

Information Theory for Wireless Communication

Lecture 2: Conditionally and Jointly Typical Sequences

Instructor: Dr. Saif K. Mohammed

Scribe: T. V. K. Chaitanya

Spring 2012

In this lecture, we extend the letter typicality sequence definition in [1] to the typicality of input and output sequences of a discrete memoryless channel, together.

I. NOTATION AND DEFINITIONS

In this Section, we introduce the notation and definitions used in this lecture notes. Upper case letters and lower case letters are used to denote random variables and their realizations respectively.

The output of the discrete memoryless source (DMS) is denoted by X and it outputs symbols belonging to an alphabet of size M denoted as $\mathcal{X} \triangleq \{a_1, a_2, \dots, a_M\}$. We denote the probability that X takes a value a_i as

$$p_i \triangleq \text{P}(X = a_i) \quad (1)$$

and we therefore have $\sum_{i=1}^M p_i = 1$. We denote the n -length output of the DMS as $X^n \triangleq (X_1, X_2, \dots, X_n)$.

Since the source is memoryless, we have

$$\text{P}(X_1 = x_1, X_2 = x_2, \dots, X_n = x_n) = \prod_{k=1}^n \text{P}(X_k = x_k).$$

A. Discrete Memoryless Channel (DMC)

Consider the following scenario shown in Fig. 1, where we have the random variable X denoting the output of a DMS and which acts as an input to a discrete memoryless channel (DMC) and produces the

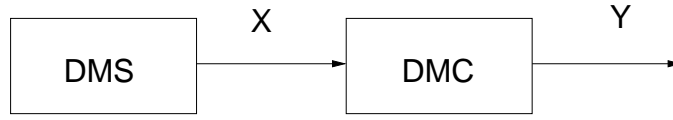


Figure 1. Communication over a DMC.

output random variable $Y \in \mathcal{Y} \triangleq \{b_1, b_2, \dots, b_{M'}\}$. For a DMC, the output Y_k at time instant k depends only on the input at time k (i.e., X_k). Hence, for the model shown in Fig. 1, we have

$$P(Y_1 = y_1, \dots, Y_n = y_n | X_1 = x_1, \dots, X_n = x_n) = \prod_{k=1}^n P(Y_k = y_k | X_k = x_k) \quad (2)$$

We define $p(j|i) \triangleq P(Y = b_j | X = a_i)$ and we have $\sum_{j=1}^{M'} p(j|i) = 1, \forall i = 1, 2, \dots, M$. We also define

$$p_j \triangleq P(Y = b_j) = \sum_{i=1}^M p(j|i) p_i. \quad (3)$$

II. CHANNEL CODING FOR DMC

A (n, N, λ) code is denoted by the set $\{(u_1, A_1), (u_2, A_2), \dots, (u_N, A_N)\}$. The code can be used to communicate N distinct messages to the receiver. If the i th message is to be communicated, the transmitter sends $u_i \in \mathcal{X}^n$ over the DMC. At the receiver, if the received sequence $Y^n \in \mathcal{Y}^n$ belongs to the j th decoding set $A_j \subset \mathcal{Y}^n$, the receiver declares that the j th message was sent by the transmitter. The rate of the code in bits per channel use (bpcu) is defined as

$$R \triangleq \frac{\log_2 N}{n}. \quad (4)$$

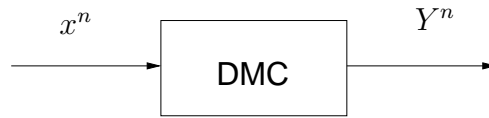
The probability of error corresponding to a codeword u_k is defined as

