ARTICLE IN PRESS

Discrete Applied Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

The optimal average information ratio of secret-sharing schemes for the access structures based on unicycle graphs and bipartite graphs

Hui-Chuan Lu [a,*], Hung-Lin Fu [b]

[a] Center for Basic Required Courses, National United University, Miaoli, 36003, Taiwan
[b] Department of Applied Mathematics, National Chiao Tung University, Hsinchu, 30010, Taiwan

ARTICLE INFO

Article history:
Received 5 October 2016
Received in revised form 29 July 2017
Accepted 4 August 2017
Available online xxxx

Keywords:
Secret-sharing scheme
Average information ratio
Complete multipartite covering
Star decomposition
Fractional star covering
Maximum independent set
Bipartite graph
Unicycle graph

ABSTRACT

In this paper, we derive bounds on the optimal average information ratio of the access structures based on general graphs and investigate the value of the ratio for unicycle graphs and some bipartite graphs. We determine the exact values of this ratio for some infinite classes of bipartite graphs and unicycle graphs. This extends previous results. We also provide good bounds on the optimal average information ratio for all unicycle graphs.

1. Introduction

A *secret-sharing scheme* on a simple graph G is a protocol by which the dealer distributes the shares among the vertices of G privately in such a way that only the sets of vertices containing an edge of G can recover the secret, and the shares given to any independent set in G reveal no information about the secret. If we let the random variable ζ_S be the secret and ζ_v be the share of v, $v \in V(G)$, then a secret-sharing scheme Σ on G is a collection of random variables ζ_S and ζ_v, for all $v \in V(G)$, with a joint distribution such that

(i) if $uv \in E(G)$, then ζ_u and ζ_v together determine the value of ζ_S;
(ii) if $A \subseteq V(G)$ is an independent set in G, then ζ_S and the collection $\{\zeta_v | v \in A\}$ are statistically independent.

The information ratio of the scheme Σ can be defined, using Shannon entropy H, as $R_\Sigma = \max_{v \in V(G)}\{H(\zeta_v)/H(\zeta_S)\}$ and the average information ratio of Σ is defined as $AR_\Sigma = \sum_{v \in V(G)} H(\zeta_v)/(|V(G)|H(\zeta_S))$. The optimal information ratio $R(G)$ of G and the optimal average information ratio $AR(G)$ of G are the infimum of the information ratio and the average information ratio over all possible secret-sharing schemes on G respectively.

Due to the difficulty of determining the exact values of $R(G)$ and $AR(G)$, most known results give bounds on them [2–8,10,13,15–18]. The exact values of the optimal average information ratio of most graphs of order no more than five

* Corresponding author.
E-mail addresses: hjlu@nuu.edu.tw (H.-C. Lu), hlfu@math.nctu.edu.tw (H.-L. Fu).

http://dx.doi.org/10.1016/j.dam.2017.08.006
0166-218X/

Notations

$R(G)$:	the optimal information ratio of G
$AR(G)$:	the optimal average information ratio of G
$V(G)$:	the vertex set of G
$E(G)$:	the edge set of G
n_{Π}:	the vertex-number sum of the star covering Π
girth(G):	the girth of G
$\tilde{c}^*(T)$:	the minimum size of a core cluster of G
$\alpha(T)$:	the independence number of G
$d_G(v)$:	the degree of v in G
$\vec{G}_{\Pi}$:	a directed graph induced by a star decomposition Π of G
$\vec{G}_{\Pi}[V']$:	the subgraph of $\vec{G}_{\Pi}$ induced by V'
$d^-_{\vec{G}_{\Pi}}(v)$:	the indegree of v in the directed graph $\vec{G}_{\Pi}$
$m^-_{V'}$:	the number of directed edges in $\vec{G}_{\Pi}$ whose heads are in $V' \subseteq V(G)$ and whose tails are outside V'
$E_{(L)}$:	the fan associated with the maximum independent set L
$H + E^+_H$:	the extended graph of the subgraph H of G by adding the edges in E^+_H to H
diam(H):	the diameter of G
$d(e_1, e_2)$:	the distance of two distinct edges e_1 and e_2 of G
C_G:	the unique cycle in the unicycle graph G
$\mathscr{F}$:	the collection of all odd unicycle graphs with at least one Type I subtree and all even unicycle graphs

