Karpuk, David; **Ernvall-Hytönen, Anne-Maria**; **Hollanti, Camilla**; **Viterbo, Emanuele**
Probability estimates for fading and wiretap channels from ideal class zeta functions. (English) Zbl 1366.94768
Adv. Math. Commun. 9, No. 4, 391-413 (2015).

Summary: In this paper, new probability estimates are derived for ideal lattice codes from totally real number fields using ideal class Dedekind zeta functions. In contrast to previous work on the subject, it is not assumed that the ideal in question is principal. In particular, it is shown that the corresponding inverse norm sum depends not only on the regulator and discriminant of the number field, but also on the values of the ideal class Dedekind zeta functions. Along the way, we derive an estimate of the number of elements in a given ideal with a certain algebraic norm within a finite hypercube. We provide several examples which measure the accuracy and predictive ability of our theorems.

MSC:

94B70 Error probability in coding theory
11R42 Zeta functions and L-functions of number fields
11H71 Relations with coding theory
94B75 Applications of the theory of convex sets and geometry of numbers (covering radius, etc.) to coding theory

Keywords:

lattice codes; zeta functions; ideal lattices; inverse norm sum; Rayleigh fading channel

Software:

SageMath

Full Text: DOI arXiv

References:

[1] SAGE open source mathematics software system„ <a href=

[2] J.-C. Belfiore, Lattice code design for the rayleigh fading wiretap channel„ IEEE International Conference on Communications, 1, (2011)

[3] J.-C. Belfiore, An error probability approach to mimo wiretap channels„ IEEE Trans. on Comm., 61, 3396, (2013)

[4] J.-C. Belfiore, Secrecy gain: A wiretap lattice code design„ IEEE International Symposium on Information Theory and its Applications, 174, (2010)

[5] J.-C. Belfiore, Unimodular lattices for the gaussian wiretap channel„ IEEE Information Theory Workshop, 1, (2010)

[6] J. Ducoat, An analysis of small dimensional fading wiretap lattice codes„ IEEE International Symposium on Information Theory, 966, (2014)

[7] A.-M. Ernvall-Hytönen, On the Eavesdropper's Correct Decision in Gaussian and Fading Wiretap Channels Using Lattice Codes,, IEEE Information Theory Workshop, (2011)

[8] C. Hollanti, Analysis on Wiretap Lattice Codes and Probability Bounds from Dedekind Zeta Functions,, IEEE International Congress on Ultra-Modern Telecommunications and Control Systems and Workshops, (2011)

[9] C. Hollanti, Nonasymptotic probability bounds for fading channels exploiting Dedekind zeta functions„ preprint

[10] S. Lang, Algebraic Number Theory„ Second edition. Graduate Texts in Mathematics, (1994) · Zbl 0811.11001

[11] S. Leung-Yan-Cheong, The Gaussian wire-tap channel„ IEEE Trans. on Inf. Theory, 24, 451, (1978) · Zbl 0384.94014

[12] F. Oggier, Lattice codes for the wiretap gaussian channel: Construction and analysis„ Information Theory, pp, (2015) · Zbl 1359.94149

[13] F. Oggier, Algebraic number theory and code design for rayleigh fading channels„ Foundations and Trends in Communications and Information Theory, 1, 333, (2004) · Zbl 1137.94014

[14] S. Ong, Wiretap lattice codes from number fields with no small norm elements„ Designs, 73, 425, (2014) · Zbl 1335.94106

[15] R. Vehkalahti, An algebraic look into MAC-DMT of lattice space-time codes„ IEEE International Symposium on Information

Theory, 2831, (2011)

[16] R. Vehkalahti, Diversity-multiplexing gain tradeoff: A tool in algebra?„ IEEE Information Theory Workshop, 135, (2011)

[17] R. Vehkalahti, Inverse Determinant Sums and Connections Between Fading Channel Information Theory and Algebra„ IEEE Trans. on Inf. Theory, 59, 6060, (2013) · Zbl 1364.94472

[18] R. Vehkalahti, Connecting DMT of division algebra space-time codes and point counting in lie groups„ IEEE International Symposium on Information Theory, 3038, (2012)

[19] A. Wyner, The wire-tap channel„ Bell Syst. Tech. Journal, 54, 1355, (1975) · Zbl 0316.94017