# Fisher information and Stam inequality on a finite group 

Paolo Gibilisco and Tommaso Isola


#### Abstract

We prove a discrete version of the Stam inequality for random variables taking values on a finite group.


## 1. Introduction

The Fisher information $I_{X}$ of a real random variable (with strictly positive differentiable density function $f$ ) is defined as

$$
\begin{equation*}
I_{X}:=\int \frac{f^{\prime}(x)^{2}}{f(x)} d x . \tag{1.1}
\end{equation*}
$$

If $X, Y$ are independent random variables such that $I_{X}, I_{Y}<\infty$, Stam was able to prove the inequality

$$
\begin{equation*}
\frac{1}{I_{X+Y}} \geqslant \frac{1}{I_{X}}+\frac{1}{I_{Y}}, \tag{1.2}
\end{equation*}
$$

where equality holds if and only if $X, Y$ are Gaussian (see $[\mathbf{1}, \mathbf{1 7}]$ ).
This result has been very useful in a multitude of different areas: analysis, probability, statistics, information theory, statistical mechanics and so on (see [2, 4, 5, 12, 18]). Therefore it is not surprising that different proofs and generalizations have appeared in the recent literature on the subject (see, for example, $[\mathbf{1 4}, \mathbf{2 0}]$ ).

A free analogue of Fisher information has been introduced in free probability. Also, in this case one can prove a Stam-like inequality. The equality case characterizes the Wigner distribution that, in many respects, is the free analogue of the Gaussian distribution (see [19]).
Discrete versions of Fisher information and the Stam inequality are well known. On the integers $\mathbb{Z}$, equality characterizes the Poisson distribution, while on the cyclic group $\mathbb{Z}_{n}$, equality occurs for the uniform distribution (see $[\mathbf{6 - 1 1}, \mathbf{1 3}, \mathbf{1 5}, \mathbf{1 6}]$ ).

It has been observed that there are group-theoretical features in the proof of Stam inequality (see [10]). Nevertheless, up to now, inequality (1.2) has been proved only on specific groups like $\mathbb{R}, \mathbb{Z}$ and $\mathbb{Z}_{n}$. In this paper we consider the family of all finite groups and we show that, mutatis mutandis one can introduce Fisher information and prove Stam inequality on an arbitrary finite group.

## 2. Preliminaries

We recall the formulation of Stam inequality in the known cases, where it has already been proved.

### 2.1. Stam inequality on $\mathbb{R}$ and $\mathbb{R}^{n}$

Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be a differentiable, strictly positive density. One may define the Fisher $f$-score $J_{f}: \mathbb{R} \rightarrow \mathbb{R}$ by

$$
J_{f}:=\frac{f^{\prime}}{f}
$$

Let $(\Omega, \mathcal{F}, p)$ be a probability space. In general, if $X:(\Omega, \mathcal{F}, p) \rightarrow \mathbb{R}$ is a random variable with density $f$, then we write $J_{X}=J_{f}$ and define the Fisher information as

$$
I_{X}:=\operatorname{Var}_{f}\left(J_{f}\right)=E_{f}\left(J_{f}^{2}\right)
$$

namely,

$$
\begin{equation*}
I_{X}=\int_{\mathbb{R}}\left(\frac{f^{\prime}(x)}{f(x)}\right)^{2} f(x) d x \tag{2.1}
\end{equation*}
$$

Theorem $2.1[\mathbf{1}, \mathbf{1 7}]$. If $X, Y:(\Omega, \mathcal{F}, p) \rightarrow \mathbb{R}$ are independent random variables such that $I_{X}, I_{Y}<\infty$, then

$$
\begin{equation*}
\frac{1}{I_{X+Y}} \geqslant \frac{1}{I_{X}}+\frac{1}{I_{Y}} \tag{2.2}
\end{equation*}
$$

with equality if and only if $X, Y$ are Gaussian (with the same covariance).

