ACADÉMIE D'ORLÉANS-TOURS
Liberté
Égalité
Fraternité

Ressource complémentaire

Olympiades nationales de mathématiques 2023

Ressource complémentaire à l'exercice académique n°3.

CODE DE HAMMING : COMPLEMENTS

Une discussion à travers les âges entre Ada Lovelace et Hedy Lamarr

Figure 1Ada Lovelace et Hedi Lamarr - Illustration MidJourney

Table des matières

Un peu d'histoire

Richard Hamming : code correcteur d'erreur

Richard Wesley Hamming, né le 11 février 1915 à Chicago (Illinois) et décédé le 7 janvier 1998 à Monterey (Californie) est un mathématicien célèbre à qui on doit les codes de Hamming et la distance de Hamming. Il reçut le prix Turing en 1968.

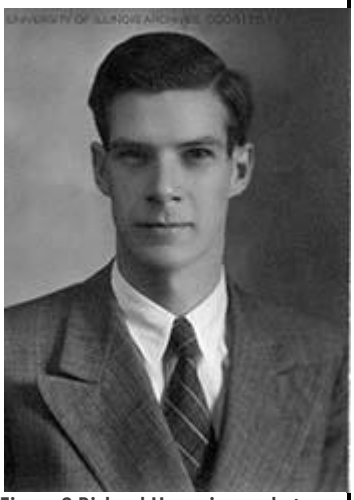

Figure 2 Richard Hamming – photo « réelle » de l'unervisté de L'illinois (1938)

Richard Hamming travaillait avec Claude Shannon en 1947. Avant chaque week-end, il lançait ses calculs sur l'ordinateur du laboratoire et revenait en début de semaine suivante pour s'apercevoir que l'ordinateur avait souvent arrêté l'exécution de son programme suite à une erreur. Hamming se disait que si la machine était en mesure de détecter une erreur, elle devait bien pouvoir détecter l'endroit où l'erreur se produisait et, tant qu'à faire, la corriger.

Le code de Hamming a ainsi été inventé en 1947 et est référencé dans l'article de Shannon de 1948. Marcel Golay (mathématicien, physicien et théoricien de l'information) a publié en 1949 les caractéristiques d'un code d'une longueur de 23 bits, dont 12 bits d'information, capable de corriger 3 erreurs par mot, tandis que celui de Hamming corrigeait une erreur pour une longueur de 7 bits dont 4 d'information.

L'article de Hamming n'a été publié qu'en 1950, le temps que le dépôt de brevet soit effectué ; s'en suivit une polémique entre Golay et Hamming sur la paternité de l'invention du premier code. Le minitel utilisait un code de Hamming de longueur 128. Le code de Golay a été utilisé dans les sondes Viking dans leur voyage vers Mars, et par la sonde Voyager, lancée en 1979 en direction de Jupiter. À la fin des années 90, Voyager continuait à émettre des messages vers la Terre au-delà de l'orbite de Pluton.

Dans la partie C de l'exercice d'Olympiade proposé, vous avez travaillé sur ce code qui permettait de détecter et corriger une erreur dans un message de 11 bits d'information. Nous verrons plus loin dans ce document que le code de Hamming peut être utilisé pour corriger des messages plus long. Mais avant cela présentons les deux femmes, Ada et Hedy, qui cherchaient à communiquer ensemble.

Ada Lovelace

On cite souvent Alan Turing comme le père de l'informatique, d'autres personnes avant lui ont contribué à la naissance de cette science. Une des plus marquante est Augusta Ada King (née Byron), Lady Ada Lovelace.

Née le 15 décembre 1815 à Londres, et morte en novembre 1852 à Londres elle travailla avec Charles Babbage. Ce dernier a imaginé une machine à calculer programmable qui ne verra jamais le jour : la machine analytique. Cette machine devait être constituée de roues et d'engrenages mécaniques, elle devait recevoir ses instructions via des cartes perforées.

