



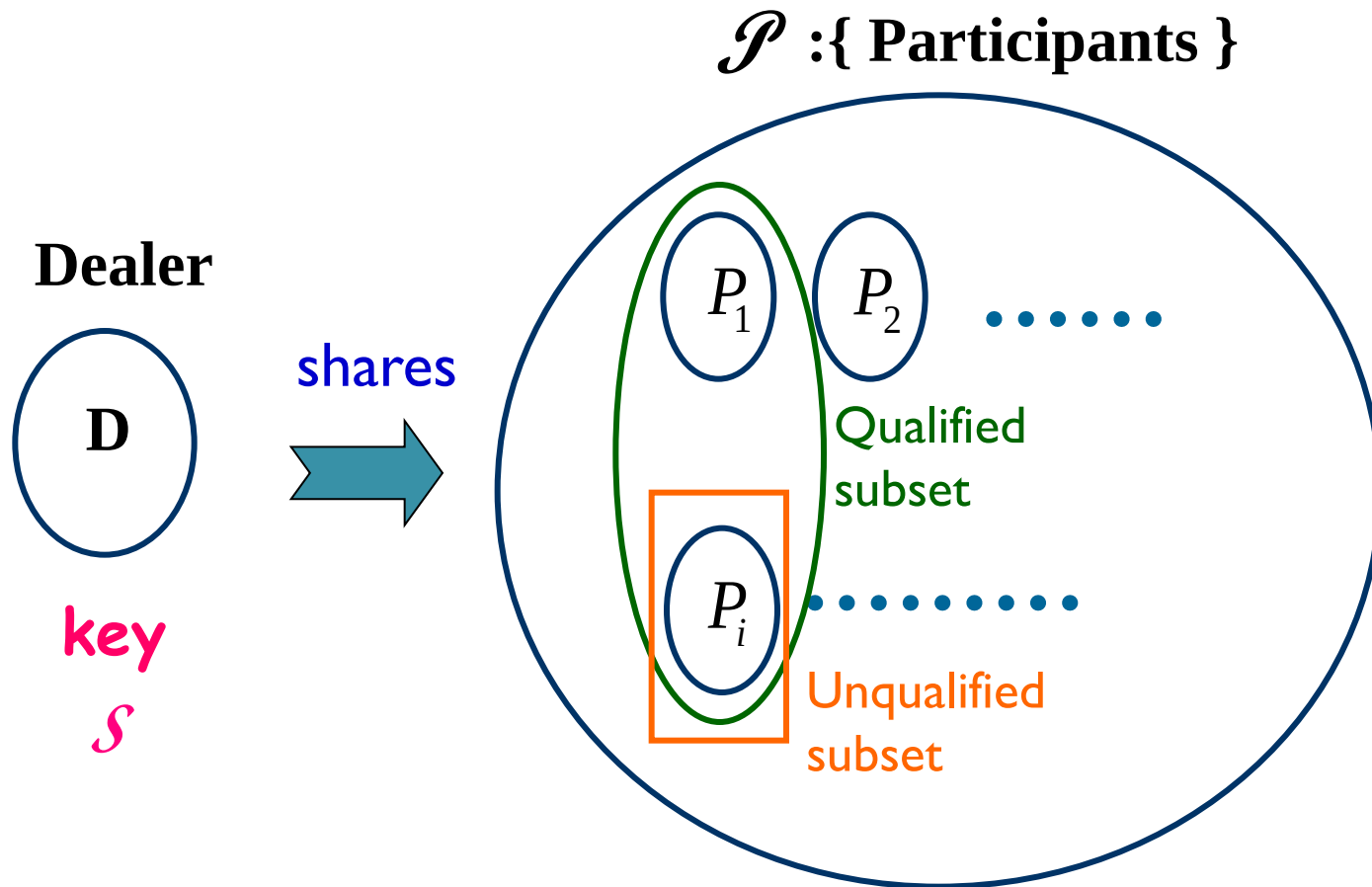
The optimal average information ratio of perfect secret-sharing schemes for access structure based on graphs