The same result holds for random vectors. Let $f: \mathbb{R}^{n} \rightarrow \mathbb{R}$ be a differentiable, strictly positive density. We use the notation $f_{x_{i}}=\frac{\partial f}{\partial x_{i}}$. One may define the Fisher $f$-score (in the direction $x_{i}$ ) $J_{f}^{x_{i}}: \mathbb{R}^{n} \rightarrow \mathbb{R}$ by

$$
J_{f}^{x_{i}}:=\frac{f_{x_{i}}}{f}
$$

Let $(\Omega, \mathcal{F}, p)$ be a probability space. In general, if $X:(\Omega, \mathcal{F}, p) \rightarrow \mathbb{R}^{n}$ is a random vector with density $f$, then we write $J_{X}^{x_{i}}=J_{f}^{x_{i}}$ and define the Fisher information as (see [2, p. 201; 3, p. 838])

$$
I_{X}:=\sum_{i=1}^{n} E_{f}\left[\left(J_{f}^{x_{i}}\right)^{2}\right] .
$$

Note that in this case $I_{X}$ is the trace of the Fisher information matrix

$$
E_{f}\left[\frac{\partial \log (f)}{\partial x_{i}} \frac{\partial \log (f)}{\partial x_{j}}\right], \quad i, j=1, \ldots, n
$$

Theorem 2.2. If $X, Y:(\Omega, \mathcal{F}, p) \rightarrow \mathbb{R}^{n}$ are independent random vectors such that $I_{X}$, $I_{Y}<\infty$, then

$$
\begin{equation*}
\frac{1}{I_{X+Y}} \geqslant \frac{1}{I_{X}}+\frac{1}{I_{Y}} \tag{2.3}
\end{equation*}
$$

with equality if and only if $X, Y$ are Gaussian (with the same covariance matrix).

### 2.2. Stam inequality on $\mathbb{Z}$

Let $f: \mathbb{Z} \rightarrow \mathbb{R}$ be a (discrete) density. We say that $f$ belongs to the class RSP (right side positivity) if

$$
f(k)>0 \quad \Longrightarrow \quad f(k+1)>0 .
$$

If $f \in \operatorname{RSP}$, then we may define the Fisher $f$-score by

$$
J_{f}(k)= \begin{cases}\frac{f(k)-f(k-1)}{f(k)} & f(k)>0, \\ 0 & f(k)=0 .\end{cases}
$$

If $X:(\Omega, \mathcal{F}, p) \rightarrow \mathbb{Z}$ is a random variable with (discrete) density $f \in \operatorname{RSP}$, then we write $J_{X}=J_{f}$ and define the Fisher information as

$$
I_{X}:=\operatorname{Var}_{f}\left(J_{f}\right)=E_{f}\left(J_{f}^{2}\right) .
$$

Theorem $2.3[\mathbf{1 0}, \mathbf{1 6}]$. If $X, Y:(\Omega, \mathcal{F}, p) \rightarrow \mathbb{Z}$ are independent random variables with densities in RSP and such that $I_{X}, I_{Y}<\infty$, then

$$
\begin{equation*}
\frac{1}{I_{X+Y}} \geqslant \frac{1}{I_{X}}+\frac{1}{I_{Y}}, \tag{2.4}
\end{equation*}
$$

with equality if and only if $X, Y$ have (possibly shifted) Poisson distribution.

### 2.3. Stam inequality on $\mathbb{Z}_{n}$

Let $f: \mathbb{Z}_{n} \rightarrow \mathbb{R}$ be a (discrete) density that is strictly positive. We define the Fisher $f$-score by

$$
J_{f}(k)=\frac{f(k)-f(k-1)}{f(k)} .
$$

If $X:(\Omega, \mathcal{F}, p) \rightarrow \mathbb{Z}_{n}$ is a random variable with positive (discrete) density $f$, then we write $J_{X}=J_{f}$ and define the Fisher information as

$$
I_{X}:=\operatorname{Var}_{f}\left(J_{f}\right)=E_{f}\left(J_{f}^{2}\right) .
$$

Theorem 2.4 [6]. If $X, Y:(\Omega, \mathcal{F}, p) \rightarrow \mathbb{Z}$ are independent random variables with positive densities, then

$$
\begin{equation*}
\frac{1}{I_{X+Y}} \geqslant \frac{1}{I_{X}}+\frac{1}{I_{Y}}, \tag{2.5}
\end{equation*}
$$

with equality if and only if $X$ and $Y$ have uniform distribution.

