Preface

This book contains the abstracts of the talks presented in the International Conference on Graph Theory and Information Security (ICGTIS) 2007. The conference was hosted by Combinatorial Mathematics Research Group, Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Indonesia in co-operation with School of ITMS, University of Ballarat Australia. This conference was dedicated to Prof. Mirka Miller on her 57th birthday.

ICGTIS 2007 was held at ITB, Indonesia on February 10 - 13, 2007. The main themes of this conference are general topics in graph theory and information Security. There were 17 invited and 48 contributed talks in this conference.

We would like to thank the invited speakers and all those who submitted papers to this conference. The selected papers which are presented in the conference will be published as a special volume in Journal of Combinatorial Mathematics and Combinatorial Computing (JCMCC).

The organizer is grateful to School of ITMS University of Ballarat Australia, the Abdus Salam ICTP Trieste Italy, and Institut Teknologi Bandung Indonesia for giving financial supports to the conference. We also thank to the Indonesian Mathematical Society (IndoMS) and The Indonesian Combinatorial Mathematics Society (InaCombS) for the support. The organizer wishes you a successful conference and an exciting stay in Bandung.

Bandung, February 10th, 2007

E. T. Baskoro, J. Ryan, A. N. M. Salman

Co-chair
Organization

The International Conference on Graph Theory and Information Security (ICGTIS) 2007 is hosted by Combinatorial Mathematics Research Group, Faculty of Mathematics and Natural Sciences Institut Teknologi Bandung, Indonesia, in co-operation School of ITMS University of Ballarat Australia.

Program and Organizing Committee

Co-chairs: E. T. Baskoro, J. Ryan, A. N. M. Salman


Program Committee: H. Assiyatun (Institut Teknologi Bandung, Indonesia), B. Widjaja (Universitas Indonesia, Indonesia), Y. M. Cholily (Universitas Muhammadiyah Malang, Indonesia), N. N. Gaos (Institut Teknologi Bandung, Indonesia), Y. Lin (University of Newcastle, Australia), A. Lladó (Universitat Politècnica de Catalunya, Spain), F. A. Muntaner-Batle (Universitat Politècnica de Catalunya, Spain), R. Simanjuntak (Institut Teknologi Bandung, Indonesia), Slamin (Universitas Jember, Indonesia), K. A. Sugeng (Universitas Indonesia, Indonesia), Surahmat (Universitas Islam Malang, Indonesia), S. Suwilo (Universitas Sumatra Utara, Indonesia), S. Uttunggadewa (Institut Teknologi Bandung, Indonesia).
## Table of Contents

### Invited Talks

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>On antimagic labelings of graphs</td>
<td>1</td>
</tr>
<tr>
<td>M. Bača</td>
<td></td>
</tr>
<tr>
<td>Progress on one old and one new graph labeling problem</td>
<td>2</td>
</tr>
<tr>
<td>G. S. Bloom</td>
<td></td>
</tr>
<tr>
<td>Mathematics of privacy</td>
<td>3</td>
</tr>
<tr>
<td>L. Brankovic</td>
<td></td>
</tr>
<tr>
<td>The structure of the critically connected graphs</td>
<td>4</td>
</tr>
<tr>
<td>K. Budayasa</td>
<td></td>
</tr>
<tr>
<td>Labeled graphs and applications</td>
<td>5</td>
</tr>
<tr>
<td>S. M. Hegde</td>
<td></td>
</tr>
<tr>
<td>On the security of individual data</td>
<td>6</td>
</tr>
<tr>
<td>G. O. H. Katona</td>
<td></td>
</tr>
<tr>
<td>Distance constrained graph labelings</td>
<td>7</td>
</tr>
<tr>
<td>J. Kratochvil</td>
<td></td>
</tr>
<tr>
<td>On the bigraceful conjecture</td>
<td>8</td>
</tr>
<tr>
<td>A. Lladó</td>
<td></td>
</tr>
<tr>
<td>Constructive enumeration without isomorphs</td>
<td>9</td>
</tr>
<tr>
<td>B. McKay</td>
<td></td>
</tr>
<tr>
<td>Moore graphs and beyond</td>
<td>10</td>
</tr>
<tr>
<td>M. Miller</td>
<td></td>
</tr>
</tbody>
</table>
Algorithms to obtain cryptographically suitable elliptic curves ........................................ 11
  J. M. Miret

A bridge between engineering and mathematics .......... 12
  B. Rahardjo

Eccentric digraphs..................................................... 13
  J. Ryan

Closures and stable properties .................................... 14
  Z. Ryjáček

New constructions of anonymous membership broadcast-
ing schemes .......................................................... 15
  H. van Tilborg

Elliptic curve cryptography ....................................... 16
  M. Valls

Enterprise graphs and small worlds ............................ 17
  W. D. Wallis

Contributed Talks

Exploration of graph-based conceptual representations using a financial ex-
ample ................................................................. 18
  J. Aisbett¹, J. Rickard², G. Gibbon¹

On the Ramsey numbers for a combination of paths and
Jahangirs .............................................................. 19
  K. Ali³, E. T. Baskoro²

3-star factors in random $d$-regular graphs .................... 20
  H. Assiyatun, L. Yulianti
Ramsey \((K_{1,2}, C_4)\)-minimal graphs ........................................ 21
E. T. Baskoro, L. Yulianti, H. Assiyatun

The critical sets of a double star ................................. 22
E. T. Baskoro\(^1\), U. Wijayanti

On some chromatic properties of Jahangir graph ............ 23
A. A. Bhatti

Smart card applications as security media on fixed-line telephone communications .................................................. 24
S. Cahyono\(^1\), I. Rahayu\(^2\), D. Priyasta\(^3\), A. Sarotama\(^3\), F. R. Triputra\(^3\), Sobar\(^4\), M. M. Sarinanto\(^3\)

Antimagic labeling of disconnected graphs .................... 25
Dafik\(^1,2\), M. Miller\(^1,3\), J. Ryan\(^1\), M. Bača\(^1,4\)

Toughness threshold for the existence of 2-walks in \(K_4\)-minor free graphs ......................................................... 26
Z. Dvořák\(^1\), D. Král\(^1\), J. Teska\(^2\)

Gödel numbering method for coding finite graphs .......... 27
Ernastuti, R. A. Salim

On a new family of Fibonacci-like cubes ...................... 28
Ernastuti, A. Juarna

Labeling generating matrices ........................................ 29
R. M. Figueroa-Centeno\(^1\), R. Ichishima\(^2\), F. A. Muntaner-Batle\(^3\), M. Rius-Font\(^4\)

State of the art frequent semistructured pattern: mining, searching and its application .......................... 30
F. L. Gaol, B. Widjaja

Some Ramsey numbers involving bipartite graph .......... 31
Hasmawati, H. Assiyatun, E. T. Baskoro, A. N. M. Salman
Super edge-magic total labeling of banana trees .......................... 32
M. Hussain¹, E. T. Baskoro², Slamín³

Critical set of caterpillar graph for secret sharing scheme .......... 33
C. Imron¹, B. Setiyono¹, R. Simanjuntak², E. T. Baskoro²

Metric dimensions of some corona graphs ................................. 34
H. Iswadi, E. T. Baskoro, R. Simanjuntak, A. N. M. Salman

On the partition dimension of unicyclic graphs .......................... 35
I. Javaid

The balance property of three-symbol cutting sequences ............... 36
R. A. D. Kooswinarsinindiyah

A closure concept in $K_{1,r}$-free graphs ................................. 37
R. Kužel

On describing the incidence matrix of a finite projective
plane via orthogonal latin squares and via a digraph complete
set of latin squares ......................................................... 38
C. Levesque

Edge span of $L(p, q)$-labelings on wheel graphs ............ 39
Y. L. Lai, S. J. Wu

On the extremal graph of maximum size with given order
and girth ................................................................. 40
Y. Lin², M. Miller²

About the number of semi-latin squares orthogonal to a
particular latin square ................................................... 41
S. Malik

$P_h$-supermagic labeling of $S_n^{(m_1, m_2, \ldots, m_n)}$ .................. 42
T. K. Maryati, E. T. Baskoro, A. N. M. Salman
On the structure of path-like trees......................... 43
   F. A. Muntaner-Batle\textsuperscript{1}, M. Rius-Font\textsuperscript{2}

On super edge-magic deficiency of graphs ............... 44
   A. A. G. Ngurah, E. T. Baskoro, R. Simanjuntak, S. Uttunggadewa

Diagram-based verification of parameterized systems ... 45
   C. E. Nugraheni

The total edge-irregular strengths of the corona product
   of graphs .................................................. 46
   Nurdin, A. N. M. Salman, E. T. Baskoro

Characterization of graphs of maximum degree 3, with
   small diameters and defect at most 4 ................. 47
   G. Pineda-Villavicencio\textsuperscript{1,2}, M. Miller\textsuperscript{1,3}

Hamiltonian properties of generalized Halin graphs .... 48
   A. M. Qureshi, S. Malik

Network manager for key management on secure fixed-
   line telephone ................................................. 49
   I. Rahayu\textsuperscript{1}, S. Cahyono\textsuperscript{2}, D. Priyasta\textsuperscript{3}, A. Sarotama\textsuperscript{3}, F. R. Triputra\textsuperscript{3},
   Soabar\textsuperscript{4}, M. M. Sarinanto\textsuperscript{3}

Vertex-magic total labeling of the union of suns ........ 50
   M. T. Rahim\textsuperscript{1}, Slamin\textsuperscript{2}

A note on chromaticity of certain bipartite graphs .... 51
   H. Roslan \textsuperscript{1}, Y. H. Peng\textsuperscript{2}

On vertex irregular total labeling of Petersen graph .... 52
   M. Roswita, D. Indriati, T. A. Kusmayadi

The computational complexity of $\lambda$-backbone coloring of
   graphs with $n$-complete backbones .................... 53
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Isoperimetric orderings in cartesian powers of graphs</td>
<td>54</td>
</tr>
<tr>
<td>O. Serra</td>
<td></td>
</tr>
<tr>
<td>Some open problems on edge antimagic total labeling</td>
<td>55</td>
</tr>
<tr>
<td>D. R. Silaban and K. A. Sugeng</td>
<td></td>
</tr>
<tr>
<td>On 3-defective colourings of complementary graphs</td>
<td>56</td>
</tr>
<tr>
<td>M. Simanihuruk(^1), N. Achuthan(^2), N. R. Achuthan(^2)</td>
<td></td>
</tr>
<tr>
<td>New constructions of (A)-magic graphs using labeling matrices</td>
<td>57</td>
</tr>
<tr>
<td>K. A. Sugeng(^1), M. Miller(^2)</td>
<td></td>
</tr>
<tr>
<td>Optimum sum labeling of finite union of sum graphs</td>
<td>58</td>
</tr>
<tr>
<td>K. A. Sugeng, R. Rusin, H. Burhan</td>
<td></td>
</tr>
<tr>
<td>A survey on Ramsey numbers of cycles with respect to wheels or</td>
<td>59</td>
</tr>
<tr>
<td>generalized wheels</td>
<td></td>
</tr>
<tr>
<td>Surahmat</td>
<td></td>
</tr>
<tr>
<td>The mesh-connected model in parallel computing for shortest path</td>
<td>60</td>
</tr>
<tr>
<td>M. Susmikanti</td>
<td></td>
</tr>
<tr>
<td>Primitive graphs with exponent 4</td>
<td>61</td>
</tr>
<tr>
<td>S. Suwilo</td>
<td></td>
</tr>
<tr>
<td>HSAGA and its application to the construction of Near-moore</td>
<td>62</td>
</tr>
<tr>
<td>digraphs</td>
<td></td>
</tr>
<tr>
<td>J. Tang(^1), Y. Lin(^2), M. Miller(^1,(^3)</td>
<td></td>
</tr>
<tr>
<td>Tree-path size multipartite Ramsey numbers</td>
<td>63</td>
</tr>
<tr>
<td>S. Uttunggadewa, Syafirzal Sy, H. Assiyatun, E. T. Baskoro</td>
<td></td>
</tr>
</tbody>
</table>
Total vertex irregular labelings of wheels, fans, suns and friendship graphs

K. Wijaya¹, Slamin

Efficient traitor-tracing algorithms based on list decoding

X. W. Wu¹, M. Kuijper², P. Udaya²
On antimagic labelings of graphs

M. Bača

Department of Applied Mathematics
Technical University of Košice
Slovak Republic
Martin.Baca@tuke.sk

Abstract. A labeling of a graph is any map that carries some set of graph elements to numbers (usually to the positive integers). Magic labelings are one-to-one maps onto the appropriate set of consecutive integers starting from 1, with some kind of "sum" property. An edge-magic total labeling on a graph with \(v\) vertices and \(e\) edges is defined as a one-to-one map taking the vertices and edges onto the integers 1, 2, \ldots, \(v + e\) with the property that the sum of the label on an edge and the labels of its endpoints is constant independent of the choice of edge. If the sums of the labels on the edges and the labels of their endpoints form an arithmetic progression starting from \(a\) and having common difference \(d\) then the labeling is called \((a, d)\)-edge-antimagic total.

