

Curriculum Vitae for Jon-Lark Kim

January 24, 2007

Department of Mathematics
328 Natural Sciences Building
University of Louisville
Louisville, KY 40292, U.S.A.

Phone : (502) 852-2727
Fax : (502) 852-7132
email : jl.kim@louisville.edu
<http://www.math.louisville.edu/~jlkim>

A. Areas of Main Interest:

- [1] Discrete Math/Combinatorics with applications to algebraic coding theory
- [2] Number theory with applications to cryptography

B. Education:

2002	PhD	mathematics	University of Illinois–Chicago
		thesis title	Construction of new self-dual codes and quantum codes and their connections
		thesis advisor	Professor Vera Pless
1997	MS	mathematics	Seoul National University, S. Korea
1993	BS	mathematics	Pohang University of Science and Technology, S. Korea

C. Professional Experiences:

8/2005 – present	Assistant Professor	University of Louisville, KY
8/2002 - 8/2005	Research Assistant Professor	University of Nebraska–Lincoln
	post doctoral advisor	Professor Judy Walker
1/2002 – 5/2002	Instructor	University of Illinois–Chicago
8/1998 – 12/2001	Teaching Assistant/University Fellow	University of Illinois–Chicago
3/1998 – 6/1998	Part time instructor	Dongyang Technical College, Korea
9/1996 – 12/1996	Teaching Assistant	Seoul National University
9/1994 – 3/1996	Soldier	Military service in Navy, Korea
3/1993 – 6/1994	Teaching Assistant	Seoul National University

D. Research Trips:

5/2005 – 7/2005	Visiting Researcher	Korea Institute for Advanced Study
	local host	Dr. Eunjeong Lee
7/2004 – 8/2004	Visiting Assistant Professor	Pohang Univ. of Sci. & Tech., Korea
	local host	Professor Hyun Kwang Kim
6/9/2003 – 7/9/2003	Visiting Researcher	Ghent University, Belgium
	local host	Professor Leo Storme
6/2000 – 8/2000	Visiting Research Fellow	Pohang Univ. of Sci. & Tech., Korea
	local host	Professor Hyun Kwang Kim

E. Research Papers:**a. Refereed Journal Papers:**

- [1] J.-L. Kim, K.E. Mellinger, and L. Storme, Small weight codewords in LDPC codes defined by (dual) classical generalized quadrangles, *Designs, Codes and Cryptography*, 42 (2007), 73-92.
- [2] S.T. Dougherty, J.-L. Kim, and P. Sole, Double circulant codes from two class association schemes, *Advances in Mathematics of Communication*, 1 (2007), 45-64.
- [3] E.P. Bautista, P. Gaborit, J.-L. Kim, and J.L. Walker, s-extremal Additive F_4 codes, *Advances in Mathematics of Communication*, 1 (2007), 111-130.
- [4] J.-L. Kim and Y. Lee, Euclidean and Hermitian self-dual MDS codes over large finite fields, *J. Combinatorial Theory, Ser. A*, Vol. 105 (2004) pp. 79-95.
- [5] J.-L. Kim, U.N. Peled, I. Perepelitsa, V. Pless and S. Friedland, Explicit construction of families of LDPC codes with no 4-cycles, *IEEE Trans. Inform. Theory*, Vol. 50, No. 10 (2004), pp. 2378- 2388.
- [6] T.A. Gulliver and J.-L. Kim, Circulant based extremal additive self-dual codes over $GF(4)$, *IEEE Trans. Inform. Theory*, Vol. 50, No. 2 (2004), pp 359-366 .
- [7] J.-L. Kim, K. Mellinger and V. Pless, Projections of binary linear codes onto larger fields, *SIAM journal on Discrete Math*, Vol. 16, No. 4 (2003), pp. 591-603.
- [8] J.-L. Kim and V. Pless, Designs in additive codes over $GF(4)$, *Designs, Codes and Cryptography*, Vol. 30 (2003), pp. 187-199.
- [9] P. Gaborit, J.-L. Kim, and V. Pless, Decoding binary $R(2, 5)$ by hand, a special issue on Com²Mac Conference on Association Schemes, Codes and Designs, Pohang, Korea, 7/3 - 7/7, 2000, *Discrete Math*. Vol. 264 (2003), pp. 55-73.
- [10] T. A. Gulliver, M. Harada, and J.-L. Kim, Construction of some extremal self-dual codes, *Discrete Math*, Vol. 263 (2003), pp. 81-91.
- [11] J.-L. Kim, New self-dual codes over $GF(4)$ with the highest known minimum weights, *IEEE Trans. Inform. Theory*, Vol. 47 (2001), pp. 1575-1580.
- [12] J.-L. Kim, New extremal self-dual codes of lengths 36,38, and 58, *IEEE Trans. Inform. Theory*, Vol. 47 (2001), pp. 386-393.
- [13] J.-L. Kim, Relation between weight distribution and combinatorial identities, *Bulletin of the Institute of Combinatorics and its Application*, Canada, Vol. 31 (2001), pp. 69-79.

