The Euler, Hall, and Kirkman Medals
Call for Nominations for 2005

Euler Medals are recognition for distinguished lifetime career contributions to combinatorial research by Fellows of the ICA who are still active in research. At most two medals per year may be awarded. A nominations should be made by two Fellows of the ICA, should include a complete curriculum vitae, and should include a letter detailing the significance of the nominee's achievements.

Hall Medals recognize extensive quality research by ICA members in mid-career. At most 3 Hall Medals per year may be given. Recipients must be ICA Fellows who have not reached age 41 by the end of 2005. Nominations should be made by two Fellows of the ICA, and should be accompanied by a curriculum vitae and a letter explaining the importance of the nominee's research.

Kirkman Medals recognize excellent work by ICA members in their early research careers. At most 3 Kirkman Medals per year may be given. Recipients must have received their doctorates during the four-year period 2001-2004. The medals are not given merely for an excellent doctoral thesis, but rather for an excellent body of published research. Nominations should be made by two Fellows of the ICA, and should be accompanied by a curriculum vitae and a letter explaining the importance of the nominee's research.

Nominations for the 2005 Euler, Hall, and Kirkman Medals must reach the Registrar by November 30, 2004. Award of the medals is determined by majority vote of the ICA Council (members of Council, as well as Honorary Fellows of the ICA, are not eligible for these awards). Nominators should phrase their letters so that the letters may be reproduced, in whole or in part, in the Bulletin of the ICA in case the nomination is successful; nominators should also indicate whether they are willing, in the latter case, to have their identities revealed.

Historical Summary of ICA Medallists

EULER MEDAL.
1993: Claude Berge, Ron Graham.
1994: J.A. Thas.
1995: Hanfried Lenz.
1996: J.H. Van Lint.
1997: No award.
1998: Peter Hammer, Anthony Hilton.
1999: D.K. Ray-Chaudhuri,

2000: Richard Brualdi, Horst Sachs.
2001: Spyros Magliveras.
2002: Herbert Wilf.
2003: Peter Cameron, Charles Colbourn.
2004: Doron Zeilberger, Zhu Lie

HALL MEDAL.
1994: Ortrud Oellermann, Chris Rodger, Douglas Stinson.
1995: Donald Kreher.
1996: Christos Koukouvinos, Christine O'Keefe, Tim Penttila.
1997: Reinhard Diestel.
1998: Marco Buratti, Arrigo Bonisoli.
1999: Rolf Rees, Hendrik Van Maldeghem.
2000: Michael Henning, Klaus Metsch.
2001: Alfred Menezes, Alexander Pott.
2002: Saad El-Zanati.
2003: Antonio Cossidente.
2004: Dirk Hachenberger, Masaaki Harada.

KIRKMAN MEDAL.
1994: Robert Craigen, Jonathan Jedwab.
1995: Darryn Bryant.
1996: Greg Gutin, Patric Östergård.
1997: Makoto Matsumoto, Bernhard Schmidt.
1998: Peter Adams, Cai Heng Li.
1999: Qing Xiang, Nicholas Hamilton.
2000: Michael Raines.
2001: Matthew Brown, Alan Ling, Ying Miao.
2002: Ian Wanless.
2003: Ken-ichi Kawarabayashi, Mateja Sajna, Sanming Zhou.
2004: Andreas Enge, Jon-Lark Kim.

The 2004 Euler, Hall, and Kirkman Medals

For 2004, **Euler Medals** were awarded to Doron Zeilberger and Zhu Lie. **Hall Medala** were awarded to Dirk Hachenberger and Masaaki Harada. **Kirkman Medals** were awarded to Andreas Enge and Jon-Lark Kim. We give summaries, abbreviated from the lengthy material submitted to ICA Council members, of the achievements of the medallists. This year, we are taking the material directly from the letters of nomination.

