

# Counterexamples to a Proposed Stam Inequality on Finite Groups

Venkat Anantharam, *Fellow, IEEE*

**Abstract**—Gibilisco and Isola have recently proposed a definition of Fisher information for random variables taking values in a finite group that is analogous to the definition for real valued random variables with a density. Based on this Fisher information concept, they claim to prove a Stam inequality for finite-group valued random variables that is analogous to the one in the case of real values. In this note we show these results, unfortunately, do not hold for nonabelian groups in general, by constructing explicit counterexamples.

**Index Terms**—Finite group, Fisher information, group-valued random variables, Stam inequality.

## I. INTRODUCTION

FOR a real-valued random variable  $X$  with differentiable density  $f_X(x)$ , the Fisher information is defined by [2, Eqn. (17.69)]

$$I_X := \int_{-\infty}^{\infty} \left[ \frac{\partial}{\partial x} \frac{f_X(x)}{f_X(x)} \right]^2 f_X(x) dx = E[J_X(X)^2]$$

where

$$J_X(x) := \frac{\partial}{\partial x} \frac{f_X(x)}{f_X(x)}$$

is called the score function of  $X$  [2, Eqn. (11.264)]. Since  $E[J_X(X)] = 0$ , the Fisher information is the variance of the score [2, p. 394]. If  $X$  and  $Y$  are independent random variables and  $Z := X + Y$ , one has the remarkable inequality of Stam [2, Eqn. (17.88)], [10]

$$\frac{1}{I_Z} \geq \frac{1}{I_X} + \frac{1}{I_Y}.$$

As is well known, this underlies the powerful and extremely useful entropy-power inequality [1], [2, Sec. 17.8], [9], [11].

Let  $G$  be a finite group and let  $X$  be a  $G$ -valued random variable having strictly positive probability distribution. See [5] or any other decent book covering group theory for basic facts

about finite groups. Given  $g \in G$ , Gibilisco and Isola [4] define the function  $J_X^g$  on  $G$  by

$$J_X^g(h) := \frac{f_X(h) - f_X(g^{-1}h)}{f_X(h)} \quad (1)$$

where  $f_X(h) := P(X = h)$  for  $h \in G$  and the left multiplication of  $h_1 \in G$  by  $h_2 \in G$  is simply written as  $h_2 h_1$ . This is analogous to the score function in the case of real valued random variables. Indeed, one can immediately check that  $E[J_X^g(X)] = 0$  [4, Eqn. (3.1)]. Let  $\Gamma := \{\gamma_1, \dots, \gamma_n\}$  be a fixed set of generators for  $G$ . Gibilisco and Isola [4] make the interesting definition

$$I_X := \sum_{\gamma \in \Gamma} E \left[ (J_X^\gamma(X))^2 \right].$$

They call  $I_X$  the “Fisher information” of  $X$ . Of course, it depends on the choice of generators for  $G$ .

Given independent  $G$ -valued random variables  $X$  and  $Y$  with strictly positive distributions, let  $Z = XY$  denote their product. It is claimed in [4, Eqn. (3.10)] that

$$\frac{1}{I_{XY}} \geq \frac{1}{I_X} + \frac{1}{I_Y}, \quad (\text{this is actually false}) \quad (2)$$

and this is called “the Stam inequality on the finite group  $G$ .” Since every finite abelian group can be written as a direct sum of cyclic groups [5, Thm. II.2.1], the kind of “Fisher information” defined in [4] essentially reduces, in the case of finite abelian groups, to a discussion on  $\mathbf{Z}_n$ , the group of integers modulo  $n$ . This case has been published separately in [3]. Notable developments in the train of thought motivating the definition in (1) and the claimed inequality (2) include [6], [7], and [8].

The main purpose of our note is to point out that the “Stam inequality” of (2) claimed in [4] is actually wrong for nonabelian groups. We do this by illustrating how to construct counterexamples and giving an explicit counterexample. The nature of our counterexample illustrates the difficulty in proving such a result and also identifies where the problem lies in [4].

## II. COUNTEREXAMPLES

Consider the symmetric group  $S_3$  of permutations on three letters. We list its elements as

$$S_3 = \{e, (12), (13), (23), (123), (132)\}$$

using the notation  $e$  for the identity permutation and cycle notation [5, Sec. I.6] for the other entries. Since  $(12) * (13) = (132) \neq (123) = (13) * (12)$ , the group is nonabelian.

