Nicolas Sendrier

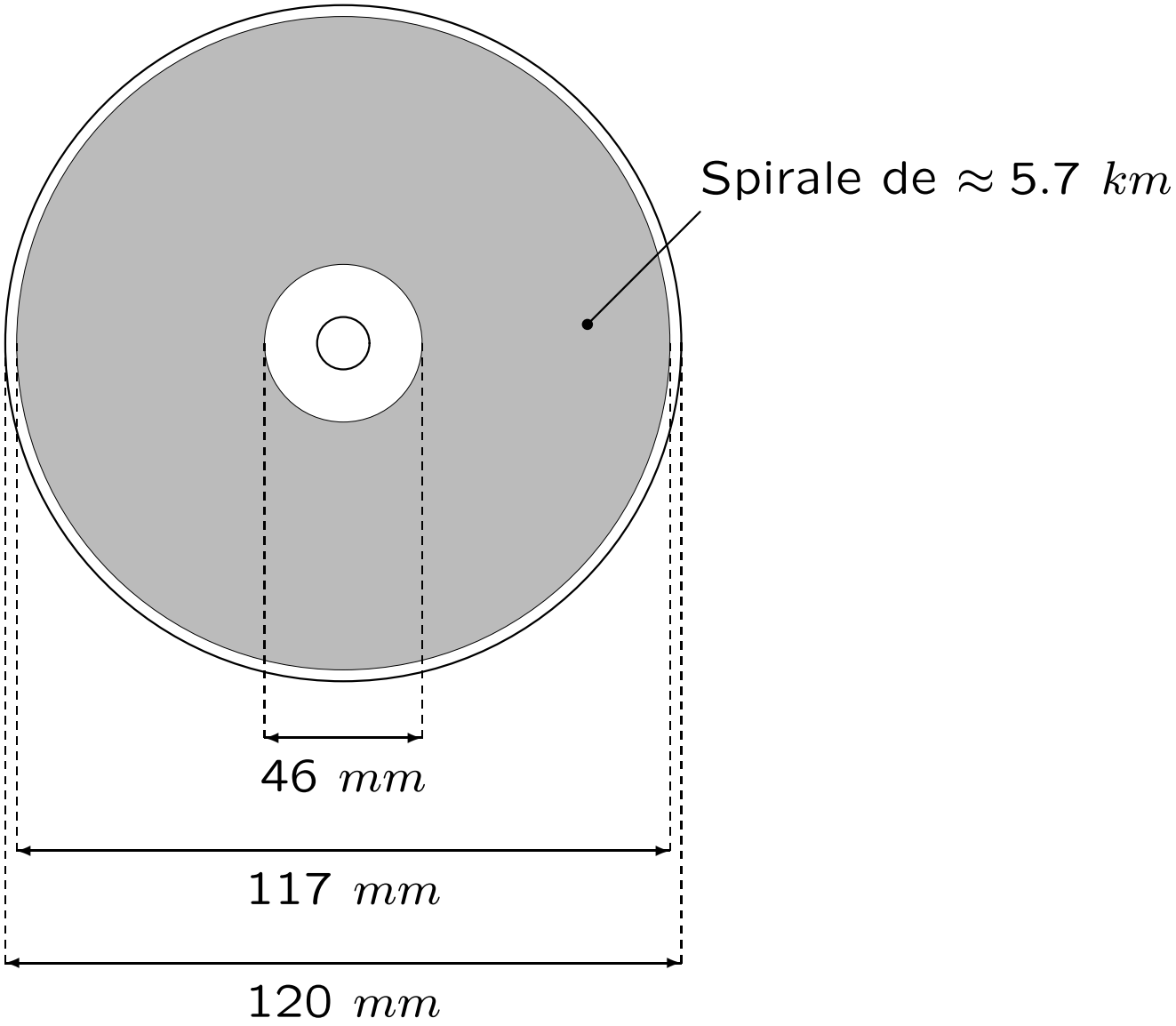
Majeure d'informatique

Introduction à la théorie de l'information

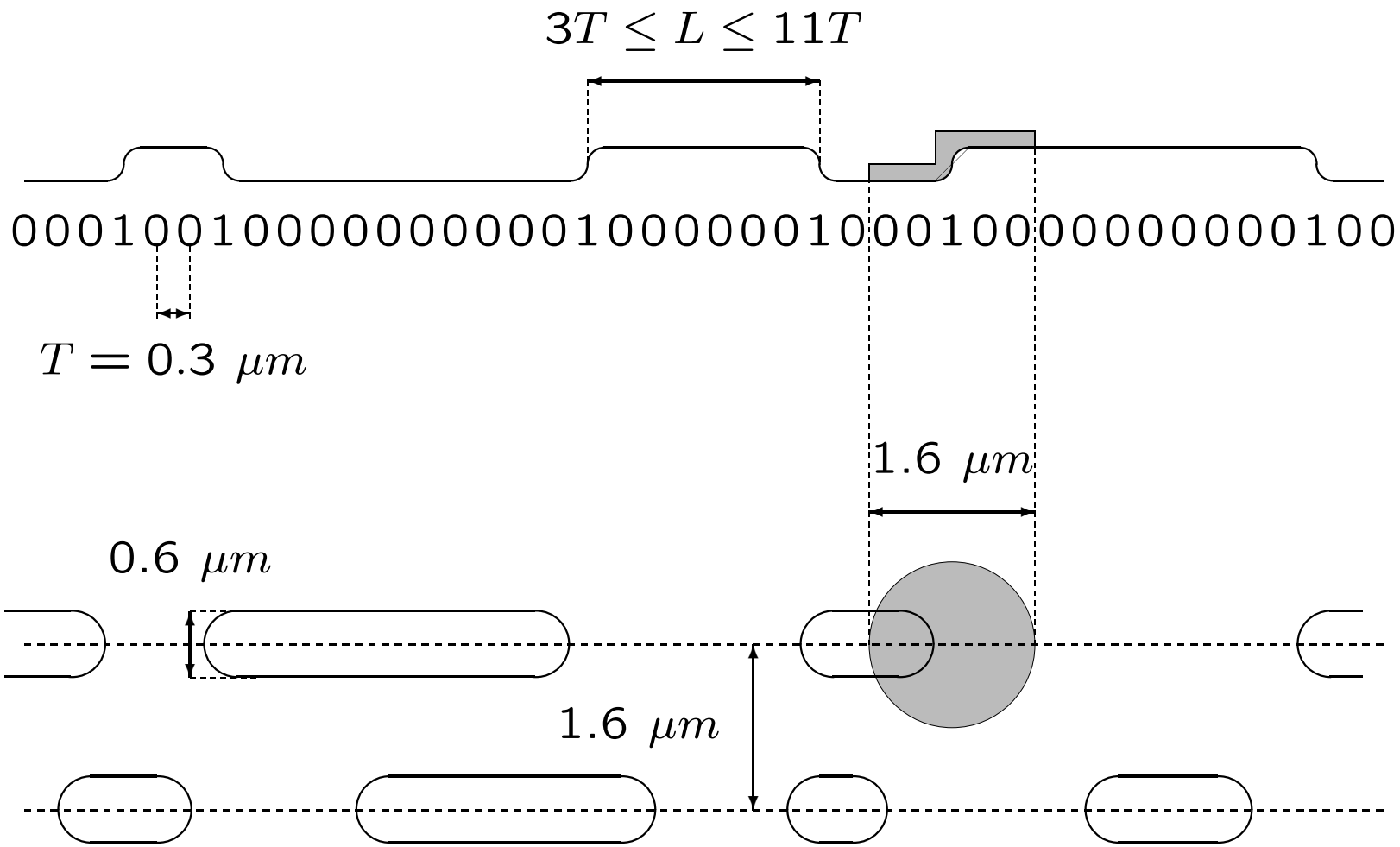
Cours n°9

Le CD audio

Dimensions du CD audio



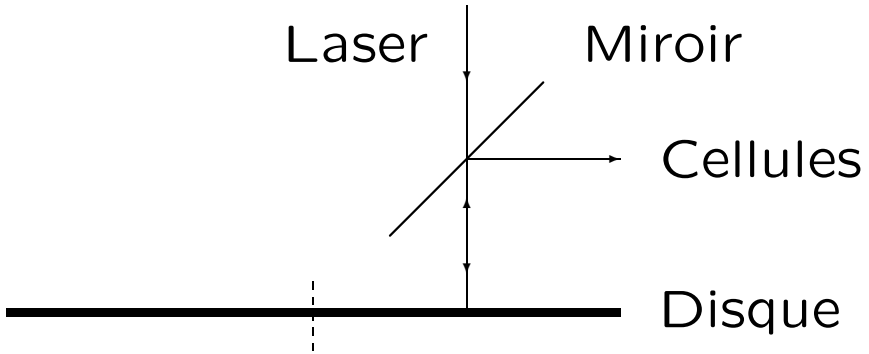
Lecture par laser



Lecture par laser

La lecture s'effectue de l'intérieur vers l'extérieur à vitesse linéaire constante, et à une vitesse angulaire variable.

Le spot laser traverse un miroir sans tain, est réfléchi par le disque, le miroir, puis mesuré par les cellules.



