Une introduction au codage de réseau aléatoire
Correction d'erreurs dans le codage de réseau

Christine Bachoc

Université Bordeaux I, IMB

École de printemps Codage et Cryptographie
17 - 21 Mars 2014, Université Joseph Fourier, Grenoble

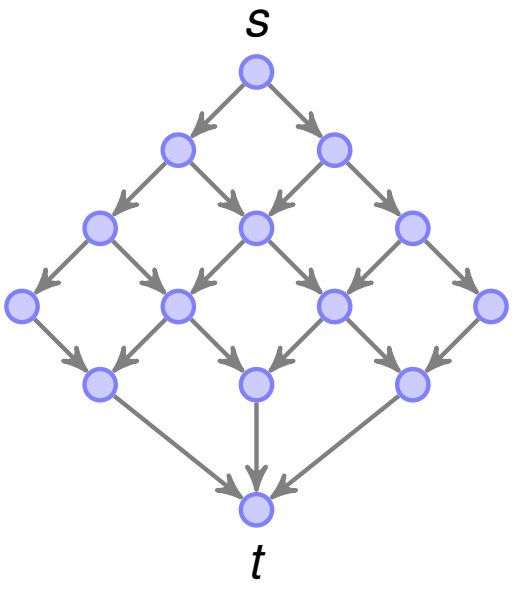
Erreurs

- Le réseau transmet des éléments (paquets) de $\mathbb{F}_q^m$.
- Une insertion d'erreur à l'arête e est modélisée par l'ajout d'un paquet E_e:

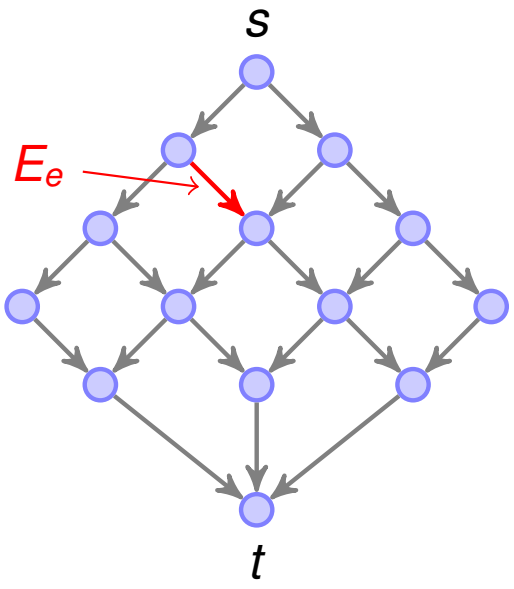
$$x'_e = x_e + E_e$$

- Un effacement à l'arête e est la perte de la valeur de x_e.
- On suppose le codage linéaire aléatoire.
- Problème: la propagation des erreurs au cours du codage.

