MA4261 Information Theory and Coding Theory
Paper Review Assignment

A review of V. Guruswami and M. Sudan "Improved decoding of Reed-Solomon and algebraic-geometric codes"

Nguyen Ngoc Khanh - A0275047B

November 2024

1 SUMMARY

The summary provides an exploratory approach to this paper rather than the original declarative approach.

1.1 REED-SOLOMON CODES

Definition 1 (Reed-Solomon Codes)**.** *Let $\mathbb{F}_q$ be a field of order q, for $n \leq q$, let $\alpha_1, \alpha_2, ..., \alpha_n$ be distinct in $\mathbb{F}_q$, for each message $m = (m_0, m_1, ..., m_k) \in \mathbb{F}_q^{k+1}$, the polynomial $f_m \in \mathbb{F}_q[x]$ defined by $f_m(x) = m_0 + m_1 x + ... + m_k x^k$*

The $\mathbb{F}_q$-linear map below defines a linear $[n, k+1, n-k]_q$ code

$$\begin{aligned} \mathbb{F}_q^{k+1} &\to \mathbb{F}_q^n \\ m &\mapsto (f_m(\alpha_1), f_m(\alpha_2), ..., f_m(\alpha_n)) \end{aligned}$$

Definition 2 (polynomial reconstruction)**.** *Given natural numbers $k \leq t < n$ and a collection of points $\{(x_i, y_i) \in \mathbb{F}_q \times \mathbb{F}_q\}_{i=1}^n$, polynomial reconstruction is an algorithm that gives all polynomial $p(x) \in \mathbb{F}_q[x]$ of degree at most k such that $y_i = p(x_i)$ for at least t values of (x_i, y_i)*

1.1.1 FACTORING POLYNOMIAL AND SUDAN ALGORITHM

We first mentioned a fact about shifted polynomial as follows:

Lemma 1. *Let $Q(x, y) \in \mathbb{F}[x, y]$, $(x_i, y_i) \in \mathbb{F} \times \mathbb{F}$, and $Q^{(i)}(x, y) = Q(x + x_i, y + y_i)$. Let*

$$Q(x, y) = \sum_{j_1, j_2} q_{j_1, j_2} x^{j_1} y^{j_2} \text{ and } Q^{(i)}(x, y) = \sum_{j_1, j_2} q^{(i)}_{j_1, j_2} x^{j_1} y^{j_2}$$

Then each $q^{(i)}_{j_1, j_2}$ can be written as a $\mathbb{F}$-linear combination of $\{q_{j_1', j_2'}\}_{j_1' \geq j_1, j_2' \geq j_2}$, that is, there exists $a_{i, j_1', j_2'} \in \mathbb{F}$ such that

$$q^{(i)}_{j_1, j_2} = \sum_{j_1' \geq j_1} \sum_{j_2' \geq j_2} a_{i, j_1', j_2'} q_{j_1', j_2'} = 0$$

Now, we will build up Sudan polynomial reconstruction algorithm. Let $\mathbb{F}$ be a field and $p(x) \in \mathbb{F}[x]$ be a polynomial over $\mathbb{F}$ so that $x_i \in \mathbb{F}$ and $y_i = p(x_i) \in \mathbb{F}$. Define $p'(x) \in \mathbb{F}[x]$ by $p'(x) = p(x + x_i) - y_i$. Since, $p'(x) = 0$, then $p'(x) = xp''(x)$ for some polynomial $p''(x) \in \mathbb{F}[x]$. Let $Q(x, y) \in \mathbb{F}[x, y]$ be a polynomial over $\mathbb{F}$, let $Q^{(i)}(x, y) = Q_{x_i, y_i}(x, y)$ be the shifted polynomial of $Q(x, y)$. Let

