

INVESTING COMBINATORICS

Hung-Lin Fu (傅 恒 霖)

Department of Applied Mathematics

National Chiao Tung University

Hsin Chu, Taiwan

WHAT IS COMBINATORICS?

- Combinatorics is a branch of mathematics concerning the study of finite or countable structures.
- Well-known fields: Graph theory, Design Theory, Enumerative Combinatorics, Algebraic Combinatorics, Algorithms and Combinatorial Optimization.
- Others: Coding Theory, Cryptography, Networks and Group Testing.



HANDBOOK OF COMBINATORICS



Volume I

Preface

List of Contributors

Part I: Structures

Graphs

1. Basic Graph Theory: Paths and Circuits
J.A. Bondy 3
2. Connectivity and Network Flows
A. Frank 111
3. Matchings and Extensions
W.R. Pulleyblank 179
4. Colouring, Stable Sets and Perfect Graphs
B. Toft 233
- Appendix to Chapter 4: Nowhere-Zero Flows
P.D. Seymour 289
5. Embeddings and Minors
C. Thomassen 301
6. Random Graphs
M. Karoński 351

Finite Sets and Relations

7. Hypergraphs
P. Duchet 381
8. Partially Ordered Sets
W.T. Trotter 433

Matroids

9. Matroids: Fundamental Concepts
D.J.A. Welsh 481
10. Matroid Minors
P.D. Seymour 527
11. Matroid Optimization and Algorithms
R.E. Bixby and W.H. Cunningham 551

Symmetric Structures	611
12. Permutation Groups	
<i>P.J. Cameron</i>	647
13. Finite Geometries	
<i>P.J. Cameron</i>	693
14. Block Designs	
<i>A.E. Brouwer</i>	747
15. <u>Association Schemes</u>	
<i>A.E. Brouwer and W.H. Haemers</i>	773
16. <u>Codes</u>	
<i>J.H. van Lint</i>	

Combinatorial Structures in Geometry and Number Theory

17. <u>Extremal Problems in Combinatorial Geometry</u>	809
<i>P. Erdős and G. Purdy</i>	
18. Convex Polytopes and Related Complexes	875
<i>V. Klee and P. Kleinschmidt</i>	
19. Point Lattices	919
<i>J.C. Lagarias</i>	
20. Combinatorial Number Theory	967
<i>C. Pomerance and A. Sárközy</i>	

Author Index	XIII
--------------	------

Subject Index	LIX
---------------	-----

Volume II

<i>Preface</i>	v
----------------	---

<i>List of Contributors</i>	xi
-----------------------------	----

Part II: Aspects	1019
------------------	------

21. <u>Algebraic Enumeration</u>	
<i>I.M. Gessel and R.P. Stanley</i>	1021
22. Asymptotic Enumeration Methods	
<i>A.M. Odlyzko</i>	1063
23. <u>Extremal Graph Theory</u>	
<i>B. Bollobás</i>	1231
24. <u>Extremal Set Systems</u>	
<i>P. Frankl</i>	1293
25. <u>Ramsey Theory</u>	
<i>J. Nešetřil</i>	1331

26. Discrepancy Theory <i>J. Beck and V.T. Sós</i>	1405
27. Automorphism Groups, Isomorphism, Reconstruction <i>L. Babai</i>	1447
28. <u>Combinatorial Optimization</u> <i>M. Grötschel and L. Lovász</i>	1541
29. <u>Computational Complexity</u> <i>D.B. Shmoys and É. Tardos</i>	1599

Part III: Methods 1647

30. Polyhedral Combinatorics <i>A. Schrijver</i>	1649
31. Tools from Linear Algebra <i>C.D. Godsil</i>	1705
Appendix <i>L. Lovász</i>	1740
32. <u>Tools from Higher Algebra</u> <i>N. Alon</i>	1749
33. <u>Probabilistic Methods</u> <i>J. Spencer</i>	1785
34. <u>Topological Methods</u> <i>A. Björner</i>	1819