Fix  $0 < \alpha < 1$ . Let  $X$  be an  $S_3$ -valued random variable with

$$P(X = g) = \frac{1 - \alpha}{6} \quad \text{for } g \neq (12)$$

Manuscript received July 28, 2009; revised November 14, 2009. Current version published March 17, 2010. The work of V. Anantharam was partially supported by the NSF by Grants CCF-0500023, CCF-0635372, and CNS-0627161, by the ARO MURI Grant W911NF-08-1-0233, by Marvell Semiconductor Inc., ST Microelectronics Inc., the U.C. Micro program, and by the U. C. Discovery program.

The author is with the Department of Electrical Engineering and Computer Sciences, University of California, Berkeley, CA 94720 USA (e-mail: ananth@eecs.berkeley.edu).

Communicated by I. Kontoyiannis, Associate Editor for Shannon Theory.

Digital Object Identifier 10.1109/TIT.2010.2040972

and

$$P(X = (12)) = \alpha + \frac{1 - \alpha}{6}.$$

Let  $Y$  be an  $S_3$ -valued random variable with

$$P(Y = g) = \frac{1 - \alpha}{6} \quad \text{for } g \neq (23)$$

and

$$P(Y = (23)) = \alpha + \frac{1 - \alpha}{6}.$$

Assume that  $X$  and  $Y$  are independent. Let  $Z = X * Y$ . Then one can verify that

$$P(Z = g) = \frac{1 - \alpha^2}{6} \quad \text{for } g \neq (123)$$

and

$$P(Z = (123)) = \alpha^2 + \frac{1 - \alpha^2}{6}.$$

For the group  $S_3$ , with  $X, Y$ , and  $Z = X * Y$  as above, the last line of the proof of [4, Lemma 3.1] states that for every  $g, h \in S_3$  we have

$$J_Z^g(h) = E[J_Y^g(Y) | Z = h], \text{ (this is actually false).} \quad (3)$$

However, if one takes  $g = (132)$  and  $h = e$  for instance, one can check that this statement is false for all  $0 < \alpha < 1$ . To see this, observe that

$$f_Z(g^{-1}h) = f_Z((123)) = \alpha^2 + \frac{1 - \alpha^2}{6}.$$

On the other hand, if we consider

$$\sum_{u \in G} f_X(hu^{-1})f_Y(g^{-1}u) = \sum_{u \in S_3} f_X(u^{-1})f_Y((123) * u)$$

then, since  $u^{-1} = (12)$  would imply that  $(123) * u = (123) * (12) = (13) \neq (23)$ , this sum equals

$$4 \left( \frac{1 - \alpha}{6} \right)^2 + 2 \left( \alpha + \frac{1 - \alpha}{6} \right) \left( \frac{1 - \alpha}{6} \right) = \frac{1 - \alpha^2}{6}$$

so for this example, for all  $0 < \alpha < 1$ , the two sides of (3) cannot be equal.

Indeed, for a general finite group  $G$ , independent  $G$ -valued random variables  $X$  and  $Y$  with strictly positive distributions, and  $Z = XY$ , the left-hand side (LHS) of (3) is given by

$$J_Z^g(h) = \frac{f_Z(h) - f_Z(g^{-1}h)}{f_Z(h)}$$

by definition, while the right-hand side (RHS) may be manipulated to read

$$E[J_Y^g(Y) | Z = h] = \frac{f_Z(h) - (\sum_{u \in G} f_X(hu^{-1})f_Y(g^{-1}u))}{f_Z(h)}.$$

To require equality in (3) is in effect to require that

$$f_Z(g^{-1}h) \stackrel{?}{=} \sum_{u \in G} f_X(hu^{-1})f_Y(g^{-1}u)$$

for all  $h, g \in G$ . This can hardly be expected to be the case for a nonabelian group. This is the source of the problem in [4].

We next give an explicit counterexample in the nonabelian case to the inequality (2) called “the Stam inequality on a finite group” in [4]. Consider again the group  $S_3$ , and consider the set of generators  $\Gamma = \{(12), (13)\}$ . Examples showing that (2) is false can be constructed by perturbing the kinds of random variables considered in proving that (3) is wrong. Listing the elements of  $S_3$  as  $\{e, (12), (13), (23), (123), (132)\}$  as above, we may, for instance, let  $X$  have the distribution

$$(0.003, 0.990, 0.003, 0.002, 0.001, 0.001)$$

and  $Y$  have the distribution

$$(0.002, 0.002, 0.990, 0.002, 0.001, 0.003)$$

with  $X$  and  $Y$  being independent, which results in  $Z := X * Y$  having the distribution

$$(0.004964, 0.002987, 0.005952, 0.002001, 0.003974, 0.980122).$$

One can verify that for this choice one has

$$\frac{1}{I_Z} = 0.0015637 < 0.0019937 = \frac{1}{I_X} + \frac{1}{I_Y}$$

where the precise numerical values have been rounded off.

