

Graph Covering and Its Applications

Hung-Lin Fu (傅 恒 霖)

Department of Applied Mathematics

National Chiao Tung University

Hsin Chu, Taiwan 30010

We need your support!



Graph Covering

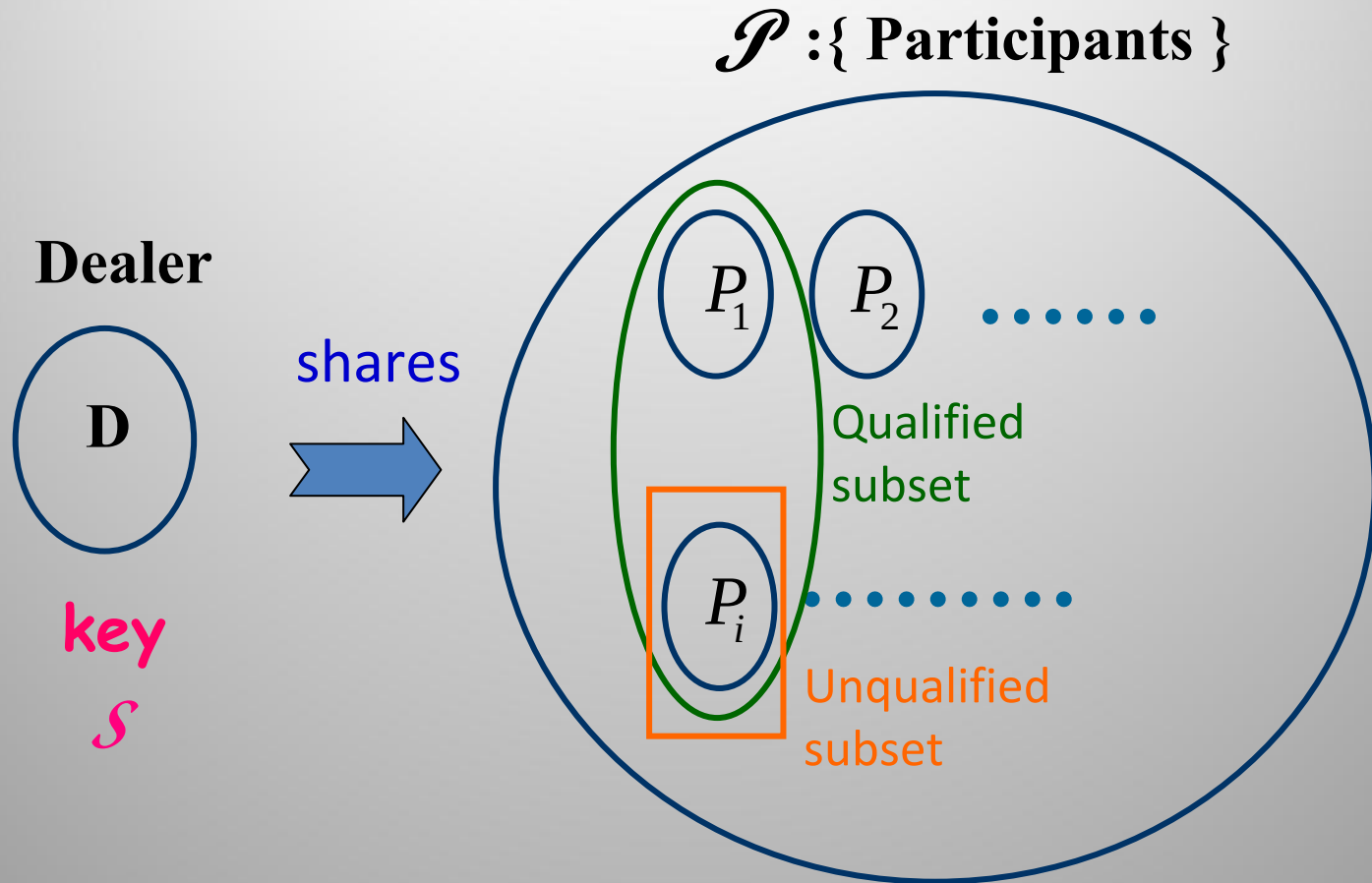
- Let G be a graph. A *graph covering* of G denoted by $\mathbf{C}_G = \{G_1, G_2, \dots, G_t\}$ is a collection of subgraphs of G such that each edge of G is belonged to *at least one* subgraph in $\mathbf{C}_G$.
- *At most one* $\Rightarrow$ *graph packing*
- *Exactly one* $\Rightarrow$ *graph decomposition*
- *Both of graph packing and graph decomposition are very applicable!*

Every pair counts

- In case that we need cover all the pairs considered in the problem, then covering is needed.
- This phenomenon occurs in many applications and I will show you two of them.
- The work obtained on these two topics is a joint work with Dr. Hui-Chuan Lu (吕惠娟) and several other researchers.

