Heera Lal Janwa
(Catedratico, (Full Professor), Mathematics, UPR, Rio Piedras): (http://ramanujan.uprrp.edu)

MAIN RESEARCH INTERESTS:

Coding Theory (Combinatorial, Algebraic, Algebraic Geometric, LDPC codes, Expander Codes, Convolutional Codes, Network Coding); Rate Distortion and Data Compression. Combinatorics; Discrete Mathematics; Cryptography; Cryptography, Number Theory and Algebraic Geometry (Public Key Cryptosystems based on Codes; Signature Schemes; Sequence Design; Expanders, Magnifiers and Ramanujan Graphs and Their Applications; Algebraic Geometry over Finite Fields and Its Applications; Parallel Computation; Interaction between Algebraic Topology and Graph Theory; Bioinformatics; Ecological Informatics.

Education

M.Sc. (Hons.) Integrated	1975–80	Birla Institute of Technology & Science (BITS), Pilani, India *Five years* **(B.Sc.+M.Sc.) MATH*)* (NSTS Fellow)**
B.E. (Hons.)	1978–81	Birla Institute of Technology & Science, Pilani, India (*Electrical and Electronics Engineering*)
Grad. Studies	1981–82	University of Illinois at Urbana-Champaign (in *Mathematics*)
Ph.D.	1982–1986	Syracuse University (School of Computer and Information Science)

TEACHING/RESEARCH APPOINTMENTS

- *Full Professor (tenured)* **(July 01, 2002——)**, *Associate Professor* (**August '97—-June 2002)** Department of Mathematics (and Computer Science until few years ago), University of Puerto Rico(UPR), at the main Campus (at Rio Piedras).
- *Visiting Member,* Courant Institute of Mathematical Sciences, NYU, **Aug. 2009–Aug. 2010**, and **Aug. 2003–Aug. 2004.** During Spring Semesters **2010** and **2004**, **also as** Scholar in Residence, FRN, NYU. (on Sabbatical leaves from UPR).
- *Associate Professor*, tenured (A rank somewhat similar to that of a Full Professor in the USA system. The ranking system at MRI was: *Post-Doc → Fellow→ Reader → Professor (A FACULTY member as*

Assoc. Prof./ Full Professor/Senior Professor)). [1], School of Mathematics, Mehta Research Institute of Mathematics and Mathematical Physics (MRI)/ Harish-Chandra Research Institute (HRI)) India **(August 1997—July 1999)**. (On sabbatical **'97–98**; on leave. **'98–99'**)

- Reader (*confirmed (= tenured),* **April 1996**)), Department of Mathematics, M.R.I (HRI)., **October 1992—-July 1997**.
- *Full Professor*, Center for Advanced Studies in Mathematics, University of Bombay, **January 1991–October 1992** (moved to MRI);
- Visiting Fellow, School of Mathematics, Tata Institute of Fundamental Research, **July 1990- July 1991**; Joined Univ. Bombay in January **1991**.
- Visiting Assistant Professor, Department of Mathematics, Michigan State University (MSU), **1989–90**;
- Harry Bateman Research Instructor (Faculty), Department of [Pure] Mathematics, California Institute of Technology (CALTECH), **1987–1989**. (Junior Faculty Position.).
- Visiting Member, Courant Institute of Mathematical Sciences (CIMS), NYU, **1986–1987**: *(Computational Algebraic Geometry Group)*
- Graduate Assistant, School of Computer and Information Science, Syracuse University (SU), **1982–1986**.
- Graduate Teaching Assistant, Department of Mathematics, UIUC **1981–1982**.
- MRI Faculty eligible to supervise Ph.D. students registered at Allahabad University, India, **1996–1999**;
- Faculty in the BITS/MRI M.Phil collaborative program, **1995–1999**.

Among Other Positions Offered

IISc, Bangalore (India) (Senior Leccturer, 1990); ISI (Senior Lecturer); IIT Delhi (Assistant Professor (Mathematics), 1990); Institute of Mathematical Sciences (IMSc), Madras (Fellow, 1991); Reader (1991) IIT-Kanpur (Assistant Professor–invited for interview); IIT-Kanpur (invited for Associate Professor for Electrical Engineering-invited for interview.) Visiting Membership in the Special Year in Combinatorics,
Institute for Mathematics and Its Applications (IMA), University of Minnesota (1987-88)

Current Professional/ Affiliations

- Professor (Catedratico) Department of Mathematics
- Professor of MATH & CS- (from Aug. 1997—-until recently when we had a joint Department of Mathematics and Computer Science Dept. Currently, the affiliation with CS Dept. is not a formalized.)

[1] Most prestigious positions in the TIFR system. were the most prestigious positions, responsible for all the decision making in the Institutes. In 1997, of the around 20 faculty members in Mathematics and Theoretical Physics at MRI, there were, only member of the FACULTY (Professors at various ranks) the Director, one Full Professor, two Associate Professors, and the rest were Readers or Fellows.

- Core faculty Member in the Ph.D. Option in Discrete Mathematics, and Ph.D. Option in Computational Mathematics, options (since 1997)
- Faculty Member in the joint Doctoral Program in Computing and Information Sciences and Engineering (CISE), since 1997
- Director, CCTCR
- Participating Core Faculty Member in the Doctoral Program in the Department of Environmental Sciences (since April 2007) **Already Supervising the Ph.D. Thesis of Dionisio Perez Montes, under the NSF-IGERT program**

SELECTED HONORS

(**Other Honors** include being members of several external Ph.D. review committees; **one of the main invited speakers** at several international conferences; (see appropriate sections below))

2016	Plenary Speaker WMC2016, Santander, Spain
2015	Invited Speaker IWSDA 2015, Bangalore
2013	Invited Speaker AGCT, Mubai, India Dec.2013.
2012	Invited Speaker at the Annual TIFR International Conference: 2012 Theme, "Recent Trends in Disc
2011	Invited Speaker at the AMS Annual Sectional Meeting, UNLV, Nov. 2011
2010	Invited to Organize AAECC-18 in Puerto Rico
2010	Scholar in Residence (awarded by Faculty Resource network)(NYU), Spring Semester
2008	One hour Invited Speaker at the AMS Annual Meeting, San Diego, January 2008.
2007	Co-Chair of International Symposium on AAECC, Bangalore, India, Dec. 16-20
2005	Invited Speaker at the AMS Annual Meeting, Atlanta, 2005
2000	UPR President Maldonado's citation for *distinguished research* and *service to UPR* in the area of science and technology.
2005	Scholar in Residence (awarded by Faculty Resource network)(NYU), Spring Semester
1987–1989	Harry Bateman Research Instructor, CALTECH, 87–89.
1987–88	Visiting Membership in the Special Year in Combinatorics, Institute for Mathematics and Its Applications (IMA), University of Minnesota (declined)
1986–1987	NSF funded visiting membership in the CIMS (NYU).
1986	Syracuse University (SU) Doctoral Prize for one of the two best Ph.D. dissertations submitted to SU (out of approximately 140) during 1985-86
1980-81	Doctoral Fellowship: Nat. Council of Educational Res. & Training, India
1975-80	National Science Talent Search Scholarship, Government of India
1974-75	Secondary School Merit Scholarship, 4th in the State of Rajasthan, India

SELECTED VISITS TO INSTITUTES/UNIVERSITIES:

1. Courant Institute of Mathematical Sciences (CIMS), NYU: **Three full year visits** and **numerous periodic short term from 1986—-**. From UPR **visits every year 1997—-2013**(From one week to one month). **Longer Term visits: August 2009– August 2010 (one year Sabbatical)**, **August 2003– August 2004 (one year Sabbatical)**. **August 1986– June 87 (Visiting Member as a one Year Courant NSF-Fellow).**
2. Technical University of Denmark (DTU), August 2012 (2 weeks), January 2012 (two weeks), June 2011 (two weeks), July 23, 2010—August 08, 2010; October 10—November 15, 2009; Aug. 2—Aug 23, 2008, June 1–June 22, 2007
3. Indian Institute of Technology (IIT Bombay): September 19–22, 2015. **November 26—January 14, 2013** (three weeks); **December 23, 2012—January 08** (two weeks); **December 2007** (one week.
4. University of Zurich, November 10—-December 15, 2009. University of Basel (one day visit and Colloquium in November 2010); EPFL (one day visit and Colloquium in December 2010).
5. Tata Institute of Fundamental Research (TIFR): **December 16—21, 2012**.
6. Institute for Mathematics and Its Applications (IMA) Univ. of Minnesota (Summer 1988; two weeks), (Summer 1999, One wee k), April 2007, One week; December 2009 (one week);
7. Indian Institute of Science (IISc), Bangalore: September 11-19, 2015, 2007 (one week), 2015 (one week); Three visits during 1990–2000.
8. Indian Statistical Institute, Bangaore, 2007 (one week), 2015 (one week), three visits during 1990—2000.
9. SU 2000 (Aug. 10–13) 1998 (Aug. 19–22); 1993, 1991, 1988, 1987, 1986 (1-3 days).
10. MIT, August 18, 1998.
11. UPR, San Juan, PR, USA, UPR-Mayaguez (1995, 1998,1999—for one day), UPR-Humacao (1995,1997-for one day)
12. Gauss Research Lab., UPR, San Juan, PR, USA
    i) **(September 1994–March 1995)**;
    ii) May 1993 (one week);
    iii) November–January 1992 (two months);
    iv) October-November 1991 (one month);
    v) May 1990 (two weeks). funded by NSF).
13. Cornell Univ. (1993, three days), (1988, 1 day).
14. INRIA, Sophia Antipolis, France (1993) (1 day)
15. ENST, Paris, France, 1993 (1 day).
16. USC, 1991.

