Product codes and the Singleton bound

Nicolas Sendrier
INRIA, Domaine de Voluceau, Rocquencourt,
BP 105, 78153 Le Chesnay CEDEX, FRANCE

Abstract

Minimum distance is not always the most determinant factor to acheive high performance for error correction. Of course the knowledge of the whole weight distribution of the code is more accurate than the knowledge of the mere minimum distance, and the phenomenon amplifies for a high noise level. Besides this fact, the use of error-correcting codes in practical situations requires a trade-off between the algorithmic complexity and the performance of the decoding procedure. We show here that for low rates a very good trade-off is possible using product codes, although they are known for their poor minimum distance.

1 Introduction

We consider transmission of information through a memoryless q-ary symmetric channel which can model an additive channel for instance. In such a model, the probability of transition from a word to another is a decreasing function of their Hamming distance. This means that finding codes with a large minimum distance is desirable, though not necessary, to acheive good performance. The "best" decoding algorithm for any given code is the maximum likelihood decoder. Unfortunately, this algorithm usually has a prohibitive algorithmic cost. It is thus necessary to find a trade-off between algorithmic complexity and performance.

One of the most efficient pair code/decoder is the Berlekamp-Massey decoding algorithm for alternant codes. This algorithm is bounded by the designed distance and has a relatively low algorithmic complexity. But it cannot correct error patterns of weight larger than half the designed distance.

Some other classes of codes, like product codes, have a relatively bad minimum distance but possess a natural decoding algorithm that can correct many error patterns of weight larger than half the minimum distance. We have obtained very good decoding performance for such codes. Furthermore we will prove that the algorithmic complexity of the product code decoder is less than the complexity of the Berlekamp-Massey algorithm for a code of same length and dimension, that acheives similar performance.

We will give in sections 2 and 3 the definitions and tools that help to highlight the main result, and in section 4 we will give an example of a good product code; the product code $RS(256;15,7,9) \otimes RS(256;15,7,9)$, where $RS(256;15,7,9)$ is the shortened Reed-Solomom code over $GF(256)$, has parameters $(225,49,81)$ and acheives a residual error rate of 10^{-6} for a channel error probability of 0.254. For the same channel error probability, the shortened Reed-Solomom code $RS(256;225,49,177)$ over $GF(256)$ using Berlekamp-Massey decoding algorithm has a residual error rate of $2.2\,10^{-6}$ and a higher algorithmic complexity.

2 Error correcting algorithm

Let $C(n,k,d)$ denote a linear code over $GF(q)$, of length n dimension k and minimum distance d.

Definition 1 *An* error-correcting algorithm *for C is a mapping γ from $GF(q)^n$ into $C \cup \{\infty\}$ such that for all x in C, $\gamma(x) = x$. (The symbol ∞ denotes a decoding failure)*

The error-correcting algorithm γ is said to be C-additive *if for all y in $GF(q)^n$ and all x in C, $\gamma(y+x) = \gamma(y) + x$ (with the convention $\infty + x = \infty$).*

Definition 2 *An error pattern y in $GF(q)^n$ is said to be* correctable *if for all x in C, $\gamma(x+y) = x$.*

When an error-correcting algorithm γ is C-additive, an error pattern y in $GF(q)^n$ is correctable if and only if $\gamma(y) = 0$. From now on, we will only consider C-additive algorithms. This is the case for all syndrome based decoders.

Let γ be a C-additive decoding algorithm. We will denote by $\mathcal{P}_\gamma(p)$ the probability of correct transmission of a codeword transmitted through a q-ary symmetric channel of error probability p; its complement to one $1 - \mathcal{P}_\gamma(p)$ is called the residual error rate. These probabilities can be computed if we are able to describe the set $\{y \in GF(q)^n, \gamma(y) = 0\}$ of correctable error patterns.

Proposition 1 *Let γ be a C-additive error-correcting algorithm, we call* decoding region *of γ the set*

$$E_\gamma = \{y \in GF(q)^n, \gamma(y) = 0\}$$

of correctable error patterns. The probability of correct transmission of a codeword from C transmitted through a memoryless q-ary symmetric channel of error probability p and decoded by γ is equal to

$$\mathcal{P}_\gamma(p) = \sum_{y \in E_\gamma} \left(\frac{p}{q-1}\right)^{w_H(y)} (1-p)^{n-w_H(y)} = \sum_{i=0}^{n} a_i \left(\frac{p}{q-1}\right)^i p^{n-i},$$

where w_H denotes the Hamming weight over $GF(q)$, and a_i is the number of correctable error patterns of weight i.