Curriculum Vitae

Yoonjin Lee

Department of Mathematics
Ewha Womans University
11-1 Daehyun-Dong, Seodaemun-Gu
Seoul, 120-750, S. Korea

Tel: 82-2-3277-6653
Fax: 82-2-3277-2289
E-mail: yoonjinl@ewha.ac.kr

Education

Ph.D. in Mathematics, Brown University, USA, 1999.
Sc.M. in Mathematics, Brown University, USA, 1996.
Sc.M. in Mathematics, Ewha Womans University, S. Korea, 1994.
B.S. in Mathematics Education, Ewha Womans University, S. Korea, 1992.

Honors and Awards

Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology 2019-2025 (Grant No. 2019R1A6A1A11051177).

Award for the S-OIL Excellent Research Paper, awarded by KAST (*The Korean Academy of Science and Technology), 2018.*

Leader of BK21 PLUS research team – "Mathematical Science Team for Global Woman Leaders" awarded by *the National Research Foundation of Korea* (2013-2020).

NRF Research Grant, March 1, 2017 - Feb. 28, 2022, awarded by *the National Research Foundation of Korea* (NRF-2017R1A2B2004574). (Jung-Gyun Haik-Shim (Mid-career core grant), five year grant)

NRF Research Grant, May 1, 2015 - April 30, 2017, awarded by *the National Research Foundation of Korea.* (Jung-Gyun Haik-Shim, three year grant)

Priority Research Centers Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2009-0093827), 9/1/2009-8/31/2018 (nine year grant).

LG Research Grant Award for visiting abroad faculty awarded by *L.G. YONAM Foundation*, June 18, 2012.

Grant for the Korea-Japan Basic Scientific Cooperation Program for 2013 (July 2, 2012) – Organizer of the Korea-Japan Number Theory Conference, Jan. 21-24, 2013

NRF Research Grant, May 1, 2011 - April 30, 2014, awarded by *the National Research Foundation of Korea.* (Jung-Gyun Haik-Shim, three year grant)

Best Teacher Award, September 17, 2009, awarded by Ewha Womans University.

KOSEFF Research Grant awarded by *Korea Research Foundation*, 2009 - 2011 (three year grant)

Research Grant awarded by *KOSEF (Korea Science and Engineering Foundation)*
(Haik-Shim-Gee-Cho) 2008 - 2010 (three year grant)
Ewha Womans University Research Grant Award, Sep. 1, 2007 - Sep. 30, 2008,
NSERC Discovery Grant Award , 2006 - 2010 (five year grant),
(awarded by Natural Sciences and Engineering Research Council of Canada)
(Project title: *Algebraic Function Fields and Cryptography*).
President's Research Grant Award (awarded by SFU), Oct. 2005 - Oct. 2007,
University Start-up Fund (awarded by SFU), August 2005 - August 2006.
NSF-AWM Standard Travel Grant Award, March 2004.
McCoy Fellowship Award, Smith College, 2003 - 2004.
CFCD Fund for equipment, Smith College, 2003 - 2004.
NSF-AWM Mentoring Travel Grant Award, June 2002 - May 2003.
Number Theory Foundation Travel Grant Award, December 2000.
NSF-AWM Travel Grant Award, March 2000.
Research Fellowship, Brown University, Spring 1998.
Teaching Fellowships, Brown University, 1996-1998 and Fall 1999.
Teaching Assistantships, Brown University, 1995-1996.
Teaching Assistantships, Ewha Womans University, 1992-1993.
Honors Scholarships, Ewha Womans University, 1988-1991.
L.G. YONAM Honors Scholarships, LG company, 1989-1991.

Employment

Professor,

- Dept. of Mathematics, Ewha Womans University, Sep. 1, 2007 - current.
- Vice President for Admissions, Ewha Womans University, 2017 - current.
- Leader of *BK21 PLUS project* team awarded by *the NRF of Korea*, 2013-2020, (*"Mathematical Science Team for Global Women Leaders"*).
- Associate Editor (since 2016), Chief-In-Editor (2017-2018) of BKMS, *Bulletin of the Korean Mathematical Society* (BKMS).
- Chair of *Information Protection Associated Major* Program, 2/1/2016 - 6/30/2017.
- Adjunct Professor, Scranton Honors Program, Scranton College, March 1, 2009 – current.
- Associate Director of *EIMS*, Sep. 1, 2012 - Aug. 31, 2015. (Ewha Institute of Mathematical Sciences)

Visiting Professor,
Dept. of Mathematics, Brown University, Aug. 1, 2013 - July 31, 2014.
Chair of Information Protection Associated Major Program, 2/1/2010 – 7/31/2014.
Head of Division of Mathematical and Physical Sciences, 8/1/2010 – 1/31/2012.
Department Chair, Feb. 1, 2010 – Jan. 31, 2012.
Assistant Professor,
Dept. of Mathematics, Simon Fraser University, Aug. 1, 2005 - Aug. 31, 2007.
Assistant Professor,
Dept. of Mathematics, Smith College, July 1, 2002 - July 31, 2005.
Visiting Assistant Professor,

Dept. of Mathematical Sciences, University of Delaware,
Sep. 1, 2000 - June 30, 2002.

Visiting Assistant Professor,
Dept. of Mathematics, Arizona State University,
Aug. 15, 1999 - Aug. 31, 2000.

Instructor,
Dept. of Mathematics, Brown University, 1997-1999.

Teaching Assistant and Research Assistant,
Dept. of Mathematics, Brown University, 1995-1996.

Teaching Assistant,
Dept. of Mathematics, Ewha Womans University, 1992-1994.

Teaching Experience

Ewha Womans University

2019:
Linear Algebra I, Spring, 2019 (lectured in English).
Graduate Algebraic Number Theory I, Fall, 2019 (lectured in English).
2018:
Abstract Algebra I, Spring, 2018 (lectured in English).
Graduate Applied Algebra, Fall, 2018 (lectured in English).
2017:
Number Theory, Spring & Fall (lectured in English).
Graduate Algebra I , Spring (lectured in English).
2016:
Abstract Algebra I, II, Spring & Fall, 2016 (lectured in English).
Graduate Algebraic Number Theory I, II, Spring & Fall, 2016 (lectured in English).
Calculus II, Fall of 2016 (lectured in English).
2015:
Abstract Algebra I, II, Spring & Fall, 2015(lectured in English).
Graduate Algebra I, Spring of 2015 (lectured in English).
Calculus II, Spring of 2015 (lectured in English).
Fall 2014: Calculus II, Applied Algebra (Graduate course)
– both lectured in English
Abstract Algebra I, Spring & 2013 (lectured in English).
Graduate Algebra I, Spring & 2013 (lectured in English).
Number Theory, Spring 2012, 2010 (lectured in English).
Algebraic Number Theory I (Graduate course, lectured in English),
– Spring 2012, 2009
Abstract Algebra I, II, Spring & Fall, 2011 (lectured in English).
Graduate Algebra I, II, Spring & Fall 2011 (lectured in English).
Calculus II, Fall of 2014, 2012, 2010, 2009 (lectured in English).
Selected Topics in Number Theory II (Graduate course), Fall 2010.
Selected Topics in Number Theory I (Graduate course), Spring 2010.
Algebraic Number Theory II (Graduate course), Fall of 2012, 2009

Algebraic Number Theory I (Graduate course), Spring 2009
Number Theory, Spring 2009 (lectured in English).
Algebra II (Graduate course), Fall 2008.
Number systems and Cryptography, Fall 2008 (lectured in English).
Algebra I (Graduate course), Spring 2008.
Linear Algebra I, Spring 2008 (lectured in English).
Applied Algebra (Graduate course), Fall 2014, Fall 2007.
Abstract Algebra II, Fall 2007 (lectured in English).

Simon Fraser University
Introduction to Applied Algebraic Systems (MATH 332), Fall of 2005 and 2006.
Discrete Mathematics II (MACM 201), Spring 2005 and Fall 2006.
Calculus I for Biological Sciences (MATH 154), Spring 2006.

Smith College
Topics in Number Theory (MATH238), Springs of 2003, 2004, and 2005.
Linear Algebra (MATH211), Fall 2002, Spring 2004.
Discrete Mathematics (MATH153), Fall 2002, 2003 and 2004.
Calculus II (MATH112), Spring 2005.

University of Delaware
Discrete Mathematics (MATH210), Fall 2000, 2001, Spring 2002.
Analytic Geometry and Calculus III (MATH243), 2001, Spring 2002.
Analytic Geometry and Calculus II (MATH242), Fall 2000.

Arizona State University
Calculus with Analytic Geometry I (MAT270), Spring 2000.
Calculus with Analytic Geometry I (MAT270), Fall 1999.

Brown University
Calculus II, Spring & Fall 1999, Spring & Fall 1996.
Advanced Placement Calculus, Fall 1998.
Intermediate Calculus, Spring 1997.
Calculus I, Fall 1995.

Research Trips

Visiting Professor of Math. Dept. at Brown University, US,
July 27, 2013 - July 27, 2014.

Nanyang Technological University, Singapore,
May 22 - May 27, 2011, Jan. 10 - Jan. 16, 2011, August 1 - August 7, 2010.
(Collaboration with C. Xing)

Associate member of KIAS (*Korean Institute for Advanced Study*),
Sep. 1, 2007 - current.

University of Louisville, US, March 25, 2010 - March 27, 2010.
(Collaboration with J. Kim)

University of Calgary, Canada, July 20, 2009 - July 25, 2009.

(Collaboration with R. Scheidler, M. Jacobson, H. Williams)

Visiting Scholar at KIAS (*Korean Institute for Advanced Study*),
Dec. 15, 2004 - Dec. 30, 2005.
May 20, 2004 - July 31, 2005, Dec. 20, 2004 - Jan. 20, 2005.
June 23, 2003 - Aug. 25, 2003, May 20, 2004 - Aug. 20, 2004.

University of Calgary, June 15 - July 15, 2002.
(Collaboration with H. Williams, R. Scheidler, and M. Jacobson)

Dissertation advisor: Prof. Michael I. Rosen

Dissertation area: Algebraic Number Theory

Dissertation title: Cohen-Lenstra Heuristics and the Spiegelungssatz.

Research Interests

- Algebraic Number Theory
  Arithmetic of algebraic function fields
  Galois representation associated to Drinfeld modules
  Class group structure of a cyclotomic function field.
  Structure of ideal (or divisor) class groups of global fields.
  Classical geometry of number method in function fields
  Modularity of a various types of continued fractions
  Torsion group structure of elliptic curves

- Algebraic Coding Theory and Discrete Mathematics
  Self-dual (or Formally self-dual) codes and cyclic (or Quasi-cyclic) codes
  Algebraic Geometric codes and Number field codes
  Cryptographic functions: bent functions and plateaued functions
  Lattice codes and theta series
  Cheeger constants of distance regular graphs

Research Publications

[1] Cohen-Lenstra Heuristics and the Spiegelungssatz: Number Fields,
Journal of Number Theory **92**, No. 1, 37-66 (2002).

Abstract In this paper we study the compatibility of Cohen-Lenstra heuristics with Leopoldt's Spiegelungssatz (the reflection theorem). We generalize Dutarte's ([1983, *in* "Théorie des nombres, Besançon, 1983-1984"]) work to every prime number p : he proved the compatibility of the Cohen-Lenstra conjectures with the Spiegelungssatz in the case $p = 3$. We also show that the Spiegelungssatz is compatible with the conjectural probabilities on the p-rank of some subgroups of the class group of a cyclic extension of degree q over Q, where q is a prime number dividing $p - 1$.

[2] Computation of the Fundamental Units and the Regulator of a Cyclic Cubic Function Field, (with Lee, R. Scheidler and C. Yarrish)
Experimental Mathematics, Vol. **12**, No. 2, 211-225 (2003).

Abstract This paper presents algorithms for computing the two fundamental units and the regulator of a cyclic cubic extension of a rational function field over a field of order $q \equiv 1 \pmod 3$. The procedure is based on a method originally due to Voronoi that was recently adapted to purely cubic function fields of unit rank one. Our numerical examples show that the two fundamental units tend to have large degree, and frequently, the extension has a very small ideal class number.

[3] Euclidean and Hermitian Self-Dual MDS Codes Over Large Finite Fields (with J. Kim) *Journal of Combinatorial Theory Series A* , Vol. **105**, No. 1, 79-95 (2004).