$$\lambda(u_k) \triangleq P(Y^n \notin A_k | u_k \text{ was transmitted}).$$

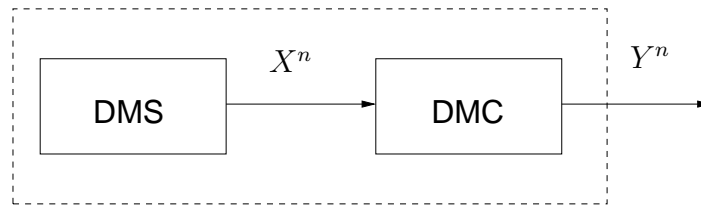
A (n, N, λ) code $\{(u_1, A_1), (u_2, A_2), \dots, (u_N, A_N)\}$ satisfies

$$\max_{k=1,2,\dots,N} \lambda(u_k) \leq \lambda.$$

Code Construction: Starting with message $u_1 \in \mathcal{X}^n$ which is k_0 -input typical, we construct a decoding set $A_1 \subset \mathcal{Y}^n$ such that $\lambda(u_1) \leq \lambda$. As we will discuss later, for a fixed k_0 -input typical sequence as the channel input, the output sequence belongs to a typical set with very high probability. The size of this set is of roughly $2^{nH(Y|X)}$. In the case of u_1 , A_1 is chosen to be the output typical set given that u_1 is

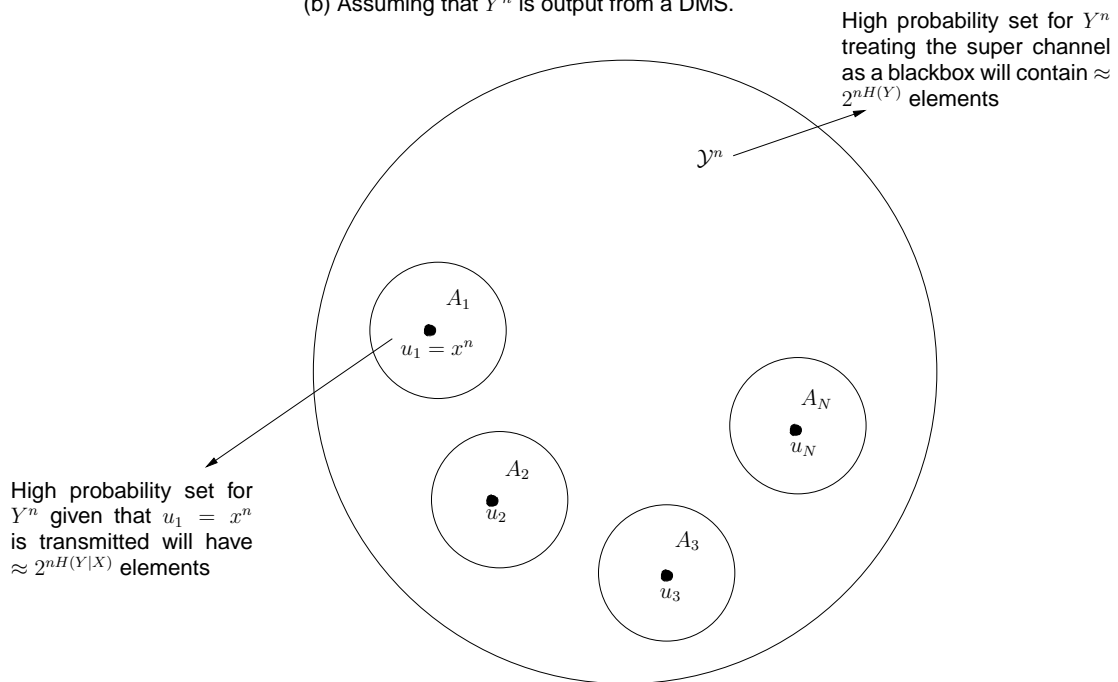


(a) Assuming that input to the DMC is x^n , which is some k_0 -input typical sequence.



Blackbox

(b) Assuming that Y^n is output from a DMS.



(c) Capacity of a DMC.

