Projets de codes correcteurs

Julien Coolen

13 mars 2022

Table des matières

1 Décodage par syndrôme **1**
1.1 Algorithme de Prange 1
1.2 Algorithme de Lee-Brickell 3
1.3 Algorithme de Stern 6
1.4 Vérification empirique des complexités 7

2 Décodage en liste **8**

1 Décodage par syndrôme

1.1 Algorithme de Prange

Données : $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$, $\mathbf{s} \in \mathbb{F}_q^{n-k}$, $w \in [\![0, n]\!]$.
Résultat : $\mathbf{e} \in \mathbb{F}_q^n$ tel que $\mathbf{He}^T = \mathbf{s}$ et $|\mathbf{e}| \leq w$.
répéter
  Choisir $I \subseteq [\![1, n]\!]$ tel que $|I| = k$ et $J = [\![1, n]\!] \setminus I$
  si $\boldsymbol{H}_J$ *est inversible* **alors**
    $\mathbf{s}' \leftarrow \mathbf{H}_J^{-1}\mathbf{s}^T$
  fin
jusqu'à $|s'| \leq w$;
retourner $\boldsymbol{e}$ *tel que* $\boldsymbol{e}_I = \boldsymbol{0}$ *et* $\boldsymbol{e}_J = \boldsymbol{s}'^T$.

Algorithme 1 : Algorithme de Prange (1962) (type Las Vegas)

Preuve de l'algorithme de Prange. On a bien $|\mathbf{e}| = \underbrace{|\mathbf{e}_I|}_{=0} + |\mathbf{e}_J| \leq w$ car I et J sont disjoints.

De plus la sortie $\mathbf{e}$ de l'algorithme vérifie bien

$$\begin{aligned} \mathbf{He}^T &= \mathbf{H}(\mathbf{e}_I + \mathbf{e}_J)^T \\ &= \mathbf{H}_I\mathbf{e}_I^T + \mathbf{H}_J\mathbf{e}_J^T \\ &= \mathbf{0} + \mathbf{H}_J\mathbf{H}_J^{-1}\mathbf{s} \\ &= \mathbf{s}. \end{aligned}$$

Soit un code linéaire $[n,k]_q$ et $w \in [\![0, (1-\frac{1}{q})(n-k)]\!]$. La complexité de Prange est

$$T_{\text{Prange}} = O\left(\frac{\min\left\{\binom{n}{w}(q-1)^w, q^{n-k}\right\}}{\binom{n-k}{w}(q-1)^w}\right).$$

Démonstration. La probabilité de succès d'une itération de l'algorithme est dans le pire cas ($|\mathbf{e}| = w$) :

$$\mathbb{P}_{\text{succès}} \geq \frac{\binom{n-k}{w}(q-1)^w}{\binom{n}{w}(q-1)^w} \max\{1, |\text{DecSynd}(\mathbf{H}, \mathbf{s}, w)|\}$$

avec

$$|\text{DecSynd}(\mathbf{H}, \mathbf{s}, w)| = q^k \frac{\binom{n}{w}(q-1)^w}{q^n}.$$

D'où

$$\begin{aligned}
\mathbb{P}_{\text{succès}} &\geq \frac{\binom{n-k}{w}(q-1)^w}{\binom{n}{w}(q-1)^w} \max\left\{1, \frac{\binom{n}{w}(q-1)^w}{q^{n-k}}\right\} \\
&\geq \binom{n-k}{w}(q-1)^w \max\left\{\frac{1}{\binom{n}{w}(q-1)^w}, \frac{1}{q^{n-k}}\right\} \\
&\geq \binom{n-k}{w}(q-1)^w \frac{1}{\min\{\binom{n}{w}(q-1)^w, q^{n-k}\}}.
\end{aligned}$$

Le coût C d'une itération est dominé par le coût polynomial de l'élimination gaussienne sur $\mathbb{F}_q$: $C = n(n-k)^2 \log^2 q$. En effet, on effectue $n(n-k)$ opérations sur les colonnes, et une multiplication sur $\mathbb{F}_q$ requiert $O(\log^2 q)$ opérations en bits.