Abstract The first author constructed new extremal binary self-dual codes and new self-dual codes over $GF(4)$ with the highest known minimum weights. The method used was to build self-dual codes from given self-dual codes of a smaller length. In this paper we develop a complete generalization of this method for the Euclidean and Hermitian self-dual codes over finite fields $GF(q)$. Using this method we construct many Euclidean or Hermitian self-dual MDS (or near MDS) codes of length up to 12 over various finite fields $GF(q)$, where $q = 8, 9, 16, 25, 32, 41, 49, 53, 64, 81, 128$. Our results on the minimum weights of (near) MDS self-dual codes over large fields give a better bound than the Pless-Pierce bound obtained from a modified Gilbert-Varshamov bound.

[4] Cohen-Lenstra heuristics and the Spiegelungssatz: Function Fields, *Journal of Number Theory* **106**, No. 2, 187-199 (2004).

Abstract In this paper we study the compatibility of Cohen-Lenstra heuristics with Leopoldt's Spiegelungssatz (= the reflection theorem) in the case of cyclic function fields. First, we prove a group-theoretical version of the Spiegelungssatz for cyclic function fields. Then we show the internal consistency of the function field analogue of Cohen-Lenstra heuristics in the case of cyclic function fields. It thus supports the validity of Cohen-Lenstra heuristics in function fields.

[5] MDS Self-dual Codes (with J. Kim), *Proceedings of the 2004 IEEE International Symposium on Information Theory*, Chicago, USA, June 27-July 2, pp. 526 (2004).

Abstract In this paper we develop a complete generalization of the building-up method in [*New extremal self-dual codes of lengths 36,38, and 58*, *IEEE Trans. Inform. Theory*, vol. 47, pp. 386–393, 2001] for the Euclidean and Hermitian self-dual codes over finite fields $GF(q)$. Using this method we construct many new Euclidean and Hermitian self-dual MDS (or near MDS) codes of length up to 12 over various finite fields $GF(q)$, where $q = 8, 9, 16, 25, 32, 41, 49, 53, 64, 81$, and 128.

[6] The Unit Rank Classification of a Cubic Function Field by its Discriminant, *Manuscripta Mathematica*, **Vol.** 116, No. 2, 173 - 181 (2005).

Abstract An arbitrary cubic function field can have 0, 1, or 2 for its unit rank. This paper presents the complete classification of the unit rank of

an arbitrary cubic function field by its discriminant and the polynomial discriminant of its generating polynomial. The notions of Kummer Theory and Cardano's formula are used.

[7] Class groups of imaginary function fields: The inert case,
(with A. Pacelli) *Proc. Amer. Math. Soc.*, **Vol.** 133, 2883-2889 (2005).

Abstract Let F be a finite field and T a transcendental element over F. An imaginary function field is defined to be a function field such that the prime at infinity is inert or totally imaginary. For the totally imaginary case, in a recent paper the second author constructed infinitely many function fields of any fixed degree over $F(T)$ in which the prime at infinity is totally ramified and with ideal class numbers divisible by any given positive integer greater than 1. In this paper, we complete the imaginary case, by proving the corresponding result for function fields in which the prime at infinity is inert. Specifically, we show that for any relatively prime integers m and n with $m, n > 1$ and relatively prime to the characteristic of F, there are infinitely many function fields of fixed degree m such that the class group contains a subgroup isomorphic to $(Z/nZ)^{m-1}$ and the prime at infinity is inert.

[8] The structure of the class groups of global function fields with any unit rank,
J. Ramanujan Math. Soc. **20**, No. 2, 1-21 (2005).

Abstract Let F be a finite field and T a transcendental element over F. We construct, for positive integers m, n and r with $0 \leq r \leq m-1$, infinitely many global function fields K of degree m over $F(T)$ such that K has unit rank r and the ideal class group of K contains a subgroup isomorphic to $(Z/nZ)^{m-r}$. This completes previous result [Higher Rank Subgroups in the Class Groups of Imaginary Function Fields (2004), preprint] of the author and Pacelli. In the previous result we worked on the inert case (unit rank $r = 0$ case), so in this paper we focus on the totally ramified case for the unit rank $r = 0$. This work also improves Pacelli's work [The prime at infinity and the rank of the class group of a global function field (2004), preprint] by increasing the subgroup rank from $m - r - 1$ to $m - r$.

[9] Higher rank subgroups in the class groups of imaginary function fields,
(with A. Pacelli), *Journal of Pure and Applied Algebra*, **Vol.** 207, 51-62 (2006).

Abstract Let F be a finite field and T a transcendental element over F. In this paper, we construct, for integers m and n relatively prime to the characteristic of $F(T)$, infinitely many imaginary function fields K of degree m over $F(T)$ whose class groups contain subgroups isomorphic to $(Z/nZ)^m$. This increases the previous rank of $m - 1$ found by the authors in [Class groups of imaginary function fields: The inert case, To appear in Proc. Amer. Soc.].

[10] Class number divisibility of relative quadratic function fields,
Acta Arithmetica, 121, No. 2, 161-173 (2006).

Abstract Let K be a function field over a finite field. We find necessary and sufficient conditions for the class numbers of *relative quadratic* extension

fields of K to be divisible by 3. More specifically, we obtain complete descriptions for relative quadratic extension fields of K whose ideal class numbers are divisible by 3, and also for relative quadratic extension fields of K such that their divisor class numbers are divisible by 3.

[11] The Scholz Theorem in function fields,
Journal of Number Theory **122**, No. 2, 408-414 (2007).

Abstract The *Scholz Theorem* in function fields states that the l-rank difference between the class groups of an imaginary quadratic function field and its associated real quadratic function field is either 0 or 1 for some prime l. Furthermore, Leopoldt's *Spiegelungssatz* (= *the Reflection Theorem*) in function fields yields a comparison between the m-rank of some subgroup of the class group of an imaginary cyclic function field and the m-rank of some subgroup of the class group of its associated real cyclic function field for some prime number m; then their m-ranks also equal or differ by 1. In this paper we find an explicit necessary condition for their m-ranks (resp. l-ranks) to be the same in the case of cyclic function fields (resp. quadratic function fields). In particular, in the case of quadratic function fields, if l does not divide the *regulator* of L_2, then their l-ranks are the same, equivalently if their l-ranks differ by 1, then l divides the regulator of L_2.

[12] Construction of MDS Self-dual codes over Galois rings,
(with J. Kim), *Designs, Codes and Cryptography*, Vol. 45, No. 2, 247-258 (2007).

Abstract The purpose of this paper is to construct nontrivial MDS self-dual codes over Galois rings. We consider a building-up construction of self-dual codes over Galois rings as a GF(q)-analogue of [J.-L. Kim and Y. Lee, Euclidean and Hermitian Self-Dual MDS Codes over Large Finite Fields, J. Combin. Theory Ser. A, Vol. 105 (2004) pp. 79–95]. We give a necessary and sufficient condition on which the building-up construction holds. We construct MDS self-dual codes of lengths up to 8 over $GR(3^2, 2)$, $GR(3^3, 2)$ and $GR(3^4, 2)$, and near-MDS self-dual codes of length 10 over these rings. In a similar manner, over $GR(5^2, 2)$, $GR(5^3, 2)$ and $GR(7^2, 2)$, we construct MDS self-dual codes of lengths up to 10 and near-MDS self-dual codes of length 12. Furthermore, over $GR(11^2, 2)$ we have MDS self-dual codes of lengths up to 12.

[13] Eta pairing computation on general divisors over hyperelliptic curves, $y^2 = x^7 - x \pm 1$ (with E. Lee, H. Lee), Lecture Notes in Comput. Sci. 4575, Springer, 349-366 (2007).

Abstract Recent developments on the Tate or Eta pairing computation over hyperelliptic curves by Duursma-Lee and Barreto et al. have focused on *degenerate* divisors. We present two efficient methods that work for *general* divisors to compute the Eta paring over divisor class groups of the hyperelliptic curves $H/F_{7^n} : y^2 = x^7 - x \pm 1$ of genus 3. The first method generalizes the method of Barreto et al. so that it holds for general divisors, and we call it the *pointwise* method. For the second method, we take a novel approach using *resultant.* We focus on the case that two divisors of the pairing have supporting points in $H(F_{7^{3n}})$, not in $H(F_{7^n})$. Our analysis shows that the

resultant method is faster than the pointwise method, and our implementation result supports the theoretical analysis. In addition to the fact that the two methods work for general divisors, they also provide very explicit algorithms.

[14] Construction of hyperelliptic function fields of high three rank,
(with M. Bauer, M. Jacobson, R. Scheidler),
Mathematics of Computation, Vol. 77, Number 261, 503-530 (2008).

Abstract We present several explicit constructions of hyperelliptic function fields whose Jacobian or ideal class group has large l-rank, with particular emphasis on the case $l = 3$. Some of our methods are adapted from analogous techniques used for generating quadratic number fields of high 3-rank, while others are new and unique to function fields. Algorithms, examples, and numerical computations are included.

[15] Tate pairing computation on the divisors of hyperelliptic curves of genus 2,
(with E. Lee), *J. Korean Math. Soc.* Vol. 45, No. 4, 1057-1073 (2008).

Abstract We present an explicit method for computing the Tate pairing on *general divisors* of hyperelliptic curves H_b of genus 2, where $H_b : y^2+y = x^5+x^3+b$ is over a binary field F_{2^n} with $b = 0$ or 1. We use *Elimination method* for computing the Tate pairing on general divisors. Our method is very general since they can be used for *general* divisors, not only for *degenerate* divisors. In the pairing-based cryptography, the efficient Tate pairing implementation on general divisors is significantly important because the decryption process definitely requires computing a pairing of general divisors.

[16] Eta pairing computation on general divisors over hyperelliptic curves
$y^2 = x^p - x + d$ (with E. Lee, H. Lee),
Journal of Symbolic Computation, Vol 43, issues 6-7, pp. 452-474, 2008.

Abstract Recent developments on the Tate or Eta pairing computation over hyperelliptic curves by Duursma-Lee and Barreto et al. have focused on *degenerate* divisors. We present efficient methods that work for *general* divisors to compute the Eta paring over divisor class groups of the hyperelliptic curves $H_d : y^2 = x^p - x + d$ where p is an odd prime. On the curve H_d of genus 3, we provide two efficient methods: The first method generalizes the method of Barreto et al. so that it holds for general divisors, and we call it the *pointwise* method. For the second method, we take a novel approach using *resultant*. Our analysis shows that the resultant method is faster than the pointwise method, and our implementation result supports the theoretical analysis. We also emphasize that the Eta pairing technique is generalized to the curve $y^2 = x^p - x + d, p \equiv 1 \pmod 4$. Furthermore, we provide the closed formula for the Eta pairing computation on general divisors by Mumford representation of the curve H_d of genus 2.

[17] Construction of self-dual codes over finite rings Z_{p^m} (with H. Lee),
Journal of Combinatorial Theory, Series A 115, 407–422 (2008).

Abstract We present an efficient method for constructing self-dual or self-orthogonal codes over finite rings Z_{p^m} (or Z_m) with p an odd prime and m

a positive integer. This is an extension of the previous work [J. Kim and Y. Lee, Euclidean and Hermitian Self-dual MDS codes over large finite fields, J. Combin. Theory Ser. A, Vol. **105**, No. 1, 79-95 (2004)] over large finite fields $GF(p^m)$ to finite rings Z_{p^m} (or Z_m). Using this method we construct self-dual or self-orthogonal codes of length at least up to 10 over various finite rings Z_{p^m} or Z_{pq} with q an odd prime, where $p^m = 25,\ 125,\ 169,\ 289$ and $pq = 65,\ 85$. All the self-dual codes we obtained are MDS, MDR, near MDS, or near MDR codes.

[18] Reflection Theorem for divisor class groups of quadratic function fields, *Journal of Number Theory* 128, 2127-2137 (2008).

Abstract We present the *Reflection Theorem* for divisor class groups of relative quadratic function fields. Let K be a global function field with constant field F_q. Let L_1 be a quadratic geometric extension of K and let L_2 be its twist by the quadratic constant field extension of K. We show that for every odd integer m that divides $q+1$ the divisor class groups of L_1 and L_2 have the same m-rank.

[19] New MDS and Near-MDS Self-Dual Codes (with T.A. Gulliver, J.-L. Kim), *IEEE Transactions on Information Theory*, Vol. 54, No. 9, 4354-4360 (2008).