Hung-Lin Fu

Department of Applied Mathematics

National Chiao Tung University, Hsin Chu, Taiwan

Introduction



Access structure: $\Gamma = \{ A \subseteq \mathcal{P} \mid A \text{ is a qualified subset} \}$

Definition

$\mathcal{P} = \{P_1, P_2, \dots, P_n\}$; Σ : secret-sharing scheme

$\mathcal{S}$ = the set of all keys; $S_i = \{\text{all the shares of participant } P_i\}$

➤ Γ is a monotone access structure if

$\forall B \subseteq \mathcal{P}$, if $A \subseteq B$ for some $A \in \Gamma$, then $B \in \Gamma$.

➤ $\Gamma_0 = \{A \subseteq \mathcal{P} \mid A \text{ is a minimal qualified subset}\}$ is a basis of Γ

➤ The information ratio of Σ is $R_\Sigma = \frac{\max\{\log_2 |S_i| : 1 \leq i \leq n\}}{\log_2 |\mathcal{S}|} \geq 1$

➤ The average information ratio of Σ is

$$R_\Sigma \geq AR_\Sigma = \frac{\sum_{i=1}^n \log_2 |S_i|}{n \log_2 |\mathcal{S}|} \geq 1$$

$$R_\Sigma \geq AR_\Sigma \geq 1$$

$$R_\Sigma = 1 \Leftrightarrow AR_\Sigma = 1$$

Graph-based access structure

G : a finite simple graph without isolated vertices.

Let $\mathcal{P} = V(G)$ and $\Gamma_0 = E(G)$

- A secret-sharing scheme for the access structure based on G is a collection of random variables $\zeta_{\mathcal{S}}$ and ζ_v for $v \in V(G)$ with a joint distribution such that
- (i) $\zeta_{\mathcal{S}}$ is the secret and ζ_v is the share of v ;
 - (ii) if $uv \in E(G)$, then ζ_u and ζ_v together determine the value of $\zeta_{\mathcal{S}}$;
 - (iii) if $A \subseteq V(G)$ is an independent set in G , then $\zeta_{\mathcal{S}}$ and the collection $\{\zeta_v \mid v \in A\}$ are statistically independent.

Optimal average information ratio of G

Σ : secret-sharing scheme

H : the Shannon entropy

➤ The information ratio of Σ is $R_\Sigma = \max_{v \in V(G)} \{H(\zeta_v) / H(\zeta_s)\}$.

➤ The average information ratio of Σ is

$$AR_\Sigma = \frac{\sum_{v \in V(G)} H(\zeta_v)}{nH(\zeta_s)} .$$

➤ The optimal information ratio of G is

$$R(G) = \inf \{R_\Sigma \mid \Sigma \text{ is a secret-sharing scheme on } G\}$$

➤ The optimal average information ratio of G is

$$AR(G) = \inf \{AR_\Sigma \mid \Sigma \text{ is a secret-sharing scheme on } G\}$$

$$R(G) \geq AR(G) \geq 1 \qquad R(G) = 1 \Leftrightarrow AR(G) = 1$$

Shannon entropy

X : discrete random variable with values $x_1, x_2, x_3, \dots, x_n$, and a probability distribution $\{p(x_i)\}_{i=1}^n$.

➤ The Shannon entropy of X is defined as

$$H(X) = -\sum_{i=1}^n p(x_i) \log(p(x_i))$$

➤ Then $0 \leq H(X) \leq \log |X|$

➤ Assume uniform distributions in the secret-sharing scheme,

then $H(\zeta_s) = \log |\mathcal{S}|$

$$H(\zeta_v) = \log |S_v|$$

Known results

Theorem (Brickell and Devenport,1991)

G : connected of order n

G is a complete multipartite graph

$$\Leftrightarrow R(G) = AR(G) = 1$$

Theorem (Blundo et al.,1995)

G : connected of order n

G is not a complete multipartite graph

$$\Leftrightarrow R(G) \geq \frac{3}{2} \Leftrightarrow AR(G) \geq \frac{n+1}{n}$$

Graph covering

Theorem (Stinson, 1994)

G : a connected graph with $V(G) = \{1, 2, \dots, n\}$. Suppose $\Pi = \{G_1, G_2, \dots, G_h\}$ is a complete multipartite covering of G .

