1,i} p_{2,j} \log \frac{p_{1,i} p_{2,j}}{q_{1,i} q_{2,j}},$$

$$S_\beta(p_1, p_2 || q_1, q_2) = \frac{\log Z_\beta(p_1, p_2 || q_1, q_2)}{1 - \beta}, \quad Z_\beta(p_1, p_2 || q_1, q_2) = \sum_{i,j} (p_{1,i} p_{2,j})^\beta (q_{1,i} q_{2,j})^{1-\beta}.$$

このとき次の加法性が成立している:

$$S(p_1, p_2 || q_1, q_2) = S(p_1 || q_1) + S(p_2 || q_2), \quad S_\beta(p_1, p_2 || q_1, q_2) = S_\beta(p_1 || q_1) + S_\beta(p_2 || q_2).$$

後者は

$$Z_\beta(p_1, p_2 || q_1, q_2) = Z_\beta(p_1 || q_1) Z_\beta(p_2 || q_2)$$

と同値である. 証明は以下の通り:

$$\begin{aligned} S(p_1, p_2 || q_1, q_2) &= - \sum_{i,j} p_{1,i} p_{2,j} \log \frac{p_{1,i}}{q_{1,i}} - \sum_{i,j} p_{1,i} p_{2,j} \log \frac{p_{2,j}}{q_{2,j}} \\ &= - \sum_i p_{1,i} \log \frac{p_{1,i}}{q_{1,i}} - \sum_j p_{2,j} \log \frac{p_{2,j}}{q_{2,j}} = S(p_1 || q_1) + S(p_2 || q_2), \\ Z_\beta(p_1, p_2 || q_1, q_2) &= \sum_{i,j} (p_{1,i} p_{2,j})^\beta (q_{1,i} q_{2,j})^{1-\beta} = \sum_{i,j} p_{1,i}^\beta q_{1,i}^{1-\beta} \cdot p_{2,j}^\beta q_{2,j}^{1-\beta} \\ &= \sum_i p_{1,i}^\beta q_{1,i}^{1-\beta} \cdot \sum_j p_{2,j}^\beta q_{2,j}^{1-\beta} = Z_\beta(p_1 || q_1) Z_\beta(p_2 || q_2). \end{aligned}$$

相対 Tsallis エントロピー

$$T_\beta(p_\nu || q_\nu) = \frac{Z_\beta(p_\nu || q_\nu) - 1}{1 - \beta}, \quad T_\beta(p_1, p_2 || q_1, q_2) = \frac{Z_\beta(p_1, p_2 || q_1, q_2) - 1}{1 - \beta}$$

は加法性を満たしていないが,

$$T_\beta(p_1, p_2 || q_1, q_2) = T_\beta(p_1 || q_1) + T_\beta(p_2 || q_2) + (1 - \beta) T_\beta(p_1 || q_1) T_\beta(p_2 || q_2)$$

を満たしている. 証明は次の通り:

$$T_\beta(p_1, p_2 || q_1, q_2) - T_\beta(p_1 || q_1) - T_\beta(p_2 || q_2)$$

$$\begin{aligned}
&= \frac{Z_\beta(p_1||q_1) Z_\beta(p_2||q_2) - 1 - (Z_\beta(p_1||q_1) - 1) - (Z_\beta(p_2||q_2) - 1)}{1 - \beta} \\
&= \frac{Z_\beta(p_1||q_1) Z_\beta(p_2||q_2) - Z_\beta(p_1||q_1) - Z_\beta(p_2||q_2) + 1}{1 - \beta} \\
&= \frac{(Z_\beta(p_1||q_1) - 1)(Z_\beta(p_2||q_2) - 1)}{1 - \beta} \\
&= (1 - \beta) T_\beta(p_1||q_1) T_\beta(p_2||q_2).
\end{aligned}$$

これは  $q$  数  $(x)_q = (1 - q^x)/(1 - q)$  に関する公式

$$(x + y)_q = (x)_q + (y)_q + (q - 1)(x)_q(y)_q$$

に似ている. Tsallis エントロピー<sup>19</sup> に関係した数学的構造に関する議論および文献については [6] を参照せよ. そこでは  $n \rightarrow \infty$  の漸近挙動に Tsallis エントロピーが現われる多項係数の類似物が扱われている.  $\square$