Cover with isomorphic subgraphs

- The most common idea in the application of graph decomposition, graph packing or graph covering of a graph G is to use a fixed subgraph of G , say a 3-cycle.
- That is to say, all the subgraphs in covering we use are isomorphic.
- We may use a different constraint!



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

Definition

- 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
- Γ is called r -homogeneous if all subsets in its basis are of size r .

Definition

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

$S_i = \{\text{all the shares of participant } P_i\}$

➤ 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

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

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

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

➤ A secret-sharing scheme Σ with $R_\Sigma = 1$ is called ideal.

Definition: graph-based access structure

$\mathcal{P} = V(G)$ and $\Gamma_0 = E(G)$ where G has no isolated vertices.

- $R(G)$ = the optimal information ratio of G
= the infimum of the information ratio of all perfect secret-sharing schemes realizing G
- $AR(G)$ = the optimal average information ratio of G
= the infimum of the information ratio of all perfect secret-sharing schemes realizing G

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

- G is called ideal if there exists an ideal secret-sharing scheme on it.

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

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

Known results

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

Upper bound

- It is not too surprising to conclude that the best covering (**minimum vertex-number sum**) of G by complete multipartite graphs provides an upper bound of $AR(G)$.
- Note that if the graph we consider does not contain a 4-cycle, then the graph can only be covered with stars.

Known results

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.

The exact value of $AR(G)$

- First, we find a good upper bound A .
- Then, we derive a lower bound B .
- Hence, we have $A \geq AR(G) \geq B$.
- Now, $A = B \implies AR(G) = A = B$.
- This is a typical type of max-min problem in combinatorial optimization.

How about trees?

- Theorem (Lu and Fu, Des. Code Cryptogr. 2013)

If T is a tree of order n , then

$$AR(T) = (n + \text{in}(T) - d^*)/n$$

where $\text{in}(T)$ is the number of vertices in T with degree at least 2 and d^* is the minimum deduction in a complete multipartite covering, that is $n + \text{in}(T) - d^*$ equals to the minimum vertex-number sum. (Covering gives an upper bound in general.)

(*) Idea: use the so-called *core cluster* to play the role of lower bound.

Core and Core cluster

- A *core* of a connected graph G is a vertex subset of $V(G)$, S , such that (1) S induced a connected subgraph of G , (2) each vertex v of S has a distinct out neighbor v' and (3) the set of all out neighbors forms an independent set of G .
- A *core cluster* of G is a partition of $IN(G)$ such that each subset is a core where $IN(G)$ is the set of vertices in G which are of degree larger than 1.
- We need an example!

Example on trees

- **Theorem** (Csirmaz and Tardos, Tatracrypt 2007)
The exact value of the optimal ratio of all trees $R(G) = 2 - (1/c(T))$, where $c(T)$ is the maximum size of a core in the tree T .
- **Theorem** (Lu and Fu, Des. Code Cryptogr. 2013)
If C is a core cluster of a graph G , then
 $AR(G) \geq (n + in(T) - c^*(G))/n$ where $c^*(G)$ denotes the minimum size of all core clusters of G .