$$g'(x) = Q^{(i)}(x, p'(x)) = Q^{(i)}(x, xp''(x))$$

If all coefficients of $Q^{(i)}(x, y)$ with total degree less than a positive integer $r \in \mathbb{N}$ are zeros, then $g'(x) = Q^{(i)}(x, p'(x)) = Q^{(i)}(x, xp''(x))$ with all coefficients of $g'(x)$ with degree less than r are zeros. We can write $g'(x) = x^r g''(x)$. Moreover,

$$\begin{aligned} Q(x, p(x)) &= Q^{(i)}(x - x_i, p(x) - y_i) && \text{(shifted polynomial)} \\ &= Q^{(i)}(x - x_i, p'(x - x_i)) && \text{(definition of } p') \\ &= g'(x - x_i) = (x - x_i)^r g''(x - x_i) \end{aligned}$$

Assumption 1. *Given a polynomial $Q(x, y) \in \mathbb{F}[x, y]$, let $(x_i, y_i) \in \mathbb{F} \times \mathbb{F}$. If all coefficients of $Q^{(i)}(x, y)$ with total degree less than $r \in \mathbb{N}$ are zeros, then $(x - x_i)^r$ divides $Q(x, p(x))$*

Let $\{(x_i, y_i) \in \mathbb{F} \times \mathbb{F}\}_{i=1}^n$ be a collection of points and $r \in \mathbb{N}$. If $p(x) \in \mathbb{F}[x]$ is a polynomial such that $y_i = p(x_i)$ for all $i \in S \subseteq [n]$ such that $|S| \geq t$, then $\prod_{i \in S}(x - x_i)^r$ divides $Q(x, p(x))$

As $\prod_{i \in S}(x - x_i)^r$ is of degree at least rt, if we make the total degree of coefficients of $Q(x, y)$ less than rt, then the degree of $Q(x, p(x))$ is less than rt. The condition $y_i = p(x_i)$ for at least t values of (x_i, y_i) on $p(x) \in \mathbb{F}[x]$ implies $y = p(x)$ is a root of $Q(x, y) \in \mathbb{F}[x][y]$ as a polynomial on y over the ring $\mathbb{F}[x]$

Assumption 2. *Suppose all coefficients of $Q(x, y)$ have total degree less than rt, if $p(x) \in \mathbb{F}[x]$ is a polynomial such that $y_i = p(x_i)$ for at least t values of (x_i, y_i), then $y = p(x)$ is a root of $Q(x, y) \in \mathbb{F}[x][y]$ as a polynomial on y over the ring $\mathbb{F}[x]$, in other words, $y - p(x)$ divides $Q(x, y)$ as polynomials on y over the ring $\mathbb{F}[x]$*

We have built up the necessary machinery for an algorithm of polynomial reconstruction. The algorithm is described below

Definition 3 (Sudan [**?**])**.** *Given natural numbers $k < t \leq n$ and a collection of points $\{(x_i, y_i) \in \mathbb{F} \times \mathbb{F}\}_{i=1}^n$. Choose $r \in \mathbb{N}$, The algorithm consists of steps below*

1. *Construct a nonzero polynomial $Q(x,y) \in \mathbb{F}[x,y]$ so that the total degree of all coefficients is less than rt (assumption 2) and moreover, all coefficients of $Q^{(i)}(x,y)$ with total degree less than r are zeros (assumption 1). That is, the coefficients of $Q(x,y)$ satisfy: for every j_1, j_2*

$$q^{(i)}_{j_1,j_2} = \sum_{j_1' \geq j_1} \sum_{j_2' \geq j_2} a_{i,j_1',j_2'} q_{j_1',j_2'} = 0$$

2. *The set of candidate polynomials is the collection of roots of $Q(x,y) \in \mathbb{F}_q[x][y]$ as a polynomial over the ring $\mathbb{F}_q[x]$*

1.1.2 WEIGHTED DEGREE AND GURUSWAMI-SUDAN ALGORITHM

The Sudan algorithm does not specify how to choose r and how to construct the polynomial $Q(x,y)$, and the existence of $Q(x,y)$ was not asserted. In [**?**], the Guruswami and Sudan introduced a way to choose $r \in \mathbb{N}$ and $Q(x,y)$ by notion of weighted degree

