# ON AN INEQUALITY BY ANDRICA AND RAŞA AND ITS APPLICATION FOR THE SHANNON AND RÉNYI'S ENTROPY 

S. S. DRAGOMIR, J. ŠUNDE AND J. ASENSTORFER


#### Abstract

Applications of a result by Andrica and Raşa involving twice differentiable mappings for Shannon's and Rényi's entropy are given.


## 1. Introduction

The following converse of Jensen's discrete inequality for convex mappings of a real variable was proved in 1994 by Dragomir and Ionescu in [2].

Theorem 1. Let $f: I \subseteq \mathbb{R} \rightarrow \mathbb{R}$ be a differentiable convex function on the interval $I$, $x_{i} \in \check{I}$ (İ is the interior of $I$ ), $p_{i} \geq 0(i=1, \ldots, n)$ and $\sum_{i=1}^{n} p_{i}=1$. Then we have the inequality:

$$
\begin{align*}
0 & \leq \sum_{i=1}^{n} p_{i} f\left(x_{i}\right)-f\left(\sum_{i=1}^{n} p_{i} x_{i}\right)  \tag{1.1}\\
& \leq \sum_{i=1}^{n} p_{i} x_{i} f^{\prime}\left(x_{i}\right)-\sum_{i=1}^{n} p_{i} x_{i} \sum_{j=1}^{n} p_{j} f^{\prime}\left(x_{j}\right) .
\end{align*}
$$

It also pointed out some natural applications of (1.1) in connection to the arithmetic mean-geometric mean inequality, the generalized triangle inequality, etc...

For other results in connection to Jensen's inequality for convex functions see for example the book [1] and the Ph.D. Dissertation [6].

A generalization of (1.1) for differentiable convex mappings of several variables was obtained in 1996 by Dragomir and Goh [3]. They also considered the following analytic inequality for the logarithmic map $\log _{b}(\cdot)$.

[^0]Theorem 2. Let $\xi_{i}, p_{i}>0(i=1, \ldots, n)$ with $\sum_{i=1}^{n} p_{i}=1$ and $b>1$. Then

$$
\begin{align*}
0 & \leq \log _{b}\left(\sum_{i=1}^{n} p_{i} \xi_{i}\right)-\sum_{i=1}^{n} p_{i} \log _{b} \xi_{i}  \tag{1.2}\\
& \leq \frac{1}{\ln b}\left[\sum_{i=1}^{n} \frac{p_{i}}{\xi_{i}} \sum_{j=1}^{n} p_{j} \xi_{j}-1\right] \\
& =\frac{1}{\ln b} \sum_{1 \leq i<j \leq n}^{n} p_{i} p_{j} \frac{\left(\xi_{i}-\xi_{j}\right)^{2}}{\xi_{i} \xi_{j}} .
\end{align*}
$$

Equality holds in (1.2) if and only if $\xi_{1}=\ldots=\xi_{n}$.
They also applied inequality (1.2) to Information Theory for the entropy mapping, conditional entropy, mutual information, conditional mutual information, etc...

An integral version of (1.2) was employed by Dragomir and Goh in [11] to obtain new bounds for the entropy, conditional entropy and mutual information of continuous random variables. In addition, some applications of an integral counterpart of Jensen's inequality in Torsion Theory were done by Dragomir and Keady in 1996 [9].

For recent generalizations, for both the discrete case and the continuous case, as well as extensions for mappings defined on normed linear spaces, see M. Matić's Ph.D. Dissertation [6], where further applications in Information Theory are given.