Bipartite graphs

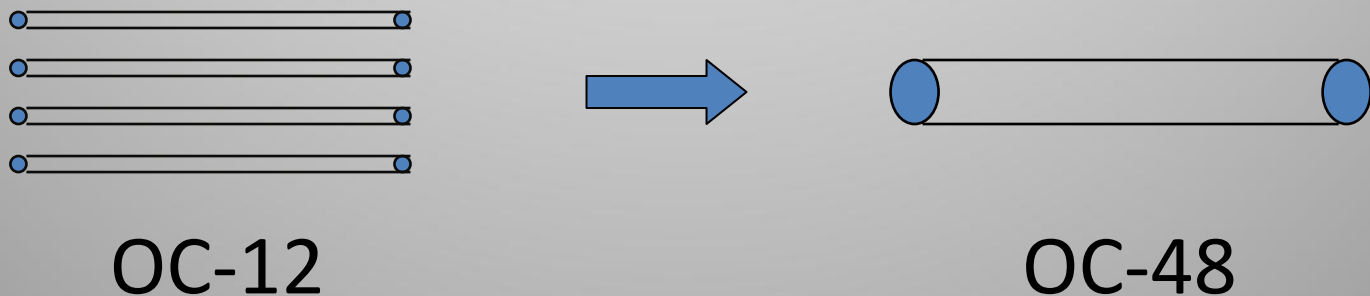
- We can find the exact value $AR(G)$ for some classes of bipartite graphs G , mainly G is of girth 8 or more, and certain constraints are also required. (Star covering is easier to control.)
- Still rooms for improvement.
- If you are interesting in knowing more details, please consult Dr. Lu in National United University.

Another application

A **synchronous optical network (SONET)** ring is an optical interconnection device constructed by using fibers to connect SONET **add drop multiplexers (ADM)s**.

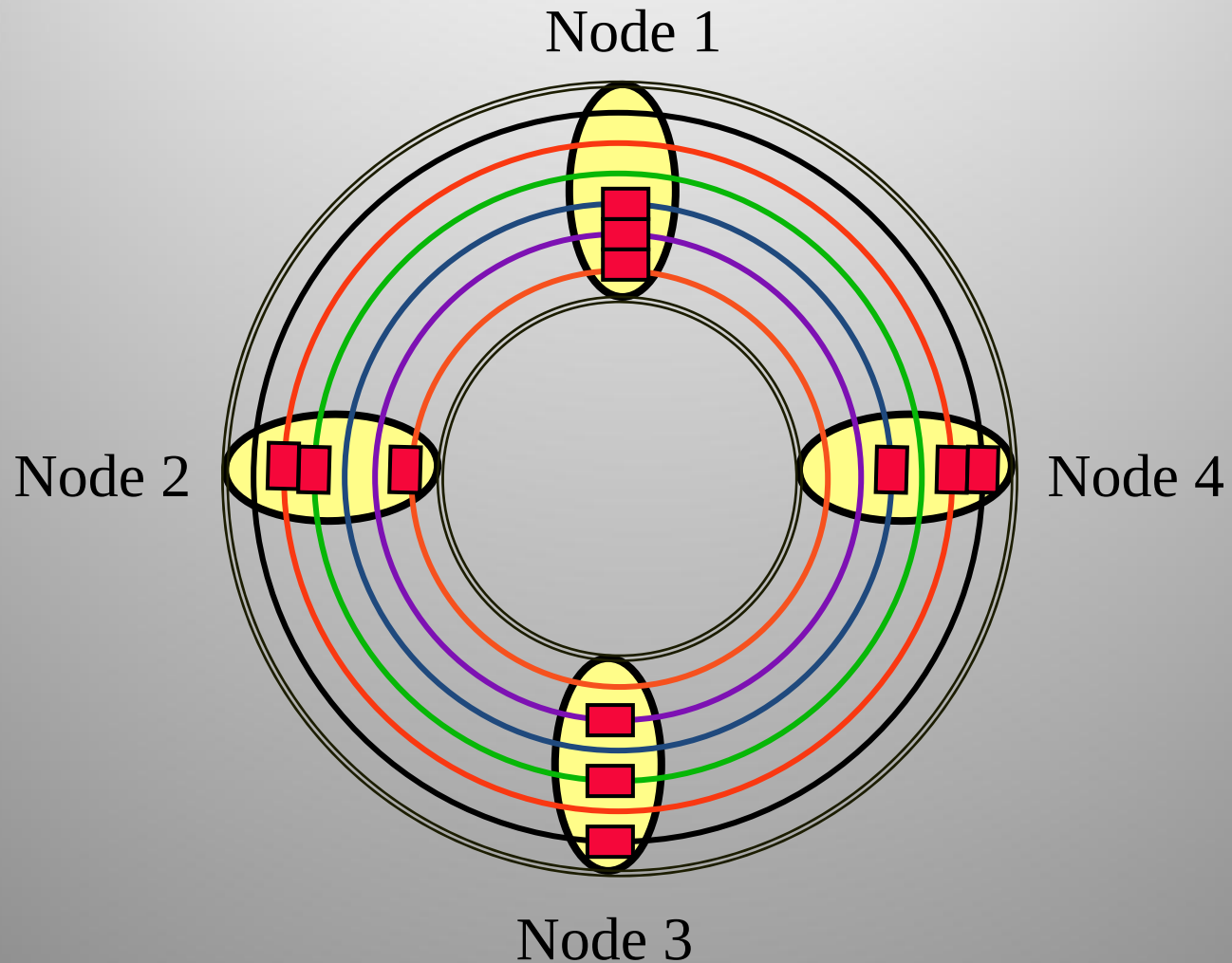
An **ADM** can multiplex multiple lower rate streams to form higher rate ones.