L'énergie mesurée par les cellules diminue lors d'un changement de niveau.

Codage et protection de l'information

1. Échantillonnage
2. Codage de source (EFM)
3. Synchronisation
4. Code correcteur d'erreurs (CIRC)
   (a) Codes de Reed-Solomon
   (b) Entrelacement à retard 4
5. Permutation des échantillons – Interpolation

Échantillonnage

La fréquence d'échantillonage est de 44 100 Hertz sur 16 bits.

Une seconde de signal audio stéréo va donc représenter une quantité d'information égale à :

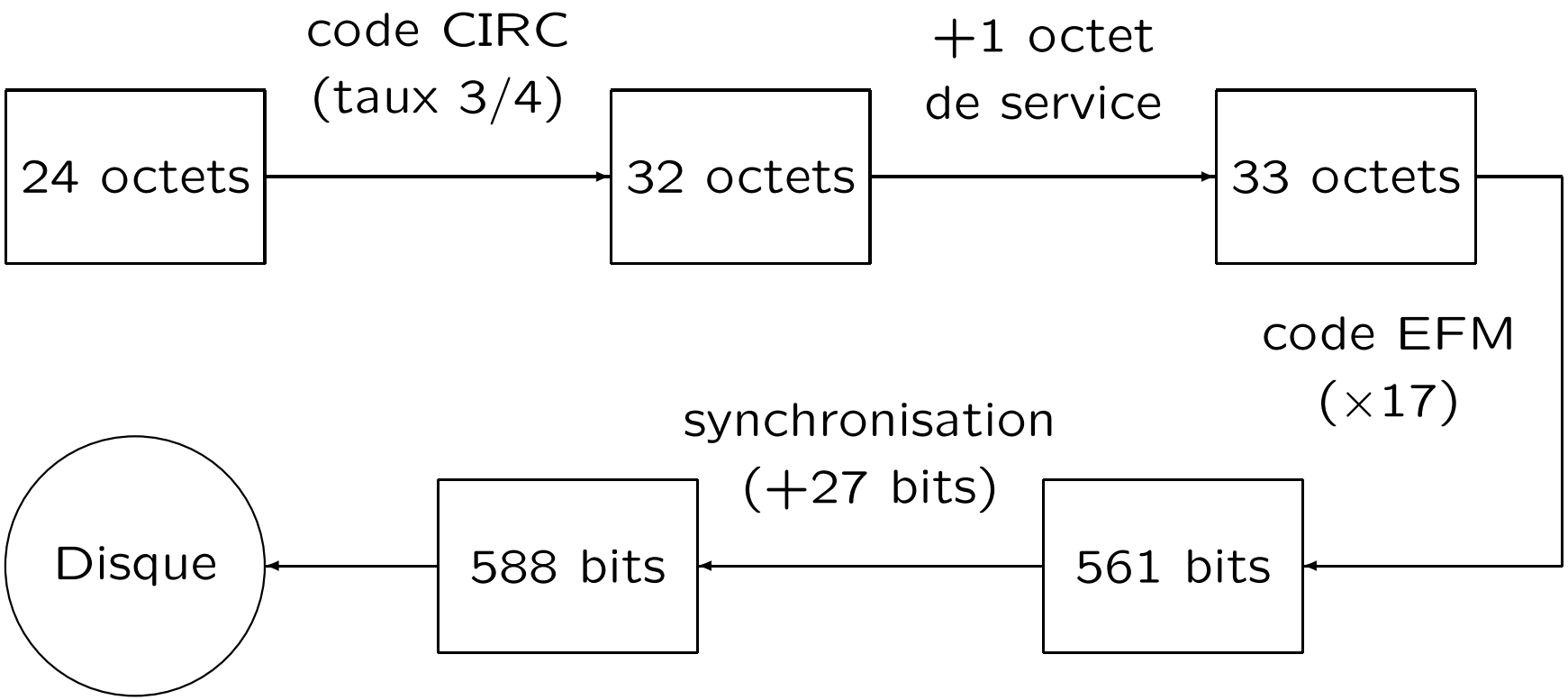
$$44\,100 \times 16 \times 2 = 1\,411\,200 \text{ bits}$$

