

Projets de codes correcteurs

Julien Coolen

20 avril 2022

Table des matières

1	Décodage par syndrome	1
1.1	Algorithme de Prange	1
1.2	Algorithme de Lee-Brickell	4
1.3	Algorithme de Stern	6
2	Décodage en liste	9
3	Décodage des codes LDPC	9

1 Décodage par syndrome

1.1 Algorithme de Prange

Données : $H \in \mathbb{F}_q^{(n-k) \times n}$, $s \in \mathbb{F}_q^{n-k}$, $w \in \llbracket 0, n \rrbracket$.

Résultat : $e \in \mathbb{F}_q^n$ tel que $He^T = s$ et $|e| \leq w$.

```
1 répéter
2   Choisir  $I \subseteq \llbracket 1, n \rrbracket$  tel que  $|I| = k$  et  $J = \llbracket 1, n \rrbracket \setminus I$ 
3   si  $H_J$  est inversible alors
4      $s' \leftarrow H_J^{-1} s^T$ 
5   fin
6 jusqu'à  $|s'| \leq w$ ;
7 retourner  $e$  tel que  $e_I = 0$  et  $e_J = s'^T$ .
```

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

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

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

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

□

Soit un code linéaire $[n, k]_q$ et $w \in \llbracket 0, (1 - \frac{1}{q})(n - k) \rrbracket$. 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) :

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

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

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

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 $\binom{n}{d_{GV}}(q - 1)^{d_{GV}} = O(q^{nh_q(d_{GV}/n)}) = O(q^{nh_q(h_q^{-1}(1 - k/n))}) = O(q^{n-k})$.

La complexité de cet algo de décodage par ensemble d'information est donc exponentielle en le nombre d'erreurs w du mot à décoder si l'on cherche une solution particulière. Et pour w fixé, il faut n grand pour obtenir une complexité (= borne supérieure sur la sécurité) de l'ordre de 2^{100} (donc la taille des clés = longueur des lignes de la matrice de parité = longueur des colonnes de la matrice génératrice du code augmente exponentiellement).

