様 式 Ｃ－１９、Ｆ－１９－１、Ｚ－１９ （共通）

科研費 KAKENHI

科学研究費助成事業 研究成果報告書

平成 ２９ 年 ６ 月 ８ 日現在

機関番号： １３３０２
研究種目： 基盤研究(B)（一般）
研究期間： 2014～2016
課題番号： ２６２８９１１９

研究課題名（和文）LatticeNET: Practical Lattice Codes for Cooperative Wireless Networks

研究課題名（英文）LatticeNET: Practical Lattice Codes for Cooperative Wireless Networks

研究代表者

ＫＵＲＫＯＳＫＩ Ｂｒｉａｎ（Kurkoski, Brian）

北陸先端科学技術大学院大学・先端科学技術研究科・准教授

研究者番号：８０４４４１２３

交付決定額（研究期間全体）：（直接経費） 12,400,000円

研究成果の概要（和文）：無線通信システムのスペクトル効率を向上するために新しい実用的な有限長の格子符号化方式を開発した。以下の3つの重要な特性を有する新しい格子符号化方式を提案した：（1）AWGN送信電力制約を満たす(シェーピング利得を高める)、（2）高い誤り訂正能力を有する(符号化利得を高める)、（3）効率的な量子化および復号アルゴリズムを有する。性能・複雑性のトレードオフを改善するために2つの新しい確率伝搬法に基づく格子復号アルゴリズムを開発した。格子計算転送(compute and forward)手法を2つのガウスネットワークに適用し、格子符号化が無線ネットワークのスペクトル効率を改善できることを示した。

研究成果の概要（英文）：We developed new practical, finite-length lattice coding schemes to improve spectral efficiency of wireless communication systems. We developed a new lattice encoding scheme that possesses three important properties: (1) satisfies the AWGN transit power constraint (high shaping gain) (2) has high error-correction capability (high coding gain) (3) efficient quantization and decoding algorithms (low computational complexity). We developed two new belief-propagation lattice decoding algorithms to improve the performance-complexity tradeoff. Lattice compute-and-forward techniques were applied to two Gaussian networks, showing that lattice coding can improve the spectral efficiency of wireless networks.

研究分野： 情報科学

キーワード： 情報理論 符号理論 格子 ネットワーク符号 無線通信

1. 研究開始当初の背景

Wireless communications has become a fundamental societal necessity. From today's smartphones, to tomorrow's autonomous vehicles and the huge variety of "internet of things," an increasingly large number of devices need to share a limited wireless spectrum. In addition, since many devices are battery operated, this must be done in a low power and computationally efficient manner.

Wirelessly networked devices communicate more efficiently by working together. They cooperate in their use of electromagnetic spectrum, where signals use real algebra. Lattices are error-correcting codes which provide reliable transmission using real-valued algebra.

２．研究の目的

The research goal is the development of practical lattices for reliable communication, and their application to wireless networks of networked wireless devices, hence the project name LatticeNet. This work concentrates on lattices, which are codes defined on the real numbers, which differs from error-correcting codes based on finite fields. This work concentrates on the design of finite-length lattices, which differs from recent work on asymptotically long lattices. This work aims to exploit and investigate practical approaches to compute-and-forward, a recent theoretical technique to improve spectrum efficiency in Gaussian wireless networks.

３．研究の方法

The research method consists of the design of lattices and lattice codes, mathematical statements and their proofs, development of decoding algorithms and their software implementation. By separating into the these parts, we can deal with the problems systematically.

４．研究成果

The LatticeNet project is separated into five work packages WP1–WP5, the results are described for each one.

(1) WP1 Cubic Lattice Codes

For cubic lattice codes, two major results dealing with efficient decoding algorithms have been published:

① For decoding low-density lattice codes, we gave a Gaussian belief-propagation decoding algorithm which has the best performance-complexity tradeoff among all decoders, at

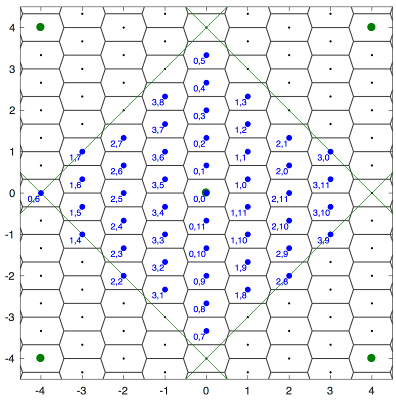

Figure 1: Nested lattice code, where the shaping lattice (green) differs from the coding lattice (blue). While nested lattice codes are known, this research showed how to map information (blue numbers) to lattice code points. This is an important advance towards the use of lattice codes in practical systems.

low and medium dimension [論文4] [発表7].