b. Accepted Papers:

- [14] J.-L. Kim and V. Pless, A note on formally self-dual even codes of length divisible by 8, to appear in *Finite Fields and Their Applications*, (accepted in Sep. 2005).

c. Conference Proceedings (refereed):

- [15] E. P. Bautista, P. Gaborit, J.-L. Kim, and J. L. Walker, s -Extremal additive codes over $GF(4)$, *IEEE International Symposium on Information Theory*, Seattle, July 2006, 1296-1300.
- [16] J.-L. Kim, New quantum error correcting codes from Hermitian self-orthogonal codes over $GF(4)$, *Proc. of the 6th International conference on Finite fields and applications*, at Oaxaca, Mexico, May 21 - 25, 2001, Springer Verlag (2002), pp. 209-213.
- [17] J.-L. Kim and V. Pless, Decoding some doubly-even self-dual $[32, 16, 8]$ codes by hand, *Codes and Designs : Proc. of a conference honoring Professor Dijen K. Ray-Chaudhuri, (Columbus, OH, 2000)*, Ohio State University Math. Resear. Inst. Publ., 10, *de Gruyter*, Berlin, (2002), pp. 165-178.
- [18] P. Gaborit, W. C. Huffman, J.-L. Kim and V. Pless, On additive $GF(4)$ codes, *DIMACS Workshop on Codes and Association Schemes*, DIMACS Series in Discrete Math. and Theoret. Computer Science, Amer. Math. Soc., Vol. 56 (2001), pp. 135-149.
- [19] J.-L. Kim, U.N. Peled, I. Perepelitsa, V. Pless and S. Friendland, Explicit construction of families of LDPC codes with no 4-cycles, *Proc. of 2004 IEEE International Symposium on Information Theory*, Chicago, USA, June 27-July 2 (2004), pp. 235.
- [20] J.-L. Kim and Y. Lee, MDS self-dual codes, *Proc. of 2004 IEEE International Symposium on Information Theory*, Chicago, USA, June 27-July 2 (2004), pp. 526.
- [21] T.A. Gulliver and J.-L. Kim, Classification of circulant and 4-circulant extremal additive self-dual codes, *Proc. of 2002 IEEE International Symposium on Information Theory*, Lausanne, Switzerland, June 30-July 5 (2002), pp. 457.
- [22] P. Gaborit, J.-L. Kim and V. Pless, Decoding binary $R(2, 5)$ by hand and by machine, *Proc. of 2001 IEEE International Symposium on Information Theory*, Washington, D.C., June 24-29 (2001), pp. 86.
- [23] J.-L. Kim, New good Hermitian self-dual codes over $GF(4)$, *Proc of 2001 IEEE International Symposium on Information Theory*, Washington, D.C., June 24-29 (2001), pp. 177.

d. Conference Proceedings (invited papers):

- [24] J.-L. Kim, Dual cyclic codes with two zeros, *Proceedings of the 40th Allerton Conference on Communication, Control and Computing*, Univ. of Illi. at Urbana-Champaign, IL, (2002), pp. 1017-1023.
- [25] J.-L. Kim, U. L. Peled, I. Perepelitsa, and V. Pless, Explicit construction of families of LDPC codes with girth at least six, *Proceedings of the 40th Allerton Conference on Communication, Control and Computing*, Univ. of Illi. at Urbana-Champaign, IL., (2002), 1024-1031.