Bien que le coût d'une itération est dominé par les facteurs exponentiels, on doit le garder dans le grand O car c'est un facteur non constant (polynomial) :

$$\begin{aligned}
T_{Prange} &= O\Big(C \cdot \frac{1}{\mathbb{P}_{\text{succès}}}\Big) \\
&= O\left(\frac{n(n-k)^2(\log^2 q)\min\left\{\binom{n}{w}(q-1)^w, q^{n-k}\right\}}{\binom{n-k}{w}(q-1)^w}\right).
\end{aligned}$$

On pose $w = \lfloor \omega n \rfloor$. La complexité asymptotique de Prange est $\tilde{O}(q^{n\alpha})$ avec

$$\alpha := \min\left\{h_q(\omega), 1-R\right\} - (1-R)h_q\left(\frac{\omega}{1-R}\right).$$

Remarque. T_{Prange} est maximal lorsque $\binom{n}{w}(q-1)^w = q^{n-k}$ donc lorsque $w = d_{GV} := h_q^{-1}(1-R)$. En effet $\delta_{GV}(R) := d_{GV}/n = h_q^{-1}(1-R) + o(1)$ et $\binom{n}{d_{GV}}(q-1)^{d_{GV}} = O(q^{nh_q(d_{GV}/n)}) = O(q^{nh_q(h_q^{-1}(1-k/n))}) = O(q^{n-k})$.

