Advances in Mathematics of Communications
Volume 2, No. 1, 2008, 15–33
Web site: http://www.aimSciences.org

DUALITY FOR SOME FAMILIES OF CORRECTION CAPABILITY OPTIMIZED EVALUATION CODES

Maria Bras-Amorós

Departament d'Enginyeria Informàtica i Matemàtiques
Universitat Rovira i Virgili
Avinguda Països Catalans, 26
43007 Tarragona, Catalonia, Spain

Michael E. O'Sullivan

Department of Mathematics and Statistics
San Diego State University
5500 Campanile Drive
San Diego, CA 92182-7720, USA

(Communicated by Joachim Rosenthal)

Abstract. Improvements to code dimension of evaluation codes, while maintaining a fixed decoding radius, were discovered by Feng and Rao, 1995, and nicely described in terms of an order function by Høholdt, van Lint, Pellikaan, 1998. In an earlier work, 2006, we considered a different improvement, based on the observation that the decoding algorithm corrects an error vector based not so much on the weight of the vector but rather the "footprint" of the error locations. In both cases one can find minimal sets of parity checks defining the codes by means of the order function. In this paper we show that these minimal sets have a very useful closure property. For several important families of codes that we consider, this property allows us to construct a generating matrix for the code that has properties amenable to encoding. The generating matrix can be constructed by evaluating monomials in a set which also has the closure property.

1. Introduction

Goppa's introduction of algebraic geometry into coding theory led to several methods for constructing codes. One prominent and very general family is codes from order domains, whose theory is developed in [7, 11, 14, 17, 19]. Order domains yield Reed-Solomon codes, Reed-Muller codes, the one-point codes from algebraic curves, and codes from higher dimensional algebraic varieties. For these codes there is a lower bound on the minimum distance and an efficient generalization of the Berlekamp-Massey algorithm based on Sakata's algorithm for finding linear recurrence relations in multidimensional arrays [23]. Using the majority voting method of Feng, Rao, and Duursma, [5, 6] the algorithm corrects up to half the above mentioned bound on the minimum distance.

Improvements to code dimension, while maintaining a fixed decoding radius were discovered by Feng and Rao [6] and described by means of an order function by

2000 *Mathematics Subject Classification:* 94B27.

Key words and phrases: Algebraic-geometry code, Reed-Muller code, Hermitian code, toric code, dual code.

©2008 AIMS-SDU