## 7.5 相対 Tsallis エントロピーを漸近挙動に含む多項分布の拡張 (1)

Suyari [6] は多項係数のある拡張の  $n \rightarrow \infty$  の漸近挙動が Tsallis エントロピーで記述されることを示した. 以下ではその結果を多項分布と相対 Tsallis エントロピーの場合に拡張する<sup>20</sup>. 以下では細かいことを気にせずに大雑把な素描を行なう.

以下ではパラメーター  $h$  とパラメーター  $\beta$  のあいだには

$$h = \beta - 1, \quad h + 1 = \beta$$

という関係があると仮定する. パラメーター  $h = \beta - 1$  による指数関数の拡張  $e_h(x)$  と対数関数の拡張  $\ell_h(x)$  を

$$e_h(x) = (1 + hx)^{1/h}, \quad \ell_h(x) = \frac{x^h - 1}{h}$$

と定める. これらは互いに相手の逆関数になっており,  $h \rightarrow 0$  ( $\beta \rightarrow 1$ ) で通常の指数関数と対数関数に収束する. この記号法を使うと, 第 7.3 節で導入した相対 Tsallis エントロピー  $T_\beta(p||q)$  を次のように表わせる<sup>21</sup>:

$$T_\beta(p||q) = - \sum_{i=1}^r p_i \ell_h \left( \frac{p_i}{q_i} \right).$$

なぜならば

$$- \sum_{i=1}^r p_i \ell_h \left( \frac{p_i}{q_i} \right) = - \frac{1}{h} \sum_{i=1}^r \left( p_i \left( \frac{p_i}{q_i} \right)^h - p_i \right) = - \frac{1}{\beta - 1} \sum_{i=1}^r (p_i^\beta q_i^{1-\beta} - p_i)$$

<sup>19</sup>相対 Tsallis エントロピーの定義で  $q_i = 1$  とすると Tsallis エントロピーの定義が得られる.

<sup>20</sup>ほぼ自明な拡張でしかない.

<sup>21</sup>これを相対 Tsallis エントロピーの定義だと思ってもよい. この形式の定義では, 相対 Tsallis エントロピー  $T_\beta(p||q)$  が相対エントロピー  $S(p||q) = - \sum_{i=1}^r p_i \log(p_i/q_i)$  のパラメーター  $h = \beta - 1$  による拡張になっていることが分かり易い.

$$= -\frac{\sum_{i=1}^r p_i^\beta q_i^{1-\beta} - 1}{\beta - 1} = \frac{1 - \sum_{i=1}^r p_i^\beta q_i^{1-\beta}}{\beta - 1} = T_\beta(p||q).$$

これが漸近挙動に現われるような多項分布の拡張を構成することが以下の目標である。  
通常が多項分布における確率は

$$a(n; k) = \frac{n!}{k_1 \cdots k_r} q_1^{k_1} \cdots q_r^{k_r} \quad (k = (k_1, \dots, k_r), k_i \geq 0, k_1 + \cdots + k_r = n)$$

であり, この対数は次のように表わされる:

$$\log a(n; k) = \sum_{\nu=1}^n \log \nu - \sum_{i=1}^r \sum_{\nu=1}^{k_i} \log \left( \frac{\nu_i}{q_i} \right).$$

これを拡張して次の条件によって  $\ell_h(a_h(n; k))$  を定義する:

$$\ell_h(a_h(n; k)) = \sum_{\nu=1}^n \ell_h(\nu) - \sum_{i=1}^r \sum_{\nu=1}^{k_i} \ell_h \left( \frac{\nu_i}{q_i} \right).$$

