



Unique decoding of m -point codes using lists

Gretchen L. Matthews, Clemson University

gmatthe@clemson.edu

Abstract. An m -point AG code is constructed by evaluating functions which are allowed to have poles at m specified points on a curve X . While such a code can have better parameters than comparable one-point codes on the same curve, one-point codes are certainly better understood. Here, we view an m -point code as a subcode of a one-point code and discuss the implications for list decoding. In particular, we consider how list decoding in the supercode may yield unique decoding for the m -point code up to its minimum distance.

m -point codes are AG codes where the functions to be evaluated are allowed to have poles at m points



2/7

Let X be a curve over a finite field \mathbb{F} , and let $P_1, \dots, P_n, Q_1, \dots, Q_m$ be distinct \mathbb{F} -rational points of X .

Set $D := P_1 + \dots + P_n$ and $G := a_1Q_1 + \dots + a_mQ_m$ where $a_i \geq 0$.

Let

$$\mathcal{L}\left(\sum_{i=1}^m a_i Q_i\right) = \left\{ f \in \mathbb{F}(X) : (f) \leq -\sum_{i=1}^m a_i Q_i \right\}$$

denote the space of rational functions f on X such that

- the only poles of f are at Q_1, \dots, Q_m , and
- the pole order at Q_i at most a_i for all i .

An m -point AG code is of the form

$$C(D, G) = \{(f(P_1), \dots, f(P_n)) : f \in \mathcal{L}(G)\}.$$

m -point codes may be viewed as subcodes of one-point codes



3/7

Since \mathbb{F} is finite, $\exists f$ such that $b_i \geq a_i$ for all $2 \leq i \leq m$, $b_1 = \sum_{i=2}^m b_i$, and

$$(f) = b_2 Q_2 + \cdots + b_m Q_m - b_1 Q_1.$$

Multiplication by f induces an isomorphism

$$\mathcal{L} \left(\sum_{i=1}^m a_i Q_i \right) \rightarrow \mathcal{L} \left((a_1 + b_1) Q_1 - \left(\sum_{i=2}^m (b_i - a_i) Q_i \right) \right) : h \mapsto fh$$

which gives rise to an isometry of codes

$$\begin{aligned} C_m := C_{\mathcal{L}} \left(D, \sum_{i=1}^m a_i Q_i \right) &\cong C_{\mathcal{L}} \left(D, (a_1 + b_1) Q_1 - \left(\sum_{i=2}^m (b_i - a_i) Q_i \right) \right) \\ &\subseteq C_{\mathcal{L}} \left(D, (a_1 + b_1) Q_1 \right) =: C_1. \end{aligned}$$

Hence, we may consider the m -point code as a subcode of a one-point code:

$$C_m = C_{\mathcal{L}} \left(D, \sum_{i=1}^m a_i Q_i \right) \subseteq C_{\mathcal{L}} \left(D, (a_1 + b_1) Q_1 \right) = C_1.$$

List decoding the one-point code may give unique decoding of the m -point code up to its minimum distance



Suppose $w \in \mathbb{F}^n$ is a received word using C_m , with $t := \left\lfloor \frac{d(C_m)-1}{2} \right\rfloor$ errors.

Step 0: Find b so that C_1 is $(n-t, b)$ -decodable.

Step 1: Apply list decoding algorithm to C_1 to find all $h \in \mathcal{L}((a_1 + b_1)Q_1)$ satisfying

$$d((h(P_1), \dots, h(P_n)), w) \leq n - t.$$

Step 2: Compute $v_{Q_i}(h)$ for each h until the unique one is found with

$$v_{Q_i}(h) \geq b_i - a_i \text{ for all } 2 \leq i \leq m.$$

Then $(h(P_1), \dots, h(P_n))$ is the unique codeword in C_m within distance t of w .

Decode w as $(h(P_1), \dots, h(P_n))$.

Example



Consider the $[511, 14, \geq 476]$ two-point code

$$C_2 := C_{\mathcal{L}}(D, 35P_{\infty} + 3P_{00})$$

constructed from the Hermitian curve $y^8 + y = x^9$ over \mathbb{F}_{64} .

C_2 is capable of correcting any 237 or fewer errors, and

$$C_2 \cong C_{\mathcal{L}}(D, 44P_{\infty} - 6P_{00}) \subseteq C_{\mathcal{L}}(D, 44P_{\infty}) =: C_1$$

C_1 is a $[511, 20, 468]$ code and so corrects 233 errors.

Suppose (using C_2) that we receive a word

$$w \in \mathbb{F}_{64}^{511}$$

in which 237 or fewer errors have occurred.

Applying a $(274, 2)$ -list decoding algorithm to C_1 gives 2 words

$$(h_i(P_1), \dots, h_i(P_n))$$

at distance ≤ 274 from codewords in C_1 .

In particular, it returns

$$h_1, h_2 \in \mathcal{L}(44P_\infty)$$

such that

$$d(y, (h_i(P_1), \dots, h_i(P_n), h_i(P_{00}))) \leq 274.$$

Since $d(C_2) \geq 476$, there is a unique function $h \in \mathcal{L}(44P_\infty - 6P_{00})$ such that

$$d(w, (h_i(P_1), \dots, h_i(P_n))) \leq 237.$$

So $h = h_1$ or $h = h_2$.

Check to see which h_i satisfies

$$v_{P_{00}}(h) \geq 6$$

Then **decode** w as $(h_i(P_1), \dots, h_i(P_n))$.



References

- V. Guruswami and M. Sudan, Improved decoding of Reed-Solomon and algebraic-geometric codes, *IEEE Trans. Inform. Theory* **47** (2001), no. 4, 1610–1613.
- W. Mingsheng, Parameter choices on Guruswami-Sudan algorithm for polynomial reconstruction, *Finite Fields Appl.*, to appear.
- M. A. Shokrollahi and H. Wasserman, List decoding of algebraic-geometric codes, *IEEE Trans. Inform. Theory* **45** (1999), 432–437.
- H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, 1993, Universitext.
- M. Sudan, Decoding of Reed-Solomon codes beyond the error correction bound, *J. Compl.* **13**, 180–193, 1997.