Au total un CD audio permet d'enregistrer 74 minutes de musique stéréophonique, soit

$$74 \times 60 \times 1\,411\,200 \approx 6\,265 \text{ Mbits} \approx 780 \text{ Mo}$$

La trame

Chaque trame est constituée de 6 échantillons, soit $6 \times 16 \times 2 = 192$ bits, ou 24 octets.



Codage de source – Le code EFM

Le but du code d'enregistrement EFM (*Eight to Fourteen Modulation*) est de transformer une séquence binaire quelconque en une séquence binaire respectant la contrainte – dite (2,10) – liées au support, à savoir :

– chaque "1" sera séparé d'au moins 2 "0",

– chaque "1" sera séparé d'au plus 10 "0".

Codage EFM

Il existe 267 mots binaires de longueur 14 vérifiant la contrainte (2,10). La concaténation de deux quelconques de ces mots ne permet pas toujours de vérifier la contrainte.

Par exemple la concaténation des deux mots

$$01000010000000$$

$$00000100010010$$

produit une séquence comportant 12 “0” consécutifs :

$$0100001\underbrace{0000000\,00000}_{12}100010010$$

Codage EFM

Il est cependant possible d'en choisir 256 tels que l'on puisse toujours les relier entre eux à l'aide d'un des triplets

$$000,\ 100,\ 010,\ 001$$

en obtenant une séquence vérifiant la contrainte (2,10).

Les deux mots de notre exemple reliés à l'aide du triplet 100 produisent la séquence

$$0100001\underbrace{0000000}_{7}\,\mathbf{1}\underbrace{\mathbf{00}\,00000}_{7}100010010$$

Chaque octet sera ainsi représenté par 17 symboles binaires sur le disque.

Synchronisation

Les incertitudes mécaniques rendent nécessaire l'adjonction d'une séquence de synchronisation à intervalles réguliers. Cette séquence de longueur 27 est ajoutée tous les 33 mots, l'ensemble forme une trame de longueur

$$33 \times (14 + 3) + 27 = 588 \text{ symboles binaires}$$

Cette séquence de synchronisation sera

$$1\underbrace{0000000000}_{10}1\underbrace{0000000000}_{10}100xy$$

où x et y sont 2 bits de liaisons assurant la contrainte $(2, 10)$.

Code correcteur d'erreurs

Deux modèles d'erreurs sont à redouter :

– des erreurs isolées de petite tailles (1 ou 2 octets).
  Ces erreurs sont dues à des imprécisions mécaniques, à des défauts du support ...

– des erreurs en rafales pouvant affecter des centaines d'octets.
  Ces erreurs sont provoquées par une dégradation du support ; rayures, traces de doigts, ...