このとき, 右辺の  $\ell_h(x) = x^h/h - 1/h$  の中の  $-1/h$  の部分はキャンセルして消えるので,

$$\ell_h(a_h(n; k)) = \frac{1}{h} \left( \sum_{\nu=1}^n \nu^h - \sum_{i=1}^r \sum_{\nu=1}^{k_i} \left( \frac{\nu_i}{q_i} \right)^h \right) = \frac{1}{h} \left( \sum_{\nu=1}^n \nu^h - \sum_{i=1}^r q_i^{-h} \sum_{\nu=1}^{k_i} \nu_i^h \right).$$

$h > 0$  ( $\beta > 1$ ) と仮定し,  $n \rightarrow \infty$  で  $k_i/n$  はほぼ一定  $k_i = np_i + O(1) = n(p_i + O(1/n))$  という条件を仮定する.  $n \rightarrow \infty$  のとき  $\ell_h(a_h(n; k))$  がどのように振る舞うかを知りたい.  
 $h > 0$  と仮定したので,

$$\sum_{\nu=1}^r \nu^h = \frac{n^{h+1}}{h+1} + O(n^h) = \frac{n^\beta}{\beta} + O(n^{\beta-1}) \quad (n \rightarrow \infty).$$

さらに  $k_i = np_i + O(1)$  と仮定したので,

$$\sum_{\nu=1}^{k_i} \nu_i^h = \frac{(np_i)^{h+1}}{h+1} + O(n^h) = \frac{n^\beta}{\beta} p_i^\beta + O(n^{\beta-1}).$$

ゆえに

$$\ell_h(a_h(n; k)) = \frac{n^\beta}{\beta} \frac{1 - \sum_{i=1}^r p_i^\beta q_i^{1-\beta}}{\beta - 1} + O(n^{\beta-1}) = \frac{n^\beta}{\beta} T_\beta(p||q) + O(n^{\beta-1}) \quad (n \rightarrow \infty).$$

これが目標としていた結果である<sup>22</sup>. この結果は多項分布の漸近挙動

$$\log a(n; k) = \log \left( \frac{n!}{k_1! \cdots k_r!} q_1^{k_1} \cdots q_r^{k_r} \right) = nS(p||q) + O(\log n)$$

の拡張になっている.

<sup>22</sup>この結果 (もしくはその拡張) を使えば相対 Tsallis エントロピーの場合に関する Sanov の定理の拡張を証明できるだろう. しかし, 2016年6月23日の時点で筆者はパラメーター  $h = \beta - 1$  による多項分布の拡張  $a_h(n; k)$  が出て来る必然性を理解できていない.

## 7.6 相対 Tsallis エントロピーを漸近挙動に含む多項分布の拡張 (2)

Suyari-Scarfone [7] に第 7.6 節とは異なる多項分布の拡張の仕方が書いてあったので以下で紹介することにする. 第 7.6 節の  $a_h(n; k)$  以外の記号を引き継ぐ. 文献 [7] の  $q$  と第 7.6 節の  $h = \beta - 1$  は  $h = 1 - q$ ,  $h + 1 = \beta = 2 - q$  によって対応している.

函数  $e_h(x)$  とその逆函数を  $\ell_h(x)$  を

$$e_h(x) = (1 + hx)^{1/h} > 0 \quad \left(x > -\frac{1}{h}\right), \quad \ell_h(x) = \frac{x^h - 1}{h} > -\frac{1}{h} \quad (x > 0)$$

と定めると相対 Tsallis エントロピーは

$$T_\beta(p||q) = \frac{1 - \sum_{i=1}^r p_i^\beta q_i^{1-\beta}}{\beta - 1} = \frac{1}{h} \left(1 - \sum_{i=1}^r p_i^{h+1} q_i^{-h}\right) = -\sum_{i=1}^r p_i \ell_h\left(\frac{p_i}{q_i}\right)$$

と表わせるのであった.