We will present edge-magic and edge-antimagic labelings for some families of graphs.
Progress on one old and one new graph labeling problem

G. S. Bloom

Computer Science Department The City College of
The City University of New York
&
The CUNY Graduate Center
New York, NY
bloom@cs.ccny.cuny.edu

Abstract. The NEW PROBLEM: Any $N \times N$ Magic Square can be used to assign weights to the nodes and arcs of a $N$-node bi-directed complete graph. That resulting digraph labeling has the property that one common sum $M$ results from adding the value at any particular node $v$ to the values on the out-going arcs from $v$. Also, that same $M$ equals the sum at any node $v$ of the value at that node plus the values on the in-coming arcs to $v$. We call this labeling of the bi-directed $K_n$ a magic labeling, and because of the existence of this labeling, we say that the bi-directed $K_n$ is a magic digraph. In this talk, we list some necessary conditions for any digraph to have a magic labeling. These include constraints on the relative number of nodes and arcs, as well as a growing but incomplete list of sub-digraphs whose presence is forbidden in any magic digraph. We will discuss how our computer search for magic labelings among the 742 five-node digraphs with an appropriate number of arcs has been leading us to discover more of the forbidden subgraphs.

The OLD PROBLEM: We will look at the highly provoking question of whether all trees are graceful from the perspective of Canonical Adjacency Matrices (CAMs). CAMs allow us to see patterns of graceful labelings in various classes of graphs and may yet steer us to the tools that grant a state of grace to all trees.
Mathematics of privacy

L. Brankovic

School of Electrical Engineering and Computer Science
University of Newcastle, Callaghan, Australia 2308
Ljiljana_Brankov@cs.newcastle.edu.au

Abstract. Data mining and statistical analysis are now becoming a matchless tool for research and strategic planning and are used by companies, governments and research institutions alike. They both depend on massive databases often containing personal information but it is commonly assumed that only aggregate values and patterns will be made available to users and that no confidential individual values could be disclosed. There are two general approaches to ensure this: adding noise to the original data and restricting queries that can be asked of the database. In either case it may still be possible to "compromise" the database, that is, to compute individual values or other sensitive information from a suitable combination of aggregate values.

In this talk we pay a special attention to the balance between the usability and the privacy of the individual records in the database and we focus on the interplay between mathematics and security. We show, for example, the connection between compromise-free query collections and graphs with least eigenvalue -2, and the relationship between maximal compromise-free query collection and a maximum antichain of a finite set.
The structure of the critically connected graphs

K. Budayasa

Department of Mathematics Faculty of Mathematics and Natural Sciences
State University of Surabaya, Indonesia
ketutbudayasa@yahoo.com

Abstract. In the application of graph theory to problems arising in network design and analysis, one considers a number of graph parameters such as connectivity, edge-connectivity, distance, diameter, degree. For instance, the number of line interfaces available at a communication centre imposes a degree constraint on the vertex representing that centre. The minimum number of link (centre) failures required to destroy communication between at least two centres in the network corresponds to the edge(vertex)-connectivity of the graph representing the network. Thus the edge-connectivity and vertex-connectivity of a graph yield information concerning the reliability of a network subject to link and centre failures, respectively. Usually the design problem reduces to an extremal problem (or graph optimization problem) concerning one or more graph parameters. To solve such problems one needs a characterization of the particular graph parameter of interest. In the characterization of such parameters it is very often useful to study a restricted class of graphs, the so called critical graphs.

The term critical is used in the literature in several ways. Usually it is used with respect to a specified graph parameter P and applies when the graph G under consideration has the property P but alteration of G (such as edge deletion or vertex deletion) results in a graph not having property P. The resultant critical class of graphs has more structure than the general class and this structure can be utilized to yield a considerable amount of useful information. Often there is no loss of generality and quite a lot to again, in considering this class of graphs.

In this paper we consider graphs which are critical with respect to edge-connectivity under single operation of edge deletion. A comprehensive structure of this class of graphs will be presented in the paper. Also, we will mention some unsolved problems.
Labeled graphs and applications

S. M. Hegde

Dept. of Mathematical and Computational Sciences
National Institute of Technology Karnataka
Surathkal, Srinivasnagar-575025, India
smhegde@nitk.ac.in

Abstract. Graph labelings, where the vertices and edges are assigned real values or subsets of a set subject to certain conditions, have often been motivated by their utility to various applied fields and their intrinsic mathematical interest (logico - mathematical). Labeled graphs are becoming an increasingly useful family of Mathematical Models for a broad range of applications. While the Qualitative labelings of graph elements have inspired research in diverse fields of human enquiry such as Conflict resolution in social psychology, electrical circuit theory and energy crisis, quantitative labelings of graphs have led to quite intricate fields of application such as Coding Theory problems, X-Ray Crystallographic analysis, to Design Communication Network addressing Systems, in determining Optimal Circuit Layouts and Radio- Astronomy, Additive Number Theory and Algebra, etc.

If a nonnegative integer (or subset of a set) $f(v)$ is assigned to each vertex $v$ of $G$ then the vertices of $G$ are said to be labeled. $G$ is itself a labeled graph if each edge $e = uv$ is given the label $f(uv) = f(u) * f(v)$, where * is a binary operation. In literature one can find that the binary operation * is either, addition or multiplication or modulo addition or absolute difference or symmetric difference.

In the absence of additional constraints, every graph can be labeled in infinitely many ways. Thus, utilization of labeled (numbered) graph models requires imposition of additional constraints which characterize the problem being investigated.

In this talk we present some equivalence, redundancy and ambiguities in graph labeling problems followed by some of the applications in detail.
On the security of individual data

G. O. H. Katona

Alfréd Rényi Institute of Mathematics, HAS
Budapest P.O.B. 127 H-1364, Hungary
ohkatona@renyi.hu

Abstract. We will consider the following problem in the present paper: Assume there are $n$ numerical data $\{x_1, x_2, \ldots, x_n\}$ (like salaries of $n$ individuals) stored in a database and some subsums of these numbers are made public or just available for persons not eligible to learn the original data. Our first question is: at most how many of these subsums may be disclosed such that none of the numbers $x_1, x_2, \ldots, x_n$ can be uniquely determined from these sums. These types of problems arise in the cases when certain tasks concerning a database are done by subcontractors who are not eligible to learn the elements of the database, but naturally should be given some data to fulfill there task.

Mirka Miller and her co-authors in a nice and surprising theory have shown that this problem is equivalent to the following question: If there are $n$ real, non-zero numbers $\{x_1, x_2, \ldots, x_n\}$ given, what is the maximum number of their 0 subsums. This approach, together with the Sperner theorem shows that no more than $\binom{n}{n/2}$ subsums of a given set of secure data may be disclosed without disclosing at least one of the data. This bound is sharp.

However, it is natural to assume that the disclosed subsums of the original elements of the database will contain only a limited number of elements, say at most $k$ (in real applications the number $n$ of data is usually huge, while the number of operations is in most of the cases limited). We have now the same question: at most how many of these subsums of at most $k$ terms may be disclosed in such a way that none of the numbers $x_1, x_2, \ldots, x_n$ can be uniquely determined from these sums. A similar, but more complicated approach gives the main result of the paper: the maximum number of them is exactly $\sum_{i=1}^{k/2} \binom{n/2}{i}^2$ for $n > n(k)$. 
Distance constrained graph labelings

J. Kratochvíl

Department of Applied Mathematics, Charles University
Malostranské nám. 25, 11800 Praha 1, Czech Republic
honza@kam.mff.cuni.cz

Abstract. Motivated by a very practical problem of Frequency Assignment, the distance constrained graph labelings provide a graph invariant which turns out to be quite interesting also from the theoretical point of view. For instance, this problem belongs to the very few problems known to be solvable in polynomial time for trees but NP-complete already for tree-width two graphs (series-parallel graphs). We will survey recent results and open problems in this area, including the problem of bounds on the optimal span of a labeling in terms of maximum degree which is closely related to the existence of graphs close to the Moore bound.
On the bigraceful conjecture

A. Lladó

Departament de Matemàtika Aplicada IV
Universitat Politècnica de Catalunya, Barcelona, Spain
allado@ma4.upc.es

Abstract. The validity of the well-known graceful conjecture would imply Ringel’s Conjecture from 1963, which says that every tree with $m$ edges decomposes the complete graph $K_{2m+1}$. In the same way the closely related bigraceful conjecture would solve the conjecture stated by Hagkvist in 1989 saying that the complete bipartite graph $K_{m,m}$ can be decomposed by any arbitrary tree with $m$ edges. For a bipartite graph $G$ with stable sets $V = A \cup B$ and $m$ edges, a map $f : A \cup B \to [1;m]$ is bigraceful if (i) the restrictions of $f$ to each stable set are injective maps, and (ii) the values of $f$ over all the edges are pairwise distinct positive integers, where the value of $f$ on an edge $uv \in E(G)$ with $u \in A$ is defined by $f(uv) = f(u) - f(v)$. The bigraceful conjecture, formulated by Lladó and Ringel in 1995, says that every tree admits a bigraceful map. We will give an overview of the known results on the bigraceful conjecture and present some new ones, particularly concerning the number of bigraceful maps of some classes of trees.
Constructive enumeration without isomorphs

B. McKay

Australian National University
bdm@cs.anu.edu.au

Abstract. We survey the problem of generating classes of combinatorial objects without isomorphic objects appearing. The methods considered will include orderly generation and the method of canonical augmentation, as well as more brute-force methods. Examples will be given from graph theory.
Moore graphs and beyond

M. Miller

School of ITMS
University of Ballarat
AUSTRALIA
m.miller@ballarat.edu.au

Abstract. In this paper we consider the well known degree/diameter problem: Given natural numbers $\triangle$ and $D$, find the largest possible number of vertices $n(\triangle, D)$ in a graph of maximum degree and diameter at most $D$.