EULER MEDALS

Doron Zeilberger's mathematical career began in his early teens. He became enchanted by the beautiful world of mathematics, eventually receiving a Ph.D. in mathematics from the Weizmann Institute of Science in 1976 under the direction of Harry Dym (an academic descendent of Courant and Hilbert). His early mathematical works were mainly in the theory of discrete analytic functions; in which he published several research papers in the late 1970's. In the early 1980's, he discovered some interesting results that connect partial difference equations and combinatorics. Since then, he has published over 140 research papers in combinatorics, number theory, and algorithmic proof theory.

Zeilberger's work on binomial coefficient identities, using his generalization of Sister Mary Celine's techniques, gave rise to what is now known as the Wilf-Zeilberger (WZ) method which gives a unified approach for evaluating sums involving terms $F(n,k)$ where $F(n,k)$ is a hypergeometric term in both variables. Zeilberger has recently obtained a sharp upper bound for the orders of the recurrence relations generated by Zeilberger and q-Zeilberger algorithms. This new algorithm has smaller program-length complexity and provides an improved bound to those obtained using the older version.

The WZ method has added significanceto the field of combinatorics. George Andrews, who is one of the leading experts in q-series, wrote: "In my proof of Capparelli's Conjecture, I was completely guided by the Wilf-Zeilberger method, even if I didn't use Doron's program [EKHAD] explicitly. I couldn't have produced my proof without knowing the principle behind the WZ-method."

Donald Knuth wrote, in his foreword to the book A=B by Petkovsek, Wilf, and Zeilberger: "Science is what we understand well enough to explain to a computer. Art is everything else. During the past several years, an important part of mathematics [binomial coefficients identity] has been transformed from an Art to Science. No longer do we need brilliant insight to evaluate sums of binomial coefficients; we can now follow a mechanical procedure [guided by Zeilberger's program EKHAD] and discover the answers quite systematically."

Zeilberger's stellar achievements in combinatorics include proving the Alternating Sign Matrix Conjecture in 1996. His proof combines computer algebra and results from partition theory, symmetric functions, constant term identities, and difference operators. He has also proved Dyson's and q-Dyson's conjectures, the G2 and G2-dual cases of the MacDonald's conjecture, and Julian West's conjecture on 2-stack-sortable permutations.

Recently, Zeilberger has written a 5-paper series on the so-called umbral transfer matrix method. He has blended the transfer matrix method of statistical physics with the umbral calculus to develop a method for counting difficult combinatorial structures, such as self-avoiding walks.

Zeilberger, a champion of using computers and algorithms to do mathematics quickly and efficiently, is in the forefront of curent combinatorial research.

Zhu Lie of Suzhou University is one of the world's leading experts in the field of combinatorial design theory and its applications. He began research in the 1970's with the study of mutually orthogonal Latin squares. Of particular note was his short and elegant disproof of Euler's Conjecture, essentially relying only on an application of Sade's singular direct product construction.

Zhu has written about 150 research papers that encompass large sets of Kirkman triple systems, Hadamard matrices, difference families, perpendicular arrays, group divisible designs, resolvable designs, Steiner systems, perfect Mendelsohn designs, a variety of orthogonal arrays, and connections with graph decompositions, coding theory, and cryptography.

Some examples of results due to Zhu and his co-authors point out the depth and breadth of his research. His solution of the embedding problem for Steiner systems $S(2,4,v)$ was achieved through powerful recursive constructions. His research on $V(m,t)$ vectors using Weil's theorem on character sums is noteworthy. He solved the problem of $(q,4,1)$ and $(q,5,1)$ prime power difference families through a combination of theoretical and computational work.

After returning to China from the University of Waterloo in 1985, Zhu built a design theory research group at Suzhou University and played a leading role in China in combinatorial design theory. He has devoted much time to supervising graduate students and young colleagues, some of whom have gone on to gain strong international reputations of their own.