17. MSU, (August 1989–July 1990) **one year)**; 1991 (two days).
18. OSU, 1991 (two days).
19. CALTECH (June 1987–August 1989) **(two years)**; (1991, two days,), 2005 (one week).
20. CUNY (Graduate Center). Several Visits during 1986–87; August 15, 2000; January 24, 2003.
21. IAS, Princeton (2006, one week)
22. IIT-Bombay (several times), IIT-Kanpur (four times), IIT-Delhi (three times, IIT-Madras (three times), IIT-Khargarpur (once), Institute of Mathematical Scienes (now Chennai Mathematical Institute) (three times), SPIC Science Foundation (three times)
23. University of Bombay (several times), University of Delhi, Madras University, Poona University, Udaipur University

PROFESSIONAL RECOGNITIONS AND DISTINGUISHED SERVICES

1. One of the four research exchange professors from the UPR system (selected by the Vice President for Research for the UPR system) as part of a high-level delegation that visited the Microsoft Research Headquarters in Redmond, WA, on January 18, 2001, and presented one of the four research talks.
2. April 2000: Dean's committee to recommend chair for mathematics (elected by Math Dept.)
3. Member, Conference Committee of the International Symposium on AAECC-18, Spain, June 2009 AAECC-17, Bangalore, India, December, 16–2007 (Co-Chair) AAECC-16, Las Vegas, USA, February 20-24, 2005 AAECC–15,Toulouse, France, May 12–16, 2003, AAECC–14, Australia, November, 2001, AAECC–13, Hawaii, November, 1999; AAECC–12 Toulouse (France), July 15-18, 1997; AAECC–11, Paris, July 1995; AAECC–10, San Juan, PR, USA, May, 10–14, 1993.
   AAECC $\equiv$ *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*
4. Member of the program, *The 1st Institute of Mathematical Statistics (IMS) and International Mathematical Statistics (ISBA) Joint Meeting,* July 24–26, 2003, San Juan, PR, USA.
5. Scientific Committee, COLLOQUIUM: Algorithmic, Arithmetic and Geometry in the Theory of Error-Correcting Codes, 1–5 April, 1996, Universite Antilles, Guyane, Guadeloupe, (Scientific Committee: Hoholdt, Janwa, Lachaud, Moreno, Rolland, Tsfasman).
6. One of the main invited speakers at several International Conferences (**see the list after PUBLICATIONS below**.)
7. Long paper, at the 1995 IEEE International Symposium on Information Theory (ISIT-95), British Columbia, CANADA, Sept. 22, 1995 (with O. Moreno). (19 of the approximately 600 presentations were long); and at the ISIT-97, Ulm, Germany June 29–July 3, 1997 (with O. Moreno). (18 of the approximately 550 papers were long).

8. "The non-existence of projective planes of order 10: Recent solution to a problem of Euler," *Annual Day Lecture* in Mathematics, at the MRI, Allahabad on July 19, 1993.
9. Served on National Committee set up by the Chairman of the Department of Atomic Energy (DAE), India, for linking of Libraries in the 13 Institutions funded by DAE (October 1996–February 1997).

GRANTS

SELECTED GRANTS:

CURRENT GRANTS:

-
- H. Janwa (PI)
  Support: Letter of Intent Submitted; Final Proposal to be Submitted, February,2016
  Project/Proposal Title: Graphs, Codes, Cryptosystems, Number Theory, and Algebraic Geometry: :
  Source of Support: NSF
  Total Award Amount: $6 million
  Location of Project: University of Puerto Rico-Rio Piedras Campus
  Status: Letter of Intent Submitted 10, January, 2017: Proposal be submitted February 10,2017
  Period:08/01/2017—07/31/2022

- H. Janwa (PI)
  Support: Submitted
  Project/Proposal Title: Graphs, Codes, Cryptosystems, Number Theory, and Algebraic Geometry: :
  Source of Support: NSF
  Total Award Amount: $496,383 K
  Location of Project: University of Puerto Rico-Rio Piedras Campus
  Status:Pending
  Period:04/01/2017—05/31/2020

- H. Janwa (PI)
  Support: Submitted
  Project/Proosal Title:Exceptional Almost Non-Linear (APN) Polynomials and Absolute Irreducibility of Multivariate Polynomials
  Source of Support: NSF
  Total Award Amount: $157,787 K
  Location of Project: University of Puerto Rico-Rio Piedras Campus
  Status:Pending
  Period:08/01/2017—05/31/2020

- H. Janwa (Co-PI)
  Support: Submitted
  Project/Proosal Title: Codes from New Expander Graphs with Reed-Solomon Component Codes

Source of Support: NSF
Total Award Amount: $218, 613 K
Location of Project: University of Puerto Rico-Rio Piedras Campus
Status:Pending
Period:08/01/2017—05/31/2020

PAST GRANTS:

- H. Janwa (PI)
  Support: Submitted
  Project/Proosal Title: Building a STEM-Ready Talent Pipeline at the University of Puerto Rico
  Source of Support: DOE
  Total Award Amount: $1million 199k 987K
  Location of Project: University of Puerto Rico-Rio Piedras Campus
  Status: Declined (90 % Score in Qualify, Services, and Significance)
  Period:09/01/2016—08/31/2019

- H. Janwa (Senior Personnel; Director of Project:**BioInformatic Modeling** in the Knowledge Systems Group) Support: Submitted
  Project/Proosal Title: NOAA Center
  Source of Support: NSF
  Total Award Amount: $15 million
  Location of Project: University of Puerto Rico-Rio Piedras Campus
  Status: Declined
  Period:2016—2021

- Co-PI and Co-Director for NSF-STEM (NSF-DUE#)0630927, [2006–20011]; extension expected (2011–2012). for **$5000K**
- NSF-IGERT Grant, 2008—2013, for **$3 million** one of the core faculty members in establishing an interdisciplinary Ph.D. program in the Environmental Scienes. Role: One of the dozen core faculty members whose CV was included in the NSF-IGERT main proposal and NSF-IGERT pre-proposal; And the only one from Mathematics in the proposal. From NSF data and discussions with some colleagues from NYU, odds for approval of pre-proposal for selection of NSF-IGERT pre-proposal is approximately 1 in 20. And extremely difficult to get through the final proposal. **Already Supervising the Ph.D. Thesis of Dionisio Perez Montes, under the NSF-IGERT program**
- H. Janwa (PI) Support: Submitted
  Project/Proposal Title: LDPC Codes for Deep Space Applications:
  Source of Support: NASA IDEAS Grant (via RSCE)
  Total Award Amount: $ 30K

Location of Project: University of Puerto Rico-Rio Piedras Campus
Status: Declined
Person-Months Per Year Committed to the Project. Cal:0 Acad: 0 Sumr:
(Travel, Visitors and Student Support) June], 2010–June, 2011

OTHER GRANTS SUBMITTED/APPROVED

- (H. Janwa (PI), F. Castro (Co-PI), C. Corrada (Research Collaborator), I. Rubio (Research Collaborator), F. Castro (Research Collaborator), R. Pericchi (Research Collaborator), P. Rivera (Research Collaborator)).
  Support: Submitted:

  Project/Proposal Title:
  Explicit Constructions and Decoding of LDPC/Expander Codes for Rapid, Reliable, and Secure Communication: Algebraic, Algebraic Geometric, Combinatorial and Probabilistic Approaches
  Source of Support: DoD
  Total Award Amount: $ 714, 641
  Dates: August 1, 2009—July 31, 2012
  Location of Project: University of Puerto Rico-Rio Piedras Campus
  Person-Months Per Year Committed to the Project. Cal: 0 Acad: 2/9 Sumr: 2/9
  Status: submitted. **(Selected one of the top three proposals from UPRRP, and one of the top five from PR Institutions, under DESPSCoR solicitation.)**. Our proposal was declined. We none of the other five proposal from PR got approved.
- (H. Janwa (PI), F. Castro (Co-PI), C. Corrada (Research Collaborator), I. Rubio (Research Collaborator), F. Castro (Research Collaborator), R. Pericchi (Research Collaborator), P. Rivera (Research Collaborator)).
  Support: Submitted:

  Project/Proposal Title:
  Explicit Constructions and Decoding of LDPC/Expander Codes for Rapid, Reliable, and Secure Communication: Algebraic, Algebraic Geometric, Combinatorial and Probabilistic Approaches
  Source of Support: NASA-EPSCoR
  Total Award Amount: $ 714, 641
  Dates: August 1, 2009—July 31, 2012
  Location of Project: University of Puerto Rico-Rio Piedras Campus
  Person-Months Per Year Committed to the Project. Cal: 0 Acad: 2/9 Sumr: 2/9
  Status: submitted. PREPROPOSAL.

