Rényi 信息合并的链式法则

Christoph Hirche*†、Xinyue Guan‡、Marco Tomamichel†§
*数学中心，慕尼黑工业大学，85748 加兴，德国
†量子技术中心，新加坡国立大学，新加坡
‡立化中学，新加坡§电气与计算机工程系，新加坡国立大学，新加坡

arXiv:2305.02589v1 [cs.IT] 4 May 2023

摘要

信息合并界是编码理论中的一项基础工具，尤其适用于分析极化码和置信传播。它们通常根据香农熵来界定随机变量的演变。近期的研究将这一方法推广到了 Rényi α-熵。然而，由于 Rényi 熵缺乏传统的链式法则，相关理论仍不完整。本文通过给出 Rényi 链式法则，建立了这一缺失的联系，将 Hayashi 和 Arimoto 提出的不同 Rényi 熵定义联系起来。这使我们得以为 Arimoto Rényi 熵给出新的信息合并界。在第二部分，我们将链式法则推广到量子情形，并说明如何借此推广先前仅针对冯·诺伊曼熵提出的结果和猜想。在 $\alpha = 2$ 的特殊情形下，我们给出了首个针对量子侧信息的最优信息合并界。

I. 引言

信息论中的许多任务都涉及随机变量及其相应熵在某些“合并操作”下的演变。一个尤为相关的操作例子是将两个相互独立的随机变量（取值于某个群中）相加。在这种情况下，由于我们知道两个随机变量之和的概率分布对应于各个随机变量概率分布的卷积，因此可以轻松计算其熵。当随机变量带有侧信息时，情况就不同了。此时，我们关心的是在给定所有可用侧信息的条件下，随机变量之和的熵。对此进行计算要困难得多。信息合并界 这一领域致力于寻找对所得条件熵的最优熵界。

一个特别重要的情形是具有任意有限维侧信息的两个二元随机变量。这正是本文将要研究的情形，因为它在许多领域都有应用，例如极化码的编码理论 [1] 和香农理论 [5], [13]。Wyner 和 Ziv 在 [18], 著名的 *Gerber* 夫人引理 中给出了所得香农熵的一个最优下界。在这一结果之后，人们提出了其他解决该问题的方法，这些方法还得出了组合随机变量的条件熵的一个上 界。例如， [13] 中给出了一种证明方法、若干其他应用以及最优上界。

在这项工作中，我们讨论将这些信息合并界推广至 Rényi 熵。虽然无条件 Rényi 熵有着明确的定义，但文献中存在许多不同的条件 Rényi 熵定义。我们重点关注其中两种，即 H_α^H和 H_α^A，它们表现出尤为优良的性质。最近，关于最优界的研究成果...

$$H_\alpha^*(X_1 + X_2|Y_1Y_2) \tag{I.1}$$

已在 [8] 中展示。这对应于置信传播中校验节点的熵，或极化编码中的较差信道。然而，对于许多应用，例如编码理论，还需要对互补熵给出界。

$$H_\alpha^*(X_2|X_1 + X_2, Y_1Y_2), \tag{I.2}$$

这对应于变量节点或更优的信道。在香农熵的情况下，即 $\alpha = 1$，可以利用众所周知的条件熵链式法则，将关于第一个熵的界转换为关于第二个熵的界。然而，一般而言，对于所考虑的 Rényi 熵，并不存在这样简洁的链式法则。本工作的核心主题是一些等式，它们可以发挥信息合并链式法则的作用。正如我们将看到的，这些 Rényi 熵链式法则直接关联 H_α^H和 H_α^A，其含义是可以直接在它们之间转换界。

$$H_\alpha^H(X_1 + X_2|Y_1Y_2) \quad \text{and} \quad H_\alpha^A(X_2|X_1 + X_2, Y_1Y_2). \tag{I.3}$$

乍看之下，这种联系可能令人感到意外，不过我们随后将会看到，在量子信息论的框架下，这种联系显得更加自然。

信息合并的界这一主题在 [9] 中得到了推广，以纳入量子侧信息。在 [9] 中给出了关于 $H(X_1 + X_2|Y_1Y_2)$ 的非最优下界，并讨论了量子极化码 [7], [12], [17] 的一项应用。此外，还提出了一个猜想，即最优下界和上界是经典界的对称化版本。将冯·诺依曼熵的链式法则与对偶信道的概念结合起来， [10]–[12]结果表明，这种对称性实际上是任何最优冯·诺伊曼界在量子情形下的一个基本特征。量子情形

由于我们尚未充分理解如何处理以量子侧信息为条件的情况，因此这本质上更为困难。

将先前结果推广到Rényi 熵时，另一个困难在于：尽管我们已经知道条件Rényi熵的若干经典版本，但在量子情形下可选的定义却多得多。在本文中，我们主要考虑扩展 $\widetilde{H}_\alpha^\downarrow$ 和 $\bar{H}_\alpha^\uparrow$，并将看到它们满足许多理想性质，其中包括 Rényi 熵链式法则的量子推广。随后，冯·诺伊曼情形的若干性质也可延伸到Rényi情形，包括最优界的对称性以及这种联系

$$\widetilde{H}_\alpha^\downarrow(X_1+X_2|Y_1Y_2) \longleftrightarrow \bar{H}_\alpha^\uparrow(X_2|X_1+X_2,Y_1Y_2). \tag{I.4}$$

最后，我们为一些特殊情形给出最优界，并对一般 α的最优界提出猜想。在附录中，我们讨论数值证据，也涉及其他条件Rényi熵。所有技术性证明也均在附录中给出。

先前结果： 在开始之前，我们将简要回顾 [8]中的一些核心结果。这些结果既将作为比较基准，之后也会作为工具使用。为简便起见，我们在此陈述 [8, 定理IV.8与引理IV.10] 的一个组合，适用于 H_α^H，其定义将在(II.1)中精确给出。在下文中，我们将二元 Rényi熵记作 h_α。

定理 I.1 (H_α^HBSC 界 [8])。对于 $\alpha\in(0,2]\cup[3,\infty)$,

$$H_\alpha^H(X_1+X_2|Y_1Y_2)\geq h_\alpha(h_\alpha^{-1}(H_\alpha^H(X_1|Y_1))*h_\alpha^{-1}(H_\alpha^H(X_2|Y_2))). \tag{I.5}$$

对于 $\alpha\in[2,3]$，将 $\geq$ 与 $\leq$交换后结论同样成立。注意，对于 $\alpha\in\{2,3\}$，上述结论取等号。这些界是紧的，即二元对称信道能够达到等号。

我们定义 $\delta_\alpha := 2^{1-\alpha}$ 和 $K_\alpha^*(X|Y) := e^{(1-\alpha)H_\alpha^*(X|Y)}$。结合 [8, 定理 IV.9 和引理 IV.10]，我们得到以下结果。

定理 I.2 (H_α^HBEC 界 [8])对于 $\alpha\in(0,2]\cup[3,\infty)$,

$$H_\alpha^H(X_1+X_2|Y_1Y_2)\leq\frac{1}{1-\alpha}\log\frac{(\delta_\alpha-K_\alpha^H(X_1|Y_1))(\delta_\alpha-K_\alpha^H(X_2|Y_2))}{1-\delta_\alpha}+\delta_\alpha. \tag{I.6}$$

对于 $\alpha\in[2,3]$，将 $\geq$ 与 $\leq$互换后，同样成立。请注意，对于 $\alpha\in\{2,3\}$，上述结论取等号。这些界是紧的，因为二元擦除信道可以达到等号。

Arimoto条件熵也有类似的结果， [8]中也可以找到相关内容。

II. Classical Rényi entropies

本节将正式定义所考虑的经典 Rényi 熵，并给出一些重要性质。主要定义为：

$$H_\alpha^H(X|Y)_p := \frac{1}{1-\alpha}\log\sum_y\sum_x p(y)p(x|y)^\alpha \tag{II.1}$$

$$H_\alpha^A(X|Y)_p := \frac{\alpha}{1-\alpha}\log\sum_y p(y)\left(\sum_x p(x|y)^\alpha\right)^{\frac{1}{\alpha}}, \tag{II.2}$$

其中，第一个最早由 Hayashi 和 Skoric 等人 [6], [14] 讨论，第二个则由 Arimoto [3]提出。对于后者，我们通常将 α取倒数，

$$H_{\frac{1}{\alpha}}^A(X|Y)_p=\frac{1}{\alpha-1}\log\sum_y p(y)\left(\sum_x p(x|y)^{\frac{1}{\alpha}}\right)^\alpha. \tag{II.3}$$