There is a straightforward upper bound on the largest possible order (i.e., the number of vertices) $n(\triangle, D)$ of a graph $G$ of maximum degree $\triangle$ and diameter $D$. Trivially, if $\triangle = 1$ then $D = 1$ and $n(1, 1) = 2$. For $\triangle > 1$ and $D > 1$, we have

$$n(\triangle, D) \leq M(\triangle, D) = 1 + \triangle + \triangle(\triangle - 1) + \cdots + \triangle(\triangle - 1)^{D-1}.$$ 

The right-hand side of the inequality, $M(\triangle, D)$, is called the Moore bound. A graph whose order is equal to the Moore bound $M(\triangle, D)$, is called a Moore graph; such a graph is necessarily regular of degree $\triangle$.

The directed version of the problem is: Given natural numbers $d$ and $k$, find the largest possible number of vertices $n(d, k)$ in a digraph of maximum out-degree $d$ and diameter at most $k$.

As in the case of undirected graphs, there is a natural upper bound $n(d, k)$ on the order of directed graphs (digraphs), given maximum out-degree $d$ and diameter $k$,

$$n(d, k) \leq M(d, k) = 1 + d + d^2 + \cdots + d^k.$$ 

The right-hand side, $M(d, k)$, is called the Moore bound for digraphs. If the equality holds then the digraph is called a Moore digraph.

We will give an overview of the degree/diameter problem for both undirected and directed graphs and present several open problems in this area.
Algorithms to obtain cryptographically suitable elliptic curves

J. M. Miret
Mathematics Department
Escola Polit'ecnica Superior
Universitat de Lleida, Spain
miret@eps.udl.es

Abstract. Elliptic curve cryptosystems are nowadays widely used, since they can offer significant security levels but using small key-lengths. Nevertheless there still arise some open problems concerning the procedure to obtain elliptic curves which fit security requirements for being used in the cryptosystems setup. Security policies suggest that this setup should be refreshed periodically, hence a bunch of good curves is needed. In this talk we will present a couple of such techniques. On the one hand, we will provide an efficient algorithm to determine the order and the structure, including generators, of the \( \ell \)-Sylow subgroup. A successive \( \ell \)-dividing points process allows us to reach points whose order is the maximum \( \ell \)-power. Non-suitable elliptic curves can be rejected from the knowledge of this structure. On the other hand, we will describe an algorithm to obtain cryptographically good elliptic curve from a given one. This algorithm takes benefit from the fact that isogenous curves have the same cardinal. The core of the algorithm consists on traversing the volcano-graph of isogenies of a suitable curve.
A bridge between engineering and mathematics

B. Rahardjo

School of Electrotechnics and Informatics
Institut Teknologi Bandung, Indonesia
br@paume.itb.ac.id

Abstract. We live in an exciting time in which business is done through electronic means. Electronic business, transactions, and communications are now part of our daily lives. We do not go to physical bank anymore but go to ATM machines. We, at least in Indonesia, use our cellular phones everyday. We feel insecure if we left our cellular phones at home. Some say that we become too dependent on electronic devices. All of this is possible due to the technology development in computers and telecommunication.

One key aspect of electronic business acceptance is security. Confidentiality, privacy, integrity, and availability are aspects of security that must be guaranteed in electronic business transactions. Encryption is one means to provide security. Encryption depends heavily on math. Encryption algorithms such as RSA or ECC are basically mathematical equations.

These encryption algorithms must be implemented in software or hardware. This task falls upon the shoulder of engineers, be that software engineers or hardware engineers. Thus, engineers must understand the mathematics behind them and how to implement them in software or hardware.

Implementing encryption, which is basically math equations, in software or hardware is not straightforward. There is a limited resource in hardware implementation. Small and portable electronic devices have limited memory and CPU cycle. Computing the equations must be done in real-time if the solution is going to be implemented in real applications. We do not want to wait for five minutes in an ATM booth for the machine to finish its encryption process. The time it takes to process the data should be acceptable.

When an electronic engineer creates a circuit, be that analog or digital circuit, she actually creates a set of mathematical equations. In digital circuit, the mathematical equation is "simpler" but they have a large number of such equations. For example, a chip may have two million variables. The scale of the problem what makes it difficult to solve, even with the help of computers.

Engineers may have strong foundation in mathematics. They may even have interest in it, but many times we hear complain that math is not taught properly in engineering classes. The materials taught in these classes are boring and too abstracts for engineering students. The result is a hate towards mathematics.

A bridge between engineering and mathematics must be built.

There have been many examples of digital heroes who got interested in engineering because they read books on certain topics, including mathematics. These books inspire them to become engineers and develop products that make our live better. Let us develop such a bridge.
Eccentric digraphs

J. Ryan

School of Information Technology and Mathematical Sciences
University of Ballarat, Ballarat 3350, Victoria, Australia
joe.ryan@ballarat.edu.au

Abstract. The eccentricity \( e(u) \) of a vertex \( u \) in a digraph \( G \) is the maximum distance from \( u \). A vertex \( v \) is an eccentric vertex of \( u \) if the distance from \( u \) to \( v \) is equal to \( e(u) \). The eccentric digraph \( ED(G) \) of a digraph \( G \) has the same vertex set as \( G \), but with an arc from \( u \) to \( v \) in \( ED(G) \) if and only if \( v \) is an eccentric vertex of \( u \) in \( G \). Eccentric digraphs were introduced by Buckley (Buckley, 2001) as a function of a graph. Later Boland and Miller (Boland and Miller, 2001) extended the concept to include digraphs in the function domain. This development enabled eccentric digraphs to be viewed as part of a sequence. Given a positive integer \( k \), the \( k \)th iterated eccentric digraph of \( G \) is defined as \( ED^k(G) = ED(ED^{k-1}(G)) \), where \( ED^0(G) = G \). In this talk we will present an overview of the behaviour of eccentric digraphs including known results about the sequences of eccentric digraphs, characterisation of eccentric digraphs, the relationship between eccentric digraph and complement operators and special cases such as when the eccentric digraph is symmetric or disconnected.
Closures and stable properties

Z. Ryjáček

University of West Bohemia, Pilsen, Czech Republic
ryjacek@kma.zcu.cz

Abstract. Closure techniques are a powerful tool in studying various graph properties. In the talk we survey recent results on variations of closure concepts in line graphs and claw-free graphs and on stability of graph properties with respect to these closure operations.
New constructions of anonymous membership broadcasting schemes

H. van Tilborg
Technische Universiteit Eindhoven
H.C.A.v.Tilborg@tue.nl

Abstract. An anonymous membership broadcast scheme is a method in which a sender broadcasts the secret identity of one out of $n$ participants, in such a way that only the right participant knows that he is the intended recipient, while the others do not have any information about this identity (except that they know that they are not the intended one).

In a $w$-anonymous membership broadcast scheme any coalition of at most $w$ participants not containing the selected participant cannot determine any information about the identity of the selected participant.

After an introduction, we shall present two new constructions of $w$-anonymous membership broadcast schemes. The first construction is based on error-correcting codes and we show that there exist schemes that allow a flexible choice of $w$, while complexities for broadcast communication, user storage and required randomness are polynomial in $\log n$.

The second construction is based on the concept of collision-free arrays. The construction results in more flexible schemes, allowing trade-offs between different complexities.
Abstract. Since Koblitz and Miller pointed out the interest of the usage of elliptic curves in the design of cryptosystems, they have captured a lot of attention from the cryptographic community. The cornerstone of Elliptic Curve Cryptosystems (ECC) lies on the fact that the discrete logarithm problem (DLP) is harder in the group of points of an elliptic curve rather that in the multiplicative group of a finite field. Hence, ECC can offer equivalent security than DLP-based cryptosystems (like ElGamal, for instance) but using significantly smaller key-lengths. This breakthrough makes these cryptosystems more suitable for being used in devices which present computational and memory restrictions, such as smart cards or RFID tags.

In this talk, we will overview the main aspects concerning elliptic curve cryptography, beginning with an introduction to the basic concepts and properties, surveying then several cryptosystems based on elliptic curves, and ending with some applications.
Enterprise graphs and small worlds

W. D. Wallis

Department of Mathematics Southern Illinois University
Carbondale, IL 62901-4408 USA
Phone: 1 618 453 6577, Fax: 1 618 453 5300
wdwallis@rocketmail.com

Abstract. Recently there has been a great deal of study of the "small world" phenomenon, and the way in which social communications networks grow.

An enterprise network is the communications network of an enterprise such as a large business, military organization, etc. Such networks grow from a strict hierarchical basis, and as such one might expect them to be very different from the "small world" model.

We shall discuss the characteristics of these two types of networks and in particular of their underlying graphs.
Exploration of graph-based conceptual representations
using a financial example

J. Aisbett¹, J. Rickard², G. Gibbon¹

¹The University of Newcastle
{Janet.Aisbett, Greg.Gibbon}@newcastle.edu.au
²Lockheed Martin Corporation

Abstract. Concepts are often described in terms of membership in a set of properties, for example as green round objects or tall thin people. The relationship between properties may also be critical, as when tall thin and short wide rectangles are assigned to the same concept class of medium size rectangles. Concepts have therefore been previously defined as labeled weighted graphs in which the nodes are properties and the edge strengths are the associations between properties. Nodes may also have weights, according to the importance or salience of that property to that concept. Many graph matching algorithms are then available to compute the similarity of two concepts. Such an algorithm typically involves penalties for differing weights between nodes and edges, including penalties for unmatched nodes. In conceptual spaces, properties are defined to be regions in sets (called domains) which have some geometrical structure, such as a distance function. This allows an observation on a domain to be compared to a property, that is, to be assigned some degree of membership in that property. An arbitrary observation over several domains can thus be represented as a weighted graph in which node weights are property membership values, and edge strengths are a function of the weights on the nodes linked by that edge. The properties used in this construction typically depend on context and/or on an attention setting mechanism. The weighted graph representing the observation can then be compared with concepts with the graph matching algorithm, to perform tasks such as prediction and classification. However, there are many design decisions in the specification of domains, properties and similarity measures which affect task performance. This paper looks at the effect of overlapping properties and of the choice of graph matching algorithm on a specific application area: the prediction of stock market prices.

Keywords: conceptual space, weighted graph
On the Ramsey numbers for a combination of paths and Jahangirs

K. Ali\textsuperscript{1}, E. T. Baskoro\textsuperscript{2}

\textsuperscript{1}School of Mathematical Sciences, Government College University

Lahore, Pakistan

akashifali@gmail.com

\textsuperscript{2}Combinatorial Mathematics Research Group

Faculty of Mathematics and Natural Science, Institut Teknologi Bandung

Jalan Ganesa 10 Bandung, Indonesia

ebaskoro@dns.math.itb.ac.id

Abstract. For given graphs $G$ and $H$, the Ramsey number $R(G, H)$ is the least natural number $n$ such that for every graph $F$ of order $n$ the following condition holds: either $F$ contains $G$ or the complement of $F$ contains $H$. In this paper, we improve the Surahmat and Tomescu’s result on the Ramsey number of paths versus Jahangirs. We also determine the Ramsey number $R(\cup G, H)$, where $G$ is a path and $H$ is a Jahangir graph, where for $m \geq 2$, the Jahangir graph $J_{2m}$ is a graph consisting of a cycle $C_{2m}$ with one additional vertex adjacent alternating to $m$ vertices of $C_{2m}$.

Keywords: Jahangir graph, path, Ramsey number
3-star factors in random $d$-regular graphs

H. Assiyatun, L. Yulianti

Combinatorial Mathematics Research Group
Faculty of Mathematics and Natural Science, Institut Teknologi Bandung
Jalan Ganesa 10 Bandung, Indonesia
hilda@math.itb.ac.id, lyra@students.itb.ac.id

Abstract. The Small Subgraph Conditioning Method has been used to study the almost sure existence and the asymptotic distribution of the number of regular spanning subgraphs of various types in random $d$-regular graphs. In this paper we use the method to determine the almost sure existence and the asymptotic distribution of the number of 3-star factors in random $d$-regular graphs for $4 \leq d \leq 10$.

