Problématique :

Un expéditeur A envoie un message m à B.
Le message m envoyé est codé en binaire : on associe au message m un n-uplet M d'éléments de l'ensemble $\{0, 1\}$.

Expérience 1 :

A choisit un nombre entier m compris entre 0 et 15.
Pour envoyer le message m à B, A répond par oui (codé 1) ou non (codé 0) à une série de quatre questions.
Le message envoyé sera le quadruplet M formé des quatre réponses.

- **Question 1 :** m est-il supérieur ou égal à 8 ?
- **Question 2 :** m est-il dans l'ensemble $\Big\{4, 5, 6, 7, 12, 13, 14, 15\Big\}$
- **Question 3 :** m est-il dans l'ensemble $\Big\{2, 3, 6, 7, 10, 11, 14, 15\Big\}$
- **Question 4 :** m est-il impair ?

Notons m_1, m_2, m_3 et m_4 les réponses aux 4 questions.

Ces 4 valeurs correspondent aux 4 chiffres du codage binaire de m.

Plus précisément : $m = m_1 \times 8 + m_2 \times 4 + m_3 \times 2 + m_4 \times 1$

Résultat qui s'écrit également : $m = \underline{m_1\, m_2\, m_3\, m_4}_{\,2}$ (*écriture binaire de* m)

- **Question 1 :** m est-il supérieur ou égal à 8 ?

- **Question 2 :** m est-il dans l'ensemble $\Big\{4, 5, 6, 7, 12, 13, 14, 15\Big\}$

- **Question 3 :** m est-il dans l'ensemble $\Big\{2, 3, 6, 7, 10, 11, 14, 15\Big\}$

- **Question 4 :** m est-il impair ?

Problème :

Des erreurs peuvent se produire pendant la phase de transmission du message.

B reçoit alors un message M' qui comporte peut-être des erreurs.

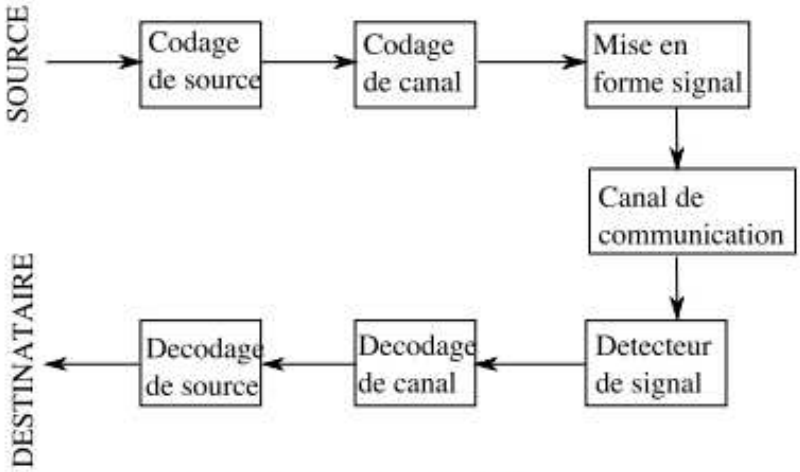

Figure 1.1: Chaîne de communication

Solution :

On dispose de méthodes permettant de détecter et corriger des erreurs qui surviennent lors de la transmission.

Expérience 2 :

A choisit un nombre entier m compris entre 0 et 15.

Pour envoyer le message m à B, A répond par oui (codé 1) ou non (codé 0) à une **série de sept questions** (trois questions ont été rajoutées pour détecter éventuellement une erreur et la corriger).

Comme le message transmis peut éventuellement contenir une erreur, **A est autorisé à mentir une fois**.

Le message envoyé sera le quadruplet M formé des sept réponses.

- **Question 1 :** m est-il supérieur ou égal à 8 ?
- **Question 2 :** m est-il dans l'ensemble $\Big\{4, 5, 6, 7, 12, 13, 14, 15\Big\}$
- **Question 3 :** m est-il dans l'ensemble $\Big\{2, 3, 6, 7, 10, 11, 14, 15\Big\}$
- **Question 4 :** m est-il impair ?

- **Question 5 :** m est-il dans l'ensemble $\Big\{1, 2, 4, 7, 9, 10, 12, 15\Big\}$

- **Question 6 :** m est-il dans l'ensemble $\Big\{1, 2, 5, 6, 8, 11, 12, 15\Big\}$

- **Question 7 :** m est-il dans l'ensemble $\Big\{1, 3, 4, 6, 8, 10, 13, 15\Big\}$

Notons m_i (avec $1 \leq i \leq 7$) les réponses aux 7 questions.

On définit les matrices : $M = \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_7 \end{pmatrix}$ et $H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$

Le résultat (modulo 2) du produit $Y = HM$ est une matrice colonne à 3 lignes.

Les coefficients de cette matrice Y correspondent aux chiffres de l'écriture binaire du numéro k de la question où A a menti (ce nombre sera égal à 0 dans le cas où il n'y a pas d'erreurs).

Plus précisément, $k = y_1 \times 1 + y_2 \times 2 + y_3 \times 4$

Exemple : analysons les résultats correspondants aux réponses enregistrées dans

$$M^T = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$M^T = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$

A ment à la question $k = 3$ et $m = 9$

- **Question 1 :** m est-il supérieur ou égal à 8 ?
- **Question 2 :** m est-il dans l'ensemble $\Big\{4, 5, 6, 7, 12, 13, 14, 15\Big\}$
- **Question 3 :** m est-il dans l'ensemble $\Big\{2, 3, 6, 7, 10, 11, 14, 15\Big\}$
- **Question 4 :** m est-il impair ?
- **Question 5 :** m est-il dans l'ensemble $\Big\{1, 2, 4, 7, 9, 10, 12, 15\Big\}$
- **Question 6 :** m est-il dans l'ensemble $\Big\{1, 2, 5, 6, 8, 11, 12, 15\Big\}$
- **Question 7 :** m est-il dans l'ensemble $\Big\{1, 3, 4, 6, 8, 10, 13, 15\Big\}$