## 2. Some Analytic Inequalities

We use the following result due to Andrica and Raşa [10].
Theorem 3. Let $f:[a, b] \rightarrow \mathbb{R}$ be twice differentiable on $(a, b)$ and $m \leq f^{\prime \prime}(x) \leq M$ for all $x \in(a, b)$. If $x_{i} \in(a, b)(i=\overline{1, n})$ and $p=\left(p_{i}\right)_{i=\overline{1, n}}$ is a probability distribution, then

$$
\begin{align*}
& \frac{m}{4} \sum_{i, j=1}^{n} p_{i} p_{j}\left(x_{i}-x_{j}\right)^{2}  \tag{2.1}\\
\leq & \sum_{i=1}^{n} p_{i} f\left(x_{i}\right)-f\left(\sum_{i=1}^{n} p_{i} x_{i}\right) \\
\leq & \frac{M}{4} \sum_{i, j=1}^{n} p_{i} p_{j}\left(x_{i}-x_{j}\right)^{2} .
\end{align*}
$$

For the sake of completeness, we present here a short proof of this result.

Proof. Consider the mapping $g:[a, b] \rightarrow \mathbb{R}, g(x)=f(x)-\frac{1}{2} m x^{2}$. Then $g$ is twice differentiable on ( $a, b$ ) and

$$
\begin{aligned}
g^{\prime}(x) & =f^{\prime}(x)-m x, x \in(a, b) \\
g^{\prime \prime}(x) & =f^{\prime \prime}(x)-m, x \in(a, b),
\end{aligned}
$$

which shows that the mapping $g$ is convex on $[a, b]$.
Apply Jensen's discrete inequality for the convex mapping $g$, i.e.,

$$
g\left(\sum_{i=1}^{n} p_{i} x_{i}\right) \leq \sum_{i=1}^{n} p_{i} g\left(x_{i}\right),
$$

to obtain

$$
\begin{aligned}
& f\left(\sum_{i=1}^{n} p_{i} x_{i}\right)-\frac{1}{2} m\left(\sum_{i=1}^{n} p_{i} x_{i}\right)^{2} \\
\leq & \sum_{i=1}^{n} p_{i}\left[f\left(x_{i}\right)-\frac{1}{2} m x_{i}^{2}\right] \\
= & \sum_{i=1}^{n} p_{i} f\left(x_{i}\right)-\frac{1}{2} m \sum_{i=1}^{n} p_{i} x_{i}^{2},
\end{aligned}
$$

which is equivalent to

$$
\begin{aligned}
& \sum_{i=1}^{n} p_{i} f\left(x_{i}\right)-f\left(\sum_{i=1}^{n} p_{i} x_{i}\right) \\
\geq & \frac{1}{2} m\left[\sum_{i=1}^{n} p_{i} x_{i}^{2}-\left(\sum_{i=1}^{n} p_{i} x_{i}\right)^{2}\right] \\
= & \frac{1}{4} m \sum_{i, j=1}^{n} p_{i} p_{j}\left(x_{i}-x_{j}\right)^{2}
\end{aligned}
$$

and the first inequality in (2.1) is proved.
The proof of the second inequality goes likewise for the mapping $h:[a, b] \rightarrow \mathbb{R}$, $h(x)=\frac{1}{2} M x^{2}-f(x)$ which is convex on $[a, b]$. We omit the details.

Now, consider the means:

1) The weighted arithmetic mean $A_{n}(w, a)$

$$
A_{n}(w, a):=\frac{1}{W_{n}} \sum_{i=1}^{n} w_{i} a_{i},
$$

where $W_{n}=\sum_{i=1}^{n} w_{i}$.
2) The weighted geometric mean $G_{n}(w, a)$

$$
G_{n}(w, a):=\left(\prod_{i=1}^{n} a_{i}^{w_{i}}\right)^{\frac{1}{W_{n}}}
$$

and
3) The weighted harmonic mean $H_{n}(w, a)$

$$
H_{n}(w, a)=\frac{W_{n}}{\sum_{i=1}^{n} \frac{w_{i}}{a_{i}}},
$$

where $a_{i}, w_{i}>0(i=1, \ldots, n)$.
The following inequality is well known in the literature as the arithmetic meangeometric mean-harmonic mean inequality

$$
\begin{equation*}
A_{n}(w, a) \geq G_{n}(w, a) \geq H_{n}(w, a) . \tag{2.2}
\end{equation*}
$$