Part IV: Applications 1873

35. <u>Combinatorics in Operations Research</u> <i>A.W.J. Kolen and J.K. Lenstra</i>	1875
36. <u>Combinatorics in Electrical Engineering and Statics</u> <i>A. Recski</i>	1911
37. Combinatorics in Statistical Physics <i>C.D. Godsil, M. Grötschel and D.J.A. Welsh</i>	1925
38. <u>Combinatorics in Chemistry</u> <i>D.H. Rouvray</i>	1955
39. <u>Applications of Combinatorics to Molecular Biology</u> <i>M.S. Waterman</i>	1983
40. <u>Combinatorics in Computer Science</u> <i>L. Lovász, D.B. Shmoys and É. Tardos</i>	2003
41. <u>Combinatorics in Pure Mathematics</u> <i>L. Lovász, L. Pyber, D.J.A. Welsh and G.M. Ziegler</i>	2039

Part V: Horizons 2083

42. Infinite Combinatorics	2085
----------------------------	------

43. Combinatorial Games*R.K. Guy*

44. The History of Combinatorics

N.L. Biggs, E.K. Lloyd and R.J. Wilson

Author Index

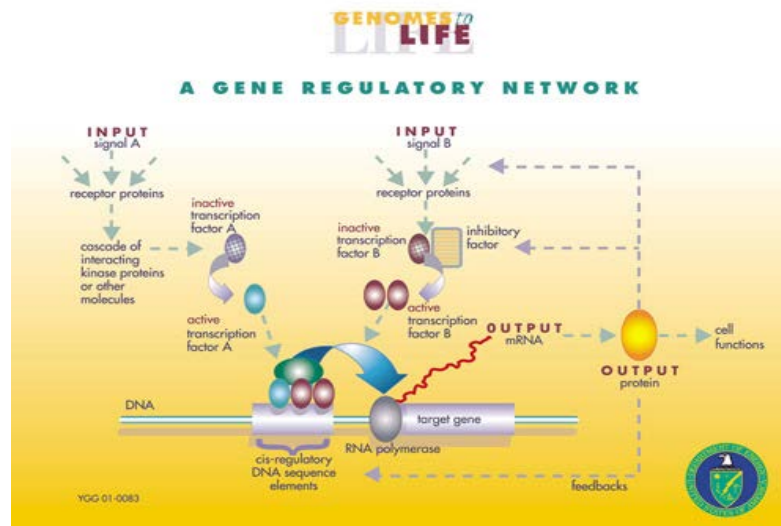
Subject Index

You may find something
interesting there.



GRAPHS

- They are everywhere.
- With colorings, graphs are beautiful.
- Digraphs are applicable to many aspects of our life. (Complex networks)



