On Erasure Decoding of AG-codes

Iwan M. Duursma

July 1994

Abstract

We present a scheme for erasure decoding of AG-codes of complexity $O(n^2)$. This improves on methods involving Fourier transforms.

The trivial scheme for erasure decoding of AG-codes (Algebraic Geometry codes in full, or Geometric Goppa codes) solves a system of linear equations. The scheme is of complexity $O(n^3)$, where n denotes the codelength. Fast schemes, that use a Fourier transform of all syndromes, improve on the complexity. For codes over $GF(q)$ defined with curves in r-dimensional affine space, there are $(q-1)^r$ syndromes to be computed. The transformation itself is of complexity $O(nq^r)$ [1]. In general, $q^r > n$.

The determination of syndromes is computationally equivalent to the determination of the message symbols. We give a scheme for the computation of the message symbols. It avoids the computation of the syndromes and the use of the Fourier transform. The scheme requires $3kn$ field multiplications, with k the dimension of the code.

Notation 1 The notation will be as follows. Let C be a linear code of type $[n, k]$, with generator matrix G and parity check matrix H. Let $\mathbf{m} = (m_i), \mathbf{c} = (c_i), \mathbf{e} = (e_i), \mathbf{y} = (y_i)$ denote a message, the encoded message, an error vector, and the received message respectively. The vectors are related via

$$\begin{aligned} \mathbf{c} &= \mathbf{m}G, \\ \mathbf{y} &= \mathbf{c} + \mathbf{e}. \end{aligned}$$

Let it be known that errors occurred only at the coordinates $I \subset \{1, 2, \ldots, n\}$. For a fixed code C, erasure decoding concerns the determination of the message $\mathbf{m}$, given the received message $\mathbf{y}$ and the set of unreliable positions I.

In algebraic decoding, the set of unreliable positions I will in general be given as the set of zeros of an error-locating vector [2].

Definition 2 By $\mathbf{u} * \mathbf{e} == (u_i e_i)$ we denote the componentwise product of vectors $\mathbf{u}$ and $\mathbf{e}$. A vector $\mathbf{u}$ is called error-locating if it has the support of $\mathbf{e}$ among its zeros. Equivalently, if $\mathbf{u} * \mathbf{e} = \mathbf{0}$.

We recall two known solutions to erasure decoding. Both compute the error vector first.

Proposition 3 The error vector $\mathbf{e}$ can be computed from the system of linear equations

$$\begin{aligned} &H\mathbf{e}^T = H\mathbf{y}^T, \\ &e_i = 0, \text{ for } i \notin I. \end{aligned} \tag{1.1}$$

Alternatively, for a regular square matrix $\bar{H}$ of size $n' \geq n$, and a complete syndrome vector $\mathbf{s}^T = \bar{H}\mathbf{e}^T$, it can be obtained as

$$\mathbf{e}^T = \bar{H}^{-1}\mathbf{s}^T. \tag{1.2}$$

The computation of the message vector then proceeds in both cases via

(2) Compute $\mathbf{c} = \mathbf{y} - \mathbf{e}$.
(3) Compute $\mathbf{m}$, with $\mathbf{c} = \mathbf{m}G$.

The complexity of the procedure is determined by the first step. It equals $O(n^3)$ and $O(nn')$ respectively for the two different versions.

Proof. We consider the complexities. Solving a general system of lineair equations of size $(n-k) \times t$ is of complexity $O((n-k)t^2)$. For the second version, note that the computation of each of the unknown coordinates in $\mathbf{e}$ requires $O(n')$ operations. □

For AG-codes, the procedures can be improved in several ways. The main idea is that message symbols can be computed with the same complexity as syndromes.