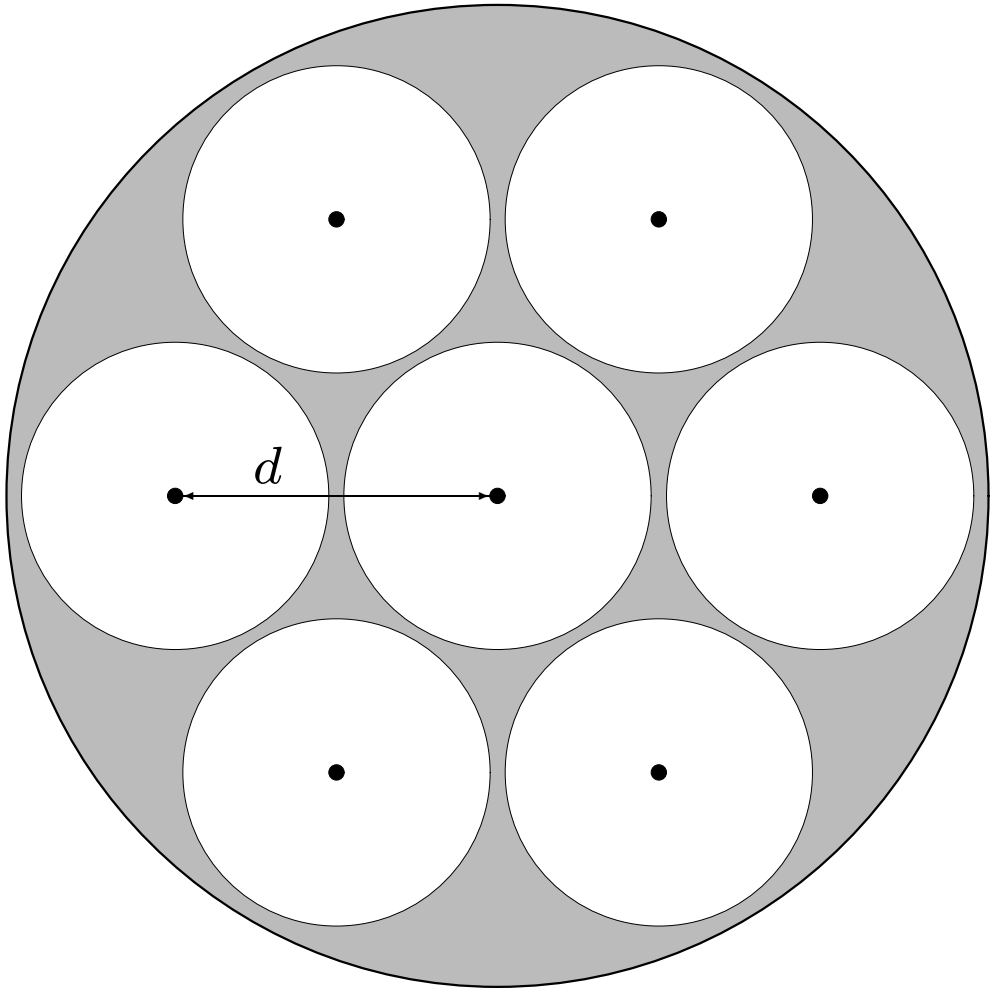
Codes linéaires q-aires

Nous noterons $\mathbf{F}_q$ le corps fini à q éléments. Pour tout $x = (x_1, \ldots, x_n)$ et tout $y = (y_1, \ldots, y_n)$ dans $\mathbf{F}_q^n$, la distance de Hamming de x à y est

$$d_H(x, y) = |\{i, 1 \leq i \leq n, x_i \neq y_i\}|$$

Un code linéaire $C(q; n, k, d)$ est un sous-espace vectoriel de $\mathbf{F}_q^n$ de dimension k dont tous les éléments sont deux à deux à distance de Hamming d au moins (i.e. d est distance minimale de C).

Espace de Hamming – Sphères de Hamming



Toute occurence de $w < d/2$ erreurs permet de retrouver le mot de code.

Généralement le décodage n'est "possible" qu'à l'intérieur des sphères de Hamming.

Codes cycliques

Soit $\mathbf{F}_q$ le corps fini à q éléments et soit $n \mid q^m - 1$.

Un code cyclique de longueur n sur $\mathbf{F}_q$ est un idéal de $R_n = \mathbf{F}_q[x]/(x^n - 1)$.

Soit $\mathcal{C}$ un code cyclique, nous avons :
– $\mathcal{C} = (g(x))$ car l'anneau R_n est principal,
– si $g(x)$ est de degré minimal, alors $g(x) \mid x^n - 1$,
– $\mathcal{C}$ est stable par permutation circulaire (multiplication par x)

Codes de Reed-Solomon

Soit $n = q - 1$ et soit α un élément générateur de $\mathbf{F}_q^*$:

$$\mathbf{F}_q^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\} \quad \text{et} \quad x^n - 1 = \prod_{i=0}^{n-1} \left(x - \alpha^i\right)$$

Le code de Reed-Solomon sur $\mathbf{F}_q$ de distance construite δ est le code cyclique de longueur n sur $\mathbf{F}_q$ de polynôme générateur :

$$g(x) = (x - \alpha)(x - \alpha^2) \ldots (x - \alpha^{\delta-1}).$$

Ce code a pour distance minimale $d = \delta$ et pour dimension $k = n - \delta + 1$. Nous noterons $RS(q; n, k, d)$.

Définitions équivalentes

$$RS(q;n,k,d) = (g(x)), \quad g(x) = \prod_{i=1}^{d-1} \left(x - \alpha^i\right)$$

$$RS(q;n,k,d) = \{f(x)g(x) \mid f(x) \in \mathbf{F}_q[x], \deg f(x) < k = n - d + 1\}$$

$$RS(q;n,k,d) = \{c(x) \in \mathbf{F}_q[x] \mid \deg c(x) < n \text{ et } c(\alpha^i) = 0, i = 0 \ldots d-1\}$$

$$RS(q;n,k,d) = \left\{ \sum_{i=0}^{n-1} u(\alpha^i)x^i \mid u(z) \in \mathbf{F}_q[z], \deg u(z) < k \right\}$$

$$c(x) = \sum_{i=0}^{n-1} u(\alpha^i)x^i \Longleftrightarrow u(z) = n \sum_{j=0}^{n-1} c(\alpha^{n-j})z^j$$

Décodage

Un mot $c(x)$ du code $RS(q; n, k, d)$ est utilisé pour transmettre de l'information.

Ce mot sera entaché d'une erreur $e(x)$ de petit poids (*i.e.* comportant un petit nombre de monômes).

Le mot reçu, le seul dont disposera le décodeur, sera $b(x) = c(x) + e(x)$.

Le décodeur pourra calculer pour tout i, $1 \leq i \leq d-1$, la valeur $e(\alpha^i) = b(\alpha^i) - c(\alpha^i) = b(\alpha^i)$.

Exemple – Correction d'une erreur

Soit le code $RS(16; 15, 13, 3)$, et soit α un générateur de $\mathbf{F}_{16}^*$ vérifiant $\alpha^4 + \alpha + 1$.

Nous supposerons l'erreur de poids 1, soit $e(x) = Yx^l$.

Le mot reçu $b(x)$ évalué en α et α^2 donne

$$\begin{cases} b(\alpha) &= e(\alpha) &= Y\alpha^l &= \alpha^2 \\ b(\alpha^2) &= e(\alpha^2) &= Y\alpha^{2l} &= \alpha^{13} \end{cases}$$

Il vient immédiatement $l = 11$ et $Y = \alpha^{-9} = \alpha^6$.