EARLIER GRANTS/PROPOSALS

- (H. Janwa (PI), F. Castro (Co-PI), C. Corrada (Research Collaborator), I. Rubio (Research Collaborator), F. Castro (Research Collaborator), R. Pericchi (Research Collaborator), P. Rivera (Research Collaborator)).
  Satus:
  Support: Submitted:

  Project/Proposal Title:
  Explicit Constructions and Decoding of LDPC/Expander Codes for Rapid, Reliable, and Secure Communication: Algebraic, Algebraic Geometric, Combinatorial and Probabilistic Approaches
  Source of Support: DoD
  Total Award Amount: $ 714, 641
  Dates: August 1, 2009—July 31, 2012
  Location of Project: University of Puerto Rico-Rio Piedras Campus
  Person-Months Per Year Committed to the Project. Cal: 0 Acad: 2/9 Sumr: 2/9
  Status: **(Selected one of the top three proposals from UPRRP and one of the top five proposals from PR, under DESPSCoR solicitation and submitted to DOD. None of the five proposals submitted from PR was funded.**
- (H. Janwa (PI),
  Support: Submitted:

  Project/Proposal Title:
  Explicit Constructions and Decoding of LDPC/Expander Codes for Rapid, Reliable, and Secure Communication: Algebraic, Algebraic Geometric, Combinatorial and Probabilistic Approaches
  Source of Support: NASA-EPSCOR
  Total Award Amount: $ 750K
  Dates: August 1, 2010—July 31, 2013
  Location of Project: University of Puerto Rico-Rio Piedras Campus
  Person-Months Per Year Committed to the Project. Cal: 0 Acad: 2/9 Sumr: 2/9
  Satus: Declined.
- H. Janwa (PI) Support: (Not considered: Proposal Was not uploaded correctly under GRANTS.GOV under the Sponsored Research Office at UPRR-RP)
  Project/Proposal Title: CYBER SECURITY IN THE CLASSICAL AND POST-QUANTUM CRYPTOGRAPHY AGE:
  Code Based Cryptosystems And Their Applications Source of Support: DHS
  Total Award Amount: $ 188K
  Location of Project: University of Puerto Rico-Rio Piedras Campus
  Status: Not considered, as the UPR office did not submit under GRANTS.GOV in time
  Person-Months Per Year Committed to the Project. Cal:0 Acad: 0 Sumr: 2/9

December 31, 009—December 31, 2012

- H. Janwa (PI)
  Project/Proposal Title: POST-QUANTUM PKCs: On Our Public Key Cryptosystem
  Based on Subfield Subcodes of
  Algebraic-Geometric (AG) Codes
  Source of Support: NSF
  Total Award Amount: $ 188K
  Location of Project: University of Puerto Rico-Rio Piedras Campus
  Status: Declined **(wrongly classified in the CISE as TCS rather than Communications Research.**
  Person-Months Per Year Committed to the Project. Cal:0 Acad: 0 Sumr: 2/9
  Aug. 1, 009—July 31, 2012
- H. Janwa (PI)
  Project/Proposal Title: On Our Public Key Cryptosystems Based on Subfield Subcodes of Algebraic Geometric Codes
  Based on Subfield Subcodes of
  Algebraic-Geometric (AG) Codes
  Source of Support: NSF
  Total Award Amount: $ 188K
  Location of Project: University of Puerto Rico-Rio Piedras Campus
  Status: Declined **NSA does not support directly cryptography related research—conflict of interest.**
  Person-Months Per Year Committed to the Project. Cal:0 Acad: 0 Sumr: 2/9
  Aug. 1, 009—July 31, 2012
- H. Janwa (PI)
  Project/Proposal Title: Error-Correcting Codes Based on LDPC codes for Secure and Reliable Communication.
  Source of Support: DoD (ARO)
  Total Award Amount: $ 250K
  Location of Project: University of Puerto Rico-Rio Piedras Campus
  Status: **ARO Recommended (Accept); ARO an AFSOR-Collective Decision (Decline)**
  Person-Months Per Year Committed to the Project. Cal:0 Acad: 0 Sumr: 2/9
  Aug. 1, 009—July 31, 2012
- PI, UPR-DEGI grant for "Expander codes and LDPC" , **2008–2010**, for **$ 57K**.
- "Ramanujan Graphs, Codes, Exponential Sums, and Sequences" NSF Grant: **$ 206,650**), (July 1999- June 2003)
  (Heeralal Janwa, *Principal Investigator (***PI***)*, and Oscar Moreno (Co-PI)
- NSF-CSME grant Number: #9986985 for **$154,000** (200l-2005).
  (Heeralal Janwa (Co-PI) and Herman Acuna, PI)

- UPR-RP, CISE-NSF,(Five years, 08/01/2000—07/31/2005. **$ 1.5 million)**. Of the seven research projects included in this grant, I am PI of three and Co-PI of one proposals. The over all director for this proposal is O. Moreno.
- DEPSCOR Proposal for 2005–2008 for $500,000 (H. Janwa (PI); Co-PIs R. Pericchi, I. Rubio, H.F. Mattson, Jr. **(selected by EPSCoR as one of the five best proposals from PR for DEPSCOR and was then submitted as a part of the package to the Department of Defense). None of the ten proposals from PR was funded.**
- DEPSCOR Proposal for 2004–2007 for $500,000 (H. Janwa (PI); Co-PIs R. Pericchi, I. Rubio, H.F. Mattson, Jr. **(selected by EPSCoR as one of the ten best proposals from PR for DEPSCOR and was then submitted as a part of the package to the Department of Defense).**
- "New Families of Infinite Classes of Constant Degree Expander Graphs and Their Tanner Codes ad Decoding," UPR FIPI - Institutional Funds for Research for 2004–2006, (**$ 26,000**)

OTHER GRANTS:

- *The MRI faculty won a 5-year grant of Rupees 150 million from the DAE. I was a senior member of the faculty at that time. This amount was equivalent to the average salary for approximately 1500 faculty members for one year in 1995.*
- "Ramanujan Graphs, Codes, Exponential Sums, and Sequences"
  UPR FIPI - Fondo Institucional para la Investigacion Grant for 2001–2002 (**$10,000**)
- "Genetic Algorithms to Design Good Codes," UPR FIPI - Fondo Institucional para la Investigacion Grant for 1998–2000 (**$10,000**)
- Equipment Grant from the Dean of Faculty of Natural Sciences **$ 9,000**, in 1999.
- **International Travel grant from MRI,** India to visit Universities and participate in International Conferences in 1997. [**Remark**. Very high currency exchange rates make these grants highly competitive.]
- National Board of Higher Mathematics (NBHM) (INDIA) **International Travel Grant** to participate in the *10th International Conference on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes,* UPR, PR, USA, May 1993.

  [**Remark**. Because of very high currency exchange rates, these grants are highly selective with all India level competition.]
- Travel and Lodging paid by the Organizing Committee of AAECC-9 to participate as an invited speaker at the Conference held in New Orleans, USA, October 07–11, 1991 and for honorarium. $\approx$ **$ 2,500**.
- International Travel Grant (from India): Visited the Gauss Research Lab. (UPR), funded by EPSCoR of PR and CISE-NSF, October-November 1992 (one month), November-December 1992 (six weeks), May 1993 (one week) and September 1994-December 1994, January-March 1995.
- Travel Support from Gauss Research Lab. to participate in the International Conference on Algebraic Geometry over Finite Fields and Applications, 1990.

- Travel support and honoraria to visit Institute for Mathematics and Its Applications, University of Minnesota (two weeks: summer 1988); USC, SU, MSU, OSU, UPR (1991), SU (1993,1998,2000), INRIA (1993), IMSC Madras (1990, 1992, 1993), IISc. Bangalore, (1991, 1992), IIT Kanpur (1991), ISI Bangalore (twice), University of Bombay (1994), Poona University (1990, 1991, 1994), ISI-Delhi (twice), BHU (once), Delhi University (1995), SU (1998), MIT 1998.
- Visited many other Institutes such as IIT Delhi, ISI Delhi, IIT Bombay with support.
- $500.00 by UPR, RP, PR, USA, to participate in the *Workshop on Applications of Algebraic Geometry,* January 7-13, 1990.
- $700.00 by IMA, Minnesota to participate in the *IMA Workshops on Coding Theory and Design Theory,* June 13-24, 1988.
- $500.00 by American Mathematical Society to participate in the *AMS Centennial Conference*, Providence, RI, August 1988.
- Summer Research support at SU, 1982–1985 and Summer teaching support at SU, 1983–85. (Only few of the Graduate Students received such additional support besides regular academic year support.)
- Several other trips to attend conferences and invitations were partially supported by various agencies and universities
- "CDMA Sequence Designs and Designs for Department of Defense-Office of Naval Research, (for **$500,002**, 04/01/00–03/31/03) (H. Janwa (Co-PI), O. Moreno (PI), D. Bollman (Co-PI), F. Castro (Co-P I)) **(selected by EPSCoR as one of the ten best proposals from PR for DEPSCOR and was then submitted as a part of the package to the Department of Defense).**
- "A Multidisciplinary Graduate Program Option in Communication Science," (Co-PI), a pre-proposal submitted to NSF, 06/28/2001

PUBLICATIONS (At least over 500 citations (in over two dozen citations in Books

. A google search yields many times more.