有：

$$\lim_{\alpha\to1}H_\alpha^*(X|Y)=H(X|Y). \tag{II.4}$$

文献中还给出了几种条件 Rényi 熵的定义，其中一些已被用于研究信息合并界 [8]。然而，我们在此选用的定义是其中唯一满足单调性的定义，

$$H_\alpha^*(X|YZ)\leq H_\alpha^*(X|Z). \tag{II.5}$$

遗憾的是，这两种定义都不满足传统的链式法则，这意味着一般而言

$$H_\alpha^*(X|YZ) \neq H_\alpha^*(XY|Z) - H_\alpha^*(Y|Z). \tag{II.6}$$

然而，在考虑信息合并时，可以证明以下观察结果能够取代传统的链式法则。

引理 II.1（经典 Rényi 链式法则）。设 $p(x,y)$ 和 $\bar{p}(x,y)$ 是满足以下关系的联合概率分布，

$$\bar{p}(x,y) = \frac{p(x|y)^\alpha p(y)}{\sum_{x,y} p(x|y)^\alpha p(y)}, \tag{II.7}$$

then

$$H_\alpha^H(X|Y)_p = H_{\frac{1}{\alpha}}^A(X|Y)_{\bar{p}}. \tag{II.8}$$

类似地，设

$$\hat{p}(x,y,z) = \frac{p(z)p(x,y|z)^\alpha}{\sum_{x,y,z} p(z)p(x,y|z)^\alpha}, \tag{II.9}$$

then

$$H_\alpha^H(XY|Z)_p = H_{\frac{1}{\alpha}}^A(X|YZ)_{\hat{p}} + H_\alpha^H(Y|Z)_p \tag{II.10}$$

$$= H_{\frac{1}{\alpha}}^A(XY|Z)_{\hat{p}}. \tag{II.11}$$

注意，前一个引理中的关系都是双射。例如，公式 (B.1) 的逆映射为

$$p(x,y) = \bar{p}(x|y)^{\frac{1}{\alpha}}\bar{p}(y)\frac{\left(\sum_x \bar{p}(x|y)^{\frac{1}{\alpha}}\right)^{\alpha-1}}{\sum_y \bar{p}(y)\left(\sum_x \bar{p}(x|y)^{\frac{1}{\alpha}}\right)^\alpha}. \tag{II.12}$$

或许令人意外的是，这些新法则将所讨论的两类条件熵结合在了一起。下一节我们将讨论它们在信息合并中的应用。随后，在考虑量子侧信息时，我们会看到，从某种意义上说，这两种熵实际上互为对偶，从而在这一更一般的情形下建立起一种自然联系。

III. RÉNYI INFORMATION COMBINING BOUNDS

我们首先明确所考虑的设定。给定两个联合概率分布 $p_1(x_1, y_1)$ 和 $p_2(x_2, y_2)$，我们将它们与信道相关联

$$W_1 \sim p_1(x_1, y_1), \tag{III.1}$$

$$W_2 \sim p_2(x_2, y_2), \tag{III.2}$$

省略输入变量，并且我们经常使用以下记法

$$H_\alpha^*(W_i) = H_\alpha^*(X_i|Y_i)_{p_i}. \tag{III.3}$$

这里，我们考虑通过异或运算进行信息合并，同时保留 X_2 的一个副本。记 $Z = X_1 + X_2$，则合并后的概率为

$$p(z, x_2, y_1, y_2) = p_1(z \oplus x_2, y_1)p_2(x_2, y_2). \tag{III.4}$$

Fr根据该分布，我们可以合成两个不同的组合信道，其对应的熵为

$$H_\alpha^*(W_1 \boxplus W_2) = H_\alpha^*(X_1 + X_2|Y_1Y_2)_p \tag{III.5}$$

$$H_\alpha^*(W_1 \circledast W_2) = H_\alpha^*(X_2|X_1 + X_2, Y_1Y_2)_p. \tag{III.6}$$

这些合成信道在例如著名的极化码 [2] 中发挥着核心作用。为了评估这些信道组合所导致的熵变化，我们关注如何用原始的 $H_\alpha^*(W_i)$ 来界定上述量。这类界在 $\alpha = 1$ 的情况下早已广为人知。此外，$H_\alpha^*(W_1 \boxplus W_2)$ 的界最近也已在 [8] 中针对 H_α^* 的几种不同取值得到证明。

由于众所周知的链式法则，$\alpha = 1$ 界的 $H(W_1 \circledast W_2)$ 可以很容易地由 $H(W_1 \boxplus W_2)$ 的界得到。具体而言，我们有

$$H(X_2|X_1 + X_2, Y_1Y_2) + H(X_1 + X_2|Y_1Y_2) \tag{III.7}$$

$$= H(X_1 + X_2, X_2|Y_1Y_2) \tag{III.8}$$
$$= H(X_1, X_2|Y_1Y_2) = H(X_1|Y_1) + H(X_2|Y_2), \tag{III.9}$$

这也可以等价地写成

$$H(W_1 \circledast W_2) + H(W_1 \boxtimes W_2) = H(W_1) + H(W_2). \tag{III.10}$$

链式法则还意味着，合并操作（如极化码）能够保持整体熵不变；这是证明极化码达到信道容量的关键性质 [2]。然而，将香农熵替换为 Rényi 熵后，通常不再成立如此简洁的链式法则。不过，我们可以改用上一节提出的新链式法则。

引理 III.1 (信息合并链式法则)。给定信道 W_1 和 W_2，存在信道 W_1' 和 W_2'，满足$H_\alpha^H(W_i) = H_1^A(W_i')_\alpha$

$$H_\alpha^H(W_1) + H_\alpha^H(W_2) = H_{\frac{1}{\alpha}}^A(W_1' \circledast W_2') + H_\alpha^H(W_1 \boxtimes W_2). \tag{III.11}$$

更具体地说，这些信道由下式给出

$$W_i' \sim \bar{p}_i(x_i, y_i) = \frac{p_i(x_i|y_i)^\alpha p_i(y_i)}{\sum_{x,y} p_i(x_i|y_i)^\alpha p_i(y_i)}. \tag{III.12}$$

利用这条新链式法则，我们可以证明关于 Arimoto Rényi 熵的新信息合并界。值得注意的是，证明使用了 Hayashi Rényi 熵，但最终结果仅用 Arimoto 熵表示。

定理 III.2. 对于 $\alpha \in (0, \frac{1}{3}] \cup [\frac{1}{2}, \infty)$，有

$$H_\alpha^A(X_2|X_1 + X_2, Y_1Y_2) \leq H_\alpha^A(X_1|Y_1) + H_\alpha^A(X_2|Y_2) - h_{\frac{1}{\alpha}}(h_{\frac{1}{\alpha}}^{-1}(H_\alpha^A(X_1|Y_1)) * h_{\frac{1}{\alpha}}^{-1}(H_\alpha^A(X_2|Y_2))). \tag{III.13}$$

对于 $\alpha \in [\frac{1}{3}, \frac{1}{2}]$，将 $\leq$ 换成 $\geq$ 时，同样成立。注意，对于 $\alpha \in \{\frac{1}{3}, \frac{1}{2}\}$，上述结论取等号。这些界是紧的，因为二元对称信道可以达到等号。

对于下一个结果，回顾一下 $\delta_{\frac{1}{\alpha}} = 2^{\frac{\alpha-1}{\alpha}}$ 和 $K_{\frac{1}{\alpha}}^*(X|Y) := e^{\frac{\alpha-1}{\alpha} H_\alpha^*(X|Y)}$。

定理 III.3。对于 $\alpha \in (0, \frac{1}{3}] \cup [\frac{1}{2}, \infty)$，有

$$H_\alpha^A(X_2|X_1 + X_2, Y_1Y_2) \geq H_\alpha^A(X_1|Y_1) + H_\alpha^A(X_2|Y_2) - \frac{\alpha}{\alpha - 1} \log \frac{(\delta_{\frac{1}{\alpha}} - K_{\frac{1}{\alpha}}^A(X_1|Y_1))(\delta_{\frac{1}{\alpha}} - K_{\frac{1}{\alpha}}^A(X_2|Y_2))}{1 - \delta_{\frac{1}{\alpha}}} + \delta_{\frac{1}{\alpha}}. \tag{III.14}$$

对于 $\alpha \in [\frac{1}{3}, \frac{1}{2}]$，将 $\geq$ 换成 $\leq$ 时，同样成立。注意，对于 $\alpha \in \{\frac{1}{3}, \frac{1}{2}\}$，上述结论取等号。这些界是紧的，因为二元擦除信道可以达到等号。