Exemple – Correction de deux erreurs

Prenons le code $RS(16; 15, 11, 5)$ et une erreur de poids 2, $e(x) = Y_1 x^{l_1} + Y_2 x^{l_2}$. Il faudra résoudre dans $\mathbf{F}_{16}$ le système :

$$\begin{cases} Y_1 X_1 + Y_2 X_2 = e(\alpha) \\ Y_1 X_1^2 + Y_2 X_2^2 = e(\alpha^2) \\ Y_1 X_1^3 + Y_2 X_2^3 = e(\alpha^3) \\ Y_1 X_1^4 + Y_2 X_2^4 = e(\alpha^4) \end{cases}$$

où $X_1 = \alpha^{l_1}$ et $X_2 = \alpha^{l_2}$.

De façon générale il faut disposer de deux fois plus d'équations que d'erreurs.

Exemple – Correction d'effacements

Un effacement est une erreur dont la position est connue. Prenons le code $RS(16; 15, 11, 5)$, avec l'erreur $e(x) = Y_1 x^{l_1} + Y_2 x^{l_2} + Y_3 x^{l_3} + Y_4 x^{l_4}$, les $X_i = \alpha^{l_i}$ étant connus.
Le système d'équations à résoudre est :

$$\begin{cases} Y_1 X_1 + Y_2 X_2 + Y_3 X_3 + Y_4 X_4 = e(\alpha) \\ Y_1 X_1^2 + Y_2 X_2^2 + Y_3 X_3^2 + Y_4 X_4^2 = e(\alpha^2) \\ Y_1 X_1^3 + Y_2 X_2^3 + Y_3 X_3^3 + Y_4 X_4^3 = e(\alpha^3) \\ Y_1 X_1^4 + Y_2 X_2^4 + Y_3 X_3^4 + Y_4 X_4^4 = e(\alpha^4) \end{cases}$$

mais cette fois, seuls les Y_i sont inconnus.

Équation clé

Soit $e(x) = \sum_{i=1}^{w} Y_i x^{l_i}$, pour tout i on pose $X_i = \alpha^{l_i}$.

Les polynômes

$$\sigma(z) = \prod_{i=1}^{w} (1 - X_i z) \quad \text{et} \quad \omega(z) = \sum_{i=1}^{w} Y_i X_i \prod_{j \neq i} (1 - X_i z)$$

sont les seuls, à une constante multiplicative scalaire près, à vérifier

$$(\mathcal{S}) \ : \ \begin{cases} \omega(z) = \sigma(z) S(z) \\ \deg \sigma = w \\ \deg \omega < w \\ \text{pgcd}(\sigma(z), \omega(z)) = 1 \end{cases}$$

où

$$S(z) = \sum_{j=1}^{\infty} e(\alpha^j) z^{j-1}$$

Algorithme d'Euclide étendu

L'algorithme d'Euclide étendu permet de trouver une solution au système $(\mathcal{S})$, lorsqu'elle existe, à condition que les $2w$ premiers termes de la série

$$S(z) = \sum_{j=1}^{\infty} e(\alpha^j) z^{j-1}$$

soient connus, c'est-à-dire $e(\alpha)$, $e(\alpha^2)$, ... $e(\alpha^{2w})$.

En pratique cela signifie que l'algorithme d'Euclide permet de corriger w erreur dans un mot du code $RS(q; n, k, d)$ à condition que $2w \leq d-1$, c'est-à-dire $w < d/2$.

Codes de Reed-Solomon raccourcis

Tout code de Reed-Solomon $RS(q; n, k, d) = (g(x))$ peut être raccourci pour obtenir un code $RS(q; n' = n - r, k' = k - r, d)$ défini par

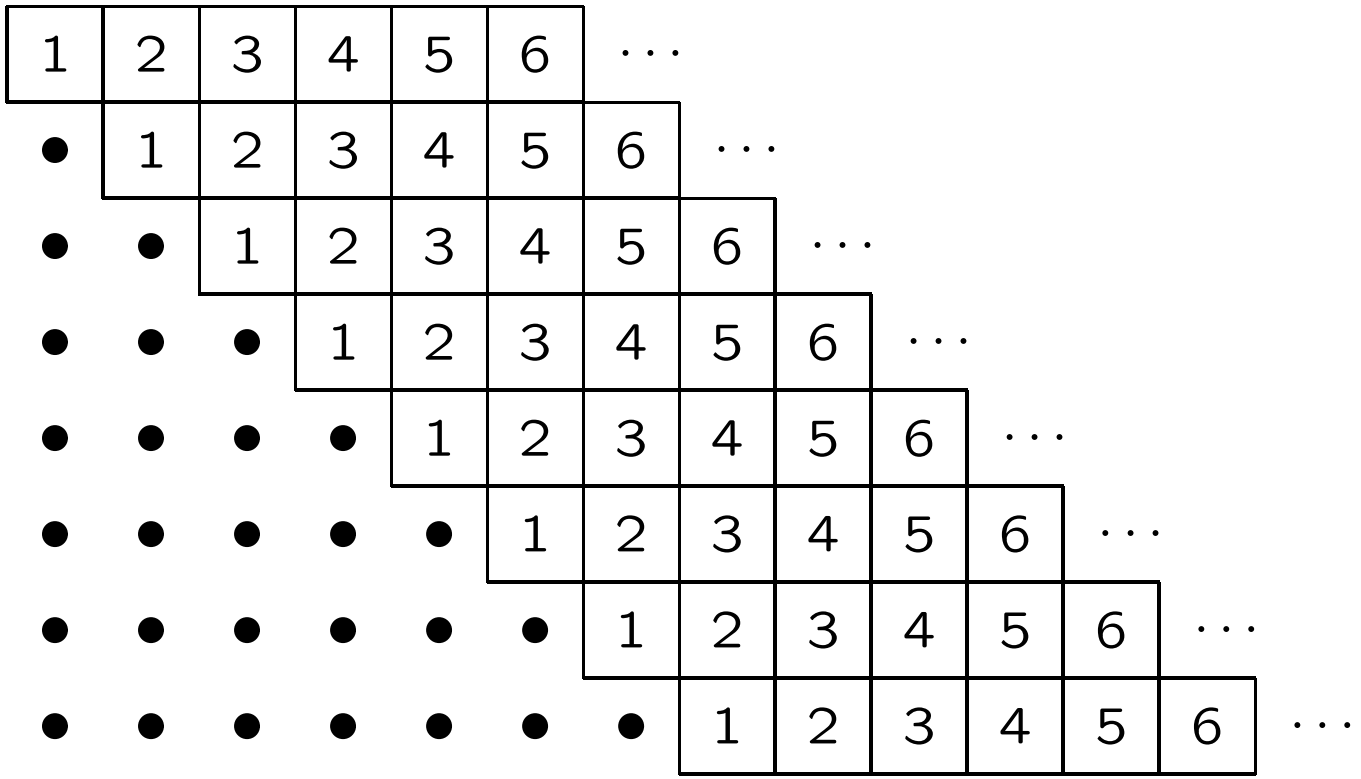
$$RS(q; n', k', d) = \{f(x)g(x) \mid f(x) \in \mathbf{F}_q[x], \deg f < k'\}$$