- [26] J.-L. Kim and V. Pless, Designs in additive codes over $\text{GF}(4)$, *Proceedings of the 38th Annual Allerton Conference on Communication, Control and Computing*, UIUC, Oct. 4-6, (2000), pp. 1010-1018.
- [27] P. Gaborit, W. C. Huffman, J.-L. Kim and V. Pless, On the classification of extremal additive codes over $\text{GF}(4)$, *Proceedings of the 37th Allerton Conference on Communication, Control and Computing*, Univ. of Illi. at Urbana-Champaign, IL., Sep. (1999), pp. 535-544.

e. Preprints:

- [25] J.-L. Kim and Leo Storme, A combinatorial construction of low-density parity-check codes, Nov. 28, 2003.
- [26] J.-L. Kim, Codes constructed from non-symmetric association schemes, Dec. 1997.

f. Submitted Article:

- [27] T. A. Gulliver, J.-L. Kim and Yoonjin Lee New MDS or near-MDS self-dual codes, submitted, Dec. 4, 2006.
- [28] J.-L. Kim and J.L. Walker, Nonbinary quantum error-correcting codes from algebraic curves, submitted to *Discrete Math*, as a special issue of Com²MaC Conference on Association Schemes, Codes and Designs, Pusan, Korea, July 2004
- [29] H. K. Kim, D. K. Kim, and J.-L. Kim, Euclidean Type I codes over $\text{GF}(4)$, submitted, June 3, 2006.

g. Papers in Preparation:

- [1] Remarks on s -extremal self-dual codes.

F. Awards/Fellowships/Nominations:

- [1] 3/2005 : 2004 Kirkman medal, Institute of Combinatorics and its Applications (ICA), Winnipeg, Canada (the medal recognizes outstanding work by ICA members in their early research careers), Bulletin of ICA, Vol 44, May 2005.
- [2] 6/2004 : Travel award, IEEE Inform. Theory Society, Piscataway, NJ.
- [3] 2002/2003 : Leitzel Project NExT Fellow awarded by the Mathematical Association of America.
- [4] 2002 : Nomination for a Clay 2002 Liftoff Fellow by Department of Mathematics, Stat, & Computer Science, University of Illinois-Chicago (only one nominated).
- [5] 2001 : Nomination for Provost award by Department of Mathematics, Stat, & Computer Science, University of Illinois-Chicago (only one nominated).

- [6] 2000/2001 : University Fellowship (university-wide competition), Graduate College, University of Illinois-Chicago.
- [7] Spring, 2000 : TA teaching award from Department of Mathematics, Stat, & Computer Science, University of Illinois-Chicago.
- [8] 6/2001 : Travel award, IEEE Inform. Theory Society, Piscataway, NJ.
- [9] 9/30 - 10/8, 2000 : Travel award from Yamagata University, Japan.
- [10] 3/11 - 3/15, 2000 : Travel scholarship, Winter School 2000, University of Arizona, Tucson.

G. List of Presentations: (* marked for invited talks)

2007

- [1*] 1/5 - 1/8, 07 : Joint Mathematics meeting, New Orleans, LA, “Skew Hadamard Designs and Their Codes”.