Figure 2. Capacity of a DMC illustrated using high probability sets.

the channel input. Next, we add other input k_0 -typical sequences to the code in a successive manner and we construct the corresponding decoding sets in such a way that maximum probability error constraint is satisfied in each of the corresponding decoding sets and that they are disjoint. Each of these sets are of approximate size $2^{nH(Y|X)}$. Later, we will also show that for the system in Fig. 2(b), the high probability of all possible output sequences is of size $\approx 2^{nH(Y)}$. The process of successively adding codewords to the code will stop after a finite number of steps, since at some point, the decoding set of any new codeword will have sufficient overlap with the previous decoding sets, such that the probability of error for the new codeword will exceed λ . Let N denote this maximum number of codewords for which A_1, A_2, \dots, A_N are disjoint and satisfy the maximum probability error constraint. This construction gives us an (n, N, λ) code. With this code construction, we have the following result:

$$|(A_1 \cup A_2 \cup \dots \cup A_N)| \approx N2^{nH(Y|X)} \lesssim 2^{nH(Y)} \implies R \lesssim H(Y) - H(Y|X) = I(X; Y) \quad (5)$$

More detailed description of this will be given during the next lecture while proving the channel coding theorem. Now we state the channel coding theorem which relates the number of codewords required to achieve a given λ .

Theorem 1. *Let $0 < \lambda \leq 1$ be any arbitrary number, there exists a positive scalar constant $k(\lambda)$ such that for any given n , there exists a code with parameters (n, N, λ) with $N > 2^{n(C - \frac{k(\lambda)}{\sqrt{n}})}$. Where $C = \max_{\{p_i\}} I(X; Y)$.*

Proof: Proof can be found in [2] and will be covered in the next lecture. ■

From the above theorem, it implies that a code with rate $R = \frac{\log_2 N}{n} > C - \frac{k(\lambda)}{\sqrt{n}}$ can be constructed for a given maximum probability of error λ .

Now we briefly describe a useful tool for bounding the cardinality of any given set. Let $Z \in \mathcal{Z}$ denote a random source, and let B denote the set containing output sequences which satisfy some property. For example, let $B = \{z^n \in \mathcal{Z}^n | z^n \text{ satisfies some property } E\}$. Suppose that we have

- 1) $\alpha < \Pr(z^n \in B) < \beta$, and
- 2) For each $z^n \in B$, $\Pr(Z^n = z^n)$ is bounded as $\gamma < \Pr(Z^n = z^n) < \eta$, then

we have

$$\alpha < \Pr(z^n \in B) = \sum_{z^n \in B} \Pr(Z^n = z^n) < \eta |B|,$$

from which we have

$$|B| > \frac{\alpha}{\eta}. \quad (6)$$

Similarly, we have

$$\beta > \Pr(z^n \in B) = \sum_{z^n \in B} \Pr(Z^n = z^n) > \gamma |B|,$$

from which it follows that

$$|B| < \frac{\beta}{\gamma}. \quad (7)$$

From (6) and (7), we have

$$\frac{\alpha}{\eta} < |B| < \frac{\beta}{\gamma}.$$

Lemma 1. For any arbitrary constant $k_0 > 2$, the output of a DMS X^n is said to be k_0 -letter typical if

$$\left| \frac{f_i(x^n) - np_i}{\sqrt{np_i(1-p_i)}} \right| < \sqrt{Mk_0}, \quad \forall i = 1, 2, \dots, M.$$

We denote the set of k_0 -letter typical sequences by \mathcal{T}_{k_0} . A direct result of the lemma is that

$$\Pr(X^n \notin \mathcal{T}_{k_0}) < \frac{1}{k_0}.$$

Definition 1. For any arbitrary constant $\delta > MM'$, $y^n \in \mathcal{Y}^n$ is said to be δ -generated by $x^n \in \mathcal{X}^n$ if

$$\left| \frac{f_{i,j}(x^n, y^n) - f_i(x^n)p(j|i)}{\sqrt{f_i(x^n)p(j|i)(1-p(j|i))}} \right| < \delta, \quad \forall i = 1, 2, \dots, M, j = 1, 2, \dots, M'.$$

where $f_{i,j}(x^n, y^n)$ is the number of locations l such that $x_l = a_i$ and $y_l = b_j$. For the system in Fig. 2(a),

we have $\mathbb{E}_{Y^n}[f_{i,j}(x^n, Y^n)] = f_i(x^n)p(j|i)$ and $\text{Var}[f_{i,j}(x^n, Y^n)] = f_i(x^n)p(j|i)(1-p(j|i))$.

