Performance Analysis of a Decoding Algorithm for Algebraic Geometry Codes

Jensen, Helge Elbrønd; Nielsen, Rasmus Refslund; Høholdt, Tom

Published in:
Information Theory, 1998. Proceedings. 1998 IEEE International Symposium on

Link to article, DOI:
10.1109/ISIT.1998.708983

Publication date:
1998

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

Performance Analysis of a Decoding Algorithm for Algebraic Geometry Codes

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

R.Refslund Nielsen
Dept. of Mathematics
Technical University of Denmark
Bldg.303
DK-2800 Lyngby Denmark
Email stud-rrn@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 $\lfloor (d_{FR}-1)/2 \rfloor + 1$, 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 Høholdt [1] decodes any error pattern of weight up to $\lfloor (d_{FR}-1)/2 \rfloor$ where d_{FR} is the so-called Feng-Rao distance of the code. In this paper we analyse the performance of the decoding algorithm, when the number of errors is greater than or equal to $\lfloor (d_{FR}-1)/2 \rfloor + 1$.

II. The codes and the decoding algorithm

Let $P_1, P_2, \ldots, P_n, Q$ be F_q-rational points on a nonsingular absolutely irreducible curve χ of genus g defined over F_q. We consider an algebraic geometry code C_m of type $C_L(D,G)^\perp = C_\Omega(D,G)$, where $D = P_1 + P_2 + \ldots + P_n$ and $G = mQ$.

If $f \in R$ and $\underline{y} \in F_q^n$ we define the *syndrome* $S_{\underline{y}}(f)$ to be

$$S_{\underline{y}}(f) = \sum_{i=1}^{n} y_i f(P_i)$$

so we have $\underline{y} \in C \iff S_{\underline{y}}(f) = 0$ for all f such that $\rho(f) \leq m$.

In the decoding situation we receive a vector $\underline{y}$ which is the sum of a codeword $\underline{c}$ and an error vector $\underline{e}$.We have $S_{\underline{e}}(f) = S_{\underline{y}}(f)$ if $\rho(f) \leq m$, so the syndromes $S_{\underline{e}}(f)$ can be calculated directly from the received word if $\rho(f) \leq m$.

If τ is the Hamming weight of $\underline{e}$ then it is well known e.g. [1] or [2] that if one knows the syndromes $S_{\underline{e}}(f)$ where $\rho(f) \leq 2(\tau + 2g) - 1$ then the error vector can be easily found. The objective of the decoder is therefore to determine the syndromes $S_{\underline{e}}(f)$ where $m < \rho(f) \leq 2(\tau+2g) - 1$.

The decoding algorithm is a version of Sakata's generalization of the Berlekamp-Massey algorithm.

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

III. The results

Let $P_1, \ldots, P_\tau$ be the error points. We call these *independent*, if they give independent conditions on a function passing through these points, or equivalently that

$$\mathrm{L}(\rho Q - (P_1 + \cdots + P_\tau)) = 0 \text{ for } \rho \leq \rho_\tau$$

Theorem 1 *If $m \geq 4g-2$, $\tau > \lfloor (d_{FR}-1)/2 \rfloor$, 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_{r^2} given by the equation

$$x^{r+1} + y^r + y = 0$$

which has genus $g = \frac{r(r-1)}{2}$ and r^3 F_{r^2}-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 $\tau = \lfloor (d_{FR}-1)/2 \rfloor + 1$ and

$$\mathrm{L}(\rho Q - (P_1 + \cdots + P_\tau)) = 0 \text{ for } \rho < \rho_\tau$$

but $\mathrm{L}(\rho_\tau Q - (P_1 + \cdots + P_\tau)) \neq 0$, we have the following two theorems:

Theorem 2 *The function in F_M with lowest poleorder ρ at Q is an element of $L(\rho Q - (P_1 + \cdots + P_\tau))$ for at least $(q-1)^{\tau-1}$ of the $(q-1)^\tau$ possible choices of the error values.*

Theorem 3 *The algorithm corrects $\tau = \lfloor (d_{FR}-1)/2 \rfloor + 1$ 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

[1] S. Sakata, H. Elbrønd Jensen and T. Høholdt: "Generalized Berlekamp-Massey Decoding of Algebraic-Geometric Codes up to half the Feng-Rao Bound" *IEEE Trans. Inform. Theory*, vol 41, no. 6, pp. 1762-1768, nov. 1995.

[2] M.E. O'Sullivan: "Decoding of Codes Defined by a single Point on a Curve" *IEEE Trans. Inform. Theory*, vol. 41, no. 6, pp. 1709-1719, nov. 1995.

[3] M.E. O'Sullivan: "Decoding Hermitian Codes beyond $(d_{\min} - 1)/2$" *Proceedings of the 1997 IEEE International Symposium on Information Theory*, June 20-July 4, 1997, Ulm, Germany.