Keywords: small subgraph conditioning method, random $d$-regular graph, 3-star factor

* Permanent address: Department of Mathematics, Universitas Andalas, Kampus UNAND Limau Manis Padang, Indonesia
Ramsey \((K_{1,2}, C_4)\)-minimal graphs

E. T. Baskoro, L. Yulianti*, H. Assiyatun
Combinatorial Mathematics Research Group
Faculty of Mathematics and Natural Science, Institut Teknologi Bandung
Jalan Ganesa 10 Bandung, Indonesia
\{ebaskoro, hilda\}@math.itb.ac.id, lyra@students.itb.ac.id

Abstract. For any given graphs \(G, F\) and \(H\), we write \(G \rightarrow (F, H)\) to mean that any red-blue coloring of the edges of \(G\) contains a red copy of \(F\) or a blue copy of \(H\). Graph \(G\) is \((F, H)\)-minimal (Ramsey Minimal) if \(G \rightarrow (F, H)\) but \(G^* \nrightarrow (F, H)\) for any proper subgraph \(G^* \subset G\). The class of all \((F, H)\)-minimal graphs will be denoted by \(\mathcal{R}(F, H)\). In this paper we will determine the graphs in \(\mathcal{R}(K_{1,2}, C_4)\).

Keywords : Ramsey-minimal graph

* Permanent address: Department of Mathematics, Universitas Andalas, Kampus UNAND Limau Manis Padang, Indonesia
The critical sets of a double star

E. T. Baskoro¹, U. Wijayanti

¹Combinatorial Mathematics Research Group
Faculty of Mathematics and Natural Science
Institut Teknologi Bandung
Jl. Ganesa 10 Bandung 40132, Indonesia
ebaskoro@math.itb.ac.id, utari_w@telkom.net

Abstract. Let $\lambda$ be an edge magic total (EMT) labelling of graph $G(V,E)$. Any partial labelling of $\lambda$ is called a partial EMT labelling on $G$. A partial EMT labelling $\pi$ on graph $G$ is said to be uniquely completable if it is expanded in exactly one EMT labelling on $G$. A partial EMT labelling $\pi$ is a critical set if (1) $\pi$ is uniquely completable and (2) no proper partial labelling of $\pi$ satisfies property 1. In this paper we study the critical sets in an edge magic total labelling on a double star. For the purpose, we introduce a concept, i.e. label sharing on every leaf or leaf’s edge.

Keywords: caterpillar graph, critical sets, double star, edge-magic total labelling, Kotzig-Rosa EMT labelling
On some chromatic properties of Jahangir graph

A. A. Bhatti

School of Mathematical Sciences, Government College University
68-B, New Muslim Town, Lahore, Pakistan
akhlaq4782003@yahoo.com

Abstract. In this note we compute the chromatic polynomial of the Jahangir graph $J_{2p}$ and we prove that it is chromatically unique for $p = 3$.

Keywords: chromatic polynomial, chromatic uniqueness, Jahangir graph
Smart card applications as security media on fixed-line telephone communications

S. Cahyono¹, I. Rahayu², D. Priyasta³, A. Sarotama³, F. R. Triputra³, Sobar⁴, M. M. Sarinanto³

¹National Crypto Institute, Bogor, Indonesia
setyo18@yahoo.com
²Crypto Assessment Center, LSN, Jakarta, Indonesia
ints06@yahoo.com
³ICT Center, BPPT, Jakarta, Indonesia
{darma, afrias, fadjar, nanto}@inn.bppt.go.id
⁴Bakti Jaya Transecurindo, Jakarta, Indonesia

Abstract. Currently in the information age, security requirement of information increased together with awareness of the importance of the information sense for individual or institutions. To protect the information that communicate by communication media, we can do protection on communication mode and access control on communication device. Smart card has superiority such as programmable, support Cryptographic service i.e. encryption/decryption and hash function, high mobility, privacy utilization and adhere to certain individual, accordingly smart card is interesting alternative technology to access control and protection the communication device. In this paper, we report a study of smart card utility as security media on Crypto Module which developed on on fixed-line telephone. The smart card will consist of user authentication value, encryption/decryption algorithm, and cryptographic keys that will be use by encryption and decryption process. The cryptographic keys on smart card will be authenticated and encrypted. Particularly, smart card will be used as media to distribute to each communication device, so the Cryptographic keys will be used as input to Cryptographic algorithm on Crypto Module. Optimization of Smart Card application design on communication fixed-line telephone is main target of this study, in order to yield to robust application. This paper will discuss about configuration of application that gained to fulfill the need of high mobility, security and configurability.

Keywords: authentication, cryptography, decryption, encryption, hash function, security media, smart card
Antimagic labeling of disconnected graphs

Dafik$^{1,2}$, M. Miller$^{1,3}$, J. Ryan$^1$, M. Bača$^{1,4}$

$^1$School of Information Technology and Mathematical Sciences
University of Ballarat, Australia
$^2$Department of Mathematics Education
Universitas Jember, Indonesia
$^3$Department of Mathematics
University of West Bohemia, Plzeň, Czech Republic
$^4$Department of Appl. Mathematics
Technical University, Košice, Slovak Republic
d.dafik@students.ballarat.edu.au, \{m.miller,
joe.ryan\}@ballarat.edu.au
Martin.Baca@tuke.sk

Abstract. This paper deals with a certain type of labeling and its evaluation for a finite graph $G$, consisting of a vertex-set $V(G)$ and an edge-set $E(G)$. More specifically, an $(a, d)$-edge-antimagic total labeling on $G$ is a one-to-one map $f$ from $V(G) \cup E(G)$ onto the integers $1, 2, \ldots, |V(G)| + |E(G)|$, with the property that the evaluation, called edge-weights, $w(uv) = f(u) + f(v) + f(uv)$, $uv \in E(G)$, form an arithmetic progression starting from $a$ and having the common difference $d$. Such a labeling is referred to as super if the smallest labels appear on the vertices.

The aim of this talk is to present recent results concerning super $(a, d)$-edge-antimagic total labelings of a certain class of disconnected graphs. The talk will conclude with several related open problems.

Keywords: disconnected graphs, super $(a, d)$-edge-antimagic total labeling
Toughness threshold for the existence of 2-walks in $K_4$-minor free graphs

Z. Dvořák¹, D. Král¹*, J. Teska²

¹Institute for Theoretical Computer Science (ITI)
Faculty of Mathematics and Physics, Charles University
Malostranské Náměstí 25, 118 00 Prague 1, Czech Republic
{rakdver,kral}@kam.mff.cuni.cz.

²School of ITMS, University of Ballarat, VIC 3353, Australia and
Department of Mathematics, University of West Bohemia
Univerzitní 8, 306 14 Plzeň, Czech Republic
teska@kma.zcu.cz

Abstract. A 2-walk is a closed spanning trail which uses every vertex at most twice. The toughness of a non-complete graph is $t(G) = \min(\frac{|S|}{c(G - S)})$, where the minimum is taken over all nonempty vertex sets $S$, for which $c(G - S) \geq 2$ and $c(G - S)$ denotes the number of components of the graph $G - S$. We show that every $K_4$-minor free graph with toughness $t(G) > \frac{4}{7}$ has a 2-walk. We also give an example of a $\frac{4}{7}$-tough $K_4$-minor free graph with no 2-walk.

Keywords : chordal, $K_4$-minor free, toughness, 2-walk

* Institute for Theoretical Computer Science is supported as project 1M0021620808 by Czech Ministry of Education
Godel numbering method for coding finite graphs

Ernastuti, R. A. Salim
Fakultas Ilmu Komputer, Universitas Gunadarma
{ernas, ajuarna}@staff.gunadarma.ac.id

Abstract. Godel Numbering is a method for associating finite sequence of positive integers \(a_1, a_2, \ldots, a_n\) to a positif integer \(p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}\), \(p_1 = 2\) (the first prime number), \(p_2 = 3\) (the second prime number), \(p_3 = 5\) (the third prime number), \(p_n = n\)-th prime number. This method employs prime number decompositions to map a finite sequence to a unique positive integer which will be called its Godel Number. This paper shows the uniqueness property of Godel numbers, this serves as a point of departure coding finite sequences as follows. Encoding: Given a finite sequence of positive integers \(a_1, a_2, \ldots, a_n\), then its unique Godel Number is \(p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}\). Decoding: Given any positive integer, then it can be transformed into a unique finite sequence of positive integers. A graph \((V, E)\) can be viewed as a sequence of positive integers by a certain way. This paper will show how to use Godel numbering for the purpose of coding finite graphs.

Keywords: coding, finite graph, godel numbering, godel number, prime number
Abstract. A Fibonacci string is a length $n$ binary string contains no two consecutive 1s. Fibonacci cubes, extended Fibonacci cubes and Lucas cubes are subgraphs of hypercube defined in terms of Fibonacci strings; all these cubes were introduced by Hsu (1993), Wu (1997), and Munarini (2002), respectively, as models for interconnection networks. In 2005, Sandi Klavzar shown that all these Fibonacci-like cubes are median graphs; these facts are useful in research on interconnection networks. The research use the expansion property of Fibonacci and Lucas cubes to obtain several enumerative results concerning the number of edges and squares in these cubes, which in turn enable to obtain some identities involving Fibonacci and Lucas numbers. In this paper, we propose a new family of Fibonacci-like cube, namely Extended Lucas Cube ($ELC$), and we present the enumeration of vertices, edges, and squares of $ELC$ by means of reducing it to the corresponding problems in extended Fibonacci cubes and Lucas cubes.

Keywords : cartesian product, fibonacci number, (extended) fibonacci cube, (extended) lucas cube, lucas number, median graph
Labeling generating matrices

R. M. Figueroa-Centeno\textsuperscript{1}, R. Ichishima\textsuperscript{2},
F. A. Muntaner-Batle \textsuperscript{*3}, M. Rius-Font \textsuperscript{**4}

\textsuperscript{1}Mathematics Department
University of Hawai’i at Hilo
200 W. Kawili St.
Hilo, HI 96720-4091

\textsuperscript{2}College of Humanities and Sciences,
Nihon University, 3-25-40 Sakurajosui Setagaya-Ku
Tokyo 156-8550, Japan

\textsuperscript{3}Facultat de Ciències Polítics i Jurídiques
Universitat Internacional de Catalunya, Immaculada 22
08017 Barcelona, Spain

\textsuperscript{4}Departament de Matemàtica Aplicada i Telemàtica
Universitat Politècnica de Catalunya, Jordi Girona Salgado 1
08034 Barcelona, Spain

Abstract. This paper is mainly devoted to generating (special)(super)
edge-magic labelings of graphs using matrices. Matrices are used in order
to find lower bounds for the number of non-isomorphic (special)(super)
edge-magic labelings of certain types of graphs. Also, new applications
of graph labelings are discussed.

Keywords : matrix, (special)(super) edge-magic labeling

\textsuperscript{*} wants to acknowledge Dr. Eduardo Canale since without the mathematical discussions with him and
his very useful advice this work would have been impossible.