Abstract We construct new MDS or near-MDS self-dual codes over large finite fields. In particular we show that there exists a Euclidean self-dual MDS code of length $n = q$ over $GF(q)$ whenever $q = 2^m$ $(m \geq 2)$ using a Reed-Solomon (RS) code and its extension. It turns out that this MDS self-dual code is an extended duadic code. We construct Euclidean self-dual near-MDS codes of length $n = q - 1$ over $GF(q)$ from RS codes when $q \equiv 1 \pmod 4$ and $q \leq 113$. We also construct many new MDS self-dual codes over $GF(p)$ of length 16 for primes $p \leq 113$. Finally we construct Euclidean/Hermitian self-dual MDS codes of lengths up to 14 over $GF(q^2)$ where $q = 19, 23, 25, 27, 29$.

[20] Class groups of global function fields with certain splitting behaviors of the infinite prime, *Proc. Amer. Math. Soc.*, Vol 137, No. 2, 415-424 (2009).

Abstract For certain two cases of random splitting behaviors of the prime at infinity with the unit rank r, we construct infinitely many global function fields K such that the ideal class group of K has n-rank at least $m - r - 1$ and the prime at infinity splits in K as given. In detail, let F be a finite field and T a transcendental element over F. For positive integers m, n and r with $0 \leq r \leq m-1$ with a given signature (e_i, f_i), $1 \leq i \leq r+1$ such that $\sum_{i=1}^{r+1} e_i f_i = m$, in the following two cases that e_i is arbitrary and $f_i = 1$ for each i, or $e_i = 1$ and f_i's are the same for each i, we construct infinitely many global function fields K of degree m over $F(T)$ such that the ideal class group of K contains a subgroup isomorphic to $(Z/nZ)^{m-r-1}$ and the prime at infinity P_∞ splits into $r+1$ primes $f_1, f_2, \cdots, f_{r+1}$ in K with $e(P_i/P_\infty) = e_i$ and $f(P_i/P_\infty) = f_i$ for $1 \leq i \leq r+1$ (so, K is of unit rank r).

[21] Construction of cubic self-dual codes (with S. Han, J. Kim, H. Lee), *Proceedings of the 2009 IEEE International Symposium on Information Theory*,

2396-2399 (2009).

Abstract We present a building-up construction method for quasi-cyclic self-dual codes over finite fields. By using this, we give *cubic* (i.e., l-quasi-cyclic codes of length $3l$) self-dual codes over various finite fields, which are optimal or have the best known parameters. In particular, we find a new quasi-cyclic self-dual $[24, 12, 9]$ code over F_5, whose corresponding lattice by Construction A is shown to be the odd Leech lattice O_{24}. Only one self-dual $[24, 12, 9]$ code over F_5 was known before up to monomial equivalence.

[22] Self-dual codes using building-up constructions (with J. Kim),
Proceedings of the 2009 IEEE International Symposium on Information Theory,
2400-2402 (2009).

Abstract In this paper we develop a complete generalization of the building-up method in [*New extremal self-dual codes of lengths 36,38, and 58*, *IEEE Trans. Inform. Theory*, vol. 47, pp. 386–393, 2001] for the Euclidean and Hermitian self-dual codes over finite fields $GF(q)$. Using this method we construct many new Euclidean and Hermitian self-dual MDS (or near MDS) codes of length up to 12 over various finite fields $GF(q)$, where $q = 8, 9, 16, 25, 32, 41, 49, 53, 64, 81$, and 128.

[23] The ℓ-Rank Structure of a Global Function Field,
(with L. Berger, J.-L. Hoelscher, J. Paulhus, R. Scheidler),
Fields Institute Communications 60, Amer. Math. Soc., 145-166 (2011).

Abstract For any prime ℓ, it is possible to construct global function fields whose Jacobians have high ℓ-rank by moving to a sufficiently large constant field extension. This was investigated in some detail by Bauer et al. in the paper *Construction of hyperelliptic function fields of high three rank*. The two main results of the paper by Bauer et al. are an upper bound on the size of the field of definition of the ℓ-torsion $J[\ell]$ of the Jacobian, and a lower bound on the increase in the base field size that guarantees a strict increase in ℓ-rank. Here, we provide improvements to both these results, and give examples which illustrate that our techniques have the potential to yield the correct ℓ-rank over any intermediate field of the field of definition of $J[\ell]$, including base fields that might be too large to be handled directly by computer algebra packages.

[24] Families of elliptic curves over cubic number fields with prescribed torsion subgroups
(with D. Jeon and C. Kim), *Mathematics of Computation* 80, No. 273, 579-591 (2011).

Abstract In this paper we construct infinite families of elliptic curves with given torsion group structures over cubic number fields. This result provides explicit examples of the theoretical result recently developed by the first two authors and Schweizer; they determined all the group structures which occur infinitely often as the torsion of elliptic curves over cubic number fields. In fact, this paper presents an efficient way of constructing such families of elliptic curves with prescribed torsion group structures over cubic number fields.

[25] Binary formally self-dual odd codes (with S. Han, H. Lee and Y. Lee),

Designs, Codes and Cryptography, Vol. 61, No. 2, 141-150 (2011).

Abstract Most of the research on *formally self-dual* (f.s.d.) codes has been made for binary f.s.d. even codes, but not much has been developed for binary f.s.d. odd codes. In this paper we complete the classification of binary f.s.d. odd codes of lengths up to 12. We also classify optimal binary f.s.d. odd codes of length 18 and 24, and so our classification completes the classification of binary optimal f.s.d. odd codes of lengths up to 26. For the classification we first find a relation between binary f.s.d. odd codes and binary f.s.d. even codes, and then we use this relation and the known classification results on binary f.s.d. even codes. Finally we also classify (possibly) optimal binary double circulant f.s.d. odd codes of lengths up to 40.

[26] Families of elliptic curves over quartic number fields with prescribed torsion subgroups (with D. Jeon, C. Kim),
Mathematics of Computation, Vol. 80, No. 276, 2395-2410 (2011).

Abstract We construct infinite families of elliptic curves with given torsion group structures over quartic number fields. Recently the first two authors and Park determined all the group structures which occur infinitely often as the torsion of elliptic curves over quartic number fields. Our result presents explicit examples of their theoretical result. This paper also presents an efficient way of finding such families of elliptic curves with prescribed torsion group structures over quadratic or quartic number fields.

[27] Construction of self-dual codes with an automorphism of order p
(with H.J. Kim, H. Lee, J. Lee),
Advances in Mathematics of Communications, Vol. 5, No. 1, 23–36 (2011).

Abstract We develop a construction method for finding self-dual codes with an automorphism of order p with c independent p-cycles. In more detail, we construct a self-dual code with an automorphism of type $p-(c, f+2)$ and length $n+2$ from a self-dual code with an automorphism of type $p-(c, f)$ and length n, where an *automorphism of type* $p-(c, f)$ is that of order p with c independent cycles and f fixed points. Using this construction, we find three new inequivalent extremal self-dual $[54, 27, 10]$ codes with an automorphism of type $7-(7, 5)$ and two new inequivalent extremal self-dual $[58, 29, 10]$ codes with an automorphism of of type $7-(8, 2)$. We also obtain an extremal self-dual $[40, 20, 8]$ code with an automorphism of type $3-(10, 10)$, which is constructed from an extremal self-dual $[38, 19, 8]$ code of type $3-(10, 8)$, and at least 482 inequivalent extremal self-dual $[58, 29, 10]$ codes with an automorphism of type $3-(18, 4)$, which is constructed from an extremal self-dual $[54, 27, 10]$ code of type $3-(18, 0)$; we note that the extremality is preserved.

[28] MDS poset- codes satisfying the asymptotic Gilbert-Varshamov bound in Hamming weights (with J. Hyun),
IEEE Transactions on Information Theory, Vol. 57, No. 12, 8021-8026 (2011).

Abstract We prove that the MDS linear poset-codes satisfy Gilbert-Varshamov bound for their Hamming weights asymptotically. We also construct the

MDS linear poset-codes on arbitrary poset-metric spaces by using the Dilworth's chain decomposition theorem and results about the Hermite interpolation problem over a finite field. We prove that there exist linear poset-codes with large weights for both poset-metrics and Hamming metrics as well.

[29] Decomposition of places in dihedral and cyclic quintic trinomial extensions of global fields (with B. Im),
Manuscripta Mathematica, Vol. 137, No. 1-2, 107–127 (2012).

Abstract In this paper, we give a complete and explicit description of the splitting behavior of any place in a quintic trinomial dihedral extension of a rational function field of finite characteristic distinct from 2 and 5. Our characterization depends only on the order of the base field and a parametrization of the coefficients of the generating trinomial. Moreover, we contrast some of our results to trinomial dihedral number fields of prime degree, where the unit rank behaves quite differently from the function field scenario.

[30] Constructions of self-dual codes over $F_2 + uF_2$, (with S. Han, H. Lee)
Bull. Korean. Math. Soc., Vol. 49, No. 1, 135-143 (2012).

Abstract We present two kinds of construction methods for self-dual codes over $F_2 + uF_2$. Specially, the second construction (respectively, the first one) preserves the types of codes, that is, the constructed codes from Type II (respectively, Type IV) is also Type II (respectively, Type IV). Every Type II (respectively, Type IV) code over $F_2 + uF_2$ of free rank larger than three (respectively, one) can be obtained via the second construction (respectively, the first one). Using these constructions, we update the information on self-dual codes over $F_2 + uF_2$ of length 9 and 10, in terms of the highest minimum (Hamming, Lee, or Euclidean) weight and the number of inequivalent codes with the highest minimum weight.

[31] Construction of quasi-cyclic self-dual codes (with S. Han, J.-L. Kim, H. Lee),
Finite Fields and their applications, Vol. 18, No. 3, 613-633 (2012).

Abstract There is a one-to-one correspondence between ℓ-quasi-cyclic codes over a finite field F_q and linear codes over a ring $R = F_q[Y]/(Y^m - 1)$. Using this correspondence, we prove that every ℓ-quasi-cyclic self-dual code of length $m\ell$ over a finite field F_q can be obtained by the *building-up* construction, provided that $\mathrm{char}(F_q) = 2$ or $q \equiv 1 \pmod 4$, m is a prime p, and q is a primitive element of F_p. We determine possible weight enumerators of a binary ℓ-quasi-cyclic self-dual code of length $p\ell$ (with p a prime) in terms of divisibility by p. We improve the result of Bonnecaze et al by constructing new optimal binary cubic (i.e., ℓ-quasi-cyclic codes of length 3ℓ) self-dual codes of lengths $30, 36, 42, 48$ (Type I), 54 and 66. We also find optimal quasi-cyclic self-dual codes of lengths 40, 50, and 60. When $m = 5$, we obtain a new 8-quasi-cyclic self-dual $[40, 20, 12]$ code over F_3 and a new 6-quasi-cyclic self-dual $[30, 15, 10]$ code over F_4. When $m = 7$, we find a new 4-quasi-cyclic self-dual $[28, 14, 9]$ code over F_4 and a new 6-quasi-cyclic self-dual $[42, 21, 12]$ code over F_4.

[32] MacWilliams duality and a Gleason-type theorem on self-dual bent functions,

(with J. Hyun, H. Lee) *Designs, Codes and Cryptography*, Vol. 63, No. 3, 295-304 (2012).

Abstract We prove that the MacWilliams duality holds for bent functions, and by using the MacWilliams duality, we prove the Gleason-type theorem on self-dual bent functions. As an application, we obtain a general explicit formula for an upper bound of the total number of self-dual bent functions.

[33] Coefficients of exponential functions attached to Drinfeld modules of rank 2, (with I. Chen), *Manuscripta Mathematica*, Vol. 139, No. 1-2, 123-136 (2012).

Abstract Let ϕ be a Drinfeld A-module of rank 2 defined over C_∞. We explicitly determine the pattern of valuations of the exponential functions attached to ϕ and discuss applications to the study of zeroes of para-Eisenstein series.

[34] Construction of extremal self-dual codes over $F_2 + uF_2$ with an automorphism of odd order(with H.J. Kim),
Finite fields and their applications, Vol. 18, No. 5 (2012), 971-992.

Abstract We complete the classification the Lee-extremal self-dual codes over the ring $F_2 + uF_2$ of lengths 21 and 22 with a nontrivial automorphism of odd prime order except the case for an automorphism of order 3 with seven cycles, and we partially classify the exceptional case. In particular, we show that there are 647 (respectively, 13165) inequivalent Lee-extremal self-dual codes of length 21 (respectively, 22) with an automorphism of odd prime order. We use the decomposition theory for self-dual codes over $F_2 + uF_2$ with an automorphism of odd prime order as the same approaches made by Huffman. And we also use an extension method as a new approach, and the current approach is extending the even subcode part while the fixed subcode part is extended in the authors' previous work.