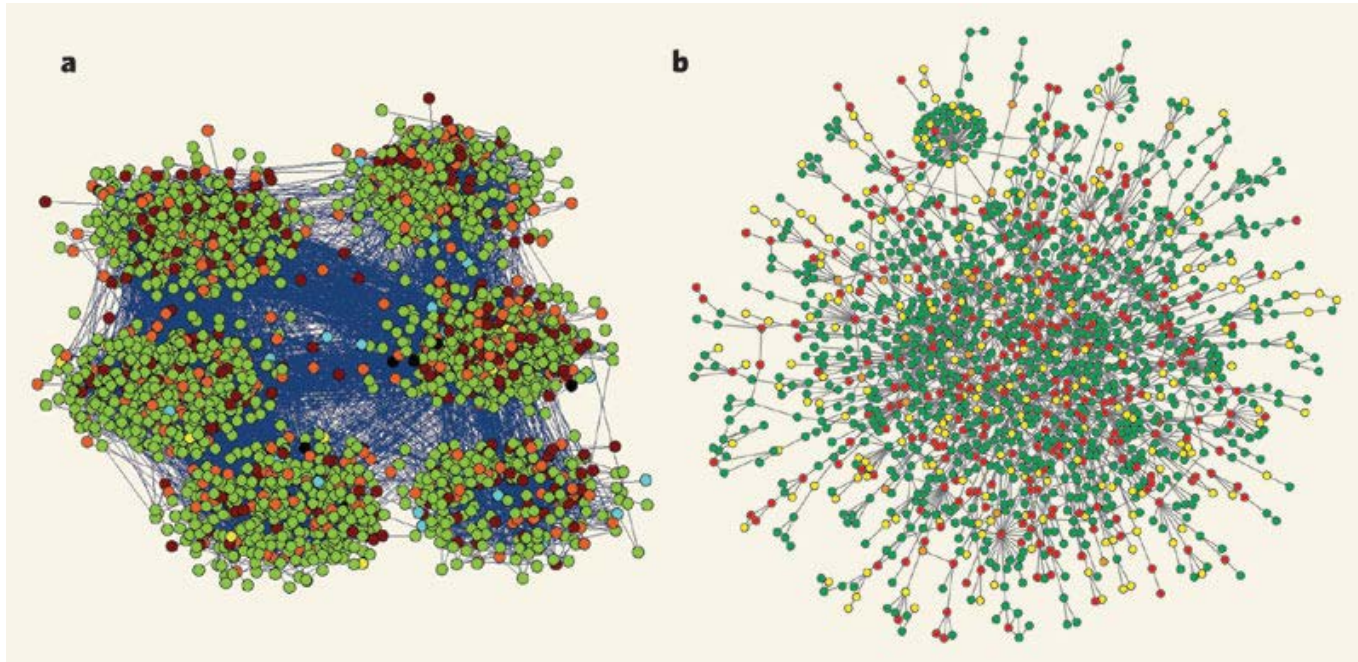
MOST INTERESTS

- Graph coloring (Various versions)
- Graph labelling
- Graph decomposition
- Domination problem (Various types)
- Hamiltonian problem
- Independent sets
- De-cycling numbers
- Networks
- Extremal graphs



HOW MANY?

- There are a lot of them, but how to count.
- Are they really different?
- Explicit answers are needed.



ENUMERATIVE COMBINATORICS

- Many young researchers are involved in this research recently.
- There are topics in Combinatorics which we have done an excellent job (in the world). This subject is one of them!
- For those who are interested in Data Analysis, they should not forget to learn more combinatorics, it is going to play an important role.



THE SOONER THE BETTER

- How fast can we obtain the answer?
- Does many mean more than one?
- We can not live without an algorithm!
- Simply, we are asking ourselves: what's next?

What is algorithm?

- A method that can be used by a computer for the solution of a problem.
- A sequence of computational steps that transform the input into the output.
- Examples of algorithms in the nature: DNA and cook book.
- The word "algorithm" comes from the name of [Abu Ja'far Mohammed ibn Musa al Khowarizmi](#) (780–825 A.D.), an Arab mathematician who wrote a textbook on mathematics.



IT DOES EXIST!

- Who knows what it looks like.
- But, it exists.
- This is not only for talking about random graphs or random walks.
- Random is great!



PROBABILISTIC METHOD

- A non-constructive method, primarily used in **combinatorics** and pioneered by **Paul Erdős**, for proving the existence of a prescribed kind of mathematical object.
- It works by showing that if one randomly chooses objects from a special class, **the probability that the result is of the prescribed kind is more than zero.**
- Although the proof uses probability, the final conclusion is determined for ***certain***, without any possible error.



AS EVENLY AS POSSIBLE

- This takes care of constructing a good experimental **design**. (**Combinatorial Design**)
- Also, it provides a chance to construct an optimal **code**.
- In **cryptography**, it plays an important role!
- “**Balanced**” life is what we are looking for.
- Balanced designs are candidates of optimal designs.

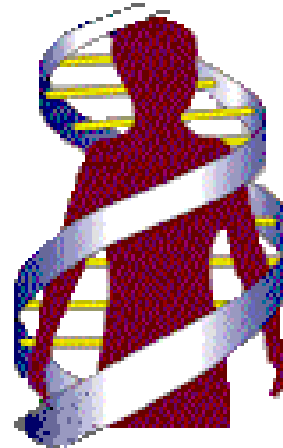


GREAT DESIGN!