Let $R_i = |\{j : i \in V(G_j)\}|, 1 \leq i \leq n$.

Then there exists a secret - sharing scheme with information ratio R and average information ratio AR , where

$$R = \max \{R_i : 1 \leq i \leq n\} \quad \text{and} \quad AR = \frac{\sum_{i=1}^n R_i}{n} = \frac{\sum_{i=1}^h |V(G_i)|}{n}$$

vertex-number sum of Π

About information ratio

Theorem (Stinson, 1994)

(1) Suppose G is a connected graph of order n and d is the maximum degree of G . Then

$$R(G) \leq \frac{d+1}{2}.$$

$$(2) \quad R(P_n) = \frac{3}{2}, \text{ if } n \geq 3; \quad R(C_n) = \frac{3}{2}, \text{ if } n \geq 5.$$

The exact value of $R(G)$ is known for all graphs of order ≤ 6 but some exceptions.

Average information ratio

Theorem (Stinson, 1994)

$$AR(G) \leq \frac{2e + n}{2n} \text{ where } e = |E(G)|.$$

Theorem (Blundo et al., 1995)

$$(1) \ AR(C_n) = \frac{3}{2}, \text{ if } n \geq 5.$$

$$(2) \ AR(P_n) = \begin{cases} \frac{3n}{2(n+1)}, & n : \text{even} \\ \frac{3n+1}{2(n+1)}, & n : \text{odd} \end{cases}, \text{ if } n \geq 3.$$

The exact value of $AR(G)$ is known for all graphs of order ≤ 5 but some exceptions.

A break through on trees

Theorem (Csirmaz and Tardas, 2007)

Let T be a tree. Then $R(T) = 2 - \frac{1}{c(T)}$
where $c(T)$ is the maximum size of a core of T .

Theorem (Csirmaz and Ligeti, 2009)

Let d be the maximum degree of G , then $R(G) = 2 - 1/d$
provided that G satisfies the following conditions:

- (i) every vertex has at most one neighbor of degree one,
- (ii) vertices of degree at least three are not adjacent, and
- (iii) the girth of G is at least six.

Our previous contributions

Theorem (with Lu, 2013)

If T be a tree of order n , then $AR(T) = \frac{n + in(T) - d^*(T)}{n}$

$$in(T) = \# \{ v \in V(T) \mid \deg_T(v) \geq 2 \}$$

$d^*(T)$: the deduction of T .

Theorem (with Lu, 2013)

Let G be a graph in which every cycle has two degree-two vertices of distance at least four, then

$$AR(G) = \frac{n + in(G) - d^*(G)}{n}$$

- The main idea of our works is to create a min-max pair!



From covering

Theorem (Stinson, 1994)

G : a connected graph with $V(G) = \{1, 2, \dots, n\}$. Suppose $\Pi = \{G_1, G_2, \dots, G_h\}$ is a complete multipartite covering of G .

Let $R_i = |\{j : i \in V(G_j)\}|, 1 \leq i \leq n$.

Then there exists a perfect secret - sharing scheme with information ratio R and average information ratio AR , where

$$R = \max \{R_i : 1 \leq i \leq n\} \quad \text{and} \quad AR = \frac{\sum_{i=1}^n R_i}{n} = \frac{\sum_{i=1}^h |V(G_i)|}{n}.$$

vertex-number sum of Π

Stinson's upper bound on $AR(G)$

$\Pi = \{T_1, T_2, \dots, T_h\}$: a star covering of G with vertex-number sum m_Π .

➤ $d_\Pi = |V(G)| + in(G) - m_\Pi$: the deduction of Π .

➤ $d^*(G) = \max\{d_\Pi \mid \Pi \text{ is a star covering of } G\}$
= the deduction of G .