Traffic grooming is the generic term for multiplexing low rate streams to form higher rate streams.

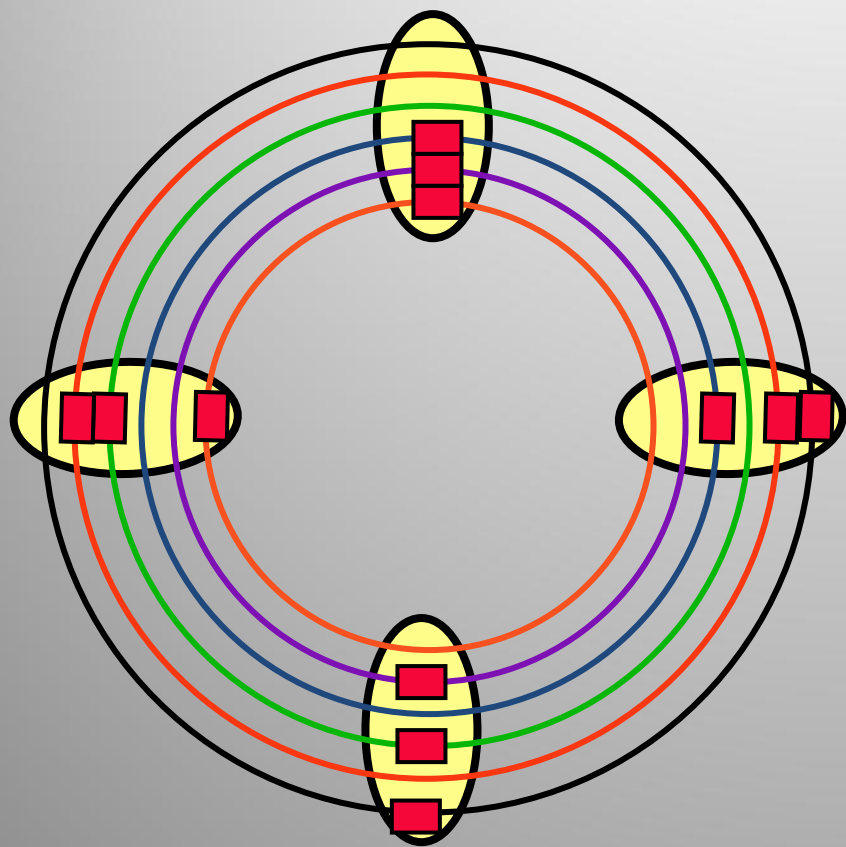


Grooming ratio $C = 4$

Unidirectional WDM ring with
static uniform symmetric all-to-all traffic

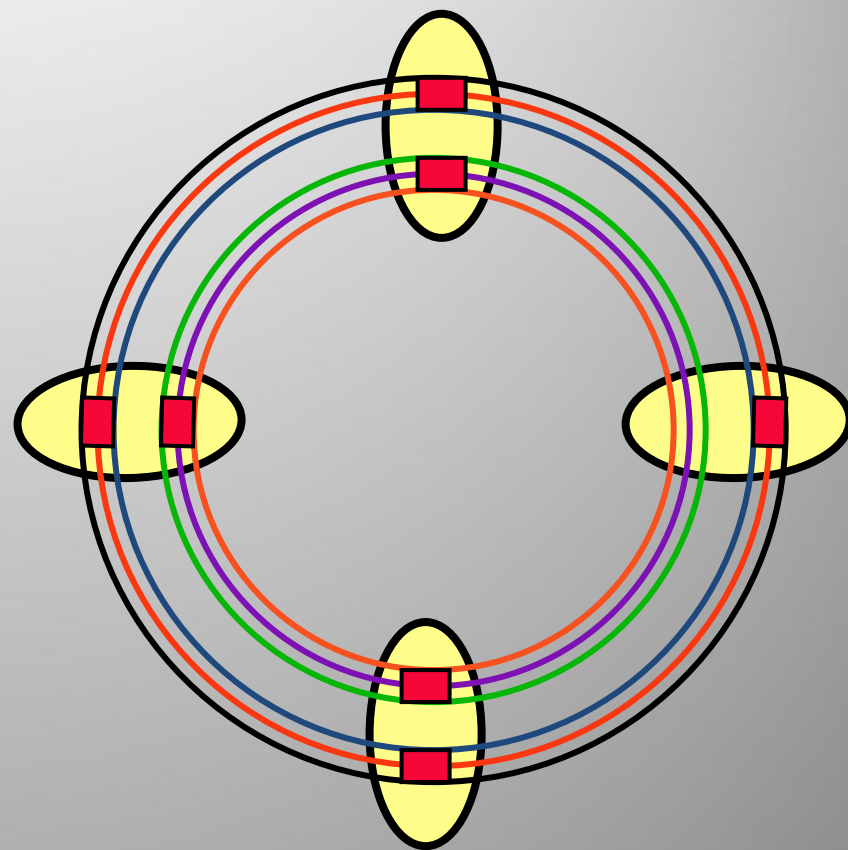


No grooming



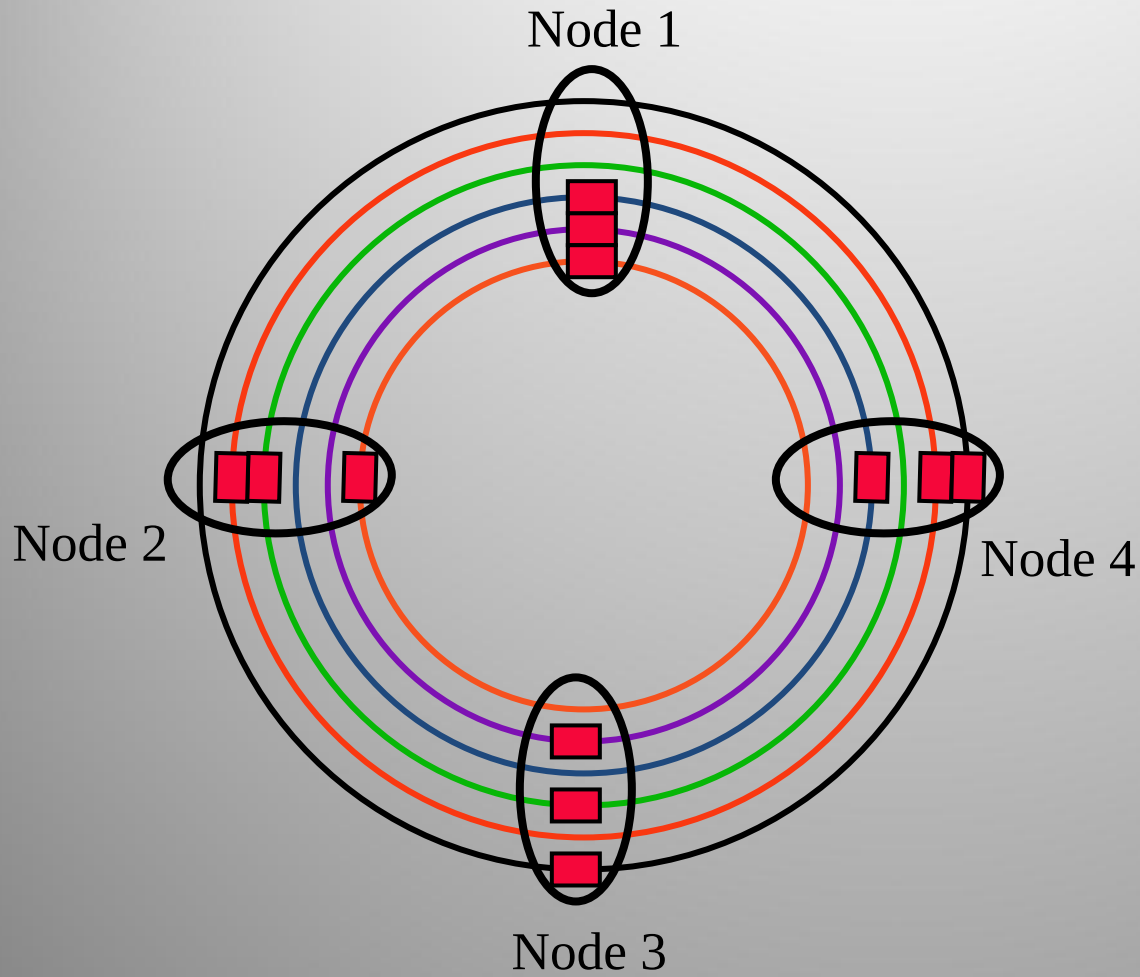
$$A = 12$$

Grooming with ratio $C = 3(?)$

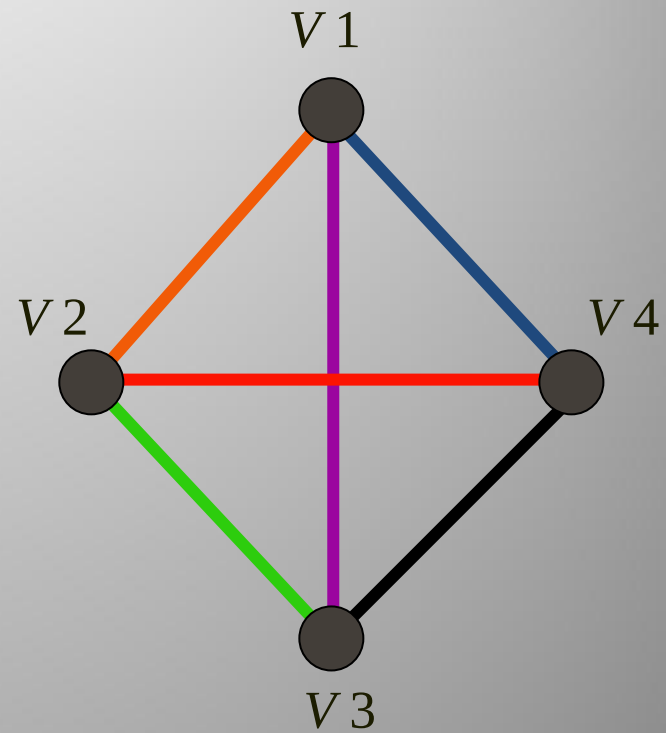


$$A = 7$$

No grooming

