# Chapter 8 A New Approach to Construction and Decoding of Linear Block Codes Based on Polar Codes

#### **Driss Khebbou**

Polydisciplinary Faculty of Safi, Cadi Ayyad University of Marrakech, Morocco

Idriss Chana ESTM, Moulay Ismail University of Meknes, Morocco

Hussain Ben-Azza ENSAM, Moulay Ismail University of Meknes, Morocco

#### ABSTRACT

In the field of channel coding theory, there are two main branches. The first is related to the design and construction of codes capable of facilitating identification of errors at the receiver despite potential alterations during transmission; this is known as the encoding operation. The second branch focuses on developing mechanisms for correcting errors caused by the transmission channel, by devising valid and suitable algorithms; this is known as the decoding operation. The authors have delved into both aspects. In the first part, a novel method for constructing good linear codes is studied. It is based on the Hadamard matrix, which shares the same structure as the kernel of polar codes, and on the generator matrix of several existing linear codes. In the second part, a new decoding algorithm is proposed. This involves adapting the SSCL polar code decoder to decode the codes designed in the first part, as well as some of the most well-known block codes.

DOI: 10.4018/979-8-3693-0497-6.ch008

# 1. INTRODUCTION

In the field of channel coding theory, two main branches can be identified. The first is related to the design and construction of codes that represent the information to be transmitted, and are capable of facilitating its identification at the receiver despite the alterations it may undergo during transmission; this is known as the coding operation. The second branch focuses on conceiving mechanisms for error correction caused by the transmission channel, by developing valid and appropriate algorithms; this is referred to as the decoding operation. Both operations are grouped under an aspect known as error-correcting codes.

In general, error-correcting codes can be divided into two categories: convolutional codes and block codes. In this paper, we limit our discussion to block codes, which involve breaking down the message to be transmitted into blocks, to which redundancy bits are added and utilized by the decoder to correct transmission errors. A highly significant class of block codes is linear block codes, which leverage algebraic principles to provide a structure that is both algebraically straightforward and less complex. However, the design of linear codes, known for their appealing algebraic structure and substantial error-correction capabilities, remains an open challenge in coding theory. Consequently, working with existing codes may be an intriguing street for constructing linear codes with excellent performance (*Error-Correction Coding and Decoding*, n.d.). In the literature, several works have relied on this principle to construct error-correcting codes with attractive properties, such as the construction X presented by N. Sloane in (Grassl, 2006; Sloane et al., 1972), which essentially involves adding a codeword from an auxiliary code to the existing code.

On the other hand, despite their many appealing properties, most algebraic codes, particularly linear block codes, suffer from a major drawback: the lack of low-complexity, soft decoding algorithms. A well-known soft decoding algorithm for binary linear block codes is the "Ordered Statistics Decoder (OSD)," presented in (Fossorier & Lin, 1995), inspired by the Dorsh algorithm (Dorsch, 1974), which has claimed performances close to those of Maximum Likelihood Decoding (MLD) for many linear block codes. However, these exceptional performances can only be achieved by using Ordered Statistics Decoder with high orders, which implies relatively significant complexity and a substantial memory.

In this work, we aim to summarize our research efforts, which revolve around two main aspects. The first involves proposing a approach for constructing good binary linear codes based on existing codes (Khebbou, Benkhouya, et al., 2021, 2022). The term "good" refers to the optimality of the rate between the bloc message and the redundant part on one hand, and error-correction capability on the other. This method is based on a well-known matrix, the Hadamard matrix (Hadamard, 1893).

The second aspect, introduces a new decoding method by adapting the Simplified Successive Cancellation List (SSCL) of Polar codes (Arikan, 2009), used in the 5G standard, to decode the linear bloc codes designed in the first part and some well-known block codes (Khebbou, Chana, et al., 2021; Khebbou et al., n.d.-b, n.d.-a, 2023; Khebbou, Idriss, et al., 2022). In addition to simplifying and reducing the complexity of the decoding process, the performance evaluation of the proposed decoders demonstrates their advantages over other decoders in the literature, notably OSD, which is considered most suitable for all linear block codes, despite its limitations in terms of complexity and order saturation.

The rest of this paper is organized as follows. In the next section, we will introduce important aspects for describing the proposed construction and decoding methods, such as linear block codes, Polar codes, and their decoding techniques. In the third section, we will describe the method for constructing good binary linear block codes, along with some obtained results and interpretations. In the fourth section, we

17 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/a-new-approach-to-construction-and-decodingof-linear-block-codes-based-on-polar-codes/337456

# **Related Content**

#### Adaptation of Blockchain Architecture to the Internet of Things and Performance Analysis

Mevlut Ersoy, Asm Sinan Yükseland Cihan Yalcin (2023). Research Anthology on Convergence of Blockchain, Internet of Things, and Security (pp. 210-227).

www.irma-international.org/chapter/adaptation-of-blockchain-architecture-to-the-internet-of-things-and-performanceanalysis/310449

#### A New Block Cipher System Using Cellular Automata and Ant Colony Optimization (BC-CaACO)

Charifa Hanin, Fouzia Omary, Souad Elbernoussi, Khadija Achkounand Bouchra Echandouri (2018). International Journal of Information Security and Privacy (pp. 54-67). www.irma-international.org/article/a-new-block-cipher-system-using-cellular-automata-and-ant-colony-optimization-bccaaco/216849

#### User Perceptions of Security Technologies

Douglas M. Kline, Ling Heand Ulku Yaylacicegi (2011). International Journal of Information Security and Privacy (pp. 1-12).

www.irma-international.org/article/user-perceptions-security-technologies/55376

## Ethical Dilemmas in Data Mining and Warehousing

Joseph A. Cazierand Ryan C. LaBrie (2007). *Encyclopedia of Information Ethics and Security (pp. 221-228).* 

www.irma-international.org/chapter/ethical-dilemmas-data-mining-warehousing/13476

## On the Security of Self-Certified Public Keys

Cheng-Chi Lee, Min-Shiang Hwangand I-En Liao (2011). *International Journal of Information Security and Privacy (pp. 54-60).* 

www.irma-international.org/article/security-self-certified-public-keys/55379