2006

- [1*] 10/21, 06 : AMS sectional meeting, Cincinnati, OH “Optimal subcodes of self-dual codes.
- [2] 7/1-7/2, 06: A *Mini Workshop on Coding Theory* at Pohang Univ. of Sci. and Tech., “Quadratic double circulant codes and their generalization”.
- [3] 7/9-7/14, 06: IEEE International Symp. Information Theory, Seattle, “ s -extremal additive codes over $GF(4)$.”
- [4] 6/26- 6/30, 06: Algebraic Combinatorics, An International Conference in Honour of Eiichi Bannais 60th Birthday, “Small weight codewords in LDPC codes defined by (dual) classical generalized quadrangles”
- [5*] 2/6, 06 : The math department talk at Clemson University, Clemson, SC, “Capacity-approaching low-density parity-check codes”.

2005

- [1*] 11/1, 05 : Algebra-Combinatorics-Number Theory seminar, University of Louisville, “Some open problems on formally self-dual codes”.
- [2*] 5/26, 05 : Number Theory Seminar, Korea Institute for Advanced Study, “Capacity-approaching low-density parity-check codes”.
- [3*] 4/2 - 4/3, 05 : The 2005 AMS sectional meeting, Special Session on Designs, Codes, and Geometries, University of Delaware, “LDPC codes from geometries”.
- [4*] 2/25, 05 The math department talk at the Georgia State University, Atlanta, “Two constructions of low-density parity-check codes”.

- [5*] 2/21, 05 The talk for undergraduate students at the SUNY at Brockport, “Application of graphs to error-correcting codes”.
- [6*] 2/14, 05 The math department talk at the University of Missouri, Kansas City, “A journey to error-correcting codes”.
- [7*] 2/11, 05 The math department talk at the University of Louisville, “Two constructions of low-density parity-check codes”.
- [8*] 1/5 - 1/8, 05 Joint Mathematics Meeting, SIAM Minisymposium on Error-Correcting Codes, Atlanta, “Algebraic or combinatorial constructions of LDPC codes”.

2004

- [1*] 10/23 - 10/24, 04 : The 2004 AMS sectional meeting, Special session on Codes and Applications, Evanston, IL, “Formally self-dual even codes of length divisible by 8”.
- [2*] 7/19 - 7/23, 04 : The 2004 Com²MaC Conference on Association Schemes, Codes, and Designs at Pusan National University, Korea, “Nonbinary quantum error-correcting codes from algebraic curves”.
- [3] 6/27 - 7/2, 04 : The 2004 IEEE International Symposium on Information Theory at Chicago Downtown, IL, “MDS self-dual code”.
- [4*] 6/8 - 6/26, 04 : The 2004 IMA PI Summer Program for Graduate Students on Coding and Cryptography at the University of Notre Dame, “Construction of LDPC codes”.
- [5*] 5/13 - 5/15, 04 : Joint AMS-SMM International Meeting, Special Session on Coding Theory and Cryptography at Houston, TX, “LDPC codes and their constructions”.
- [6*] 3/23, 04 The math department talk at the Florida Atlantic University at Boca Raton.
- [7*] 3/5, 04 The Rocky Mountain Algebraic Combinatorics Seminar, Colorado State University, Fort Collins
- [8*] 2/23, 04 The math department talk at the Wright State University at Dayton.
- [9*] 2/19, 04 The math department talk at the University of Wyoming at Laramie.
- [10*] 2/17, 04 The math department talk at the WPI (Worcester Polytechnic Institute) and a talk for undergraduate students titled “What color is my hat?”.
- [11*] 2/7, 04 The math department talk at the University of Virginia at Charlottesville.

2003

- [1] 11/7 - 11/9, 03 : The Workshop on the Mathematics of Public-Key Cryptography, at the University of Illinois-Chicago, IL., “Code-based public-key cryptosystems”.
- [2*] 10/23, 03 : The 2003 Fall department colloquium, at the University of Nebraska, Lincoln, NE., “Codes, graphs, and generalized polygons”.