Les codes correcteurs utilisés dans le disque compact sont les codes

$$C_1 = RS(256; 28, 24, 5) \quad \text{et} \quad C_2 = RS(256; 32, 28, 5)$$

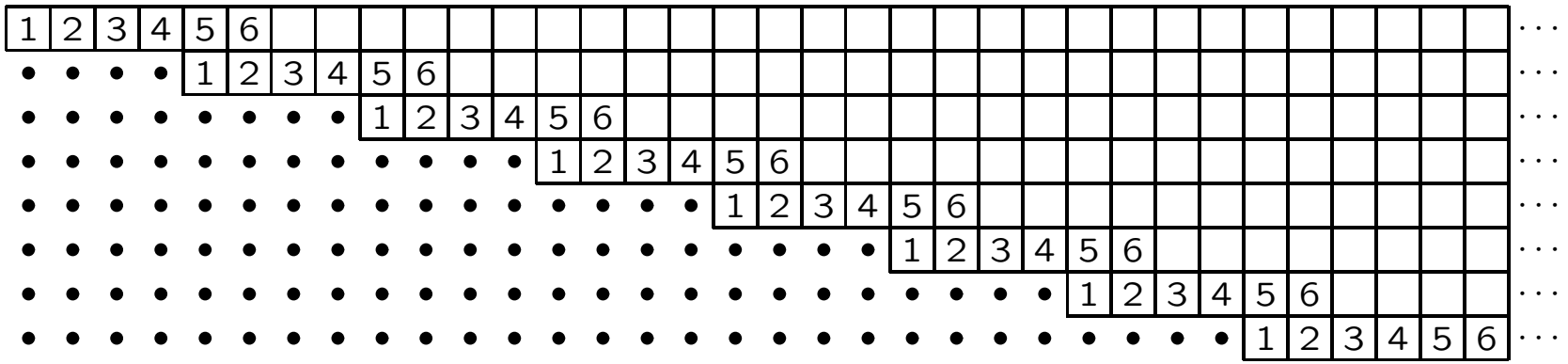
obtenus par raccourcissement du $RS(256; 255, 251, 5)$.

Entrelacement à retard 1



Les mots sont ensuite transmis par colonne.

Entrelacement à retard 4



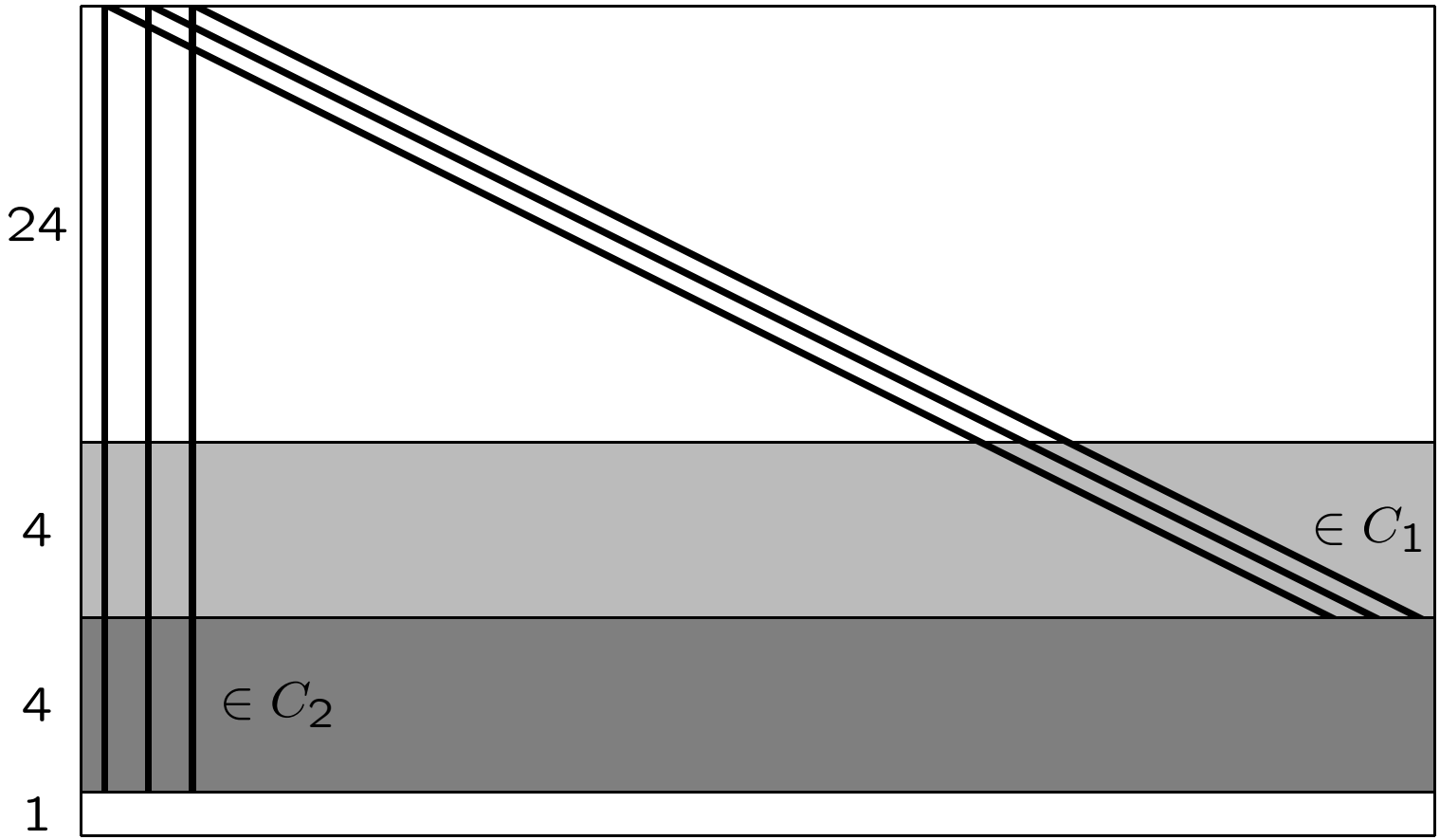
Les mots sont ensuite transmis par colonne.

