

# Symmetric LDPC Codes and Local Testing

*Tali Kaufman and Avi Wigderson*

## Abstract

Coding theoretic and complexity theoretic considerations naturally lead to the question of generating symmetric, sparse, redundant linear systems. This paper provides new way of constructions with better parameters and new lower bounds.

Low Density Parity Check (*LDPC*) codes are linear codes defined by short constraints (a property essential for *local testing* of a code). Some of the best (theoretically and practically) used codes are LDPC. *Symmetric* codes are those in which all coordinates “look the same”, namely there is some transitive group acting on the coordinates which preserves the code. Some of the most commonly used locally testable codes (especially in PCPs and other proof systems), including all “low-degree” codes, are symmetric. Requiring that a symmetric binary code of length  $n$  has large (linear or near-linear) distance seems to suggest a “conflict” between 1/rate and density (constraint length). In known constructions, if one is constant then the other is almost worst possible –  $n/\text{poly}(\log n)$ .

Our main positive result simultaneously achieves *symmetric* low density, constant rate codes generated by a *single* constraint. We present an *explicit* construction of a symmetric and transitive binary code of length  $n$ , near-linear distance  $n/(\log \log n)^2$ , of constant rate and with constraints of length  $(\log n)^4$ .

The construction is in the spirit of Tanner codes, namely the code words are indexed by the edges of a sparse regular expander graph. The main novelty is in our construction of a transitive (non Abelian!) group acting on these edges which preserves the code. Our construction is one instantiation of a framework we call *Cayley Codes* developed here, that may be viewed as extending zig-zag product to symmetric codes.

Our main negative result is that the parameters obtained above cannot be significantly improved, as long as the acting group is solvable (like the one we use). More specifically, we show that in constant rate and linear distance codes (aka “good” codes) invariant under solvable groups, the density (length of generating constraints) cannot go down to a constant, and is bounded below by  $\log^{(\Omega(\ell))} n$  if the group has a derived series of length  $\ell$ . This negative result precludes natural local tests with constantly many queries for such solvable “good” codes.