The equality holds in (2.2) if and only if $a_{1}=\ldots=a_{n}$.
The following corollary holds.
Corollary 1. Let $a_{i}, w_{i}>0(i=1, \ldots, n)$. If $0<m \leq a_{i} \leq M<\infty(i=1, \ldots, n)$, then we have the inequalities:

$$
\begin{align*}
1 & \leq \exp \left[\frac{1}{4 M^{2}} \cdot \frac{1}{W_{n}^{2}} \sum_{i, j=1}^{n} w_{i} w_{j}\left(a_{i}-a_{j}\right)^{2}\right]  \tag{2.3}\\
& \leq \frac{A_{n}(w, a)}{G_{n}(w, a)} \\
& \leq \exp \left[\frac{1}{4 m^{2}} \cdot \frac{1}{W_{n}^{2}} \sum_{i, j=1}^{n} w_{i} w_{j}\left(a_{i}-a_{j}\right)^{2}\right]
\end{align*}
$$

and

$$
\begin{align*}
1 & \leq \exp \left[\frac{1}{4} m^{2} \cdot \frac{1}{W_{n}^{2}} \sum_{i, j=1}^{n} \frac{w_{i} w_{j}\left(a_{i}-a_{j}\right)^{2}}{a_{i}^{2} a_{j}^{2}}\right]  \tag{2.4}\\
& \leq \frac{G_{n}(w, a)}{H_{n}(w, a)} \\
& \leq \exp \left[\frac{1}{4} M^{2} \cdot \frac{1}{W_{n}^{2}} \sum_{i, j=1}^{n} \frac{w_{i} w_{j}\left(a_{i}-a_{j}\right)^{2}}{a_{i}^{2} a_{j}^{2}}\right] .
\end{align*}
$$

Equality holds in both (2.3) and (2.4) if and only if $a_{1}=\ldots=a_{n}$.

Proof. The proof follows by Theorem 3, choosing $f(x)=-\ln x$. For this mapping we have $f^{\prime \prime}(x)=\frac{1}{x^{2}} \in\left[\frac{1}{M^{2}}, \frac{1}{m^{2}}\right]$, and if we assume that $p_{i}=\frac{w_{i}}{W_{n}}, x_{i}=a_{i}$, then, by Theorem 3, we deduce (2.3).

The inequality (2.4) follows by (2.3) applied for $\frac{1}{a_{i}}$ instead of $a_{i}(i=1, \ldots, n)$. We omit the details.

## 3. Applications for the Shannon's Entropy

Let $X$ be a discrete random variable with the range $R=\left\{x_{1}, \ldots, x_{n}\right\}$ and the probability distribution $p_{1}, \ldots, p_{n}\left(p_{i}>0, i=1, \ldots, n\right)$. Define the Shannon entropy mapping

$$
H(X):=-\sum_{i=1}^{n} p_{i} \ln p_{i} .
$$

The following theorem is well known in the literature and concerns the maximum possible value of $H(X)$ in terms of the size of $R$ [4, p. 27].

Theorem 4. Let $X$ be defined as above. Then

$$
0 \leq H(X) \leq \ln n .
$$

Furthermore, $H(X)=\ln n$ if and only if $p_{i}=\frac{1}{n}$ for all $i \in\{1, \ldots, n\}$.
In a recent paper [3], Dragomir and Goh proved the following counterpart result.
Theorem 5. Let $X$ be defined as above. Then

$$
\begin{equation*}
0 \leq \ln n-H(X) \leq \sum_{1 \leq i<j \leq n}\left(p_{i}-p_{j}\right)^{2} . \tag{3.1}
\end{equation*}
$$

Equality holds in both inequalities simultaneously if and only if $p_{i}=\frac{1}{n}$ for all $i \in$ $\{1, \ldots, n\}$.