- [3] 10/15, 03 : The *coding theory seminar*, at the University of Nebraska, Lincoln, NE., “MDS self-dual codes”.
- [4*] 10/2 - 10/4, 03 : The *2003 AMS sectional meeting*, at the University of Colorado, Boulder, CO., “Nonbinary quantum error-correcting codes from algebraic curves”.
- [5] 5/20 - 5/24, 03 : The *Conference and Workshop on Coding theory and Quantum Computing* at the University of Virginia, Charlottesville, “Nonbinary quantum error-correcting codes from algebraic curves”.
- [6] 5/5 - 5/9, 03 : The *7th Conference on Finite Fields and Applications*, Toulouse, France, “Projections of binary linear codes onto larger fields”.
- [7*] 4/14, 03 : A *Special Mathematics Lecture*, One hour talk at the department of Mathematics, Smith College, “Codes on graphs”.
- [8*] 1/6 - 1/7, 03 : A *Mini Workshop on Coding Theory* at Pohang Univ. of Sci. and Tech., “Codes on graphs” and “Cyclic codes and exponential sums”.

2002

- [1] 11/2002 : *Mathematical Landscapes seminar*, for the first-year graduate students, University of Nebraska-Lincoln, “Perspectives : Discrete Math”.
- [2] 10/2002 : *Quantum coding seminar*, University of Nebraska-Lincoln, “Classification of additive self-dual quantum codes”.
- [3*] 10/2 - 10/4, 02 : *the 40th Allerton Conference on Communication, Control and Computing*, invited speaker, Univ. of Illi. at Urbana-Champaign, IL, “Dual cyclic codes with two zeros”.
- [4*] 4/2002 : *Combinatorics/Algebra seminar*, Iowa State University, invited speaker, “Application of exponential sums to coding theory”.

2001

- [1] 10, 2001 : *Coding seminar*, University of Illinois, Chicago, “Quantum error correcting codes”.
- [2*] 9/21- 9/23, 2001 : *2001 AMS sectional meeting on Codes and Designs*, invited speaker, Columbus, OH, “Assmus-Mattson theorem on additive codes over $\text{GF}(4)$ ”.
- [3] 6/24 - 6/29, 2001 : *2001 IEEE International Symposium on Information Theory*, Washington, D.C., “New good Hermitian self-dual codes over $\text{GF}(4)$ ”.
- [4] 5/21 - 5/25, 2001 : *the Sixth International Conference on Finite Fields and Applications*, Oaxaca, Mexico, “New self-dual codes over $\text{GF}(4)$ with the highest known minimum weights”.

2000

- [1] 10/5 - 10/8, 2000 : *International workshop on combinatorics, 12th Franco-Japanese conference*, Yamagata, Japan, “New extremal type I codes over $\text{GF}(4)$ ”.
- [2*] 10/2 - 10/4, 2000 : *International workshop on Codes, Lattices, Modular forms, and VOA*, invited speaker at Yamagata, Japan, “Additive self-dual codes over $\text{GF}(4)$ and lattices”.
- [3*] 7/3 - 7/7, 2000 : *Com²Mac Conference on Association Schemes, Codes and Designs*, Pohang, Korea, invited speaker “A method to build up binary self-dual codes”.
- [4] 5/18 - 5/21, 2000 : *The XXVth Ohio State-Denison conference*, Ohio State University, “New extremal self-dual codes of lengths 36,38, and 38”.

H. Referee/Reviewer:

- [1] Referee for journals (number of times) : **(a)** IEEE Transactions on Information Theory (7), **(b)** the SIAM journal on Discrete Math (2), **(c)** Ars Combinatoria (2), **(d)** Discrete Math (1), **(e)** Designs, Codes, and Cryptography (3), **(f)** Journal of Combinatorial Theory, Ser. A (1), **(g)** J. of Pure and Applied Math (1), **(h)** Finite Fields and Their Applications (1), **(i)** Discrete Applied Math (1), **(j)** Advances in Mathematics of Communication (2), **(k)** Graphs and Combinatorics (1), **(l)** Math Magazine (1)
- [2] Referee for conferences : (a) 2001 Proceedings of the Louisiana / Mississippi section of the Math. Assoc. of Amer., (b) 2004 IEEE International Symposium on Information Theory at Chicago, (c) the Workshop on “Coding and Cryptography” organized by MIRIAM, (d) ICC 2005 - IEEE International Conference on Communication - in Seoul, (e) 16th AAEECC Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes.
- [3] Reviewer for AMS Mathematical Reviews (15 times) and the Encyclopedia of Information Systems (Academic Press).