Zhu has also contributed to the links that exist between the Chinese and Canadian research communities in design theory. These arose from Zhu's numerous visits to Canada to collaborate with Canadian researchers such as Frank Bennett. Many of Zhu's students have studied in North America, and many Canadian researchers have visited conferences in China.

Zhu Lie serves on editorial boards of leading journals such as Annals of Combinatorics, Ars Combinatoria, and the Journal of Combinatorial Designs. He has also organized several major conferences and workshops in China.

Zhu's research has had great impact. Over 20% of articles published in the 2004 issues of the Journal of Combinatorial Designs are written or co-authored by researchers from the "Zhu School" in China. Zhu's legacy of excellence and innovation has had a dramatic influence on the many young mathematicians whom he has guided.

HALL MEDALS

Dirk Hachenberger wrote his Ph.D. thesis and his Habilitation under Dieter Jungnickel's supervision. He is now is a member of the group in Discrete Mathematics and Optimization at the University of Augsburg.

Dr Hachenberger's research covers two rather different parts of Discrete Mathematics. He has significantly advanced our knowledge of translation geometries and of the structural properties of finite fields. His work on Finite Geometry used algebraic methods to study many geometric objects (nets, transversal designs, and generalized quadrangles) admitting a translation group. Such problems can be translated into combinatorial problems about finite groups, and Hachenberger's results are the strongest known to date. He has improved previous work and partially resolved several open questions.

On the other hand, Hachenberger has studied structural properties of Finite Fields, in particular normal bases and various other types of generators for extension fields, a topic of practical interest because of the importance of explicit computations with often very large finite fields in applied areas of Cryptography, Coding Theory, and Signal Processing. He has made far-reaching generalizations of the primitive normal basis theorem, and his constructive work leads to the explicit determination of various types of generators and bases. Recently, he has worked on function field codes with Niederreiter and Xing.

Dr Hachenberger has written over 30 papers most of which have been published in leading journals such as Journal of the London Mathematical Society; Journal of Combinatorial Theory; Journal of Algebra; Acta Arithmetica; Designs, Codes and Cryptography; Finite Fields and their Applications. He also has published a monograph on normal bases and completely free elements (with Kluwer, in 1997). He is also an exceptional teacher, and received the 2004 award for excellence in teaching from the University of Augsburg.

Because of Dr Hachenberger's impressive work, he was selected as an invited speaker at the Fifth International Conference on Finite Fields and Applications in Augsburg (1999) and at Combinatorics 2000 (in Gaeta). On both occasions, he gave outstanding lectures which met with high praise. Since 2000, he has served on the editorial board of Designs, Codes, and Cryptography.

Masaaki Harada of Yamagata University works in areas that include algebraic coding theory, combinatorial designs, and unimodular lattices. He has written 90 papers published in highly rated journals that contain many innovative ideas and important contributions to the field. He wrote his first paper as a Master of Science student under the supervision of Prof. Hiroshi Kimura. This paper gave an elegant method for constructing extremal self-dual codes that generalized a previous construction using symmetric block designs. The old construction yielded four extremal codes of length 64, while the new construction produced thousands of inequivalent codes. Self-dual codes and their links with combinatorial designs and lattices are a major topic in Harada's research, and he is now a leading expert in this area. The impact of his work is apparent from the fact that the Elsevier "Handbook of Coding Theory" (Pless and Huffman eds) and the third edition of "Sphere Packings, Lattices and Groups" (by Conway and Sloane) contain over 50 citations of papers by Harada. His fresh ideas have inspired many others to start research in this exciting area. His collaborators include researchers from all over the world.

Much of Harada's research deals with applications of combinatorics to coding theory, and vice-versa, the use of techniques from the theory of codes for the constructing combinatorial designs. Harada introduced new methods for constructing optimal codes based on block designs, orthogonal designs, Hadamard and weighing matrices, and discovered several designs supported by self-dual codes. A high point of this work is the combinatorial characterization of putative binary extremal self-dual codes of length 72 (with Kitazume and Munemasa) and 96 (Harada 2004) in terms of the 5-designs supported by the vectors of minimum weight. The existence of such codes has long been an open problem, first formulated over 30 years ago.