Definition 4 (weighted degree)**.** *Given $w_x, w_y \in \mathbb{N}_0$, the (w_x, w_y)-weighted degree of a monomial $\alpha x^i y^j \in \mathbb{F}_q[x,y]$ is defined by $iw_x + jw_y$. The (w_x, w_y)-weighted degree of $Q(x,y) \in \mathbb{F}_q[x,y]$ is the maximum (w_x, w_y)-weighted degree over all monomials with nonzero coefficients*

The authors construct $Q(x,y)$ so that the $(1,k)$-weighted degree of $Q(x,y)$ is $l = rt - 1$, it is obvious that $Q(x,y)$ satisfies assumption 2. Moreover, a stronger condition of the space of $Q(x,y)$ to be nontrivial is that the number of constraints on the coefficients $q_{j_1',j_2'}$ of $Q(x,y)$ is strictly less than the number of unknowns which is the number of coefficients of $Q(x,y)$, that is

$$n\binom{r+1}{2} < \frac{l(l+2)}{2k}$$

Solving the quadratic equation and taking the smallest positive integer r gives

$$r = 1 + \left\lfloor \frac{kn + \sqrt{k^2n^2 + 4(t^2 - kn)}}{2(t^2 - kn)} \right\rfloor$$

Definition 5 (Guruswami-Sudan)**.** *Given natural numbers $k < t \leq n$ and a collection of points $\{(x_i, y_i) \in \mathbb{F}_q \times \mathbb{F}_q\}_{i=1}^n$, define r, t as above. The algorithm consists of the steps below*

1. *Construct a nonzero polynomial $Q(x,y) \in \mathbb{F}[x,y]$ so that the $(1,k)$-weighted degree of $Q(x,y)$ is less than or equal l (assumption 2) and moreover, all coefficients of $Q^{(i)}(x,y)$ with total degree less than r are zeros (assumption 1)*

2. *The set of candidate polynomials is the collection of roots of $Q(x,y) \in \mathbb{F}_q[x][y]$ as a polynomial over the ring $\mathbb{F}_q[x]$*

Moreover, provided $t > \sqrt{kn}$, when $n \to \infty$, the choice of r is bounded by a constant which yields a polynomial time in n algorithm.

Theorem 1 (Guruswami-Sudan)**.** *Provided $t > \sqrt{kn}$, Guruswami-Sudan is a polynomial time in n algorithm.*

1.2 EASY EXTENSIONS

In the paper, Guruswami and Sudan also mentioned some easy extensions of the polynomial reconstruction algorithm:

- Alternant codes
- Erasure error
- Decoding with uncertain receptions
- Weighted polynomial reconstruction

1.3 ALGEBRAIC-GEOMETRY CODES

1.3.1 ALGEBRAIC-GEOMETRY CODES

Some basic of algebraic-geometry codes (note that, this is a simplified version of AG codes, details can be found at [**?**])

Definition 6 (function field)**.** *Let $\overline{\mathcal{X}}$ be a finite set and $\mathcal{F}_q$ be a finite field of order q, then the set of functions $\mathrm{Hom}\big(\overline{\mathcal{X}}, \overline{\mathbb{F}}_q \cup \{\infty\}\big)$ is a field extension of $\mathbb{F}_q$ and a subfield $K \subseteq \mathrm{Hom}\big(\overline{\mathcal{X}}, \overline{\mathbb{F}}_q \cup \{\infty\}\big)$ is called a function field.*

Definition 7 (order (a generalized notion of degree)). *Let $\overline{\mathcal{X}}$ be a finite set and $\mathcal{F}_q$ be a finite field of order q and $K \subseteq \mathrm{Hom}\big(\overline{\mathcal{X}}, \overline{\mathbb{F}}_q \cup \{\infty\}\big)$ be a function field, a function $\mathrm{ord} : K \times \overline{\mathcal{X}} \to \mathbb{Z}$ is called order if the following satisfy*