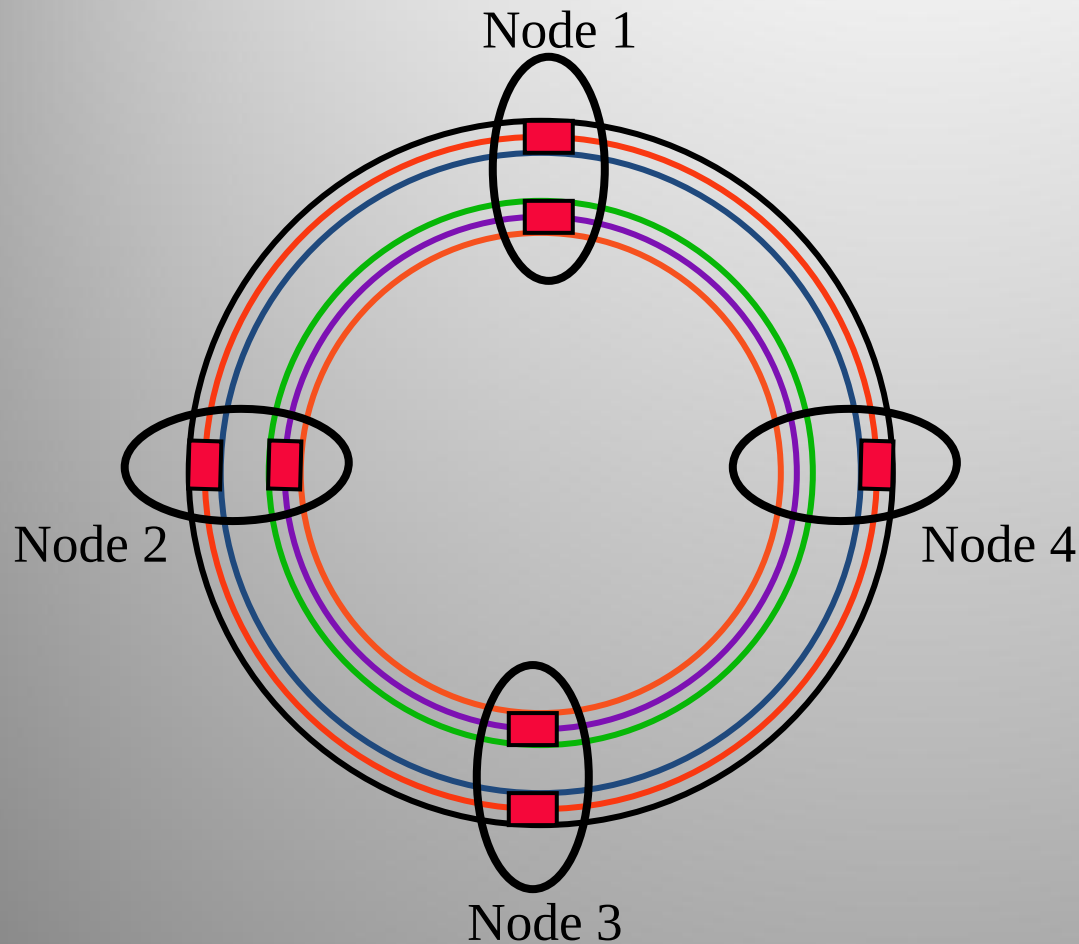


$$A = 12$$

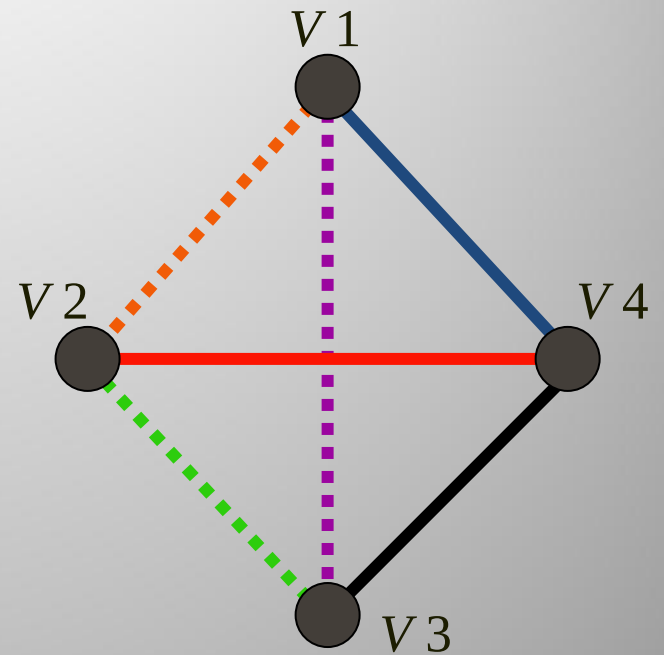


$$A = 12$$

Grooming with ratio $C = 3$



$$A = 7$$



$$B_1 = K_3; \quad B_2 = K_{1,3}$$

$$A = \sum_i |V(B_i)|$$

To minimize the number of ADMs for a unidirectional WDM

Partition the edges of the complete graph K_N into connected subgraphs B_i , $i = 1, 2, \dots, W$, with $|E(B_i)| \leq C$ where $\sum_{i=1}^W |V(B_i)|$ is minimized.

$E(B_i)$: the circles groomed on the wavelength i

$V(B_i)$: the nodes at which the wavelength i is used

$|V(B_i)|$ = the number of ADMs required for wavelength i .

W = the number of wavelength used

$\sum_{i=1}^W |V(B_i)|$ = the total number of ADMs needed.

Preliminary

$$\rho(G) = |E(G)|/|V(G)|$$

$$\rho(m) = \max\{\rho(G) \mid |E(G)| = m\}$$

$$\rho_{\max}(C) = \max_{m \leq C} \rho(m) = \max\{\rho(G) \mid |E(G)| \leq C\}$$

Theorem 2.1 [Bermond & Coudert]

Any grooming of R circles with a grooming ratio C needs at least $R/\rho_{\max}(C)$ ADMs.

In particular, $A(C, N) \geq N(N-1)/(2\rho_{\max}(C))$

Working on $C = 7$

- Minimizing SONET ADMs in unidirectional WDM rings with grooming rate 7 (with C. Colbourn, G. Ge, A. Ling and Hui-Chuan Lu), SIAM J. Discrete Math., 2008).
- We try to cover all the edges of a complete graph by using those small graphs with **at most** 7 edges. (Minimize the vertex-number sum as mentioned in the first application.)