We wish to point out that equation (3.1) is not new, but it is rather a special case of the inequality upperbounding the Kullback-Liebler divergence by the $\chi^{2}$-divergence:

$$
\sum_{i} p_{i} \log \frac{p_{i}}{q_{i}} \leq \sum_{i} \frac{\left(q_{i}-p_{i}\right)^{2}}{q_{i}}
$$

corresponding to the case when $q$ is the uniform distribution. This inequality can be found in [12] where authors derived the inequality for evaluating the expected length of codewords of an arithmetic coding.

Before we point out another result for the entropy mapping, let us consider the following analytic inequality for the logarithmic mapping.

Lemma 1. Let $\xi_{i} \in[m, M] \subset(0, \infty), p_{i}>0(i=1, \ldots, n)$ with $\sum_{i=1}^{n} p_{i}=1$. Then

$$
\begin{align*}
0 & \leq \frac{1}{4 M^{2}} \sum_{i, j=1}^{n} p_{i} p_{j}\left(\xi_{i}-\xi_{j}\right)^{2}  \tag{3.2}\\
& \leq \ln \left(\sum_{i=1}^{n} p_{i} \xi_{i}\right)-\sum_{i=1}^{n} p_{i} \ln \xi_{i} \\
& \leq \frac{1}{4 m^{2}} \sum_{i, j=1}^{n} p_{i} p_{j}\left(\xi_{i}-\xi_{j}\right)^{2} .
\end{align*}
$$

Equality holds in all inequalities simultaneously if and only if $\xi_{1}=\ldots=\xi_{n}$.
The proof is obvious by (2.1) for the mapping $f:(0, \infty) \rightarrow \mathbb{R}, f(x)=-\ln x$.
The following theorem provides an estimation (a lower bound and an upper bound) for the distance between $H(X)$ and its maximum $\ln n$.

Theorem 6. Let $X$ be as above. Define

$$
\begin{align*}
0 & <p:=\min \left\{p_{i} \mid i=1, \ldots, n\right\}  \tag{3.3}\\
P & :=\max \left\{p_{i} \mid i=1, \ldots, n\right\}<1
\end{align*}
$$

Then we have the inequality

$$
\begin{align*}
0 & \leq \frac{1}{2} p^{2} \sum_{1 \leq i<j \leq n} \frac{\left(p_{i}-p_{j}\right)^{2}}{p_{i} p_{j}}  \tag{3.4}\\
& =\frac{1}{4} p^{2} \sum_{i, j=1}^{n} \frac{\left(p_{i}-p_{j}\right)^{2}}{p_{i} p_{j}} \\
& \leq \ln n-H(X) \\
& \leq \frac{1}{4} P^{2} \sum_{i, j=1}^{n} \frac{\left(p_{i}-p_{j}\right)^{2}}{p_{i} p_{j}} \\
& =\frac{1}{2} P^{2} \sum_{1 \leq i<j \leq n} \frac{\left(p_{i}-p_{j}\right)^{2}}{p_{i} p_{j}} .
\end{align*}
$$

Equality holds in all inequalities simultaneously if and only if $p_{i}=\frac{1}{n}$ for all $i \in$ $\{1, \ldots, n\}$.
Proof. Choose in (3.2) $\xi_{i}=\frac{1}{p_{i}} \in\left[\frac{1}{P}, \frac{1}{p}\right]$ (by the condition in (3.3)). A simple calculation gives the desired inequality (3.4).

The case of equality is also obvious.
The following corollary also holds.