In the following section we generalize this result to an arbitrary finite group.

## 3. Stam inequality on a finite group

Let $G$ be a finite group. Introduce the class $\mathcal{P}$ of strictly positive densities; that is,

$$
\mathcal{P}:=\left\{f: G \longrightarrow \mathbb{R} \mid \sum_{j \in G} f(j)=1, \quad f(k)>0 \quad \forall k \in G\right\} .
$$

We assume, from now on, that all densities belong to $\mathcal{P}$.
Let $f \in \mathcal{P}, g \in G$. In analogy with the previous definitions; we may introduce $J_{f}^{g}: G \rightarrow \mathbb{R}$, the $f$-score in the direction $g$, by

$$
J_{f}^{g}(k):=\frac{f(k)-f\left(g^{-1} k\right)}{f(k)} .
$$

Then $J_{f}^{g}$ is an $f$-centred random variable

$$
\begin{equation*}
\mathbb{E}_{f}\left[J_{f}^{g}\right]:=\sum_{k \in G} J_{f}^{g}(k) f(k)=0 . \tag{3.1}
\end{equation*}
$$

If $X:(\Omega, \mathcal{F}, p) \rightarrow G$ is a random variable with density $f_{X}(k):=p(X=k)$ and if $f_{X} \in \mathcal{P}$, then define the score $J_{X}^{g}:=J_{f}^{g}$.

Lemma 3.1. Let $g \in G$, let $X, Y:(\Omega, \mathcal{F}, p) \rightarrow G$ be two independent random variables with densities $f_{X}, f_{Y} \in \mathcal{P}$ and let $Z:=X Y$. Then

$$
J_{Z}^{g}(Z)=\mathbb{E}_{p}\left[J_{X}^{g}(X) \mid Z\right]=\mathbb{E}_{p}\left[J_{Y}^{g}(Y) \mid Z\right]
$$

Proof. Let $f_{Z}$ be the density of $Z$; namely,

$$
f_{Z}(k)=\sum_{j \in G} f_{X}(j) f_{Y}\left(j^{-1} k\right), \quad k \in G
$$

so that $f_{Z} \in \mathcal{P}$. Then

$$
\begin{aligned}
f_{Z}(k)-f_{Z}\left(g^{-1} k\right) & =\sum_{j \in G} f_{X}(j) f_{Y}\left(j^{-1} k\right)-\sum_{j \in G} f_{X}(j) f_{Y}\left(j^{-1} g^{-1} k\right) \\
& =\sum_{j \in G}\left(f_{X}(j)-f_{X}\left(g^{-1} j\right)\right) f_{Y}\left(j^{-1} k\right)
\end{aligned}
$$

Therefore, for $k \in G$,

$$
\begin{aligned}
J_{Z}^{g}(k) & =\frac{f_{Z}(k)-f_{Z}\left(g^{-1} k\right)}{f_{Z}(k)} \\
& =\sum_{j \in G} \frac{f_{X}(j) f_{Y}\left(j^{-1} k\right)}{f_{Z}(k)} \frac{f_{X}(j)-f_{X}\left(g^{-1} j\right)}{f_{X}(j)} \\
& =\sum_{j \in G} J_{X}^{g}(j) p(X=j \mid Z=k) \\
& =\mathbb{E}_{f_{X}}\left[J_{X}^{g} \mid Z=k\right] \\
& =\mathbb{E}_{p}\left[J_{X}^{g}(X) \mid Z=k\right]
\end{aligned}
$$

Similarly, by symmetry of the convolution formula one obtains

$$
J_{Z}^{g}(k)=\mathbb{E}_{p}\left[J_{Y}^{g}(Y) \mid Z=k\right], \quad k \in G
$$

proving the claim.