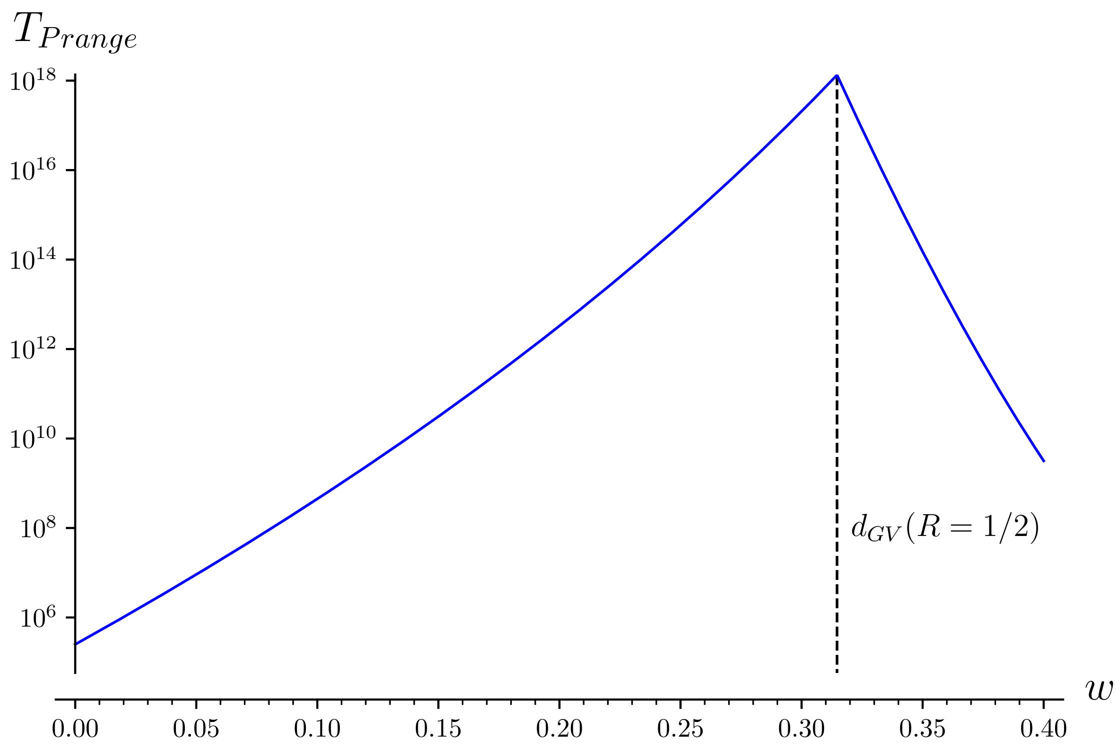

FIGURE 1 – Complexité asymptotique de Prange pour un rendement $R = \frac{1}{2}$. T_{Prange} est bien maximal pour la distance de Gilbert-Varshamov, la distance la plus difficile à décoder.

1.2 Algorithme de Lee-Brickell

L'idée est de relaxer la condition de Prange ($|\mathbf{e}_I| = 0$) pour amortir le coût de l'élimination gaussienne : on prend $p \geq 0$ petit et on l'on retourne un vecteur $\mathbf{e}$ tel que $|\mathbf{e}_I| = p$ et $|\mathbf{e}_J| \leq w - p$. Si $p = 0$ il s'agit exactement de l'algo de Prange.

Données : $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$, $\mathbf{s} \in \mathbb{F}_q^{n-k}$, $w \in [\![0, n]\!]$.
Résultat : $\mathbf{e} \in \mathbb{F}_q^n$ tel que $\mathbf{He}^T = \mathbf{s}$ et $|\mathbf{e}| \leq w$.

répéter
  Choisir un ensemble d'information $I \subseteq [\![1, n]\!]$, $|I| = k$, et son complémentaire J
  si $\boldsymbol{H}_J$ *est inversible* **alors**
    $\mathcal{L} \leftarrow \{\mathbf{H}_J^{-1}\mathbf{s} - \mathbf{H}_J^{-1}\mathbf{H}_I\mathbf{x}^T : |\mathbf{x}| = p\}$
  fin
jusqu'à $\exists \boldsymbol{y} \in \mathcal{L}, |\boldsymbol{y}| \leq w - p$;
retourner $\boldsymbol{e}$ *tel que* $\boldsymbol{e}_I = \boldsymbol{x}$ *et* $\boldsymbol{e}_J = \boldsymbol{y}^T$ *($\boldsymbol{y}$ obtenu à partir de $\boldsymbol{x}$, $\mathcal{L}$ est une table de hachage).*

Algorithme 2 : Algorithme de Lee-Brickell

Preuve de l'algorithme de Lee-Brickell. On a bien $|\mathbf{e}| = |\mathbf{e}_I| + |\mathbf{e}_J| \leq p + (w - p) \leq w$

car I et J sont disjoints. De plus la sortie $\mathbf{e}$ de l'algorithme vérifie bien

$$\begin{aligned}
\mathbf{He}^T &= \mathbf{H}(\mathbf{e}_I + \mathbf{e}_J)^T \\
&= \mathbf{H}_I\mathbf{x}^T + \mathbf{H}_J\mathbf{y} \\
&= \mathbf{H}_I\mathbf{x}^T + \mathbf{H}_J(\mathbf{H}_J^{-1}\mathbf{s} - \mathbf{H}_J^{-1}\mathbf{H}_I\mathbf{x}^T) \\
&= \mathbf{s}.
\end{aligned}$$

Le coût d'une itération est dominé par l'énumération $C = n(n-k)^2(\log^2 q) + \binom{k}{p}(q-1)^p = O(\binom{k}{p}(q-1)^p)$ et non plus par le pivot de Gauss.