POSITIVE OR NEGATIVE

- A simple idea: Just ask!
- How to ask?
- What can we get from the answers?
- Group testing is a wonderful tool in modern era.
- In the research of this field, several leading experts are in Taiwan!



HAVE YOU SEEN SOMETHING DIFFERENT?



FINGERPRINTS IN MULTI-MEDIA

- We may water-mark several pixels of a picture by using colors which are very closed to nearby pixels; colors are represented by binary vectors.
- Each buyer has his or her own fingerprints in order to make sure they have the right to see the picture.
- Any one who did not pay and used the picture will be recognized right away.
- The idea comes from the construction of **identifiable parent property codes (IPP)**.



Definitions

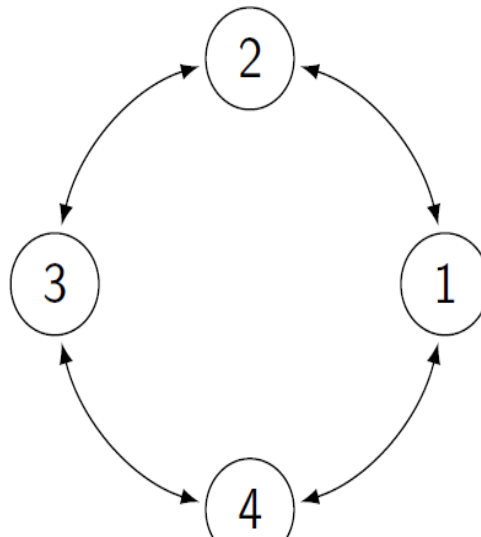
Definition

A path system of G with respect to N is a set of directed paths

$$\mathcal{P} := \{P_{(a,b)} : a, b \in N, a \neq b\},$$

one for each distinct ordered node pair.

- $\mathfrak{B}_{G,N}$: the set of all path systems of (G, N) .



GLOBAL PACKING NUMBER

- Given $\mathcal{P} \in \mathfrak{B}_{G,N}$.
- A **k -global packing** of $(G, N, \mathcal{P})$ is a mapping $\phi : \mathcal{P} \rightarrow \{1, 2, \dots, k\}$, such that $\phi(P) \neq \phi(P')$ if $P, P' \in \mathcal{P}$ and P, P' have one or more arrows in common.
- $\Phi(G, N, \mathcal{P})$: the smallest k that allows a k -global packing of $(G, N, \mathcal{P})$.