Theorem (Stinson, 1994)

If $\Pi = \{T_1, T_2, \dots, T_h\}$ is a star covering of G , then

$$AR(G) \leq \frac{|V(G)| + in(G) - d_\Pi}{|V(G)|}.$$

Core cluster

$$IN(G) = \{v \in V(G) \mid \deg_G(v) \geq 2\}, \quad in(G) = |IN(G)|$$

- A core of G is a connected subset $V_0 \subseteq IN(G)$ satisfying
 - (1) each $v \in V_0$ has a neighbor $\bar{v} \notin V_0$ such that $\bar{v}$ is not a neighbor of any other vertex in V_0 , and
 - (2) $\{\bar{v} \mid v \in V_0\}$ is an independent set in G .
- A core cluster of G is a partition $\mathcal{E} = \{V_1, V_2, \dots, V_k\}$ of $IN(G)$ such that each V_i is a core of G .
- The size k of $\mathcal{E}$ is denoted as $c_{\mathcal{E}}$.
- $c^*(G) = \min\{c_{\mathcal{E}} \mid \mathcal{E} \text{ is a core cluster of } G\}$
= the core number of G .

A Lower Bound on $AR(G)$

Theorem

If $\mathcal{E}$ is a core cluster of G , then

$$AR(G) \geq \frac{|V(G)| + in(G) - c_{\mathcal{E}}}{|V(G)|}.$$



Which one is larger?

- If $\mathcal{C}$ is a core cluster of a graph G and Π is star covering of G , then the size of $\mathcal{C}$ is at least the deduction of Π , i.e., $c^*(G) \geq d^*(G)$.
- If there exists a core cluster whose size is equal to the deduction of a star covering of G , then $c^*(G) = d^*(G)$.

Possible for trees and some bipartite graphs

So, we need to find a good pair of star covering and core cluster.

Corollary

If there exists a core cluster and a star covering of G such that $c_{\mathcal{T}} = d_{\Pi}$, then $c^*(G) = d^*(G) = c = d_{\Pi}$ and

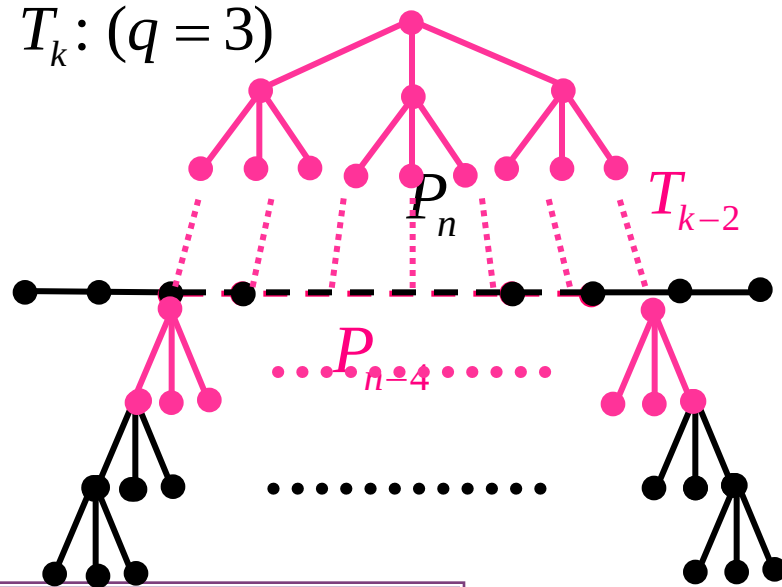
$$AR(G) = \frac{|V(G)| + in(G) - c^*(G)}{|V(G)|}$$

G is called realizable if $c^*(G) = d^*(G)$.

$AR(T)$ for complete q -ary trees

Theorem (Blundo et al., 1995)

$$AR(P_n) = \begin{cases} \frac{3n}{2(n+1)}, & n : \text{even} \\ \frac{3n+1}{2(n+1)}, & n : \text{odd} \end{cases}$$



Theorem

Let T_k be a complete q -ary tree with k levels, then

$$AR(T_k) = \begin{cases} \frac{q^{k+2} + 2q^{k+1} - q^2 - 2q}{(q+1)(q^{k+1} - 1)}, & k : \text{even}; \\ \frac{q^{k+2} + 2q^{k+1} - q^2 - 2q}{(q+1)(q^{k+1} - 1)}, & k : \text{odd}. \end{cases}$$

Open problem

- For which graphs G , $c^*(G) = d^*(G)$?