and the optimal information ratio of most graphs of order no more than six have been determined [7,13,18]. Before 2007, apart from a specially defined class of graphs [6], the paths and cycles were the only infinite classes of graphs whose optimal information ratio and optimal average information ratio are known. Csirmaz and Tardos's [12] excellent work appeared in 2007. They determined the exact value of the optimal information ratio of all trees. In 2009, Csirmaz and Ligeti [11] showed that $R(G) = 2 - 1/d$, where d is the maximum degree of G, for any graph G satisfying the following conditions: (i) every vertex has at most one neighbor of degree one; (ii) vertices of degree at least three are not connected by an edge; (iii) the girth of G is at least six. In 2012, Lu and Fu [14] went on settling the exact values of the optimal average information ratio of all trees. Recently Beimel et al. [1] investigated the total share size of secret-sharing schemes realizing very dense graphs and showed excellent results. In this paper, we deal with the optimal average information ratio of unicycle graphs and some bipartite graphs.

This paper is organized as follows. In Section 2, we recall basic definitions and some known results. Some bounds on the optimal average information ratio for general graphs are derived in Section 3. In Section 4, we investigate the problem for bipartite graphs and determine the exact values of this ratios for some infinite classes of bipartite graphs. This extends the result in [14]. Subsequently, we determine the values of the optimal average information ratio for some unicycle graphs and give good bounds on this ratio for all unicycle graphs in Section 5. A concluding remark will be given in Section 6.

2. Preliminaries

In this section, we introduce some basic notions and important results for our discussion in the following sections. All graphs considered in this paper are simple connected graphs without loops and isolated vertices. The vertex number $|V(G)|$ of a graph G is called the *order* of G and the edge number $|E(G)|$ of G is the *size* of it. In addition, the minimum length of a cycle in G is referred to as the *girth* of G and is denoted as girth(G). We collect all the notations used at the end of this paper. For connected graphs with at least two vertices, it is well known that $R(G) \geq AR(G) \geq 1$ [9] and that $R(G) = 1$ if and only if $AR(G) = 1$. Birckell and Davenport [2] have given a complete characterization of the graphs with $R(G) = 1$.

Theorem 2.1 ([2]). *Suppose that G is a connected graph. Then $R(G) = AR(G) = 1$ if and only if G is a complete multipartite graph.*

For graphs which are not complete multipartite, we consider bounds on $AR(G)$. The average information ratio of any secret-sharing scheme on G makes a natural upper bound on $AR(G)$. Stinson's decomposition construction [17] enables us to build up a secret-sharing scheme on a graph via its *complete multipartite covering*. A complete multipartite covering of a graph G is a collection of complete multipartite subgraphs $\Pi = \{G_1, G_2, \ldots, G_l\}$ of G such that each edge of G appears in at least one subgraph in this collection. The sum $n_{\Pi} = \sum_{i=1}^{l} |V(G_i)|$ is called the *vertex-number sum* of Π.

Theorem 2.2 ([17]). *Suppose that $\Pi = \{G_1, G_2, \ldots, G_l\}$ is a complete multipartite covering of a graph G of order n. Then there exists a secret-sharing scheme Σ on G with average information ratio $AR_{\Sigma} = n_{\Pi}/n$.*

Please cite this article in press as: H.-C. Lu, H.-L. Fu, The optimal average information ratio of secret-sharing schemes for the access structures based on unicycle graphs and bipartite graphs, Discrete Applied Mathematics (2017), http://dx.doi.org/10.1016/j.dam.2017.08.006.