1. *$f(x) = 0 \iff \mathrm{ord}(f, x) < 0$ and $f(x) = \infty \iff \mathrm{ord}(f, x) > 0$ for all $f \in K \setminus \{0\}$ and $x \in \overline{\mathcal{X}}$*
2. *$\mathrm{ord}(fg, x) = \mathrm{ord}(f, x) + \mathrm{ord}(g, x)$ for all $f, g \in K \setminus \{0\}$ and $x \in \overline{\mathcal{X}}$*
3. *$\mathrm{ord}(f + g, x) \leq \max\{\mathrm{ord}(f, x), \mathrm{ord}(g, x)\}$ for all $f, g \in K \setminus \{0\}$ and $x \in \overline{\mathcal{X}}$*
4. *if $\sum_{x \in \overline{\mathcal{X}}} \mathrm{ord}(f, x) < 0$, then $f = 0$*

Definition 8 (algebraic function field). *Let $\overline{\mathcal{X}}$ be a finite set and $\mathcal{F}_q$ be a finite field of order q and $K \subseteq \mathrm{Hom}\big(\overline{\mathcal{X}}, \overline{\mathbb{F}}_q \cup \{\infty\}\big)$ be a function field, and an order $\mathrm{ord} : K \times \overline{\mathcal{X}} \to \mathbb{Z}$ be an order. Let $\mathcal{X} \subseteq \overline{\mathcal{X}}$ be a subset of $\mathcal{X}$ called rational points so that for every $f \in K$, the image of $\mathcal{X}$ under f is a subset of $\mathbb{F}_q \cup \{\infty\}$. Moreover, let $i \in \mathbb{Z}$ and $x \in \overline{\mathcal{X}}$, let $V_{i,x} = \{f \in K : \mathrm{ord}(f, x) \leq i\}$, and*

$$L_{i,x} = V_{i,x} \cap \left(\bigcap_{y \in \overline{\mathcal{X}} \setminus \{x\}} V_{0,y} \right) = \{f \in K : \mathrm{ord}(f, x) \leq i \text{ and for every } y \in \overline{\mathcal{X}} \setminus \{0\}, \mathrm{ord}(f, y) \leq 0\}$$

$L_{i,x}$ is a vector space over $\mathbb{F}_q$ for every $i \in Z$ and $x \in \overline{\mathcal{X}}$. Let $g \in \mathbb{N}_0$ be a nonnegative integer then the tuple $\mathcal{A} = (\mathbb{F}_q, \mathcal{X}, \overline{\mathcal{X}}, K, \mathrm{ord}, g)$ satisfying the above properties is called an algebraic function field.

Theorem 2 (Riemann-Roch). *There exists an algebraic function field such that*

$$\dim(L_{k+g-1,x}) \geq k$$

Proposition 1 (algebraic-geometry codes). *Let $\mathcal{A} = (\mathbb{F}_q, \mathcal{X}, \overline{\mathcal{X}}, K, \mathrm{ord}, g)$ be an algebraic function field with $n + 1$ distinct rational points $x_0, x_1, x_2, ..., x_n$. Let $k \in \mathbb{N}$, the $\mathbb{F}_q$-linear map below defines a $[n, k', d']_q$ code for some $k' \geq k$ and $d' \geq n - k - g + 1$*

$$\begin{aligned} L_{k+g-1,x_0} &\to \mathbb{F}_q^n \\ f &\mapsto (f(x_1), f(x_2), ..., f(x_n)) \end{aligned}$$

Proposition 2 (Reed-Solomon codes as an algebraic-geometry codes [**?**] Proposition 2.3.5). *Every generalized Reed-Solomon code can be represented as a rational AG code*

From the defintion of algebraic function field, below are some necessary lemmas to develop the decoding algorithm for AG code.

