2012 International Symposium on Information Theory and its Applications

(ISITA 2012)

Honolulu, Hawaii, USA
28 – 31 October 2012

IEEE

IEEE Catalog Number: CFP1205E-PRT
ISBN: 978-1-4673-2521-9

Program

2012 International Symposium on Information Theory and its Applications

LDPC Codes 1

3-Bit Decoding Algorithm for AWGN Channels
Hiroshi Kamabe (Gifu University, Japan), Hiroshi Ono (Gifu University, Japan) 1

Multi-bit flip type gradient descent bit flipping decoding using no thresholds
Ryoji Haga (Meijo University, Japan), Shogo Usami (Meijo University, Japan) 6

An Improved LT Encoding Scheme with Extended Chain Lengths
Kuo-Kuang Yen (National Chiao Tung University, Taiwan), Chih-Lung Chen (National Chiao Tung University, Taiwan), Hsie-Chia Chang (National Chiao Tung University, Taiwan) 11

Generalization of Lu's Linear Time Encoding Algorithm for LDPC Codes
Kazuki Kobayashi (Sophia University, Japan), Tomoharu Shibuya (Sophia University, Japan) 16

Communication Systems 1

Proposal of New Decision Feedback Carrier Synchronization Method for Meteor Burst Communications
Keisuke Komatsubara (Shizuoka University, Japan), Kaiji Mukumoto (Shizuoka University, Japan), Tadahiro Wada (Shizuoka University, Japan) 21

A study on Read-back Signal Generation Modeling for Shingled-Write Magnetic Recording from Experimental Results
Kohsuke Harada (Toshiba Corp., Japan), Yasushi Tomizawa (Toshiba Corp., Japan), Akihiko Takeo (Toshiba Corp., Japan), Yuuichi Yamada (Toshiba Crop., Japan), Kazuto Kashiwagi (Toshiba Corp., Japan), Kenji Yoshida (Toshiba Corp., Japan) 26

N-PE Transmission System for Narrow-Band PLC
Shinji Tsuzuki (Ehime University, Japan), Yukiaki Yoshizawa (Ehime University, Japan), Intan Sari Areni (Ehime University, Japan), Yoshio Yamada (Ehime University, Japan) 31

Unequal Error Protection with CRC-16 Bits in EPC Class-1 Generation-2 UHF RFID Systems
Robert H Morelos-Zaragoza (San Jose State University, USA) 36

Maximum Mutual Information Rate for The Uniformly Symmetric Variable Noise FSMC without Channel State Information
Benshuai Xu (University of Greenwich, United Kingdom), Zarko B. Krusevac (Australian National University, Australia), Predrag Rapajic (University of Greenwich, United Kingdom), Yifan Chen (South University of Science and Technology of China, P.R. China) 41

Shannon Theory

On Two Strong Converse Theorems for Discrete Memoryless Channels
Yasutada Oohama (University of Electro-Communications, Japan) 46

Optimal Reliability over a DMC with Feedback via Deterministic Sequential Coding
Mohammad Naghshvar (University of California, San Diego, USA), Tara Javidi (UCSD, USA) 51

Non-Binary Serially Concatenated Codes for Distributed Source Coding
Satoru Nakagawa (Kwansei Gakuin University, Japan), Motohiko Isaka (Kwansei Gakuin University, Japan) 56

Wireless Mesh Networks Allowing Intra-Link Errors: CEO Problem Viewpoint
Xin He (Japan Advanced Institute of Science and Technology, Japan), Xiaobo Zhou (Japan Advanced Institute of Science and Technology, Japan), Khoirul Anwar (Japan Advanced Institute of Science and Technology, Japan), Tad Matsumoto (Japan Advanced Institute of Science and Technology, Japan) 61

Power Controlled Adaptive Sum-Capacity in the Presence of Distributed CSI
Krishnamoorthy Iyer (IIT Bombay, India), Sibi Raj B Pillai (IIT Bombay, India), Bikash K Dey (Indian Institute of Technology Bombay, India) 66

Detection and Estimation -- Theory

Bayesian Criteria based on Universal Measures
Joe Suzuki (Osaka University, Japan) 71

The Multiple Sensor Positive Detection Problem
Rhonda Phillips (MIT Lincoln Laboratory, USA) 76

Mean Square Error Reduction by Precoding of Mixed Gaussian Input
John Flåm (Norwegian University of Science and Technology, Norway), Mikko Vehkaperä (Aalto University, Finland), Dave Zachariah (KTH EE, Sweden), Efthymios Tsakonas (KTH, Sweden) 81

Asymptotics of Bayesian estimation for nested models under misspecification
Nozomi Miya (Waseda University, Japan), Tota Suko (Waseda University, Japan), Goki Yasuda (Waseda University, Japan), Toshiyasu Matsushima (Waseda University, Japan) 86

Coding for Flash Memories

Comparing Euclidean, Kendall tau Metrics Toward Extending LP Decoding
Justin Kong (University of Hawaii, USA), Manabu Hagiwara (Advanced Industrial Science and Technology, Japan) 91

On Codes Correcting Bidirectional Limited-Magnitude Errors for Flash Memories
Myeongwoon Jeon (Seoul National University, School of EE, Korea), Jungwoo Lee (Seoul National University, Korea) 96