Secret-sharing on infinite graphs

G_∞ : an infinite graph without isolated vertices.

➤ The optimal information ratio of G_∞ is

$$R(G_\infty) = \sup\{R(G') \mid G' \text{ is an induced finite subgraph of } G_\infty\}$$

➤ The optimal average information ratio of G_∞ is

$$AR(G_\infty) = \sup\{AR(G') \mid G' \text{ is an induced finite subgraph of } G_\infty\}$$

$$R(G_\infty) \geq AR(G_\infty) \geq 1 \quad R(G_\infty) = 1 \Leftrightarrow AR(G_\infty) = 1$$

About information ratio

Theorem (Csirmaz, 2008)

$$(1) R(P_{\infty}) = \frac{3}{2}$$

$$(2) R(\text{Comb}_{\infty}) = 2$$

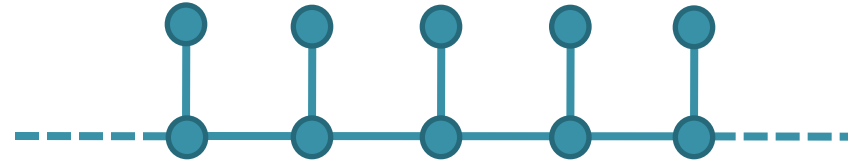
$$(3) R(\text{Honeycomb}_{\infty}) = 2$$

$$(4) R(2\text{-lattice}) = 2$$

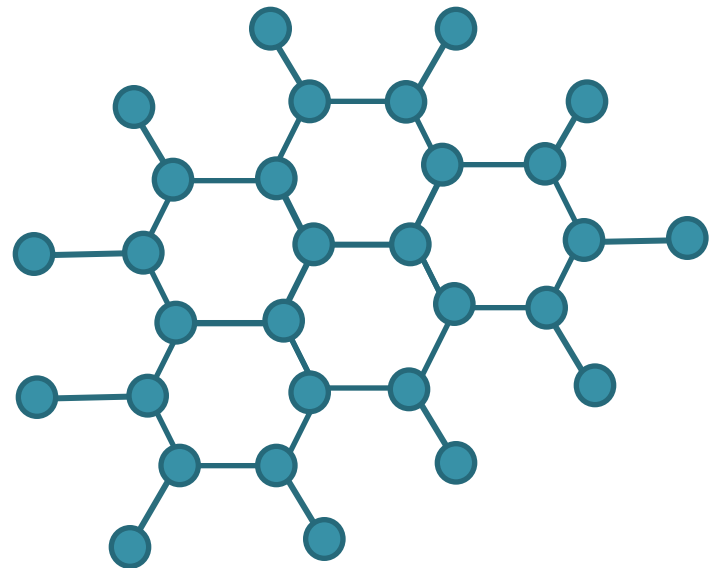
$$(5) 2 \leq R(\text{Triangle lattice}) \leq \frac{12}{5}$$

$$(6) \frac{10}{6} \leq R(\text{Infinite ladder}) \leq \frac{11}{6}$$

Comb_{∞} :

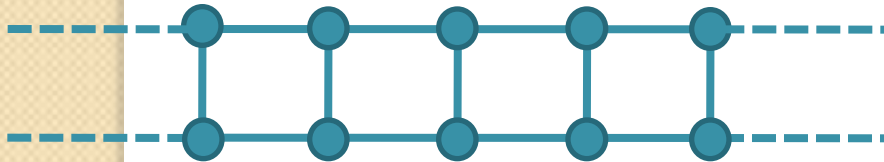


$\text{Honeycomb}_{\infty}$:

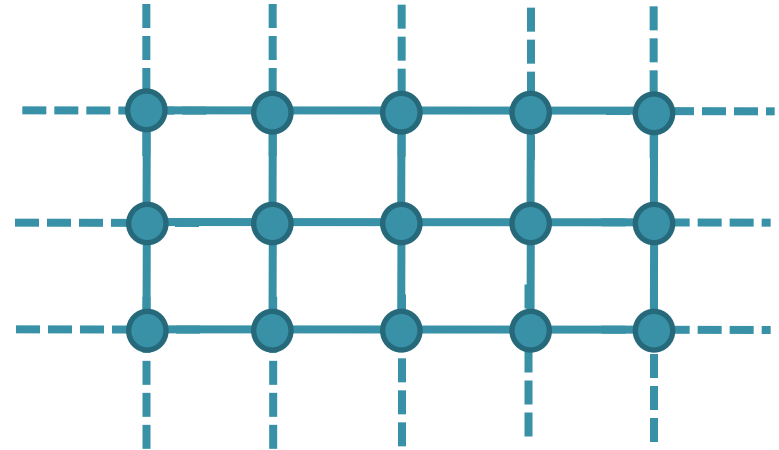


Continued

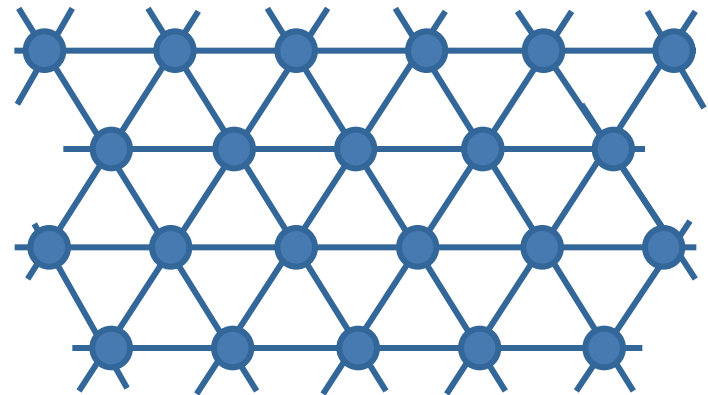
Infinite ladder :



2-lattice :



Triangle lattice :



Review

Theorem

If $\mathcal{E}$ is a core cluster of G , then

$$AR(G) \geq \frac{|V(G)| + in(G) - c_{\mathcal{E}}(G)}{|V(G)|}.$$

Theorem (Stinson, 1994)