La proba de succès est dans le pire cas ($|\mathbf{e}| = w$) :

$$\begin{aligned}
\mathbb{P}_{\text{succès}} &\geq \frac{\binom{n-k}{w-p}(q-1)^{w-p}\binom{k}{p}(q-1)^p}{\binom{n}{w}(q-1)^w} \max\{1, |\mathrm{DecSynd}(\mathbf{H}, \mathbf{s}, w)|\} \\
&\geq \frac{\binom{n-k}{w-p}\binom{k}{p}}{\binom{n}{w}} \max\{1, |\mathrm{DecSynd}(\mathbf{H}, \mathbf{s}, w)|\} \\
&\geq \frac{\binom{n-k}{w-p}\binom{k}{p}}{\binom{n}{w}} \max\{1, q^k \frac{\binom{n}{w}(q-1)^w}{q^n}\} \\
&\geq \binom{n-k}{w-p}\binom{k}{p} \max\{\frac{1}{\binom{n}{w}}, \frac{(q-1)^w}{q^{n-k}}\} \\
&\geq \binom{n-k}{w-p}\binom{k}{p} \frac{1}{\min\{\binom{n}{w}, \frac{q^{n-k}}{(q-1)^w}\}} \\
&\geq \binom{n-k}{w-p}\binom{k}{p} \frac{(q-1)^w}{\min\{\binom{n}{w}(q-1)^w, q^{n-k}\}}.
\end{aligned}$$

On ne gagne jamais plus qu'un facteur polynomial sur Prange (le coût du pivot) :

$$\begin{aligned}
T_{LB} &= C \cdot \frac{1}{\mathbb{P}_{\text{succès}}} \\
&= \left(n(n-k)^2(\log^2 q) + \binom{k}{p}(q-1)^p\right) \frac{\min\{\binom{n}{w}(q-1)^w, q^{n-k}\}}{\binom{n-k}{w-p}\binom{k}{p}(q-1)^w} \\
&= \left(\frac{n(n-k)^2(\log^2 q)}{\binom{k}{p}} + (q-1)^p\right) \frac{\min\{\binom{n}{w}(q-1)^w, q^{n-k}\}}{\binom{n-k}{w-p}(q-1)^w} \\
&\geq \frac{\min\{\binom{n}{w}(q-1)^w, q^{n-k}\}}{\binom{n-k}{w-p}(q-1)^w} \\
&\geq \frac{\min\{\binom{n}{w}(q-1)^w, q^{n-k}\}}{\binom{n-k}{w}(q-1)^w} \\
&\geq \frac{1}{n(n-k)^2(\log^2 q)} T_{Prange}.
\end{aligned}$$

La complexité de Lee-Brickell est donc (pivot dominé par l'énumération), pour $w = \lfloor \omega n \rfloor$ et $\rho = \lfloor \frac{p}{n} \rfloor$:

$$O\left(\frac{\min\{\binom{n}{w}(q-1)^w, q^{n-k}\}}{\binom{n-k}{w-p}(q-1)^{w-p}}\right).$$

La complexité asymptotique de Lee-Brickell est $\tilde{O}(q^{n\alpha})$ pour

$$\alpha := \min\{h_q(\omega), 1-R\} - (1-R)h_q\left(\frac{\omega-\rho}{1-R}\right).$$