Definition 4 Let $\bar{H}$ be a regular square matrix of size n with rows $\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_n$. We assume that the rows of H are given by $\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_{n-k}$. Similarly, let a regular square matrix $\bar{G}$ have rows $\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_n$, such that the rows of G are given by $\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_k$. In addition, we assume that

$$\begin{aligned} \mathbf{g}_i \cdot \mathbf{h}_j &= 0, \text{ for } i+j \leq n, \\ \mathbf{g}_i \cdot \mathbf{h}_j &= 1, \text{ for } i+j = n+1. \end{aligned}$$

A message vector for the code C will be given as a vector of length n, with only the first k symbols nonzero.

Proposition 5 Let $\bar{H}$ and $\bar{G}$ be as in the definition. The message $\mathbf{m}$ and the syndromes $\mathbf{s}$ satisfy the relation

$$\mathbf{m} = \mathbf{y}\bar{H}^T(\bar{G}\bar{H}^T)^{-1} - \mathbf{s}(\bar{G}\bar{H}^T)^{-1}.$$

Proof. After substitution of $\mathbf{s} = \mathbf{e}\bar{H}^T$, the right hand side reduces to $(\mathbf{y}-\mathbf{e})\bar{G}^{-1}$. With Notation 1, and $\mathbf{m}$ of length n as in the definition, we are done. □

Remark 6 The constant part $\mathbf{y}\bar{H}^T(\bar{G}\bar{H}^T)^{-1}$ in the relation can be computed as soon as a word is received. Thus, as part of an error-correction scheme it can be computed at the time that the errors in the word are being located. For the time complexity of an error-correction scheme, only the multiplication of $\mathbf{s}$ by $(\bar{G}\bar{H}^T)^{-1}$ is relevant. From the definition it is clear that the matrix $\bar{G}\bar{H}^T$ is triangular with zeros above the back-diagonal and ones

on the back-diagonal. For AG-codes, its entries will in general be contained in the field of definition of the curve. Often this will be the prime field. More precisely, this will hold if the set of rational points in the code construction and the defining divisor of the code are stable under conjugation.

With the proposition, the transformation of the syndrome vector to the error vector can be ommitted in the calculation of the message. Provided that we dispose of suitable vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$, the syndromes can be computed recursively.

Definition 7 Let $\mathbf{u}$ be an error-locating vector for the errorpattern $\mathbf{e}$. Also, for the given vector $\mathbf{u}$, let vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ be given, such that

$$\mathbf{v}_i * \mathbf{u} = \mathbf{h}_{n+1-i} + \sum_{j<n+1-i} \lambda_{i,j} \mathbf{h}_j.$$

Lemma 8 Let $\mathbf{u}$, $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ be as in the definition. Let $\mathbf{s}^T = \bar{H}\mathbf{e}^T$. The syndromes $s_{n-k+1}, \ldots, s_n$ can be computed recursively via

$$s_{n+1-i} = -\sum_{j<n+1-i} \lambda_{i,j} s_j.$$

Proof. For the vectors $\mathbf{v}_i$, we have

$$\begin{aligned} 0 &= \mathbf{v}_i \cdot (\mathbf{u} * \mathbf{e}) \\ &= (\mathbf{v}_i * \mathbf{u}) \cdot \mathbf{e} \\ &= (\mathbf{h}_{n+1-i} + \sum_{j<n+1-i} \lambda_{i,j} \mathbf{h}_j) \cdot \mathbf{e} \\ &= s_{n+1-i} + \sum_{j<n+1-i} \lambda_{i,j} s_j. \end{aligned}$$

□

In Proposition 5, the calculation of the error vector was ommitted. But in fact, for the computation of the message symbols, we can also ommit the calculation of the syndromes. And, for this computation, we do need to know neither the coefficients $\lambda_{i,j}$, nor the entries of $\bar{G}\bar{H}^T$.

Lemma 9 Let $\mathbf{y}_i = \mathbf{e} + m_1\mathbf{g}_1 + m_2\mathbf{g}_2 + \ldots + m_i\mathbf{g}_i$. Let $\mathbf{u}$,$\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ be as in the definition. Then $m_i = (\mathbf{v}_i * \mathbf{u}) \cdot (\mathbf{y}_i)$.