Lattice-Based WOM Codebooks that Allow Two Writes
Brian Michael Kurkoski (Japan Advanced Institute of Science and Technology (JAIST), Japan) 101

Index-Less Flash Codes with Arbitrary Small Slices
Hiroyuki Nagahara (Nara Institute of Science and Technology, Japan), Yuichi Kaji (Nara Institute of Science and Technology, Japan) 106

Error Control and Applications

A Soft-Decision Sphere Decoding based on the Recursive Vector Generator
Takuya Kusaka (Okayama University, Japan), Ryuhei Yokoyama (Okayama University, Japan), Toru Fujiwara (Osaka University, Japan) 111

Some Results and Challenges on Codes and Iterative Decoding with Non-equal Symbol Probabilities
Bowen Dai (Unversity of Central Florida, USA), Lei Wei (University of Central Florida, USA) 116

Write-Margin Evaluation of LDPC Coding and Iterative Decoding System in BPM R/W Channel with Write-Errors 121
Yasuaki Nakamura (Ehime University, Japan), Yoshihiro Okamoto (Ehime University, Japan), Hisashi Osawa (Ehime University, Japan), Hajime Aoi (Tohoku University, Japan), Hiroaki Muraoka (Tohoku University, Japan)

Mixed-Scheduling Belief Propagation for LDPC Decoders in the Magnetic Recording Systems
..... 125

Watid Phakphisut (King Mongkut's Institute of Technology Ladkrabang, Thailand), Pornchai Supnithi (KMITL, Thailand)

Communication Systems 2

Novel 64QAM Space-Time Codes Using a Large Number of Receive Antennas
Tatsumi Konishi (Aichi Institute of Technology, Japan) 130

Cooperative Reception Scheme Using Multiple Terminals for Digital Terrestrial Television Broadcasting One-Segment Service
Ryo Araki (Tokyo University of Science, Japan), Naoki Kobayashi (Tokyo University of Science, Japan), Akira Nakamura (Tokyo University of Science, Japan), Kohei Ohno (Tokyo University of Science, Japan), Makoto Itami (Tokyo University of Science, Japan) 135

A Theoretical Study on Demodulation of Pre-Coded OFDM by Pre-Coded Symbol Replacement
Naoki Sunaga (Tokyo University of Science, Japan), Kohei Ohno (Tokyo University of Science, Japan), Makoto Itami (Tokyo University of Science, Japan) 140

Complexity reduction using QRD-M or SD in MIMO Interleaved SC-FDMA receiver with iterative detection
Masaaki Moriyama (Nagoya Institute of Technology, Japan), Yasunori Iwanami (Nagoya Institute of Technology, Japan) 145

Interference Mitigation Depending on the Number of Antennas and CSI Available at Femtocells
Genji Hayashi (Keio University, Japan), Tomoaki Ohtsuki (Keio University, Japan) 150

Multi-User Coding 1

On the Redundancy of Variable-Rate Slepian-Wolf Coding
Shigeaki Kuzuoka (Wakayama University, Japan) 155

Computing Polynomial Functions of Correlated Sources: Inner Bounds
Sheng Huang (KTH Royal Institute of Technology, Sweden), Mikael Skoglund (KTH Royal Institute of Technology, Sweden) 160

Layered LDPC Convolutional Codes for Compression of Correlated Sources under Adversarial Attacks
Farshad Naghibi (KTH Royal Institute of Technology, Sweden), Ragnar Thobaben (KTH Royal Institute of Technology, Sweden), Somayeh Salimi (KTH Royal Institute of Technology, Sweden), Mikael Skoglund (KTH Royal Institute of Technology, Sweden) 165

Source Coding with Side Information at the Decoder: Models with Uncertainty, Performance Bounds, and Practical Coding Schemes
Elsa Dupraz (L2S - CNRS - SUPELEC - UniversityParis-Sud, France), Aline Roumy (INRIA Rennes, France), Michel Kieffer (L2S - CNRS - SUPELEC - UniversityParis-Sud, France) 170

An Optimization Algorithm for Scalable Multiple Description Scalar Quantizers
Shahid Satti (Vrije Universiteit Brussel - IBBT, Belgium), Nikos Deligiannis (Vrije Universiteit Brussel – IBBT, Belgium), Adrian Munteanu (Vrije Universiteit Brussel, Belgium), Peter Schelkens (Vrije Universiteit Brussel, Belgium), Jan P.H. Cornelis (Vrije Universiteit Brussel, Belgium) 175

Detection and Estimation -- Applications

Signal Detection and Modulation Classification Using a Goodness of Fit Test *180*
Chiaki Honda (Osaka City University, Japan), Ikuo Oka (Osaka City University, Japan), Shingo Ata (Osaka City University, Japan)

A Study on Location Tracking System using Kalman Filter based on Sensor Information 184

Ryo Ogawara (Utsunomiya University, Japan), Masahiro Fujii (Utsunomiya University, Japan), Yu Watanabe (Utsunomiya University, Japan)