Corollary 2. Let $X$ be as in Theorem 6 and $\varepsilon>0$. If

$$
\begin{equation*}
1+k-\sqrt{k(k+2)} \leq \frac{p_{i}}{p_{j}} \leq 1+k+\sqrt{k(k+2)} \tag{3.5}
\end{equation*}
$$

for $1 \leq i<j \leq n$, where

$$
k:=\frac{2 \varepsilon}{P^{2} n(n-1)}(n \geq 2)
$$

then we have the bound

$$
\begin{equation*}
0 \leq \ln n-H(X) \leq \varepsilon \tag{3.6}
\end{equation*}
$$

Proof. Consider the following inequality in $\mathbb{R}$

$$
\frac{(l-t)^{2}}{2 l t} \leq k, \quad l, \quad t>0
$$

which is equivalent to

$$
l^{2}-2(1+k) l t+t^{2} \leq 0, l, t>0
$$

i.e.,

$$
s^{2}-2(1+k) s+1 \leq 0, s=\frac{l}{t}
$$

or

$$
1+k-\sqrt{k(k+2)} \leq s \leq 1+k+\sqrt{k(k+2)} .
$$

Consequently, we can assert that

$$
1+k-\sqrt{k(k+2)} \leq \frac{p_{i}}{p_{j}} \leq 1+k+\sqrt{k(k+2)}
$$

for $1 \leq i<j \leq n$, if and only if

$$
\frac{\left(p_{i}-p_{j}\right)^{2}}{2 p_{i} p_{j}} \leq k, 1 \leq i<j \leq n
$$

Now, if (3.5) holds, then, by the second inequality in (3.4), we have

$$
\begin{aligned}
\ln n-H(X) & \leq \frac{1}{4} P^{2} \sum_{i, j=1}^{n} \frac{\left(p_{i}-p_{j}\right)^{2}}{p_{i} p_{j}} \\
& =\frac{1}{2} P^{2} \sum_{1 \leq i<j \leq n} \frac{\left(p_{i}-p_{j}\right)^{2}}{p_{i} p_{j}} \\
& =P^{2} k \cdot \frac{n(n-1)}{2} \\
& =P^{2} \cdot \frac{n(n-1)}{2} \cdot \frac{2 \varepsilon}{P^{2} n(n-1)} \\
& =\varepsilon
\end{aligned}
$$

and the estimation (3.6) is obtained.

The following corollary provides a sufficient condition for the probability distribution $p_{i}$ such that $\ln n-H(X) \geq \mu>0$ ( $\mu$ is small enough).

Corollary 3. Let $X$ be as in Theorem 6 and $\varepsilon>0$ ( $\varepsilon$ is small enough ). If

$$
\begin{equation*}
\frac{p_{i}}{p_{j}} \leq 1+\mu-\sqrt{\mu(\mu+2)} \quad \text { for } 1 \leq i<j \leq n \tag{3.7}
\end{equation*}
$$

or

$$
\begin{equation*}
\frac{p_{i}}{p_{j}} \geq 1+\mu+\sqrt{\mu(\mu+2)} \text { for } 1 \leq i<j \leq n \text {, } \tag{3.8}
\end{equation*}
$$

where

$$
\mu=\frac{2 \epsilon}{p^{2} n(n-1)},
$$

then

$$
\begin{equation*}
\ln n-H(X) \geq \epsilon>0 \tag{3.9}
\end{equation*}
$$

Proof. The elementary inequality in $\mathbb{R}$

$$
\frac{(l-t)^{2}}{2 l t} \geq \mu, l, t>0
$$

is equivalent to

$$
\begin{aligned}
s & \leq 1+\mu-\sqrt{\mu(\mu+2)} \\
\text { or } s & \geq 1+\mu+\sqrt{\mu(\mu+2)}, s=\frac{l}{t} .
\end{aligned}
$$

Consequently, if either (3.7) or (3.8) hold, then

$$
\frac{\left(p_{i}-p_{j}\right)^{2}}{2 p_{i} p_{j}} \geq \mu, \text { for all } 1 \leq i<j \leq n
$$