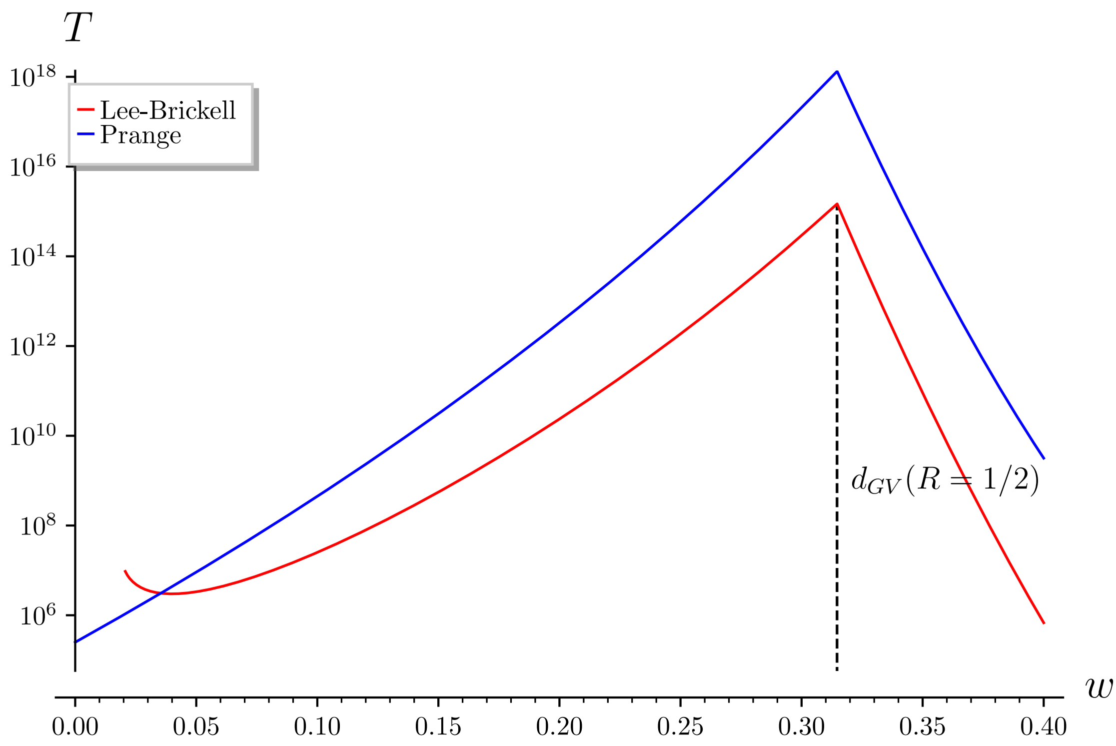

FIGURE 2 – Complexité asymptotique de Lee-Brickell pour un rendement $R = \frac{1}{2}$ et $p = 2$. La distance de Gilbert-Varshamov est la plus difficile à décoder. On observe bien le gain d'un facteur polynomial $O(n^3)$ avec l'échelle logarithmique : pour de petites valeurs de w l'amélioration se dégrade.

Quelle est la valeur optimale de p ?

On suppose que $R = \frac{1}{2}$ et n très grand constant. Étudions les variations de la fonction

$$f(w) = \frac{1}{2}h_q\left(\frac{2(w-p)}{n}\right).$$

Sauf pour w très petit ou très grand, $p = 2$ est optimal.

1.3 Algorithme de Stern

L'idée est de combiner Lee-Brickell et le décodage par paradoxe des anniversaires. On effectue une élimination gaussienne partielle.

Décodage par le paradoxe des anniversaires : Problème : trouver au plus w colonnes de $\mathbf{H}$ dont la somme vaut $\mathbf{s}$ sur $\mathbb{F}_q$.

Solution : scinder $\mathbf{H}$ en deux parties égales et énumérer les deux ensembles

$$\mathcal{L}_1 = \{\mathbf{s} - \mathbf{H}_1\mathbf{e}_1^T : wt(\mathbf{e}_1) = \frac{w}{2}\}$$

et

$$\mathcal{L}_2 = \{\mathbf{H}_2\mathbf{e}_2^T : wt(\mathbf{e}_2) = \frac{w}{2}\}.$$

Si $\mathcal{L}_1 \cap \mathcal{L}_2 \neq \emptyset$, on a des solutions $\mathbf{s} - \mathbf{H}\mathbf{e}_1^T - \mathbf{H}_2\mathbf{e}_2^T = \mathbf{0}$.

Données : $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times n}$, $\mathbf{s} \in \mathbb{F}_q^{n-k}$, $w \in [\![0, n]\!]$.
Résultat : $\mathbf{e}_{\in}\mathbb{F}_q^n$ tel que $\mathbf{H}\mathbf{e}^T = \mathbf{s}$ et $|\mathbf{e}| \leq w$.