Lemma 3.2. Let $g \in G$, let $X, Y:(\Omega, \mathcal{F}, p) \rightarrow G$ be two independent random variables with densities $f_{X}, f_{Y} \in \mathcal{P}$ and let $Z:=X Y$. Then, for any $a, b \in \mathbb{R}$, we have

$$
\begin{equation*}
(a+b)^{2} \mathbb{E}_{p}\left[J_{Z}^{g}(Z)^{2}\right] \leqslant a^{2} \mathbb{E}_{p}\left[J_{X}^{g}(X)^{2}\right]+b^{2} \mathbb{E}_{p}\left[J_{Y}^{g}(Y)^{2}\right] \tag{3.2}
\end{equation*}
$$

Moreover, if equality holds in $(3.2)$ then $J_{X}^{g}, J_{Y}^{g}$ are constant on $G$.

Proof. By Lemma 3.1,

$$
\begin{equation*}
\mathbb{E}_{p}\left[a J_{X}^{g}(X)+b J_{Y}^{g}(Y) \mid Z\right]=a \mathbb{E}_{p}\left[J_{X}^{g}(X) \mid Z\right]+b \mathbb{E}_{p}\left[J_{Y}^{g}(Y) \mid Z\right]=(a+b) J_{Z}^{g}(Z) \tag{3.3}
\end{equation*}
$$

Hence by applying Jensen's inequality it holds that

$$
\begin{align*}
\mathbb{E}_{p}\left[\left(a J_{X}^{g}(X)+b J_{Y}^{g}(Y)\right)^{2}\right] & =\mathbb{E}_{p}\left[\mathbb{E}_{p}\left[\left(a J_{X}^{g}(X)+b J_{Y}^{g}(Y)\right)^{2} \mid Z\right]\right] \\
& \geqslant \mathbb{E}_{p}\left[\mathbb{E}_{p}\left[a J_{X}^{g}(X)+b J_{Y}^{g}(Y) \mid Z\right]^{2}\right]  \tag{3.4}\\
& =\mathbb{E}_{p}\left[(a+b)^{2} J_{Z}^{g}(Z)^{2}\right] \\
& =(a+b)^{2} \mathbb{E}_{p}\left[J_{Z}^{g}(Z)^{2}\right]
\end{align*}
$$

and thus

$$
\begin{aligned}
(a+b)^{2} \mathbb{E}_{p}\left[J_{Z}^{g}(Z)^{2}\right] & \leqslant \mathbb{E}_{p}\left[\left(a J_{X}^{g}(X)+b J_{Y}^{g}(Y)\right)^{2}\right] \\
& =a^{2} \mathbb{E}_{p}\left[J_{X}^{g}(X)^{2}\right]+2 a b \mathbb{E}_{p}\left[J_{X}^{g}(X) J_{Y}^{g}(Y)\right]+b^{2} \mathbb{E}_{p}\left[J_{Y}^{g}(Y)^{2}\right] \\
& =a^{2} \mathbb{E}_{p}\left[J_{X}^{g}(X)^{2}\right]+b^{2} \mathbb{E}_{p}\left[J_{Y}^{g}(Y)^{2}\right]
\end{aligned}
$$

where the last equality follows from independence and is due to (3.1).
We now consider the case of equality in (3.2). Set $c=a+b$, and let us prove that equality in (3.2) holds if and only if

$$
\begin{equation*}
a J_{X}^{g}(X)+b J_{Y}^{g}(Y)=c J_{Z}^{g}(X Y) \tag{3.5}
\end{equation*}
$$

Indeed, let $H:=a J_{X}^{g}(X)+b J_{Y}^{g}(Y)$; then equality in (3.4) occurs if and only if

$$
\mathbb{E}_{p}\left[H^{2} \mid Z\right]=\left(\mathbb{E}_{p}[H \mid Z]\right)^{2}
$$

that is,

$$
\mathbb{E}_{p}\left[\left(H-\mathbb{E}_{p}[H \mid Z]\right)^{2} \mid Z\right]=0
$$

