Fast Decoding Algorithms for First Order Reed-Muller and Related Codes

ALEXEY E. ASHIKHMIN
Institute for Problems of Information Transmission, Ermolovoy 19, Moscow, Russia

SIMON N. LITSYN*
Department of Electrical Engineering Systems, Tel Aviv University, Ramat Aviv 69978 Israel

Communicated by: D. Jungnickel

Received April 28, 1993; Revised February 2, 1995

Abstract. Fast decoding algorithms for short codes based on modifications of maximum likelihood decoding algorithms of first order Reed-Muller codes are described. Only additions-subtractions, comparisons and absolute value calculations are used in the algorithms. Soft and hard decisions maximum likelihood decoding algorithms for first order Reed-Muller and the Nordstrom-Robinson codes with low complexity are proposed.

Keywords: First order Reed-Muller codes, the Nordstrom-Robinson code, decoding algorithms.

1. Introduction

Maximum likelihood (ML) decoding algorithms for short codes are of great practical significance. The cases of hard and soft decisions at the output of RSC (for hard decoding) and AWGN (for soft decoding) channels are both relevant for communication systems and were extensively studied (see [1, 6, 7, 9, 10, 11, 12, 15, 21, 23, 24]). In the forementioned channels the ML decoding coincides with determining the code word having minimum distance (the Hamming distance for hard and the Euclidean distance for soft decoding) from the received vector. Hence, in what follows we will not distinguish between ML and minimum distance decoding.

The aim of the paper is to design new simple decoding algorithms for first order Reed-Muller codes and other short codes.

One of the essential questions about analysis of decoding algorithms is introducing an adequate definition of the algorithm's complexity. In recent papers [6, 10, 12, 23] the most popular one defines the complexity of soft decoding as the amount of operations with real numbers, while the operations in finite fields are treated as having zero complexity. This approach is motivated by a possibility of organizing such procedures as memory operations. In some cases this approach seems to be non-adequate, since some algorithms, possessing low complexity according to the above mentioned definition, may require extremely large additional memory.

* Supported by the Gustafsson Foundation and a grant from the Ministry of Science and Technology, Israel
In this paper we restrict ourselves to decoding algorithms using only real numbers operations and count their complexity in number of additions-subtractions, comparisons and absolute value calculations. A property of the described algorithms is that for both cases—hard and soft decoding—only real number (for hard decoding-integer number) operations are needed. We do not count the assignment operations, the increment-decrement operations for index variables, etc. In fact, this definition reflects the situation of decoder's implementing as a combinational circuit or software implementation of the decoder with restrictions on operations with memory (we count the amount of computations in all branches of the algorithm). We also forbid using indirect addressing. More precisely, we estimate the complexity of the indirect addressing in an array of dimension \( M \) as requiring \( M - 1 \) comparisons, in contrast to zero complexity in the above mentioned approach.

For decoding low rate codes, use of the fact Hadamard (Walsh-Hadamard, Walsh) transform (FHT) leads to significant gain in decoding complexity (see [6, 13, 19]). In the paper we consider ML decoding algorithms of first order Reed-Muller (RM) codes and the Nordstrom-Robinson (NR) code. The proposed algorithms may be applied to decoding such codes as the Golay code, RM codes of arbitrary order, and other codes which may be represented as a union of cosets of first order RM codes. We also consider some sub-optimal decoding algorithms of listed codes whose complexity grows linearly with code length. Analysis of these algorithms demonstrates that their performance is close to one of ML decoding, while their complexity is essentially smaller. The key idea of this simple decoding is truncating intermediate results of the FHT according to the value of a function calculated at each step.

The paper is organized as follows. In Section 2 we consider ML soft decoding algorithms of first order RM codes. In Section 3 we analyze decoding algorithms for first order RM codes, whose complexity grows linearly with code length, that provide error correction up to the limits guaranteed by the minimum distance of the code. In Section 4 we develop the ideas of Section 2 for soft and hard ML decoding of the NR code. We summarize our results on the complexities of proposed algorithms in the following table: Note that Algorithms A, B, C, A1, C1, F1, G1 and B2 presented in the table are ML algorithms.

In the paper we survey, along with new results, several of our papers [2, 3, 5] published earlier in Russian.

In what follows, we will use the following notation:

- \( \text{RM}_n \) = the first order RM code of length \( n \);
- \( \text{NR} \) = the Nordstrom-Robinson code;
- \( H_n \) = the Hadamard matrix of dimension \( n \);
- \( \mathbf{x}^T \) = the transpose of vector \( \mathbf{x} \);
- \( \text{bsign}(y) = \begin{cases} 0 & \text{if } y \geq 0 \\ 1 & \text{if } y < 0 \end{cases} \);
- \( \ast \) = componentwise multiplication of vectors;
- \( \times \) = multiplication of a vector by a scalar;