Heart Rate Detection from Waist ECG/PCG Sensors for a Vital Signal Acquisition System for Athletes
Nao Masuoka (Osaka City University, Japan), Tetsuo Tsujioka (Osaka City University, Japan), Shinsuke Hara (Osaka City University, Japan) 189

On Real-Time Arrhythmia Detection in ECG Monitors Using Antidictionary Coding
Takahiro Ota (Nagano Prefectural Institute of Technology, Japan), Hiroyoshi Morita (University of Electro-Communications, Japan) 194

Quantum Information Processing 1

Improvement of 2-EPP using quantum error correcting codes and binary search
Shigeyori Nagahashi (Nagoya Institute of Technology, Japan), Tsuyoshi Usuda (Aichi Prefectural University, Japan), Ichi Takumi (Nagoya Institute of Technology, Japan) 199

Superiority of 2-EPPs to 1-EPPs with finite entangled resources
Yoshiaki Yazaki (Meijo University, Japan), Shogo Usami (Meijo University, Japan), Tsuyoshi Usuda (Aichi Prefectural University, Japan) 203

On the Hardness of Decoding Quantum Stabilizer Codes under the Depolarizing Channel
Kao-Yueh Kuo (National Tsing Hua University, Taiwan), Chung-Chin Lu (National Tsing Hua University, Taiwan) 208

Property of capacity by WDM for attenuated quantum channel
Kazuha Ohashi (Aichi Prefectural University, Japan), Tsuyoshi Usuda (Aichi Prefectural University, Japan) 212

Error Control and Synchronization

An Improvement of Insertion/Deletion/Substitution Error Correction Capabilities of LDPC codes Using Slide Decoding
Tooru Shigehiro (Tokyo University of Science, Japan), Hirohisa Yabe (Tokyo University of Science, Japan), Keiichi Iwamura (Tokyo University of Science, Japan) 216

Insertion/Deletion/Substitution Error Correction using Adaptive Inversion of Synchronization Marker
Masato Inoue (Tokyo Institute of Technology, Japan), Haruhiko Kaneko (Tokyo Institute of Technology, Japan) 221

A direct product construction for high-rate self-synchronizing codes
Yuichiro Fujiwara (Michigan Technological University, USA), Vladimir D. Tonchev (Michigan Technological University, USA) 226

Combined Permutation Codes for Synchronization
Reolyn Heymann (University of Johannesburg, South Africa), Hendrik C Ferreira (University of Johannesburg, South Africa), Theo G. Swart (University of Johannesburg, South Africa) 230

MIMO Diversity Techniques

An Adaptive Conditional Zero-Forcing Decoder with Full-diversity, Least Complexity and Essentially-ML Performance for STBCs
Lakshmi Prasad Natarajan (Indian Institute of Science, Bangalore, India), B. Sundar Rajan (Indian Institute of Science, India) 235

Large System Analysis of Power Minimization in Multiuser MISO Downlink with Transmit-side Channel Correlation
Yichao Huang (University of California, San Diego, USA), Chee Wei Tan (City University of Hong Kong, Hong Kong), Bhaskar Rao (University of California, San Diego, USA) 240

Large-System Analysis of Joint User Selection and Vector Precoding with Zero-Forcing Transmit Beamforming for MIMO Broadcast Channels
Keigo Takeuchi (The University of Electro-Communications, Japan), Ralf R. Müller (Norwegian University of Science and Technology, Norway), Tsutomu Kawabata (University of Electro-Communications, Japan) 245

An Alternate View of Transmit Diversity for the Collocated MIMO System
Vijayvaradharaj Muralidharan (Indian Institute of Science, India), B. Sundar Rajan (Indian Institute of Science, India) 250

Secret Sharing Schemes

Secret sharing schemes based on minimum bandwidth regenerating codes
Masazumi Kurihara (University of Electro-Communications, Japan), Hidenori Kuwakado (Kobe University, Japan) 255

On the Role of Mutual Infomation between the Shares in a Robust (k,n)-Threshold Scheme
Hiroki Koga (University of Tsukuba, Japan), Kazuya Koyano (University of Tsukuba, Japan) 260

Consideration for multi-threshold multi-secret sharing schemes
Atsushi Waseda (National Institute of Information and Communications Technology, Japan), Masakazu Soshi (Hiroshima City University, Japan) 265

Churn Resilience in Network Coding-based Anonymous P2P System
Todorka Alexandrova (Waseda University, Japan), Gergely Huzsak (University of Electro-Communications, Tokyo, Japan), Hiroyoshi Morita (University of Electro-Communications, Japan) 270

Signal Processing

A Design Method for FIR Filters with Complex Coefficients by Successive Projection Method
Toma Miyata (Tokyo University of Science, Japan), Kosuke Teramoto (Free, Japan), Naoyuki Aikawa (Tokyo University of Science, Japan) 275

An L1-Method for Designing FIR Digital Filters with Complex coefficients
Ikuya Murakami (Tokyo University of Science, Japan), Yukio Mori (Salesian Polytechnic, Japan), Naoyuki Aikawa (Tokyo University of Science, Japan) 279

On Statistical Restricted Isometry Property of a New Class of Deterministic Partial Fourier Compressed Sensing Matrices
Nam Yul Yu (Lakehead University, Canada) 284