Definition

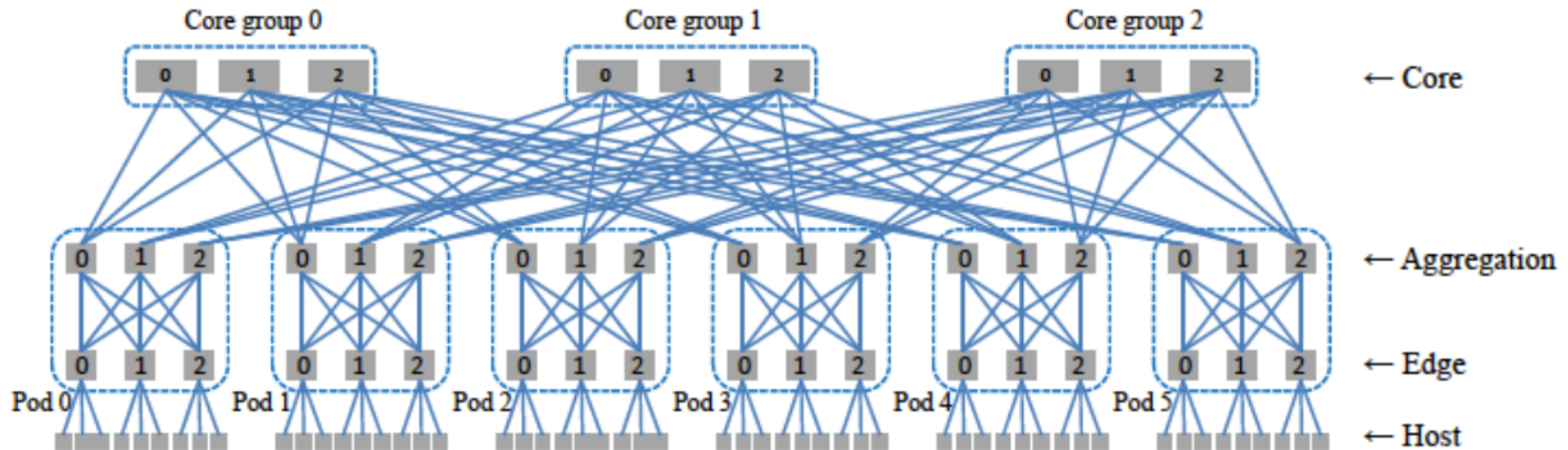
The global packing number of (G, N) is

$$\Phi(G, N) := \min_{\mathcal{P} \in \mathfrak{B}_{G,N}} \Phi(G, N, \mathcal{P}).$$

- $\mathcal{P}$ is said to be **ideal** if $\Phi(G, N) = \Phi(G, N, \mathcal{P})$.



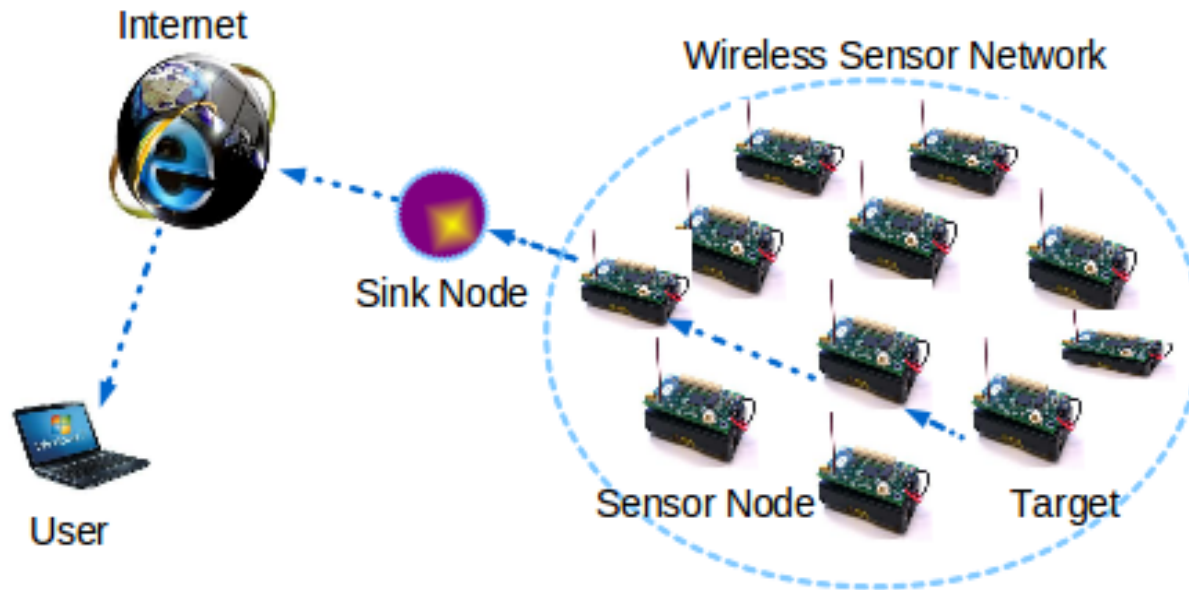
Fat-tree network



- $\mathbf{T}_n$: n -ary fat-tree network. Each switch has $2n$ ports and the number of pods is $2n$.
- $c_{i,j}$: the j -th core switch in the i -th core group. $|C_n| = n^2$
- $a_{i,j}$: the j -th aggregation switch in the i -th pod. $|A_n| = 2n^2$.
- $e_{i,j}$: the j -th edge switch in the i -th pod. $|E_n| = 2n^2$.
- $h_{t,i,j}$: the j -th host under the edge switch $e_{t,i}$. $|H_n| = 2n^3$.