② For decoding low-density parity-check codes, used as a component of Code Formula lattices, our "max-LUT" method can result in performance better than belief-propagation decoding, while using only 4 bits/message, suitable for an efficient hardware implementation [論文6] [発表9].

These improved decoding algorithms are important both for rapidly evaluating lattice designs, and for power-efficient implementations in battery-powered devices.

In addition, a new construction of low-density lattice codes (LDLC) lattices based on the idea of array codes, borrowed from array low-density parity-check (LDPC) codes, was developed. A triangular matrix structure is highly suitable for practical encoding. These constructions outperform existing LDLC lattice constructions [発表12].

(2) WP2: Nested Lattice Codes & Quantization

We discovered and solved an important lattice coding problem. It was known that "nested lattice codes" can be constructed using separate coding lattices and shaping lattices. This is important because good coding lattices do not usually have efficient quantization algorithms. The problem we solved is how to encode information to lattice code points when the coding lattice and shaping lattices are distinct. This is an important practical aspect, since any communication system must encode information to lattice points. At the same time, the shaping lattice must be selected to have an efficient decoding algorithm. Figure 1 illustrates such a two-dimensional lattice code, and the corresponding encoding of information; the method is valid for lattices of any dimension.

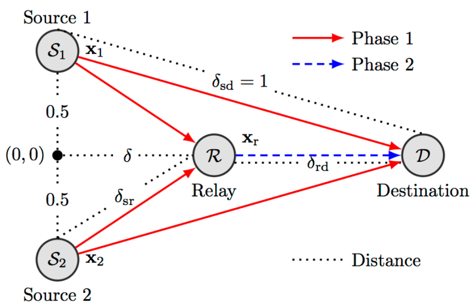

Figure 2: A multiple-access relay channel (MARC) is an important type of Gaussian network. It has two sources (or, transmitters) which both want to transmit data to the destination, with the aid of a relay. Lattice-based compute-and-forward allows sources to transmit at the same time.

There are two types of lattices which are suitable for nested lattice codes, because there exist efficient quantization algorithms. A well-known lattice such as E8 or Barnes-Wall can be used as the shaping lattice and can be combined with a coding lattice to obtain 0.65 to 0.86 dB of shaping gain (out of a maximum of 1.53 dB) [論文3] [発表10]. When the shaping lattice is based on a convolutional code, we showed a nested lattice code with 1.24 dB of shaping gain, when the coding lattice is a low-density lattice code [論文1]. This work has been generalized to shaping and coding lattices which satisfy specific conditions, and is currently under review for journal publication.

(3) WP3: Simple networks: Gaussian Relay Channels

The relay channel is a simple Gaussian network. Write-once memory (WOM) codes allow writing multiple times to a "write-once" memory. We showed that these codes are effective when applied to the relay channel. This is surprising since WOM codes were developed for data storage applications. We showed that WOM codes can achieve the maximum sum-rate for the asymmetric multiple access channel, for one specific rate pair. While WOM codes are not optimal in general, they induce an efficient decoding strategy, to reduce decoding complexity at the destination, when the source and relay transmit simultaneously [論文2] [発表11].

For the parallel relay channel, a new mechanism increases the efficiency when applying hybrid-ARQ to the lossy-forwarding method. We showed that by selectively allowing the relay to either transmit an imperfect packet, or to request retransmission, the end-to-end throughput is significantly improved [論文7].

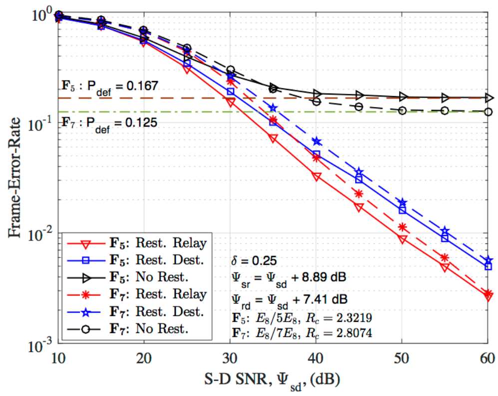

Figure 3: Frame-error rate for the MARC versus signal-to-noise ratio (SNR) for the source-destination, using various compute-and-forward strategies. Naive application of compute-and-forward has an error floor around 10^{-1}, which can be resolved by our proposed strategies.