[35] Corrigendum to "Construction of extremal self-dual codes over $F_2 + uF_2$ with an automorphism of odd order" (with H.J. Kim),
Finite fields and their applications, Vol. 23, (2013) 103–104.

Abstract In the published version, we claim that there is no Lee-extremal self-dual code of length 22 with an automorphism of type 5-(2,22)(2,22), and there are exactly 106 inequivalent Lee-extremal self-dual codes of length 22 with an automorphism of type 5-(4,2)(4,2). However, we confirm that in fact there exist 23 inequivalent Lee-extremal self-dual codes of length 22 with an automorphism of type 5-(2,22)(2,22), and there are exactly 113 inequivalent Lee-extremal self-dual codes of length 22 with an automorphism of type 5-(4,2)(4,2).

[36] Newton polygons, successive minima, and different bounds for Drinfeld modules of rank 2, (with I. Chen)
Proc. Amer. Math. Soc., 141 (2013), no. 1, 83–91.

Abstract Let ϕ be a Drinfeld A-module of rank 2 defined over C_∞. We explicitly determine the Newton polygons of exponential functions attached to ϕ and the successive minima of the lattice associated to ϕ by uniformization.

When ϕ is defined over K_∞, we give a refinement of Gardeyn's bounds for the action of wild inertia on the torsion points of ϕ, as well as a criterion for the lattice field to be unramified over K_∞.

[37] Thin additive bases for monic polynomials in $F_q[t]$ (with A. Bender, B. Im), Bull. Korean Math. Soc. 50 (2013), No. 2, pp. 399–405.

Abstract We explicitly construct a thin basis for the set M of monic polynomials in one variable t over a finite field F_q.

[38] Infinite families of elliptic curves over Dihedral quartic number fields, *Journal of Number Theory*, Vol. 133, Issue 1, 115-122 (2013).
(with D. Jeon and C. Kim)

Abstract We find infinite families of elliptic curves over quartic number fields with torsion group Z/NZ with $N = 20, 24$. We prove that for each elliptic curve E_t in the constructed families, the Galois group $Gal(L/Q)$ is isomorphic to the Dihedral group D_4 of order 8 for the Galois closure L of K over Q, where K is the defining field of (E_t, Q_t) and Q_t is a point of E_t of order N. We also notice that the plane model for the modular curve $X_1(24)$ found in [JKL] is in the optimal form, which was the missing case in Sutherland's work [Su].

[39] Classification of extremal self-dual quaternary codes of lengths 30 and 32 (with H.J. Kim), *IEEE transactions on information theory*, Vol. 59 (April, 2013), No. 4, 2352-2358.

Abstract We classify extremal self-dual codes of lengths 30 and 32 over F_4 with an automorphism of odd prime order greater than 3. We prove that there exists exactly one extremal self-dual $[30, 15, 12]$ code over F_4 with an automorphism of prime order greater than 3, up to equivalence; the order of the automorphism group is 36540. We also show that there exists no extremal self-dual $[32, 16, 12]$ code over F_4 with an automorphism of prime order greater than 3.

[40] Galois Characters arising from Drinfeld modules (with S. Chang), J. Number Theory 133 (2013), no. 3, 888–896.

Abstract We characterize Galois characters that arise from Drinfeld modules over finite fields in the sense that they can be constructed by the Galois action on the torsion points of Drinfeld modules.

[41] Explicit expression of the Krawtchouk polynomial via a discrete Green's function, *J. Korean Math. Soc.*, 50 (2013), No. 3, pp. 509-527.

Abstract A Krawtchouk polynomial is introduced as the classical MacWilliams identity, which can be expressed in weight-enumerator-free form of a linear code and its dual code over a Hamming scheme. In this paper we find a new explicit expression for the p-number and the q-number, which are more generalized notions of the Krawtchouk polynomial in the P-polynomial schemes by using an extended version of a discrete Green's function. As corollaries, we obtain a new expression of the Krawtchouk polynomial over the Hamming

scheme and the Eberlein polynomial over the Johnson scheme. Furthermore, we find another version of the MacWilliams identity over a Hamming scheme.

[42] Explicit isogeny theorems for Drinfeld modules (with I. Chen), *Pacific Journal of Mathematics*, 263 (2013), No. 1, 87-116.

Abstract Let $F = F_q(T)$, $A = F_q[T]$. Given two non-isogenous rank r Drinfeld A-modules ϕ and ϕ' over K, where K is a finite extension of F, we obtain a partially explicit upper bound (dependent only on ϕ and ϕ') on the degree of primes p of K such that $P_p(\phi) \neq P_p(\phi')$, where $P_p(*)$ denotes the characteristic polynomial of Frobenius at p on a Tate module of $*$. The bounds are completely explicit in terms of the defining coefficients of ϕ and ϕ', except for one term, which can be made explicit in the case of $r = 2$. An ingredient in the proof of the partially explicit isogeny theorem for general rank is an explicit bound for the different divisor of torsion fields of Drinfeld modules which detects primes of potentially good reduction. Our results are a Drinfeld module analogue of Serre's work, but the results we obtain are unconditional because GRH for function fields holds.

[43] A Cheeger inequality of a distance regular graph using the Green's function (with G. Kim), *Discrete Mathematics*, Vol. 313 (2013), Issue 20, 2337-2347.

Abstract We give a Cheeger inequality of distance regular graphs in terms of the smallest positive eigenvalue of the Laplacian and a value α_d which is defined using q-numbers. We can approximate α_d with arbitrarily small positive error β. The method is to use a Green's function, which is the inverse of the β-Laplacian.

[44] Nonexistence of certain types of plateaued functions (with J. Hyun, H. Lee), *Discrete Applied Mathematics*, Vol. 161, Issues 16-17 (2013), 2745-2748.

Abstract The class of plateaued functions (or r-plateaued functions) are Boolean functions with many cryptographically desirable properties, and this class of plateaued functions include bent functions. In fact, bent functions are exactly 0-plateaued functions. There are some results on the nonexistence of homogeneous 0-plateaued functions in n variables by Xia et al, Meng et al, and by the authors. In this paper we present a result on the nonexistence of r-plateaued functions in n variables ($0 < r < n$): for a given $n \geq N$ and r, we prove the nonexistence of r-plateaued functions with certain degrees, where N is some integer depending on r.

[45] Hermitian self-dual codes over $F_{2^{2m}} + uF_{2^{2m}}$ (with H.J. Kim), *Finite fields and their applications*, 25 (2014), 106-131.

Abstract We present a method for construction of Hermitian self-dual codes over $F_{2^{2m}} + uF_{2^{2m}}$ from Hermitian self-dual codes over $F_{2^{2m}}$ via *Gray map* we define, where m is a positive integer. For constructing Hermitian self-dual codes over $F_2 + uF_2$ with an automorphism of odd order using the decomposition theory, it is necessary to find Hermitian self-dual codes over $F_{2^{2m}} + uF_{2^{2m}}$ for some appropriate positive integer m. Using the Gray map, we can figure out checking the equivalence of codes over $F_{2^{2m}} + uF_{2^{2m}}$ from the information on the equivalence of codes over $F_{2^{2m}}$. We thus classify all Hermitian self-dual codes over $F_{2^2} + uF_{2^2}$ of lengths up to 8. Using these

codes, we complete the classification of the Lee-extremal self-dual codes over $F_2 + uF_2$ of lengths 21 and 22 with a nontrivial automorphism of odd order; these were open cases in the authors' previous work.

[46] Necessary conditions for the existence of regular p-ary bent functions,
IEEE transactions on information theory, Vol. 60, No. 3 (2014), 1665-1672.
(with J.Y. Hyun, H. Lee)

Abstract We prove some necessary conditions for the existence of regular p-ary bent functions (from Z_p^n to Z_p), where p is a prime. In more detail, we show that there is no regular p-ary bent function in n variables with *magnitude* larger than $n/2$, and for a given nonnegative integer k there is no regular p-ary bent function in n variables with magnitude $n/2 - k$ ($(n+3)/2 - k$, respectively) for an even $n \geq N_{p,k}$ (an odd $n \geq N_{p,k}$, respectively), where $N_{p,k}$ is some positive integer which is explicitly determined and the magnitude of a p-ary function f is some value related to the power of each monomial of f.

For the proof of our main results, we use some properties of regular p-ary bent functions such as the MacWilliams duality, which is proved to hold for regular p-ary bent functions in this paper.

[47] Boolean functions with MacWilliams duality (with J.Y. Hyun, H. Lee),
Designs, Codes and Cryptography, Volume 72, Issue 2 (2014), 273-287.

Abstract We introduce a new class of Boolean functions for which the MacWilliams duality holds, called *MacWilliams-dual* functions, by considering a dual notion on boolean functions. By using the MacWilliams duality, we prove the Gleason-type theorem on MacWilliams-dual functions. We show that a collection of MacWilliams-dual functions contains all the bent functions and all formally self-dual Boolean functions. We also obtain the Pless power moments for MacWilliams-dual functions. Furthermore, as an application, we prove the nonexistence of bent functions in $2n$ variables with minimum degree $n - k$ for any nonnegative integer k and $n \geq N$ with some positive integer N under a certain condition.

[48] Families of elliptic curves with prescribed torsion subgroups over dihedral quartic fields,
(with D. Jeon and C. Kim)
Journal of Number Theory, 147 (2015) 342-363.

Abstract We construct the infinite families of elliptic curves with cyclic torsion groups over quartic number fields K such that the Galois closure of K is dihedral of order 8; such a quartic number field K is called a *dihedral quartic number field*. In fact, all the cyclic torsion groups of elliptic curves which occur over quartic extension fields (not over quadratic extension fields) are Z/NZ with $N = 17, 20, 21, 22, 24$. The cases of $N = 20$ and 24 are treated in the previous work of authors, and the current work completes the construction of the infinite families of elliptic curves over dihedral quartic number fields with cyclic torsion groups (which do not occur over quadratic extension fields).

[49] An Efficient Construction of Self-Dual Codes (with J. Kim),
Bull. Korean Math. Soc., Vol 51, No. 3 (2015) 915-923.

Abstract Self-dual codes have been actively studied because of their connections with other mathematical areas including t-designs, invariant theory, group theory, lattices, and modular forms. We presented the building-up construction for self-dual codes over $GF(q)$ with $q \equiv 1 \pmod 4$, and over other certain rings. Since then, the existence of the building-up construction for the open case over $GF(q)$ with $q = p^r \equiv 3 \pmod 4$ with an odd prime p satisfying $p \equiv 3 \pmod 4$ with r odd has not been solved. In this paper, we answer it positively by presenting the building-up construction explicitly. As examples, we present new optimal self-dual $[16, 8, 7]$ codes over $GF(7)$ and new self-dual codes over $GF(7)$ with the best known parameters $[24, 12, 9]$.

[50] Codes over Rings and Hermitian Lattices (with S. Dougherty, J-L. Kim), *Designs, Codes and Cryptography*, Vol 76, No 3, (2015) 519-535.

Abstract The purpose of this paper is to study a further connection between linear codes over three kinds of finite rings and Hermitian lattices over a complex quadratic field $K = Q(\sqrt{-\ell})$, where $\ell > 0$ is a square free integer such that $\ell \equiv 3 \pmod 4$. Shaska et al. consider a ring $R = O_K/pO_K$ (p is a prime) and study Hermitian lattices constructed from codes over the ring R. We consider a more general ring $R = O_K/p^eO_K$, where $e \geq 1$. Using p^e allows us to make a connection from a code to a much larger family of lattices. That is, we are not restricted to those lattices whose minimum norm is less than p. We first show that R is isomorphic to one of the following three non-isomorphic rings: a Galois ring $GR(p^e, 2)$, $Z_{p^e} \times Z_{p^e}$, and $Z_{p^e} + uZ_{p^e}$. We then prove that the theta functions of the Hermitian lattices constructed from codes over these three rings are determined by the complete weight enumerators of those codes. We show that self-dual codes over R produce unimodular Hermitian lattices. We also discuss the existence of Hermitian self-dual codes over R. Furthermore, we present MacWilliams' relations for codes over R.