Using the first inequality in (3.4), we obtain

$$
\begin{aligned}
\ln n-H(X) & \geq \frac{1}{4} p^{2} \sum_{i, j=1}^{n} \frac{\left(p_{i}-p_{j}\right)^{2}}{p_{i} p_{j}} \\
& =\frac{1}{2} p^{2} \sum_{1 \leq i<j \leq n} \frac{\left(p_{i}-p_{j}\right)^{2}}{p_{i} p_{j}} \\
& \geq p^{2} \mu \cdot \frac{n(n-1)}{2} \\
& =p^{2} \cdot \frac{n(n-1)}{2} \cdot \frac{2 \varepsilon}{p^{2} n(n-1)} \\
& =\varepsilon
\end{aligned}
$$

and the estimation (3.9) is obtained.

## 4. Applications for the Rényi $\alpha$-Entropy

Define the Rényi $\alpha$-Entropy $\alpha \in((0,1) \cup(1, \infty))$ by [ 8$]$

$$
H_{\alpha}(X):=\frac{1}{1-\alpha} \ln \left(\sum_{i=1}^{n} p_{i}^{\alpha}\right)
$$

Consider the classical Jensen's discrete inequality for convex mappings, i.e.,

$$
\begin{equation*}
f\left(\sum_{i=1}^{n} p_{i} x_{i}\right) \leq \sum_{i=1}^{n} p_{i} f\left(x_{i}\right) \tag{4.1}
\end{equation*}
$$

where $f: I \subseteq \mathbb{R} \rightarrow \mathbb{R}$ is a convex mapping on $I, x_{i} \in I(i=1, \ldots, n)$ and $\left(p_{i}\right)_{i=1, \ldots, n}$ is a probability distribution. For the convex mapping $f(x)=-\ln x$ in (4.1), we obtain

$$
\begin{equation*}
\ln \left(\sum_{i=1}^{n} p_{i} x_{i}\right) \geq \sum_{i=1}^{n} p_{i} \ln x_{i} . \tag{4.2}
\end{equation*}
$$

If we choose $x_{i}:=p_{i}^{\alpha-1}(i=1, \ldots, n)$ in (4.2), we obtain

$$
\ln \left(\sum_{i=1}^{n} p_{i}^{\alpha}\right) \geq(\alpha-1) \sum_{i=1}^{n} p_{i} \ln p_{i}
$$

which is equivalent to

$$
\begin{equation*}
(1-\alpha)\left[H_{\alpha}(X)-H(X)\right] \geq 0 \tag{4.3}
\end{equation*}
$$

Now, if $\alpha \in(0,1)$, then $H_{\alpha}(X) \geq H(X)$ and if $\alpha>1$ then $H_{\alpha}(X) \leq H(X)$. Equality holds iff $\left(p_{i}\right)_{i=1, \ldots, n}$ is a uniform distribution and this fact follows by the strict convexity of $-\ln (\cdot)$.

The following theorem, which is an improvement on the inequality (4.3), holds.
Theorem 7. Let $X$ be a random variable having the probability distribution $p_{i}(i=1, \ldots, n)$ and assume that

$$
\begin{aligned}
0 & <p:=\min \left\{p_{i} \mid i=1, \ldots, n\right\} \\
P & :=\max \left\{p_{i} \mid i=1, \ldots, n\right\}<1
\end{aligned}
$$

If $\alpha \in(0,1)$, then we have the inequality

$$
\begin{align*}
& \frac{1}{4} p^{2(1-\alpha)} \sum_{i, j=1}^{n} p_{i} p_{j}\left(p_{i}^{\alpha-1}-p_{j}^{\alpha-1}\right)^{2}  \tag{4.4}\\
\leq & (1-\alpha)\left[H_{\alpha}(X)-H(X)\right] \\
\leq & \frac{1}{4} P^{2(1-\alpha)} \sum_{i, j=1}^{n} p_{i} p_{j}\left(p_{i}^{\alpha-1}-p_{j}^{\alpha-1}\right)^{2} .
\end{align*}
$$

or on the other side, if $\alpha \in(1, \infty)$, then the inequality is reversed.