\textsuperscript{**} Supported by the Spanish Research Council under project MTM2004-07891-C02-01 and by the Catalan
Research Council under project 2001SGR00258.
State of the art frequent semistructured pattern: mining, searching and its application

F. L. Gaol, B. Widjaja

Faculty of Computer Science-University of Indonesia
flg50@ui.ac.id

Abstract. Scalable analytical algorithms and tools for large Semistructured pattern data sets are in great demand across domains from software engineering to computational biology as it is very difficult, if not impossible, for human beings to manually analyze any reasonably large collection of Semistructured pattern due to their high complexity. In this paper, we investigate two long standing fundamental problems: Given a Semistructured pattern data set, what are the hidden structural patterns and how can we find them? and how can we perform similarity search in large Semistructured pattern data sets?

Semistructured pattern can be formally modeled as Graph. Semistructured pattern mining is an expensive computational problem since sub-Semistructured pattern isomorphism is NP-complete. Previous solutions generate inevitable overheads since they rely on joining two Semistructured pattern to form larger candidates. Semistructured pattern searching, the second problem addressed in this paper, may incur an exponential number of entries if all of the substructures in a Semistructured pattern database are used for searching. The solution proposes a novel, frequent and discriminative Semi structured pattern mining approach that leads to the development of a compact but effective Semistructured pattern searching structure that is orders of magnitude smaller in size but an order of magnitude faster in performance than traditional approaches.

Besides Semistructured pattern mining and search, we provides thorough investigation of pattern summarization, pattern-based classification, constraint pattern mining, and Semistructured pattern similarity searching, which could leverage the usage of Semistruc- tured patterns. It also explores several critical applications in bioinformatics, computer systems and software engineering, including gene relevance network analysis for functional annotation, and program flow analysis for automated software bug isolation.

The developed concepts, theories, and systems may significantly deepen the understanding of data mining principles in structural pattern discovery, interpretation and search. The formulation of a general Semistructured pattern information system through this study could provide fundamental supports to Semistructured pattern -intensive applications in multiple domains.

Keywords: semistructured pattern
Some Ramsey numbers involving bipartite graph

Hasmawati*, H. Assiyatun, E. T. Baskoro, A. N. M. Salman

Combinatorial Mathematics Research Group
Faculty of Mathematics and Natural Sciences
Institut Teknologi Bandung (ITB)
Jalan Ganesa 10 Bandung 40132, Indonesia
{hasmawati,hilda,ebaskoro,msalman}@math.itb.ac.id

Abstract. The Ramsey number for given graphs $G$ versus $H$, denoted by $R(G, H)$ is the smallest positive integer $n$ such that for any graph $F$ of order $n$, either $F$ contains $G$ as a subgraph or $\overline{F}$ contains $H$ as a subgraph.

We study the Ramsey numbers for multiple of copies complete bipartite graphs $R(kK_{1,p}, K_{2,m})$ for $k \geq 1$ and certain values of $p$ and $m$. Some results about the Ramsey numbers for complete bipartite graphs have been known. Burr in 1983 showed that $R(K_{2,3}, K_{2,3}) = 10$, Parsons in 1975 showed that $R(K_{1,7}, K_{2,3}) = 13$, and Lawrence in 1973 showed that $R(K_{1,15}, K_{2,2}) = 20$. Recently, Hasmawati et al. (2006) in two separated papers proved that $R(K_{1,3}, K_{2,2}) = 6$ and $R(K_{1,5}, K_{2,2}) = 8$.

In this paper, we show that $R(K_{1,7}, K_{2,2}) = 10$, and $R(kK_{1,p}, K_{2,2}) = k(p + 1) + 1$ for $k \geq 2$ and $p \geq 3$.

Keywords : complete bipartite graph, Ramsey number

---

*Permanent address: Jurusan Matematika FMIPA, Universitas Hasanuddin (UNHAS), Jln. Perintis Kemerdekaan KM.10 Makassar 90245, Indonesia
Super edge-magic total labeling of banana trees

M. Hussain¹, E. T. Baskoro², Slamin³

¹School of Mathematical Sciences, Government College University
Lahore, Pakistan
mhmaths@yahoo.com

²Combinatorial Mathematics Research Group
Faculty of Mathematics and Natural Science, Institut Teknologi Bandung
Jalan Ganesa 10 Bandung, Indonesia
ebaskoro@dns.math.itb.ac.id

³Mathematics Education Study Program
Universitas Jember, Jl. Kalimantan 37 Jember, Indonesia
slamin@unej.ac.id

Abstract. Let \( G_1, G_2, \ldots, G_n \) be a family of disjoint stars. The tree obtained by joining a new vertex \( a \) to one pendant vertex of each star is called a banana tree. In this paper we consider the super edge magic total labeling of banana trees that have not been covered by previous results.

Keywords : banana tree, super edge-magic total labeling
Critical set of caterpillar graph for secret sharing scheme

C. Imron¹, B. Setiyono¹ *, R. Simanjuntak², E. T. Baskoro²

¹Department of Mathematics
Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia
imron-its@matematika.its.ac.id, mazh_budi@yahoo.com
²Combinatorial Mathematics Research Group
Faculty of Mathematics and Natural Sciences
Institut Teknologi Bandung, Indonesia.
{rino, ebaskoro}@dns.math.itb.ac.id

Abstract. We investigate the critical set of edge-magic labeling on caterpillar graphs and application on secret sharing scheme. We construct a distribution scheme based on supervisinal secret sharing scheme. The schemes use the notion of critical sets to distribute the share and reconstruct the key.

Keywords : caterpillar graph, critical set, edge-magic total labeling, secret sharing scheme

* Supported by Hibah Pekerti Dikti
Metric dimensions of some corona graphs

H. Iswadi*, E. T. Baskoro, R. Simanjuntak, A. N. M. Salman

Combinatorial Mathematics Research Group
Faculty of Mathematics and Natural Science, Institut Teknologi Bandung
Jalan Ganesa 10 Bandung 40132, Indonesia
hazrul@students.itb.ac.id, {ebaskoro, rino, msalman}@math.itb.ac.id

Abstract. For an ordered set $W = \{w_1, w_2, \ldots, w_k\}$ of vertices and a vertex $v$ in a connected graph $G$, the representation of $v$ with respect to $W$ is the ordered $k$-tuple $r(v|W) = (d(v, w_1), d(v, w_2), \ldots, d(v, w_k))$ where $d(x, y)$ represents the distance between the vertices $x$ and $y$. The set $W$ is called a resolving set for $G$ if every two vertices of $G$ has distinct representations. A resolving set containing a minimum number of vertices is called a basis for $G$. The dimension of $G$, denoted by $\dim(G)$, is the number of vertices in a basis of $G$. In this paper, we determine the dimensions of corona graphs $G \odot K_m$, $G \odot C_m$, $G \odot P_m$, and $G \odot K_m$.

Keywords : basis, corona graph, dimension, resolving set

* Permanent address: Department of MIPA, Gedung TG lantai 6, Universitas Surabaya, Jalan Raya Kalirungkut Surabaya 60292, Indonesia
On the partition dimension of unicyclic graphs

I. Javaid
School of Mathematical Sciences
Government College University, Lahore, Pakistan
imranjavid45@gmail.com

Abstract. Let $G$ be a connected graph. For a vertex $v \in V(G)$ and an ordered $k$-partition $\Pi = \{S_1, S_2, \cdots, S_k\}$ of $V(G)$, the representation of $v$ with respect to $\Pi$ is the $k$-vector $r(v|\Pi) = (d(v,S_1), d(v,S_2), \cdots, d(v,S_k))$. The $k$-partition $\Pi$ is said to be resolving if the $k$-vectors $r(v|\Pi)$, $v \in V(G)$, are distinct. The minimum $k$ for which there is a resolving $k$-partition of $V(G)$ is called the partition dimension of $G$, denoted by $pd(G)$. A resolving $k$-partition $\Pi = \{S_1, S_2, \cdots, S_k\}$ of $V(G)$, is said to be connected if each subgraph $\langle S_i \rangle$ induced by $S_i$ $(1 \leq i \leq k)$ is connected in $G$. The minimum $k$ for which there is a connected resolving $k$-partition of $V(G)$ is called the connected partition dimension of $G$, denoted by $cpd(G)$. In this note, we give a formula for the partition dimension as well as the connected partition dimension of unicyclic graphs.

Keywords: connected partition dimension, resolving $k$-partition, unicyclic graph
The balance property of three-symbol cutting sequences

R. A. D. Kooswinarsinindyah

Combinatorial Mathematics Research Group
Faculty of Mathematics and Natural Sciences
Institut Teknologi Bandung (ITB)
Jalan Ganesa 10 Bandung 40132, Indonesia
indah@math.itb.ac.id

Abstract. Extensions of Sturmian words, both in the direction of cutting sequences of more than two symbols and that of two-symbol cutting sequences in the dimension higher than two, are studied extensively by many authors. Here, we study the balance property of cutting sequences of three symbols from combinatorial point of view. Especially, we investigate our claim that the balance value for all symbols are the same, which is 2.

Keywords: balance property, cutting sequence
A closure concept in $K_{1,r}$-free graphs

R. Kužel

Department of Mathematics and Institute for Theoretical Computer Science
University of West Bohemia
Univerzitní 8, 306 14 Plzeň, Czech Republic
rkuzel@kma.zcu.cz

Abstract. A graph $G$ is called $K_{1,r}$-free if $G$ has no $K_{1,r}$ as an induced subgraph. A hyper- graph $H$ is called $k$-uniform if all its edges have cardinality $k$. Clearly a 2-uniform hypergraph is a graph in an usual sense. A line graph of a hypergraph $H = (V, E)$ is a graph $L(H)$ with vertex set $E$ and with two vertices adjacent in $L(H)$ iff the corresponding edges of $H$ have a nonempty intersection. Let $v$ be a vertex of a graph $G$, we say that $v$ is locally connected if the neighborhood of $v$ in $G$ induces a connected subgraph in $G$. If a locally connected vertex $v$ induces a non complete subgraph we call the vertex $v$ eligible. Let $G$ be a graph and $v \in V(G)$ be its eligible vertex. A graph $G_v$ obtained from a graph $G$ by adding all missing edges into a neighborhood of $v$ is called a local completion of $G$ at vertex $v$. A closure of a graph $G$ is a graph $Cl(G)$ obtained by repeating of an operation of a local completion at eligible vertices until no other eligible vertex remains. A $k$-walk in a graph $G$ is a closed walk visiting each vertex at most $k$ times, where $k \geq 1$ is an integer. Note, that in our notations a $k$-walk in a graph $G$ need not to span all vertices of $G$. We can then view a cycle in a graph as an 1-walk. A $k$-circumference of a graph $G$ is a cardinality of a vertex set of a $k$-walk $W \subset G$ spanning maximum possible number of vertices of $G$. We denote by $ck(G)$ the $k$-circumference of a graph $G$. We show the following generalization of a well-known closure concept in $K_{1,3}$-free graphs. Let $r \geq 3$ be an integer and let $G$ be a $K_{1,r}$-free graph. Then (i) $c_{r-1}(G) = c_{r-1}(Cl(G))$, (ii) $Cl(G)$ is unique, (iii) there is an $(r-1)$-uniform hypergraph $H$ such that $Cl(G) = L(H)$.

Keywords : closure, $K_{1,r}$-free graph

* Supported by project 1M0545 and Research Plan MSM 4977751301 of the Czech Ministry of Education.
On describing the incidence matrix of a finite projective plane via orthogonal latin squares and via a digraph complete set of latin squares

C. Levesque
Department of Mathematics and Statistics
University of Laval, Canada
Claude.Levesque@mat.ulaval.ca

Abstract. A fast direct method of obtaining the incidence matrix of a finite projective plane of order \( n \) via \( n - 1 \) mutually orthogonal \( n \times n \) latin squares is described. Conversely, \( n - 1 \) mutually orthogonal \( n \times n \) latin squares are directly exhibited from the incidence matrix of a projective plane of order \( n \). A projective plane of order \( n \) can also be described via a digraph complete set of latin squares and a new procedure for doing it will also be described.