Lemma 2. *For every $f, g \in K$ and $x \in \overline{\mathcal{X}}$, there exists $\alpha, \beta \in \mathbb{F}_q$ with $(\alpha, \beta) \neq (0, 0)$ such that*

$$\mathrm{ord}(\alpha f + \beta g, x) < \max\{\mathrm{ord}(f, x), \mathrm{ord}(g, x)\}$$

Lemma 3. *Given $\{\phi_{j_1} \in K : j_1 \in [p]\}$ of distinct orders at rational point $x_0 \in \mathcal{X}$ such that $\phi_{j_1} \in L_{j_1+g-1,x_0}$. For any rational point $x_1 \neq x_0$, there exists $\{\psi_{j_3,x_i} \in K : j_3 \in [p]\}$ such that $\mathrm{ord}(\phi_{j_3}, x_i) \leq 1 - j_3$ and*

$$[\phi_{j_1}] = [\alpha_{x_i,j_1,j_3}][\psi_{x_i,j_3}]$$

where $[\phi_{j_1}] = (\phi_1, \phi_2, ..., \phi_p)^T \in M_p(K)$ is a column vector of p elements from K, $[\psi_{x_i,j_3}] = (\psi_1, \psi_2, ..., \psi_p)^T \in M_p(K)$, and $[\alpha_{x_i,j_1,j_3}] \in M_{p \times p}(K)$ is a matrix of $p \times p$ elements from $\mathbb{F}_q \subseteq K$

1.3.2 THE DECODING ALGORITHM

Provided the form of $Q(y)$, the analogous shifted polynomial can be solved as a system of linear equations

Assumption 3 (shape of $Q(y)$). *Given an algebraic code, let $\alpha = k + g - 1$, $s = \left\lfloor \frac{l-g}{\alpha} \right\rfloor$, suppose $Q(y)$ is of the form*

$$Q(y) = \sum_{j_2}^{s} \sum_{j_1}^{l-g+1-\alpha j_2} q_{j_1,j_2} \phi_{j_i} y^{j_2}$$

where the functions $\phi_1, \phi_2, ..., \phi_{l-g+1} \in K$ satisfy $\mathrm{ord}(\phi_{j_1}, x_0) \leq j_1 + g - 1$ and $\mathrm{ord}(\phi_j, x_0) \leq \phi_{j+1}, x_0$ (constructed from lemma 2)

The authors also provided the generalization of shifted polynomial for AG code.

Lemma 4 (shifted polynomial)**.** *Let $y_i \in \mathbb{F}_q$ and $Q(y) \in K$, define the shifted polynomial $Q^{(i)} \in K$ by $Q^{(i)}(y) = Q(y+y_i)$. Given an algebraic code, suppose $Q(y)$ is of the shape in assumption 3. Then, from lemma 3, we have*

$$Q(y)(x) = \sum_{j_2}^{s} \sum_{j_1}^{l-g+1-\alpha j_2} \sum_{j_3=1}^{l-g+1} q_{j_1,j_2} \alpha_{x_1,j_1,j_3} \psi_{x_i,j_3}(x) y^{j_2}$$

and the shifted polynomial $Q^{(i)}(y)$ is

$$Q^{(i)}(y)(x) = \sum_{j_4=0}^{s} \sum_{j_3=1}^{l-g+1} q^{(i)}_{j_3,j_4} \psi_{x_i,j_3}(x) y^{j_4}$$

where each $q^{(i)}_{j_3,j_4}$ is a $\mathbb{F}_q$-linear combination of $\{q_{j_1,j_2}\}$, that is, $q^{(i)}_{j_3,j_4} = \sum_{j_2=j_4}^{s} \sum_{j_4}^{l-g+1-\alpha j_2} \beta_{x_i,j_1,j_2,j_3,j_4} q_{j_1,j_2}$ where $\beta_{x_i,j_1,j_2,j_3,j_4} \in \mathbb{F}_q$

Given the form of $Q(y)$, we can deduce

Lemma 5. *For $i \in [n]$, if $h \in K$ such that $h(x_i) = y_i$, then $\operatorname{ord}(Q(h), x_i) \leq -r$*