Performance Bounds for Vector Quantized Compressive Sensing
Amirpasha Shirazinia (KTH Royal Institute of Technology, Sweden), Saikat Chatterjee (KTH - Royal Institute of Technology, Sweden), Mikael Skoglund (KTH Royal Institute of Technology, Sweden) 289

Logarithmic Cubic Vector Quantization: Concept and Analysis
Christian Rohlfing (RWTH Aachen University, Germany), Hauke Krüger (RWTH Aachen University, Germany), Peter Vary (RWTH Aachen University, Germany) 294

Quantum Information Processing 2

Lower Bounds on the Error Probability in Classical and Quantum State Discrimination
Takuya Kubo (University of Electro-Communications, Japan), Hiroshi Nagaoka (University of Electro-Communications, Japan) 299

Explicit receivers for pure-interference bosonic multiple access channels
Mark M Wilde (McGill University, Canada), Saikat Guha (Raytheon BBN Technologies, USA) 303

Error performance of semi-classical quantum receivers for CPPM signals in KCQ key generation
Hiro Yamashita (Aichi Prefectural University, Japan), Tsuyoshi Usuda (Aichi Prefectural University, Japan), Shogo Usami (Meijo University, Japan) 308

Security on the Quantum-type Even-Mansour Cipher
Hidenori Kuwakado (Kobe University, Japan), Masakatu Morii (Kobe University, Japan) 312

Quantum Key Distribution using Mean King Problem with Modified Measurement Schemes
Masakazu Yoshida (Chuo University, Japan), Takayuki Miyadera (AIST, Japan), Hideki Imai (Chuo University, Japan) 317

Ensemble Analysis

Average Growth Rate of Low-Density Generator-Matrix Codes Ensembles
Kazushi Mimura (Hiroshima city university, Japan), Tadashi Wadayama (Nagoya Institute of Technology, Japan), Yoshiyuki Kabashima (Tokyo Institute of Technology, Japan) 322

Probabilistic Analysis of the Network Reliability Problem on a Random Graph Ensemble
Akiyuki Yano (Nagoya Institute of Technology, Japan), Tadashi Wadayama (Nagoya Institute of Technology, Japan) 327

A Coding Theoretic Approach for Evaluating Accumulate Distribution on Minimum Cut Capacity of Weighted Random Graphs
Yuki Fujii (Nagoya Institute of Technology, Japan), Tadashi Wadayama (Nagoya Institute of Technology, Japan) 332

Asymptotic Analysis of Spatially Coupled MacKay-Neal and Hsu-Anastasopoulos LDPC Codes
David G. M. Mitchell (University of Notre Dame, USA), Kenta Kasai (Tokyo Institute of Technology, Japan), Michael Lentmaier (Dresden University of Technology, Germany), Daniel J. Costello, Jr. (University of Notre Dame, USA) 337

Spread Spectrum Systems

Extrinsic Information Transfer Analysis of Finite Field Spreading
Guanghui Song (Doshisha University, Japan), Yuta Tsujii (Doshisha University, Japan), Jun Cheng (Doshisha University, Japan), Yoichiro Watanabe (Doshisha University, Japan) 342

A Novel Spreading Sequence and its Performances for Code-Diversity in DS/CDMA Communication Systems
Hayato Noguchi (Nagaoka National College of Technology, Japan), Shinichi Tachikawa (Nagaoka National College of Technology, Japan) 347

A Novel Synchronization Scheme for Bi-orthogonal Modulation Using Modified Pseudo-Ternary M-sequence
Masaya Yamagata (Ibaraki University, Japan), Hiromasa Habuchi (Ibaraki University, Japan) 352

Analysis of hierarchical multi-pulse PPM using modified pseudo orthogonal M-sequence set
Yusuke Kozawa (Tokyo University of Science, Japan), Hiromasa Habuchi (Ibaraki University, Japan) 357

Performance Analysis of Multi-pulse PPM/CSK on Ultra Wideband Impulse Radio
Tomoyuki Mochizuki (Graduate School of Engineering, Shizuoka University, Japan), Kouji Ohuchi (Shizuoka University, Japan) 362

Multi-User Coding 2

Minimal-Rate Description for Multiple-Access Channels
..... 367

Sue-May Huang (National Chiao Tung University, Taiwan), Hsiao-feng Francis Lu (National Chiao Tung University, Taiwan), Stefan M. Moser (National Chiao Tung University NCTU, Taiwan)

Sending Two Gaussians over the Gaussian MAC with Bandwidth Expansion
Nan Jiang (Texas A&M University, USA), Yang Yang (Texas A&M University, USA), Anders Høst-Madsen (University of Hawaii, USA), Zixiang Xiong (Texas A&M University, USA) 372

Finite Blocklength Bounds for Multiple Access Channels with Correlated Sources
Hideki Yagi (University of Electro-Communications, Japan) 377

Decoding for non-binary signature code
Shan Lu (Doshisha University, Japan), Jun Cheng (Doshisha University, Japan), Yoichiro Watanabe (Doshisha University, Japan) 382

Network Coding

Weighted Sum-rate Functional Dependence Bound for Network Coding Capacity
Xiaoli Xu (Nanyang Technological University, Singapore), Satyajit Thakor (Institute of Network Coding, The Chinese University of Hong Kong, Hong Kong), Yong Liang Guan (Nanyang Technological University, Singapore) 387