Therefore $H=\mathbb{E}_{p}[H \mid Z]$ so that

$$
\mathbb{E}_{p}\left[a J_{X}^{g}(X)+b J_{Y}^{g}(Y) \mid Z\right]=a J_{X}^{g}(X)+b J_{Y}^{g}(Y)=c J_{Z}^{g}(Z)
$$

due to (3.3). Conversely, if (3.5) holds, then by applying the squared power and the expectation operator we obtain equality in (3.2).

Using (3.5), we now prove the last statement of the lemma. Let us choose a set of generators of the group $G$, that is, $\Gamma:=\left\{\gamma_{1}, \ldots, \gamma_{n}\right\} \subset G$ such that the subgroup generated by them is the whole $G$. Let us also denote $\Gamma^{-1}:=\left\{\gamma_{1}^{-1}, \ldots, \gamma_{n}^{-1}\right\}$. Now let $x, y \in G$; because of independence, for any $\gamma \in \Gamma \cup \Gamma^{-1}$,

$$
\begin{aligned}
& p(X=x \gamma, Y=y)=p(X=x \gamma) \cdot p(Y=y)>0 \\
& p(X=x, Y=\gamma y)=p(X=x) \cdot p(Y=\gamma y)>0
\end{aligned}
$$

Thus it makes sense to write equality (3.5) on

$$
A:=\{X=x \gamma\} \cap\{Y=y\} \quad \text { and } \quad B:=\{X=x\} \cap\{Y=\gamma y\}
$$

so that

$$
\begin{aligned}
& a J_{X}^{g}(x \gamma)+b J_{Y}^{g}(y)=c J_{Z}^{g}(x \gamma y) \\
& a J_{X}^{g}(x)+b J_{Y}^{g}(\gamma y)=c J_{Z}^{g}(x \gamma y)
\end{aligned}
$$

Subtracting these relations, one has

$$
a\left[J_{X}^{g}(x \gamma)-J_{X}^{g}(x)\right]=b\left[J_{Y}^{g}(\gamma y)-J_{Y}^{g}(y)\right] \quad \forall x, y \in G
$$

Therefore, for any $\gamma \in \Gamma \cup \Gamma^{-1}$, there is $a(\gamma) \in \mathbb{R}$ such that $J_{X}^{g}(x \gamma)-J_{X}^{g}(x)=a(\gamma)$, for any $x \in G$. Thus, if $n$ is the order of $\gamma$ in $G$, that is, $\gamma^{n}=e$, the identity of $G$, then

$$
J_{X}^{g}(x)=J_{X}^{g}\left(x \gamma^{n}\right)=J_{X}^{g}(x)+n a(\gamma)
$$

for any $x \in G$, which implies that $a(\gamma)=0$. Therefore

$$
\begin{equation*}
J_{X}^{g}(x \gamma)=J_{X}^{g}(x), \quad x \in G, \quad \gamma \in \Gamma \cup \Gamma^{-1} \tag{3.6}
\end{equation*}
$$

Since any $k \in G, k \neq e$, can be written as a product of elements in $\Gamma \cup \Gamma^{-1}$, that is,

$$
k=\gamma_{i_{1}} \gamma_{i_{2}} \cdot \ldots \cdot \gamma_{i_{\ell}}, \quad \text { for } \gamma_{i_{j}} \in \Gamma \cup \Gamma^{-1}
$$

we can use (3.6) iteratively, and obtain

$$
J_{X}^{g}(x k)=J_{X}^{g}\left(x \gamma_{i_{1}} \gamma_{i_{2}} \cdot \ldots \cdot \gamma_{i_{\ell}}\right)=J_{X}^{g}\left(x \gamma_{i_{1}} \gamma_{i_{2}} \cdot \ldots \cdot \gamma_{i_{\ell-1}}\right)=\ldots=J_{X}^{g}(x), \quad x \in G
$$

In particular, for $x=e$ we obtain $J_{X}^{g}(k)=J_{X}^{g}(e)$, for any $k \in G$; that is, $J_{X}^{g}$ is constant on $G$. The proof for $J_{Y}^{g}$ is analogous.