Substantial research that I carry out is in Mathematics as it is applied to Error-correcting codes, Sequences, and Cryptograhy, and other modern areas of applied Mathematics. Prompt publication of research in these disciplines is of utmost importance in these highly competitive research areas and publication in prestigious conference proceedings are preferred over Journals that can take years (harmful for priority, patent, and competitiveness). For example, our article, H. Janwa and R.M. Wilson, "Hyperplane section*s of Fermat varieties in $I\!P^3$ in char. 2 and some applications to cyclic codes,"
Proceedings of the 10th International Conference on AAECC,
LNCS, No. 673, 1993, pp. 180–194. (Refereed by three referees.) , is regarded as a foundational paper in APN functions, and other non-linear functions of utmost importance for cryptography and sequences. This article has received quite high citations (70; hundreds in theses, reports and so on).

The AAECC proceedings have been regarded as highly competitive with three referees and high rejection rate.

Even among these, the article, "On the parameters of algebraic-geometric codes," *Proceedings of the 9th International Conference on Algebraic Algorithms and Error-Correcting Codes* (AAECC), New Orleans, USA, October 7-10, 1991. *Springer-Verlag Lecture Notes in Computer Science* (LNCS), No. 593, October 1991, pp. 19–28. (**Invited**). (Refereed by three referees.), was one of the five invited speakers. Two other articles below ISIT05 and ISIT07, were as a result of 40 minute invitations in the prestigious ISIT Symposia, and indeed from among 500-600 articles that appeared, only 15-17 were declared as such.

The AMS-Review does not review many of the articles that have appeared below. However, their quality can be judged from the citations they have received (as can be confirmed by multiple sources).

Many of the articles have already appeared as references in books. Several of these articles are also invited solicitations, in AAECC, in ISITs, in DCC, in AMS-Joint Annual Conferences, ...

BOOKS

1. H. Janwa, Relationships among parameters of codes,
   Published by the University of Michigan Dissertation Publication Services, 1986.
   (Based on the award winning Ph.D. Dissertation, School of Computer and Information Science, Syracuse University, August 1986.)
2. H. Janwa and S.S. Rangachari (TIFR), Ramanujan Graphs and Their Applications. **RESEARCH MONOGRAPH.** Preprint dated January 15, 2010. 200 pages. (Cambridge University Press has solicited this book for publication in Their Cambridge Tracts in Mathematics, and also In Their Communications Series.).
3. H. Janwa, *Algebraic Geometry over Finite Fields and Its Applications.*
   (Status as of 20/06/2010: A preliminary draft version.)

t

Publications I (in print)

4. H. Janwa and H. F. Mattson, Jr., "The covering radii of even subcodes of t-dense codes," *Springer-Verlag Lecture Notes in Computer Science*, vol. 229, pp. 120-130, 1986. (**Invited**.)
5. H. Janwa and H.F. Mattson, Jr., "The covering radii and normality of t-dense codes," *Proceeding of the IEEE International Symposium on Information Theory (ISIT)*, Ann Arbor, Michigan, October 6-9, 1986.
6. H. Janwa, "Some new upper bounds on the covering radii of binary linear codes," *IEEE Transactions on Information Theory,* vol. IT-35, no. 1, pp. 110–122, January 1989.
7. H. Janwa, "Some optimal codes from algebraic geometry and their covering radii," *European Journal of Combinatorics,* vol. 11, pp. 249–266, 1990.
8. H. Janwa, "On the covering radii of q-ary codes." *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, January 14–19, 1990, San Diego, California.
9. R. Dougherty and H. Janwa, "Covering radius computations for binary cyclic codes,", MATHEMATICS OF COMPUTATION, Vol. 57, no. 195, July 1991, pp. 415–434.
10. R. Doubherty and H. Janwa, "Appendix–Results of Covering Radius Computations," MATHEMATICS OF COMPUTATION, Vol. 57, no. 195, July 1991, **s38—-s218**. (As Microfiche supplements.)
11. H.T. Cao, R. Dougherty and H. Janwa, "A [55,16,19] Binary Goppa Code and Related Codes Having Large Minimum Distance," *IEEE Transactions on Information Theory,* Vol. 37, no. 5, September 1991, pp. 1432–1433.
12. H. Janwa, "On the parameters of algebraic-geometric codes," *Proceedings of the 9th International Conference on Algebraic Algorithms and Error-Correcting Codes* (AAECC), New Orleans, USA, October 7-10, 1991. *Springer-Verlag Lecture Notes in Computer Science* (LNCS), No. 593, October 1991, pp. 19–28. (**Invited**). (Refereed by three referees.)
13. H. Janwa, *THE MAN WHO KNEW INFINITY: A Life of the Genius Ramanujan,* in *The Political and Economical Weekly of India,* September 26, 1992,
    pp. 2105–2106.
14. H. Janwa and R.M. Wilson, "Hyperplane section*s of Fermat varieties in $I\!P^3$ in char. 2 and some applications to cyclic codes,"
    Proceedings of the 10th International Conference on AAECC,
    LNCS, No. 673, 1993, pp. 180–194. (Refereed by three referees.)
15. H. Janwa, *THE MAN WHO KNEW INFINITY: A Life of the Genius Ramanujan,* By Robert Kanigel; *Bombay Mathematical Colloquium,* March 1993;
16. H. Janwa and O. Moreno, "McEliece-Public Key Cryptosystems Using Algebraic Geometric Codes," *Proceedings of the 1995 IEEE International Symposium on Information Theory (ISIT), British Columbia, Sept. 17–22, 1995,* p. 484-484.
    The conference had 19 long papers among 600 total.

17. H. Janwa, G. McGuire, and R.M. Wilson, "Double-error-correcting cyclic codes and absolutely irreducible polynomials over $GF(2)$," JOURNAL OF ALGEBRA, vol. 178, pp. 665–676, 1995.

18. H. Janwa and O. Moreno, "Elementary Constructions of Some Ramanujan Graphs," CONGRESSUS NUMERANTIUM, vol. 112, pages 7-15, December 1995.

19. H. Janwa, "Public Key Cryptosystems Using Algebraic Geometric Codes," *Proceedings of the National Discussion Meeting on Cryptography and Computation*, held at JNCASR, IISc. Bangalore, India, September, 1995.

20. H. Janwa and O. Moreno, "McEliece like public-key cryptosystems using algebraic-geometric codes," *Designs, Codes and Cryptography*, vol. 8, no. 3, pp. 293–307, 1996.

21. H. Janwa and A.K. Lal, "On the generalized Hamming weights of cyclic codes," *IEEE Transactions on Information Theory,* Vol. 43, No. 1, pp. 298–308, January 1997.

22. H. Janwa and O. Moreno, "Strongly Ramanujan graphs from codes, polyphase-sequences, and Combinatorics," *Proceedings of the International Symposium on Information Theory, 1997 (ISIT-97)* Ulm, Germany., 1997, pp. 408-408,
    The Conference had 18 long papers among total about 600.

23. H. Janwa and O. Moreno, "Coding theoretic constructions of some number theoretic Ramanujan graphs," CONGRESSUS NUMERANTIUM, Vol. 130, pp. 63–76, 1998.

16. H. Janwa and H.F. Mattson, Jr., "Some Upper Bounds on the Covering Radii of Linear Codes over F_q and Their Applications," *Designs, Codes and Cryptography,* Vol. 18, no. 1-3, December 1999, *pp. 163–181.* (**invited.**)

24. H. Janwa, Jr., "Relations among Expander Graphs, Codes, Sequence Design, and Their Applications," in *Proceedings of the 4th World Multi-conference on Systemics, Cybernetics and Informatics (SCI2000) and ISAS2000)*, Orlando Florida, July 23-26, 2000, Vol. XI, pp. 122-124.(**invited—Organized by Jacque Wolfmann**)

25. H. Janwa and H.F. Mattson, Jr., "The Projective Hypercube and Its Properties and Applications," *Proceedings of the 2001 International Symposium on Information Theory, (ISIT-2001)* June 2001, Washington, USA., p. 312-312. (3 1/2 regular size printed pages.)

26. H. Janwa and A.K. Lal, ""A Comparison of Minimum Distance Bounds on Tanner Codes," *Proceedings of the 39th Allerton Conference on Communication, Control, and Computing,* pp. 1294–1296, December 2001.

27. H. Janwa and A.K.Lal, "On Tanner Codes: Parameters and Decoding," **Applicable Algebra** *in Engineering, Communication and Computing,*
    A Springer Journal, **Vol. 13**, pp. 335–347, 2003.