Harada broadened the classical construction of 5-designs from extremal self-dual codes over a finite field of order 2, 3, or 4, by discovering the first 5-designs in codes over the ring Z_4. He made important contributions to the development of a theory of self-dual codes over general rings of order 2^k or 2k. He used this to find new constructions of the Leech and Niemeier lattices, to discover a 39-dimensional optimal unimodular lattice of minimum norm 4, an orthogonal basis of norm 22 in the Leech lattice, and extremal odd unimodular lattices in dimensions 44, 46, and 47.

KIRKMAN MEDALS

Andreas Enge's research concentrates on those aspects of finite fields which are of interest for applications in Cryptography, that is, algorithmic questions concerning the arithmetic and, in particular, curves over Galois fields. He has significantly advanced our understanding of such curves.

In his Diplomarbeit, Dr Enge provided an elementary treatment of elliptic curves over finite fields that avoided the use of algebraic number theory or algebraic geometry. Also, he explicitly dealt with the case of characteristic 2 which is often excluded in the literature even though it is of particular practical importance in Cryptography. Such an elementary treatment is needed by people working on applications. and not having an extensive mathematical background. His results were published as a monograph with Kluwer.

Dr Enge's research bridges the fields of Computer Science, Mathematics, and Communications Engineering and mainly concerns curves over finite fields with emphasis on their applications to Cryptography. Work in this area requires familiarity with advanced techniques from Algebra, Algebraic Geometry, and Algebraic Number Theory as well as expertise in computational and algorithmic aspects. In his papers, Enge has used methods from these areas in a deep and ingenious way. His work is of considerable theoretical interest, but also addresses applied, algortihmic and computational questions.

A few of the highlights of his work are: (1) a careful analysis of the arithmetic complexity of the group operations on Jacobians of hyperelliptic curves, including explicit formulas for the bit complexity of multiplication depending on the genus of the curve and the cardinality of the underlying field; (2) the first proven subexponential algorithms for computing discrete logarithms in situations of cryptographic interest; (3) a general framework allowing the axiomatic treatment of index calculus algorithms which is then applied to specific situations such as the multiplicative groups of finite fields, Jacobians of quadratic hyperelliptic curves, and ideal class groups of imaginary quadratic number fields.

Dr Enge is now a tenured research scientist at INRIA (in the group of Prof. Morain at the Laboratory of Computer Science at Palaiseau, as well as a part-time assistant professor in the Computer Science Department at the Ecole Polytechnique in Palaiseau). He has recently worked on a fast arithmetic for superelliptic cubics. He has already been an invited speaker at several venues, and his research papers have been accepted by leading professional journals such as Acta Arithmetica; Designs, Codes and Cryptography; Journal of Cryptology; and Mathematics of Computation. Recently, he has been appointed to the editorial board of Designs, Codes and Cryptography, in recognition of his role as one of the leading young researchers in Cryptology.

Jon-Lark Kim received his Ph.D. in 2002 from the University of Illinois at Chicago. In his first paper, he derived combinatorial identities from formulas about the weight distributions of self-dual codes, and described the relationship between the MacWilliams equations and certain binomial identities.

Dr Kim has done much work on the combinatorial classification of extremal self-dual codes. He constructed new extremal binary self-dual codes and new self-dual codes over GF(4) with the highest known minimum weights. His method was to build self-dual codes from a given self-dual code of a smaller length. In a joint paper, Kim and Lee generalized the method for the Euclidean and Hermitian self-dual codes over finite fields GF(q) to construct many Euclidean or Hermitian self-dual MDS (or near MDS) codes of length up to 12 over many finite fields GF(q). Their results on the minimum weights of (near) MDS self-dual codes over large fields give a better bound than the Pless-Pierce bound.

