List Decoding RS:

① הקלט:

* $\{(x_i,y_i)\}_{i=1}^{n}$ - n נקודות מעל $\mathbb{F}^2$
* k - דרגת הפולינום המקודד
* t - מידת ההסכמה הדרושה.

② הבעיה:

למצוא את כל הפולינומים $p:\mathbb{F}\to\mathbb{F}$ עם מידת הסכמה $\geq t$ עם נקודות הקלט,

כלומר המקיימים $|\{i \mid p(x_i)=y_i\}| \geq t$.

③ האלגוריתם:

בשביל האלגוריתם - הגדרה:

יהי $Q:\mathbb{F}^2\to\mathbb{F}$ פולינום. נגדיר את הדרגה הממושקלת של מונום $q_{ij}x^iy^j$ להיות $i+kj$. הדרגה הממושקלת של Q תהיה $\max_{i,j}\{i+jk\}$.

<u>כשת האלגוריתם:</u>

(1) מצא פולינום $Q:\mathbb{F}^2\to\mathbb{F}$ כך ש:

(i) Q מדרגה ממושקלת $< m+\ell k$ (נראה את ערכי ℓ, m בהמשך).

(ii) לכל $1\le i\le n$: $Q(x_i,y_i)=0$.

(iii) Q <u>אינו</u> פולינום האפס.

(2) פרק את Q לגורמים בלתי-פריקים.

(3) אם p פולינום עם מידת הסכמה $\le t$ וגם $y-p|Q$, החזר את p.

④ <u>נכונות:</u>

(1)(i),(ii),(iii): כדי למצוא את Q, נפתור מערכת משוואות לינאריות הומוגנית.

* יש לנו n משוואות - אחת עבור כל נקודה, כי Q מתאפס
* המשוואות מהצורה $\sum_{j_2=0}^{\ell}\sum_{j_1=0}^{m+(\ell-j_2)k} q_{j_1j_2}x_i^{j_1}y_i^{j_2}=0$.

* ניתן לפתור בזמן פולינומיאלי אם יש פתרון (מס' המשתנים $> n$).

(2) בעיית Factoring - ניתן לפתור בזמן פולינומיאלי. לא ניכנס לפרטים.

(3) <u>טענה:</u> אם p פתרון ! - $t\ge m+\ell k$ אז $y-p|Q$.

<u>הוכחה:</u>

(1) <u>תזכורת מאלגברה לינארית:</u> יהי $p\in\mathbb{F}[x]$ פולינום מעל השדה $\mathbb{F}$ במשתנה x.
נניח כי קיים $a\in\mathbb{F}$ עבור $p(a)=0$. אז $x-a|p$.

הוכחה (1):

נבצע חלוקה של p ב- $x-a$ עם שארית (כמו חלוקת פולינומים). נקבל:

$$(*) \quad p(x)=(x-a)q(x)+r(x)$$

כאשר $\deg(r)<1$, כלומר $\deg(r)=0$ ולכן $r\equiv c$, עבור $c\in\mathbb{F}$.

נציב ב- $(*)$ $x=a$ ונקבל כי $c=0$:

$$p(a)=0\cdot q(a)+r(a) \Rightarrow 0=c$$

לכן $r\equiv 0$.

מכאן: $p(x)=(x-a)\cdot q(x)$.

(2) תזכורת נוספת (חוגים):

יהי R חוג קומוטטיבי. תזכורת: סגירות תחת כפל וחיבור, אסוציאטיביות, איבר יחידה ואיבר אפס.

נוכל להגדיר חוג פולינומים במשתנה y מעל החוג R ע"י $R[y]$. אלה כל הפולינומים עם מקדמים מהחוג R במשתנה y.

כעת מה יקרה אם נבחר $R=\mathbb{F}[x]$? המקדמים יהיו פולינומים במשתנה x.

(3) הוכחת הטענה:

יהא Q הפולינום שמצאנו, ונניח כי p הוא פתרון, כלומר ל-p יש מידת הסכמה $\geq t$ עם נקודות הקלט.

נתבונן בפולינום $g(x)\overset{\text{def}}{=}Q(x,p(x))$:

(א) g מתאפס ב- $\geq t$ נקודות (כי ל-p דרגת הסכמה t).

(ב) $t>m+\ell k$ כי כך בחרנו אותו.

(ג) הדרגה הממושקלת של g לא עולה על $d_x+k\cdot d_y\leq m+\ell k$.

לכן, g מתאפס ביותר נקודות מהדרגה שלו, ולכן $g\equiv 0$.

כעת נתבונן ב- $Q(x,y)$ כפולינום מעל $[\mathbb{F}[x]][y]$ (כאן $R=\mathbb{F}[x]$).

לפי טענה (1) נקבל שמכיוון ש- $Q(x,p)=0$ אז $y-p\,|\,Q$.

(5) סיבוכיות זמן ריצה:

(1) פתרון מערכת משוואות לינאריות - זמן פולי'.

(2) Factoring - זמן פולי'.

(3) הצגת הפלט - זמן פולי' (מספר הפתרונות חסום ע"י d_y).

(6) ערכי t,m,l:

נבחר: $l=\sqrt{\frac{2(n+1)}{k}}-1$, $m\geq\frac{k}{2}-1$

ואז האלגוריתם יעבוד עבור $t=\Omega(\sqrt{nk})$.