IV. Quantum Rényi entropies

现在我们讨论上述结果向量子情形的推广。从本质上说，量子态 ρ_A，即归一化的半正定矩阵，起到了概率的作用。现在考虑以下熵，参见例如 [15],

$$\widetilde{H}_\alpha^\downarrow(A|B)_\rho = \frac{1}{1-\alpha} \log \mathrm{Tr}\left(\rho_B^{\frac{1-\alpha}{2\alpha}} \rho_{AB} \rho_B^{\frac{1-\alpha}{2\alpha}}\right)^\alpha \tag{IV.1}$$
$$\bar{H}_\alpha^\uparrow(A|B)_\rho = \frac{\alpha}{1-\alpha} \log \mathrm{Tr}\left((\mathrm{Tr}_A \rho_{AB}^\alpha)^{\frac{1}{\alpha}}\right). \tag{IV.2}$$

这两种熵通过对偶关系 [16], 相联系，该关系指出，对于纯态 Ψ_{ABC},

$$\widetilde{H}_\alpha^\downarrow(A|B)_\Psi = -\bar{H}_{1/\alpha}^\uparrow(A|C)_\Psi. \tag{IV.3}$$

此外，对于经典态 ρ_{XY}，这些熵会简化为前文各节讨论的形式,

$$\widetilde{H}_\alpha^\downarrow(X|Y)_\rho = H_\alpha^H(X|Y)_p, \tag{IV.4}$$
$$\bar{H}_\alpha^\uparrow(X|Y)_\rho = H_\alpha^A(X|Y)_p. \tag{IV.5}$$

与经典情形类似，传统的链式法则并不成立。不过，当允许链式法则中出现两个熵时，我们可以证明如下结论。

引理 IV.1 (量子 Rényi 链式法则)。 设 ρ_{AB} 和 $\bar{\rho}_{AB}$ 为满足以下关系的量子态:

$$\bar{\rho}_{AB} = \frac{\left(\rho_B^{\frac{1-\alpha}{2\alpha}} \rho_{AB} \rho_B^{\frac{1-\alpha}{2\alpha}}\right)^\alpha}{\mathrm{Tr}\left(\rho_B^{\frac{1-\alpha}{2\alpha}} \rho_{AB} \rho_B^{\frac{1-\alpha}{2\alpha}}\right)^\alpha}, \tag{IV.6}$$

then

$$\widetilde{H}_\alpha^\downarrow(A|B)_\rho = \bar{H}_{\frac{1}{\alpha}}^\uparrow(A|B)_{\bar{\rho}}. \tag{IV.7}$$

此外，如果

$$\widetilde{\rho}_{ABC} = \frac{\left(\rho_C^{\frac{1-\alpha}{2\alpha}} \rho_{ABC} \rho_C^{\frac{1-\alpha}{2\alpha}}\right)^\alpha}{\mathrm{Tr}\left(\rho_C^{\frac{1-\alpha}{2\alpha}} \rho_{ABC} \rho_C^{\frac{1-\alpha}{2\alpha}}\right)^\alpha}, \tag{IV.8}$$

then

$$\widetilde{H}_\alpha^\downarrow(AB|C)_\rho = \bar{H}_{\frac{1}{\alpha}}^\uparrow(A|BC)_{\widetilde{\rho}} + \widetilde{H}_\alpha^\downarrow(B|C)_\rho = \bar{H}_{\frac{1}{\alpha}}^\uparrow(AB|C)_{\widetilde{\rho}}. \tag{IV.9}$$

另一个 Rén [4, 中的定理 3.2] 最近证明了链式法则的一般化形式，其中作者表明 w

$$\widetilde{H}_\alpha^\downarrow(AB|C)_\rho = \widetilde{H}_\alpha^\downarrow(A|BC)_{\widehat{\rho}} + \widetilde{H}_\alpha^\downarrow(B|C)_\rho, \tag{IV.10}$$

其中 $\widehat{\rho}$ 定义于 [4, 公式 (13)]。然而，在这种表述中，我们尚不清楚 $\widehat{\rho}$ 是否像在我们的链式法则中那样，代表一种有意义的信息合并操作。

V. 量子侧信息的信息合并

我们沿用该基因 [9]的一般设定。简言之，我们将经典-量子信道与经典-量子态联系起来。

$$W_1 \sim \rho_1^{X_1 B_1} \tag{V.1}$$

$$W_2 \sim \rho_2^{X_2 B_2}, \tag{V.2}$$

其中

$$\rho_i^{X_i B_i} = \frac{1}{2}|0\rangle\langle 0| \otimes \sigma_0^{B_i} + \frac{1}{2}|1\rangle\langle 1| \otimes \sigma_1^{B_i} \tag{V.3}$$

并且我们经常使用以下记号

$$H_\alpha(W_i) = H_\alpha(X_i|B_i)_{\rho_i}. \tag{V.4}$$

对经典系统应用 CNOT门后，我们得到联合状态

$$\tau^{(X_1+X_2)X_2B_1B_2} \tag{V.5}$$

$$= \sum_{z,x_2} \frac{1}{4}|z \oplus x_2\rangle\langle z \oplus x_2| \otimes |x_2\rangle\langle x_2| \otimes \sigma_z^{B_1} \otimes \sigma_{x_2}^{B_2}. \tag{V.6}$$

我们首先给出信息合并的链式法则。

引理 V.1 （信息合并链式法则）。 给定信道 W_1和 W_2，存在信道 W_1'和 W_2'，使得 $\widetilde{H}_\alpha^\downarrow$（$W_i$） = $\bar{H}_{\perp}^\uparrow$ W_i' （），使得$_\alpha$

$$\widetilde{H}_\alpha^\downarrow(W_1) + \widetilde{H}_\alpha^\downarrow(W_2) = \bar{H}_{\frac{1}{\alpha}}^\uparrow(W_1' \circledast W_2') + \widetilde{H}_\alpha^\downarrow(W_1 \boxtimes W_2). \tag{V.7}$$

更准确地说，这些信道由下式给出

$$W_i' \sim \bar{\rho}_{X_i B_i} = \frac{\left(\rho_{B_i}^{\frac{1-\alpha}{2\alpha}} \rho_{X_i B_i} \rho_{B_i}^{\frac{1-\alpha}{2\alpha}}\right)^\alpha}{\mathrm{Tr}\left(\rho_{B_i}^{\frac{1-\alpha}{2\alpha}} \rho_{X_i B_i} \rho_{B_i}^{\frac{1-\alpha}{2\alpha}}\right)^\alpha}. \tag{V.8}$$

我们还需要用到 [10]–[12] 中讨论的对偶性概念。基本上，对于每个 W，都有一个 $W^\perp$，满足 $H(W) = \log 2 - H^\perp(W^\perp)$，其中 $H^\perp$ 是按照公式 (IV.3) 定义的 H 的对偶熵。特别地，还有 $H(W_1 \boxtimes W_2) = \log 2 - H^\perp(W_1^\perp \circledast W_2^\perp)$。关于信息合并背景下对偶性质的概述，也请参见 [9]。

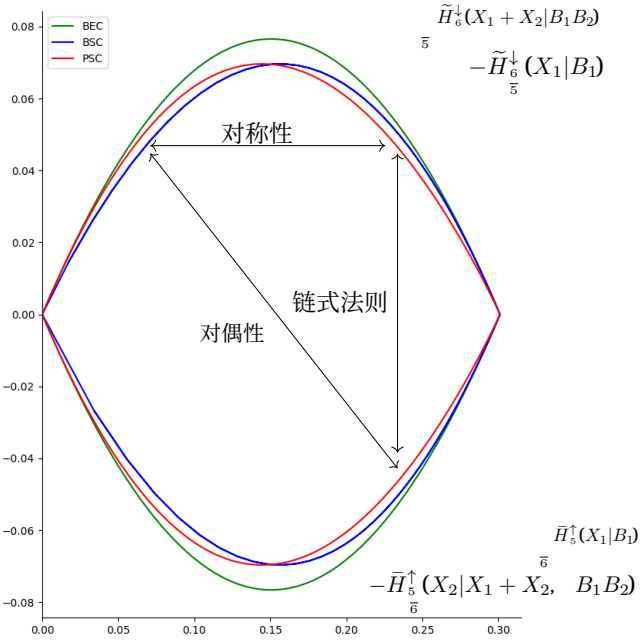


图 1：具有量子侧信息的设置。该图展示了在存在概率分布的点之间进行转换的三个规则：对偶性、对称性和链式法则。其中任意两个规则都可用于证明第三个规则。图中绘制的是二元擦除信道（BEC）、二元对称信道（BSC）和纯态信道（PSC）关于两个相互对偶的信息合并熵的界。我们考虑 $W_1 = W_2$，并在横轴上绘制合并前各个单独熵的取值。

