Paper ID: 64626
oral
student

IAF SPACE COMMUNICATIONS AND NAVIGATION SYMPOSIUM (B2)
Advances in Space-based Communication Technologies, Part 1 (4)

Author: Mr. Jose Velazquez
University of Puerto Rico, United States

Prof.Dr. Heeralal Janwa
University of Puerto Rico, Puerto Rico

LDPC CODES CONSTRUCTED VIA NEW BENT/NEAR-BENT FUNCTIONS: PROPERTIES AND APPLICATIONS TO NASA DEEP SPACE

Abstract

Efficiency and reliability of error-correction are important in NASA's deep-space missions. For the Mariner spacecraft, Reed-Solomon codes were used for error-correction and Turbo codes with faster decoding for later space missions. Recently, linear-time decodable Low-Density-Parity-Check (LDPC) codes and protograph-based LDPC codes have been proposed for future NASA deep-space missions in various proposals the Jet propulsion laboratory's (JPL) information processing group. The iterative decoding of LDPC codes using factor graphs and belief propagation has linear time complexity. Our approach copies the check nodes once and permutes the copied edges among the original message nodes. JPL has also shown how one can solve the error-floor problems of LDPC codes using protographs and working with non-binary codes. Our construction is via replacing permutations with functions that we have discovered that have exceptional properties.

Our work optimizes decoding and error-correction efficiency through belief propagation analysis of new LDPC codes by selecting Boolean functions that we have discovered with good properties, improving JPL standard. Their unique properties include: bentness and near-bentness; newer ones not obtained by Dillon and Dobbertin; satisfy McGuire Conjecture; have few weights in the dual code—some with three non-zero weights (connected to strongly regular graphs, difference sets, Hadamard matrices, Latin squares, 3-rank permutation groups; the minimum weight span the check matrix; generalize the BCH codes.

A function over Galois fields, $f : GF(q)^n \to GF(q)^m$, is called a vectorial Boolean function. Almost-Perfect-Nonlinear (APN) vectorial Boolean power functions were investigated by Janwa and Wilson (1991), and Janwa, Wilson, and McGuire (1995), and later by scores of other researchers. Janwa and Wilson gave precise conditions under which the Gold and Kasami-Welch functions lead to 2-error-correcting codes. Equivalently, they are APN functions. Carlet, Dobbertin and Dillon investigated the bent and near-bent functions $Tr(\lambda x^d), Tr(x^d)$, respectively. We generalize their results to obtain new Bent functions. We construct our LDPC codes from these new functions. For our LDPC codes, use Neal's software and give performance analysis in terms of dB gains and compare them to the existing NASA standards of LDPC codes for future space missions, as proposed by the JPL group. Our codes can be compared with LDPC codes from partial geometries and generalized quandragles that reach Shannon capacity (Diao et. al (IEEE TIT, 2015) for AWGN channels). They can also be used as polar coding for forward error-correction in space communications (in line with those proposed by Naimipour et al NASA group 2019).