If $\Pi = \{T_1, T_2, \dots, T_h\}$ is a star covering of G , then

$$AR(G) \leq \frac{|V(G)| + in(G) - d_{\Pi}(G)}{|V(G)|}.$$

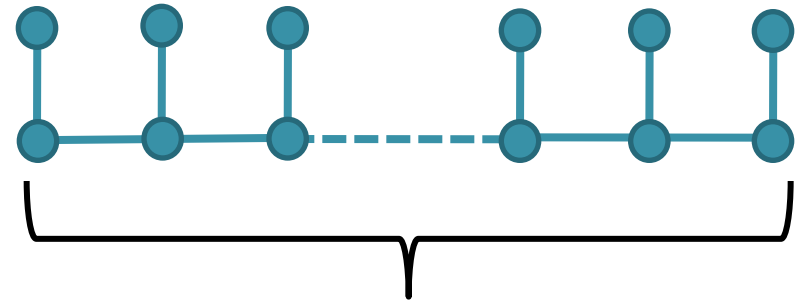
Direct counting

Theorem

$$(1) AR(P_{\infty}) = \frac{3}{2}$$

$$(2) AR(Comb_{\infty}) = \frac{3}{2}$$

$Comb_k :$

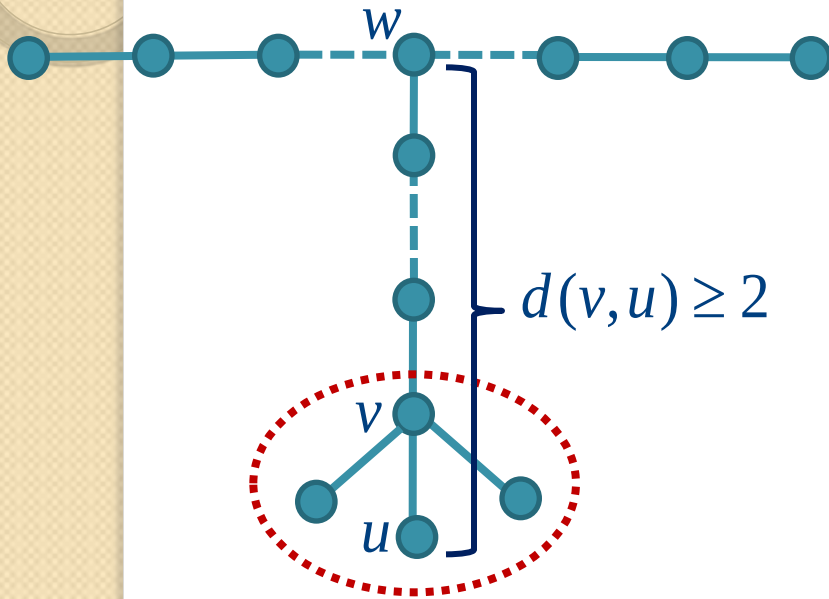


$AR(G') \leq AR(Comb_k)$, for any subgraph G' of $Comb_k$.

$$AR(Comb_k) = \frac{3k-1}{2k} \rightarrow \frac{3}{2}, \text{ as } k \rightarrow \infty$$

Arbitrary Tree

Given T (not a subgraph of a comb)



T^* : leaf star

Π : optimal star covering of T

C : optimal core cluster of T

$$d_{\Pi}(T) = c_C(T)$$

Π' : star covering of $T - T^*$

C' : core cluster of $T - T^*$

$$d_{\Pi'}(T - T^*) = c_{C'}(T - T^*) = d_{\Pi}(T) - 1$$

Key steps

$$AR(T - T^*) = \frac{|V(T - T^*)| + in(T - T^*) - d_{\Pi'}(T - T^*)}{|V(T - T^*)|}$$

$$= \frac{|V(T)| + in(T) - d_{\Pi}(T) - (\deg(v) + 1)}{|V(T)| - \deg(v)}$$

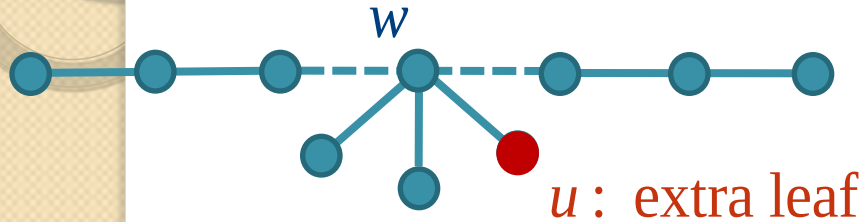
$$= \frac{AR(T)|V(T)| - (\deg(v) + 1)}{|V(T)| - \deg(v)}$$

$$= AR(T) + \frac{AR(T)\deg(v) - 1}{|V(T)| - \deg(v)}$$

$$> AR(T)$$

Key steps (continued)

Given T (not a subgraph of a comb)



Π : optimal star covering of T

C : optimal core cluster of T

$$d_{\Pi}(T) = c_C(T)$$

$$AR(T - u)$$

$$= \frac{|V(T - u)| + \text{in}(T - u) - d_{\Pi'}(T - u)}{|V(T - u)|}$$

$$= \frac{|V(T)| + \text{in}(T) - d_{\Pi}(T) - 1}{|V(T)| - 1}$$

$$> AR(T)$$

Π' : star covering of $T - u$

C' : core cluster of $T - u$

$$d_{\Pi'}(T - u) = c_{C'}(T - u) = d_{\Pi}(T)$$

Conclusion (infinite trees)

If T is not a subgraph of a comb, then

$AR(T - u) > AR(T)$, for any extra leaf u .

$AR(T - T^*) > AR(T)$, for any leaf star T^* .

$$AR(T_\infty) = \sup\{AR(T) \mid T \text{ is a tree}\}$$

$$= AR(Comb_\infty)$$

$$= \frac{3}{2}$$

Thank you for your attention