Code CIRC

Cross Interleaved Reed-Solomon Code

- l'information est codée par blocs de 24 octets en mots de C_1 de 28 octets
- Les mots de C_1 sont placés dans un tableau d'entrelacement à retard 4.
- Le colonnes du tableau sont codées en mots de C_2 de 32 octets.
- Un octet de service (non protégé) est ajouté à chaque colonne.

Code CIRC



Algorithme de décodage

Les codes sont décodés successivement en commençant par C_2

1. Le code C_2 est limité à la correction d'une erreur (au lieu de deux).
2. Le code C_1 est utilisé pour corriger 4 effacements.

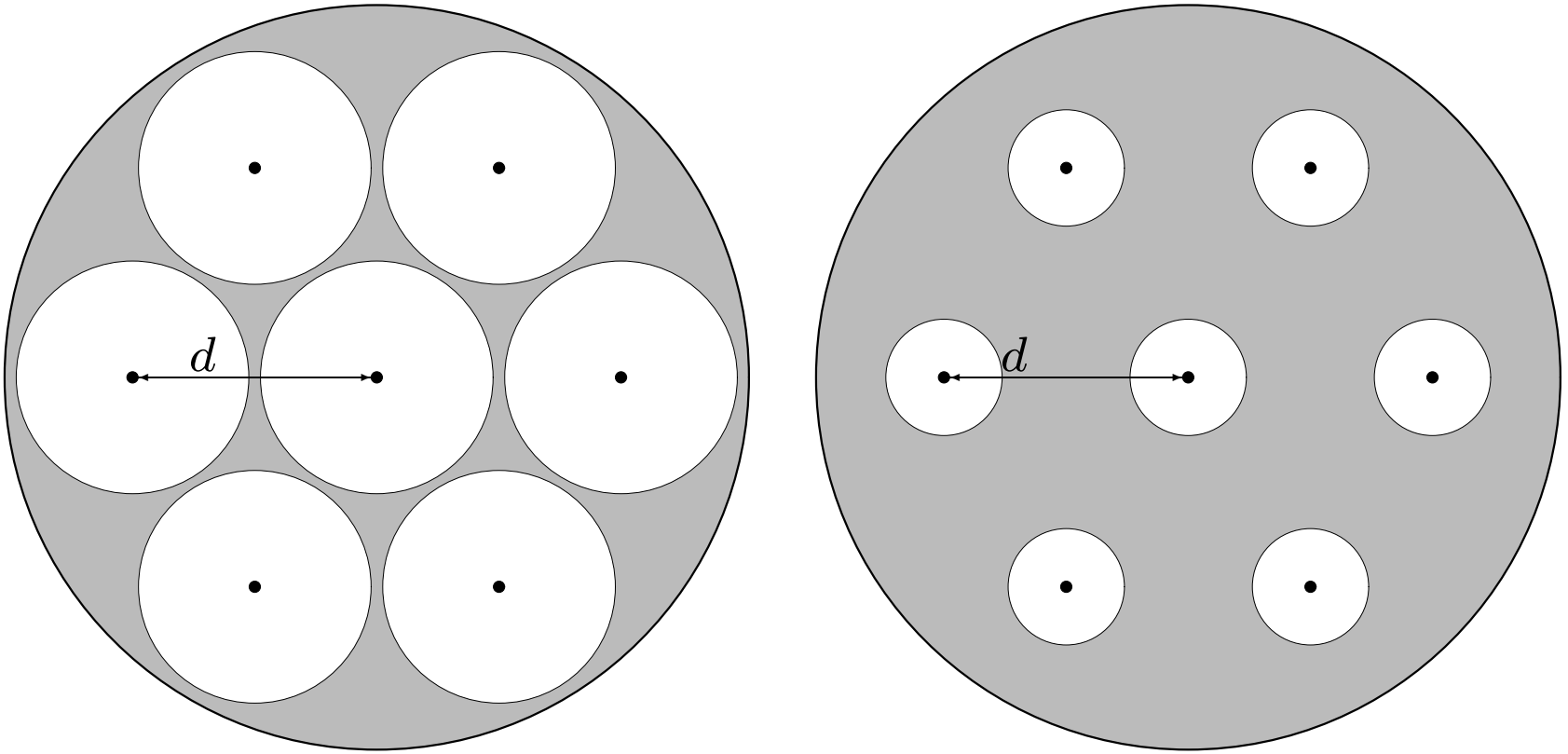
Capacité de correction de C_2

Le code C_2 peut corriger deux erreurs mais n'est utilisé que pour une seule. Cela permet d'augmenter sa capacité de détection.