Lemma 2. $\Pr(Y^n \text{ is } \delta\text{-generated by } x^n | x^n \text{ was transmitted}) > 1 - \frac{MM'}{\delta^2}$

Proof: $\Pr(Y^n \text{ is not } \delta\text{-generated by } x^n | x^n \text{ was transmitted})$ can be simplified as follows:

$$\begin{aligned} \Pr \left\{ \left| \frac{f_{i,j}(x^n, Y^n) - f_i(x^n)p(j|i)}{\sqrt{f_i(x^n)p(j|i)(1-p(j|i))}} \right| > \delta \text{ for some } i \text{ and some } j \right\} \\ \stackrel{(a)}{\leq} \sum_{i=1}^M \sum_{j=1}^{M'} \Pr \left\{ \left| \frac{f_{i,j}(x^n, Y^n) - f_i(x^n)p(j|i)}{\sqrt{f_i(x^n)p(j|i)(1-p(j|i))}} \right| > \delta \right\} \\ \stackrel{(b)}{<} \frac{MM'}{\delta^2} \end{aligned} \quad (8)$$

in (a) we have used the union bound and in (b) we have used the Chebyshev's inequality. ■

Definition 2. For any arbitrary constants $\delta > MM'$ and $k_0 > 2$, a pair (x^n, y^n) is said to be (δ, k_0) -jointly typical if

x^n is k_0 -letter input typical, and

y^n is δ -generated by x^n .

Definition 3. We define the set that consists of all pairs of (x^n, y^n) which are (δ, k_0) -jointly typical as $B^{(\delta, k_0)}$. i.e.,

$$B^{(\delta, k_0)} = \{(x^n, y^n) \mid (x^n, y^n) \text{ is } (\delta, k_0) \text{- jointly typical}\}.$$

Lemma 3. For given constants $k_0 > 2$, $\delta > MM'$, for any n , we have

$$\left(1 - \frac{1}{k_0}\right) \left(1 - \frac{MM'}{\delta^2}\right) < \Pr\{(X^n, Y^n) \text{ is } (\delta, k_0) \text{- jointly typical}\} < 1,$$

where X^n and Y^n refer to the outputs from the DMS and DMC as shown in the Fig. 2(b).

Lemma 4. If $(x^n, y^n) \in B^{(\delta, k_0)}$, then for the system in Fig. 2(b), we have

$$2^{-n(H(X, Y) + \frac{K_1}{\sqrt{n}})} < \Pr\{X^n = x^n, Y^n = y^n\} < 2^{-n(H(X, Y) - \frac{K_1}{\sqrt{n}})},$$

where $H(X, Y) = -\sum_{i=1}^M \sum_{j=1}^{M'} p(i, j) \log p(i, j)$ and K_1 is a positive constant depending on k_0, δ, M, M' and is independent of $\{p_i, p(j|i)\}$ and n .

Definition 4. We define the set $B_1^{(\delta, k_0)}$ as

$$B_1^{(\delta, k_0)} = \{y^n \in \mathcal{Y}^n \mid y^n \text{ is } \delta \text{- generated by some } k_0 \text{- input typical sequence}\}.$$

Lemma 5. We have $\left(1 - \frac{1}{k_0}\right) \left(1 - \frac{MM'}{\delta^2}\right) < \Pr(Y^n \in B_1^{(\delta, k_0)}) < 1$, where Y^n is the random variable, which is the output of the system in Fig. 2(b).