Keywords : digraph complete set, finite projective plane, orthogonal latin square


Edge span of $L(p, q)$-labelings on wheel graphs

Y. L. Lai, S. J. Wu

National Chiayi University Chaiyi, Taiwan, R.O.C.
yllai@mail.ncyu.edu.tw, shinju.wu@msa.hinet.net

Abstract. The radio channel assignment problem can be modeled by a graph and the same problem is known as graph $L(p, q)$-labeling problem. A $k - L(p, q)$-labeling of a graph $G$ for integers $p > q$ is a function $f$ which is defined from the vertex set of $G$ to the nonnegative integers from 0 to $k$ such that any pair of adjacent vertices $x$ and $y$ in $G$ has labels differ at least $p$ and the labels are differ at least $q$ when the two vertices $x$ and $y$ are at distance 2 in $G$. The $L(p, q)$ edge span of $f$, denoted as $\beta_{p,q}(G, f)$ is the maximum difference between labels of adjacent vertices. The $L(p, q)$ edge span of $G$, denoted as $\beta_{p,q}(G)$, is the minimum value of $\beta_{p,q}(G, f)$ among all $L(p, q)$-labeling of $G$. In this paper, we consider the edge spans of $L(p, q)$-labeling problem of wheel graph.

Keywords: channel assignment, edge span, $L(p, q)$-labeling, wheel graph
On the extremal graph of maximum size with given order and girth

Y. Lin\textsuperscript{2}, M. Miller\textsuperscript{2}

School of Electrical Engineering and Computer Science
The University of Newcastle, NSW2308, Australia
yuqing.lin@newcastle.edu.au
\textsuperscript{2}School of Information Technology and Mathematical Sciences
University of Ballarat, VIC 3353, Australia
m.miller@ballarat.edu.au

Abstract. $EX(n, \{c_3, c_4, \ldots, c_{g-1}\})$ is defined as graphs of maximum size with given order $n$ and girth $g$. Constructing such graphs is a challenging task and closely related to the problems of constructing many other extremal graphs. In this talk, we give a brief overview of the current known results on the properties of $EX(n, \{c_3, c_4, \ldots, c_{g-1}\})$ and present several open problems.

Keywords : $EX(n, \{c_3, c_4, \ldots, c_{g-1}\})$, $(k; g) -$ cage, cage
About the number of semi-latin squares orthogonal to a particular latin square

S. Malik
School of Mathematical Sciences, Government College University
68-B New Muslim Town Lahore, Pakistan
shabnam.malik@gmail.com

Abstract. A Latin square is an $n \times n$ square matrix whose entries consist of $n$ symbols such that each symbol appears exactly once in each row and each column. We define a semi-Latin square as any $n \times n$ square matrix whose entries consist of $n$ symbols such that each symbol appears exactly once in each row. In the article we propose an upper and lower bound for the number of Latin squares of order $n$ and those of semi-Latin squares of order $n$, which are orthogonal to a particular Latin square of order $n$. It is shown that the number of Latin squares of order $n$ is equal to the number of semi-Latin squares of order $n$, orthogonal to a particular Latin square of order $n$.

Keywords: latin square, semi-latin squares orthogonal
Abstract. A simple graph $G = (V, E)$ admits an $H$-covering if every edge in $E$ belongs to a subgraph of $G$ that is isomorphic to $H$. In this case we say that $G$ is $H$-magic if there is a total labeling $f : V \cup E \to \{1, 2, \ldots, |V| + |E|\}$ such that for each subgraph $H' = (V', E')$ of $G$ that is isomorphic to $H$, $\sum_{v \in V'} f(v) + \sum_{c \in E'} f(c)$ is constant. When $f(V) = \{1, 2, \ldots, |V|\}$, we say that $G$ is $H$-supermagic. In this paper, we study $P_h$-supermagic for graph $S_n^{(m_1, m_2, \ldots, m_n)}$ with $m_1 \leq m_2 \leq \cdots \leq m_n$. The graph $S_n^{(m_1, m_2, \ldots, m_n)}$ has a vertex set $V(S_n^{(m_1, m_2, \ldots, m_n)}) = \{c\} \cup \{x_i^j | 1 \leq i \leq n, 1 \leq j \leq m_i\}$ and an edge set $E(S_n^{(m_1, m_2, \ldots, m_n)}) = \{cx_i^1 | 1 \leq i \leq n\} \cup \{x_i^j x_i^{j+1} | 1 \leq i \leq n, 1 \leq j \leq m_i - 1\}$. We prove that $S_n^{(m_1, m_2, \ldots, m_n)}$ with $n \geq 3$ is $P_h$-supermagic for $m_n + 1 \leq h \leq m_n + m(n-1) + 1$.

Keywords: H-supermagic total labeling
On the structure of path-like trees

F. A. Muntaner-Batle¹, M. Rius-Font²

¹Universitat Internacional de Catalunya
Immaculada, 22 08017 Barcelona, Spain
fambles@yahoo.es
²Departament de Matemàtica Aplicada IV.
Universitat Politècnica de Catalunya
Jordi Girona Salgado, 1 08034 Barcelona, Spain

Abstract. Path-like trees are defined as follows. We embed the path \( P_n \) as a subgraph of the 2-dimensional grid, that is to say the graph \( P_k \times P_l \). Given such an embedding, we consider the ordered set of subpaths \( L_1, L_2, \ldots, L_m \) which are maximal straight segments in the embedding, and such that the end of \( L_i \) is the beginning of \( L_{i+1} \). Suppose that \( L_i \cong P_2 \) for some \( i \) and that some vertex \( u \) of \( L_{i-1} \) is at distance 1 in the grid to a vertex \( v \) of \( L_{i+1} \). An elementary transformation of the path consists in replacing the edge of \( L_i \) by a new edge \( uv \). We say that a tree \( T \) of order \( n \) is a path-like tree, when it can be obtained from some embedding of \( P_n \) in the grid, by a sequence of elementary transformations. We study the structure of path-like trees. In order to do this, we introduce two different sets of graphs that we call expandable trees and generalized path-like trees.

Keywords: path-like tree
On super edge-magic deficiency of graphs

A. A. G. Ngurah*, E. T. Baskoro, R. Simanjuntak, S. Uttunggadewa

Combinatorial Mathematics Research Group
Faculty of Mathematics and Natural Science, Institut Teknologi Bandung
Jalan Ganesa 10 Bandung, Indonesia
{s304agung, ebaskoro, rino, s_uttunggadewa}@dns.math.itb.ac.id

Abstract. A graph $G$ is called edge-magic if there exists a bijection $f : V(G) \cup E(G) \to \{1, 2, 3, \ldots, |V(G) \cup E(G)|\}$ such that $f(x) + f(xy) + f(y)$ is a constant for every edge $xy \in E(G)$. A graph $G$ is said to be super edge-magic if $f(V(G)) = \{1, 2, 3, \ldots, |V(G)|\}$. Furthermore, the edge-magic deficiency of a graph $G$, $\mu(G)$, is defined as the minimum nonnegative integer $n$ such that $G \cup nK_1$ is edge-magic. Similarly, the super edge-magic deficiency of a graph $G$, $\mu_s(G)$, is either the minimum nonnegative integer $n$ such that $G \cup nK_1$ is super edge-magic or $+\infty$ if there exists no such integer $n$.

In this paper, we present the super edge-magic deficiencies of some classes of graphs.

Keywords : super edge-magic labeling, super edge-magic deficiency

* Permanent address: Department of Civil Engineering, Universitas Merdeka Malang, Jalan Taman Agung 1 Malang, Indonesia
Diagram-based verification of parameterized systems

C. E. Nugraheni

Department of Computer Science
Faculty of Mathematics and Natural Sciences
Universitas Katolik Parahyangan
Jalan Ciumbuleuit 94 Bandung, Indonesia
cheni@home.unpar.ac.id

Abstract. A parameterized system consists of several similar processes whose number is determined by an input parameter. A challenging problem is to provide methods for the uniform verification of such systems, i.e. to show by a single proof that a system is correct for any value of the parameter.

This paper presents a method for verifying universal properties of parameterized systems using Parameterized Predicate Diagrams. Basically, parameterized Predicate Diagrams are graphs whose vertices are labelled with first-order formulas, representing sets of system states, and whose edges represent possible system transitions. These diagrams are used to represent the abstractions of parameterized systems described by specifications written in temporal logic.

This presented method integrates deductive verification and algorithmic techniques. Non-temporal proof obligations establish the correspondence between the original specification and the diagram, whereas model checking is used to verify properties over finite-state abstractions.

Keywords: diagram-based verification, parameterized predicate diagram, parameterized system
The total edge-irregular strengths of the corona product of graphs

Nurdin*, A. N. M. Salman, E. T. Baskoro

Combinatorial Mathematics Research Group
Faculty of Mathematics and Natural Sciences
Institut Teknologi Bandung (ITB)
Jl. Ganesa 10 Bandung 40132
nurdin1701@students.itb.ac.id
{msalman,ebaskoro}@math.itb.ac.id

Abstract. For a simple graph $G = (V(G), E(G))$ with the vertex set $V(G)$ and the edge set $E(G)$, a labeling $\lambda : V(G) \cup E(G) \rightarrow \{1, 2, \ldots, k\}$ is called an edge-irregular total $k$-labeling of $G$ if for any two different edges $e = e_1e_2$ and $f = f_1f_2$ in $E(G)$ we have $wt(e) \neq wt(f)$ where $wt(e) = \lambda(e_1) + \lambda(e) + \lambda(e_2)$. The total edge-irregular strength, denoted by $tes(G)$, is the smallest positive integer $k$ for which $G$ has an edge-irregular total $k$-labeling. The corona product of a graph $G$ with a graph $H$, denoted by $G \odot H$, is defined as a graph obtained by taking one copy of a $p$-vertex graph $G$ and $p$ copies $H_1$, $H_2$, ..., $H_p$ of $H$, and then joining the $i$-th vertex of $G$ to every vertex in $H_i$. In this paper, we determine the total edge-irregular strength of graphs produced by the corona product of paths with paths, cycles, stars, gears, friendships, or wheels.