[51] Construction of all cubic function fields of a given square-free discriminant, (with M. Jacobson, R. Scheidler and H. Williams),
International Journal of Number Theory, Vol. 11, No. 6 (2015) 1839-1885.

Abstract For any square-free polynomial D over a finite field of characteristic at least 5, we present an algorithm for generating all cubic function fields of discriminant D. We also provide a count of all these fields according to their splitting at infinity. When $D' = D/(-3)$ has even degree and a non-square leading coefficient, i.e. D' is the discriminant of a real quadratic function field, this method makes use of the infrastructure of this field. This infrastructure method was first proposed by D. Shanks for cubic number fields in an unpublished manuscript from the late 1980s. While the mathematical ingredients of our construction are largely classical, our algorithm has the major computational advantage of finding very small minimal polynomials for the fields in question.

[52] Corrigendum to *A Cheeger inequality of a distance regular graph using Green's function* (with G.C. Kim), Discrete Math. 338 (2015), no. 9, 1621-1623.

Abstract In the published version, we obtain a cheeger inequality of distance regular graphs in terms of the smallest positive eigenvalue of the Laplacian

and a value α_d. However, we confirm that we need an additional condition for our Cheeger inequality of distance regular graphs: if $tvr_i^{(t)} > \lambda_1/1+\lambda_1$ for some $t \leq \alpha_d$, then we obtain a Cheeger inequality of distance regular graphs as $h_\Gamma < \alpha_d/\lambda_1$.

[53] Explicit criterions for p-ary functions being non-bent, (with J. Hyun) *Journal of Mathematical Analysis and Applications (J. Math. Anal. Appl.)*, Vol. 433, No. 2, 1177-1189 (2016).

Abstract There has been only limited information on the existence of p-ary bent functions. Recently, there is a result by authors on finding necessary conditions for the existence of regular p-ary bent functions (from Z_p^n to Z_p), where p is a prime. The general case of p-ary bent functions is, however, an open question for finding necessary conditions for their existence. In this paper we complete this open case.

[54] Modularity of a Ramanujan-Selberg continued fraction, (with Y. Park) *Journal of Mathematical Analysis and Applications*, vol. 438, 373-394, 2016.

Abstract We study a Ramanujan-Selberg continued fraction $S(\tau)$ by employing the modular function theory. We first find modular equations of $S(\tau)$ of level n for every positive integer n by using affine models of modular curves. This is an extension of Baruah-Saikia's results for level $n = 3, 5$ and 7. We further show that the ray class field modulo 4 over an imaginary quadratic field K is obtained by the value of $S^2(\tau)$, and we prove the integrality of $1/S(\tau)$ to find its class polynomial for K with $\tau \in K \cap H$, where H is the complex upper half plane.

[55] Indivisibility of class numbers of real quadratic function fields, (with J. Lee) *Journal of Pure and Applied Algebra*, Volume 220, Issue 8, 2828-2835, 2016.

Abstract In this paper we work on indivisibility of the class numbers of *real* quadratic function fields. We find an explicit expression for a lower bound of the density of real quadratic function fields (with constant field F) whose class numbers are not divisible by a given prime ℓ. We point out that the explicit lower bound of such a density we found only depends on the prime ℓ, the degrees of the discriminants of real quadratic function fields, and the condition: either $\mid F \mid \equiv 1 \pmod{\ell}$ or not.

[56] The level 13 analogue of the Rogers-Ramanujan continued fraction and its modularity, (with Y. Park) *Journal of Number Theory*, Vol. 168, 306-333, 2016.

Abstract We prove the modularity of the level 13 analogue $r_{13}(\tau)$ of the Rogers-Ramanujan continued fraction. We establish some properties of $r_{13}(\tau)$ using the modular function theory. We first prove that $r_{13}(\tau)$ is a generator of the function field on $\Gamma_0(13)$. We then find modular equations of $r_{13}(\tau)$ of level n for every positive integer n by using affine models of modular curves; this is an extension of Cooper-Ye's results with levels $n = 2, 3$ and 7 to every level n. We further show that the value $r_{13}(\tau)$ is an algebraic unit for any $\tau \in K - Q$, where K is an imaginary quadratic field.

[57] Construction of extremal self-dual codes over Z_8 and Z_{16}, (with B. Kim)

Designs, Codes and Cryptography, 81 (2016), no. 2, 239-257.

Abstract We present a method of constructing *extremal* free self-dual codes over Z_8 or Z_{16}. We prove that every *extremal* free self-dual code over Z_{2^m} can be found from a binary extremal Type II code. In this work, extremality of codes is with respect to the Hamming weight. Our construction method is basically a lifting method. We find extremal free self-dual codes over Z_8 or Z_{16} up to lengths 40 by using our explicit algorithms.

[58] Complementary information set codes over $GF(p)$, (with H.J. Kim)
Designs, Codes and Cryptography, 81 (2016), no. 3, 541-555.

Abstract We find a method for constructing complementary information set codes (for short, CIS codes) over a finite field $GF(p)$, where p is an odd prime. We also find a criterion for checking equivalence of CIS codes over $GF(p)$. We complete the classification of all inequivalent CIS codes over $GF(p)$ of lengths up to 8 for $p = 3, 5, 7$ using this construction and criterion. The class of CIS codes over $GF(p)$ includes self-dual codes over $GF(p)$ as its subclass, and some CIS codes are formally self-dual codes as well. Furthermore, we show that long CIS codes over $GF(p)$ meet the Gilbert-Vashamov bound.

[59] Explicit criteria for construction of plateaued functions, (with J. Hyun, J. Lee)
IEEE Transactions on Information Theory, Vol. 62 (2016), Issue 12, 7555-7565.

Abstract We find explicit criteria for construction of p-ary r-plateaued functions with a prime p. We point out that 0-plateaued functions are bent functions; so plateaued functions are more general notion of bent functions. We first derive an explicit form for the Walsh-Hadamard transform of a p-ary r-plateaued function. We then obtain an upper bound on the degree of p-ary r-plateaued functions, and we classify p-ary $(n-1)$-plateaued functions in n variables for $p = 3$ and 5. We also obtain explicit criterions for the existence of p-ary r-plateaued functions. Accordingly, these results lead to much more improved bounds on the existence of p-ary bent functions, comparing with the previous bounds on them.

[60] An upper bound of the Cheeger constant of a distance regular graph,
(with G. Kim), *Bull. Korean Math. Soc.*, Vol. 54, No. 2 (2017), 507-519.

Abstract We present an upper bound of the Cheeger constant of a distance regular graph. Recently, the authors find an upper bound of a distance regular graph under a certain restriction; our new bound is much better than the previous bound, and it is a general bound with no restriction. We point out that our bound is explicitly computable by using the valencies and the intersection matrix of a distance regular graph. As a major tool, we use the discrete Green's function, which is defined as the inverse of β-Laplacian for some positive real number β. We present some examples of distance regular graphs, where we compute our upper bound of their Cheeger constants.

[61] Fundamental units and regulators of an infinite family of quartic function fields
(with J. Lee), J. Korean Math. Soc. vol. 54, No. 2 (2017), 417 - 426.

Abstract We explicitly determine fundamental units and regulators of an infinite family of cyclic quartic function fields L_h of unit rank 3 with a parameter h in a polynomial ring $F_q[t]$, where F_q is the finite field of order q

with characteristic not equal to 2. This result resolves the second part of Lehmer's project for the function field case.

[62] t-CIS codes over $GF(p)$ and orthogonal covering arrays, (with H. Kim) *Discrete Applied Mathematics*, 217, part 3 (2017), 601-612.

Abstract We first show that orthogonal arrays over $GF(p)$ can be explicitly constructed from t-CIS codes over $GF(p)$, where *t-CIS* codes are CIS codes of order $t \geq 2$. With this motivation, we are interested in developing methods of constructing t-CIS codes over $GF(p)$. We present two types of constructions; the first one is a "t-extension method" which is finding t-CIS codes over $GF(p)$ of length tn from given $(t-1)$-CIS codes over $GF(p)$ of length $(t-1)n$ for $t > 2$, and the second one is a "building-up type construction" which is finding t-CIS codes over $GF(p)$ of length $t(n+1)$ from given t-CIS codes over $GF(p)$ of length tn. Furthermore, we find a criterion for checking equivalence of t-CIS codes over $GF(p)$. We find inequivalent t-CIS codes over $GF(p)$ of length n for $t = 3, 4$, $n = 9, 12, 16$, and $p = 3, 5, 7$ using our construction and criterion, and corresponding orthogonal arrays are found.

[63] Regulators of an infinite family of the simplest quartic function fields, (with J. Lee) *Canadian Journal of Mathematics*, Vol. 69, No. 3 (2017), 579-594.

Abstract We explicitly determine regulators of an infinite family $\{L_m\}$ of quartic function fields with a parameter m in a polynomial ring $F_q[t]$, where F_q is the finite field of order q with odd characteristic. Furthermore, we find an explicit criterion for characterization of splitting types of all the places of $\{L_m\}$, and we obtain a lower bound of class numbers of the family $\{L_m\}$. We find all the cyclic quartic function fields in the family $\{L_m\}$ whose class numbers are less than or equal to 4.

[64] Lee weights of cyclic self-dual codes over Galois rings of characteristic p^2, (with B. Kim), *Finite fields and their applications*, Vol. 45 (2017), 107-130.

Abstract We completely determine the minimum Lee weights of cyclic self-dual codes over a Galois ring $GR(p^2, m)$ of length p^k, where m and k are positive integers and p is a prime number. We obtain all cyclic self-dual codes over $GR(2^2, 1) \cong Z_4$ of lengths 16 and 32 with their Lee weight enumerators. We also find cyclic self-dual codes over $GR(3^2, 1) \cong Z_9$ (respectively, $GR(3^2, 2)$) of lengths up to 27 (respectively, 9). Most of the cyclic self-dual codes we found are *extremal* with respect to the Lee weights.

[65] Construction of isodual codes over $GF(q)$, (with H. Kim) *Finite fields and their applications*, Vol. 45 (2017), 372-385.

Abstract We develop a construction method of isodual codes over F_p, where p is a prime number; we construct isodual codes over F_p of length $2n+2$ from isodual codes over F_p of length $2n$. Using this method, we find some isodual codes over F_p, where $p = 2, 3$ and 5. In more detail, we obtain binary isodual codes of lengths $32, 34, 36, 38$, and 40, where all these codes of lengths $32, 34$, and 36 are optimal and some codes of length 38 are optimal. We note that all these binary isodual codes are not self-dual codes, and in particular, in the case of length 38 all their weight enumerators are different from them of

binary self-dual codes of the same length; in fact, four binary isodual codes of length 38 are formally self-dual even codes. We construct isodual codes over F_3 and F_5 of lengths $4, 6$, and 8 as well.

[66] A level 16 analogue of Ramanujan series for $1/\pi$, (with Y. Park)
Journal of Mathematical Analysis and Applications, Vol. 456 (2017), 177-194.

Abstract The modular function $h(\tau)$ is *a level 16 analogue of Ramanujan's series for* $1/\pi$. We prove that $h(\tau)$ generates the field of modular functions on $\Gamma_0(16)$ and find its modular equation of level n for any positive integer n. Furthermore, we construct the ray class field $K(h(\tau))$ modulo 4 over an imaginary quadratic field K for $\tau \in K \cap H$ such that $Z[4\tau]$ is the integral closure of Z in K, where H is the complex upper half plane. For any $\tau \in K \cap H$, it turns out that the value $1/h(\tau)$ is integral, and we can also explicitly evaluate the values of $h(\tau)$ if the discriminant of K is divisible by 4.

[67] Constructions of formally self-dual codes over Z_4 and their weight enumerators, (with B. Kim and J. Yoo), *IEEE Transactions on Information Theory*,
Vol. 63, Issue 12 (2017), 7667-7675.

Abstract We present three explicit methods for construction of formally self-dual codes over Z_4. We characterize relations between Lee weight enumerators of formally self-dual codes of length n over Z_4 and those of length $n+2$; the first two construction methods are based on these relations. The last construction produces free formally self-dual codes over Z_4. Using these three constructions, we can find free formally self-dual codes over Z_4 as well as non-free formally self-dual codes over Z_4 of *all even lengths*. We find free or non-free formally self-dual codes over Z_4 of lengths up to 10 using our constructions. In fact, we obtain 46 inequivalent formally self-dual codes whose minimum Lee weights are larger than self-dual codes of the same length. Furthermore, we find 19 *non-linear extremal binary* formally self-dual codes of lengths 12, 16, and 20, up to equivalence, from formally self-dual codes over Z_4 by using the Gray map.