A distribution scheme of certificate revocation list by inter-vehicle communication using a random network coding
Taisuke Yamamoto (Nagoya Institute of Technology, Japan), Youji Fukuta (Aichi University of Education, Japan), Masami Mohri (Gifu University, Japan), Masanori Hirotomo (Saga University, Japan), Yoshiaki Shiraishi (Nagoya Institute of Technology, Japan) 392

A Graph Theoretical Approach to Network Encoding Complexity
Easton Li Xu (The University of Hong Kong, Hong Kong), Weiping Shang (Institute of Applied Mathematics, Chinese Academy of Sciences, P.R. China), Guangyue Han (University of Hong Kong, Hong Kong) 396

A Construction of Matroidal Error Correcting Networks
Krishnan Prasad (Indian Institute of Science, India), B. Sundar Rajan (Indian Institute of Science, India) 401

On the Existence of Generalized Rank Weights
Frederique Oggier (Nanyang Technological University, Singapore), Adnen Sboui (Nanyang Technological University, Singapore) 406

Public Key Cryptography 1

Faster Elliptic Curve Arithmetic for Double-Base Chain by Reordering Sequences of Field Operations
Chitchanok Chuengsatiansup (The University of Tokyo, Japan) 411

Improving GGH Cryptosystem for Large Error Vector
Masayuki Yoshino (Hitachi, Ltd, Japan), Noboru Kunihiro (The University of Tokyo, Japan) 416

Homomorphic Encryption Based Cancelable Biometrics Secure against Replay and Its Related Attack
Takato Hirano (Mitsubishi Electric Corporation, Japan), Mitsuhiro Hattori (Mitsubishi Electric Corporation, Japan), Takashi Ito (Mitsubishi Electric Corporation, Japan), Nori Matsuda (Mitsubishi Electric Corporation, Japan), Takumi Mori (Mitsubishi Electric Corporation, Japan) 421

Upper Bound of The Shortest Vector Coefficients and Its Applications
Ken Naganuma (Hitachi, Japan), Masayuki Yoshino (Hitachi, Ltd, Japan), Hisayoshi Sato (Hitachi, Ltd., Japan) 426

Algebraic Codes

Improved multipoint codes from Hermitian curves
Masaya Fujisawa (Tokyo University of Science, Japan), Shojiro Sakata (University of Electro-Communications, Japan) 431

Decoding a Class of Affine Variety Codes with Fast DFT
Hajime Matsui (Toyota Technological Institute, Japan) 436

The Designed Minimum Distance of Medium Lengths for Binary Cyclic Codes
Junru Zheng (Kyushu Women's University, Japan), Takayasu Kaida (Kinki University, Japan) 441

On Improved Algorithms of the Proposed Lower Bound Including Well-Known Bounds for Cyclic Codes
Takayasu Kaida (Kinki University, Japan), Junru Zheng (Kyushu Women's University, Japan) 446

On Nonbinary quantum nonprimitive non-narrow-sense BCH codes
Giuliano Gadioli La Guardia (State University of Ponta Grossa, Brazil) 450

Mobile Communications

Performance of Multihop Decode-and-Forward Relaying assisted Device-to-Device Communication Underlaying Cellular Networks
Donghoon Lee (Korea University, Korea), Sung-Il Kim (Korea University, Korea), Jae Young Lee (Korea university, Korea), Jun Heo (Korea University, Korea) 455

Carrier to Interference Ratio in Shotgun Cellular Systems over Composite Fading Channels
Asma Bagheri (Ferdowsi University of Mashhad, Iran), Ghosheh Abed Hodtani (Ferdowsi University of Mashhad, Mashhad, Iran) 460

User Pairing Algorithms for Multi-cell and Multi-user Communications
Fong-Ru Huang (National Chung Cheng University, Taiwan), Mao-Ching Chiu (National Chung Cheng University, Taiwan), Wern-Ho Sheen (Chaoyang University of Technology, Taiwan) 465

Performance Evaluation of The Modified Binary Countdown Scheme Considering The Priority of Packet
Koichiro Hashiura (Akita Prefectural University, Japan), Fumie Ono (National Institute of Information and Communications Technology, Japan) 470

A VLC Receiving Devise Using Audio Jacks with a Folding Noise
Yuta Ashida (Ryukoku University, Japan), Kuniyoshi Okuda (Ryukoku University, Japan), Wataru Uemura (Ryukoku University, Japan) 475

Data Compression and Complexity

A Fast Binary Arithmetic Coding Using Probability Table of Expanded Symbols
Shota Kanahara (Graduate School of Engineering, Utsunomiya University, Japan), Madoka Hasegawa (Utsunomiya University, Japan), Shigeo Kato (Utsunomiya University, Japan), Yuichi Tanaka (Tokyo University of Agriculture and Technology, Japan) 480

On Variable-to-Fixed Length Coding of A General Source with Infinite Alphabet
Mitsuharu Arimura (Shonan Institute of Technology, Japan), Ken-ichi Iwata (University of Fukui, Japan) 485