对偶性的概念结合上文所示的链式法则，使我们能够推导出信息合并界的一些性质。

引理 V.2（对称性）。给定信道 W_1 和 W_2，存在信道 $\bar{W}_1$ 和 $\bar{W}_2$，满足 $H(W_i) = \log 2 - H(\bar{W}_i)$，使得

$$\begin{aligned} &\widetilde{H}^{\downarrow}_{\alpha}(W_1 \boxtimes W_2) - \frac{1}{2}\Big(\widetilde{H}^{\downarrow}_{\alpha}(W_1) + \widetilde{H}^{\downarrow}_{\alpha}(W_2)\Big) \\ &= \widetilde{H}^{\downarrow}_{\alpha}(\bar{W}_1 \boxtimes \bar{W}_2) - \frac{1}{2}\Big(\widetilde{H}^{\downarrow}_{\alpha}(\bar{W}_1) + \widetilde{H}^{\downarrow}_{\alpha}(\bar{W}_2)\Big). \end{aligned} \tag{V.9}$$

由此可知，最优的下界和上界必然具有对称性。对于 $\alpha = 1$而言，这一性质此前已为人所知，而新的链式法则为将这一结果扩展到 Rényi 熵提供了缺失的纽带。对称性、对偶性与链式法则之间的相互作用如图 1 所示。

A. 特殊情形：$\alpha = 2$

根据经典结果以及量子问题的对称性，$\alpha = 2$ 情形的解似乎应当特别简单。我们现在将看到，事实确实如此。I

t is well k已知 t hat

$$\widetilde{H}^{\downarrow}_{2}(X|B) = -\log P^{\mathrm{pg}}_{\mathrm{guess}}(X|B), \tag{V.10}$$

其中，$P^{\mathrm{pg}}_{\mathrm{guess}}(X|B)$ 是使用所谓的相当好的测量得到的猜测概率，

$$P^{\mathrm{pg}}_{\mathrm{guess}}(X|B) = \sum_x p(x)\,\mathrm{Tr}\,\rho_x M_x, \tag{V.11}$$

with

$$M_x = \rho_B^{-\frac{1}{2}} p(x) \rho_x \rho_B^{-\frac{1}{2}}. \tag{V.12}$$

现在我们可以证明如下结论。

命题 V.3。我们有，

$$\begin{aligned} &\widetilde{H}_2^{\downarrow}(X_1+X_2|B_1B_2)_\tau \\ &= -\log\left[2\left(\frac{1}{2} - e^{-\widetilde{H}_2^{\downarrow}(X_1|B_1)_{\rho_1}}\right)\left(\frac{1}{2} - e^{-\widetilde{H}_2^{\downarrow}(X_2|B_2)_{\rho_2}}\right) + \frac{1}{2}\right]. \end{aligned} \tag{V.13}$$

这个结果与经典情形的结果非常相似，参见 [8, 定理 IV.9]，，而且与经典情形一样，等号成立 [8, 引理 IV.11]。

根据链式法则，这也意味着以下结论。

命题 V.4。我们有，

$$\begin{aligned} &\bar{H}_{\frac{1}{2}}^{\uparrow}(X_2|X_1+X_2,B_1B_2)_\tau \\ &= \log\left(1 + \left(e^{\overline{H}_{\frac{1}{2}}^{\uparrow}(X_1|B_1)_{\rho_1}} - 1\right)\left(e^{\overline{H}_{\frac{1}{2}}^{\uparrow}(X_2|B_2)_{\rho_2}} - 1\right)\right). \end{aligned} \tag{V.14}$$

我们指出，诸如上述表达式的等式在 $\alpha = 3$ 的情况下也应成立，但显式计算似乎更加困难。

B. 关于一般 α的猜想

以下猜想将 [9,猜想 VII.1] 和 [9, 猜想 VII.2] 推广到了 Rényi 熵。

猜想 V.5($\widetilde{H}_\alpha^{\downarrow}$ BSC-PSC 界）。令 $H_1 = \widetilde{H}_\alpha^{\downarrow}(X_1|B_1)_{\rho_1}$ 以及 $H_2 = \widetilde{H}_\alpha^{\downarrow}(X_2|B_2)_{\rho_2}$。对于 $\alpha \in (0,\ 2] \cup [3,\infty)$，

$$\begin{aligned} &\widetilde{H}_\alpha^{\downarrow}(X_1+X_2|B_1B_2)_\tau \\ &\geq \begin{cases} h_\alpha(h_\alpha^{-1}(H_1) * h_\alpha^{-1}(H_2)) & H_1+H_2 \leq \log 2 \\ H_1+H_2-\log 2 + h_\alpha(h_\alpha^{-1}(\log 2 - H_1) * h_\alpha^{-1}(\log 2 - H_2)) & H_1+H_2 \geq \log 2 \end{cases}. \end{aligned} \tag{V.15}$$

对于 $\alpha \in [2,3]$，将 $\geq$ 与 $\leq$ 互换后同样成立；对于 $\alpha \in \{2,3\}$，上述结论以等号成立。

如果属实，则这些界在以下意义上是紧的：二元对称信道和纯态信道分别能够达到等号。**猜想 V.6 (** $\widetilde{H}_\alpha^{\downarrow}$ BEC 界)。对于 $\alpha \in (0,2] \cup [3,\infty)$,

$$\begin{aligned} &\widetilde{H}_\alpha^{\downarrow}(X_1+X_2|B_1B_2)_\tau \\ &\leq \frac{1}{1-\alpha}\log\frac{(\delta_\alpha^H - \widetilde{K}_\alpha^{\downarrow}(X_1|B_1))(\delta_\alpha^H - \widetilde{K}_\alpha^{\downarrow}(X_2|B_2))}{1-\delta_\alpha^H} + \delta_\alpha^H. \end{aligned} \tag{V.16}$$

对于 $\alpha \in [2,3]$，交换 $\geq$ 和 $\leq$ 后结论同样成立；对于 $\alpha \in \{2,3\}$，上述结论取等号。

同样，如果这些界成立，那么从二元擦除信道能够达到等号这一意义上说，它们是紧的。上一节讨论了 $\alpha = 2$ 的特殊情况。猜想中的界是经典界的对称化版本。根据前面的讨论，最优界必然具有这种对称性。最后，该猜想经受住了数值检验，见附录 A。

请注意，猜想中的界还意味着关于以下界的猜想

$$\bar{H}_\alpha^{\uparrow}(X_2|X_1+X_2,B_1B_2)_\tau \tag{V.17}$$

这是通过前面讨论的信息合并链式法则得到的。

VI. Conclusions

在这项工作中，我们重新审视了经典情形和量子情形下的信息合并界。主要贡献是提出了新的 Rényi 熵链式法则，将这类熵的不同定义联系起来。在经典情形下，这些结果使我们得以完善关于 Arimoto 条件熵的 Rényi 信息合并研究图景。除了理论意义外，这些结果也可能具有实际应用，例如有助于更好地理解考虑 Rényi 熵时的信道极化现象。在量子情形下，这些链式法则使得对称性等性质可以推广至

Rényi 熵，并提出了一个关于最优量子界的新猜想，推广了以往的 $\alpha = 1$ 猜想。这些结果也有力地表明，在推广信息合并界时， $\widetilde{H}_\alpha^\downarrow$ 是首选的 Rényi 熵。

致谢

本项目获得了欧盟“地平线 2020”研究与创新计划玛丽·斯克沃多夫斯卡-居里资助协议（编号：H2020-MSCA-IF-2020-101025848）的资助。本研究得到新加坡国家研究基金会和 A*STAR 通过其 CQT 衔接资助的支持。