Keywords : corona product, total edge-irregular strength

* Permanent Address : Mathematics Department, Faculty of Mathematics and Natural Sciences, Universitas Hasanuddin (UNHAS), Jl. Perintis Kemerdekaan Km.10 Tamalanrea, Makassar, Indonesia
Characterization of graphs of maximum degree 3, with small diameters and defect at most 4*

G. Pineda-Villavicencio\textsuperscript{1,2}, M. Miller\textsuperscript{1,3}

\textsuperscript{1}School of Information Technology and Mathematical Sciences  
University of Ballarat, Australia  
\textsuperscript{2}Department of Computer Science  
University of Oriente, Santiago de Cuba, Cuba  
\textsuperscript{3}Department of Mathematics  
University of West Bohemia, Pilsen, Czech Republic  
\{g.pinedavillavicencio, m.miller\}@ballarat.edu.au

Abstract. The degree/diameter problem consists of determining the largest possible number of vertices \(n_{\Delta,D}\) in a graph of given maximum degree \(\Delta\) and diameter \(D\). It is well known that an upper bound for \(n_{\Delta,D}\) is given by the so called Moore bound \(M_{\Delta,D}\). A graph whose order attains this bound is called a Moore graph. Moore graphs exist only for certain special values of maximum degree and diameter. Therefore, we are interested in studying the existence of large graphs of given maximum degree \(\Delta\), diameter \(D\) and order \(M_{\Delta,D} - \delta\), that is, \((\Delta, D, \delta)\)-graphs, for \(\delta > 0\). The parameter \(\delta\) is called the defect. It well known that there is a unique cubic Moore graph, the Petersen graph. Since a cubic graph must have an even number of vertices, the next interesting case is when the order is \(M_{3,D} - 2\). This case was completely characterized by Jorgensen. Jorgensen proved that for \(D \geq 4\) there are no \((3, D, 2)\)-graphs and he showed the uniqueness of the two known \((3, 2, 2)\)-graphs and of the known \((3, 3, 2)\)-graph. In this paper we study graphs of maximum degree 3 and defect 4. Note that the case of \((3, D, 4)\)-graphs is particularly interesting because \((\Delta, D, \delta)\)-graphs with \(\delta > \Delta\) have not been considered before, for any values of \(D\) and \(\Delta\). In this paper we present all the \((3, D, 4)\)-graphs, for \(D = 2, 3\). The nonexistence of any \((3, 4, 4)\)-graph was proven by Jorgensen in 1993. Finally, for \(D > 4\), we conjecture that there are no \((3, D, 4)\)-graphs.

Keywords: cubic graph, degree/diameter problem, Moore bound, Moore graph

* Research supported in part by the Australian Research Council grant ARC DP0450294.
Hamiltonian properties of generalized Halin graphs

A. M. Qureshi, S. Malik

School of Mathematical Sciences, GC University
68-B, New Muslim Town, Lahore, Pakistan
{srarhad, shabnam.malik}@gmail.com

Abstract. A Halin graph is a graph $G = T \cup C$, where $T$ is a tree with no vertex of degree two, and $C$ is a cycle connecting the end vertices of $T$ in the cyclic order determined by a plane embedding of $T$. In this paper, we define classes of generalized Halin graph, called $k$-Halin graphs, and investigate their Hamiltonian properties.

Keywords: Hamiltonian, Hamiltonian connected, $k$-Halin graph, traceable
Network manager for key management on secure fixed-line telephone

I. Rahayu¹, S. Cahyono², D. Priyasta³, A. Sarotama³, F. R. Triputra³, Sobar⁴, M. M. Sarinanto³

¹Crypto Assessment Center, LSN, Jakarta, Indonesia
²National Crypto Institute, Bogor, Indonesia
³ICT Center, BPPT, Jakarta, Indonesia
⁴Bakti Jaya Transecurindo, Jakarta, Indonesia

ints06@yahoo.com
setyo18@yahoo.com
{darma, afrias, fadjar, nanto}@inn.bppt.go.id

Abstract. In the information age, information security becomes a very important factor. Security feature in communication, particularly on fixed-line telephone device that still become backbone of communication media in the government or private institutions, are widely open. Currently, we are developing a secure communication device using smart card. Smart Card is used as media storage and distributes the Cryptographic keys to each secure fixed-line telephone module. As a part of whole design of security system, in order to create a secure communication network, then distribution of Cryptographic keys to each working unit in the network should be secure and fit to the provision behave. Development of a network manager application can solve this problem. This paper will discuss about design of network manager application to manage Cryptographic keys distribution on a fixed-line telephone communication network. Some main function which designed i.e. manage and define the communication network structure, generate Cryptographic keys according to user/group and load to smart card and manage communication device on network. Optimization of network design and key management which consist of communication key and emergency key will describe in this paper.

Keywords: cryptography, key management, network manager, smart card
Vertex-magic total labeling of the union of suns

M. T. Rahim¹, Slamin²

¹School of Mathematical Sciences
Government College University, Pakistan
tariqsms@gmail.com
²Mathematics Education Study Program
Universitas Jember, Indonesia
slamin@unej.ac.id

Abstract. Let $G$ be a graph with vertex set $V = V(G)$ and edge set $E = E(G)$ and let $e = |E(G)|$ and $v = |V(G)|$. A one-to-one map $\lambda$ from $V \cup E$ onto the integers $\{1, 2, ..., v+e\}$ is called vertex magic total labeling if there is a constant $k$ so that for every vertex $x$,

$$\lambda(x) + \sum \lambda(xy) = k$$

where the sum is over all vertices $y$ adjacent to $x$. Let us call the sum of labels at vertex $x$ the weight $w_\lambda(x)$ of the vertex under labeling $\lambda$; we require $w_\lambda(x) = k$ for all $x$. The constant $k$ is called the magic constant for $\lambda$.

A sun $S_n$ is a cycle on $n$ vertices $C_n$, for $n \geq 3$, with an edge terminating in a vertex of degree 1 attached to each vertex.

In this paper, we present the vertex magic total labeling of the union of suns, including the union of $m$ non-isomorphic suns for any positive integer $m \geq 3$, proving the conjecture given by Slamin et al.

Keywords: vertex magic total labeling, union of sun
A note on chromaticity of certain bipartite graphs

H. Roslan ¹, Y. H. Peng²

¹School of Mathematical Sciences
Universiti Sains Malaysia, 11800 Penang, Malaysia
hroslan@cs.usm.my

²Department of Mathematics, and Institute for Mathematical Research
University Putra Malaysia, 43400UPM Serdang, Malaysia
yhpeng@fsas.upm.edu.my

Abstract. All graphs considered here are simple graphs. For a graph G, let $P(G, \lambda)$ be the chromatic polynomial of $G$. Two graphs $G$ and $H$ are said to be chromatically equivalent (or simply $\chi$–equivalent), symbolically $G \sim H$, if $P(G, \lambda) = P(H, \lambda)$. The equivalence class determined by $G$ under $\sim$ is denoted by $[G]$. A graph $G$ is chromatically unique (or simply $\chi$–unique) if $H \cong G$ whenever $H \sim G$, i.e, $[G] = \{G\}$ up to isomorphism. In this paper, we shall discuss on the chromaticity of bipartite graphs with five edges deleted.

Keywords : bipartite graph, chromaticity
On vertex irregular total labeling of Petersen graph

M. Roswita, D. Indriati, T. A. Kusmayadi

Faculty of Mathematics and natural Sciences, Sebelas Maret University
Jl. Ir Sutami 36A Kentingan, Surakarta 57126
mrosw@mipa.uns.ac.id

Abstract. For a graph $G = (V, E)$, a labeling $\partial : V \cup E \rightarrow \{1, 2, 3, \ldots, k\}$ is called a vertex irregular total $k$-labeling of $G$ if for every two distinct $x$ and $y$ of $G$, there is $\omega_t(x) \neq \omega_t(y)$ where $\omega_t(x) = \partial(x) + \sum_{xy \in E} \partial(xy)$.

The minimum $k$ for which there is a a vertex irregular total $k$-labeling of $G$ is called the total vertex irregularity strength of $G$, $tvs(G)$.

In this paper, we investigate the total vertex irregularity strength of Petersen graph. We prove that $tvs(G) = \lceil \frac{n+3}{4} \rceil$.

Keywords : Petersen graph, vertex irregularity strength
The computational complexity of $\lambda$-backbone coloring of graphs with $n$-complete backbones

A. N. M. Salman
Combinatorial Mathematics Research Group
Faculty of Mathematics and Natural Sciences
Institut Teknologi Bandung
Jl. Ganesa 10 Bandung, Indonesia
msalman@math.itb.ac.id

Abstract. Given an integer $\lambda \geq 2$, a graph $G = (V, E)$ and a spanning subgraph $H$ of $G$ (the backbone of $G$), a $\lambda$-backbone coloring of $(G, H)$ is a proper vertex coloring $V \rightarrow \{1, 2, \ldots\}$ of $G$, in which the colors assigned to adjacent vertices in $H$ differ by at least $\lambda$. We study the computational complexity of the problem “Given a graph $G$ with a backbone $H$, and an integer $\ell$, is there a $\lambda$-backbone coloring of $(G, H)$ with at most $\ell$ colors?” Of course, this general problem is NP-complete. In this paper, we consider this problem for collections of pairwise disjoint complete graphs with order $n$. We show that the complexity jumps from polynomially solvable to NP-complete between $\ell = (n - 1)\lambda$ and $\ell = (n - 1)\lambda + 1$.

Keywords: $\lambda$-backbone coloring, $\lambda$-backbone coloring number, computational complexity, $n$-complete backbone
Isoperimetric orderings in cartesian powers of graphs

O. Serra

Dept. of Applied Mathematics IV
Polytechnic University of Catalonia, Barcelona
oserra@ma4.upc.edu

Abstract. Let $G = (V, E)$ be a graph. The ball $B(A)$ of a set $A \subset V$ is the set of vertices at distance at most one from vertices in $A$. The vertex isoperimetric problem on $G$ consists in finding, for a given $m$, a subset $A \subseteq V$ with cardinality $m$ which minimizes the size of the ball $B(A)$. Such a set is said to be optimal. An ordering of the vertices of a graph $G = (V, E)$ is isoperimetric if the initial segments of the ordering are optimal sets. It is a Hales ordering if, in addition, the ball of an initial segment is also an optimal set. A graph which admits a Hales ordering is a Hales graph. There are few known classes of Hales graphs, the hypercubes being a well-known example with significant applications.

We will describe a general class of orderings with the following property: if $G$, $H$ and its cartesian product $G \times H$ admit an ordering in the class which is Hales, then each cartesian product $G^n \times H^m$, $n, m \geq 1$ is also a Hales graph. This result provides several new classes of Hales graphs. An exhaustive search shows that all Hales graphs with order up to 18 belong to known families of Hales graphs and their cartesian products. This is joint work with Sergei Bezrukov and Miquel Rius.

Keywords: Hales graph
Some open problems on edge antimagic total labeling

D. R. Silaban and K. A. Sugeng

Department of Mathematics University of Indonesia
Depok 16424, Indonesia
{denny-rs,kiki}@ui.edu

Abstract. Let $G = (V, E)$ be a simple and undirected graph with $v$ vertices and $e$ edges. An $(a, d)$-edge-antimagic total labeling is a bijection $\alpha$ from $V(G) \cup E(G)$ to the set of consecutive integers $\{1, 2, \ldots, v+e\}$ such that the weight of edges form arithmetical progression with initial term $a$ and common difference $d$. A super $(a, d)$-edge antimagic total labeling is an edge antimagic total labeling $\alpha$ which $\alpha(V(G)) = \{1, \ldots, v\}$. In this paper we solve some open problems on edge antimagic total labeling that proposed on several published papers, such as on paths, cycles and some families of graphs that constructed from cycles.

Keywords : edge antimagic total labeling, super edge antimagic total labeling
On 3-defective colourings of complementary graphs

M. Simanihuruk¹, N. Achuthan², N. R. Achuthan²

¹Mathematics Department Bengkulu University, Indonesia
mudinsimanihuruk@yahoo.com.au
²School of Mathematics and Statistics
Curtin University of Technology
GPO BOX U1987, Perth, Australia

Abstract. A graph $G$ is $(m, k)$-colourable if its vertices can be coloured with $m$ colours such that the maximum degree of the subgraph induced on vertices receiving the same colours is at most $k$. The $k$-defective chromatic number $\chi_k(G)$ of $G$ is the least positive integer $m$ for which $G$ is $(m, k)$-colourable. Maddox conjecture that if $G$ is a graph of order $p$ then $\chi_k(G) + \chi_k(\overline{G}) \leq 2 + \lceil \frac{p-1}{k+1} \rceil$. In this paper we prove Maddox conjecture for $k = 3$ and $G$ is a $P_4$-free graph of order $p$.