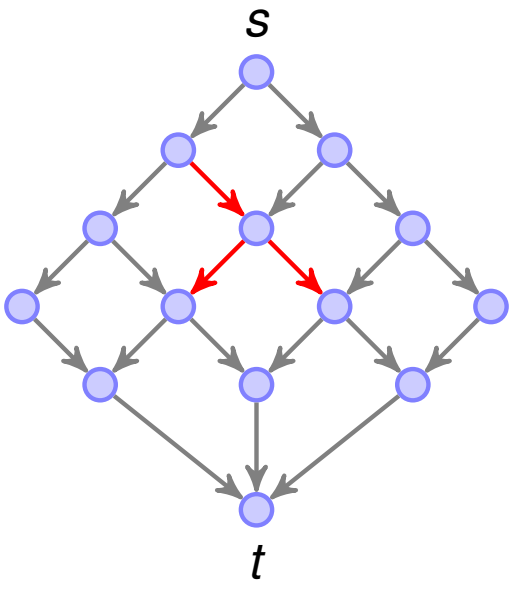
Propagation des erreurs



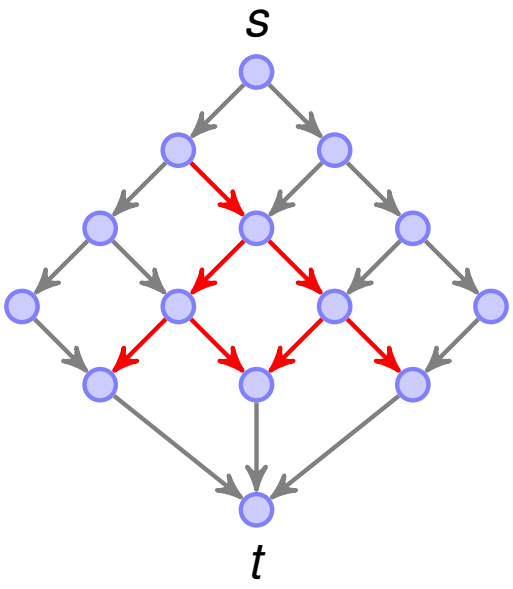
Propagation des erreurs



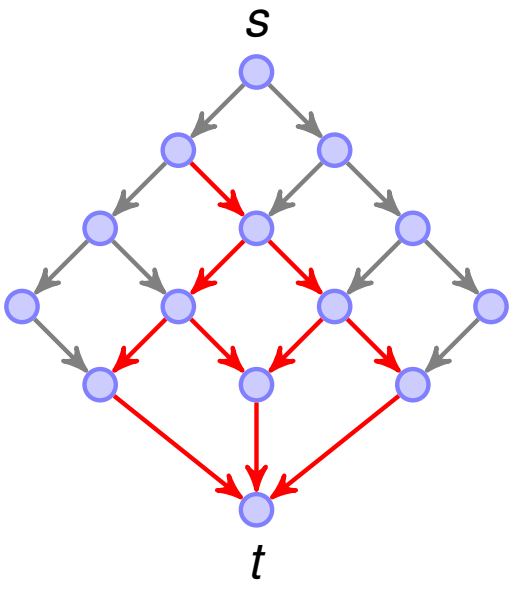
Propagation des erreurs



Propagation des erreurs



Propagation des erreurs



Erreurs

- Si $X \in \mathbb{F}_q^{n \times m}$ est envoyé par la source et Y reçu à destination, en présence d'erreurs on a:

$$Y = TX + UE$$

- Kschischang, Koetter, 2008: proposent de modéliser l'information transmise par un sous-espace vectoriel V de $\mathbb{F}_q^m$. Si une base de V est injectée dans le réseau, le codage linéaire préserve la propriété d'appartenance: les paquets transmis au destinataire appartiennent à V.
- Avantage: en cas d'erreur, on peut espérer que V sera modifié en V' un sev 'proche' de V au sens d'une métrique raisonnable.
- Alors, on peut appliquer les principes des codes correcteurs d'erreurs: sélectionner un ensemble de sev (code) suceptibles d'être transmis, et appliquer à la réception un décodage par l'élément du code le plus proche.
- Autre avantage: on n'a pas besoin de connaitre la topologie du réseau (cas non cohérent).

Distances entre sous-espaces

- Subspace distance d_S [Koetter Kschischang 2008]:

$$d_S(U,V) = \dim(U+V) - \dim(U \cap V) = \dim(U) + \dim(V) - 2\dim(U \cap V)$$

- C'est la distance du plus court chemin dans le graphe dont les sommets sont les sous-espaces de $\mathbb{F}_q^m$ et les arêtes relient U, V si $U \subset V$ et $\dim(V) = \dim(U) + 1$.
- Injection distance d [Kschischang Silva 2008]:

$$d(U,V) = \max(\dim(U), \dim(V)) - \dim(U \cap V)$$

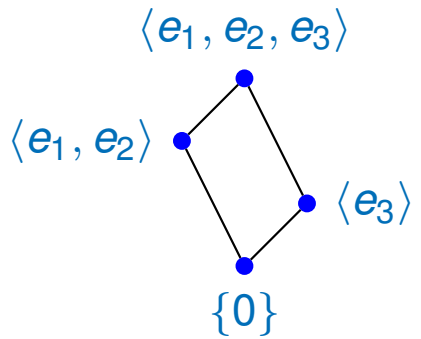
- $d(U,V)$ mesure le plus petit nombre d'erreurs insérées nécessaires pour transformer une base de U en une base de V.

Distances entre sous-espaces

- Comparaison:

$$d_S(U,V)/2 \leq d(U,V) \leq d_S(U,V).$$

- Égalité à gauche si $\dim(U) = \dim(V)$.
- Exemple: $\{e_1, e_2, e_3\}$ la base canonique de $\mathbb{F}_q^3$. $U = \langle e_1, e_2 \rangle$, $V = \langle e_3 \rangle$.



