

Réseaux, information et communications (INFO-F303)

Partie Théorie de l'Information

9. Conclusion

Christophe Petit

Université libre de Bruxelles

Plan du cours

1. Notion de code
2. Source aléatoire et codes efficaces
3. Entropie et codage efficace
4. Compression sans perte
5. Canal bruité
6. Codes correcteurs d'erreurs
7. Codes linéaires
8. Quelques familles de codes linéaires
- A. Rappels mathématiques (chapitre 7.1 du syllabus)

Théorie des codes

- ▶ Shannon : *“il existe un code qui transmet sans erreur sur un canal bruité, tant que le débit du code est inférieur à la capacité du canal”*
- ▶ Théorème d'existence, preuve non constructive
- ▶ En pratique, on souhaite des codes avec bon débit et capacité de correction, et des fonctions d'encodage et de décodage efficaces

Rappel : contraintes connues

- ▶ Second théorème de Shannon : $k/n \leq C_p$
- ▶ Borne de Singleton : $d \leq n - k + 1$
- ▶ Borne de Hamming : $B_s \leq q^{n-k}$ avec $s = \left\lfloor \frac{d-1}{2} \right\rfloor$
- ▶ Borne de Gilbert-Varshamov : $B_{d-1} \geq q^{n-k}$

Codes approchant la capacité maximale

- ▶ Pour canal bruité donné, par exemple un canal symétrique de paramètres p et r , on veut un code $[n, k, d]$ avec
 - ▶ Grande capacité de détection et correction d'erreurs (asymptotiquement on veut $d \geq 2pn$)
 - ▶ Haut débit k/n (approchant la capacité du canal)
 - ▶ Algorithmes rapides de détection et correction

Au-delà du cours

- ▶ Preuve de Shannon utilise un code aléatoire
- ▶ Codes algébriques très structurés ; pas aléatoires
- ▶ Hard vs soft decoding : plutôt que de choisir le mot de code le plus probable, garder une liste de mots potentiels avec les probabilités associées
- ▶ Autres modèles d'erreurs, par exemple erreurs en blocs
- ▶ Autres bornes existantes
- ▶ Codes géométriques

Familles “récentes”

Turbo codes (Berrou 1993) Notion de **décodage itératif**, combinant une paire de codes convolutifs. Premiers codes à approcher la capacité de Shannon en pratique.

Codes LDPC (Gallager 1963, redécouverts en 1996) Décodage itératif dans un **graphe de Tanner épars**.

Codes polaires (Arikan, 2009) Première famille de codes avec une construction explicite à atteindre la capacité d'un canal binaire symétrique avec une dépendance polynomiale en fonction de l'écart à la capacité, et encodage et décodage en temps $O(n \log n)$.

Questions ?

?

Crédits et remerciements

- ▶ Mes transparents suivent fortement les notes de cours développées par le Professeur Yves Roggeman pour le cours INFO-F303 à l'Université libre de Bruxelles
- ▶ Une partie des transparents et des exercices ont été repris ou adaptés des transparents développés par le Professeur Jean Cardinal pour ce même cours
- ▶ Je remercie chaleureusement Yves et Jean pour la mise à disposition de ce matériel pédagogique, et de manière plus large pour toute l'aide apportée pour la reprise de ce cours
- ▶ Les typos et erreurs sont exclusivement miennes (merci de les signaler !)