28. H. Janwa, "Good Expander Graphs and Expander Codes: Parameters and Decoding," *Proceedings of the 15th International Symposium on Algebraic Algorithms and Error-Correcting Codes* (AAECC-15), Toulouse, France, May 2003. *Springer-Verlag Lecture Notes in Computer Science* (LNCS), No. 2643, May, 2003, pp. 119–128. **(Refereed)**

29. "H. Janwa (With A.K. Lal). On Expander Graphs: Parameters and Applications" **arXiv:cs.IT/0406048:2004, pp. 1—11.**.
30. H. Janwa, "New (Explicit) Constructions of Asymptotic Families of Constant Degree Expander Graphs from AG Codes and Their Applications to Tanner Codes," ABSTRACTS OF THE AMS, Volume 26, no. 1, pp. 197. (JOINT AMS ANNUAL MEETING, Atlanta, USA, 2005; (Invitation only) Special session on Algebraic Geometry and Codes.)) (Invited Talk)
31. H. Janwa, "Explicit Constructions of Asymptotic Families of Constant Degree Expander Graphs from Algebraic Geometric (AG) Codes," *CONGRESSUS NUMERANTIUM*, vol. 179, 2006, pp. 193–207.
32. H. Janwa and A.K. Lal,"On the Generalized Hamming Weights and the Covering Radius of Linear Codes," **Lecture Notes in Computer Science**, **Vol.** 4871, **pp.** 347—356, December 2007.
33. H. Janwa, "Ramanujan graphs and Optimal Expander Graphs from Algebraic Geometric Codes," H. Janwa, "Expanders and Ramanujan Graphs: Construction and Applications." **ABSTRACTS of the AMS**, *Volume 29*, No. 1, **P. 223.** (JOINT AMS ANNUAL MEETING, San Diego, CA, USA, 2008; (Invitation Only) Special session on Expander Graphs and Ramanujan Graphs.)) **(one hour invited talk)**.
34. H. Janwa, Tom Hoeholdt, "Optimal Bipartite Ramanujan Graphs from Balanced Incomplete Block Designs: Their Characterizations and Applications to Expander/ LDPC Codes" **Lecture Notes in Computer Science**, **Vol. 5527**, **pp.** 53—64, June 2009.
35. H. Janwa, F. Pinero, "On the Parameters of Norm Trace codes," CONGRESSUS NUMERANTIUM, Vol. 206 (2010), PP. 99-113.
36. H. Janwa, F. Pinero, "On the Subfield Subcodes of Hermitian Codes," it Proceedings of the 3rd International Castle Meeting on Coding Theory and Applications, J. Borges and M. Villanueva (eds.), pp. 223—229, 2011
37. H. Janwa (with Tom Hoeholdt), "Eigenvalues and expansion of bipartite graphs" *Designs, Codes and Cryptography* **(invited article in Honor of Prof. R. M. Wilson's 65th birthday)**, December 2012, Volume 65, Issue 3, pp 259-273.
38. H. Janwa (with M. Delgado), "On the Conjecture on APN Function," **arXiv:1207.5528[cs.IT][math.AG][math.C 23 July 2012, pp. 1—15.**
39. H. Janwa, "Some Applications of Groebner Bases to Combinatorics," in *Combinatorial Topology and Algebra. Lecture Notes in Mathematics, Ramanujan Mathematical Society, Journal.* Vol. 18, pages 1994–205, 2013.
40. H. Janwa (with M. Delgado), "Further Results on Exceptional APN Functions," **www.math.iitb.ac.in/ srg/AGCT India-2013/Slides/HeeralalJanwa.pdf.**
41. H. Janwa (with F. Pinero), "On the subfield subcodes of Hermitian codes," *Designs, Codes and Cryptography,*, *Designs, Codes and Cryptography*, January 2014, Volume 70, issue 1-2m pp. 157-173.
42. H. Janwa (with P. Vijay Kumar and Andrew Z. Tirkel), "In Memoriam: Oscar Moreno de Ayala (1946–2015), **IEEE Information Theory Society News Letter**, December 2015, pp. 43–44.
43. H. Janwa (with F. Castro, G. Mullen, and I. Rubio), "On perfect like codes," *Bulletin of the Institute of Combinatorial Mathematics and its Applications,* Vol 76, pp. 1—7, January 2016.

44. H. Janwa (with M. Delgado), "Progress Towards the Conjecture on APN Functions and Absolutely Irreducible Polynomials," **arXiv:1602.02576 [math.NT] 30 Jan. 2016**

45. H. Janwa (with F. Pinero) "On Parameters of Subfield Subcodes of Extended Norm-Trace Codes," **arXiv:1604.05777 [math.AG] , 20 Apr 2016.**

46. H. Janwa (with M. Delgado), "On the absolute irreducibility of hyperplane sections of generalized Fermat varieties in $\mathbb{P}^3$ and the conjecture on exceptional APN functions: the Kasami-Welch degree case," **arXiv:1612.05997 [math.AG] 18 Dec.2016**

47. H. Janwa (with M. Delgado), "On the Conjecture on Non-linear APN Functions and Absolutely Irreducibility of Polynomials," **Designs, Codes and Cryptography,** Springer-Verlag, 82, no. 3, (2017) 627–627. DOI: 10.1007/s10623-015-0168-1

48. H. Janwa (with M. Delgado), "Some New Results on the Conjecture on Exceptional APN Functions and Absolutely Irreducible Polynomials: the Gold Case," **Advances in Mathematics of Communications (AMC)**, vol. 11, nov. 2, (2017), pp. 389–396.

49. H. Janwa (with F. Pinero), "On the Parameters of Subfield Subcodes of Norm Trace Codes," **Advances in Mathematics of Communications (AMC)**, vol. 11, no. 2, (2017), pp. 379–388.

50. . Janwa (with M. Delgado) "On the Completion of the Exceptional APN Conjecture in the Gold Degree Case and Absolutely Irreducible Polynomials," **Congressos Numerantium,** October 2017 (accepted)

51. .Janwa (with F. Pinero), BCH-like Codes from Extended Norm-Trace Codes, **Congressos Numerantium,** October 2017 (accepted)

52. H. Janwa and R. M. Wilson, "Rational Points on the Klein Quartic and the Binary Cyclic Codes $\langle \mathbf{m_1 m_7} \rangle$," *IEEE Transactions on Information Theory* (Accepted for publication subject to revision). (12 printed pages.)

53. H. Janwa (with H.F. Mattson, Jr.), "Codes and Their Groups," **submitted**.

54. H. Janwa (with M. Delgado), "On the conjecture on APN Function and Absolute Irreducibility of Polynomials," **submitted.**.

55. "Ramanujan graphs, codes, exponential sums, and Sequences" *to be submitted.* (with O. Moreno) (as a regular paper) (24 pages).

56. H. Janwa, F. Pinero, "On the Parameters and Decoding of Hermitian Codes," *to be submitted.*.

57. H. Janwa (with P. Guan), "Amalgamated Graph Based Codes from Cut-Sets with Fast Decoding Algorithms," *to be Submitted .*

58. H. Janwa, B. Mishra, P. Franquin, "Applications of expander graphs in bioinformatics." (preliminary preprint in preparation).

59. H. Janwa (with S. Cappell and S. Miller), "Constructions of some Ramanujan graphs based on insights from algebraic topology and Riemannin geometry," in preparation.

60. H. Janwa (with Tom Hoeholdt), Optima Regular and Irregular Bipartite Expander and Ramanujan Graphs and Expander Graphs: Their Characterizations and Applications to Expander/ LDPC Codes. In Preparation.
61. H. Janwa (with R. Dougherty), "Further results on the covering radius computation of cyclic codes'," in preparation.
62. H. Janwa (with S. Cappell and S. Miller) "Expander graphs from symmetries, " in preparation.
63. H. Janwa, "Post Quantum Cryptography: On our generalization of McEleice public key cryptosystems based on subfield subcodes of algebraic geometric codes," (preprint-12 pages) to be submitted. **presented at GeoCrypt2009, Guadalupe, France, June 2009**. Also presented at **EPFL Lausanne**, December 2009; **University of Zurich**, November 2009 and at EPFL Lausanne, Switzerland.
64. H. Janwa, "A General Framework for public key cryptosystems based on subfield subcodes of algebraic geometric codes and their security," (prerint-15 pages). To be submitted. (Presented at the **University of Basel**, November 2009; **EPFL**, December 2009, Switzerland)
65. H. Janwa (with P. Guan), "New Graph Based Code Constructions with Good Parameters and Fast Decoding Algorithm." (preprint-10 pages) (to be submitted).
66. H. Janwa, F. Pinero, "On the parameters of Hermitian codes: Theoretical and Algorithmic Results," (preprint-20 pages). (to be submitted.)
67. H. Janwa, "New Explicit Families of Constant Degree Expander from Algebraic Geometry Graphs and Their Tanner Codes," (preprint-15 pages-to be submitted.)
68. H. Janwa and A.K. Lal "On Expander Graphs: Parameters and Applications" to be (12 pages-submitted).
69. "New Families of Infinite Classes of Constant Degree Expander Graphs and Their Tanner Codes and Decoding," preprint.
70. H. Janwa and A.K. Lal, "Further Results on the generalized Hamming weights and the covering radius of cyclic codes" (10 pages-preprint.)
71. H. Janwa, "On the covering radii of AG codes," (12 pages preprint.)
72. H. Janwa and A.K. Lal, "Comparison of various bounds on the parameters of Tanner Codes," (15 pages, preprint.)
73. H. Janwa and H.F. Mattson, Jr. "Sparse Graph topologies for parallel computing," (10 pages, preprint.)
74. H. Janwa, and C. Beltran, "Algorithms for computing the generalized hamming of q-ary cyclic codes, and their applications to the existence of some optimal cyclic codes for wire-tap channels," in process.