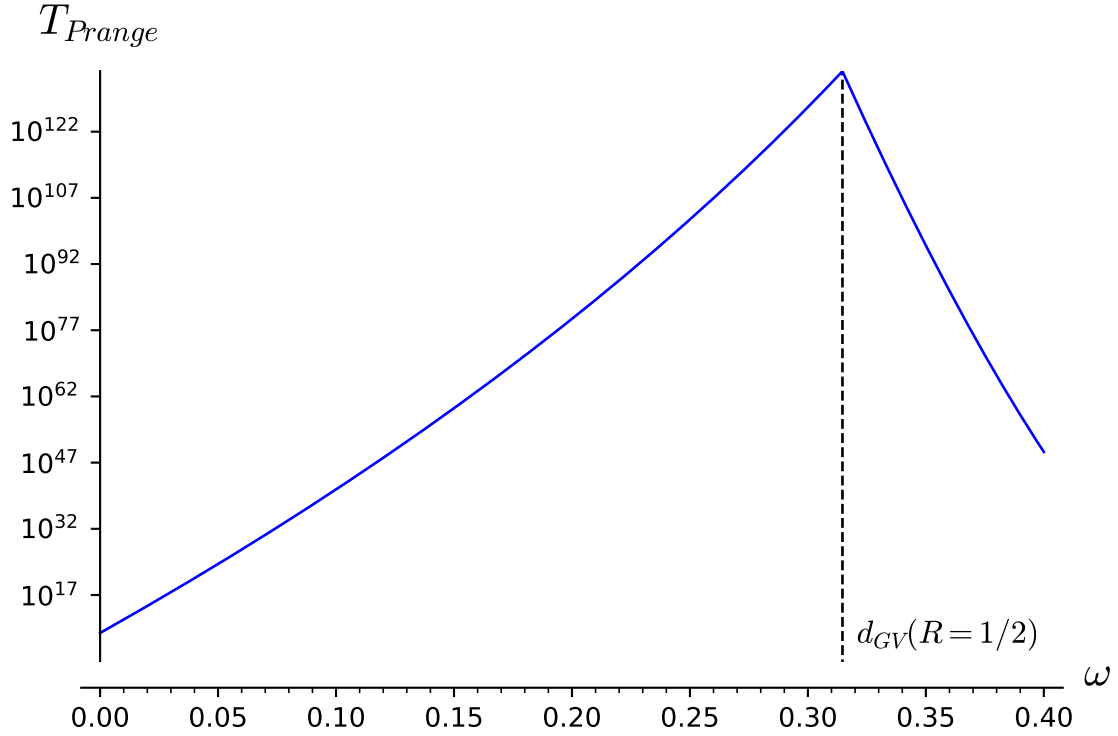


FIGURE 1 – Complexité asymptotique de Prange pour un rendement $R = \frac{1}{2}$. T_{Prange} est bien maximal pour la distance de Gilbert-Varshamov, la distance la plus difficile à décoder.

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 : $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$, $\mathbf{s} \in \mathbb{F}_q^{n-k}$, $w \in \llbracket 0, n \rrbracket$.

Résultat : $\mathbf{e} \in \mathbb{F}_q^n$ tel que $\mathbf{H}\mathbf{e}^T = \mathbf{s}$ et $|\mathbf{e}| \leq w$.

```

1  $X = \{\mathbf{x} \in \mathbb{F}_q^k : |\mathbf{x}| = p\}$ 
2  $\mathcal{L}$  est une table de hachage, indexée par des éléments de  $\mathbb{F}_q^{n-k}$ 
3 répéter
4   Choisir un ensemble d'information  $I \subseteq \llbracket 1, n \rrbracket$ ,  $|I| = k$ , et son complémentaire  $J$ 
5   pour tous les  $\mathbf{x} \in X$  faire
6     si  $\mathbf{H}_J$  est inversible alors
7        $\mathcal{L}[\mathbf{H}_J^{-1}\mathbf{s} - \mathbf{H}_J^{-1}\mathbf{H}_I\mathbf{x}^T] \leftarrow \mathbf{x}$ 
8     fin
9   fin
10 jusqu'à  $\exists(\mathbf{y}, \mathbf{x}) \in \mathcal{L}, |\mathbf{y}| \leq w - p$ ;
11 retourner  $\mathbf{e}$  tel que  $\mathbf{e}_I = \mathbf{x}$  et  $\mathbf{e}_J = \mathbf{y}^T$  ( $\mathbf{y}$  clé obtenue à partir de  $\mathbf{x}$ ).
```

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

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

□

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 ($|\mathbf{e}| = w$) :

