Decoding Xing-Ling codes

Nielsen, Rasmus Refslund

Published in:

Link to article, DOI:
10.1109/ISIT.2002.1023360

Publication date:
2002

Document Version
Publisher's PDF, also known as Version of record

Link back to DTU Orbit

Citation (APA):
Decoding Xing-Ling codes

R. Refslund Nielsen
Research Center COM, building 371
Technical University of Denmark (DTU)
DK-2800 Lyngby, Denmark.
E-mail: rrm@com.dtu.dk.

Abstract — This paper describes an efficient decoding method for a recent construction of good linear codes as well as an extension to the construction. Furthermore, asymptotic properties and list decoding of the codes are discussed.

I. XING-LING CODES

In [1] Xing and Ling describe a new construction of a class of linear codes (here referred to as Xing-Ling codes) which resulted in several improvements to Brouwer’s table [2] of good linear codes.

A Xing-Ling code is a subfield subcode of a Reed-Solomon code over \(F_{qz}\). While a Reed-Solomon code of dimension \(K\) is obtained by evaluating elements of \(F_{qz}\) in all polynomials of degree at most \(K - 1\), a Xing-Ling code is obtained by evaluating certain elements of \(F_{qz}\) in certain polynomials of degree at most \(K - 1\). The elements and polynomials are chosen in such a way that the result is a code over \(F_q\).

For any integer, \(K\), let \(V_K\) denote the \(F_q\)-vector space spanned by all monomials and monic binomials of degree less than \(K\) which only give values in \(F_q\) when evaluated in elements from \(F_{qz}\).

We then have the following definition of Xing-Ling codes:

**Definition 1** Let \(A \subseteq \mathbb{F}_q\) and \(B \subseteq \mathbb{F}_q^2 \backslash \mathbb{F}_q\) be given such that \(\beta^q \notin B\) for all \(\beta \in B\) and let \(K\) be given such that \(V_K \neq V_{K-1}\). Then the following set is a Xing-Ling code:

\[
XL(A, B, K) = \{f(A, B) \mid f \in V_K\}
\]

The main parameters of Xing-Ling codes are summarized in the following theorem:

**Theorem 2** ([1], Theorem 2.5, 2.6, 2.9, and 2.10) The code \(XL(A, B, K)\) satisfies the following:

1. The code is a linear code over \(F_q\).
2. Let the number of elements of \(A\) and \(B\) be denoted by \(n_A := |A|\) and \(n_B := |B|\).
3. The length of the code is then \(n = n_A + n_B\) and if \(K - 1 = qr + s\) where \(0 \leq s \leq q\) then the dimension is \(k = \frac{(r(r+1))}{2} + s + 1\).
4. Let \(z := \left\{ \begin{array}{ll} \max\{2(r-1), r + s\} & \text{if } q \text{ is odd} \\ \max\{r-1, s\} & \text{if } q \text{ is even} \end{array} \right. \) (1)

Then the minimum distance, \(d\), satisfies \(d \geq d^*\) where

\[
d^* := n - \left\lfloor \frac{K - 1 + \max\{z, n_A\} - 2n_A - \delta q\}}{2} \right\rfloor
\]

with \(\delta = 2\) for \(q\) odd and \(\delta = 1\) for \(q\) even. Notice that for \(q\) odd the first term of the max-expression is always largest since \(n_A \leq q\).

In the definition of Xing-Ling codes we have the constraints \(n_A \leq q\) and \(n_B \leq (q^2 - q)/2\) so the length of a Xing-Ling code is at most \(q(q + 1)/2\). However, the paper [3] describes how to extend the code with one position by evaluating in the point at infinity on the projective line. This gives a few improvements to Brouwer’s table.

II. DECODING

Suppose that a word \(r \in \mathbb{F}_q^2\) is received. The goal is to find the polynomial \(f \in V_K\) such that \(f\) corresponds to the Xing-Ling codeword closest to \(r\). The paper describes an efficient method that calculates \(f\) if the corresponding codeword has distance less than half the designed minimum distance from the received word. The method is sketched below.

The word \(r\) is decomposed into two blocks, \(r = (r_A, r_B)\) where \(r_A\) are the received values on the \(A\)-positions and \(r_B\) are the received values on the \(B\)-positions.

If \(n_A \leq z\) (with \(z\) defined in Eqn. (1)) then it turns out that it suffices to decode the word \((r_A, r_B)\) with a suitable Reed-Solomon code over \(F_q\).

If \(n_A > z\) then this approach fails if too many errors occurred on the \(B\)-positions. In that case the word \(r_A\) is decoded with a Reed-Solomon code over \(F_q\). This results in an estimate, \(u\), of \(f(\mathbb{F}_q)\). If \(q\) is even then decoding \((u, r_B, r_B)\) with a Reed-Solomon code gives the result. If \(q\) is odd then the decoding is done with a so-called generalized Reed-Solomon \(m\)-code which is defined in the paper.

III. ASYMPTOTIC RESULTS

Let an infinite sequence of Xing-Ling codes be constructed for alphabet sizes tending to infinity such that for each alphabet size, \(q\), we have \(n_A = 0\) and \(n_B = n = (q^2 - q)/2\) and such that the information rate \((k/n)\) tends to a constant, \(\kappa\).

For \(q \to \infty\) it is then shown that the designed minimum distance, \(d^*\), satisfies

\[
d^*/n \to 1 - \sqrt{\kappa}
\]

and that a fraction of errors, \(t/n \to \tau\), can be efficiently list decoded whenever

\[
\tau < 1 - \sqrt{\kappa}.
\]

REFERENCES