Proof:

$$\begin{aligned} \Pr(Y^n \in B_1^{(\delta, k_0)}) &= \sum_{\{y^n \mid y^n \in B_1^{(\delta, k_0)}\}} \Pr(Y^n = y^n) \\ &= \sum_{\{y^n \mid y^n \in B_1^{(\delta, k_0)}\}} \sum_{x^n \in \mathcal{X}^n} \Pr(Y^n = y^n, X^n = x^n) \\ &\geq \sum_{\{x^n \mid x^n \in \mathcal{T}_{k_0}\}} \sum_{\{y^n \mid y^n \text{ is } \delta\text{-generated by } x^n\}} \Pr(Y^n = y^n, X^n = x^n) \end{aligned}$$

$$\begin{aligned}
&= \sum_{\{x^n | x^n \in \mathcal{T}_{k_0}\}} \Pr(X^n = x^n) \sum_{\{y^n | y^n \text{ is } \delta\text{-generated by } x^n\}} \Pr(Y^n = y^n | X^n = x^n) \\
&\stackrel{(c)}{>} \left(1 - \frac{MM'}{\delta^2}\right) \sum_{\{x^n | x^n \in \mathcal{T}_{k_0}\}} \Pr(X^n = x^n) \\
&\stackrel{(d)}{>} \left(1 - \frac{MM'}{\delta^2}\right) \left(1 - \frac{1}{k_0}\right) \tag{9}
\end{aligned}$$

in (c), we have used result from Lemma 2 and in (d), we have used the result from Lemma 1. \blacksquare

Lemma 6.

$$2^{n(H(Y) - \frac{K_4}{\sqrt{n}})} < |B_1^{(\delta, k_0)}| < 2^{n(H(Y) + \frac{K_4}{\sqrt{n}})},$$

where $H(Y) \triangleq -\sum_{j=1}^{M'} p_j \log p_j$.

Proof: We have $\Pr(Y^n = y^n) = \prod_{j=1}^{M'} p_j^{f_j(y^n)}$, which implies

$$-\frac{\log \Pr(Y^n = y^n)}{n} = \sum_{j=1}^{M'} \frac{f_j(y^n)}{n} \log \frac{1}{p_j}. \tag{10}$$

For any $y^n \in B_1^{(\delta, k_0)}$, y^n must be δ -generated by some k_0 -typical x^n . This implies that

$$\left| \frac{f_{i,j}(x^n, y^n) - f_i(x^n) p(j|i)}{\sqrt{f_i(x^n) p(j|i) (1 - p(j|i))}} \right| < \delta, \quad \forall i = 1, 2, \dots, M, j = 1, 2, \dots, M', \text{ and} \tag{11}$$

$$\left| \frac{f_i(x^n) - np_i}{\sqrt{np_i(1 - p_i)}} \right| < \sqrt{Mk_0}, \quad \forall i = 1, 2, \dots, M \tag{12}$$

We can write

$$\begin{aligned}
f_j(y^n) &= \sum_{i=1}^M f_{i,j}(x^n, y^n) \\
&< \sum_{i=1}^M \left\{ f_i(x^n) p(j|i) + \delta \sqrt{f_i(x^n) p(j|i) (1 - p(j|i))} \right\} \\
&< \sum_{i=1}^M \left\{ \left[np_i + \sqrt{Mk_0 np_i (1 - p_i)} \right] p(j|i) \right\} \\
&+ \delta \sum_{i=1}^M \left\{ \sqrt{\left[np_i + \sqrt{Mk_0 np_i (1 - p_i)} \right] p(j|i) (1 - p(j|i))} \right\} \\
&< \sum_{i=1}^M \left\{ \left[np_i + \sqrt{Mk_0 np_i} \right] p(j|i) \right\} + \delta \sum_{i=1}^M \left\{ \sqrt{\left[np_i + \sqrt{Mk_0 np_i} \right] p(j|i)} \right\} \tag{13}
\end{aligned}$$