The global packing number of this network has been obtained recently.

WIRELESS SENSOR NETWORK



INTERFERENCE FREE GT AND REACTIVE JAMMING ATTACKS

- Reactive Jamming attack has a great security threat to **wireless sensor networks (WSN)**.
- There exist many studies against these attacks, however, these methods such as **frequency hopping or channel surfing**, require excessive computational capabilities on wireless devices.
- With the help of using **group testing**, the jammers can be located efficiently.

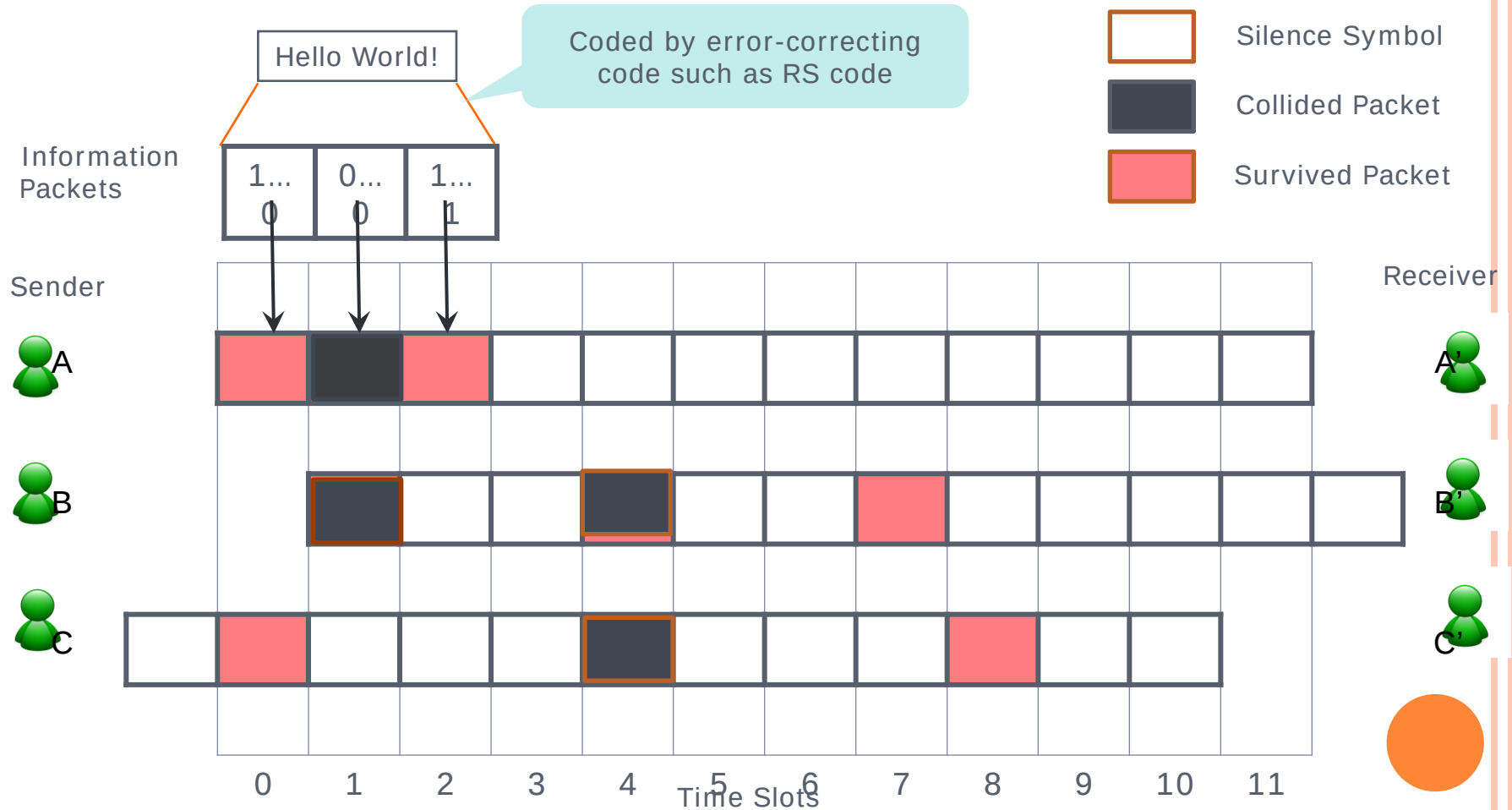


KEY IDEA

- We can apply an interference free group testing to identify the *trigger nodes*, whose transmissions activate any *reactive jammers*.
- The identification of these trigger nodes can help us to (1) design a better routing protocol by switching these nodes into only receivers to avoid activating jammers and (2) locate the jammers based on the trigger nodes, thus providing a mechanism against reactive jamming attacks.



IMAGE OF USAGE



CONFLICT-AVOIDING CODES

Conflict-avoiding codes (CAC) are sets of **protocol sequences** for a **multiple-access channel** (collision channel) without feedback.

CDMA (Code Division Multiple Access) spread spectrum communication systems are typical examples using a multiple-access channel without feedback.

A **protocol sequence** is a binary (0,1) sequence such as

0000**1011010111010100000000001010001111**

where an **information packet** is sent if a slot has “**1**”,
a silence symbol is sent if a slot has “0”.



CONFLICT-AVOIDING CODE

- A conflict-avoiding code (**CAC**) of length n and weight k is defined as a set $C \subseteq \{0,1\}^n$ of binary vectors, called codewords, all of Hamming weight k such that the distance of arbitrary *cyclic* shifts of two distinct codewords in C is at least $2k - 2$.
- We denote the class of all the CACs of length n and weight k by $\text{CAC}(n, k)$. Note that a code $C \in \text{CAC}(n, k)$ can be viewed as an $(n, k, 1)$ optical orthogonal code without the autocorrelation property.