参考文献

[1] M. Alsan 和 E. Teletar。《非平稳信道极化与极化的一个简单证明》。*2014* 年 *IEEE* 国际信息论研讨会论文集，第 301–305 页，2014 年 7 月。[2] E. Arikan。《信道极化：为对称二进制输入无记忆信道构造达到容量码的方法》。*IEEE* 信息论汇刊，55(7):3051–3073，2009 年。[3] S. Arimoto。《离散无记忆信道的 a 阶信息测度与容量》。信息论专题（*Bolyai* 数学学会专题论文集），16:41—52，1977 年。[4] F. Dupuis、O. Fawzi 和 R. Renner。《熵累积》。数学物理通信，379(3):867–913，2020 年。[5] A. E. Gamal 和 Y.-H. Kim。《网络信息论》。剑桥大学出版社，美国纽约，2012 年 1 月。[6] M. Hayashi。《通用随机隐私放大中泄露信息的指数衰减率》。*IEEE* 信息论汇刊，57(6):3989–4001，2011 年。[7] C. Hirche。《量子信息论中的极化码》。硕士论文，*arxiv:1501.03737*，2015 年。[8] C. Hirche。《信息合并的 Rényi 界》。载于*2020* 年 *IEEE* 国际信息论研讨会（*ISIT*），第 2297–2302 页。IEEE，2020 年。[9] C. Hirche 和 D. Reeb。《带量子侧信息的信息合并界》。*IEEE* 信息论汇刊，64 4757，2018 7 4739( ): – 。[10] J. M. Renes。《信道与码的对偶性》。*IEEE* 信息论汇刊，64(1):577–592，2017 年。[11] J. M. Renes、D. Sutter 和 S. H. Hassani。《极化集合的对齐》。*IEEE* 通信领域精选期刊，34(2):224–238，2015 年。[12] J. M. Renes 和 M. M. Wilde。《任意信道上的私密通信与量子通信极化码》。*IEEE* 信息论汇刊，60(6):3090–3103，2014 年。[13] T. Richardson 和 R. Urbanke。《现代编码理论》。剑桥大学出版社，美国纽约，2008 年。[14] B. Škori´c 、 C. Obi 、 E. Verbitskiy 和 B. Schoenmakers。《非均匀源可提取随机性的紧下界》。信息与计算，209(8):1184–1196，2011 年。[15] M. Tomamichel。《有限资源下的量子信息处理：数学基础》，第 5 卷。 Springer，2015 年。[16] M. Tomamichel、M. Berta 和 M. Hayashi。《不同量子推广的条件 Rényi 熵之间的关系》。数学物理杂志，55(8):082206，2014 年。[17] M. M. Wilde 和 S. Guha。《经典-量子信道的极化码》。*IEEE* 信息论汇刊，59(2):1175–1187，2012 年。[18] A. D. Wyner 和 J. Ziv。《关于某些二进制序列熵的一个定理及其应用——I》。*IEEE* 信息论汇刊，19(6):769–772，1973 年 11 月。

APPENDIX A
NUMERICAL RESULTS

本节将讨论量子侧信息情形下的一些数值结果。在所有情形中，我们固定 $W_1 = W_2$ ，并绘制差值

$$H_\alpha^\star(X_1 + X_2|B_1B_2) - H_\alpha^\star(X_1|B_2) \tag{A.1}$$

与初始熵 $H_\alpha^\star(X_1|B_2)$的关系。各条曲线给出了针对二元擦除信道（BEC，绿色）、二元对称信道（BSC，蓝色）以及纯态信道（PSC，红色）计算得到的界。此外，我们还绘制了 1000 个点，这些点基于随机选取的信道，且其 B_i 为二维。首先，我们考虑图 2 中的 $\widetilde{H}_\alpha^\downarrow$ 情形，这也是正文重点讨论的情形。很容易验证此前证明的对称性。此外，随机选取的信道似乎支持第 V-B 节提出的猜想。

接下来，我们考虑图 3 中的 $\bar{H}_\alpha^\downarrow$ 情形。首先注意到，在这种情形下，先前观察到的对称性对应性质似乎并不成立。此外，与之前 BSC 和 PSC 似乎共同给出下界或上界不同，这种情况下的顺序并不明确。特别是在 $\alpha = 1.4$ 处，可以观察到 PSC 似乎给出上界，BSC 给出下界，而 BEC 介于两者之间。总之，尽管 BSC、BEC 和 PSC 似乎仍给出了外界，但 $\alpha = 1$ 情形中的许多性质似乎不再成立。

最后，我们考虑图4中的 $\bar{H}_\alpha^\uparrow$ 。我们再次看到，所需的对称性似乎并不成立。此外，我们注意到，所考虑的信道似乎不再给出外界，见 $\alpha = 1.7$。不过请注意，即使在经典情形下，通常的信息合并界对于此 α也不成立，详情见 [8] 。因此，这里观察到的例子多少是意料之中的。

总之，我们猜想，尽管对于其他 Rényi 熵的选取，性质并非如此。这似乎意味着，在推广信息合并界时， $\widetilde{H}_\alpha^\downarrow$ 应当是首选的 Rényi 熵。

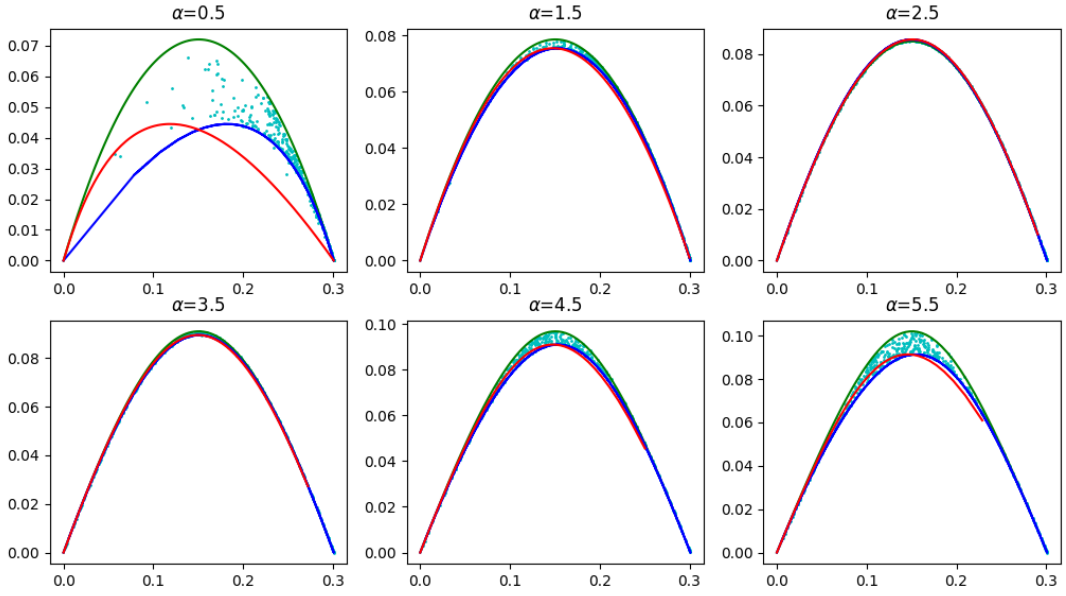


图 2：对不同 α 取值下的 $\widetilde{H}_\alpha^\downarrow$ 界进行数值检验，所用状态为随机抽取。第五节 B 中提出的猜想似乎成立。

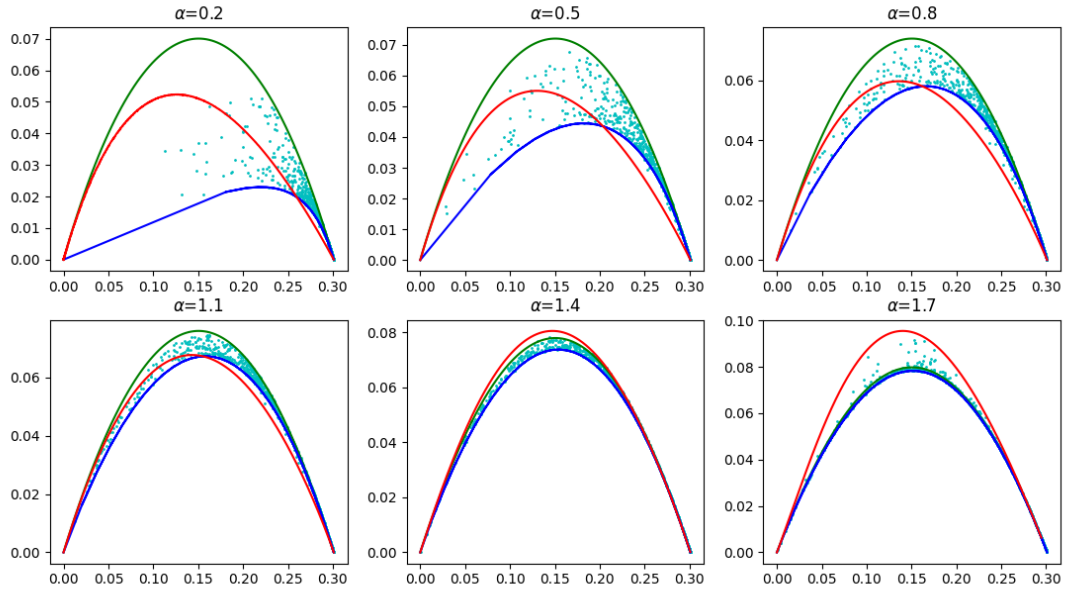


图 3：对 $\bar{H}_\alpha^\downarrow$进行数值检验。我们显然没有观察到 $\alpha = 1$所具有的相同对称性。尽管如此，基于图示信道得到的外界似乎成立。