$d_S(U,V) = 3$, $d(U,V) = 2$.
$d_S(U,V)/2 < d(U,V) < d_S(U,V)$.

$$\{e_1, e_2\} \to \{e_1 + (e_3 - e_1), e_2\} \to \{e_3, e_2 + (e_3 - e_2)\} \to \{e_3, e_3\}$$

Correction d'erreurs

- $\mathcal{P}_q(m)$ l'ensemble des sous-espaces vectoriels de $\mathbb{F}_q^m$
- $\mathcal{C} \subset \mathcal{P}_q(m)$
- $d(\mathcal{C})$ la distance minimale du code $\mathcal{C}$:

$$d(\mathcal{C}) = \min\{d(U, V) \ : \ U \in \mathcal{C}, \ V \in \mathcal{C}, \ U \neq V\}.$$

- ρ le nombre d'effacements, t le nombre d'insertions d'erreurs.

Théorème: [Kschischang Silva 2008] Le décodage par l'élément du code le plus proche corrige correctement ρ effacements et t insertions en position quelconque ssi

$$d(\mathcal{C}) > 2t + \rho.$$

Relèvements de matrices

- Soit $M \in \mathbb{F}_q^{k \times m}$. On associe à M le sous-espace vectoriel $\Lambda(M)$ engendré par les lignes de la matrice $[I_k \; M]$:

$$\Lambda(M) := \left\langle \begin{bmatrix} I_k & M \end{bmatrix} \right\rangle$$

- Soit $\mathcal{G}_q(n,k)$ l'ensemble des sous-espaces vectoriels de $\mathbb{F}_q^n$ de dimension k (espace Grassmannien). On a

$$\Lambda(M) \in \mathcal{G}_q(m+k,k).$$

- Soit $\mathcal{C} \subset \mathbb{F}_q^{k \times m}$, on note

$$\Lambda(\mathcal{C}) := \{\Lambda(M) \; : \; M \in \mathcal{C}\}.$$

Métrique rang

- L'espace $\mathbb{F}_q^{k\times m}$ est naturellement muni de la métrique rang:

$$d_R(M,N) = \text{rang}(M-N).$$

- On a :

$$d(\Lambda(M),\Lambda(N)) = \text{rang}(M-N) = d_R(M,N).$$

- Preuve:

$$\begin{aligned} d(\Lambda(M),\Lambda(N)) &= \dim(\Lambda(M)+\Lambda(N)) - \min(\dim(\Lambda(M)),\dim(\Lambda(N))) \\ &= \dim\left\langle \begin{bmatrix} I_k & M \\ I_k & N \end{bmatrix} \right\rangle - k \\ &= \dim\left\langle \begin{bmatrix} I_k & M \\ 0 & N-M \end{bmatrix} \right\rangle - k \\ &= (k + \text{rang}(N-M)) - k = d_R(M,N). \end{aligned}$$

Espaces de Delsarte

- Les espaces: $\mathcal{G}_q(n,k)$ et $\mathbb{F}_q^{k\times n}$ sont des espaces de Delsarte au même titre que l'espace de Hamming et l'espace de Johnson binaire.
- Delsarte 1973: cadre uniforme des schémas d'association *P*-*Q* polynomiaux pour les codes, anticodes, formule de Mac Williams, méthode de programmation linéaire, etc..
- Delsarte 1978: étude spécifique des espaces $\mathcal{G}_q(n,k)$ (comme q-analogue du Johnson binaire) et $\mathbb{F}_q^{k\times n}$ (en particulier construction des 'codes de Gabidulin').
- Point de vue théorie des groupes: ce sont des espaces 2-point homogènes pour l'action d'un groupe G. Leurs polynômes orthogonaux sont leurs fonctions zonales sphériques.