$X = \{\mathbf{x} \in \mathbb{F}_q^{k/2} : |\mathbf{x}| = \frac{p}{2}\}$
répéter
  Choisir un ensemble d'information $I \subseteq [\![1, n]\!]$, $|I| = k$, et son complémentaire J
  si $\boldsymbol{H}_J$ *est inversible* **alors**
    $\bar{\mathrm{s}} \leftarrow \mathbf{H}_J^{-1}\mathbf{s}$
    $\bar{\mathbf{A}} \leftarrow \mathbf{H}_J^{-1}\mathbf{H}_I$
    On extrait les deux sous-matrices $\bar{\mathbf{A}} = [\bar{\mathbf{A}}_1\bar{\mathbf{A}}_2]$
    $\mathcal{L}_1 \leftarrow \{(\mathbf{x}, \bar{\mathrm{s}} - \bar{\mathbf{A}}_1\mathbf{x}^T) : \mathbf{x} \in X\}$
    $\mathcal{L}_2 \leftarrow \{(\mathbf{x}, \bar{\mathbf{A}}_2\mathbf{x}^T) : \mathbf{x} \in X\}$
    Choisir un ensemble L de l positions
  fin
jusqu'à $\exists(\boldsymbol{x}_1, \boldsymbol{y}), (\boldsymbol{x}_2, \boldsymbol{y}) \in \mathcal{L}_1 \cap \mathcal{L}_2, |\boldsymbol{y}_{[\![1,n]\!]\setminus L}| \leq w - p$;
retourner $\boldsymbol{e}$ *tel que* $\boldsymbol{e}_I = \boldsymbol{x}$ *et* $\boldsymbol{e}_J = \boldsymbol{y}^T$ *(*$\boldsymbol{y}$ *obtenu à partir de* $\boldsymbol{x}$*,* $\mathcal{L}$ *est une table de hachage).*

Algorithme 3 : Algorithme de Stern

L'algorithme est correct, et la preuve est analogue à celle de Lee-Brickell (même calcul avec $\mathbf{e}_I = \mathbf{x}_1 + \mathbf{x}_2$).

On se place dans le pire des cas ($|\mathbf{e}| = w$). Une solution est trouvée à la fin d'une itération si $\mathbf{e}_i$ est de poids p (événement E_1), que de plus le poids de $\mathbf{e}_i$ soit distribué de manière égale en $\mathbf{x}_1$ et $\mathbf{x}_2$ (événement E_2), et enfin que l positions de $\mathbf{e}_j$ de poids $w - p$ soient nulles (événement E_3).

On obtient, les événements étant indépendants :

$$
\begin{aligned}
\mathbb{P}_{\text{succès}} &\geq P(E_1 \wedge E_2 \wedge E_3) \\
&\geq \mathbb{P}(E_1)\mathbb{P}(E_2)\mathbb{P}(E_3) \\
&\geq \frac{\binom{k}{p}\binom{n-k}{w-p}}{\binom{n}{w}} \frac{\binom{k/2}{p/2}^2}{\binom{k}{p}} \frac{\binom{n-k-(w-p)}{l}}{\binom{n-k}{l}} \quad \text{car les puissances de } (q-1) \text{ se simplifient} \\
&\geq \frac{\binom{k/2}{p/2}^2 \binom{n-k-l}{w-p}}{\binom{n}{w}} \quad \text{car } \frac{\binom{n-k}{w-p}\binom{n-k-(w-p)}{l}}{\binom{n-k}{l}} = \binom{n-k-l}{w-p} \text{ en explicitant les factorielles.}
\end{aligned}
$$

Le coût d'une itération est dominé par la recherche de collision et les multiplications de matrices : $C = \binom{k/2}{p/2}(q-1)^{p/2}(k/2)^3$.

