On relative constant-weight codes.

Summary: In this paper, relative two-weight and three-weight codes are studied, which are both called relative constant-weight codes. A geometric approach is introduced to construct and characterize relative constant-weight codes, using the finite projective geometry. A sufficient and necessary condition is derived for linear codes to be relative constant-weight codes, based on the geometric approach. A family of infinite number of relative constant-weight codes are constructed, which includes dual Hamming codes and subcodes of punctured Reed-Muller codes as special instances. It is well known that determining all the minimal codewords is a hard problem for an arbitrary linear code. For relative constant-weight codes, minimal codewords are completely determined in this paper. Based on the above-mentioned results, applications of relative constant-weight codes to wire-tap channel of type II and secret sharing are discussed. A comparative study shows that relative constant-weight codes form a new family. They are not covered by the previously well-known three-weight codes or linear codes for which minimal codewords can be determined.

Keywords: relative two-weight code; relative three-weight code; minimal codeword; finite projective geometry; wire-TAP channel of type II; secret sharing