Figure 3 Ada et Charles - Illustration Midjourney

Ada a initié l'écriture des instructions sur ces cartes et est devenue ainsi la première programmeuse informatique de l'histoire, avant même la fabrication du premier ordinateur !

Ada était une étudiante enthousiaste des mathématiques, devenant compétente à une époque où il était extrêmement rare qu'une femme le fasse. Elle mourut d'un cancer à l'âge de 36 ans. Tombée dans l'oubli, Ada Lovelace et ses travaux furent exhumés avec l'avènement de l'informatique. Et c'est en son hommage qu'on a appelé Ada le langage de programmation conçu entre 1977 et 1983 pour le département de la Défense américain.

Hedy Lamarr

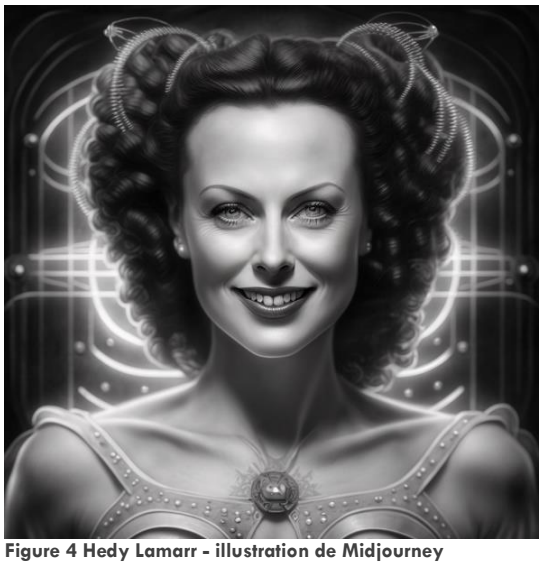

Figure 4 Hedy Lamarr - illustration de Midjourney

Hedy Lamarr, nom de scène de Hedwig Eva Maria Kiesler, est une actrice américaine d'origine autrichienne, née le 9 novembre 1914 à Vienne et morte le 19 janvier 2000 (à 85 ans) à Casselberry (Floride).

Remarquée par sa beauté, elle se présente aux portes d'un studio de cinéma viennois pour aider financièrement ses parents. Commence alors une carrière dans le cinéma.

Elle épouse Friederich Mandl, un marchand d'armes. Bien que malheureuse en ménage, Hedy Lamarr côtoie le monde de l'armée par le biais de son mari. Elle participera à des conversations autour des missiles radioguidés ce qui donnera naissance à une invention visionnaire. Elle traverse l'Atlantique en 1937 pour fuir son mari et prend alors le nom d'Hedy Lamarr.

À l'occasion d'une soirée mondaine Hedy Lamarr rencontre le pianiste George Antheil. Tous les deux discutent longuement de l'armement, un sujet d'Hedy maîtrise parfaitement et qui passionne George Antheil. Nous sommes en 1941 et la seconde guerre mondiale ravage l'Europe. George et Hedy imaginent ensemble un système de cryptage des communications applicables aux torpilles radioguidées trop souvent détournées.

Le système est basé sur un émetteur-récepteur qui permet à la torpille de changer de fréquence de transmission pour ne pas être détectée par les ennemis. Appelé aussi « étalement de spectre par évasion de fréquence » ou FHSS en anglais, ce principe de transmission régit toujours nos technologies modernes sans fils comme les GPS, les communications militaires.

Les deux inventeurs déposent un brevet au Bureau des brevets américains le 10 juin 1941 intitulé « Secret communication system ». Leur invention passe totalement inaperçue et c'est seulement 21 ans plus tard, avec le progrès électronique, que l'armée américaine y voit une utilité. Tombée dans le domaine public, elle fait le bonheur des concepteurs d'appareil à transmission dans les années 80. Aujourd'hui, la plupart des téléphones portables utilisent le système pensé par le duo Lamarr-Antheil.