多項分布における確率は

$$a(n; k) = \frac{n!}{k_1 \cdots k_r} q_1^{k_1} \cdots q_r^{k_r} \quad (k = (k_1, \dots, k_r), k_i \geq 0, k_1 + \cdots + k_r = n)$$

であり, これの対数は次のように表わされる:

$$\log a(n; k) = \sum_{\nu=1}^n \log \nu - \sum_{i=1}^r \left( \sum_{\nu_i=1}^{k_i} \log \nu_i + k_i \log q_i^{-1} \right).$$

この節ではこれを拡張して  $\ell_h(a_h(n; k))$  を次のように定義する<sup>23</sup>:

$$\ell_h(a_h(n; k)) = \sum_{\nu=1}^n \ell_h(\nu) - \sum_{i=1}^r \left( \sum_{\nu_i=1}^{k_i} \ell_h(\nu_i) + \frac{k_i^{h+1}}{h+1} \ell_h(q_i^{-1}) \right).$$

これは次のように書き直される:

$$\ell_h(a_h(n; k)) = \frac{1}{h} \left( \sum_{\nu=1}^n \nu^h - \sum_{i=1}^r \left( \sum_{\nu_i=1}^{k_i} \nu_i^h + \frac{k_i^{h+1}}{h+1} (q_i^{-h} - 1) \right) \right).$$

$h > 0$  ( $\beta > 1$ ) と仮定し,  $n \rightarrow \infty$  で  $k_i/n$  はほぼ一定  $k_i = np_i + O(1) = n(p_i + O(1/n))$  という条件を仮定する.  $n \rightarrow \infty$  のとき  $\ell_h(a_h(n; k))$  がどのように振る舞うかを知りたい.  $h > 0$  と仮定したので,

$$\sum_{\nu=1}^r \nu^h = \frac{n^{h+1}}{h+1} + O(n^h) = \frac{n^\beta}{\beta} + O(n^{\beta-1}) \quad (n \rightarrow \infty).$$

さらに  $k_i = np_i + O(1)$  と仮定したので,

$$\sum_{\nu_i=1}^{k_i} \nu_i^h = \frac{(np_i)^{h+1}}{h+1} + O(n^h) = \frac{n^\beta}{\beta} p_i^\beta + O(n^{\beta-1}),$$

<sup>23</sup>2016年7月6日現在, この定義の必然性を筆者は理解できていない.

$$\frac{k_i^{h+1}}{h+1} = \frac{(np_i)^{h+1}}{h+1} + O(n^h) = \frac{n^\beta}{\beta} p_i^\beta + O(n^{\beta-1}).$$

そして  $q_i^{-h} = q_i^{1-\beta}$  である. ゆえに,  $n \rightarrow \infty$  において,

$$\ell_h(a(n; k)) = \frac{1}{h} \left( \frac{n^\beta}{\beta} - \sum_{i=1}^r \frac{n^\beta}{\beta} p_i^\beta q_i^{1-\beta} \right) + O(n^{\beta-1}) = \frac{n^\beta}{\beta} T_\beta(p||q) + O(n^{\beta-1}).$$

これが目標としていた結果である. この結果は多項分布の漸近挙動

$$\log a(n; k) = \log \left( \frac{n!}{k_1! \cdots k_r!} q_1^{k_1} \cdots q_r^{k_r} \right) = nS(p||q) + O(\log n)$$

の拡張になっている.

## 8 付録: 上極限と下極限に関する簡単な解説

上極限  $\limsup$  と下極限  $\liminf$  は収束先として  $\pm\infty$  を許せば常に収束するので, 収束するかどうかわからない実数列の漸近挙動を調べるときにとっても便利である.

数学科の学生であれば上極限と下極限についても講義で習っていてよく知っているだろうが, 他学科の出身者は詳しく習ったことがないかもしれない. だから, この付録で上極限と下極限について簡単に解説しておくことにした.

### 8.1 上極限と下極限の定義

$a_1, a_2, \dots$  は実数列であるとする.

