Performance Analysis of a Decoding Algorithm for Algebraic Geometry Codes

II. Elbrønd Jensen
Dept. of Mathematics
Technical University of Denmark
Bldg. 303
DK-2800 Lyngby Denmark
Email h.elbrond.jensen@mat.dtu.dk

R. Reffstrup Nielsen
Dept. of Mathematics
Technical University of Denmark
Bldg. 303
DK-2800 Lyngby Denmark
Email stud-re@mat.dtu.dk

T. Hoeholdt
Dept. of Mathematics
Technical University of Denmark
Bldg. 303
DK-2800 Lyngby Denmark
Email tom@mat.dtu.dk

Abstract — We analyse the known decoding algorithms for algebraic geometry codes in the case where the number of errors is greater than or equal to \((d_{FR} - 1)/2 + 1\), where \(d_{FR}\) is the Feng-Rao distance.

I. INTRODUCTION

The fast decoding algorithm for one-point algebraic geometry codes of Sakata, Elbrønd Jensen, and Hoeholdt [1] decodes any syndromes \(S_2(f)\) (with \(2g + 1 \leq 1\)) where \(g\) is the genus of the curve and \(2g + 1 \leq m\). The objective of the decoder is therefore to determine the number of errors is greater than or equal to \((d_{FR} - 1)/2 + 1\).

II. THE CODES AND THE DECODING ALGORITHM

Let \(P_1, P_2, \ldots, P_r\) be \(F_q\)-rational points on a nonsingular absolutely irreducible curve \(C\) of genus \(g\) defined over \(F_q\). We consider an algebraic geometry code \(C_m\) of type \(C_m(D,G) = \mathbb{C}_2(D,G)\), where \(D = P_1 + P_2 + \cdots + P_r\) and \(G = mQ\).

If \(f \in R\) and \(y \in F_q^m\) we define the syndrome \(S_2(f)\) to be

\[
S_2(f) = \sum_{i=1}^{n} y_i f(P_i)
\]

so we have \(y \in C \iff S_2(f) = 0\) for all \(f\) such that \(p(f) \leq m\).

In the decoding situation we receive a vector \(y\) which is the sum of a codeword \(g\) and an error vector \(e\). We have \(S_2(f) = S_2(g) + S_2(e)\) if \(p(f) \leq m\), so the syndromes \(S_2(f)\) can be calculated directly from the received word if \(p(f) \leq m\).

If \(r = \text{the Hamming weight of } g\) then it is well known e.g. [1] or [2] that if one knows the syndromes \(S_2(f)\) where \(p(f) \leq 2(r + 2g) - 1\) then the error vector can be easily found.

The objective of the decoder is therefore to determine the syndromes \(S_2(f)\) where \(m < p(f) \leq 2(r + 2g) - 1\). The decoding algorithm is a version of Sakata’s generalization of the Berlekamp-Massey algorithm.

This algorithm indeed solves the decoding problem when \(\tau \leq (d_{FR} - 1)/2\) (with \(\tau\) being the number of errors). See [2] or [1].

III. THE RESULTS

Let \(P_1, \ldots, P_r\) be the error points. We call these independent, if they give independent conditions on a function passing through these points, or equivalently that

\[
L(pQ - (P_1 + \cdots + P_r)) = 0
\]

Theorem 1: If \(m \geq 4g - 2\), \(\tau \geq (d_{FR} - 1)/2\), and the error points are independent then the algorithm fails.

The algorithm can fail by either giving no answer or a wrong answer, and indeed both cases can occur.

When \(m < 4g - 2\) the situation is different. We have developed a fairly simple procedure to determine the performance of the decoding algorithm in this case also. We mention that for the Hermitian curve over \(F_q\), given by the equation

\[
z^n + y^n + y = 0
\]

which has genus \(g = \frac{(q-1)}{2}\) and \(q\) \(F_q\)-rational points we can often do much better than predicted by the Feng-Rao bound.

If \(r = 4\) we can get a \((64,57,4)\)-code over \(F_{16}\), but two independent errors are always decoded correctly.

If \(r = 8\) we get a \((512,476,9)\)-code over \(F_{64}\), but here one can always decode 10 independent errors correctly. By similar considerations we can explain the results presented by O’Sullivan in [3].

The error points can fail to be independent in different ways. If we look at the case where \(r = (d_{FR} - 1)/2 + 1\) and

\[
L(pQ - (P_1 + \cdots + P_r)) = 0
\]

but \(L(pQ - (P_1 + \cdots + P_r)) \neq 0\), we have the following two theorems:

Theorem 2. The function in \(F_q\) with lowest order \(p\) at \(Q\) is an element of \(L(pQ - (P_1 + \cdots + P_r))\) for at least \((q-1)^{-1}\) of the \((q-1)^{r}\) possible choices of the error values.

Theorem 3. The algorithm corrects \(\tau \geq (d_{FR} - 1)/2\) dependent errors correctly in almost all cases.

The question whether a random selected set of points on a curve are independent or not seems difficult. We have some numerical evidence for conjecturing that (at least on a Hermitian curve) that the probability of getting independent points is \(1 - \frac{1}{q}\).

REFERENCES