Space	Group	Polynomial
Hamming space $\mathbf{q}^n$	$S_q \wr S_n$	Krawtchouk
Johnson space	S_n	Hahn
q-Johnson space	$\mathrm{Gl}_n(\mathbb{F}_q)$	q-Hahn
Maximal totally isotropic subspaces of dimension k, for a nonsingular bilinear form:		
Symmetric	$\mathrm{SO}_{2k+1}(\mathbb{F}_q)$	q-Krawtchouk
	$\mathrm{SO}_{2k}(\mathbb{F}_q)$	q-Krawtchouk
	$\mathrm{SO}^-_{2k+2}(\mathbb{F}_q)$	q-Krawtchouk
Symplectic	$\mathrm{Sp}_{2k}(\mathbb{F}_q)$	q-Krawtchouk
Hermitian	$\mathrm{SU}_{2k}(\mathbb{F}_{q^2})$	q-Krawtchouk
	$\mathrm{SU}_{2k+1}(\mathbb{F}_{q^2})$	q-Krawtchouk
Spaces of matrices:		
$\mathbb{F}_q^{k\times n}$	$\mathbb{F}_q^{k\times n}.(\mathrm{Gl}_k(\mathbb{F}_q) \times \mathrm{Gl}_n(\mathbb{F}_q))$	Affine q-Krawtchouk
$\mathrm{Skew}_n(\mathbb{F}_q)$	$\mathrm{Skew}_n(\mathbb{F}_q).\,\mathrm{Gl}_n(\mathbb{F}_q)$	Affine q-Krawtchouk
$\mathrm{Herm}_n(\mathbb{F}_{q^2})$	$\mathrm{Herm}_n(\mathbb{F}_{q^2}).\,\mathrm{Gl}_n(\mathbb{F}_{q^2})$	Affine q-Krawtchouk

Table: Some finite two-point homogeneous spaces, their groups and their spherical functions

Codes de Gabidulin

- Delsarte 1978 (définition et paramètres), Gabidulin 1985 (décodage), Kschischang Koetter 2008 (network coding).
- Analogues des codes de Reed-Solomon, en mieux!
- **Notations:** $m \geq n$, $\mathbb{F}_q^{m\times n}$ s'identifie à $(\mathbb{F}_{q^m})^n$ par le choix d'une $\mathbb{F}_q$-base $\{\alpha_1, \ldots, \alpha_m\}$ de $\mathbb{F}_{q^m}$:

$$\begin{bmatrix} a_{11} & \ldots & a_{1n} \\ a_{21} & \ldots & a_{2n} \\ \vdots & & \vdots \\ a_{m1} & \ldots & a_{mn} \end{bmatrix} \in \mathbb{F}_q^{m\times n} \longleftrightarrow (x_1, \ldots, x_n) \in \left(\mathbb{F}_{q^m}\right)^n$$

si

$$x_j = \sum_{i=1}^{m} a_{ij}\alpha_i.$$

Polynômes linéarisés

- Un polynôme linéarisé à coefficients dans $\mathbb{F}_{q^m}$ est un polynôme de la forme:
$$P(X) = \sum_{\text{finie}} a_i X^{q^i}, \ a_i \in \mathbb{F}_{q^m}.$$
Le degré $\deg_q(P)$ de P est le plus grand indice i tel que $a_i \neq 0$.
- Ensemble noté $\mathbb{L}_{q^m}[X]$. C'est un anneau non commutatif pour la multiplication:
$$(PQ)(X) := P(Q(X)).$$

- Explicitement, si $P(X) = \sum_i a_i X^{q^i}$ et $Q(X) = \sum_i b_i X^{q^i}$, alors $(PQ)(X) = \sum_i c_i X^{q^i}$ avec
$$c_i = \sum_{k+\ell=i} a_k b_\ell^{q^k}.$$

- À part la commutativité, l'anneau $\mathbb{L}_{q^m}[X]$ a toutes les bonnes propriétés de l'anneau des polynômes usuel, en particulier une division euclidienne à droite, un algorithme d'Euclide étendu à droite (resp à gauche).
- **Linéarité:** si $P \in \mathbb{L}_{q^m}[X]$, pour tout $x, y \in \mathbb{F}_{q^m}$, $\lambda, \mu \in \mathbb{F}_q$,

$$P(\lambda x + \mu y) = \lambda P(x) + \mu P(y)$$

car

$$(\lambda x + \mu y)^{q^i} = \lambda x^{q^i} + \mu y^{q^i}.$$

(d'où le nom de polynôme linéarisé)

- **Zéros:** En particulier, les zéros de P forment un $\mathbb{F}_q$-espace vectoriel de dimension au plus égale à $\deg_q(P)$ (car leur nombre est majoré par $\deg_X(P) = q^{\deg_q(P)}$).

