Performance Analysis of a Decoding Algorithm for Algebraic Geometry Codes

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

Published in:

Link to article, DOI:
10.1109/ISIT.1998.708983

Publication date:
1998

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

Citation (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.
Performance Analysis of a Decoding Algorithm for Algebraic Geometry Codes

II. 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 \((d_{FR}-1)/2\) + 1, where \(d_{FR}\) is the Feng-Rao distance.

I. INTRODUCTION

The fast decoding algorithm for one-point algebraic geometry codes of Sakata, Elbrond Jensen, and Høholdt [1] decodes any code of genus \(g\) defined over \(F_q\). We consider an algebraic geometry code \(C_m\) of type \(G(D, G)\), where \(D = P_1 + P_2 + \ldots + P_r\) and \(G = mQ\).

Let \(P_1, P_2, \ldots, P_r, Q\) be \(F_q\)-rational points on a nonsingular absolutely irreducible curve \(X\) of genus \(g\) defined over \(F_q\). We have \(S_1(f) = S_2(f)\) for all \(f \in F_q\) such that \(p(f) \leq m\).

In the decoding situation we receive a vector \(y\) which is the sum of a codeword \(c\) and an error vector \(e\). We have \(S_1(f) = S_2(f)\) if \(p(f) \leq m\), so the syndromes \(S_1(f)\) can be calculated directly from the received word if \(p(f) \leq m\).

II. THE CODES AND THE DECODING ALGORITHM

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

If \(f \in R\) and \(y \in F_q^r\) 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 \(c\) and an error vector \(e\). We have \(S_1(f) = S_2(f)\) if \(p(f) \leq m\), so the syndromes \(S_1(f)\) can be calculated directly from the received word if \(p(f) \leq m\).

If \(r\) is the Hamming weight of \(y\) then it is well known that \(S_1(f) = S_2(f)\) if \(p(f) \leq m\), so the syndromes \(S_1(f)\) can be calculated directly from the received word if \(p(f) \leq m\).

The objective of the decoder is therefore to determine the syndromes \(S_1(f)\) where \(m < p(f) \leq 2(r + 2g) - 1\) then the error vector can be easily found.

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 \(\tau\) 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

\[ L(\rho Q - (P_1 + \ldots + P_r)) = 0 \]

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

Theorem 2. The function in \(F_q\) with lowest poleorder \(\rho\) at \(Q\) is an element of \(L(\rho Q - (P_1 + \ldots + P_r))\) for at least \((q-1)^{-1}\) 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 \(1 - \frac{1}{q^r}\).

REFERENCES