[68] A continued fraction of order twelve as a modular function, (with Y. Park)
Mathematics of Computation, Vol. 87, Number 312, July (2018), 2011-2036.

Abstract We study a continued fraction $U(\tau)$ of order twelve using the modular function theory. We obtain the modular equations of $U(\tau)$ by computing the affine models of modular curves $X(\Gamma)$ with $\Gamma = \Gamma_1(12) \cap \Gamma_0(12n)$ for any positive integer n; this is a complete extension of the previous result of Mahadeva Naika et al. and Dharmendra et al. to every positive integer n. We point out that we provide an explicit construction method for finding the modular equations of $U(\tau)$. We also prove that these modular equations satisfy the Kronecker congruence relations. Furthermore, we show that we can construct the ray class field modulo 12 over imaginary quadratic fields by using $U(\tau)$ and the value $U(\tau)$ at an imaginary quadratic argument is a unit. In addition, if $U(\tau)$ is expressed in terms of radicals, then we can express $U(r\tau)$ in terms of radicals for a positive rational number r.

[69] J. Lee and Y. Lee,
Regulators and class numbers of an infinite family of quintic function fields,

Acta Arithmetica, 185 (2018), no. 2, 107–125.

Abstract We explicitly determine regulators and the system of fundamental units of an infinite family of totally real quintic function fields K_h with a parameter h in a polynomial ring $F_q[t]$, where F_q is the finite field of order $q = p^r$ with characteristic $\neq 5$. We use the notion of Lagrange resolvents of the generating quintic polynomials of K_h. In fact, this infinite family of quintic function fields are subfields of maximal real subfields of cyclotomic function fields, where they have the same conductors. As an application, we obtain some result on the divisibility of the divisor class numbers of maximal real subfields $k(\Lambda_{P(h)})^+$ of cyclotomic function fields with the same conductor $P(h)$ as K_h. Furthermore, we obtain infinitely many irregular primes of second class $f(t) \in F_q[t]$ such that $h(k(\Lambda_f)^+) \equiv 0 \pmod{p^4}$. Moreover, we find the explicit ideal class number formula of K_h and a lower bound of ideal class numbers of K_h.

[70] Three Ramanujan continued fractions and their modularity (with Y. Park), *Journal of Number Theory*, Vol. 188 (2018), 299-323.

Abstract We study three Ramanujan continued fractions $c(\tau), W(\tau)$ and $T(\tau)$. In fact, $c(\tau)$ and $W(\tau)$ are modular functions on level 16 and $T(\tau)$ is a modular function on level 32. We first find the modular equations of $c(\tau), T(\tau)$ and $W(\tau)$ for any level, which extends the recent work by Saikia, and we compute a list of the modular equations. We prove that the values of $c(\tau)$ and $W(\tau)$ can generate the ray class field modulo 4 over an imaginary quadratic field K. We also prove that $2/(1-c(\tau))$, $1/W(\tau)$, $T(\tau)+1/T(\tau)$ are algebraic integers for any $\tau \in K \cap H$, where H denotes the complex upper half plane. Furthermore, we can express the value $c(r\tau)$ (respectively, $T(r\tau), W(r\tau)$) in terms of radicals for any positive rational number r when the value $c(\tau)$ can be written as radicals (respectively, $T(\tau), W(\tau)$).

[71] A mass formula for cyclic codes over Galois rings of characteristic p^3 (with B. Kim), *Finite fields and their applications*, Vol. 52 (July 2018), 214-242.

Abstract We explicitly determine the generators of cyclic codes of length p^k ($k \geq 1$) over a Galois ring of characteristic p^3 by their *residue degree*, and their two *torsional degrees*; there are exactly three types of cyclic codes, that is, one-generator, two-generator and three-generator cyclic codes. Using this classification result, we obtain a mass formula for cyclic codes over a Galois ring of length p^k.

[72] Characterization of certain types of plateaued functions (with J. Hyun, J. Lee), J. Korean Math. Soc. 55 (Jan. 2018), No. 6, 1469-1483.

Abstract We study a subclass of p-ary functions in n variables, denoted by A_n, which is a collection of p-ary functions in n variables satisfying a certain condition on the exponents of its monomial terms. Firstly, we completely classify all p-ary $(n-1)$-plateaued functions in n variables by proving that every $(n-1)$-plateaued function should be contained in A_n. Secondly, we prove that if f is a p-ary r-plateaued function contained in A_n with $degf > 1+(n-r)(p-1)/4$, then the highest degree term of f is only a single term. Furthermore, we prove that there is no p-ary r-plateaued function in A_n with

maximum degree $(p-1)(n-r)/2+1$. As application, we partially classify all $(n-2)$-plateaued functions in A_n when $p=3,5$, and 7, and p-ary bent functions in A_2 are completely classified for the cases $p=3$ and 5.

[73] Extremal quasi-cyclic self-dual codes over finite fields (with H. Kim), *Finite fields and their applications*, Vol. 52 (July 2018), 301-318.

Abstract We study self-dual codes over a factor ring $R=F_q[X]/(X^m-1)$, equivalently, ℓ-quasi-cyclic self-dual codes of length $m\ell$ over a finite field F_q, provided that the polynomial X^m-1 has exactly three distinct irreducible factors in $F_q[X]$, where F_q is the finite field of order q. There are two types of the ring R depending on how the conjugation map acts on the minimal ideals of R. We show that every self-dual code over the ring R of the first type with length ≥ 6 has free rank ≥ 2. This implies that every ℓ-quasi-cyclic self-dual codes of length $m\ell \geq 6m$ over F_q can obtained by the *building-up construction*, where m corresponds to the ring R of the first type. On the other hand, there exists a self-dual code of free rank ≤ 1 over the ring R of the second type. We explicitly determine the forms of generator matrices of all self-dual codes over R of free rank ≤ 1. We obtain many extremal quasi-cyclic self-dual codes of length 68. For the case that $m=17$, we obtain at least 1566 binary 4-quasi-cyclic self-dual codes of length 68 with minimum weight 12, up to equivalence. Furthermore, for the case that $m=7$, we find at least 9828 binary 10-quasi-cyclic self-dual codes of length 70 with minimum weight 12, up to equivalence, from self-dual codes over the ring R of the second type.

[74] Indivisibility of divisor class numbers of Kummer extensions of the rational function field (with J. Yoo), *Journal of Number Theory* 192 (2018), 270–292.

Abstract We find a complete criterion for a Kummer extension K over the rational function field $k=F_q(T)$ of degree ℓ to have indivisibility of its divisor class number h_K by ℓ, where F_q is the finite field of order q and ℓ is a prime divisor of $q-1$. More importantly, when h_K is not divisible by ℓ, we have $h_K \equiv 1 \pmod{\ell}$. In fact, the indivisibility of h_K by ℓ depends on the number of finite primes ramified in K/k and whether or not the infinite prime of k is unramified in K. Using this criterion, we explicitly construct an infinite family of the maximal real cyclotomic function fields whose divisor class numbers are divisible by ℓ.

[75] The minimum weights of two-point AG codes on norm-trace curves (with B. Kim), *Finite fields and their applications*, Vol. 53, Sep. 2018, 113-139, 2018

Abstract We construct two-point algebraic geometry codes (AG codes) on algebraic curves over a finite field. We find the *order-like bound* on the minimum weights of these codes on algebraic curves, and we prove that this order-like bound is better than the Goppa bound. On norm-trace curves over the finite fields of characteristic 2, we explicitly determine the order-like bounds for one-point AG codes and two-point AG codes. Consequently, it turns out that the order-like bound for two-point AG codes on norm-trace curves is better than that of one-point codes on the same curves except for a few cases.

[76] Characterization of weakly regular p-ary bent functions in terms of

strongly regular graphs (with J. Hyun),
IEEE Transactions on Information Theory, Vol. 65 (Jan. 2019), No. 1, 676-684.

Abstract We characterize the weakly regular p-ary bent functions (from Z_p^n to Z_p) for constructing strongly regular graphs, where p is a prime number. Our work is motivated by interesting results by Chee et al and Tan et al. We, however, use completely different approach, and our parameters of strongly regular graphs include their parameters.

[77] History, tradition, and development of journals of the Korean Mathematical Society,
Science Editing, Vol. 5, No.2, 113-118, 2018.
(with K. Lee & S.D. Jung, Scopus journal)

Abstract In October 1946, mathematicians and physicists founded the Korean Society of Mathematics and Physics, which was relaunched as the Korean Mathematical Society (KMS) in March 1952. This article presents the history of three journals published by the KMS.

[78] Modular equations of a continued fraction of order six (with Y. Park),
Open Mathematics, Vol. 17, Issue 1, 202-219, 2019.

Abstract We study a continued fraction $X(\tau)$ of order six by using the modular function theory. We first prove the modularity of $X(\tau)$, and then we obtain modular equations of $X(\tau)$ of level n for any positive integer n; this includes the result of Vasuki et al. for $n = 2, 3, 5, 7$ and 11. We show that the ray class field modulo 6 over an imaginary quadratic field K can be obtained by the value $X^2(\tau)$. We also show that the value $1/X(\tau)$ is an algebraic integer. Furthermore, we find an explicit relation between $X(\tau)$ and $j(\tau)$, and we can evaluate some values $X(\tau)$ for $\tau \in K$ by using such a relation.

[79] Explicit surjectivity results for Drinfeld modules of rank 2, (with I. Chen)
Nagoya Mathematical Journal, Vol. 234, 17-45, June 2019.

Abstract Let $F = F_q(T)$, $A = F_q[T]$. Given two non-isogenous rank r Drinfeld A-modules ϕ and ϕ' over K, where K is a finite extension of F, we obtain a partially explicit upper bound (dependent only on ϕ and ϕ') on the degree of primes p of K such that $P_p(\phi) \neq P_p(\phi')$, where $P_p(*)$ denotes the characteristic polynomial of Frobenius at p on a Tate module of $*$. The bounds are completely explicit in terms of the defining coefficients of ϕ and ϕ', except for one term, which can be made explicit in the case of $r = 2$. An ingredient in the proof of the partially explicit isogeny theorem for general rank is an explicit bound for the different divisor of torsion fields of Drinfeld modules which detects primes of potentially good reduction.

Our results are a Drinfeld module analogue of Serre's work, but the results we obtain are unconditional because GRH for function fields holds.

[80] Classification of cyclic codes over a non-Galois chain ring $Z_2[u]/(u^3)$,
Finite fields and their applications, Vol. 59, 208-237, Sep. 2019.
(with B. Kim and J. Doo).

Abstract We explicitly determine explicit generators of cyclic codes over a non-Galois finite chain ring $Z_p[u]/(u^3)$ of length p^k, where p is a prime

number and k is a positive integer. We completely classify that there are three types of principal ideals of $Z_p[u]/(u^3)$ and four types of non-principal ideals of $Z_p[u]/(u^3)$, which are associated with cyclic codes over $Z_p[u]/(u^3)$ of length p^k. We then obtain a mass formula for cyclic codes over $Z_p[u]/(u^3)$ of length p^k.

[81] Infinite families of irregular primes in cyclotomic function fields (with J. Lee), *Journal of Number Theory*, Vol. 207, 1-21, Feb. 2020.

Abstract We find both a lower bound and an upper bound on the p-rank of the divisor class group of the fth cyclotomic function field $k(\Lambda_f)$ and the Jacobian of $k(\Lambda_f)\bar{F}_q$, where f is an irreducible polynomial in the rational function field $k = F_q(t)$ and F_q is the finite field of order q with characteristic p. Moreover, we find two types of infinite families of irregular primes f for which the divisor class numbers of the maximal real cyclotomic function fields $k(\Lambda_f)^+$ with conductor f are divisible by N. For the first family of irregular primes, N is equal to $p^{p(p-1)}$, a power of a prime, and for the second family of irregular primes, N is a composite number $(p\ell)^5$ for a prime ℓ different from a prime p. Furthermore, in the former case, the divisor class group of $k(\Lambda_f)^+$ has p-rank at least $p(p-1)$.

[82] Ramanujan graphs and expander families constructed from p-ary bent functions (with J. Hyun, J. Lee),
Designs, Codes and Cryptography, Vol. 88, Issue 2, 453-470, Feb. 2020.

