FARZANE AMIRZADE, Carleton University

QC-LDPC construction free of small size elementary trapping sets based on multiplicative subgroups of a finite field

An algebraic-based quasi-cyclic low-density parity-check (QC-LDPC) code is developed from an exponent matrix whose entries belong to a finite field $\mathbb{F}_q$, where q is a power of a prime. A QC-LDPC code with variable node degree m and check node degree n is an (m, n)-regular QC-LDPC code. The length of the shortest cycle in the Tanner graph is the girth. It is experimentally known that short cycles and other graphical structures of the Tanner graph named as (a, b) elementary trapping set ((a, b)-ETSs) with small size a cause high decoding failure rate.

We propose a new method to construct algebraic-based QC-LDPC codes with girth 6, using multiplicative subgroups of a finite field. Some algebraic-based QC-LDPC code constructions in the literature are special cases of our construction. Then, we provide sufficient conditions to construct $(3, n)$-regular algebraic-based QC-LDPC codes with girth 6 and free of (a, b) ETSs with $a \leq 5$ and $b \leq 2$.