Which graphs are better for use?

C	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\rho_{\max}(C)$	$\frac{1}{2}$	$\frac{2}{3}$	1	1	$\frac{5}{4}$	$\frac{3}{2}$	$\frac{3}{2}$	$\frac{8}{5}$	$\frac{9}{5}$	2	2	2	$\frac{13}{6}$	$\frac{14}{6}$

Table I

$$\rho(6) = \frac{3}{2} > \rho(7) = \frac{7}{5} \implies \rho_{\max}(7) = \frac{3}{2}$$

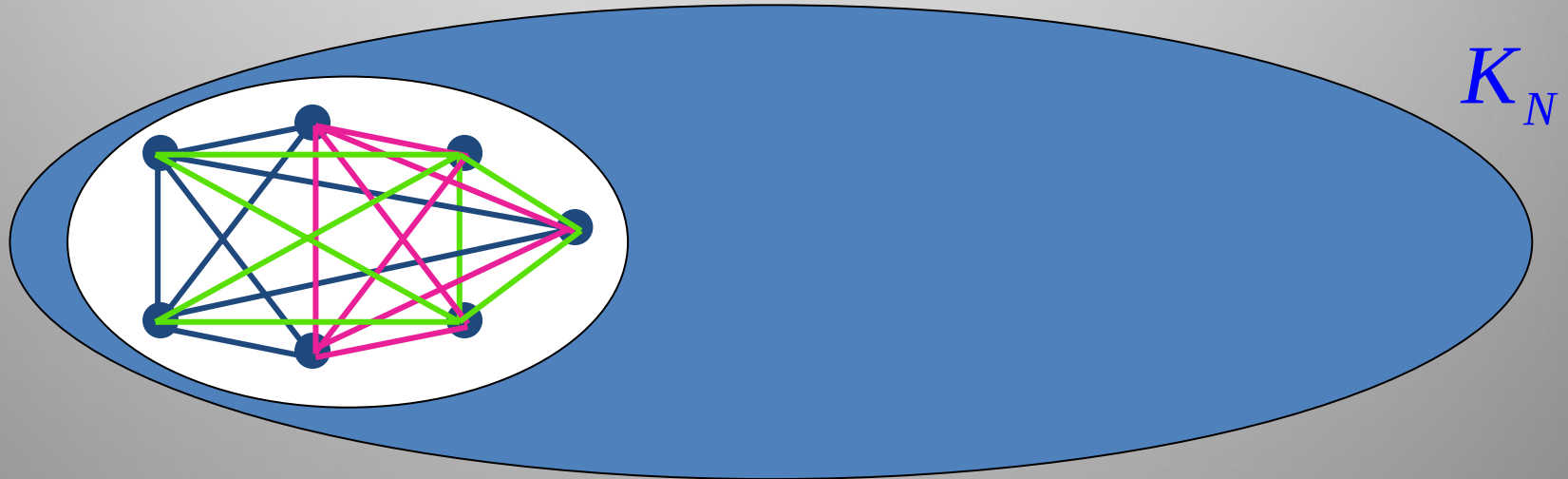
K_4 is the best option!

From combinatorial designs

- If n is congruent to 1 or 4 modulo 12, then an $(n, 4, 1)$ -design gives the answer. This is equivalent to decompose the complete graph of order n into K_4 's.
- For the other orders, it follows by many hard works especially from Dr. Lu.
- Still some orders (not many) left unknown!

Theorem [Brouwer]

A $B(N; \{4, 7^*\}, 1)$, that is, a pairwise balanced design on N points with blocks of size 4 and exactly one block of size 7 exists iff $N \equiv 7$ or $10 \pmod{12}$ and $N \neq 10, 19$.



K_N can be decomposed into K_4 's & $3 G_{7,5}$'s $\Rightarrow A = 2R/3 + 1$

Take a look at K_5

We can cover the graph with two subgraphs and their vertex-number sum is 8 which is the best.

Concluding remarks

- The more you know about mathematics, the more you have chances to apply them.
- Combinatorial mathematics is a beautiful branch of mathematics, we need to keep up our effort in order to make this study a more solid one in Taiwan.
- I am proud of being a combinatorialist and I thank all my former teachers and students who play the most important roles in my career of research!