I. Academic Membership: American Mathematical Society, Institute of Electrical and Electronics Engineers (Member), and Institute of Combinatorics and its Applications (Associate Fellow).

J. Other Academic Activities: (a) Participate for the Algebra-Combinatorics-Number Theory seminar (since Fall, 2005) at U. of Louisville (b) Serve as a senior mentor at 2004 IMA PI Summer Program for Graduate Students on Coding and Cryptography (June 8-26, 2004). (c) Organize coding theory seminar at U. of Nebraska (9/2003 - 5/2005) and an informal cryptography seminar with four graduate students (Fall, 2003).

K. Internal Grants: (a) Research Initiation Grant (\$870) Jan. 1 – Dec. 31, 2006, University of Louisville (b) Competitive Enhancement Grant (\$2750) Jan. 1 – Dec. 31, 2007, University of Louisville.

L. Taught Courses:

Undergraduate Courses:	Elementary Algebra	TA at UIC (1998)
	Calculus I, II	TA at UIC (1999-2000)
	Business Mathematics	TA at UIC (2001)
	Calculus III	Instructor at UIC (2002)
	Linear Algebra, Calculus III	UNL (2002-2003)
	Contemporary Math	UNL, Spring (2003)
	Graph Theory, Calculus III (<i>Intro. to Graph Theory by West</i>)	UNL, Spring (2004)
	Linear Algebra, Cal II (big class)	UNL, Fall (2004)
	Calculus I	U. of Louisville, Fall (2005)
	Calculus I	U. of Louisville, Spring (2006)
	Calculus II	U. of Louisville, Fall (2006)
	Calculus I	U. of Louisville, Spring (2007)
	-----	-----
Graduate Courses:	Number Theory/Cryptography	UNL, Summer (2003)
	Combinatorics (<i>Textbook : Combinatorics</i> <i>by Peter J. Cameron</i>)	UNL, Fall (2003)
	Coding Theory (reading course)	UNL, Spring (2003)
	Elliptic Curves (reading course)	UNL, Spring (2004)
	Modern Algebra I	U. of Louisville, Spring (2006)
	Modern Algebra I	U. of Louisville, Fall (2006)
	Modern Algebra II	U. of Louisville, Spring (2007)

M. Courses I can teach:

Undergraduate Courses:	Calculus, Differential Equations, Linear Algebra, Discrete Math, Abstract Algebra, Number Theory, and other upper courses
Graduate Courses:	Coding Theory, Cryptography, Abstract Algebra, Number Theory, Combinatorics, Graph Theory, and other related courses

N. References:

- [1] Dr. Alexander Barg, Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742, (301) 405-7135, abarg@ieee.org
- [2] Dr. William Cary Huffman, Department of Mathematics and Statistics, Loyola University, Chicago, IL, 60626, (773) 508-3563, wch@math.luc.edu
- [3] Dr. Vera Pless, Department of Mathematics, Statistics, and Computer Science, University of Illinois-Chicago, Chicago, IL 60607, (312) 413-2117, pless@math.uic.edu
- [4] Dr. Patrick S ole, CNRS-I3S, ESSI, BP 145, Route des Colles 06 903 Sophia-Antipolis France, ps@essi.fr
- [5] Dr. Judy Walker, Department of Mathematics, University of Nebraska-Lincoln, Lincoln, NE, 68505, (402) 472-1628, jwalker@math.unl.edu