Proof. We have

$$\begin{aligned}(\mathbf{v}_i * \mathbf{u}) \cdot (\mathbf{y}_i) &= (\mathbf{v}_i * \mathbf{u}) \cdot \mathbf{e} + (\mathbf{v}_i * \mathbf{u}) \cdot (\mathbf{y}_i - \mathbf{e}) \\ &= 0 + (\mathbf{h}_{n+1-i} + \sum_{j<n+1-i} \lambda_{i,j}\mathbf{h}_j) \cdot (\sum_{i' \le i} m_{i'}\mathbf{g}_{i'}) \\ &= \mathbf{h}_{n+1-i} \cdot m_i\mathbf{g}_i + 0 \\ &= m_i.\end{aligned}$$

□

The lemma leads to the following erasure decoding scheme.

Theorem 10 Let the notation be as in Notation 1 and Definition 7. The following scheme produces on input $\mathbf{y}, \mathbf{u}, \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k$ the output $\mathbf{m}, \mathbf{e}$.

(0) Let $i = k$. Let $\mathbf{y}_k = \mathbf{y}$
While $i > 0$,
(1) Compute $m_i = (\mathbf{v}_i * \mathbf{u}) \cdot (\mathbf{y}_i)$
(2) Compute $\mathbf{y}_{i-1} = \mathbf{y}_i - m_i\mathbf{g}_i$
(3) Decrease i by 1
Stop (i=0)

The scheme is of complexity $O(n^2)$.

Proof. The equalities in (1) and (2) follow with the lemma. The output $\mathbf{y}_0 = \mathbf{e}$. Step (1) requires $2n$ field multiplications. Step (2) requires n field multiplications. A complete run involves $3kn$ field multiplications. □

For the scheme, it is essential that the Definitions 2,4 and 7 can be justified. We claim without giving details that the definitions are natural for AG-codes in general. The following example illustrates the scheme for a special case.

Example 11 We consider codes over the field $F = \{0, 1, \omega, \bar{\omega}\}$ of four elements constructed with the Hermitian curve, defined by $Y^2Z + YZ^2 = X^3$. The only point at infinity is $(0 : 1 : 0)$. The functions $x = X/Z$ and $y = Y/Z$ have a pole at $(0 : 1 : 0)$ of order 2 and 3 respectively. The curve has eight finite rational points $P_1, P_2, \ldots, P_8$. The one-point codes have as codewords $\alpha(f) = (f(P_1), f(P_2), \ldots, f(P_8))$, for a function f with poles only at $(0 : 1 : 0)$. That is, for $f \in F[x, y]$. The dual codes can be defined in the same way.

Thus, we define

$$\bar{G} = \bar{H} = \begin{pmatrix} \alpha(1) \\ \alpha(x) \\ \alpha(y) \\ \alpha(x^2) \\ \alpha(xy)) \\ \alpha(x^3) \\ \alpha(x^2y) \\ \alpha(x^3y) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \omega & \omega & \bar{\omega} & \bar{\omega} \\ 0 & 1 & \omega & \bar{\omega} & \omega & \bar{\omega} & \omega & \bar{\omega} \\ 0 & 0 & 1 & 1 & \bar{\omega} & \bar{\omega} & \omega & \omega \\ 0 & 0 & \omega & \bar{\omega} & \bar{\omega} & 1 & 1 & \omega \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & \omega & \bar{\omega} & 1 & \omega & \bar{\omega} & 1 \\ 0 & 0 & \omega & \bar{\omega} & \omega & \bar{\omega} & \omega & \bar{\omega} \end{pmatrix}$$

And we obtain

$$\bar{G}\bar{H}^T = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Let a word sent be in the span of the first four rows of $\bar{G}$. Let $\mathbf{y} = (\omega, 0, \bar{\omega}, \omega, \omega, \bar{\omega}, 1, \omega)$ be the received word with unreliable values at the zeros of

$$\mathbf{u} = \alpha(1) + \bar{\omega}\alpha(x) + \alpha(y) = (1, 0, 0, 1, \omega, \bar{\omega}, 1, 0).$$