Proof. We use Lemma 1 for $\xi_{i}:=p_{i}^{\alpha-1}(i=1, \ldots, n)$.
If $\alpha \in(0,1)$, then

$$
\inf _{i=1, \ldots, n} \xi_{i}=P^{\alpha-1}, \sup _{i=1, \ldots, n} \xi_{i}=p^{\alpha-1}
$$

and then, from (3.2), we can state that

$$
\begin{aligned}
& \frac{1}{4} \cdot \frac{1}{p^{2(\alpha-1)}} \sum_{i, j=1}^{n} p_{i} p_{j}\left(p_{i}^{\alpha-1}-p_{j}^{\alpha-1}\right)^{2} \\
\leq & \ln \left(\sum_{i=1}^{n} p_{i}^{\alpha}\right)-(\alpha-1) \sum_{i=1}^{n} p_{i} \ln p_{i} \\
\leq & \frac{1}{4} \cdot \frac{1}{P^{2(\alpha-1)}} \sum_{i, j=1}^{n} p_{i} p_{j}\left(p_{i}^{\alpha-1}-p_{j}^{\alpha-1}\right)^{2}
\end{aligned}
$$

and the inequality (4.4) is proved.
If $\alpha \in(1, \infty)$, then

$$
\inf _{i=1, \ldots, n} \xi_{i}=p^{\alpha-1}, \sup _{i=1, \ldots, n} \xi_{i}=P^{\alpha-1}
$$

and the rest of the process is similar.
Now, if we assume that $p_{i}=\frac{1}{n}$ in (3.2), then we get the inequality

$$
\begin{align*}
& \frac{1}{4 n^{2} M^{2}} \sum_{i, j=1}^{n}\left(\xi_{i}-\xi_{j}\right)^{2}  \tag{4.5}\\
\leq & \ln \left(\frac{1}{n} \sum_{i=1}^{n} \xi_{i}\right)-\frac{1}{n} \sum_{i=1}^{n} \ln \xi_{i} \\
\leq & \frac{1}{4 n^{2} m^{2}} \sum_{i, j=1}^{n}\left(\xi_{i}-\xi_{j}\right)^{2},
\end{align*}
$$

provided that $\xi_{i} \in[m, M] \subset(0, \infty), i=1, \ldots, n$ and $G_{n}(p):=\left(\prod_{i=1}^{n} p_{i}\right)^{\frac{1}{n}}$.
Using (4.5), we can state and prove the following inequality as well.
Theorem 8. Let $X$ and $p$ be as in Theorem 7. Then we have the inequality:

$$
\begin{align*}
& \frac{1}{4 n^{2} P^{2 \alpha}} \sum_{i, j=1}^{n}\left(p_{i}^{\alpha}-p_{j}^{\alpha}\right)^{2}  \tag{4.6}\\
\leq & (1-\alpha) H_{\alpha}(X)-\ln n-\alpha \ln G_{n}(p) \\
\leq & \frac{1}{4 n^{2} p^{2 \alpha}} \sum_{i, j=1}^{n}\left(p_{i}^{\alpha}-p_{j}^{\alpha}\right)^{2} .
\end{align*}
$$

Proof. Let $\xi_{i}:=p_{i}^{\alpha}, i=1, \ldots, n$. Then

$$
\inf _{i=1, \ldots, n} \xi_{i}=p^{\alpha}, \sup _{i=1, \ldots, n} \xi_{i}=P^{\alpha}
$$

and so, from (4.5), we can state that:

$$
\begin{aligned}
& \frac{1}{4 n^{2} P^{2 \alpha}} \sum_{i, j=1}^{n}\left(p_{i}^{\alpha}-p_{j}^{\alpha}\right)^{2} \\
\leq & (1-\alpha) H_{\alpha}(X)-\ln n-\alpha \ln G_{n}(p) \\
\leq & \frac{1}{4 n^{2} p^{2 \alpha}} \sum_{i, j=1}^{n}\left(p_{i}^{\alpha}-p_{j}^{\alpha}\right)^{2}
\end{aligned}
$$

and the inequality (4.6) is obtained.