Now from (10) and (13), we can write

$$\begin{aligned} \sum_{j=1}^{M'} \frac{f_j(y^n)}{n} \log \frac{1}{p_j} &< \sum_{i=1}^M \sum_{j=1}^{M'} p_i p(j|i) \log \frac{1}{p_j} + \sqrt{\frac{Mk_0}{n}} \sum_{i=1}^M \sum_{j=1}^{M'} \sqrt{p_i} p(j|i) \log \frac{1}{p_j} \\ &+ \frac{\delta}{\sqrt{n}} \sum_{i=1}^M \sum_{j=1}^{M'} \sqrt{p_i + \sqrt{\frac{Mk_0 p_i}{n}}} \sqrt{p(j|i)} \log \frac{1}{p_j} \end{aligned} \quad (14)$$

Now using the following results (not proved here)

$$\begin{aligned} \sqrt{p_i} &< p_i^{\frac{1}{4}} \\ p(j|i) &< p(j|i)^{\frac{1}{4}} \\ \sqrt{p_i + \sqrt{\frac{Mk_0 p_i}{n}}} \sqrt{p(j|i)} &< \sqrt{Mk_0 p_i^{\frac{1}{4}} p(j|i)^{\frac{1}{4}}}, \end{aligned} \quad (15)$$

we can write (14) as:

$$\begin{aligned} \sum_{j=1}^{M'} \frac{f_j(y^n)}{n} \log \frac{1}{p_j} &< \underbrace{\sum_{i=1}^M \sum_{j=1}^{M'} p_i p(j|i) \log \frac{1}{p_j}}_{=H(Y)} + 4\sqrt{\frac{Mk_0}{n}} \sum_{i=1}^M \sum_{j=1}^{M'} [p_i p(j|i)]^{\frac{1}{4}} \log \frac{1}{p_j^{\frac{1}{4}}} \\ &+ 4\delta \sqrt{\frac{Mk_0}{n}} \sum_{i=1}^M \sum_{j=1}^{M'} [p_i p(j|i)]^{\frac{1}{4}} \log \frac{1}{p_j^{\frac{1}{4}}} \\ &= H(Y) + 4(1 + \delta) \sqrt{\frac{Mk_0}{n}} \sum_{i=1}^M \sum_{j=1}^{M'} [p_i p(j|i)]^{\frac{1}{4}} \log \frac{1}{p_j^{\frac{1}{4}}}. \end{aligned} \quad (16)$$

For any positive $\alpha_1, \alpha_2, \dots, \alpha_M$, we have the following result¹:

$$\sum_{i=1}^M \alpha_i^{\frac{1}{4}} \leq M^{\frac{3}{4}} \left(\sum_{i=1}^M \alpha_i \right)^{\frac{1}{4}} \quad (17)$$

Using (17) in (16), we have

$$\sum_{j=1}^{M'} \frac{f_j(y^n)}{n} \log \frac{1}{p_j} < H(Y) + 4(1 + \delta) M^{\frac{3}{4}} \sqrt{\frac{Mk_0}{n}} \sum_{j=1}^{M'} p_j^{\frac{1}{4}} \log \frac{1}{p_j^{\frac{1}{4}}} \quad (18)$$

Now noting that for any $x \in (0, 1)$, $f(x) = x \log_2 \frac{1}{x}$ is bounded and that the maximum value of $f(x)$

¹Can be proved using Holder's inequality $\sum_{i=1}^n |x_i y_i| \leq (\sum |x_i|^p)^{\frac{1}{p}} (\sum |y_i|^q)^{\frac{1}{q}}$ for any $1 \leq p, q \leq \infty$ with $\frac{1}{p} + \frac{1}{q} = 1$, by choosing $x_i = 1$ and $y_i = \alpha_i^{\frac{1}{4}}$ with $p = \frac{4}{3}$ and $q = 4$.

occurs at $x = \frac{1}{e}$, we have

$$p_j^{\frac{1}{4}} \log \frac{1}{p_j^{\frac{1}{4}}} < \frac{\log_2 e}{e} \quad (19)$$