Avec des erreurs isolées intervenant selon une loi gaussienne avec une probabilité de 0.1%

Correction de	1 erreurs	2 erreurs
Probabilité de décodage	0.99951	0.9999951
Probabilité d'échec	$4.8\,10^{-4}$	$4.8\,10^{-6}$
Probabilité d'erreur	$5.9\,10^{-14}$	$3.0\,10^{-8}$
Probabilité de non-détection d'une rafale	$1.9\,10^{-6}$	$7.5\,10^{-3}$

Capacité de correction de C_2

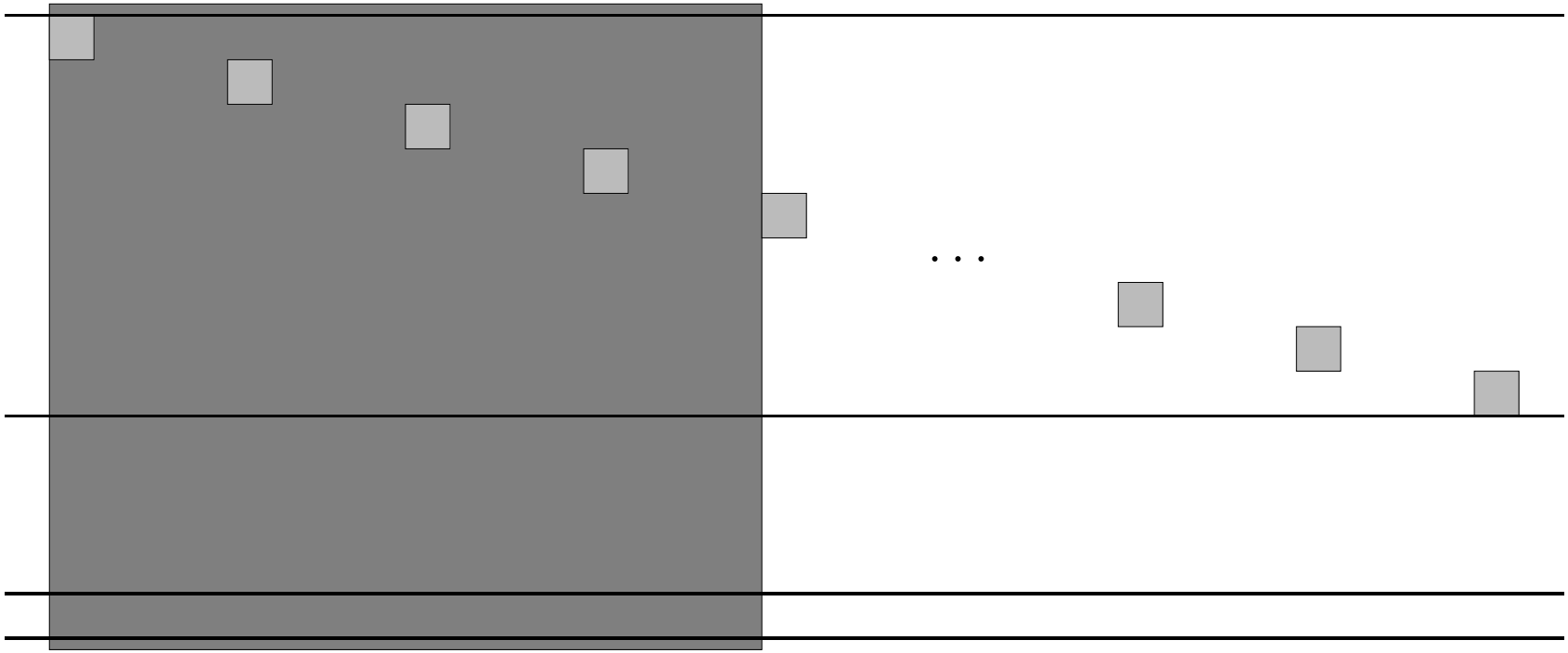


Capacité de correction de C_1

Après correction et/ou détection d'erreurs dans les colonnes, le code C_1 est utilisé pour corriger 4 effacements.

Si l'on suppose que C_2 a éliminé toutes les erreurs isolées, il ne reste plus que les erreurs en rafale. L'entrelacement à retard 4 permet de corriger les rafales d'erreurs affectant jusqu'à 16 trames consécutives.

Capacité de correction de C_1



Rafale corrigible affectant 16 trames (colonnes).

Capacité de correction de C_1

Une rafale de 16 trames représente $588 \times 16 = 9408$ symboles binaires soit environ 2.8 millimètres sur le disque.

De plus un même mot de C_1 ne pourra pas corriger 2 rafales. Un mot donné s'étend sur $4 \times 28 = 112$ trames, soit environ 2 centimètres.

Interpolation

Il existe une protection supplémentaire pour le CD audio. Lors de l'inscription sur le disque, 2 échantillons consécutifs seront espacés au maximum.

De cette manière, si un échantillon est effacé, le décodeur possédera avec une grande probabilité l'échantillon précédent ainsi que le suivant.

L'échantillon manquant peut ainsi être interpolé.

Interpolation

Chaque trame est constituée de 6 échantillons stéréo

G_1	G_2	G_3	G_4	G_5	G_6
D_1	D_2	D_3	D_4	D_5	D_6

où chaque G_i ou D_i représente 16 bits. Le mot de code de C_1 est constitué comme suit :

G_1	G_3	G_5	D_1	D_3	D_5	P	P'	G_2	G_4	G_6	D_2	D_4	D_6

où P et P' sont les symboles de parité dus à C_1.

Deux échantillons consécutifs sont séparés par au moins 6 16-uplets (12 octets). Suite à l'entrelacement à retard 4, cet espacement est de 48 trames ou 8.5 millimètres.