On the Maximum Redundancy of CSE for I.I.D. Sources
Ken-ichi Iwata (University of Fukui, Japan), Mitsuharu Arimura (Shonan Institute of Technology, Japan), Yuki Shima (University of Fukui, Japan) 489

Universal Codes on Continuous Alphabet using Sparse Matrices
Shigeki Miyake (NTT, Japan), Jun Muramatsu (NTT Corporation, Japan) 493

On the ratio between the maximal T-complexity and the T-complexity of random strings
T. Aaron Gulliver (University of Victoria, Canada), Ulrich Speidel (University of Auckland, New Zealand) 498

Data Networks

Optimal Scheduling for Two Sources over Time Varying Wireless Channels
Mohamed Kashef (University of Maryland, College Park, USA), Anthony Ephremides (University of Maryland at College Park, USA) 501

Revisiting Minimum-Length Scheduling in Wireless Networks: An Algorithmic Framework
Qing He (Linköping University, Sweden), Vangelis Angelakis (Linköping University, Sweden), Anthony Ephremides (University of Maryland at College Park, USA), Di Yuan (Linköping University, Sweden) 506

On Rate Scaling Laws with CDF-based Distributed Scheduling in Multicell Networks
Yichao Huang (University of California, San Diego, USA), Bhaskar Rao (University of California, San Diego, USA) 511

Memory Placement in Network Compression: Line and Grid Topologies
Mohsen Sardari (Georgia Institute of Technology, USA), Ahmad Beirami (Georgia Institute of Technology, USA), Faramarz Fekri (Georgia Institute of Technology, USA) 516

Secret Key Cryptography

A middletext distinguisher for full CLEFIA-128
Kazumaro Aoki (NTT, Japan) 521

A Peculiar Higher Order Differential of CLEFIA
Naoki Shibayama (Tokyo University of Science, Japan), Toshinobu Kaneko (Tokyo University of Science, Japan) 526

The Optimal Key Estimation of Stream Ciphers and Its Approximation Algorithm Based on a Probabilistic Inference
Yuji Iikubo (Waseda University, Japan), Shunsuke Horii (Waseda University, Japan), Toshiyasu Matsushima (Waseda University, Japan) 531

HB^\flat Protocol For Lightweight Authentication; Its Information Theoretic Indistinguishability Against MITM Attack Watching Reader's Response
Xuedi Song (Chuo University, Japan), Kazukuni Kobara (AIST, Japan), Kentaro Imafuku (AIST, Japan), Hideki Imai (Chuo University, Japan) 536

Another Look on the Relation between Template Attack and Higher Order DPA
Yuichi Komano (Toshiba Corporation, Japan), Hideo Shimizu (Toshiba Corporation, Japan), Chiho Mihara (Toshiba Corporation, Japan) 541

LDPC Codes 2

Unequal Error Protection QC-LDPC Codes via Masking
Chi-Jen Wu (National Tsing Hua University, Taiwan), Chung-Hsuan Wang (National Chiao Tung University, Taiwan), Chi-chao Chao (National Tsing Hua University, Taiwan) 546

An Efficient Method for Computing the Weight Spectrum of LDPC Convolutional Codes Constructed from Quasi-Cyclic Codes
Masanori Hirotomo (Saga University, Japan), Masakatu Morii (Kobe University, Japan) 551

Weight Enumerator Analysis for (2,P)- and (3,P)-SFA LDPC Codes
Manabu Hagiwara (Advanced Industrial Science and Technology, Japan), James Nation (University of Hawaii at Manoa, USA) 556

Optical Communications

Consideration on modified Gold sequences for Optical CDM
Satoru Aoyama (Meijo University, Japan), Shogo Usami (Meijo University, Japan) 561

An Evaluation of a Parallel Transmission Visible Light Communication System employing an LDPC code
Junya Amano (Shizuoka University, Japan), Tadahiro Wada (Shizuoka University, Japan), Kaiji Mukumoto (Shizuoka University, Japan) 566

A Study on Code Construction of Optical Orthogonal Codes with Variable Chip Rates
Tetsuo Tsujioka (Osaka City University, Japan) 571

BER Performance of Multiplexed CSK using Linear/Circular Polarization in Optical Wireless Communications
Chiharu Mukai (Graduate School of Engineering Shizuoka University, Japan), Kouji Ohuchi (Shizuoka University, Japan) 576

Two-Level Signaling for IPACT in Passive Optical Networks
Shoichiro Matsumoto (Chiba Institute of Technology, Japan), Koji Kamakura (Chiba Institute of Technology, Japan) 581

Applications of Information Theory

Localization of Faults in Software Programs Using Bernoulli Divergences
Shounak Roychowdhury (University of Texas at Austin, USA), Sarfraz Khurshid (University of Texas at Austin, USA) 586

Formalization of Gaussian Integers, Gaussian Rational Numbers, and Their Algebraic Structures with Mizar
Yuichi Futa (Shinshu University, Japan), Daichi Mizushima (Shinshu University, Japan), Hiroyuki Okazaki (Shinshu University Graduate School, Japan) 591

On the Second-Order Nonlinearity of Cubic Maiorana-McFarland Boolean Functions
Nicholas Kolokotronis (University of Peloponnese, Greece), Konstantinos Limniotis (National and Kapodistrian University of Athens, Greece) 596

