Chapter 8

Turbo product codes

8.1 History

Because of the Gilbert-Varshamov bound, it is necessary to have long codes in order to obtain block codes with a large minimum Hamming distance (MHD) and therefore high error correction capability. But, without a particular structure, it is almost impossible to decode these codes.

The invention of product codes, due to Elias [8.4], can be seen in this context: it means finding a simple way to obtain codes with high error correction capability that are easily decodable from simple elementary codes. These product codes can be seen as a particular realization of the concatenation principle (Chapter 6).

The first decoding algorithm results directly from the construction of these codes. This algorithm alternates the hard decision decoding of elementary codes on the rows and columns. Unfortunately, this algorithm does not allow us to reach the maximum error correction capability of these codes. The Reddy-Robinson algorithm [8.15] does allow us to reach it. But no doubt due to its complexity, it has never been implemented in practical applications.

The aim of this chapter is to give a fairly complete presentation of algorithms for decoding product codes, whether they be algorithms for hard data or soft data.

8.2 Product codes

With conventional constructions, it is theoretically possible to build codes having a high MHD. However, the decoding complexity becomes prohibitive, even for codes having an algebraic structure, like Reed-Solomon codes or BCH (see Chapter 4) codes. For example, for Reed-Solomon codes on $\mathbb{F}_{256}$, the most complex decoder to have been implemented on a circuit has an error
correction capability limited to 11 error symbols, which is insufficient for most applications today. The construction of product codes allows this problem to be circumvented: by using simple codes with low correction capability, but whose decoding is not too costly, it is possible to assemble them to obtain a longer code with higher correction capability.

**Definition**

Let $C_1$ (resp. $C_2$) be a linear code of length $n_1$ (resp. $n_2$) and with dimension $k_1$ (resp. $k_2$). The product code $C = C_1 \otimes C_2$ is the set of matrices $M$ of size $n_1 \times n_2$ such that:

- Each row is a codeword of $C_1$,
- Each column is a codeword of $C_2$.

This code is a linear code of length $n_1 \times n_2$ and with dimension $k_1 \times k_2$.

**Example 8.1**

Let $H$ be the Hamming code of length 7 and $P$ be the parity code of length 3. The dimension of $H$ is 4 and the dimension of $P$ is 2. The code $C = H \otimes P$ is therefore of length $21 = 7 \times 3$ and dimension $8 = 4 \times 2$. Let the following information word be coded:

$$I = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$ 

Each row of a codeword of $C$ must be a codeword of $H$. Therefore to code $I$, we begin by multiplying each row of $I$ by the generating matrix of code $H$:

$$\begin{bmatrix} 0 & 1 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

\[^1\text{or length of message}\]