Abstract We find explicit criterions for construction of p-ary r-plateaued functions with a prime p. We point out that 0-plateaued functions are bent functions; so plateaued functions are more general notion of bent functions. We first derive an explicit form for the Walsh-Hadamard transform of a p-ary r-plateaued function. We then obtain an upper bound on the degree of p-ary r-plateaued functions, and we classify p-ary $(n-1)$-plateaued functions in n variables for $p = 3$ and 5. We also obtain explicit criterions for the existence of p-ary r-plateaued functions. Accordingly, these results lead to much more improved bounds on the existence of p-ary bent functions, comparing with the previous bounds on them.

[83] Infinite families of MDR cyclic codes over Z_4 via constacyclic codes over $Z_4[u]/\langle u^2-1\rangle$ (with N. Han, B.H. Kim, B. Kim),
Discrete Mathematics, Vol. 343, Issue 3, 1-12, 2020.

Abstract We find infinite families of MDR cyclic codes over Z_4, which are constructed from α-constacyclic codes over a Frobenius non-chain ring $R := Z_4[u]/\langle u^2-1\rangle$. MDR codes mean *maximum distance with respect to rank* codes in terms of the Hamming weight or the Lee weight. We find an explicit generator of an ideal associated with any α-constacyclic code over R of odd length n for an arbitrary unit α of R. Taking its image under a Gray map associated with α, we find explicit generators of ideals associated with cyclic codes over Z_4 of length $2n$; this leads to construction of infinite families of MDR cyclic codes over Z_4. We obtain 202 *new* cyclic codes over Z_4 of lengths 6, 10, 14, 18, 22, 26, 30, 34, 38, 42, 46, 50 and 54; some of them are MDR codes with respect to the Hamming weight or the Lee weight.

Conference Organizers/Program Committee

Organizer of *2021 SINO conference*,
Ewha Womans University, to be held on July, 2021 (planned).
Program committee of the *ANTS XIII: Algorithmic Number Theory Symposium*:
Wisconsin, US, July 16-20, 2018.
Organizer of the *2018 International Workshop on Graph Theory*:
Ewha Womans University, Jan. 4-7, 2018.
Organizer of the *2017 International Workshop on Computational Mathematics*:
Ewha Womans University, Dec. 14-17, 2017.
Organizer of the *2016 International Workshop on Graph Theory and Combinatorics*:
Ewha Womans University, Feb. 18-20, 2016.
Organizer of the *15th SIAM Conference in Applied Algebraic Geometry (AG15)*:
Minisymposium session on *Class Groups of Global Function field*s,
August 3-7, 2015, Daejeon, S. Korea.
Organizer of *Intensive Lecture Series on Dynamical Arithmetics by C. Lee* (Soongsil University),
Ewha Womans University, June 24 - July 2, 2015 (four lectures).
Organizer of *Intensive Lecture Series on Algorithmic Number Theory on Function Fields by R. Scheidler* (University of Calgary),
Ewha Womans University, Sep. 12 - October 24, 2014 (six lectures).
Organizer of *2014 ICM Satellite Conference on Algebraic Coding Theory*,
Ewha Womans University, Aug. 11-12, 2014.
Local organizing committe of *ICWM 2014 Conference*,
Ewha Womans University, to be held on Aug. 12, Aug. 14, 2014.
Organizer of *Intensive Lectures on Drinfeld modules by Y. Taguchi* (Kyushu University),
Ewha Womans University, June 17-19, 2013.
Organizer of *Korea-Japan Conference on Number Theory and its Related Topics*,
Ewha Womans University, Jan. 21–24, 2013.
Organizer of *2012 KIAS International Conference on Coding Theory and Applications*,
KIAS(Korea Institute for Advanced Study), Seoul, Nov. 15–17, 2012.
2012 The 9th KWMS International Conference,
(Organizer of Algebra Session),
June 21 - 22, 2012, Ewha Womans University.
Organizer of *International Conference on Coding and Cryptography*,
Ewha Womans University, Aug. 24-26, 2011.
2009 International Conference for Women in Mathematics, June 18-19, 2009 (KIAS)
the Sixth KWMS International Conference (Organizer for Algebra session)
International Symposium on Automorphic Forms, L-Functions and Shimura Varieties
(organizer and chair of opening session), Nov. 25 - Nov. 27, 2008 .
2008 International Conference for Women in Mathematics,
the Fifth KWMS International Conference
(organizer, chair of opening session and algebra session),
June 16 - 17, 2008 (Ewha W. University).
2008 Ewha-KMS International Workshop on Cryptography
(organizer and chair of opening session), Ewha W. University, June 19 - 20, 2008.
Workshop: Intensive Lectures on Mathematical Problems in Cryptography
(organizer), Ewha W. University, Jan. 28-29, 2008.

Presentation: Invited Talks and Contributed Talks

The *15th SIAM Conference in Applied Algebraic Geometry (AG15)* Conference:
Minisymposium session in *Class Groups and Zeta Functions*,

August 3-7 (invited talk on Aug. 4), 2015, Daejeon, S. Korea.
(Title: Construction of All Cubic Function Fields of a Given Discriminant)

The *15th SIAM Conference in Applied Algebraic Geometry (AG15)* Conference:
Minisymposium session in Coding Theory,
August 3-7 (invited talk on Aug. 3), 2015, Daejeon, S. Korea.
(Title: Self-dual codes and quasi-cyclic self-dual codes over finite fields and finite rings)

2014 KWMS Leaders Forum, panel speaker,
Nov. 7, 2014, KIAS, S. Korea.

Conference on *the Arithmetic of Function Fields and Related Topics*,
Feb. 18-22, 2013, Pusan, S. Korea.
(Title: Explicit isogeny theorems and different bounds of Drinfeld modules)
(talk on Feb. 19, session chair on Feb. 20)

IMS-NTU Workshop on Coding and Cryptography in Singapore,
Nanyang Technological University, Singapore,
May 22-27, 2011, Invited talk presented on May 24, 2011.
(Title: *Building-up construction of self-dual codes and self-dual codes with an automorphism of prime order*)

Hanyang University Math Department Colloquium, May 12, 2011.
(Title: *Reflection Theorem for class groups of global function fields and its applications)*

Nanyang Technological University, Singapore
Invited talk presented on Aug. 4, 2010.
(Title: *Class groups of global function fields*)

AGC 2010: International Conference on Algebraic and Geometric Combinatorics,
Gyeongju, S. Korea, July 12-16, 2010.
Invited talk presented on July 15, 2010.
(Title: *Building-up construction of self-dual codes*)

2010 NCTS Taiwan-Korea Workshop on Number Theory, Taiwan, July 5-6, 2010.
Invited talk presented on July 6, 2010.
(Title: *Surjectivity results and exponential functions attached to rank 2 Drinfeld modules*)

2010 KWMS International Conference for Women in Mathematics (the 7th one)
Chungnam National University, June 21-22, 2010.
Poster presentation (with Jiae Kim).
(Title: Self-dual Code Construction over $GF(p^k)$ and Z_{p^k} via Diophantine Equations)

AMS Sectional Meeting: 2010 Spring Southeastern Sectional Meeting,
Special session on *Advances in Algebraic Coding Theory*
in Lexington (University of Kentucky) KY, US, March 27-28, 2010.
Invited talk presented on March 27, 2010.
(Title: *Construction of MDS self-dual codes and quasi-cyclic self-dual codes*)

University of Louisville, Colloquium or Department seminar, March 26, 2010
(Title: *Class Groups of Global Function Fields*)

Korea-Japan Number Theory Conference, Seoul National University, 1/20/2010-1/23/2010
invited talk presented on Jan. 20, 2010.
(Title: *Construction of Cubic Function Fields from Quadratic Infrastructure*),

AMS Joint Meetings, invited talk at AMS Special Session on Arithmetic of Function Fields,
San Francisco, USA, January 13-16, 2010 (Wed. - Sat.)
(Title: *The Reflection Theorem for class groups of global function fields and its applications*), presented on Jan. 14, 2010.

2009 IEEE International Symposium on Information Theory (ISIT 2009),
Seoul, S. Korea, July 3, 2009.
(Title: *Self-dual codes using building-up constructions*)
2009 IEEE International Symposium on Information Theory (ISIT 2009),
Seoul, S. Korea, July 3, 2009.
(Title: *Construction of cubic self-dual codes*)
Kyungpook University Math Department Colloquium, May 22, 2009.
(Title: *Class groups of global function fields*)
Ajou University Math Department Colloquium, December 5, 2008.
(Title: *The structure of class groups of global function fields*)
International Workshop: Women in Numbers (WIN) (Invited speaker)
November 2-7, 2008, Banff International Research Station, Canada
(Title: Class groups of function fields II - Increasing the class group rank)
ASARC Number Theory Conference, August 18-21, 2008.
(Title: *Class groups of global function fields*)
(organized by Algebraic Structure and its Applications Research Center)
Inha University Math Department Colloquium, May 15, 2008.
(Title: *The structure of class groups of global function fields*)
Yonsei University Math Department Colloquium, April 17, 2008.
(Title: *Class Groups of Global Function Fields*)
Korea Institute for Advanced Study Number Theory Seminar, March 27, 2008.
(Title: *Hyperelliptic function fields of high three rank*)
Invited speaker at the Number Theory special session of KMS meeting,
(Title: *Cubic Function Fields from Quadratic Infrastructure*), Oct. 21, 2007.
Ewha W. University, Invited talk at Math Department, May 2, 2007
(Title: *Construction of Cubic Function Fields from Quadratic Infrastructure*)
Ewha W. University, Invited talk at Math Department, April 27, 2007
(Title: *Number Theory and its applications to Cryptography and Coding Theory*)
University of British Columbia and Simon Fraser University joint number theory seminar,
November 9, 2006
(Title: *Construction of Cubic Function Fields from Quadratic Infrastructure*)
Invited speaker for the Workshop at the Fields Institute, Toronto, Canada,
–Computational challenges arising in algorithmic number theory and Cryptography
(Title: *Construction of Cubic Function Fields from Quadratic Infrastructure*)
Oct. 30 - Nov. 3, 2006.
Annual Summer Workshop on Computational Mathematics at Simon Fraser University:
CECM day on August 9, 2006
(Title: *Computing the fundamental units and regulators of a cubic function field*)
Simon Fraser University Math Camp, June 27, 2006
(Title: *Public Key Cryptography: Protecting our secrets and our identities*)
University of Calgary, Discrete Mathematics Seminar, March 31, 2006
(Title: *The structure of class groups of global function fields*)
Korea Institute for Advanced Study Number Theory Seminar, December 22, 2005.
(Title: *The structure of class groups of global function fields*)
University of British Columbia, UBC and SFU joint number theory seminar,
November 24, 2005
(Title: *The structure of the class groups of global function fields of any unit rank*)
Ewha Womans University, Invited talk at Math Department, May 20, 2005
(Title: *The Scholz Theorem of quadratic function fields for divisor class groups and ideal class groups)*
Simon Fraser University, Research talk, March 4, 2005.