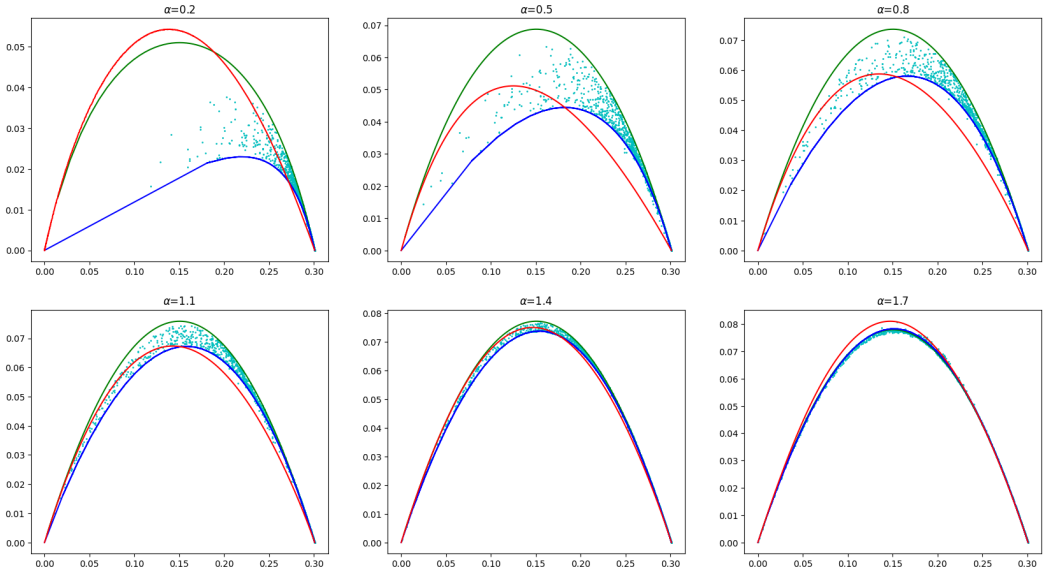


图 4：对 $\bar{H}_\alpha^\uparrow$ 的数值检验。同样，我们显然没有观察到 $\alpha = 1$ 所具有的相同对称性。某些 α 会违反外界，但这是预料之中的，详见正文。

APPENDIX B
ADDITIONAL PROOFS

在本附录中，我们给出正文中省略的证明。为方便读者，我们在证明前重述各项结果。

引理 II.1 （经典 Rényi 链式法则）。 设 $p(x, y)$ 和 $\bar{p}(x, y)$ 是满足以下关系的联合概率分布。 ，

$$\bar{p}(x,y) = \frac{p(x|y)^\alpha p(y)}{\sum_{x,y} p(x|y)^\alpha p(y)}, \tag{B.1}$$

then

$$H_\alpha^H(X|Y)_p = H_{\frac{1}{\alpha}}^A(X|Y)_{\bar{p}}. \tag{B.2}$$

类似地，令

$$\hat{p}(x,y,z) = \frac{p(z)p(x,y|z)^\alpha}{\sum_{x,y,z} p(z)p(x,y|z)^\alpha}, \tag{B.3}$$

then

$$H_\alpha^H(XY|Z)_p = H_{\frac{1}{\alpha}}^A(X|YZ)_{\hat{p}} + H_\alpha^H(Y|Z)_p \tag{B.4}$$

$$= H_{\frac{1}{\alpha}}^A(XY|Z)_{\hat{p}}. \tag{B.5}$$

证明。 我们证明最后一个陈述中的第一个等式。其余等式都可以通过代入类似地验证。

$$H_{\frac{1}{\alpha}}^A(X|YZ)_{\hat{p}} \tag{B.6}$$

$$= \frac{1}{\alpha - 1} \log \sum_y \hat{p}(y) \left(\sum_x \hat{p}(x|y)^{\frac{1}{\alpha}} \right)^\alpha \tag{B.7}$$

$$= \frac{1}{\alpha - 1} \log \sum_y \left(\sum_x \hat{p}(x,y)^{\frac{1}{\alpha}} \right)^\alpha \tag{B.8}$$

$$= \frac{1}{\alpha-1}\log\sum_y\left(\sum_x\left(\frac{p(z)p(x,y|z)^\alpha}{\sum_{x,y,z}p(z)p(x,y|z)^\alpha}\right)^{\frac{1}{\alpha}}\right)^\alpha \tag{B.9}$$

$$= \frac{1}{\alpha-1}\log\sum_y\left(\sum_x(p(z)p(x,y|z)^\alpha)^{\frac{1}{\alpha}}\right)^\alpha$$

$$- \frac{1}{\alpha-1}\log\sum_{x,y,z}p(z)p(x,y|z)^\alpha \tag{B.10}$$

$$= \frac{1}{\alpha-1}\log\sum_y\Big(p(z)^{\frac{1}{\alpha}}p(y|z)\Big)^\alpha + H_\alpha^H(X,Y|Z)_p \tag{B.11}$$

$$= -H_\alpha^H(Y|Z)_p + H_\alpha^H(X,Y|Z)_p\,. \tag{B.12}$$

□

引理 III.1 (信息合并链式法则)。 给定信道 W_1和 W_2，存在信道 W_1'和 W_2'，满足$H_\alpha^H(W_i) = H_{\frac{1}{\alpha}}^A(W_i')_\alpha$

–

$$H_\alpha^H(W_1) + H_\alpha^H(W_2) = H_{\frac{1}{\alpha}}^A(W_1'\circledast W_2') + H_\alpha^H(W_1\boxtimes W_2). \tag{B.13}$$

更准确地说，这些信道定义如下:

$$W_i' \sim \bar{p}_i(x_i,y_i) = \frac{p_i(x_i|y_i)^\alpha p_i(y_i)}{\sum_{x,y}p_i(x_i|y_i)^\alpha p_i(y_i)}. \tag{B.14}$$

证明。 这基本上是由上一节中的引理 II.1 的链式法则得出的。还需证明的是:

$$H_{\frac{1}{\alpha}}^A(A|BC)_{\hat{p}} = H_{\frac{1}{\alpha}}^A(W_1'\circledast W_2'), \tag{B.15}$$

即，\(\hat{p}\) 是一个有效的余..... 合并信道。这可以通过直接计算看出，另请参见后文的量子情形。 n. □

定理 III.2. 对于 $\alpha\in(0,\frac{1}{3}]\cup[\frac{1}{2},\infty)$，有天天彩票

$$H_\alpha^A(X_2|X_1+X_2,Y_1Y_2)$$
$$\le H_\alpha^A(X_1|Y_1) + H_\alpha^A(X_2|Y_2) - h_{\frac{1}{\alpha}}(h_{\frac{1}{\alpha}}^{-1}(H_\alpha^A(X_1|Y_1)) * h_{\frac{1}{\alpha}}^{-1}(H_\alpha^A(X_2|Y_2))). \tag{B.16}$$

对于 $\alpha\in[\frac{1}{3},\frac{1}{2}]$，将 $\le$ 与 $\ge$互换后，上述结论同样成立。注意，对于– $\alpha\in\{\frac{1}{3},\frac{1}{2}\}$，上述结论取等号。这些界是紧的，因为二元对称信道可以达到等号。

证明。 使用链式法则，我们得到

$$H_\alpha^A(X_2|X_1+X_2,Y_1Y_2)$$
$$= H_\alpha^A(W_1\circledast W_2) \tag{B.17}$$
$$= H_\alpha^A(W_1) + H_\alpha^A(W_2) - H_{\frac{1}{\alpha}}^H(W_1'\boxtimes W_2'). \tag{B.18}$$

由此，若 $\alpha\in(0,\frac{1}{3}]\cup[\frac{1}{2},\infty)$，则根据定理 I.1，

$$H_\alpha^A(X_2|X_1+X_2,Y_1Y_2) - H_\alpha^A(W_1) - H_\alpha^A(W_2) \tag{B.19}$$
$$\le -h_{\frac{1}{\alpha}}(h_{\frac{1}{\alpha}}^{-1}(H_{\frac{1}{\alpha}}^H(W_1')) * h_{\frac{1}{\alpha}}^{-1}(H_{\frac{1}{\alpha}}^H(W_2'))) \tag{B.20}$$
$$= -h_{\frac{1}{\alpha}}(h_{\frac{1}{\alpha}}^{-1}(H_\alpha^A(W_1)) * h_{\frac{1}{\alpha}}^{-1}(H_\alpha^A(W_2))) \tag{B.21}$$