## 5. Conclusion

The paper provides useful bounds for estimating Shannon and Rényi entropy. Rényi entropy has recently received greater popularity for estimating the average length of uniquely decodable source code codewords. If the cost of representing the codeword is linear with length, Shannon entropy is suitable, but if the cost is exponential in length, perhaps due to the cost of buffer overflows with long words, the Rényi entropy subsumes the role of Shannon entropy. Rényi entropy has also been utilised to great effect in modelling the computational complexity model of partial information available to a cryptanalyst and consequently in determining the "effective key length" in cryptosystems under guessing attacks. It is also known that Rényi entropy is closely related to the large deviations performance of guessers in guessing attacks. This paper conveys some new bounds that support the application of Rényi entropy to these important areas.

## References

[1] J. E. Pečarić, F. Proschan and Y.L. Tong, Convex Functions, Partial Orderings and Statistical Applications, Academic Press, 1992.
[2] S.S. DRAGOMIR and N.M. IONESCU, Some Converse of Jensen's inequality and applications, Anal. Num. Theor. Approx. (Cluj-Napoca), 23 (1994), 71 - 78.
[3] S.S. Dragomir and C.J. Goh, "A counterpart of Jensen's discrete inequality for differentiable convex mappings and applications in Information Theory", Math. Comput. Modelling, 24 (2), pp.1-11, 1996.
[4] R.J. McEliece, The Theory of Information and Coding, Addison Wesley Publishing Company, Reading, 1977.
[5] S.S. Dragomir and C.J. Goh, "Some bounds on entropy measures in information theory", Appl. Math. Lett., 10 (3), pp.23-28, 1997.
[6] M. Matić, Jensen's Inequality and Applications in Information Theory (in Croatian), Ph.D. Dissertation, Croatia, 1998.
[7] S.S. Dragomir, C.E.M. Pearce and J. E. Pečarić, "New inequalities for logarithmic map and their applications for entropy and mutual information", to appear Kyungpook Math. J. (Korea).
[8] A. Rényi, "On measures of entropy and information", Proc. Fourth Berkeley Symp. Math. Statist. Prob., Univ. of California Press, Vol. 1, pp.547-561, 1961.
[9] S.S. Dragomir and G. Keady, "A Hadamard-Jensen inequality for convex functions and an application to the elastic torsion problem", Applicable Analysis, 75 (3-4), pp.285-295, 2000.
[10] D. Andrica and I. Raşa, "The Jensen inequality: refinements and applications", Anal Num. Theor. Approx., 14, pp.105-108, 1985.
[11] S.S. Dragomir and C.J. Goh, "A counterpart of Jensen's continuous inequality and applications in information theory", submitted.
[12] H. Sato and H. Morita, Source Coding, lossless data compression, (edited by Society of Information Theory and Its Applications), Bifukan-Press, 1998 (in Japanese).

School of Communications and Informatics
Victoria University of Technology
PO Box 14428
Melbourne City MC 8001
Australia
sever@matilda.vu.edu.au
urladdrhttp://melba.vu.edu.au/~rgmia
Land Operations Division, DSTO, Po Box 1500, Edinburgh, SA 5111
Jadranka.Sunde@dsto.defence.gov.au
Communication Division, DSTO, Po Box 1500, Edinburgh, SA 5111
John.Asenstorfer@dsto.defence.gov.au


[^0]:    1991 Mathematics Subject Classification. 26D15, 94 Xxx.
    Key words and phrases. Convex functions, Jensen's Inequality, Shannon's Entropy, Rényi's entropy.