(Title: *Divisor class groups and ideal class groups of relative quadratic function fields*)
University of North Carolina, Greensboro, Math Department seminar talk, February 24, 2005.
(Title:*Divisor class groups and ideal class groups of quadratic function fields*)
Ohio State University, Research talk, February 21, 2005.
(Title: *The Scholz Theorem of quadratic function fields for both ideal class groups and divisor class groups*)
Ohio State University, Undergraduate talk, February 22, 2005.
(Title: *Public Key Cryptography: Protecting our secrets and our identities*)
California State University, Chico, Colloquium talk, February 11, 2005.
(Title: *The Scholz Theorem of quadratic function fields for both ideal class groups and divisor class groups*)
California State University, Chico, Undergraduate talk, February 11, 2005.
(Title: *Public Key Cryptography: Protecting our secrets and our identities*)
Korea Institute for Advanced Study Number Theory Seminar, December 28, 2004.
(Title: *Reflection Theorems of quadratic function fields for divisor class groups and ideal class groups)*
University of Calgary, Discrete Mathematics Seminar, November 24, 2004
(Title: *Divisor class groups and ideal class groups of relative quadratic function fields*).
Seoul National University, Number Theory Seminar, August 13, 2004.
(Title: *Divisor class groups of relative quadratic function fields*).
Seoul National University, Number Theory Seminar, August 12, 2004.
(Title: *Reflection Theorem and the distribution of class groups of number fields*).
Korea Institute for Advanced Study Number Theory Seminar, July 27, 2004.
(Title: *Subgroups of any order in class groups of global function fields*).
Korea Advanced Institute of Science Technology Math Dept Seminar, July 23, 2004.
(Title: *Subgroups of any order in class groups of global function fields*).
The 1st International Workshop for Korean Women in Mathematics
at Korea Institute for Advanced Study, June 21-23, 2004.
invited talk on June 21, 2004.
(Title: *Class Groups of Global Function Fields: Hyperelliptic Function Fields and Imaginary Function Fields).*
Seoul National University, research talk, May 29, 2004.
(Title: *Computing the Fundamental Units of cubic function fields*).
Smith College, Math Department Faculty Seminar, February 23, 2004.
(Title: *Computing invariants of cubic function fields*).
Ewha Women's University, Joint Seminar of Math Dept and Math Education Dept, August 26, 2003
(Title: *Computation of the Fundamental Units of a Cyclic Cubic Function Field*).
Korea Institute for Advanced Study Number Theory Seminar, August 7, 2003.
(Title: *Computation of the Fundamental Units and the Regulator of a Cyclic Cubic Function Field*).
Pohang University of Science and Technology Math Dept Seminar, August 1, 2003.
(Title: *Computation of the Fundamental Units and the Regulator of a Cyclic Cubic Function Field*).
Korea Institute for Advanced Study Number Theory Seminar, July 3, 2003.
(Title: *Cohen-Lenstra Heuristics and the Spiegelungssatz*).
West Coast Number Theory Conference at San Francisco State University, CA, December 18, 2002
(Title: *Escalatory case and non-escalatory case in Function Fields*).
Smith College, Math Dept Faculty Seminar, April 3, 2002
University of Calgary, Discrete Mathematics Seminar, November 23, 2001

Illinois Number Theory Conference at University of Illinois, Urbana-Champaign, May 19, 2001 (Title: *Fundamental Units in Cubic Function Fields*).
West Coast Number Theory Conference at University of San Diego, CA, December 17, 2000.
University of Delaware, Discrete Mathematics Seminar, October 27, 2000.
University of Arizona Math Dept Seminar, April 4, 2000.
Arizona State University Math Dept Seminar II, October 27, 1999.
Arizona State University Math Dept Seminar I, October 20, 1999.
Korea Institute for Advanced Study Number Theory Seminar, June 30, 1999.
Ewha Women's University Math Dept Seminar, June 23, 1999.
Korea Advanced Institute of Science & Technology Math Dept Seminar, June 21, 1999.
Pohang University of Science and Technology Math Dept Seminar, June 15, 1999.
Southwest Texas State University Math Dept Seminar, March 23, 1999.

Professional Services: Referee and Reviewer

Reviewer for *Zentralblatt MATH* since September 2013
Referee for the *Finite Fields and Their Applications* since 2012
Referee for the *Designs, Codes and Cryptography* since 2012
Referee for the *American Mathematical Monthly*, 2011
Referee for the *IEEE Transactions on Information Theory* since 2008
Referee for the *Advances in Mathematics of Communication* since 2009
Referee for the *Proceedings of the American Mathematical Society* since 2007
Referee for the *Bulletin of Korean Mathematical Society* since 2012
Referee for the *Rocky Mountain Journal*, 2007
Referee for the *International Journal of Information and Coding Theory*, 2007, 2009
Referee for the *Journal of Number Theory*, 2006
Referee for the *Applied Mathematics Letters*, 2005
Referee for the *Proceedings of the American Mathematical Society*, 2004
Reviewer for *Mathematical Reviews of American Mathematical Society* since 2002
Reviewer for *Prentice Hall Publishing Company*, 2004
(reviewed some text book on Discrete Mathematics)
Reviewer for *Jones and Bartlett Publishing Company*, 2004
(reviewed some text book on introductory number theory)

Publication of Books

- *You can count on monsters* by Richard Evan Schwartz,
  – translation of English to Korean
  Publisher: Jiyangsa, Sep. 27, 2011.
  This Korean edition was published by Kidbook Publishing Co. in 2011 by arrangement with A.K. Peters

Academic Services

- **Professional committee and members**

Leader of BK21 PLUS research team
– "Mathematical Science Team for Global Woman Leaders"
Editor of Bulletin of Korean Mathematical Society, 2015/03/01 - 2018/03/01.
Algebra Session Committee of Korea Mathematical Society, 2015/03/01 - 2018/03/01.
Associate member of KIAS (Korea Institute for Advanced Study), 2007/09/01 - current.
Member of board of directors of KWMS, 2012/06/22-2013/06/21.
(Korean Women in Mathematical Sciences)

- **Conference Session Chair**

Organizer of *ICM Satellite Conference on Algebraic Coding Theory*,
Ewha Womans University, to be held on Aug. 11-12, 2014.
Intensive Lectures on Drinfeld modules by Y. Taguchi
(organizer), Ewha W. University, June 3-5, 2013.
Organizer of *2013 Korea-Japan Conference on Number Theory*,
Ewha Womans University, to be held on Jan. 21–24, 2013.
A master of meeting with the president of *International Mathematical Union*
(Title - Sage's Path: Discovering her journey-Professor Ingrid Daubechies!),
LG convention hall, Ewha Womans Univ., July 13, 2012.
2012 The 9th KWMS International Conference,
(Organizer of Algebra Session),
June 21 - 22, 2012, Ewha Womans University.
Organizer of *International Conference on Coding and Cryptography*,
Ewha Womans University, Aug. 24-26, 2011.
2010 KMS Fall Conference, Postech, Oct. 22, 2010.
chair of special session: Coding Theory
AWMS-AWM Networking and Mentoring session,
session chair, Ewha W. University, Dec. 19, 2009.
2009 International Conference for Women in Mathematics, June 18-19, 2009 (KIAS)
the Sixth KWMS International Conference (Organizer for Algebra session)
2009 KMS Spring Conference, Ajou University, April 25, 2009
chair of special session: Coding Theory
International Symposium on Automorphic Forms, L-Functions and Shimura Varieties
(organizer and chair of opening session), Nov. 25 - Nov. 27, 2008 .
2008 International Conference for Women in Mathematics,
the Fifth KWMS International Conference
(organizer, chair of opening session and algebra session),
June 16 - 17, 2008 (Ewha W. University).
2008 Ewha-KMS International Workshop on Cryptography
(organizer and chair of opening session), Ewha W. University, June 19 - 20, 2008.
Workshop: Intensive Lectures on Mathematical Problems in Cryptography
(organizer), Ewha W. University, Jan. 28-29, 2008.

• **Ewha Womans University**

Leader of BK21 PLUS team (2013-2020)
– "Mathematical Science Team for Global Woman Leaders"
Scranton College (Scranton Honors program) Adjunct Professor, 3/1/2009 - current.
Chair of Information Protection Associated Major program,
2/1/2010 - 7/31/2013, 2/1/2016- 6/14/2017.
International Exchange Committee (in College of Natural Sciences), 9/1/2017 - 2/28/2018.
Chair of Mathematics Department, 2/1/2010 - 1/31/2012.
Head of Division of Mathematical and Physical Sciences, 8/1/2010 - 1/31/2012.
Accountant of Graduate Alumnae, 8/1/2011 - 6/30/2013.
Advisory Committee of Student Affairs, 7/1/2009 - 6/30/2010.
Special Lecture for computer science major students
- Title: *Introduction to Public-key Cryptography*, May 6, 2010
Religion Committee, 3/1/2015 - 2/28/2016, 3/1/2009 - 2/28/2010.
Supervisor of Actuarial Science Team, 3/1/2009 - 2/28/2010.
International Exchange Committee (in College of Natural Sciences), 3/1/2008 - 2/28/2010.
Organizer of Math Department Colloquium, Sep. 1, 2007 - December 10, 2008.

Supervision of Ph. D. program students:

– Boran Kim, 3/1/2011 - 8/31/2017
– Jinjoo Yoo, 3/1/2013 - 8/31/2019
– Nayoung Han, 3/1/2019 - current
– Jihye Jeong, 3/1/2020 - current
– Siyoon Lee, 9/1/2020 (planned)

Supervision of Master's Thesis students:
– Jinjoo Yoo, Jiae Kim, 9/1/2008 - 2/28/2010
– Boran Kim, 3/1/2009 - 2/28/2011
– Hyun-Hee Kim, 9/1/2010 - 8/31/2013
– Jung-Im Park, 9/1/2009 - 8/31/2012
– Yesel Jun, 3/1/2011 - 2/28/2013
– Eunhye Lee, 9/1/2011 - 2/28/2013
– Yoonkyung Jang, 3/1/2011 - 8/31/2013
– Minjung Lee, 3/1/2012 - 8/31/2014
– Boreum Kim, 3/1/2012 - 2/28/2015
– Seung Hee Kim, 3/1/2013 - 2/28/2015
– Jisoo Doo, 3/1/2016 - 2/28/2018
– Bohyun Kim, 3/1/2017 - 2/28/2019
– Nayoung Han, 3/1/2017 - 2/28/2019
– Youngin Cho, 3/1/2018 - 2/29/2020
– Jihye Jeong, 3/1/2018 - 2/29/2020
– Siyun Lee, 3/1/2019 - current
– Shinyoo Park, 3/1/2020 - current

Mentor of Post Doctoral Fellows or Research Assistant Professors:
– G. Kim, 3/1/2020 - current
– J. Yoo, 9/1/2019 - current
– H. Jung, 8/1/2019 - 2/29/2020 (current: faculty at Dankook Univ.)
– B. Kim, 9/1/2017 - 7/31/2019 (current: postdoc at Sungkyunkwan Univ.)
– Y. Park, 8/1/2015 - 8/31/2018 (current: faculty at Seoul Tech. Univ.)
– J. Lee, 3/1/2014 - 2/28/2019 (current: faculty at Gangwon Univ.)
– H.J. Kim, 3/1/2011 - 2/28/2016 (current: faculty at Yonsei Univ.)
– J.Y. Hyun, 10/1/2009 - 8/31/2015 (current: faculty at Konkuk Univ.)
– S. Choi, 9/1/2012 - 10/31/2013 (current: Samsung Electrics Company)
– G. Kim, 7/1/2011 - 2/29/2013 (current: faculty at Dong-Ah Univ.)
– S. Chang, 1/1/2010 - 2/28/2012
– S. Han, 9/1/2007 - 2/28/2008 (current: faculty at Korea Univ. of Tech. and Edu.)

• Simon Fraser University

Tenure and Promotion Committee, Simon Fraser University, Fall 2005 - Summer 2007.
MATH 491 *Honors Essay* course for Jacob Groundwater, Fall of 2006.
Supervision of undergraduate research student: May 2006 - August 2006
– Jacob Groundwater, URSA summer student funded by: NSERC
(Project title: Algebraic Coding theory- Construction of Self-dual codes and Quasicyclic codes over finite fields).
Thesis defense supervisory committee, July 27, 2006
– Desmond Leung's Master's Thesis
(Title: Small Prime Solutions to Cubic Diophantine Equations)
Giving a talk at Math camp for high school students on June 27, 2006
(Title: Public Key Cryptography: Protecting Our Secrets).
Information session for undergraduate students on preparing for graduate school:

run by Graduate Study Committee, Jan. 19, 2006.

• **Smith College**

TA supervisor for Math Forum, Fall 2004 - Spring 2005.
Career and Alumnae Panel, Smith College, Fall 2002 - Spring 2004
(Graduate advisor for senior students and arranging allumnae panel meeting).
Second reader for a review of senior's honor thesis of , Smith College, Spring 2003.
Curriculum Review Committe, Smith College, Fall 2003.

Professional Memberships

Associate member of KIAS (Korea Institute for Advanced Study)
Korean Mathematical Society (KMS)
American Mathematical Society (AMS)
Korean Women Association in Mathematical Sciences (KWMS)
Association for Women in Mathematics (AWM)

References

Prof. Michael Rosen
Department of Mathematics
Brown University, Box 1917
Providence, RI 02912
mrosen@math.brown.edu
Phone: (401) 863-2592
Fax: (401) 863-9013

Prof. Joseph Silverman
Department of Mathematics
Brown University, Box 1917
Providence, RI 02912
jhs@math.brown.edu
Phone: (401) 863-1132
Fax: (401) 863-9013

Prof. Renate Scheidler
Department of Mathematics and Statistics
University of Calgary
Calgary AB, Canada T2N 1N4
rscheidl@math.ucalgary.ca
Phone: (403) 220-6628
Fax: (403) 282-5150