Publications V (**Preprints**

75. H. Janwa, "Explicit constructions of asymptotic families of constant degree expander graphs: Their expander codes and decoding," preprint.
76. H. Janwa, "A graph theoretic proof of Delsarte's bound on the covering radius of linear codes." (7 pages)
77. H. Janwa, "l-MDS codes, threshold schemes and algebraic geometric codes." (12 pages)

78. H. Janwa, "On the covering radius of q-ary linear codes."
79. H. Janwa and H.F. Mattson, Jr., "On the covering radius of t-dense codes.'

Mehta Research Institute (MRI)/ Harish-Chandra Research Institute (HRI) TECHNICAL REPORTS

80. "Codes from some Ramanujan graphs," MRI-MATH/M970703
81. "Strongly Ramanujan graphs from codes, polyphase-sequences, and combinatorics," MRI-MATH/96-06 (with O. Moreno).
82. "Coding Theoretic constructions of some number theoretic Ramanujan graphs," MRI-MATH/96-05 (with O. Moreno)
83. "Some new upper bounds on the covering radius of codes and their applications," MRI-MATH/96-02 (with H.F. Mattson, Jr.).
84. "On the Generalized Hamming Weights of Codes Holding t-Designs," MRI-MATH/14/95.
85. "On the Generalized Hamming Weights and the Covering Radius of Linear Codes," MRI-MATH/13/95, (with A. Lal).
86. "Elementary Constructions of Some Ramanujan Graphs," MRI-MATH/10/95 (with O. Moreno).
87. "McEliece Public-Key Cryptosystems Using Algebraic-Geometric Codes," MRI-MATH/12/94 (with O. Moreno).
49. "Double-error-correcting cyclic codes and absolutely irreducible polynomials over $GF(2)$," MRI-MATH/11/94 (with G. McGuire and R.M. Wilson).
88. "A Graph Theoretic Proof of Delsarte's Bound on the Covering Radius of Linear Codes," MRI-MATH/10/94.
89. "On the Generalized Hamming Weights of Cyclic Codes." MRI-MATH/9/94 (A. Lal).
90. *Some Applications of Gröbner Bases to Combinatorics: A Survey*, MRI Report, MATHS/2/Mar94.
91. *Super Ramanujan Graphs from Combinatorics:* MRI Report, MATHS/3/Mar94.
92. *l-MDS Codes, Threshold Schemes and Algebraic Geometric Codes,* MRI Report, MATHS/3/Mar94.

Drafts.

93. H. Janwa (with G. Mullen, I. Rubio, F. Castro), "Characterization and Applications of Codes Related to the Perfect Codes," (in progress).
94. H. Janwa (with Peter Belen), "Characterization of Graphs Associated with Some Towers of Function Fields."
95. H. Janwa (with F. Bogomolov), "Distribution of the Moduli Space of Curves over Finite Fields for a Given Genus and Their Applications to cryptography."
96. H. Janwa (with S. Cappell, Ed.. Miller), "Laplacian of Graphs on Manifold, Their Isoperimetric Properties, and Applications."

97. H. Janwa (with Joachim Rosenthal), "Network Coding and and Grassmanian Varieties."
98. H. Janwa (with Maria Petkovic), "Modular Interpretation of Some Towers in Odd Powers."

PREPRINTS

99. Explicit Constructions of Good Expander Codes and Good Expander Graphs: Their Parameters and Decoding. (H.Janwa; H. Janwa and H.F. Mattson, Jr.; H. Janwa and A.K. Lal (IITK, India).
100. Algebraic geometric codes;
101. "Ramanujan graphs and expander graphs, codes, and sequence design. (with O. Moreno.)
102. "Tanner codes: their parameters and applications " (with A.K. Lal (IITK, India)).
103. "Projective hypercubes and applications (with H.F. Mattson, Jr.)
104. "Good expander graphs, codes, sequences, and exponential sums over Galois rings," (with P.Vijay Kumar, T. Helleseth, and O. Moreno).
105. "Rational point over curves over finite fields and new estimates on exponential sums and applications," with F. Castro.
106. "On McEliece's and Niederreiter's public key cryptosystems and their modifications," (with O. Moreno).
107. "On the generalized Hamming weights of codes," (with A. Lal).
108. "Improved bounds on the number of rational points on curves over finite fields."
109. "Using Genetic algorithms to construct good codes" (with P. Rivera).
110. "Optimal codes from graphs," (with P. Guan).

M.Sc. (Honors) Mathematics (1975–1980), Thesis

"Parameters of codes," M.Sc. (Hons.) Mathematics Thesis, BITS, June 1980. The M.Sc. (Hons.) was a five year (1975–1980) integrated Master of Science in Mathematics program.

"Software Implementation of BCH codes," Practice School Report submitted to *Software Development Division*, *Department of Electronics* (DOE), Government of India, for the work done during January–June 1981.

INVITED SPEAKER/ONE OF THE MAIN SPEAKERS

at International Conferences and Workshops not listed earlier, see for example, listings for ISIT-95, ISIT-97, AAECC-9, SCI2000/ISA2000, SIAM Mini-Syposium, AMS Annual Meetings, 2005, AMS Annual Meetings, 2008 (one hour speaker), one of main speakers in AMS Sectional Meeting, UNLV, 2011. See listed under HONORS or PUBLICATIONS; Also received invitations from several other international conferences.

Some major addresses were, **for example**:

- Invited Speaker at the International Conference On Algebraic Geometry and coding Theory (AGCT), 2013, IIT Bombay, India.
- Invited Speaker at the Prestigious Annual TIFR International Conference: 2012 Theme, "Recent Trends in Discrete Mathematics."
- Invited Speaker at the AMS Annual Sectional Meeting, UNLV, Nov. 2011
- Invited Speaker at CRYPTO-2009.
- 2010, Invited to Organize AAECC-18 in Puerto Rico
- 2010 Several talks as Scholar in Residence (awarded by Faculty Resource network)(NYU), Spring Semester
- One hour Invited Speaker at the AMS Annual Meeting, San Diego, January 2008, in *Special Session on Expander Graphs* (organized by Terras et. al)
- Invited Speaker at the AMS Annual Meeting, Atlanta, 2005, in *Special Session on Algebraic Geometry and Coding Theory* (Organized by Gao et al).
- **AAECC-9**: (*C. Traverso, H. Janwa, E. Kaltofen-Saunders, S.N. Litsyun, W.V. Vasconcelos),*
- **SIAM Conf.***:* *(V. Pless, G. Cohen, R. Brualdi, C. Huffman, H. Janwa)*
- **Conf. in Honor of Prof. Shrikhande:** *(P. Cameron, L.J. Dickey, H. Janwa, J.N. Srivastava).*

A list of main speakders at other conferences is available.

- "Expander Graphs, Codes, Sequence Designs: Their Relations and Applications," talk delivered (which was webcast) at the Microsoft Research Headquarters in Redmond, WA, on January 18, 2001, as one of the two research exchange professors representing the UPR, Rio Piedras campus.
- "New Constructions of Ramanujan Graphs and Good Expander Graphs from Codes, Exponential Sums and Sequences," (based on joint work with O. Moreno) at the 1999 IMA Summer Program on *Codes, Systems and Graphical Models* from August 01–08 at the Institute for Mathematics and its Applications, at Minnesota.

- *International Workshop on Discrete Mathematics* in honor of Prof. S.S. Shrikhande, at the University of Bombay, December 20, 1993– January 08, 1994. (Other invited speakers: Peter Cameron; D. Hughes; L.J. Dickey).
- "Some applications of invariant theory," invited lecture, *Instructional Conference on Combinatorial Topology and Algebra* (ICCTA-93), IIT Bombay, December 24, 1993. (Other invited lecturers included C. Musili and N.M. Singhi).

Other Presentations at International Conferences and Workshops

[**Majority of them invited participation**].
(Some of the talks were presented by co-authors).

A list of over 40 such talks is available.

Presentations at National Conferences and Workshops

A list of over 36 such talks is available.

Presentations at Universities Outside India

A list of at least 35 such talks is available. These were mostly delivered at the Universities listed on page 3. Most recently on August 16, at the Institute for Mathematics, DTU Denmark, 2012.

Presentations at Universities in India

A list of over 50 such talks are available. For the universities where the lectures were delivered, see page 3.