$a_n, a_{n+1}, a_{n+2}, \dots$  の上限  $\sup_{k \geq n} a_k$  を

$$\sup_{k \geq n} a_k = (\text{すべての } a_n, a_{n+1}, a_{n+2}, \dots \text{ 以上の } \alpha \text{ の中で最小のもの}).$$

ただし  $\alpha$  は実数または  $\infty$  であるとする<sup>24</sup>:

$$\sup_{k \geq n} a_k = \min\{ \alpha \in \mathbb{R} \cup \{\infty\} \mid a_k \leq \alpha \ (k \geq n) \}.$$

一般により小さな実数の集合の上限は小さくなるので  $n$  に関する数列  $\sup_{k \geq n} a_k$  は単調減少数列になる. したがって, 数列  $\sup_{k \geq n} a_k$  は  $n \rightarrow \infty$  で実数または  $\pm\infty$  に収束する<sup>25</sup>. その収束先を実数列  $a_n$  の上極限 (limit superior) と呼び, 次のように表わす:

$$\limsup a_n = \lim_{n \rightarrow \infty} \sup_{k \geq n} a_k.$$

同様に下極限 (limit inferior) を次のように定義する:

$$\inf_{k \geq n} a_k = \max\{ \alpha \in \mathbb{R} \cup \{-\infty\} \mid a_k \geq \alpha \ (k \geq n) \},$$

<sup>24</sup> 上限の存在は実数の連続性によって保証される. 上限が常に存在することを実数の連続性そのものだと思ってもよい.

<sup>25</sup> 収束することも実数の連続性によって保証される.



$$\liminf_{n \rightarrow \infty} a_n = \lim_{n \rightarrow \infty} \inf_{k \geq n} a_k.$$

上限  $\sup$  は下限  $\inf$  以上なので上極限と下極限は次の不等式を満たしている:

$$\liminf_{n \rightarrow \infty} a_n \leq \limsup_{n \rightarrow \infty} a_n.$$

実数列  $a_n$  が収束するならば,  $\sup_{k \geq n} a_k$  と  $\inf_{k \geq n} a_k$  の差は 0 に収束するので,

$$\liminf_{n \rightarrow \infty} a_n = \limsup_{n \rightarrow \infty} a_n = \lim_{n \rightarrow \infty} a_n$$

が成立する. 逆に  $\limsup_{n \rightarrow \infty} a_n$  と  $\liminf_{n \rightarrow \infty} a_n$  が一致するならば実数列  $a_n$  はそれらと同じ値に収束することもわかる.

**例 8.1** (上極限と下極限の例). 以下が成立していることを定義に基づいて確認してみよ:

$$\begin{aligned} \limsup_{n \rightarrow \infty} (-1)^n &= 1, & \liminf_{n \rightarrow \infty} (-1)^n &= -1, \\ \limsup_{n \rightarrow \infty} ((-1)^n n) &= \infty, & \liminf_{n \rightarrow \infty} ((-1)^n n) &= -\infty, \\ \limsup_{n \rightarrow \infty} ((-1)^n (1 + 2^{-n})) &= 1, & \liminf_{n \rightarrow \infty} ((-1)^n (1 + 2^{-n})) &= -1. \end{aligned}$$

これらの上極限と下極限を図を描いて確認すれば上極限と下極限の概念を直観的に理解できると思う. □

## 8.2 上極限と下極限の使い方

上極限と下極限の典型的な使い方について説明しよう. 数列  $a_n$  の  $n \rightarrow \infty$  での様子を知りたいとしよう. 数列  $a_n$  が  $n \rightarrow \infty$  で収束する量  $B_n, C_n$  によって

$$B_n \leq a_n \leq C_n$$

と評価されたとする (はさみうち!). このとき  $n \rightarrow \infty$  で次が成立する:

$$\lim_{n \rightarrow \infty} B_n \leq \liminf_{n \rightarrow \infty} a_n \leq \limsup_{n \rightarrow \infty} a_n \leq \lim_{n \rightarrow \infty} C_n.$$

この評価は実数列  $a_n$  が収束していなくても成立する. もしも  $B_n$  と  $C_n$  が同じ値に収束するならば, この不等式より  $a_n$  もそれらと同じ値に収束することがわかる.

以上の議論のパターンを知っていれば,  $a_n$  が収束するとは限らない弱い条件のもとで上極限と下極限に関する不等式を示しておいて, 追加の強い条件のもとで  $a_n$  が収束することを示せるようになる. Sanov の定理の定式化と証明に関する第 3 節の議論はまさにそのようなタイプの議論の典型例になっている.