否则，将初始不等式反向即可。 □

定理 III.3。 对于 $\alpha\in(0,\frac{1}{3}]\cup[\frac{1}{2},\infty)$，有

$$H_\alpha^A(X_2|X_1+X_2,Y_1Y_2) \tag{B.22}$$
$$\ge H_\alpha^A(X_1|Y_1) + H_\alpha^A(X_2|Y_2) - \frac{\alpha}{\alpha-1}\log\frac{(\delta_{\frac{1}{\alpha}} - K_{\frac{1}{\alpha}}^A(X_1|Y_1))(\delta_{\frac{1}{\alpha}} - K_{\frac{1}{\alpha}}^A(X_2|Y_2))}{1-\delta_{\frac{1}{\alpha}}} + \delta_{\frac{1}{\alpha}}. \tag{B.23}$$

对于 $\alpha\in[\frac{1}{3},\frac{1}{2}]$，将 $\ge$ 替换为 $\le$后结论同样成立。注意，对于 $\alpha\in\{\frac{1}{3},\frac{1}{2}\}$，上述结论以等式成立。这些界是紧的，因为二元擦除信道能够达到等号。

证明。 与之前类似地开始，我们得到：如果 $\alpha \in (0, \frac{1}{3}] \cup [\frac{1}{2^\gamma}, \infty)$，那么根据定理 I.2，

$$H_\alpha^A(X_2|X_1+X_2, Y_1Y_2) - H_\alpha^A(W_1) - H_\alpha^A(W_2) \tag{B.24}$$

$$\geq -\frac{\alpha}{\alpha-1}\log\frac{(2^{\frac{\alpha-1}{\alpha}} - e^{\frac{\alpha-1}{\alpha}H_{\frac{1}{\alpha}}^H(W_1')})(2^{\frac{\alpha-1}{\alpha}} - e^{\frac{\alpha-1}{\alpha}H_{\frac{1}{\alpha}}^H(W_2')})}{1-2^{\frac{\alpha-1}{\alpha}}} + 2^{\frac{\alpha-1}{\alpha}} \tag{B.25}$$

$$= -\frac{\alpha}{\alpha-1}\log\frac{(2^{\frac{\alpha-1}{\alpha}} - e^{\frac{\alpha-1}{\alpha}H_\alpha^A(W_1)})(2^{\frac{\alpha-1}{\alpha}} - e^{\frac{\alpha-1}{\alpha}H_\alpha^A(W_2)})}{1-2^{\frac{\alpha-1}{\alpha}}} + 2^{\frac{\alpha-1}{\alpha}} \tag{B.26}$$

否则，不等式的方向相反。 □

引理 IV.1 (量子 Rényi 链式法则)。 令 ρ_{AB} 和 $\bar{\rho}_{AB}$ 为相关的量子态

$$\bar{\rho}_{AB} = \frac{\left(\rho_B^{\frac{1-\alpha}{2\alpha}}\rho_{AB}\rho_B^{\frac{1-\alpha}{2\alpha}}\right)^\alpha}{\mathrm{Tr}\left(\rho_B^{\frac{1-\alpha}{2\alpha}}\rho_{AB}\rho_B^{\frac{1-\alpha}{2\alpha}}\right)^\alpha}, \tag{B.27}$$

then

$$\widetilde{H}_\alpha^\downarrow(A|B)_\rho = \bar{H}_{\frac{1}{\alpha}}^\uparrow(A|B)_{\bar{\rho}}. \tag{B.28}$$

此外，如果

$$\widetilde{\rho}_{ABC} = \frac{\left(\rho_C^{\frac{1-\alpha}{2\alpha}}\rho_{ABC}\rho_C^{\frac{1-\alpha}{2\alpha}}\right)^\alpha}{\mathrm{Tr}\left(\rho_C^{\frac{1-\alpha}{2\alpha}}\rho_{ABC}\rho_C^{\frac{1-\alpha}{2\alpha}}\right)^\alpha}, \tag{B.29}$$

then

$$\widetilde{H}_\alpha^\downarrow(AB|C)_\rho = \bar{H}_{\frac{1}{\alpha}}^\uparrow(A|BC)_{\widetilde{\rho}} + \widetilde{H}_\alpha^\downarrow(B|C)_\rho = \bar{H}_{\frac{1}{\alpha}}^\uparrow(AB|C)_{\widetilde{\rho}}. \tag{B.30}$$

证明。再次，我们只展示一个，其余情况类似。

$$\bar{H}_{\frac{1}{\alpha}}^\uparrow(A|BC)_{\widetilde{\rho}}$$

$$= \frac{1}{\alpha-1}\log\mathrm{Tr}\left(\left(\mathrm{Tr}_A\,\widetilde{\rho}_{ABC}^{\frac{1}{\alpha}}\right)^\alpha\right) \tag{B.31}$$

$$= \widetilde{H}_\alpha^\downarrow(AB|C)_\rho + \frac{1}{\alpha-1}\log\mathrm{Tr}\left(\mathrm{Tr}_A\,\rho_C^{\frac{1-\alpha}{2\alpha}}\rho_{ABC}\rho_C^{\frac{1-\alpha}{2\alpha}}\right)^\alpha \tag{B.32}$$

$$= \widetilde{H}_\alpha^\downarrow(AB|C)_\rho + \frac{1}{\alpha-1}\log\mathrm{Tr}\left(\rho_C^{\frac{1-\alpha}{2\alpha}}\rho_{BC}\rho_C^{\frac{1-\alpha}{2\alpha}}\right)^\alpha \tag{B.33}$$

$$= \widetilde{H}_\alpha^\downarrow(AB|C)_\rho - \widetilde{H}_\alpha^\downarrow(B|C)_\rho. \tag{B.34}$$

□

引理 V.1 （信息合并链式法则）。 给定信道 W_1 和 W_2，存在信道 W_1' 和 W_2'，使得 $\widetilde{H}_\alpha^\downarrow(W_i) = \bar{H}_{\frac{1}{\alpha}}^\uparrow W_i'$ （ ）满足

$$\widetilde{H}_\alpha^\downarrow(W_1) + \widetilde{H}_\alpha^\downarrow(W_2) = \bar{H}_{\frac{1}{\alpha}}^\uparrow(W_1' \circledast W_2') + \widetilde{H}_\alpha^\downarrow(W_1 \boxtimes W_2). \tag{B.35}$$

更准确地说，这些信道定义如下：

$$W_i' \sim \bar{\rho}_{X_iB_i} = \frac{\left(\rho_{B_i}^{\frac{1-\alpha}{2\alpha}}\rho_{X_iB_i}\rho_{B_i}^{\frac{1-\alpha}{2\alpha}}\right)^\alpha}{\mathrm{Tr}\left(\rho_{B_i}^{\frac{1-\alpha}{2\alpha}}\rho_{X_iB_i}\rho_{B_i}^{\frac{1-\alpha}{2\alpha}}\right)^\alpha}. \tag{B.36}$$

证明。 由上一节可知，给定的 W_i' 满足 $\widetilde{H}_\alpha^\downarrow(W_i) = \bar{H}^\uparrow{}_1(W_i')$，此外，由 引理 IV.1 中的链式法则可得

$$\widetilde{H}_\alpha^\downarrow(W_1) + \widetilde{H}_\alpha^\downarrow(W_2) = \bar{H}_{\frac{1}{\alpha}}^\uparrow(A|BC)_{\widetilde{\tau}} + \widetilde{H}_\alpha^\downarrow(W_1 \boxtimes W_2). \tag{B.37}$$

还需证明 $\widetilde{\tau}$ 对应于 W_1' 和 W_2' 的 CNOT 门。利用经典-量子态的分块结构进行直接计算即可证明。简而言之，可以验证

$$\bar{\rho}_{X_iB_i} = \frac{1}{2}|0\rangle\langle 0| \otimes \bar{\sigma}_0^{B_i} + \frac{1}{2}|1\rangle\langle 1| \otimes \bar{\sigma}_1^{B_i}, \tag{B.38}$$

where $\bar{\sigma}_i^{B_i} = \frac{\left((\sigma_0^{B_i}+\sigma_1^{B_i})^{\frac{1-\alpha}{2\alpha}}\sigma_i^{B_i}(\sigma_0^{B_i}+\sigma_1^{B_i})^{\frac{1-\alpha}{2\alpha}}\right)^{\alpha}}{\mathrm{Tr}\left((\sigma_0^{B_i}+\sigma_1^{B_i})^{\frac{1-\alpha}{2\alpha}}\sigma_i^{B_i}(\sigma_0^{B_i}+\sigma_1^{B_i})^{\frac{1-\alpha}{2\alpha}}\right)^{\alpha}}$ and

$$\widetilde{\tau} = \sum_{z,x_2}\frac{1}{4}|z+x_2\rangle\langle z+x_2| \otimes |x_2\rangle\langle x_2| \otimes \bar{\sigma}_z^{B_1} \otimes \bar{\sigma}_{x_2}^{B_2}. \tag{B.39}$$