In 1986, Pless showed that the binary Golay code of length 24 (as well as the ternary Golay code of length 12) can be easily constructed from the hexacode of length 6 over GF(4) (respectively, the tetracode of length 4 over GF(3)). It was conjectured that one can construct good large binary codes whose decoding can be reduced, in part, to the decoding of a good quaternary code. However only a few codes had the above type of projection construction. Kim, Mellinger, and Pless gave a uniform characterization of similar projections and gave many examples of good binary linear codes with these projections. They constructed binary linear codes with optimal parameters: [20,11,5], [40,22,8], [48,21,12], and [72,31,16].

A recent active area in coding theory is low-density parity-check codes. A LDPC is a binary linear code with sparse parity check matrix H (there are relatively few 1's in H compared with the length and the number of rows of H). The Tanner graph of H is a simple bipartite undirected graph that consists of one set of vertices indexed by the rows of H, called check nodes or lines, and the other set of vertices indexed by the columns of H, called bit nodes or points. There is an edge in the Tanner graph of H if there is a one in the corresponding row and column of H. LDPC codes are strong competitors to Turbo codes in terms of decoding performance using iterative decoding. There are codes from both classes which approach the Shannon limit. A major problem is to give an explicit construction of such codes whose Tanner graphs have known girth. It is believed that LDPC codes with girth at least 6 in their Tanner graphs perform well using the sum product decoding algorithm. Kim, with Peled, Perepelitsa, Pless, and Friedland, found a construction by using the q-regular bipartite graphs D(m,q) on 2qm vertices which have girth at least 2*m/2*+4 constructed by Lazebnik and Ustimenko for q a prime power and m>1. Their results come from regarding these graphs as Tanner graphs of binary codes LU(m,q).

Kim and Walker have also worked on nonbinary quantum error-correcting codes from algebraic curves. As classical error-correcting codes protect information over a noisy channel, quantum error-correcting codes were suggested by Shor to protect quantum information against noise. Kim and Walker give a generalized Calderbank-Shor-Steane construction for nonbinary quantum error-correcting codes and construct nonbinary quantum stabilizer codes from algebraic curves. They also give asymptotically good nonbinary quantum codes from a Garcia-Stichtenoth tower of function fields that are constructible in polynomial time.

Third Prairie Discrete Mathematics Workshop

The University of Winnipeg will be hosting the Third Prairie Discrete Mathematics Workshop on August 25 and 26, 2005.

This workshop follows the format of the first and second Prairie Discrete Mathematics Workshops (PDMW) held at the University of Regina in 2003 and The University of Lethbridge in 2004. The idea for these workshops was first suggested by Brian Alspach and was based on the idea of the Combinatorial Potlatches that involved Universities in British Columbia and Washington.

Confirmed invited speakers are: Jose Caceres (University of Almeria, Spain-visiting University of Winnipeg), Linda Eroh (University of Wisconsin Oshkosh, USA), David Horrocks (University of Prince Edward Island), David Jackson (University of Waterloo), Hadi Kharaghani (University of Lethbridge), Bill Kocay (University of Manitoba), Ben Li (University of Manitoba), Dave Morris (University of Lethbridge), Norbert Sauer (University of Calgary), Lorna Stewart (University of Alberta)

There is no formal registration process and no registration fee will be charged. To help us with our planning we would appreciate it if you could let us know at **math.stats@uwinnipeg.ca** if you plan to attend the workshop.

International Conference on 21st Century Graph Theory
July 13 – 16, 2005
Chiang Mai University, Chiang Mai, Thailand

This conference is intended to provide a forum for mathematicians working in the field of Graph Theory and related subjects to present their research and to communicate about their interests and cooperations.

The scientific program will be held July 13-16, 2005 The program consists of 45-minute invited talk and 25-minute contributed talks. The topics include, but are not limited to: Pure Graph Theory, Applied Graph Theory, Computational Graph Theory, Algebraic Graph Theory, Topological Graph Theory, Discrete Mathematics, Enumerative Combinatorics, Appiled Combinatorics, Computational Combinatorics. Presented papers at the conference will be published in the Proceedings after peer review.