The correctness of the decoding algorithm for AG codes is as follows:

Suppose $h \in L_{k+g-1,x_0}$, then $\operatorname{ord}(q_{j_1,j_2}\phi_{j_1}h^{j_2}, -) = \operatorname{ord}(\phi_{j_1}h^{j_2}, -) = \operatorname{ord}(\phi_{j_1}, -) + j_2 \operatorname{ord}(h, -)$. Substitute $-$ by x_0 and $x_i \neq x_0$, we have $Q(h) \in L_{l,x_0}$. If $h(x_i) = y_i$, $i \in S$ and $|S| \geq t$, given $rt > l$, we must have $\sum_{i\in S} \operatorname{ord}(Q(h), x_i) \leq -rt < -l$

As $Q(h) \in L_{l,x_0}$, then

$$\sum_{x\in\overline{\mathcal{X}}} \operatorname{ord}(Q(h), x_i) \leq \operatorname{ord}(Q(h), x_0) + \sum_{i\in S} \operatorname{ord}(Q(h), x_i) + \sum_{x\in\overline{\mathcal{X}}\setminus\{x_0\}\setminus S} \operatorname{ord}(Q(h), x) < 0$$

Hence, $Q(h) = 0$, that is, $y - h$ divides $Q(y)$

Lemma 6. *If $h \in L_{k+g-1,x_0}$ such that $h(x_i) = y_i$ for at least t values of (x_i, y_i) and $rt > l$, then $y - h$ divides $Q(y)$*

The build up for AG code was finished, the algorithm is stated below:

Definition 9 (Guruswami-Sudan)**.** *Given an algebraic-geometry code. Let $\alpha = k + g - 1$, $s = \left\lfloor \frac{l-g}{\alpha} \right\rfloor$,*

$$r = 1 + \left\lfloor \frac{2gt + \alpha n + \sqrt{(2gt + \alpha n)^2 - 4(g^2 - 1)(t^2 - \alpha n)}}{2(t^2 - \alpha n)} \right\rfloor \text{ and } l = rt - 1$$

Let $\{\phi_{j_1} \in K : j_1 \in [l - g + 1]\}$ be a collection of distinct orders at x_0 such that $\operatorname{ord}(\phi_{j_1}, x_0) \leq j_1 + g - 1$. From lemma 3, for each x_i, there is a collection $\{\phi_{x_i,j_3} \in K : j_3 \in [l - g + 1]\}$ and $\{\alpha_{x_i,j_1,j_3} : (j_1, j_3) \in [l - g + 1] \times [l - g + 1]\}$ such that

$$[\phi_{j_1}] = [\alpha_{x_i,j_1,j_3}][\psi_{x_i,j_3}]$$

and $\operatorname{ord}(\phi_{x_i,j_3}, x_i) \leq 1 - j_3$.

The algorithm consists of two steps

1. *Find a nonzero polynomial $Q \in K[y]$ of the form as in assumption 3: $Q(y) = \sum_{j_2=0}^{s} \sum_{j_1=1}^{l-g+1-\alpha j_2} q_{j_1 j_2} \phi_{j_1} y^{j_2}$ such that for every $i \in [n]$,*

$$q^{(i)}_{j_3,j_4} = \sum_{j_2=j_4}^{s} \sum_{j_4}^{l-g+1-\alpha j_2} \beta_{x_i,j_1,j_2,j_3,j_4} q_{j_1,j_2} = 0$$

2. *The set of candidate polynomials $f \in K$ is the collection of roots $h \in L_{k+g-1,x_0}$ of Q.*

Moreover, by the same analysis as above, the algorithm is of polynomial time in n given $t \geq \sqrt{k + g - 1}$

Theorem 3 (Guruswami-Sudan)**.** *Provided $t \geq \sqrt{k + g - 1}$, Guruswami-Sudan is a polynomial time in n algorithm for algebraic-geometry codes.*

2 ADVOCATE VIEW

Guruswami-Sudan algorithm is a choice of r and polynomial $Q(x, y)$ that yields a polynomial time on both Reed-Solomon codes and algebraic-geometry codes.