A Greedy Algorithm for Checking Normality of Cryptographic Boolean Functions
Nicholas Kolokotronis (University of Peloponnese, Greece), Konstantinos Limniotis (National and Kapodistrian University of Athens, Greece) 601

Sequences

On a Shannon Cover of Certain Reducible Shift of Finite Type
Akiko Manada (The University of Electro-Communications, Japan) 606

Linear complexity of quaternary sequences constructed from binary Legendre sequences
Young-Sik Kim (Chosun University, Korea), Ji-Woong Jang (LG Electronics, Korea), Sang-Hyo Kim (Sungkyunkwan University, Korea), Jong-Seon No (Seoul National University, Korea) 611

On the Linear Complexity over F_p of Quaternary Sequences from Binary Sidel'nikov Sequences
Young-Sik Kim (Chosun University, Korea), Ji-Woong Jang (LG Electronics, Korea), Sang-Hyo Kim (Sungkyunkwan University, Korea), Jong-Seon No (Seoul National University, Korea) 615

Distribution of the Loops on the Logistic Maps over Integers for the Control Parameter *620*
Takeru Miyazaki (The University of Kitakyushu, Japan), Shunsuke Araki (Kyushu Institute of Technology, Japan), Satoshi Uehara (The University of Kitakyushu, Japan)

Fourier Analysis of Sequences over a Composition Algebra of the Real Number Field
..... 625

Takao Maeda (University of Aizu, Japan), Takafumi Hayashi (University of Aizu, Japan)

Watermarking 1

Digital Watermarking Method by Selecting Suitable Pixel Value from Pixel Value Candidates Near to Original Pixel Value
Motoi Iwata (Osaka Prefecture University, Japan) 629

An Implementation of Steganography Using Construction of Huffman Tree
Hiroshi Yamamoto (Tokai University, Japan), Hayato Fujioka (Tokai University, Japan) 634

An Improvement of Steganography Scheme Based on Complete Complementary Codes
Ryusuke Mayuzumi (The University of Electro-Communications, Japan), Tetsuya Kojima (Tokyo National College of Technology, Japan) 638

Analysis of Binary Fingerprinting Codes under Relaxed Marking Assumption
Minoru Kuribayashi (Kobe University, Japan) 643

Convolutional Codes

Error-Trellises for Tailbiting Convolutional Codes
Masato Tajima (University of Toyama, Japan), Koji Okino (University of Toyama, Japan) 648

Reconstruction of Constellation Labeling with Convolutional Coded Data
Nicolas Sendrier (INRIA, France), Marion Bellard (INRIA Rocquencourt, France) 653

Theoretical analysis of bit error probability for punctured convolutional codes
Hideki Yoshikawa (Tohoku Gakuin University, Japan) 658

A Construction of High Rate Punctured Convolutional Codes
Hiroshi Sasano (Kinki University, Japan), Sen Moriya (Kinki University, Japan) 662

Cooperative Communications 1

Coupling Effects between Transmit and Receive Antennas in Frequency Offset Amplify-and-Forward Relay
Naoki Kikuchi (Keio University, Japan), Mamiko Inamori (Keio University, Japan), Yukitoshi Sanada (Keio University, Japan) 667

SAGE-based Estimation Algorithms for Time-varying Channels in Amplify-and-Forward Cooperative Networks
Nico Aerts (Ghent University, Belgium), Marc Moeneclaey (Ghent University, Belgium) 672

Trade-Off of Multiplexing-Diversity Gain for High Throughput Multiple-Hop MIMO Relay System
Pham Thanh Hiep (Yokohama national university, Japan), Ryuji Kohno (Yokohama National University, Japan) 677

MIMO Detect-and-Forward Relay scheme using Symbol LLR Threshold
Daniel Ciarlini Pinheiro (Nagoya Institute of Technology, Japan), Yasunori Iwanami (Nagoya Institute of Technology, Japan) 682

Multi-User Coding 3

Energy Efficiency in Large Interference Networks 687
Minqi Shen (University of Hawaii, USA), Anders Høst-Madsen (University of Hawaii, USA), Yabo Li (Zhejiang University, P.R. China)

Energy Efficiency in Fading Interference Channels under QoS Constraints
..... 692

Mustafa Ozmen (Syracuse University, USA), M. Cenk Gursoy (Syracuse University, USA), Pramod Varshney (Syracuse University, USA)

Cognitive Interference Channels with Confidential Messages under Randomness Constraint
Shun Watanabe (Tokushima University, Japan), Yasutada Oohama (University of Electro-Communications, Japan) 697

Machine Learning

Accuracy of Latent Variable Estimation with the Maximum Likelihood Estimator for Partially Observed Hidden Data
Keisuke Yamazaki (Tokyo Institute of Technology, Japan) 707

Fault Diagnosis Algorithm in Multi-Computer Systems based on Lagrangian Relaxation Method
Shunsuke Horii (Waseda University, Japan), Manabu Kobayashi (Shonan Institute of Technology, Japan), Toshiyasu Matsushima (Waseda University, Japan), Shigeichi Hirasawa (Waseda University, Japan) 712

