A GO-UP CONSTRUCTION AND APPLICATIONS

Eddie Arrieta Arrieta,
eddie.arrieta@upr.edu
Department of Mathematics, UPR-RP.

DISSERTATION
DEPARTMENT OF MATHEMATICS

July 16, 2021

Abstract

Given a code C over the finite field $\mathbb{F}_q$, where q is a power of a prime number, some constructions exist that permit us to obtain a new code from C over $\mathbb{F}_q$ or over a subfield of $\mathbb{F}_q$, for example as subfield subcodes. However, in some important applications, one needs codes over an extension field, such as quantum error-correcting codes (QECC). In these applications, the codes in the extension fields need only be additive. In this dissertation, we propose a novel technique that we call **Go-Up** (**GU**) construction that allows us to obtain an additive or a linear code over $\mathbb{F}_{q^m}$ from a collection of codes over $\mathbb{F}_q$. We show under what condition is this code a self-orthogonal or self-dual code, under various forms (Euclidean, or Hermitian, or Trace Hermitian, or alternating). We use these additive self-orthogonal codes to construct quantum-stabilizer codes. As a result, we give explicit classes of codes where we obtain new quantum error-correcting codes.

Under certain conditions, we show that the **GU** of two classical Goppa codes is a Goppa code. As a consequence, we obtain quantum error-correcting codes from classical Goppa codes. So far, research on QECC from Goppa codes has been limited. Also, the decoding of QECC is limited. Our result might allow fast decoding of QECC from **GU** of Goppa codes via Patterson's $O(n, log\, n)$ decoding algorithm.

Independent of the **GU** construction, we show under what conditions are classical Goppa code self-orthogonal. Using this fact, we obtain binary and quaternary QECC directly from Goppa codes. We compare our results on QECC to those obtained for QECC from BCH codes by Beth and Grassl, and by Sarvepalli et al.

The third theme of our thesis is to construct few weights codes. Such codes have applications in cryptography, association schemes, Steiner systems, t-designs, strongly regular graphs, finite group theory, finite geometries, among other disciplines. The theory and construction of two-weight linear codes have been carried out by Calderbank and Kantor, among others. Tonchev and Jungnickel, and Ding et al. have done pioneering work on three-weight codes. We use our **GU** code construction to obtain two-weight, three-weight and few-weights linear codes. Consequently, we give elementary construction of class RT1 of two-weight codes by Calderbank and Kantor. We also obtain new classes of three-weight codes.