Recent results in the decoding of Algebraic geometry codes

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

Published in:
Information Theory Workshop, 1998

Link to article, DOI:
10.1109/ITW.1998.706397

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.
Recent results in the Decoding of Algebraic Geometry Codes

H. Elbrønd Jensen, R. Refslund Nielsen, and T. Hoholdt
Dept. of Mathematics, Technical University of Denmark
Bldg. 303, DK-2800 Lyngby, Denmark.
E-mails: h.elbrond.jensen@mat.dtu.dk, stud-rrn@mat.dtu.dk, tom@mat.dtu.dk

Abstract — We analyse the known decoding algorithms for algebraic geometry codes in the case where the number of errors is \(\lceil(d_{FR} - 1)/2\rceil + 1\), 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 Hoholdt [1] checks any error pattern of weight up to \(\lceil(d_{FR} - 1)/2\rceil\) 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 \(\lceil(d_{FR} - 1)/2\rceil + 1\), and show that in the typical case where the error points are “independent” the algorithm always fails, except for high rates where it performs remarkably well. We also treat the case where we have “dependent” errors and show that in this case we can almost always correct \(\lceil(d_{FR} - 1)/2\rceil + 1\) errors.

II. THE CODES AND THE DECODING ALGORITHM

Let \(P_1, P_2, \ldots, P_n\) be \(\mathbb{F}_{q^2}\)-rational points on a nonsingular absolutely irreducible curve \(\chi\) of genus \(g\) defined over \(\mathbb{F}_q\). We consider an algebraic geometry code \(C_m\) of type \(C_L(D, G)^* = C_D(D, G)\), where \(D = P_1 + P_2 + \ldots + P_n\) and \(G = mQ\).

The code has length \(n\), and for any \(y \in \mathbb{F}_{q^2}\) we have

\[
y \in C_m \iff \sum_{j=1}^n f(P_j) y_j = 0
\]

for all \(f \in L(mQ)\).

When \(2g - 2 < m < n\), the dimension of \(C_m\) is \(n - (m - g + 1)\) and the minimum distance is lower bounded by \(d^* = m - 2g + 2\). When \(m < 4g - 2\) this estimate is improved by the Feng-Rao bound \(d_{FR}\). One has \(d_{FR} \geq d^*\) with equality if \(m \geq 4g - 2\).

Recall that a number \(P_i\) is a non-gap for \(Q\) if \(L(P_iQ) \neq L((P_i - 1)Q)\). In this case there exists a function \(\varphi_i \in L(P_iQ) \setminus L((P_i - 1)Q)\), which means that \(\varphi_i\) has a pole of order \(P_i\) at \(Q\) and no other poles. It is well known that the non-gaps satisfy

\[
0 = P_1 < P_2 < \ldots < P_g < P_{g+1} = 2g
\]

and \(P_i = i + g - 1\) for \(i \geq g + 1\).

The functions \(\varphi_i, i = 1, 2, \ldots, m - g + 1\) provide a basis for the space \(L(mQ)\).

Let \(R\) denote the ring of all rational functions on \(\chi\) with poles only at \(Q\), that is

\[
R = \bigoplus_{s=0}^\infty L(sQ)
\]

and for \(f \in R\) we let \(\rho(f)\) denote the poleorder of \(f\) at \(Q\).

If \(f \in R\) and \(y \in \mathbb{F}_{q^2}\) we define the syndrome \(S_y(f)\) to be

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

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

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

If \(\tau\) is the Hamming weight of \(e\) then it is well known e.g. [1] or [2] that if one knows the syndromes \(S_y(f)\) where \(\rho(f) \leq 2(\tau + 2g) - 1\) then the error vector can be easily found.

The objective of the decoder is to determine the syndromes \(S_y(f)\) where \(\rho(f) \leq 2(\tau + 2g) - 1\).

In the decoding algorithm we use a partial ordering \(\leq\) of the poles ordered by \(\rho(f) \leq \rho(g)\) if there exists a \(h \in R\) such that \(\rho(fh) = \rho(g)\). We define the span of an element \(f \in R\) by

\[
\text{span}(f) = \{h \in R \mid \rho(fh) = 0\text{ for all }i \leq i\}
\]

The decoding algorithm is a version of Sakata's generalization of the Berlekamp-Massey algorithm. It has two main parts. The first part is an iterative procedure that based on the syndromes \(S(\varphi_i)\), where \(\varphi_i < m\) calculates two sets of functions

\[
F_M = \{f \in R \mid S(\varphi_i f) = 0\text{ for all }j, \rho(f) + \rho_i \leq m\}
\]

\[
G_M = \{g \in R \mid S(\varphi_i g) \neq 0\text{ for some }i, \rho(f) + \rho_i \leq m\}
\]

where \(M = m - g + 1\). Furthermore, the following set of poles is calculated

\[
\Delta_M = \{\varphi(j) \mid j \in G_M\} = \{\text{span}(g) \mid g \in G_M\}
\]

The second part uses for \(M' > M\) the obtained sets \(F_{M'}, G_{M'}, \Delta_{M'}\) to determine \(S(f)\) where \(\rho(f) = m' + 1, m' \geq m\) by a voting procedure.

This algorithm indeed solves the decoding problem when \(\tau \leq \lceil(d_{FR} - 1)/2\rceil\) (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

\[
L(\varphi Q - (P_1 + \cdots + P_r)) = 0 \text{ for } \varphi \leq \varphi_r
\]

Theorem 1: If \(m \geq 4g - 2\), \(\tau \geq \lceil(d_{FR} - 1)/2\rceil\), 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 \(\mathbb{F}_{q^2}\) given by the equation

\[
x^{q^2+1} + y^{q^2+1} = 0
\]

which has genus \(g = \frac{q(q-1)}{2}\) and \(r \mathbb{F}_{q^2}\)-rational points we can often do much better than predicted by the Feng-Rao bound.
Table 1: The number of dependent and independent error patterns in randomly generated patterns with a given number of points from the Hermitian curve over $\mathbb{F}_{64}$.

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

If $r = 8$ we get a $(512, 476, 9)$-code over $\mathbb{F}_{64}$, 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 $\tau = [(d_{FR} - 1)/2] + 1$ and

$$L(\rho Q - (P_1 + \cdots + P_r)) = 0 \text{ for } \rho < \rho_r,$$

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

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

Theorem 3: The algorithm corrects $\tau = [(d_{FR} - 1)/2] + 1$ 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 e.g. table 1 for conjecturing that (at least on a Hermitian curve) that the probability of getting independent points is $1 - \frac{1}{q}$.

REFERENCES