An Error Probability Estimation of the Document Classification Using Markov Model
Manabu Kobayashi (Shonan Institute of Technology, Japan), Hiroshi Ninomiya (Shonan Institute of Technology, Japan), Toshiyasu Matsushima (Waseda University, Japan), Shigeichi Hirasawa (Waseda University, Japan) 717

Chinese Text Categorization Using the Character N-gram
Makoto Suzuki (Shonan Institute of Technology, Japan), Naohide Yamagishi (Shonan Institute of Technology, Japan), Tsai Yiching (Kang Ning University, Japan) 722

Public Key Cryptography 2

Scheme Overcoming Incompatibility of Privacy and Utilization of Personal Data
Shigeo Tsujii (Chuo University, Japan), Kohtaro Tadaki (Chuo University, Japan), Ryo Fujita (Chuo University, Japan), Hiroshi Yamaguchi (Chuo University, Japan), Masahito Gotaishi (Chuo University, Japan), Yukiyasu Tsunoo (NEC Corporation, Japan), Takahiko Syouji (YDK Technologies Company, Japan), Norihisa Doi (Chuo University, Japan) 727

Security Analysis of Shifted Odd Knapsack Public Key Encryption Scheme
Ryuichi Sakai (Osaka Electro-Communication University, Japan), Yasuyuki Murakami (Osaka Electro-Communication University, Japan), Masao Kasahara (Osaka Gakuin University, Japan) 731

A Public-key Cryptosystem Based on Decision Version of Subset Sum Problem
Yasuyuki Murakami (Osaka Electro-Communication University, Japan), Shinsuke Hamasho (Osaka Electro-Communication University, Japan), Masao Kasahara (Osaka Gakuin University, Japan) 735

A Study on Precision of Pseudorandom Number Generators Using the Logistic Map
Shunsuke Araki (Kyushu Institute of Technology, Japan), Takeru Miyazaki (The University of Kitakyushu, Japan), Satoshi Uehara (The University of Kitakyushu, Japan), Ken'ichi Kakizaki (Kyushu Institute of Technology, Japan) 740

Polar and Sparse Graph Codes

Polar codes for private classical communication
Mark M Wilde (McGill University, Canada), Joseph M Renes (ETH Zurich, Switzerland) 745

Performance of Mismatched Polar Codes over BSCs *750*
Mine Alsan (EPFL, Switzerland)

Fast Linear-Programming Decoding of LDPC Codes over GF(2^m)
..... 754

Junya Honda (The University of Tokyo, Japan), Hirosuke Yamamoto (The University of Tokyo, Japan)

A Hybrid Structured Turbo Code of CBRM in Conjunction with XOR Coded Parity Compression
Yasuhiro Kitamura (Osaka University, Japan), Shinsuke Ibi (Osaka University, Japan), Seiichi Sampei (Osaka University, Japan) 759

Cooperative Communications 2

Error-Controlling Scheme with Encoding and Spreading in Multi-hop Relay Network
Eriko Saeki (Yokohama National University, Japan), Ryuji Kohno (Yokohama National University, Japan) 764

Capacity Bounds for the Alternative Relaying Diamond Channel with Conferencing Links
Chuan Huang (Texas A&M University, USA), Shuguang Cui (Texas A&M University, USA) 769

A Design of Code-Aided Channel Estimation in Two-Way Relay Networks
Ping-Chung Wang (National Taiwan University, Taiwan), Hua-Lung Tsai (National Taiwan University, Taiwan), Mao-Chao Lin (National Taiwan University, Taiwan) 774

Speech/Image Processing

A system combining extrapolated and interpolated side information for single view multi-hypothesis distributed video coding
Daniel Louw (Tokyo Institute of Technology, Japan), Haruhiko Kaneko (Tokyo Institute of Technology, Japan) 779

Steganalysis of synthetic low-colour images
Sathiamoorthy Manoharan (University of Auckland, New Zealand) 784

A New Robust Pitch Determination Algorithm for Telephone Speech
Liang Chang (Tsinghua University, P.R. China), Jingde Xu (Tsinghua University, P.R. China), Kun Tang (Tsinghua University, Taiwan), Huijuan Cui (Tsinghua University, P.R. China) 789

Watermarking 2

Performance Characteristics of LSB Steganalysis Based on Statistics of Image Difference Signal
Tadakazu Sakakura (Kanazawa Technical College, Japan), Akira Hayashi (Kanazawa Institute of Technology, Japan) 792

New Hybrid Additive-Multiplicative Watermarking with Better Tradeoff between Image Quality and Detection Accuracy
Seigo Ikeda (Osaka University, Japan), Maki Yoshida (Osaka University, Japan), Toru Fujiwara (Osaka University, Japan) 797

Proposal of a watermarking scheme using winding number and unneeded synchronism
Hiroki Nishikawa (Tokyo University of Science, Japan), Yoshio Kakizaki (Tokyo University of Science, Japan), Keiichi Iwamura (Tokyo University of Science, Japan) 802

Private and Blind Digital Fingerprinting Schemes Based upon Complete Complementary Codes
Tetsuya Kojima (Tokyo National College of Technology, Japan), Naoki Ohtani (NHK Media Technology Inc., Japan) 806