For $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ and $\mathbf{v}_4$, we take $\alpha(x^3), \alpha(x^2), \alpha(y)$ and $\alpha(x)$ respectively. To compute the message $\mathbf{m}$ with Proposition 5, we consider the syndrome vectors

$$\begin{aligned} \mathbf{y}\bar{H}^T &= (1, 1, \omega, \bar{\omega}, 0, \bar{\omega}, \omega, \omega). \\ \mathbf{e}\bar{H}^T &= (1, 1, \omega, \bar{\omega}, s_5, s_6, s_7, s_8). \end{aligned}$$

Application of Lemma 8 yields,

$$\begin{array}{ll}
\alpha(x) * \mathbf{u} = \alpha(xy) + \bar{\omega}\alpha(x^2) + \alpha(x), & s_5 = \bar{\omega}s_4 + s_2 = \bar{\omega}. \\
\alpha(y) * \mathbf{u} = \alpha(x^3) + \bar{\omega}\alpha(xy), & s_6 = \bar{\omega}s_5 = \omega. \\
\alpha(x^2) * \mathbf{u} = \alpha(x^2y) + \bar{\omega}\alpha(x^3) + \alpha(x^2), & s_7 = \bar{\omega}s_6 + s_4 = \omega. \\
\alpha(x^3) * \mathbf{u} = \alpha(x^3y) + \alpha(x^3) + \bar{\omega}\alpha(x). & s_8 = s_6 + \bar{\omega}s_2 = 1.
\end{array}$$

And

$$\mathbf{m} = (\mathbf{y}\bar{H}^T - \mathbf{e}\bar{H}^T)(\bar{G}\bar{H}^T)^{-1} = (\bar{\omega}, 1, 0, \omega, 0, 0, 0, 0).$$

Next, we compute $\mathbf{m}$ with Theorem 10.

$$\begin{array}{lll}
 & & \mathbf{y}_4 = \mathbf{y} = (\omega, 0, \bar{\omega}, \omega, \omega, \bar{\omega}, 1, \omega). \\
i = 4: & m_4 = (\alpha(x) * \mathbf{u}) \cdot \mathbf{y}_4 = \bar{\omega}, & \mathbf{y}_3 = \mathbf{y}_4 - m_4\alpha(x^2) = (\omega, 0, 0, 1, 0, 1, 0, \bar{\omega}) \\
i = 3: & m_3 = (\alpha(y) * \mathbf{u}) \cdot \mathbf{y}_3 = 1, & \mathbf{y}_2 = \mathbf{y}_3 - m_3\alpha(y) = (\omega, 1, \omega, \omega, \omega, \omega, \omega, 0) \\
i = 2: & m_2 = (\alpha(x^2) * \mathbf{u}) \cdot \mathbf{y}_2 = 0, & \mathbf{y}_1 = \mathbf{y}_2 - m_2\alpha(x) = (\omega, 1, \omega, \omega, \omega, \omega, \omega, 0) \\
i = 1: & m_1 = (\alpha(x^3) * \mathbf{u}) \cdot \mathbf{y}_1 = \omega, & \mathbf{y}_0 = \mathbf{y}_1 - m_1\alpha(1) = (0, \bar{\omega}, 0, 0, 0, 0, 0, \omega) \\
i = 0: & \text{Stop} &
\end{array}$$

Indeed $\mathbf{y}_0 = \mathbf{e}$ has its support among the zeros of $\mathbf{u}$.

References

[1] C. Dahl, Fast decoding of codes from algebraic curves, IEEE Transactions on Information Theory, To appear.

[2] R. Pellikaan, On decoding by error location and dependent sets of error positions, Discrete Mathematics, vol.106-107, pp.369-381, 1992.

Acknowledgement

This work was done with the support of the Dutch Organization for Scientific Research, while visiting the Laboratoire de Mathématiques Discrètes at Luminy, France.