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

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

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

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

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

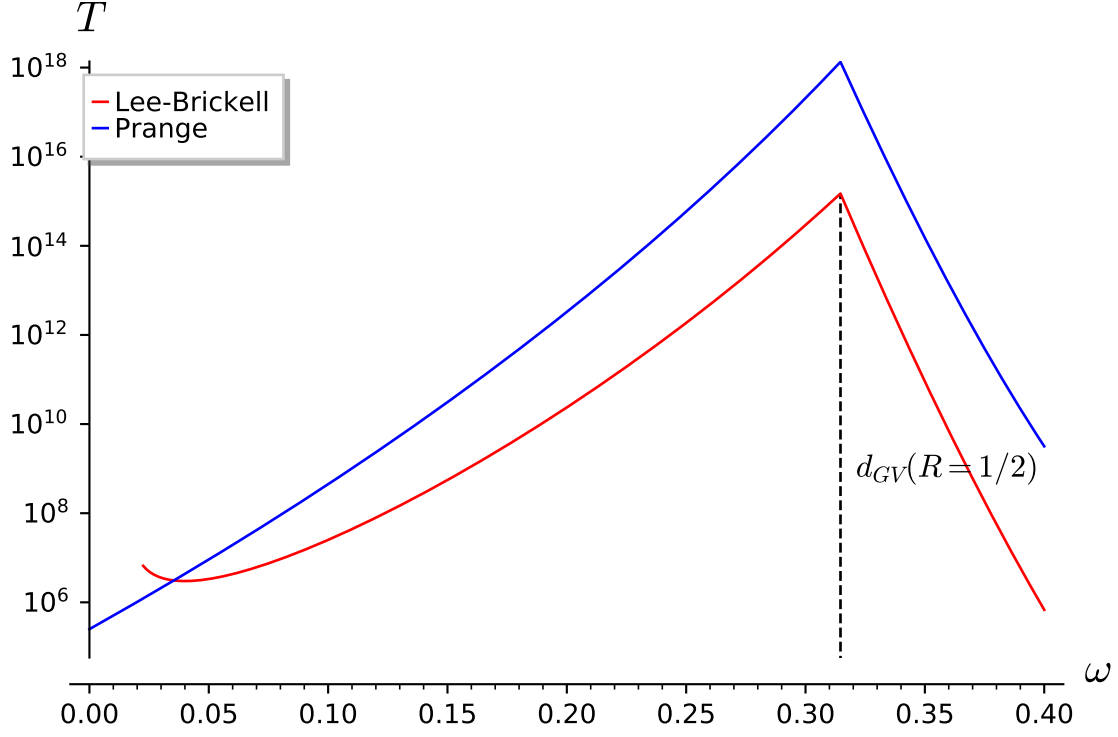


FIGURE 2 – Complexité asymptotique de Lee-Brickell pour un rendement $R = \frac{1}{2}$ et $p = 2$.
La distance de Gilbert-Varshamov est la plus difficile à décoder.

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, et $q = 2$, $p = 2$ 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 $\mathbf{s} - \mathbf{H} \mathbf{e}_1^T - \mathbf{H}_2 \mathbf{e}_2^T = 0$.

Données : $\mathbf{H} \in \mathbb{F}_q^{(n-k) \times n}$, $\mathbf{s} \in \mathbb{F}_q^{n-k}$, $w \in \llbracket 0, n \rrbracket$.