Using (19) in (18), for any $y^n \in B_1^{(\delta, k_0)}$, we have

$$-\frac{\log \Pr(Y^n = y^n)}{n} = \sum_{j=1}^{M'} \frac{f_j(y^n)}{n} \log \frac{1}{p_j} < H(Y) + \frac{1}{\sqrt{n}} \underbrace{\left(4(1+\delta) M^{\frac{3}{4}} \sqrt{M k_0} M' \frac{\log_2 e}{e}\right)}_{\triangleq K_3}$$

from which, we have

$$-\frac{\log \Pr(Y^n = y^n)}{n} < H(Y) + \frac{K_3}{\sqrt{n}}. \quad (20)$$

following similar procedure, we can prove that

$$-\frac{\log \Pr(Y^n = y^n)}{n} > H(Y) - \frac{K_3}{\sqrt{n}} \quad (21)$$

From (20) and (21), for any $y^n \in B_1^{(\delta, k_0)}$, we have

$$2^{-n\left(H(Y) - \frac{K_3}{\sqrt{n}}\right)} < \Pr(Y^n = y^n) < 2^{-n\left(H(Y) + \frac{K_3}{\sqrt{n}}\right)} \quad (22)$$

Now using Lemma 5 together with (22), and using the technique described earlier for bounding the cardinality of a given set, we have

$$\left(1 - \frac{MM'}{\delta^2}\right) \left(1 - \frac{1}{k_0}\right) 2^{n\left(H(Y) - \frac{K_3}{\sqrt{n}}\right)} < |B_1^{(\delta, k_0)}| < 2^{n\left(H(Y) + \frac{K_3}{\sqrt{n}}\right)} \quad (23)$$

We can simplify (23) further as:²

$$2^{n\left(H(Y) - \frac{K_4}{\sqrt{n}}\right)} < |B_1^{(\delta, k_0)}| < 2^{n\left(H(Y) + \frac{K_4}{\sqrt{n}}\right)},$$

2

$$\begin{aligned} \left(1 - \frac{MM'}{\delta^2}\right) \left(1 - \frac{1}{k_0}\right) 2^{n\left(H(Y) - \frac{K_3}{\sqrt{n}}\right)} &= 2^{n\left(H(Y) - \frac{K_3}{\sqrt{n}}\right) + \log_2\left(1 - \frac{MM'}{\delta^2}\right) + \log_2\left(1 - \frac{1}{k_0}\right)} \\ &= 2^{n\left(H(Y) - \frac{K_3}{\sqrt{n}} - \frac{\log_2\left(1 - \frac{MM'}{\delta^2}\right)}{n} - \frac{\log_2\left(1 - \frac{1}{k_0}\right)}{n}\right)} \end{aligned}$$

since $\frac{1}{n} \leq \frac{1}{\sqrt{n}}$, we have

$$2^{n\left(H(Y) - \frac{K_3}{\sqrt{n}} - \frac{\log_2\left(1 - \frac{MM'}{\delta^2}\right)}{n} - \frac{\log_2\left(1 - \frac{1}{k_0}\right)}{n}\right)} \geq 2^{n\left(H(Y) - \frac{K_3}{\sqrt{n}} - \frac{\log_2\left(1 - \frac{MM'}{\delta^2}\right)}{\sqrt{n}} - \frac{\log_2\left(1 - \frac{1}{k_0}\right)}{\sqrt{n}}\right)} = 2^{n\left(H(Y) - \frac{K_4}{\sqrt{n}}\right)}$$

where $K_4 \triangleq K_3 - \log_2 \left(1 - \frac{MM'}{\delta^2}\right) - \log_2 \left(1 - \frac{1}{k_0}\right)$ and we can easily see that $K_4 > K_3$. ■

REFERENCES

- [1] R. Moosavi, "Information Theory for Wireless Communication, Lecture 1: Typical Sequences", <http://www.commsys.isy.liu.se/ITWC/Lecture1.pdf>, 2012.
- [2] J. Wolfowitz, *Coding Theorems of Information Theory*, Ergebnisse Der Mathematik Und Ihrer Grenzgebiete, 2nd Ed. 1964.