- The construction is all about “design”!



MY JOURNEY ON COMBINATORICS

- I was lucky to know this term “combinatorics” when I was an undergraduate student.
- It was in the summer of 1971 (I remembered). At that year Professor Frank K. Hwang (黃光明教授) gave a short course of this topic at NTU.
- The book he used was “**An Introduction to Combinatorial Theory**” by M. Hall. (1st edition)
- This topic was fairly new at that time. Most of us in the class have not heard this “strange” term before.
- I still remember how $R(3,3) = 6$ was proved in the class! And of course, I learned **counting**.



COINCIDENCE

- I chose a university in the States to learn **Topology** which I like very much.
- I was the only student to choose that course in Fall, 1977 and therefore it was cancelled due to the choice of lecturer. (He needs to teach one extra course if he decides to do it.)
- So, besides the regular selection of courses such as Analysis and Algebra, I took “**Combinatorics**” lectured by **Curt C. Lindner** who becomes my supervisor of theses, both M.S. and Ph. D.
- In my first lesson I learned “**Latin squares**” and I ended my study at Auburn (Dec. 1980) with a thesis related to this notion.



MY INVESTMENT

- I did (do) not have much money to worry about over past years.
- So, I invested **my time!**
- Some of you may have known that I did spend a lot time in several sports, **playing and coaching.**
- Sure, I got feed back.
- But, I did not use them for living.
- With the investment on combinatorics, I am able to stand here and tell you: **it is worth of doing it for a long while.**
- **It is for real!**



YOUR INVESTMENT

- Money or Time?

Investing your time!

- Mathematics or Others?

Learning Math. gets you smarter (hopefully)!

- Combinatorics or other fields in Mathematics?

This world is full of Combinatorics!

- Winner?

We are all winners. Keep moving forward!