Let us now fix a set of generators of the group $G$, that is, $\Gamma:=\left\{\gamma_{1}, \ldots, \gamma_{n}\right\} \subset G$ such that the subgroup generated by them is the whole $G$. If $X:(\Omega, \mathcal{F}, p) \rightarrow G$ is a random variable with density $f_{X} \in \mathcal{P}$, then we define the Fisher information

$$
I_{X}:=\sum_{\gamma \in \Gamma} \mathbb{E}_{f}\left[\left(J_{f}^{\gamma}\right)^{2}\right]=\sum_{\gamma \in \Gamma} \sum_{k \in G}\left(\frac{f(k)-f\left(\gamma^{-1} k\right)}{f(k)}\right)^{2} f(k)
$$

Note that, due to the finiteness of $G$, the condition $I_{X}<\infty$ always holds. However, we cannot ensure in general that $I_{X} \neq 0$. In fact, it is easy to characterize this degenerate case.

Lemma 3.3. The following conditions are equivalent:
(1) $X$ has uniform distribution;
(2) $J_{X}^{\gamma}=0$, for any $\gamma \in \Gamma$;
(3) $I_{X}=0$;
(4) $J_{X}^{\gamma}$ is constant, for any $\gamma \in \Gamma$.

Proof. The implications $(1) \Rightarrow(2) \Rightarrow(4)$ are immediately proved. The equivalence of (2) and (3) is also easy to show.
Therefore, it is enough to prove that (4) implies (1). Therefore, for any $\gamma \in \Gamma$ there is $a(\gamma) \in \mathbb{R}$ such that $J_{X}^{\gamma}(x)=a(\gamma)$, for any $x \in G$; that is, with $f \equiv f_{X},\left(f(x)-f\left(\gamma^{-1} x\right)\right) / f(x)=a(\gamma)$, for any $x \in G$, which is equivalent to

$$
\begin{equation*}
(1-a(\gamma)) f(x)=f\left(\gamma^{-1} x\right), \quad x \in G \tag{3.7}
\end{equation*}
$$

Thus if $n$ is the order of $\gamma^{-1}$ in $G$, that is, $\gamma^{-n}=e$, the identity of $G$, then

$$
(1-a(\gamma))^{n} f(x)=(1-a(\gamma))^{n-1} f\left(\gamma^{-1} x\right)=\ldots=f\left(\gamma^{-n} x\right)=f(x)
$$

for any $x \in G$, which implies that $a(\gamma)=0$. Therefore,

$$
\begin{equation*}
f\left(\gamma^{-1} x\right)=f(x), \quad x \in G, \quad \gamma \in \Gamma \tag{3.8}
\end{equation*}
$$

From this it also follows that

$$
\begin{equation*}
f(\gamma x)=f(x), \quad x \in G, \quad \gamma \in \Gamma \tag{3.9}
\end{equation*}
$$

Since any $k \in G, k \neq e$, can be written as a product of elements in $\Gamma \cup \Gamma^{-1}$, that is,

$$
k=\gamma_{i_{1}} \gamma_{i_{2}} \cdot \ldots \cdot \gamma_{i_{\ell}}, \quad \text { for } \gamma_{i_{j}} \in \Gamma \cup \Gamma^{-1}
$$

we can use (3.8) and (3.9) iteratively, and obtain

$$
f(k x)=f\left(\gamma_{i_{1}} \gamma_{i_{2}} \cdot \ldots \cdot \gamma_{i_{\ell}} x\right)=f\left(\gamma_{i_{2}} \cdot \ldots \cdot \gamma_{i_{\ell}} x\right)=\ldots=f(x), \quad x \in G
$$

In particular, for $x=e$ we obtain $f(k)=f(e)$, for any $k \in G$; that is, $f$ is constant on $G$; that is, $X$ is uniform. This concludes the proof.