由此立即可得

$$\bar{H}^{\uparrow}_{\frac{1}{\alpha}}(A|BC)_{\widetilde{\tau}} = \bar{H}^{\uparrow}_{\frac{1}{\alpha}}(W_1' \circledast W_2'), \tag{B.40}$$

从而证明完毕。 □

引理 V.2（对称性）。给定信道 W_1 和 W_2，存在信道 $\bar{W}_1$ 和 $\bar{W}_2$，满足 $H(W_i) = \log 2 - H(\bar{W}_i)$，使得

$$\begin{aligned}&\widetilde{H}^{\downarrow}_{\alpha}(W_1 \circledast W_2) - \frac{1}{2}\Big(\widetilde{H}^{\downarrow}_{\alpha}(W_1) + \widetilde{H}^{\downarrow}_{\alpha}(W_2)\Big)\\ &= \widetilde{H}^{\downarrow}_{\alpha}(\bar{W}_1 \circledast \bar{W}_2) - \frac{1}{2}\Big(\widetilde{H}^{\downarrow}_{\alpha}(\bar{W}_1) + \widetilde{H}^{\downarrow}_{\alpha}(\bar{W}_2)\Big).\end{aligned} \tag{B.41}$$

证明。从链式法则出发，我们得到

$$\begin{aligned}&\widetilde{H}^{\downarrow}_{\alpha}(W_1 \circledast W_2) - \frac{1}{2}\Big(\widetilde{H}^{\downarrow}_{\alpha}(W_1) + \widetilde{H}^{\downarrow}_{\alpha}(W_2)\Big)\\ &= \frac{1}{2}\Big(\widetilde{H}^{\downarrow}_{\alpha}(W_1) + \widetilde{H}^{\downarrow}_{\alpha}(W_2)\Big) - \bar{H}^{\uparrow}_{\frac{1}{\alpha}}(W_1' \circledast W_2') &\text{(B.42)}\\ &= \frac{1}{2}\Big(\bar{H}^{\uparrow}_{\frac{1}{\alpha}}(W_1') + \bar{H}^{\uparrow}_{\frac{1}{\alpha}}(W_2')\Big) - \bar{H}^{\uparrow}_{\frac{1}{\alpha}}(W_1' \circledast W_2') &\text{(B.43)}\\ &= \widetilde{H}^{\downarrow}_{\alpha}(W_1'^{\perp} \circledast \bar{W}_2'^{\perp}) - \frac{1}{2}\Big(\widetilde{H}^{\downarrow}_{\alpha}(\bar{W}_1'^{\perp}) + \widetilde{H}^{\downarrow}_{\alpha}(\bar{W}_2'^{\perp})\Big), &\text{(B.44)}\end{aligned}$$

由此，结合 $\bar{W}_1 = W_1'^{\perp}$和 $\bar{W}_2 = W_2'^{\perp}$即可得到结论。 □

命题 V.3。我们有，

$$\begin{aligned}&\widetilde{H}^{\downarrow}_{2}(X_1 + X_2|B_1B_2)_{\tau}\\ &= -\log\left[2\left(\frac{1}{2} - e^{-\widetilde{H}^{\downarrow}_{2}(X_1|B_1)_{\rho_1}}\right)\left(\frac{1}{2} - e^{-\widetilde{H}^{\downarrow}_{2}(X_2|B_2)_{\rho_2}}\right) + \frac{1}{2}\right].\end{aligned} \tag{B.45}$$

证明。通过较为直接的计算，可以验证：

$$\begin{aligned}&P^{\mathrm{pg}}_{\mathrm{guess}}(X_1 + X_2|B_1B_2)\\ &= \sum_{i,j}\mathrm{Tr}(\sigma_i^{B_1} \otimes \sigma_i^{B_2})(M_j \otimes M_j) + \sum_{i,j}\mathrm{Tr}(\sigma_i^{B_1} \otimes \sigma_{i\oplus 1}^{B_2})(M_j \otimes M_{j\oplus 1}) &\text{(B.46)}\\ &= P^{\mathrm{pg}}_{\mathrm{guess}}(X_1|B_1)P^{\mathrm{pg}}_{\mathrm{guess}}(X_2|B_2) + (1 - P^{\mathrm{pg}}_{\mathrm{guess}}(X_1|B_1))(1 - P^{\mathrm{pg}}_{\mathrm{guess}}(X_2|B_2)) &\text{(B.47)}\\ &= 2(\frac{1}{2} - P^{\mathrm{pg}}_{\mathrm{guess}}(X_1|B_1))(\frac{1}{2} - P^{\mathrm{pg}}_{\mathrm{guess}}(X_2|B_2)) + \frac{1}{2}, &\text{(B.48)}\end{aligned}$$

其中，$M_i = \frac{1}{2}\bar{\sigma}^{-\frac{1}{2}}\sigma_i\bar{\sigma}^{-\frac{1}{2}}$中关于各个单独状态的相当好的测量为 $\bar{\sigma} = \frac{1}{2}(\sigma_0 + \sigma_1)$。然后对所有概率取 $-\log$，即可得证。 □

命题 V.4. 我们有，

$$\begin{aligned}&\bar{H}^{\uparrow}_{\frac{1}{2}}(X_2|X_1 + X_2, B_1B_2)_{\tau}\\ &= \log\left(1 + \left(e^{\bar{H}^{\uparrow}_{\frac{1}{2}}(X_1|B_1)_{\rho_1}} - 1\right)\left(e^{\bar{H}^{\uparrow}_{\frac{1}{2}}(X_2|B_2)_{\rho_2}} - 1\right)\right).\end{aligned} \tag{B.49}$$

证明。 通过直接计算即可验证上述结论，注意到

$$\bar{H}^{\uparrow}_{\frac{1}{2}}(X_1|B_1) = \log(1 + \operatorname{Tr}\sqrt{\sigma_0\sigma_1}) \tag{B.50}$$

$$\bar{H}^{\uparrow}_{\frac{1}{2}}(X_2|X_1 + X_2, B_1B_2) = \log(1 + \operatorname{Tr}\sqrt{\sigma_0\sigma_1}\operatorname{Tr}\sqrt{\bar{\sigma}_0\bar{\sigma}_1}). \tag{B.51}$$

然而，秉持本文的思路，我们将使用链式法则给出另一种证明。注意

$$\begin{aligned}
&\bar{H}^{\uparrow}_{1}(X_2|X_1 + X_2, \ B_1B_2) \\
&= \bar{H}^{\uparrow}_{\frac{1}{2}}(W_1 \circledast W_2) && \text{(B.52)}\\
&= -\widetilde{H}^{\downarrow}_{2}(W_1' \boxtimes W_2') + \bar{H}^{\uparrow}_{\frac{1}{2}}(W_1) + \bar{H}^{\uparrow}_{\frac{1}{2}}(W_2) && \text{(B.53)}\\
&= \log\left[2\left(\frac{1}{2} - e^{-\widetilde{H}^{\downarrow}_{2}(W_1')}\right)\left(\frac{1}{2} - e^{-\widetilde{H}^{\downarrow}_{2}(W_2')}\right) + \frac{1}{2}\right] + \bar{H}^{\uparrow}_{\frac{1}{2}}(W_1) + \bar{H}^{\uparrow}_{\frac{1}{2}}(W_2) && \text{(B.54)}\\
&= \log\left[2\left(\frac{1}{2} - e^{-\overline{H}^{\uparrow}_{\frac{1}{2}}(W_1)}\right)\left(\frac{1}{2} - e^{-\overline{H}^{\uparrow}_{\frac{1}{2}}(W_2)}\right) + \frac{1}{2}\right] + \log\left(e^{\overline{H}^{\uparrow}_{\frac{1}{2}}(W_1)+\overline{H}^{\uparrow}_{\frac{1}{2}}(W_2)}\right) && \text{(B.55)}\\
&= \log\left(1 + \left(e^{\overline{H}^{\uparrow}_{\frac{1}{2}}(X_1|B_1)} - 1\right)\left(e^{\overline{H}^{\uparrow}_{\frac{1}{2}}(X_2|B_2)} - 1\right)\right), && \text{(B.56)}
\end{aligned}$$

其中我们使用了链式法则以及所得的 W_i' 满足 $\widetilde{H}^{\downarrow}_{2}(W_i') = \bar{H}^{\uparrow}_{1}(W_i)$ 这一事实。[2] □