Exact computation of the “Fisher information” terms  $I_X, I_Y$  and  $I_Z$  requires some work, but one can also accurately estimate them by recognizing that in each of the functions  $g \mapsto f_X(g)(J_X^{(12)}(g))^2, g \mapsto f_X(g)(J_X^{(13)}(g))^2, g \mapsto f_Y(g)(J_Y^{(12)}(g))^2, g \mapsto f_Y(g)(J_Y^{(13)}(g))^2, g \mapsto f_Z(g)(J_Z^{(12)}(g))^2$ , and  $g \mapsto f_Z(g)(J_Z^{(13)}(g))^2$  there is a single overwhelmingly dominant term. One can easily compute this dominant term by hand in each case and thus convince oneself that this numerical example does demonstrate that (2) is wrong.

The pattern that we used to construct the counterexample to (2) and (3) can also be used in other nonabelian groups. It remains an interesting question if a “Stam inequality” can be proved for group-valued random variables in the nonabelian case for an appropriate notion of “Fisher information.”

### REFERENCES

- [1] N. M. Blachman, “The convolution inequality for entropy powers,” *IEEE Trans. Inf. Theory*, vol. IT-11, pp. 267–271, 1965.
- [2] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ: Wiley-Interscience, 2006.
- [3] P. Gibilisco, D. Iparato, and T. Isola, “Stam inequality on  $Z_n$ ,” *Statist. Probabil. Lett.*, vol. 78, pp. 1851–1856, 2008.
- [4] P. Gibilisco and T. Isola, “Fisher information and Stam inequality on a finite group,” *Bull. London Math. Soc.*, vol. 40, pp. 855–862, 2008.
- [5] T. W. Hungerford, *Algebra*. New York: Springer-Verlag, 1974.
- [6] A. Kagan, “A discrete version of the Stam inequality and a characterization of the Poisson distribution,” *J. Statist. Plann. Inference*, vol. 92, pp. 7–12, 2001.
- [7] I. Kontoyiannis, P. Harremoës, and O. Johnson, “Entropy and the law of small numbers,” *IEEE Trans. Inf. Theory*, vol. IT-51, pp. 466–472, 2005.

- [8] M. Madiman, O. Johnson, and I. Kontoyiannis, "Fisher information, compound Poisson approximation, and the Poisson channel," in *Proc. Int. Symp. Inf. Theory (ISIT)*, Nice, France, 2007, pp. 976–980.
- [9] M. Madiman and A. Barron, "Generalized entropy power inequalities and monotonicity properties of information," *IEEE Trans. Inf. Theory*, vol. IT-53, pp. 2317–2329, 2007.
- [10] A. J. Stam, "Some inequalities satisfied by the quantities of information of Fisher and Shannon," *Inf. Control*, vol. 2, pp. 101–112, 1959.
- [11] S. Verdú and D. Guo, "A simple proof of the entropy-power inequality," *IEEE Trans. Inf. Theory*, vol. IT-52, pp. 2165–2166, 2006.

**Venkat Anantharam** (M'86–SM'96–F'98) received the B.Tech. degree in electronics in 1980 from the Indian Institute of Technology, Madras (IIT-M), and the M.A. and C.Phil. degrees in mathematics and the M.S. and Ph.D. degrees in electrical engineering in 1983, 1984, 1982, and 1986, respectively, all from the University of California, Berkeley (UCB).

From 1986 to 1994, he was on the faculty of the School of Electrical Engineering, Cornell University, Ithaca, NY. Since 1994, he has been with the Electrical Engineering and Computer Science Department, UCB.

Dr. Anantharam received the Philips India Medal and the President of India Gold Medal from IIT-M in 1980, and an NSF Presidential Young Investigator award (1988–1993). He is a corecipient of the 2000 Stephen O. Rice Prize Paper award of the IEEE Communications Theory Society (with N. McKeown and J. Walrand). He received the Distinguished Alumnus Award from IIT-M in 2008.