On obtient donc comme complexité temporelle

$$
\begin{aligned}
T_{Stern} &= C \cdot \frac{1}{P_{Stern}} \\
&= \binom{k/2}{p/2}(q-1)^{p/2}(k/2)^3 \frac{\binom{n}{w}(q-1)^w}{\binom{k/2}{p/2}^2 (q-1)^p \binom{n-k-l}{w-p}(q-1)^{w-p}} \\
&= O\Big(k^3 \frac{\binom{n}{w}(q-1)^w}{\binom{k/2}{p/2}(q-1)^{p/2}\binom{n-k-l}{w-p}(q-1)^{w-p}}\Big).
\end{aligned}
$$

Sa complexité asymptotique est, pour $w = \lfloor \omega n \rfloor, p = \lfloor \rho n \rfloor, l = \lfloor \lambda n \rfloor$, $\tilde{O}(q^{n\alpha})$ avec

$$
\alpha := h_q(\omega) - \frac{R}{2} h_q(\frac{\rho}{R}) - (1-R-\lambda) h_q(\frac{\omega-\rho}{1-R-\lambda}).
$$

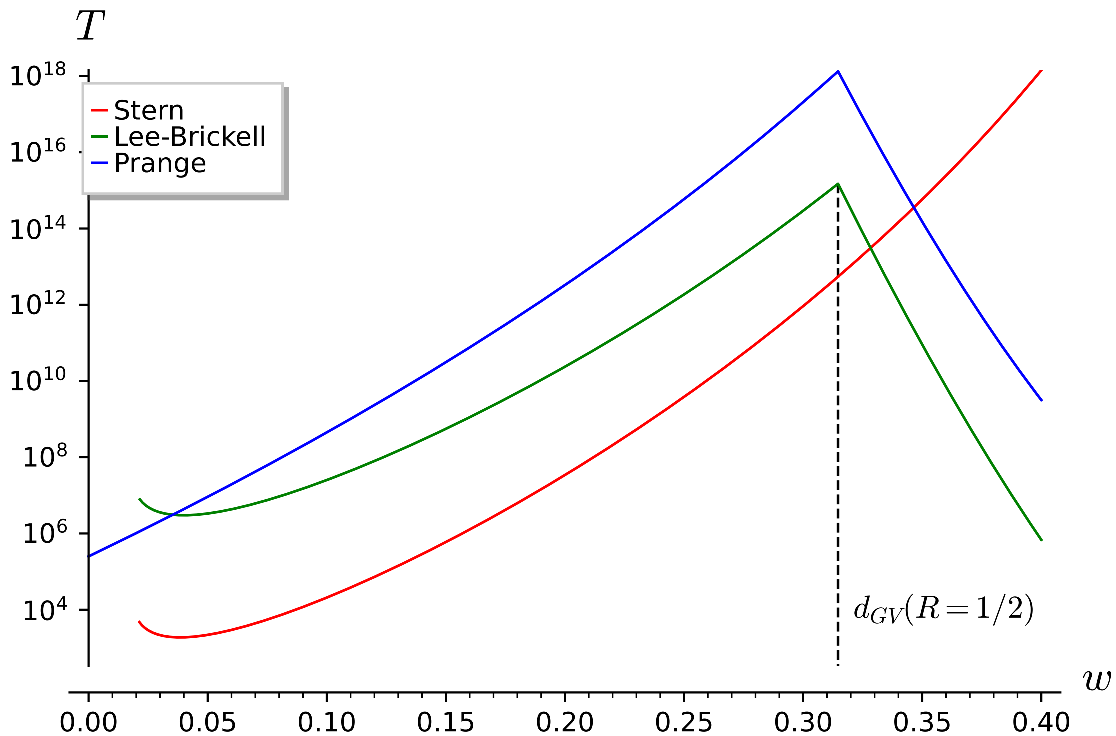

FIGURE 3 – Complexité asymptotique de Stern pour un rendement $R = \frac{1}{2}$.

2 Décodage en liste