OTHER Selected Major International Conferences/Colloquia/Workshops attended, in addition to the ones given talks

- Joint Annual AMS-MAA Meetings, Washington D.C., 2009, San Diego (2008), Atlanta 2005, Maryland 2003, ...
- AAECC-18 (Spain) 2009, AAECC-17 (India) 2007, AAECC-16 (Las Vegas), 2006, ...
- GEOCRYPT09
- IMA, Minnesota, 2007.
- ISIT-2007, Nice, France.
- IAS, Princeton, 2006 (Expander Graphs)
- IPAM, UCLA, 2004 (Expander Graphs)

- Conference on Additive Number Theory, CUNY, 2004.
- Theory Day, Columbia University, 2004.
- Theory Day, Courant Institute, 2003.
- AMS Annual Meeting, Maryland, 2003
- *AAECC-13*, Hawaii, November 1999.
- *13th International Parallel Processing Symposium & 10th Symposium on Parallel and Distributed Processing,* (IPPS/SPDP) April 12-16, 1999, San Juan, PR, USA.
- International Workshop on *Discrete Mathematics* in honor of Professor S.S. Shrikhande at the University of Bombay, from December 20, 1993–January 08, 1994;
- *International Conference on Lie Groups* in honor of Professor Harish Chandra, October 10–13, 1993 at at the MRI , Allahabad.
- International Colloquium on Geometry and Analysis, TIFR, January 6–14, 1992. International Workshop on *Applications of Algebraic Geometry*, UPR (one week in January of 1990);
- Indo-USSR Conference on Geometry, TIFR, January 1991.
- International Conference on Computational Algebraic Geometry, at Cornell University, July 1988.
- Workshop on *Design Theory and Coding Theory*, IMA (two weeks in July 1988);
- International Conference on Computational Algebraic Geometry, Columbia University, 1987.
- 12th American Association for Advancement of Science (AAAS) & EPSCoR Annual Meeting, 2000; Also, 11th, 10th, 7th, AAAS & EPSCoR Conferences.
- "Ten Lectures on the proof of Fermat's Last Theorem by Wiles," given by Prof. Ram Murty at MRI, Allahabad during September–October, 1993.
- Workshop on *Elliptic Curves*, Tata Institute of Fundamental Research (TIFR), (for one week in October 1991);
- Workshop on sl_2, TIFR, June 1992;
- Month Long Summer School for National Science Talent Scholars conducted by NCERT (INDIA) at: IIT-Kharagpur (1976); IIT- Kanpur (1977); TIFR (1979); BITS, Pilani (1980).

TEACHING

UPR:

GRADUATE: (For recent courses, see http://ramanujan.uprrp.edu)

1. Spring 2008-2009
   (a) Computational Algebraic Geometry, MATH 8995;
   (b) Recent Advances in Coding Theory, MATH8990;
2. Fall 2008-2009
   (a) Enumerative Combinatorics I, MATH 8005;
   (b) Graduate Algebra I, MATH6201;
3. Spring 2007-2008
   (a) Algebraic Combinatorics, MATH 8021;
   (b) Information Theory 8995;
4. Fall 2007-2008
   (a) Linear Algebra Mate 6150;
   (b) Advanced Cryptography 8995;
5. Spring 2006-2007:
   (a) Algebra, MATH 6202;
   (b) Coding Theory, MATH 8995.
6. Fall 2006– 2007:
   (a) Linear Algebra (Graduate), Mate 6150.
   (b) Modern Algebra I (Graduate), Mate 6201
7. Spring 2005– 2006:
   (a) MATE 8021 Algebraic Combinatorics I.
   (b) MATH 8995 Information Theory.
8. Fall 2005–2006:
   (a) Linear Algebra (Graduate Course), MATH 6150
   (b) Advanced Cryptography, MATH 8995
9. Spring 2004– 2005:
   (a) MATE 8021 Algebraic Combinatorics I.

(b) MATH 8995 Information Theory and BioInformatics.

10. Fall 2004–2005:

(a) Linear Algebra (Graduate Course), MATH 6150

Sabbatical 2003—2004 The Courant Institute of Mathematical Sciences
Expander Graphs and Expander Codes (Fall 2003)
Topics on Expander Grapns and Expander Codes (Summer 2003)
Information Theory and Bioinformatics, Spring 2003–2003
Finite Dimensional Vector Spaces, Fall 2002-2003
Some Current Topics in Coding Theory and Cryptography, Spring 2001-2002
Higher Dimensional Vector Spaces, Fall 2000-2001
Topics in Coding Theory and Cryptography, Fall 2000
Introduction to Coding Theory, Summer 1999-2000 (ad honorarium)
Topics in Coding Theory, (Independent Study, Fall 1999)
Data Structures I (Fall Semester, 1998-99).
Modern Algebra I (Fall Semester, 1997–98).

UNDERGRADUATE: (For recent Courses, see http://ramanujan.uprrp.edu)
Artificial Intelligence,
Cryptography and Computer Security, Spring 2002-2003
Parallel and Distributed Computing, Fall 2002-2003
Compiler Construction (Grad. and Undergrad. Students, Fall '97, Spring '99, Fall '2000, Spring 2003)
Theory of Computation (Spring 1997-1998, 1998–1999, 1999–200, 2000-2001)
Cryptography and Data Security, (*Fall 1999-20000*)
Parallel Computation, Spring 1999-2000
Higher Level Programming Languages: Java (Fall, 1998–99, Fall 1999-2000)
Statistics with Computers, (Summer, 1998).
Precalculus (Second Semester 1997-98)
Topics in Complexity Theory, (John Ramirez, Fall 1994.)
Artificial Intelligence, (James Irrizary, 1999)
Topics in Design and Analysis of Algorithms (Jaime Rosa, Fall 2000)

MRI:

GRADUATE:
Topics in Coding Theory, Second Semester, 1995–96.
Algebra (Fall 1993–94);
Function Fields and Codes (Reading Course, Fall 1994) and
Algebraic Geometry and Coding Theory, (Second Semester, 1994),
(Brajesh Kumar, Ph.D. Student)

BOMBAY UNIVERSITY
(Center for Advanced Studies in Mathematics):

M.Phil.

Commutative Algebra (One year M.Phil course, Univ. of Bombay, 1991–92);
Commutative Algebra (Reading Course, two Semesters 1992)

GRADUATE

Numerical Analysis (Univ. of Bombay, one year, 1991–92);

TIFR:

Organized regular research seminars in algebraic geometry and coding theory and presented 6 seminars

MSU:

GRADUATE

Numerical Analysis (MSU, one Term 1990)

UNDERGRADUATE

Three Semesters of Numerical Analysis and 2 Semesters of Calculus.

CALTECH:

GRADUATE:

Combinatorial Analysis, (full year course during 1987–88) (Text: Marshall Hall)
Algebraic Geometry (full year course, during 1988–89), *Text: Algebraic Geometry, by Hartshorne), finished about 75 percent of the text*, plus topics from Algebraic Geometric Codes.

UNDERGRADUATE:

- Huy T. Cao: *Implementation of Coding Theoretic Algorithms on Hypercubes*, Spring and Summer, 1988.
- Elizabeth Wilmer (from Harvard); *Elliptic Curve Cryptosystems*, Summer 1987.

COURANT INSTITUTE:

6 Lectures in the Seminar Series on Computational Algebraic Geometry

SYRACUSE UNIVERSITY:

Teaching assistant in several graduate and undergraduate courses during 1982–86.

Professional Experience I:

LECTURE SERIES

The highlights are:

- One of the main invited lecturers for *UGC*, India, sponsored, refresher courses for college teachers at: I) The Delhi University; II) Bombay University; III) Poona University.
- Organized weekly seminars on coding theory, cryptography and algebraic geometry at TIFR; Bombay University; and MRI. Furthermore, I presented series of lectures in these seminars such as

  Algebraic geometric codes; algebraic geometry over finite fields and Applications (bounds of Weil, Serre, Oesterle and Deligne; Drienfeld modular curves; class field towers; Ramanujan Graphs from quaternion algebras, character sums, and codes; codes, curves and lattices;
- Gave a total of ten seminars at MSU in the seminar groups in *Combinatorics*; *Commutative Algebra*; and *Group Theory.*
- Gave several seminars at CALTECH in the seminar groups in *Combinatorics*, *Algebraic Number Theory and Algebraic Geometry*, and *Information Theory.*
- At CIMS (NYU, 1986-87) Participated in Computational Algebraic Geometry seminars/Computational Number Theory Seminar (Jointly between CISM and CUNY).

Professional Experience II:

A. COMMITTEE WORK

(I have been on a dozen Ph.D. Qualifying exam Committees, and perhaps two dozen M.S. Qualifying Exam Committees), several placement exam committees, etc.)

UPR-Rio Piedras (1997——)

- Member UPR Academic Senate 2012—— (Also Member of Senate Faculty Affairs Committee (2012—-; Member of Revision of Rules of UPR Committee Representing Faculty Affairs Committee;
- Dean Search Committee for the College of Natural Sciences, 2014.
- Committee to recommend a new Chair for the Department [May 2000—May 2001 (completed)]. My election to that committee was extra-ordinary in that I had been in the department for less than three years.
- Graduate Committee, May 2001 (?)——2006

- Curriculum Committee [Elected in August 2000—] The task has been a major overhaul of the Undergraduate Program with several degree options. Another major task is to recommend a re-conceptualization of the undergraduate curriculum. The main task is to recommend a re-conceptualization of the undergraduate curriculum.
- Ph.D. Committee for Discrete Mathematics Option (1997—-)
- Ph.D. Committee for Computational Mathematics Option (1997—)
- Committee "para enlace SIDIM" (Elected February 1999; Served until February 2000).
- Faculty committee participating in the Undergraduate CS program (1997—)
- Dean's Committee for Computational Science Research in UPR-Rio Piedras Committee (1998—1999).
- Possible collaboration between UPR Mayaguez and UPR Rio Piedras campuses for an inter-campus Ph.D. program involving several departments and several campuses.(1997—-)
- Committee for Ph.D. program in CS at UPR-Rio Piedras (Fall 2000—-).