1. The method gives a wide range of possible errors $e < n - \sqrt{kn}$ for Reed-Solomon codes and $n - \sqrt{n(n-d')}$ for algebraic-geometry codes for every choice of n, k, d. Moreover, when $k/n > 1/3$, the Reed-Solomon version induces the first asymptotic improvement in four decades.

2. Other than that, the authors gave a sufficient motivation to study the list decoding problem. Moreover, they provided some other applications of Reed-Solomon version.

3 CRITIC VIEW

Even though the method provides the existence of solutions,

1. The choice of r and weighted degree remains a question whether they are the optimal choice. One example is of the number of constraints, it is exactly

$$\sum_{i=1}^{n}\sum_{j_1=0}^{\infty}\sum_{j_2=0}^{\infty} 1_{j_1+j_2<r} = nr^2 < n\binom{r+1}{2}$$

which was not tight in the paper. *due to some miscalculation, the claim on number of constraints was wrong, the bound was indeed tight, i.e.* $\sum_{i=1}^{n}\sum_{j_1=0}^{\infty}\sum_{j_2=0}^{\infty} 1_{j_1+j_2<r} = n\binom{r+1}{2}$. *by optimal choice, what I concerned was the authors did not explain why they chose the* $(1,k)$*-weighted degree over other conditions to bound the degree of* $Q(x,y)$*, whether is there any other choice can offer better bound (the* $(1,k)$*-weighted degree is a triangle on* j_1, j_2 *space). In terms of logic, this was sound but not complete. In terms of information theory, this was a proof for the achievability part but no converse part*

2. In Reed-Solomon version, at the regime where $\epsilon = \frac{t^2}{kn} - 1$ close to zero, r is unbounded below

$$\begin{aligned} r &\geq \frac{kn + \sqrt{k^2n^2 + 4(t^2 - kn)}}{2(t^2 - kn)} \\ &= \frac{1 + \sqrt{1 + 4\epsilon}}{2\epsilon} \to \infty \end{aligned}$$

That makes the runtime pseudo-polynomial. This is a gap that was not addressed in the paper.

3. In AG version, the method assumed the form of $Q(y)$ by ϕ_j and know the functions before decoding which might limit the space of AG codes. *the assumption on the shape/form of* $Q(y)$ *by* ϕ_j *was not justified. Whether if it is possible to reduce all AG codes to AG codes with fixed form of* $Q(y)$*, if it is not, the algorithm only works for a* ***subset*** *of AG codes and that should be stated at the beginning*

4. Other than that, the paper is on hard-decision decoding which has a fundamental limit on runtime and error bound in which soft-decision, probabilistic methods might edge over. *in 3.4 weighted curve lifting, the authors turned a soft-decision problem with integer weights into hard-decision problem, the authors made a remark that the large integer weights* $w_1, w_2, ..., w_n$ *should not be a problem and proposed to truncate and scale them down which is the same technique in many heuristic algorithm including Shannon code for channel coding problem. In Shannon code, the rounding of log probability was indeed a problem. And in the paper, this was addressed in a remark without any further explanation*

5. On the structure of this paper, the application part can be shorten as they are direct from the result of Reed-Solomon version, the weighted reconstruction and alternant codes can be combined with Reed-Solomon version since they are direct generalizations. At the beginning, the authors mentioned about order of singularity of curves, however, there were no apparent connection to the rest of the paper.

6. *for list decoding, probabilistic method can be applied in this scenario: at a distance* $t > \frac{d-1}{2}$*, a word* y *is decodable if and only if the ball centered at* y *with radius* t *denoted by* $B_y(t)$ *has only one codeword. For probabilistic method, we know the information (1. there is a codeword) before the information (2. the codeword is unique). If we know (2) at the beginning, the probabilistic method is better*