(4) WP4: Multi-terminal Gaussian Networks

Compute-and-forward techniques significantly improve spectrum utilization in Gaussian networks by allowing sources to transmit simultaneously. Lattices are used to form linear combinations of messages, as well as providing reliability. Two results were published:

① We applied lattice compute-and-forward techniques to the multiple-access relay channel (MARC), a type of Gaussian network. Figure 2 illustrates the MARC which was used. We showed that naive application of lattice codes results in poor performance, and solved this problem by allowing the relays to flexibly select linear equations used by compute-and-forward. Figure 3 shows a numerical result, where the naive approach has an error floor, and both the proposed methods have excellent error-rate performance [発表3]. This work demonstrates the feasibility of non-orthogonal signaling in future wireless communication systems.

② A more sophisticated Gaussian network has two sources, two relays and two destinations; part of this network is pictured in Figure 4. Lattice compute-and-forward can also be applied to this network. In this case, we applied random linear network coding (RLNC) to the network, and found that this generally improves performance in the form of reduced latency [発表2].

These results demonstrate that the theoretical promises of the compute-and-forward techniques can be realized by finite-length lattices to significantly improve spectrum utilization in wireless networks.

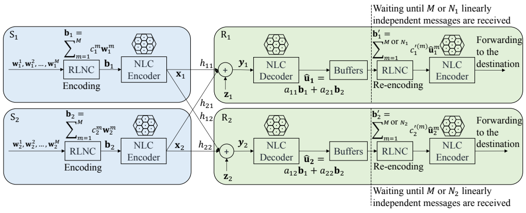

Figure 4: Two-source (blue), two-relay (green), two-destination (not shown) network. Figure shows the architecture for random linear network coding (RLNC) and nested lattice codes (NLC) used by the source and relay.

(5) WP5: Promotion of International Collaboration

Two mini-workshops were held, where project members gave progress report presentations. Overseas project members came to Japan with support from the *Kakenhi* budget. They participated in the workshops, provided feedback and suggestions for future direction. Overseas project members also gave invited seminars on their own research.

① August 25, 2014; held at Japan Advanced Institute of Science and Technology; Nomi, Ishikawa.

② June 22–23, 2015; held at University of Electro-Communications; Chofu, Tokyo

Videos of some presentations can be seen at the project web site http://www.latticenet.org/

As a result of this work package, research connections between researchers in Japan and overseas researchers have been strengthened, and are expected to lead to further collaborations, even after this project finishes.

５．主な発表論文等

〔雑誌論文〕（計７件）

[1] F. Zhou and B. M. Kurkoski, “Shaping LDLC lattices using convolutional code lattices,” *IEEE Communications Letters*, vol. 21, April 2017. DOI 10.1109/LCOMM.2017.2647922. 査読有

[2] R. Sekiya and B. M. Kurkoski, “Applying write-once memory codes to binary symmetric asymmetric multiple access channels,” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E99-A, pp. 2202-2210, December 2016. DOI 10.1587/transfun.E99.A.2202. 査読有

[3] N. S. Ferdinand, M. Nokleby, B. M. Kurkoski, and B. Aazhang, “Low-dimensional shaping for high-dimensional lattice codes,” *IEEE Transactions on Wireless Communications*, vol. 15, pp. 7405-7418, November 2016. DOI 10.1109/TWC.2016.2602205. 査読有

[4] R. A. Parrao Hernandez and B. M. Kurkoski, “The three/two Gaussian parametric LDLC lattice decoding and its analysis,” *IEEE Transactions on Communications*, vol. 64, pp. 3624-3633, September 2016. DOI 10.1109/TCOMM.2016.2594286. 査読有

[5] H. Yagi, T. Han, R. Nomura, "First- and second-order coding theorems for mixed memoryless channels with general mixture", *IEEE Transactions on Information Theory*, vol. 62, no.8, pp.4395-4412, Aug. 2016. DOI 10.1109/TIT.2016.2573310. 査読有

[6] F. J. Cuadros Romero and B. M. Kurkoski, “LDPC decoding mappings that maximize mutual information,” *IEEE Journal on Selected Areas in Communications*, vol. 34, pp. 2391-2401, August 2016. DOI 10.1109/JSAC.2016.2603708. 査読有