Keywords: chromatic, colouring, defective, and $P_4$-free.
New constructions of $A$-magic graphs using labeling matrices

K. A. Sugeng$^1$, M. Miller$^2$

$^1$Department of Mathematics, University of Indonesia
Depok 16424, Indonesia
kikiariyanti@yahoo.com

$^2$School of Information Technology and Mathematical Sciences
University of Ballarat, Vic 3353, Australia
m.miller@ballarat.edu.au

Abstract. A simple graph $G(V, E)$ is called $A$-magic if there is a labeling $f : E \rightarrow A^*$, where $A$ is an Abelian group and $A^* = A - \{0\}$ so that the induced vertex labeling $f^* : V \rightarrow A$ defined as $f^*(v) = \Sigma_{u \in N(v)} f(uv) = k$, for every $v \in V$, $k$ is a constant in $A$. The number $k$ is called the magic constant of $G$. Using this definition, edge labels can be the same. Let $f : V \rightarrow A - \{0\}$ be an $A$-magic labeling of $G$, with $A$ an arbitrary Abelian group. Let $\{v_1, ..., v_n\}$ be the set of the vertices of $G$. A labeling matrix of $f$, denoted by $A_f(G) = (a_{ij})$, is a matrix in which each row /column represents the vertices of $G$ and the entry $ij$ is a label of the edge $v_iv_j$. In this paper we show a construction of new classes of $A$-magic graphs from the known $A$-magic graphs using a labeling matrix by using the special property of the labeling matrix.

Keywords: $A$-magic labeling, labeling matrix
Optimum sum labeling of finite union of sum graphs

K. A. Sugeng, R. Rusin, H. Burhan

Department of Mathematics
Faculty of Mathematics and Natural Science
University of Indonesia
Depok 16424, Indonesia
{kiki, rahmirus, hnburhan}@ui.edu

Abstract. Let $G = (V, E)$ be a simple, finite and undirected graphs. A sum labeling is a one to one mapping $L$ from a set of vertices of $G$ to a finite set of positive integers $S$ such that if $u$ and $v$ are vertices of $G$ then $uv$ is an edge in $G$ if and only if there is a vertex $w$ in $G$ and $L(w) = L(u) + L(v)$. A graph $G$ that has a sum labeling is called sum graph. The minimal isolated vertex that needed to make $G$ a sum labeling is called sum number of $G$, notated as $\sigma(G)$. The sum number of a sum graph $G$ always greater or equal to $\Delta(G)$, a minimum degree of $G$. An optimum sum graph is a sum graph that has $\sigma(G) = \Delta(G)$. In this talk, we discuss sum numbers of finite union of some family of optimum sum graphs, such as cycles, cycles with pendants and tails, and friendship graphs.

Keywords : cycle, complete graph, friendship graph, optimal sum labeling
A survey on Ramsey numbers of cycles with respect to wheels or generalized wheels

Surahmat*

Department of Mathematics Education
Faculty of Training and Education Sciences
Universitas Islam Malang
Jalan MT Haryono 193, Malang 65144, Indonesia
caksurahmat@yahoo.com

Abstract. For given graphs $G$ and $H$, the Ramsey number $R(G, H)$ is the smallest positive integer $N$ such that for every graph $F$ of order $N$ the following holds: either $F$ contains $G$ as a subgraph or the complement of $F$ contains $H$ as a subgraph. In this paper, we will list some known results of Ramsey numbers of cycles respect to wheels or generalized wheels and we also list some open problems and conjectures.

Keywords: cycle, Ramsey number, wheel

* Research support by TWAS (Ref.:06−018 RG/MATH/AS), Trieste, Italy.
The mesh-connected model in parallel computing for shortest path

M. Susmikanti
Center for Development of Nuclear Informatics - BATAN
Kawasan PUSPIPTEK Serpong, Tangerang, Indonesia
mike@batan.go.id

Abstract. For the solutions of the shortest path in graph problem with the big node, we propose an improved the parallel computing. In the few basic features for control mechanism, the functions of its individual processors, its interconnection network, and the ways in which it can route data through its network determine a mesh-connected, like any parallel computer. Topologically, a two-dimensional array or mesh is collection of $m \times n$ processors interconnected in the same manner as the vertices of a two-dimensional mesh. Some vertex in graph problem is analog with vertex processor. This vertex executes the same program on its own local data, but under the control of the single external control processors, an arrangement that is called SIMD computers. To solve the shortest path problem, we will calculate the connectivity matrix and the connected component. The calculated connectivity matrix and the connected component in parallel algorithm are using the mesh matrix multiplication. The efficiency of this model is compared on a parallel distributed memory system versus a hypercube-connected.

Keywords: graph, mesh-connected, parallel computing, shortest path
Primitive graphs with exponent 4

S. Suwilo

Department of Mathematics University of Sumatera Utara
Medan 20155, Indonesia
saib@usu.ac.id

Abstract. A connected graph $G$ is primitive provided it has a cycle of odd length. The exponent of a primitive graph is the smallest positive integer $k$ such that for each pair of vertices in $G$ there is a walk of length $k$ connecting them. For primitive graphs on $n$ vertices, researchers have characterized primitive graphs with exponent larger than $n$, $n - 1$, and 2. This paper characterizes primitive graphs with exponent 4.

Keywords : exponent, primitive graph
Abstract. General upper bounds for the largest possible order of digraphs of given maximum out-degree $d$ and diameter $k$ are called Moore bounds. A digraph whose order reaches Moore bound is called a Moore digraph. It is well known that Moore digraphs exist only for $d = 1$ or $k = 1$. Consequently, we are interested in studying the existence of digraphs that are somehow ‘close’ to Moore digraphs. One possible meaning of ‘closeness’ is presented in this talk. We call such digraphs Near-moore digraphs and they are obtained by relaxing one of the three parameters, namely, the order $n$, or the out-degree $d$, or the diameter $k$, in order to get ‘close’ to Moore digraphs.

It is well known that simulated annealing and genetic algorithm are effective techniques for identifying global optimization solutions.

This paper describes our attempt to build a Hybrid Simulated Annealing and Genetic Algorithm (HSAGA) that can be used to construct near-Moore digraphs by relaxing the maximum out-degrees $d$. We present our new results obtained by HSAGA, as well as several related open problems.

Keywords: degree/diameter problem, diameter, digraph, genetic algorithm, HSAGA, Moore bound, out-degree, simulated annealing

* Research partially supported in part by the Australian Research Council grant ARC DP0450294.
Tree-path size multipartite Ramsey numbers

S. Uttunggadewa, Syafrizal Sy*, H. Assiyatun, E. T. Baskoro

Combinatorial Mathematics Research Group
Faculty of Mathematics and Natural Science Institut Teknologi Bandung
Jalan Ganesa 10 Bandung, Indonesia
{s_uhttunggadewa, syafrizalsy, hilda, ebaskoro}@dns.math.itb.ac.id

Abstract. Let $j \geq 2$ be a natural number. For graphs $G$ and $H$, the size multipartite Ramsey number $m_j(G, H)$ is the smallest natural number $t$ such that any red-blue coloring on the edges of $K_{j \times t}$, necessarily forces a red $G$ or a blue $H$ as a subgraph. In this note, we determine the exact values of $m_2(T_m, P_n)$ for all integers $m, n \geq 2$, and $m_j(T_m, P_n)$ for some integers $j \geq 3$ and $m, n \geq 2$, where $T_m$ denotes a tree on $n$ vertices and $P_n$ denotes a path on $n$ vertices.

Keywords: path, size multipartite Ramsey number, tree

* Permanent address: Department of Mathematics, Universitas Andalas, Padang - Indonesia 25163
Total vertex irregular labelings of wheels, fans, suns and friendship graphs

K. Wijaya¹, Slamin²

¹Department of Mathematics, Universitas Jember, Jalan Kalimantan Jember, Indonesia
kristiana wijaya@yahoo.com
²Mathematics Education Study Program, Universitas Jember, Jalan Kalimantan Jember, Indonesia
slamin@unej.ac.id

Abstract. A total vertex irregular labeling of a graph $G$ with $v$ vertices and $e$ edges is an assignment of integer labels to both vertices and edges so that the weights calculated at vertices are distinct. The total vertex irregularity strength of $G$, denoted by $\text{tvs}(G)$, is the minimum value of the largest label over all such irregular assignments. In this paper, we consider the total vertex irregular labelings of wheels, fans, suns and friendship graphs. We show that the total vertex irregularity strength of wheel $W_n$, $\text{tvs}(W_n) = \lceil \frac{n+3}{4} \rceil$ for $n \geq 3$, fan $F_n$, $\text{tvs}(F_n) = \lceil \frac{n+2}{4} \rceil$ for $n \geq 3$, sun $S_n$, $\text{tvs}(S_n) = \lceil \frac{n+1}{2} \rceil$ for $n \geq 3$, and friendship $f_n$, $\text{tvs}(f_n) = \lceil \frac{2n+2}{3} \rceil$ for all $n$.

Keywords: total vertex irregular labeling, total vertex irregularity strength
Efficient traitor-tracing algorithms based on list decoding

X. W. Wu\textsuperscript{1}, M. Kuijper\textsuperscript{2}, P. Udaya\textsuperscript{2}

\textsuperscript{1} School of Information Technology and Mathematical Sciences
University of Ballarat, VIC 3353, Australia
x.wu@ballarat.edu.au.

\textsuperscript{2}University of Melbourne, VIC 3010, Australia
m.kuijper@ee.mu.oz.au, udaya@cs.mu.oz.au.

Abstract. We consider cryptographic schemes that trace the source of leaks when copyrighted data is made available to unauthorized parities. The traitors are the legitimate users who collude to create and distribute pirate copies of the copyrighted data. Using traitor-tracing schemes, codes may be embedded in the content or may be associated with the keys used to recover the content. By analyzing the codes in the pirate copies or associated with the keys, one or more of the traitors can be identified. The idea of traitor tracing was introduced by Chor, Fiat, and Naor in 1994. In the past decade traitor-tracing schemes have been extensively studied. List decoding is a novel algebraic-decoding method, which significantly improved the capability of traditional decoding methods. The list-decoding algorithm for Reed-Solomon codes was found in 1997 and was generalized to algebraic-geometric codes and Reed-Muller codes several years later. In 2003, using list-decoding algorithms Silverberg, Staddon and Walker designed an efficient traitor-tracing algorithm. Their algorithm remarkably reduced the time complexity of previous traitor-tracing algorithms. Actually, the algorithm of Silverberg, Staddon and Walker runs in time polynomial in $\log N$, that is, $O(\log N)$, where $N$ is the number of legitimate users; while previous traitor-tracing algorithms have time complexity $O(N)$.

In this paper, we further improve the efficiency of traitor-tracing algorithms, by lowering the complexity of list-decoding algorithms. The list decoding consists of two main steps. The first step is an interpolation procedure, which can be implemented by solving a system of homogeneous linear equations and has low complexity. The second step is a procedure of finding a set of roots of a multivariate polynomial, which is the dominate step in terms of time complexity of the list decoding (and hence the traitor tracing). Our idea is to lower the complexity of the traitor tracing by lowering the complexity of the second step. We propose a fast root-finding algorithm which finds all the roots of a multivariate polynomial that are required by the list decoding. Using our algorithm, the traitor-tracing scheme can be implemented with a much lower complexity, namely $O(\log \log N)$.

\textbf{Keywords : cryptographic scheme, list decoding}