Codes de Gabidulin: définition et propriétés

- Soit $k \leq n \leq m$, et soit $\{x_1, \ldots, x_n\}$ des éléments de $\mathbb{F}_{q^m}$ linéairement indépendants sur $\mathbb{F}_q$.

$$\mathrm{Gab}(n,k) := \left\{ (P(x_1), \ldots, P(x_n)) \ : \ P \in \mathbb{L}_{q^m}[X], \deg_q(P) < k \right\}.$$

- $\mathrm{Gab}(n,k)$ est $\mathbb{F}_{q^m}$-linéaire et de dimension k.
- **Preuve:** si $(P(x_1), \ldots, P(x_n)) = (0, \ldots, 0)$, on aurait $X := \langle x_1, \ldots, x_n \rangle_q \subset Z :=$ zéros de P ce qui contredirait $n \geq k$. Donc

$$\dim_{\mathbb{F}_{q^m}} \mathrm{Gab}(n,k) = \dim_{\mathbb{F}_{q^m}} \left\{ P \in \mathbb{L}_{q^m}[X] \ : \ \deg_q(P) < k \right\} = k.$$

- Sa distance rang minimale d vérifie

$$d = n - k + 1.$$

Preuve de $d = n - k + 1$

- Comme Gab(n, k) est $\mathbb{F}_{q^m}$-linéaire, il suffit de considérer le rang minimal de ses éléments.
- Soit $(P(x_1), \ldots, P(x_n))$ de rang d minimal.
- On considère l'application linéaire $\varphi : \mathbb{F}_q^n \to \mathbb{F}_{q^m}$:

$$\varphi(\lambda_1, \ldots, \lambda_n) = \lambda_1 P(x_1) + \cdots + \lambda_n P(x_n).$$

- P est $\mathbb{F}_q$-linéaire donc:

$$\lambda_1 P(x_1) + \cdots + \lambda_n P(x_n) = P(\lambda_1 x_1 + \cdots + \lambda_n x_n)$$

- Donc : $\dim(\operatorname{Im}\varphi) = \dim(P(X)) = d$ et $\dim(\ker\varphi) = \dim(X \cap Z)$ donc

$$d = \dim(P(X)) = n - \dim(X \cap Z) \geq n - \dim(Z) \geq n - (k - 1).$$

Borne de Singleton

Théorème [Delsarte 1978] Si $\mathcal{C} \subset \mathbb{F}_q^{m \times n}$ est un code de distance minimale d pour la métrique rang, et si $m \geq n$,

$$|\mathcal{C}| \leq q^{m(n-d+1)}.$$

- En particuler, si $\mathcal{C}$ est $\mathbb{F}_{q^m}$-linéaire de dimension k, on a

  $$k \leq n - d + 1$$

  ou encore

  $$d \leq n - k + 1.$$

- **Conclusion:** Gab(n, k) vérifie $d = n - k + 1$ et atteint la borne de Singleton pour la métrique rang (on dit qu'il est MRD).

Décodage des codes de Gabidulin

- Jusqu'à $(d-1)/2$, on sait décoder par des algorithmes essentiellement analogues à ceux pour les codes de Reed-Solomon.
- Précurseur: Gabidulin (1985) exploite d'algorithme d'Euclide étendu.
- Roth (1991), Gabidulin (1992), Sidornko-Richter-Bossert (2011), Loidreau (2006), Wachter-Zeh (2013).
- Antonia Wachter-Zeh, phd 2013, survol complet de ces méthodes.
- Contrairement aux RS, il n'y a pas d'algorithme de décodage en liste pour les codes de Gabidulin.

Références

P. Delsarte *Bilinear forms over a finite field with applications to coding theory*, JCTA 25 (3) (1978)

E.M. Gabidulin *Theory of codes with maximum rank distance* Probl. Inf. Transm, 21 (1) (1985)

R. Koetter and F. R. Kschischang, *Coding for Errors and Erasures in Random Network Coding*, IEEE Trans. Inf. Th. 54 (2008)

D. Silva and F. R. Kschischang, *On metrics for error correction in network coding*, IEEE Trans. Inf. Th. 55 (2009)

D. Silva, F. R. Kschischang and R. Koetter, *A rank-metric approach to error control in random network coding* IEEE Trans. Inf. Th. 54 (2008)

A. Wachter-Zeh, *Decoding of block and convolutional codes in rank metric*, phd thesis, 2013.