[7] A. Irawan, K. Anwar and T. Matsumoto, “Lossy Forwarding HARQ for Parallel Relay Networks,” *Wireless Personal Communications*, pp. 1–16, 2016. DOI 10.1007/s11277-016-3805-8 査読有

〔学会発表〕（計１２件）

[1] B. M. Kurkoski and H. Yagi, “Single-bit quantization of binary-input, continuous-output channels,” IEEE International Symposium on Information Theory, (Aachen, Germany), June 29, 2017. 査読有

[2] R. Ngeth, B. M. Kurkoski, Y. Lim, and Y. Tan, “Random linear network coding over compute-and-forward in multi-source multi-relay networks,” IWCMC 2017 Wireless Networking Symposium, (Valencia, Spain), June 28, 2017. 査読有

[3] M. N. Hasan and B. M. Kurkoski, “Practical Compute-and-Forward approaches for the multiple access relay channel,” IEEE International Conference on Communications, (Paris, France), May 23, 2017. 査読有

[4] T. Nakano, T. Wadayama, “On Zero Error Capacity of Nearest Neighbor Error Channels with Multilevel Alphabet,” International Symposium on Information Theory and Its Applications (ISITA), (Monterey, California, USA), October 31, 2016. 査読有

[5] Y. Fujino, T. Wadayama, “A Construction of Non-Binary WOM Codes based on Integer

Programming," International Symposium on Information Theory and Its Applications (ISITA), (Monterey, California, USA), October 31, 2016. 査読有

[6] R. Nomura, H. Yagi, "Variable-length lossy source coding allowing some probability of union of overflow and excess distortion" Proceedings of IEEE International Symposium on Information Theory (ISIT2016), (Barcelona, Spain), July 15, 2016. 査読有

[7] R. A. Parrao Hernandez and B. M. Kurkoski, "The three/two Gaussian parametric LDLC lattice decoding algorithm and its analysis," IEEE Information Theory Workshop, (Jeju Island, Korea), October 13, 2015. 査読有

[8] T. X. Nguyen, R. A. Parrao Hernandez, and B. M. Kurkoski, "Robust content-based image hash functions using nested lattice codes," International Workshop on Digital Forensics and Watermarking (IWDW 2015), (Tokyo University of Sciences Katsushika Campus, Tokyo, Japan), October 9, 2015. 査読有

[9] F. J. Cuadros Romero and B. M. Kurkoski, "Decoding LDPC codes with mutual information-maximizing lookup tables," IEEE International Symposium on Information Theory, (Hong Kong, China), pp. 426-430, June 15, 2015. 査読有

[10] N. S. Ferdinand, B. M. Kurkoski, B. Aazhang, and M. Latva-aho, "Shaping low-density lattice codes using Voronoi integers," IEEE Information Theory Workshop, (Hobart, Tasmania, Australia), pp. 128-132, November 11, 2014. 査読有

[11] R. Sekiya, E. C. Garcia Alvarez, B. M. Kurkoski, and H. Yagi, "Write-once memory codes for low-complexity decoding of asymmetric multiple access channel," International Symposium on Information Theory and its Applications, (Melbourne, Victoria, Australia), pp. 610-614, October 29, 2014. 査読有

[12] R. A. Parrao Hernandez and B. M. Kurkoski, "Low complexity construction of low density lattice codes based on array codes," International Symposium on Information Theory and its Applications, (Melbourne, Victoria, Australia), pp. 264-268, October 28, 2014. 査読有

〔その他〕
ホームページ:
① http://www.latticenet.org/
② http://brian.kurkoski.org/

６．研究組織

(1) 研究代表者

クルカスキー　ブライアン (Brian Kurkoski)
北陸先端科学技術大学院大学・先端科学技術研究科・准教授
研究者番号：80444123

(2) 研究分担者

和田山　正（Tadashi Wadayama）
名古屋工業大学・工学（系）研究科（研究院）・教授
研究者番号：20275374

松本　正（Tadashi Matsumoto）
北陸先端科学技術大学院大学・先端科学技術研究科・教授
研究者番号：40452114

八木　秀樹（Hideki Yagi）
電気通信大学・大学院情報理工学研究科・准教授
研究者番号：60409737

(3) 連携研究者

なし

(4)研究協力者

なし