Résultat : $\mathbf{e} \in \mathbb{F}_q^n$ tel que $\mathbf{H} \mathbf{e}^T = \mathbf{s}$ et $|\mathbf{e}| \leq w$.

```

1  $X = \{\mathbf{x} \in \mathbb{F}_q^{k/2} : |\mathbf{x}| = \frac{p}{2}\}$ 
2  $\mathcal{L}_1, \mathcal{L}_2$  des tables de hachage, indexées par des éléments de  $\mathbb{F}_q^{n-k}$ 
3 répéter
4   Choisir un ensemble d'information  $I \subseteq \llbracket 1, n \rrbracket$ ,  $|I| = k$ , et son complémentaire  $J$ 
5   si  $\mathbf{H}_J$  est inversible alors
6      $\bar{\mathbf{s}} \leftarrow \mathbf{H}_J^{-1} \mathbf{s}$ 
7      $\bar{\mathbf{P}} \leftarrow \mathbf{H}_J^{-1} \mathbf{H}_I$ 
8     On extrait les deux sous-matrices  $\bar{\mathbf{P}} = [\bar{\mathbf{P}}_1 \bar{\mathbf{P}}_2]$ 
9     pour tous les  $\mathbf{x} \in X$  faire
10       $\mathcal{L}_1[\bar{\mathbf{s}} - \bar{\mathbf{P}}_1 \mathbf{x}^T] \leftarrow \mathbf{x}$ 
11       $\mathcal{L}_2[\bar{\mathbf{P}}_2 \mathbf{x}^T] \leftarrow \mathbf{x}$ 
12     fin
13   Choisir un ensemble  $L$  de  $l$  positions
14   fin
15 jusqu'à  $\exists (\mathbf{y}, \mathbf{x}_1), (\mathbf{y}, \mathbf{x}_2) \in \mathcal{L}_1 \times \mathcal{L}_2, |\mathbf{y}_{\llbracket 1, n \rrbracket \setminus L}| \leq w - p$ ;
16 retourner  $\mathbf{e}$  tel que  $\mathbf{e}_I = \mathbf{x}$  et  $\mathbf{e}_J = \mathbf{y}^T$  (pour une clé  $\mathbf{y}$  obtenu à partir de  $\mathbf{x}$ ,  $\mathcal{L}$  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}_J 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 que la probabilité de trouver une solution spécifique est, les événements étant indépendants :

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

Donc la probabilité de trouver n'importe quelle solution est

$$\begin{aligned}
\mathbb{P}_{\text{succès}} &\geq \frac{\left(\frac{k}{p/2}\right)^2 \binom{n-k-l}{w-p}}{\binom{n}{w}} \max\{1, |\text{DecSynd}(\mathbf{H}, \mathbf{s}, w)|\} \\
&\geq \frac{\left(\frac{k}{p/2}\right)^2 \binom{n-k-l}{w-p}}{\binom{n}{w} \min\{1, \frac{q^{n-k}}{\binom{n}{w}(q-1)^w}\}}.
\end{aligned}$$

Le coût d'une itération est dominé par la recherche de collision (parcours des clés d'une des listes \mathcal{L}_1 , linéaire en la taille de \mathcal{L}_1) et les multiplications de matrices : $C = \binom{k/2}{p/2}(q-1)^{p/2}(k/2)^3$. Il faut aussi ajouter la probabilité d'obtenir une collision.

On obtient donc comme complexité temporelle

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

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

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

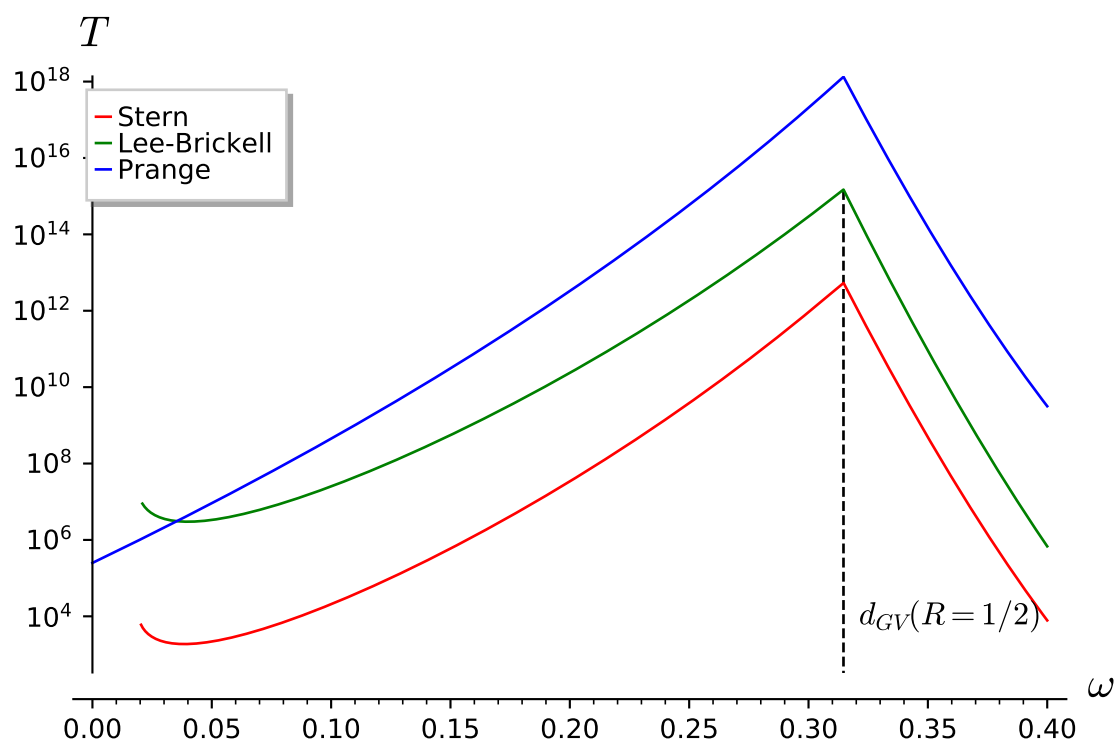


FIGURE 3 – Complexité asymptotique de Stern pour un rendement $R = \frac{1}{2}$.

2 Décodage en liste

3 Décodage des codes LDPC

Les produits de probas deviennent des sommes de LLR. Sur de petit processeurs (typiquement pour l'embarqué), les multiplications sont coûteuses, donc une version de belief propagation avec des additions est plus rapide.