Let us also recall the following result, which is immediate by using the convolution formula.

Proposition 3.4. If $X, Y:(\Omega, \mathcal{F}, p) \rightarrow G$ are independent random variables and $X$ is uniform then also $Z=X Y$ is uniform.

Proposition 3.5. Let $X, Y:(\Omega, \mathcal{F}, p) \rightarrow$ be independent random variables such that their densities belong to $\mathcal{P}$. If $X$ or $Y$ has uniform distribution, then

$$
\frac{1}{I_{X Y}}=\frac{1}{I_{X}}+\frac{1}{I_{Y}}
$$

in the sense that both sides of equality are equal to infinity.

Proof. Let $Z=X Y$. If $X$ is uniform, then $Z$ is uniform by Proposition 3.4, and by Lemma 3.3 the proof is complete.

Because of the above proposition, it remains to consider random variables with strictly positive Fisher information.

We are ready to prove the main result.

Theorem 3.6. Let $X, Y:(\Omega, \mathcal{F}, p) \rightarrow G$ be two independent random variables such that $I_{X}, I_{Y}>0$. Then

$$
\begin{equation*}
\frac{1}{I_{X Y}}>\frac{1}{I_{X}}+\frac{1}{I_{Y}} \tag{3.10}
\end{equation*}
$$

Proof. Define $Z:=X Y$, and let $a, b \in \mathbb{R}$. Then for any $\gamma \in \Gamma$ we have, from (3.2):

$$
\begin{equation*}
(a+b)^{2} \mathbb{E}_{p}\left[J_{Z}^{\gamma}(Z)^{2}\right] \leqslant a^{2} \mathbb{E}_{p}\left[J_{X}^{\gamma}(X)^{2}\right]+b^{2} \mathbb{E}_{p}\left[J_{Y}^{\gamma}(Y)^{2}\right] \tag{3.11}
\end{equation*}
$$

Summing over $\gamma \in \Gamma$, we obtain

$$
\begin{aligned}
(a+b)^{2} I_{Z} & =(a+b)^{2} \sum_{\gamma \in \Gamma} \mathbb{E}_{p}\left[J_{Z}^{\gamma}(Z)^{2}\right] \\
& \leqslant a^{2} \sum_{\gamma \in \Gamma} \mathbb{E}_{p}\left[J_{X}^{\gamma}(X)^{2}\right]+b^{2} \sum_{\gamma \in \Gamma} \mathbb{E}_{p}\left[J_{Y}^{\gamma}(Y)^{2}\right] \\
& =a^{2} I_{X}+b^{2} I_{Y}
\end{aligned}
$$

Now, take $a:=1 / I_{X}$ and $b:=1 / I_{Y}$; then we obtain

$$
\left(\frac{1}{I_{X}}+\frac{1}{I_{Y}}\right)^{2} I_{Z} \leqslant \frac{1}{I_{X}}+\frac{1}{I_{Y}}
$$

It remains to be proved that the equality sign cannot hold in (3.10). To this purpose, define $c:=a+b$, where again $a=1 / I_{X}$ and $b=1 / I_{Y}$; then equality holds if and only if

$$
c^{2} I_{Z}=a^{2} I_{X}+b^{2} I_{Y}
$$

This implies equality in (3.11), for any $\gamma \in \Gamma$. From Lemma 3.2 it follows that $J_{X}^{\gamma}, J_{Y}^{\gamma}$ are constant on $G$, for any $\gamma \in \Gamma$. But then, from Lemma 3.3, $I_{X}=I_{Y}=0$, which is absurd. Therefore equality cannot hold in (3.10).

