CORRIGENDUM TO SECRET SHARING ON INFINITE GRAPHS

LÁSZLÓ CSIRMAZ

ABSTRACT. The proof of Claim 6.8 in the Appendix of [L. Csirmaz: *Secret sharing on infinite graphs*, Tatra Mt. Math. Publ. **41** (2008), 1–18] is incorrect. Here we give a new (and hopefully correct) proof.

1. Introduction

The proof of Claim 6.8 in the Appendix of [1] is incorrect. I am indebted to Professor Hamiredza Maimani [2] who called my attention to the error.

2. The new proof

CLAIM 2.1. *The information ratio of the graph G depicted on Figure 1 is 2.*

FIGURE 1. The graph G .

Proof. The proof of the first part of the claim, namely that $R(G) \leq 2$ was correct. G is a spanned subgraph of the 2-lattice, and the 2-lattice has information ratio 2. For proving the lower bound we use the method outlined in the paper [1]. Let f be any function satisfying the Shannon inequalities (a)–(e) enlisted there, we claim that

$$f(bc) + f(BC) \geq 8. \quad (1)$$

2010 Mathematics Subject Classification: 68P25, 94A60.

Keywords: secret sharing scheme, information theory, infinite graph, lattice.

As $f(b) + f(c) + f(B) + f(C) \geq f(bc) + f(BC) \geq 8$, at least one of $f(b)$, $f(c)$, $f(B)$, and $f(C)$ must be ≥ 2 , thus the lower bound 2 follows.

To get inequality (1) we use instances of the Shannon inequalities (a)–(e) as follows:

$$\begin{array}{l}
 f(a) + f(b) \geq f(ab) \\
 f(ab) + f(bc) \geq 1 + f(b) + f(abc) \\
 f(acBD) - f(acD) \geq f(acABD) - f(acAD) \geq 1 \\
 f(acBCD) - f(acBD) \geq 1 \\
 f(ac) - f(a) \geq f(acC) - f(aC) \\
 f(acC) - f(aC) \geq 1 + f(acBCD) - f(aBCD) \\
 f(abc) - f(ac) \geq f(abcD) - f(acD) \\
 \hline
 f(bc) \geq 4 + f(abcD) - f(aBCD).
 \end{array}$$

Now the graph G is invariant under the following permutation of the vertices: $a \leftrightarrow D$, $b \leftrightarrow C$, $c \leftrightarrow B$, $d \leftrightarrow A$, thus applying this transformation to the above inequality we get another valid inequality for our graph:

$$f(CB) \geq 4 + f(DCBa) - f(Dcba).$$

Adding these latter two inequalities we get (1), as required. $\square$

REFERENCES

- [1] CSIRMAZ, L.: *Secret sharing on infinite graphs*, Tatra Mt. Math. Publ. **41** (2008), 1–18.
- [2] MAIMANI, H.: Personal communication, November, 2009.

Received November 11, 2009

*Computer and Statistic Center
Central European University
Nádor útca 9
H-1051 Budapest
HUNGARY
E-mail: csirmaz@renyi.hu*