For more information regarding the conference including Chiang Mai University, the city of Chiang Mai, see: **www.math.science.cmu.ac.th/graph21st.**

7th French International Colloquiumon Graph Theory
Hyeres, Var, France
September 12 - 16, 2005

ICGT is the international conference initiated by Claude Berge, which is organized each 4 or 5 years by the french commmunity in Graph Theory. The last edition was held in Marseille in 2000. It covers the full range of Graph Theory including applications in other areas of Mathematics, Biology, Computer Science and Engineering.

Plenary Lectures: These will be expository lectures addressed to a broad audience. The following people have already accepted to give a plenary lecture: Noga Alon (Tel Aviv University, Israel); Oleg Borodin (Sobolev Institute of Maths, Russia); Maria Chudnovsky (Princeton University, USA); Jaroslav Nesetril (Charles University, Prague, Czech Rep.); Paul Seymour (Princeton University, USA); Robin Thomas (Georgia Institute of Technology, USA); Xuding Zhu (National Sun Yat-Sen University, Taiwan).

Proceedings containing the accepted extended abstracts are published in the Electronic Journal of Discrete Mathematics (ENDM). Printed versions will be available at the conference. A special issue of Discrete Mathematics will be devoted to selected papers contributed at the Conference.

Organizing Committee: Olivier Delmas, Patricia Lachaume, Ephie Deriche, Christophe Paul, Guillaume Fertin, Andre Raspaud, Frederic Havet (chair), Dany Sergeant, Corinne Julien, Stephan Thomasse

For more info, see **icgt05@sophia.inria.fr**

19th Midwest Conference on Combinatorics, Cryptography and Computing
Rochester Institute of Technology
October 7-9, 2005

Invited Speakers: (Keynote) Peter Winkler (Dartmouth College), Walter Wallis (Southern Illinois University), Earl Glen Whitehead, Jr. (University of Pittsburgh), Eric Mendehlson (University of Toronto), Kiran Kedlaya (M.I.T), Jon Lee (IBM), Ruth Haas (Smith College), Ralph Grimaldi (Rose Hulman Institute of Technology)

Organizers: Hossein Shahmohamad, R.I.T, Ebrahim Salehi, UNLV, Darren Narayan, R.I.T, Carl Lutzer, R.I.T, Bernard Brooks, R.I.T

Conference Site: **http://www.math.rit.edu/~cvlsma/MCCCC/**

The 30th Australasian Conference in Combinatorial Mathematics and Combinatorial Computing (30ACCMCC)

VENUE: The University of Queensland, Brisbane, Australia.

DATES: Monday 5th to Friday 9th December 2005 inclusive.
(Welcome and registration on the evening of Sunday 4th December 2005.)

WEBPAGE: `http://www.maths.uq.edu.au/cdmc/30accmcc.html`

INVITED SPEAKERS:

Simon Blackburn	*Royal Holloway, University of London, UK*
Matthew Brown	*The University of Adelaide, Australia*
Mike Grannell	*The Open University, U.K.*
Lily Khadjavi	*Loyola Marymount University, U.S.A.*
Curt Lindner	*Auburn University, U.S.A.*
Brendan McKay	*The Australian National University, Canberra*
Wal Wallis	*Southern Illinois University at Carbondale, U.S.A.*

and more to be finalised.

SPONSORED BY: School of Physical Sciences, University of Queensland; The Faculty of Engineering, Physical Sciences & Architecture, University of Queensland.

Contributed talks are welcome in all areas of combinatorics, graph theory, combinatorial computing and applications. A closing date for abstracts and registration will be announced later; this will be around late October 2005.

If you wish to be included on a conference email list, please email Elizabeth Billington at `ejb@maths.uq.edu.au`