MRI ((1992—1999); (On sabbatical **'97–98**; on leave. **'98–99'**)

- Member of the core faculty for the NBHM Nurture Program for 1996–2000 (for the 1996 batch) (on leave 1997–99).
- National level committee to link libraries in the DAE system (see page 2).
- Main Coordinator for national level Joint Written Screening Test (JWST) coordinated by MRI (for MRI/IMSC/SINP) 1995-96);
- Computer Committee, MRI, January 1993—– August 1996 (Convener for one year).

University of Bombay (January 1991–October 1992):

- Member of the Computer committee at the University of Bombay, February 1991–1992.
- Several other committees.

SU (1982–6):
Graduate Student Representative on School of CIS, Tenure Committee, SU, 1983-84.

B. EXTERNAL EXAMINER

(Also, was nominated Ph.D. Examiner for Ph.D. students at IIT Kanpur, IIT Madras, and Poona University.)

1. Oral Defense of the Ph.D. of Mr. (Dr.) M. S. Garg at IIT Kanpur.

2. Ph.D. Examiner for Mr. (Dr.) N. Madhusudan, Dept. of Elect. Engg., IIT Kanpur.
3. Preliminary Examination of Ph.D. of Mr. Tony Lee at CALTECH, 1989.

C. STUDENTS

CURRENT Ph.D. STUDENTS:

Dioniso Perez Montes, 2011—-

Julian Rodriguez, 2013—

Roberto Reyes, 2012——

Juan Carlos Orosco, 2013——

PAST Ph.D. STUDENTS:

1. Hu Qin (Ph.D. May 2016) (Jointly Supervised)
2. Moises Delgado (Ph.D., 2008—, 2009–2010 (supported by DEGI-FIPI grant) (Graduated with Ph.S., May 2012)
3. Carlos Beltran(Ph.D., 2006—->2009(supported by DEGI+NSF-STEM grants)
4. Dionisio Perez Montes, NSF-IGERT Program in the Environmental Sciences, 2009—-
5. Fernando Pinero (M.S. —->Ph.D., 2006—) (supported by NSF Fellowship 2006–2008), NASA Fellowship 2008–2009 and 2009-2010.
6. Wanda Vasquez (M.S.–>Ph.D., 2009—). Supported by DEGI+NSF-STEM grants; 2009-2010 by a NASA Fellowship.
7. Haydee Guzman (M.S.—>Ph.D.) Supported by NSF Fellowships.
8. Rafael Del Valle (M.S.) (2006—-) Supported by DEGI-FIPI and NSF-STEM)
9. Ms. Guo Qi, January 2002— (Graduate Student.); M.S., April, 2004 (expected). Trained under NSF grant
10. Dachun Huang, M.S. Student (M.S., May 2003). Trained under NSF grant
11. Humberto Ortiz (working on genomics), now registered under the inter-campus Ph.D. program between UPR-Rio Piedras and UPR-Mayaguez. (2000-2001; cosupervision 2001-2002).
12. B. K. Sharma (Ph.D. student at MRI, since April 1996—)
13. I contributed, in varying extent, to the supervisions during the completion of Ph.D. Dissertations of M.S. Garg at IIT Kanpur, Dan Ashlok at CALTECH, Gary McGuire at CALTECH, and Nivedita Jain at Poona University.

POST-DOCS:

1. M.K. Garg (Ph.D. IIT Kanpur), 2003–2004 at MRI.
2. Arbind Kumar lal(Ph.D. from ISI Delhi) 2003–2006 at MRI.

CURRENT RESEARCH STUDENTS:

1. Carlos Beltran, Ph.D., 2006— (Supported by UPR-FIPI grant,2006–2007, NSF-STEM+RA, 2007–2008, NSF-STEM+UPR- DEGI Grant, 2008–2009))

2. Fernando, M.S. (Ph.D.—->) 2006—(2006–2008, NSF-PRLSAMP Fellow, 2008-2009, NASA Fellow)
3. Rafael Del Valle, M.S. (—->Ph.D.), 2006—- (Supported by UPR-FIPI grant,2006–2007, NSF-STEM+RA, 2007–2008, NSF-STEM+UPR- DEGI Grant, 2008–2009))
4. Wanda Vasquez, M.S. (—>Ph.D.) 2008— (Supported by UPRRP-DEGI Grant).
5. Haydee Guzman, M.S. (—->Ph.D.), 2008—- (Supported by NSF-PRLSAMP Fellowship).

OTHER STUDENTS:
Supervised several other undergraduate and graduate students on various research projects. Current Undergraduate Research students: Daniel Ayalla and Jose Lugo.

D. OTHER PROFESSIONAL ACTIVITIES AND SERVICES

REFEREEING

- IEEE Transactions on Information Theory;
- IEEE Transactions on Computer;
- European Journal of Combinatorics;
- Journal of Combinatorial Theory;
- Designs, Codes and Cryptography;
- Discrete Applied Mathematics;
- SIAM Journal on Discrete Mathematics;
- AAECC (Springer);
- Finite Fields and Their Applications;
- Proceedings of the Indian Academy of Sciences (Mathematical Sciences), Bangalore,
- Proceedings of the Indian Academy of Sciences, Allahabad;
- Calcutta Mathematical Society; Refereed Proposals for NBHM;
- Proceedings of AAECC-8, AAECC-9, AAECC-10, AAECC-11;
- IEEE Information Theory Symposium;
- Bombay Mathematical Colloquium;

REVIEWER FOR FUNDING AGENCIES

- NSF
- Department of Science and Technology (DST), India, *(A large proposal to establish an Institute)*
- National Board for Higher Mathematics (India)
- Council of Science and Industrial Research (India): One of the proposal was to establish a *RESEARCH INSTITUTE FOR DISCRETE MATHEMATICS* in India.

Books Referee:
Refereed a book in the Mathematics Series, Hindustan Publishers, editor Prof. Bhatia,

Chaired sessions at several conferences

Membership in Professional Societies:

(a) **AMS [(1983–91), 1998—]**
IEEE (Information Theory (1982–90, 1999–));
(b) IEEE (Computers 1999–).
(c) ACM, 20000—-
(d) SIAM, 20000-
(e) MAA (1987–90).

Professional Experience III

:

PRACTICAL EXPERIENCE IN THE AREA OF COMPUTATIONAL SCIENCES

1) Have taught graduate and undergraduate courses in Computer Sciences and Related Subjects and have been assistant in such courses for over twenty years at prestigious universities, as listed above.
2) Six months training in the *Software Development Division* of *Department of Electronics* (DOE), New Delhi, January–June, 1981 as a Practice School Program of BITS, Pilani.
3) Systems Administrator for the MRI computer systems (November 1992–);
4) In-charge of MRI email system (February 1993–);
5) Computer Committee, MRI (November 1992–; Convener for one year;
6) Computer Committee (Department of Mathematics, University of Bombay) 1990–1992;
7) I have done extensive programming in **APL, C, Java, MATHEMATICA** and **FORTRAN** in research; Some experience with **C++** and **PROLOG**. extensively used **UNIX** operating system; Also quite familiar with **VMS, DOS**, and **Mac** operating systems;
8) Used extensively in research: **Connection Machines** and **Hypercubes** (at CALTECH, UCLA and Argonne National Lab); worked with **PARAGON** at UPR; Working with Silicon Graphics Parallel Machine at UPR. Can program in **MPI**. Familiar with **PVM** and **CILK.** some experience with **AXIOM**, **Macaulay, GAP, GUAVA, PARI**;

8) Extensively used **MATHEMATICA, MATLAB and MINITAB** in teaching; Currently developing Genetic Algorithms for Coding Theoretic applications and implementing data structures and algorithms in **C** and **C++**;
9) extensive experience with **TeX, LaTeX and AMSTeX** during the past five to seven years; Some experience with **CHIWriter and WP**.

Professional experience IV

Multi-Disciplinary Graduate Course Work

In addition to the many courses in pertinent disciplines, e.g., for B.E. (Honors) in EEE at BITS ('78–81), for the five year M.Sc. (honors) in Mathematics, for graduate studies in Mathematics at UIUC, and Ph.D. course work at SU ('82-86).

In all the programs, I took over **40** graduate courses at all these universities in my research interest listed on page 4.

Some of these courses were quite interdisciplinary, such as:
Methods of Mathematical Physics I, II
Optimization Techniques
Control Theory and Modeling
I also taught many graduate and undergraduate courses listed earlier.

LANGUAGES

ENGLISH: The language of instruction and communication for twenty years
SPANISH: Continuing education courses at UPR [Fall 1994, Fall 1997, Summer 1999, Fall 2000]
[Residence in PR, 1997—-.]
Visits [1990, 1991, 1992, 1993, 1994-95].
FRENCH: Introductory course at NYU;
GERMAN: Can read mathematical and CS papers in German.
HINDI: Mother tongue (11 years in school)
SANSKRIT: Five years in High School

SOME CITATIONS BY OTHER AUTHORS

Total Citations by other researchers: Quick google count gives over thousand—- (and scores in Books and Ph.D. dissertations.)