## References

1. N. M. Blachman, 'The convolution inequality for entropy powers', IEEE Trans. Inform. Theory 11 (1965) 267-271.
2. E. Carlen, 'Superadditivity of Fisher's information and logarithmic Sobolev inequalities', J. Funct. Anal. 101 (1991) 194-211.
3. M. H. M. Costa and T. Cover, 'On the similarity of the entropy power inequality and the BrunnMinkowski inequality', IEEE Trans. Inform. Theory IT-30 (1984) 837-839.
4. A. Dembo, T. Cover and J. Thomas, 'Information theoretic inequalities', IEEE Trans. Inform. Theory 37 (1991) 1501-1518.
5. R. J. Gardner, 'The Brunn-Minkowski inequality', Bull. Amer. Math. Soc. 39 (2002) 355-405.
6. P. Gibilisco, D. Imparato and T. Isola, 'Stam inequality on $\mathbb{Z}_{n}$ ', Stat. Probab. Lett. (2008), to appear, doi:10.1016/j.spl.2008.01.040.
7. P. Harremoes, 'Binomial and Poisson distribution as maximum entropy distributions', IEEE Trans. Inform. Theory 47 (2001) 2039-2041.
8. O. T. Johnson, 'Log-concavity and the maximum entropy property of the Poisson distribution', Stoch. Proc. Appl. 117 (2007) 791-802.
9. I. M. Johnstone and B. MacGibbon, 'Une mesure d'information caractérisant la loi de Poisson', Séminaire de Probabilités, XXI, Lecture Notes in Mathematics 1247 (Springer, Berlin, 1987) 563-573.
10. A. Kagan, 'A discrete version of Stam inequality and a characterization of the Poisson distribution', J. Statist. Plann. Inference 92 (2001) 7-12.
11. A. Kagan, 'Letter to the editor: "A discrete version of Stam inequality and a characterization of the Poisson distribution"' [J. Statist. Plann. Inference 92 (2001) 7-12], J. Statist. Plann. Inference 99 (2001) 1.
12. A. KAGAN and Z. Landsman, 'Statistical meaning of Carlen's superadditivity of the Fisher information', Stat. Probab. Lett. 32 (1997) 175-179.
13. I. Kontoyiannis, P. Harremoës and O. Johnson, 'Entropy and the law of small numbers', IEEE Trans. Inform. Theory 51 (2005) 466-472.
14. M. Madiman and R. A. Barron, 'Generalized entropy power inequalities and monotonicity properties of information', IEEE Trans. Inform. Theory 53 (2007) 2317-2329.
15. M. Madiman, O. Johnson and I. Kontoyiannis, 'Fisher information, compound Poisson approximation and the Poisson channel', Proc. IEEE Int. Symp. Inform. Theory, Nice, France, 2007.
16. V. Papathanasiou, 'Some characteristic properties of the Fisher information matrix via Cacoullos-type inequalities', J. Multivariate Anal. 44 (1993) 256-265.
17. A. J. Stam, 'Some inequalities satisfied by the quantities of information of Fisher and Shannon', Inform. Control 2 (1959) 101-112.
18. C. Villani, 'Cercignani's conjecture is sometimes true and always almost true', Comm. Math. Phys. 234 (2003) 455-490.
19. D. Voiculescu, 'The analogues of entropy and of Fisher's information measure in free probability theory. V. Noncommutative Hilbert transforms', Invent. Math. 132 (1998) 189-227.
20. R. Zamir, 'A proof of the Fisher information inequality via a data processing argument', IEEE Trans. Inform. Theory 44 (1998) 1246-1250.

## Paolo Gibilisco

Dipartimento SEFEMEQ
Facoltà di Economia
Università di Roma 'Tor Vergata'
Via Columbia 2

## 00133 Rome

## Italy

gibilisco@volterra.uniroma2.it
http://www.economia.uniroma2.it/ sefemeq/professori/gibilisco

## Tommaso Isola

Dipartimento di Matematica
Università di Roma 'Tor Vergata'
Via della Ricerca Scientifica 00133 Rome
Italy
isola@mat.uniroma2.it
http://www.mat.uniroma2.it/~isola