Si, aujourd'hui, le travail d'Hedy Lamar est lié à nos vies modernes, ses idées avant-gardistes n'ont pas eu la reconnaissance qu'elles méritaient à l'époque. C'est seulement en 1997 qu'elle est récompensée du prix de l'Electronic Frontier Foundation. Elle a alors 82 ans et vit en Floride, loin de la gloire qu'elle a connue autrefois. Elle meurt trois ans plus tard. Elle et son acolyte George Antheil sont admis à titre posthume au National Inventors Hall of Fame en 2014.

Figure 5 Ada et Hedy - Illustration de Midjourney

Un mot sur les illustations

Ne vous y trompez pas, malgré leur apparente banalité, ce document est parsemé de certaines illustrations produites par *Midjourney*, une intelligence artificielle (I.A.). Celle-ci génère des images à partir de mots clés. Cette I.A. a été nourrie par un grand nombre d'images, cela permet des fantaisies comme de voir Ada et Hedy travailler ensemble malgré les années les séparant. Ou encore une Ada Lovelace à la croisée entre le Cyberpunk et le Steampunk. Une invention qui doit beaucoup à ces pionnieres et pionniers de l'informatique.

Figure 6 - Midjourney - résultat de la requête :
« Ada lovelace with cyberpunk implants hyper-realistic »

Figure 7 - Portrait "réel" d'Ada avec en fond un des premiers programmes informatiques

Compléments mathématiques

	1 1	1 2	a 3
0 4	1 5	b 6	c 7
0 8	0 9	d 10	1 11
1 12	0 13	1 14	0 15

Tableau 4

Comme cela a été vu dans l'exercice 3 du sujet académique des Olympiades de Mathématique (2023), le code correcteur de Hamming permet d'identifier et corriger une erreur dans un message long de **11 bits**. Dans cette situation, il faut ajouter **4 bits** de correction ce qui donne un message transmis de **15 bits**. Voici quelques questions (avec leurs réponses en fin de document) pour approfondir le sujet.

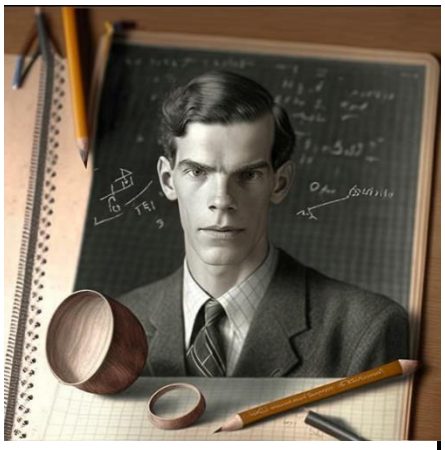

Figure 8 - Illustration de Midjourney, requête :

« Richard Hamming doing mathmatics, ultra-realistic »

1. En admettant qu'il n'y ait aucune erreur lors de la transmission, trouver les 4 bits manquants du message ci-contre.
2. Quel pourcentage ces bits de correction représentent-ils par rapport à l'ensemble des 15 bits utilisés pour transmettre le message ? Nous appellerons cela le pourcentage de redondance.
3. Quel est le pourcentage de redondance du code Goley présenté dans la partie historique du code de Hamming ?

Ce pourcentage de redondance est crucial pour ne pas alourdir les messages envoyés. La comparaison entre les codes de Hamming et Goley est difficile car les deux codes ne corrigent pas le même nombre d'erreurs de transmission. Mais regardons ce qu'il se passe si l'on augmente la taille des messages envoyés avec le code de Hamming.

Par exemple, si le message est composé de 256 bits, il ne faudra que 8 bits de correction pour trouver une erreur lors de la transmission du message. (les 8 bits correspondant au code binaire de la position de l'erreur dans le tableau, exercice laissé à la discrétion du lecteur)

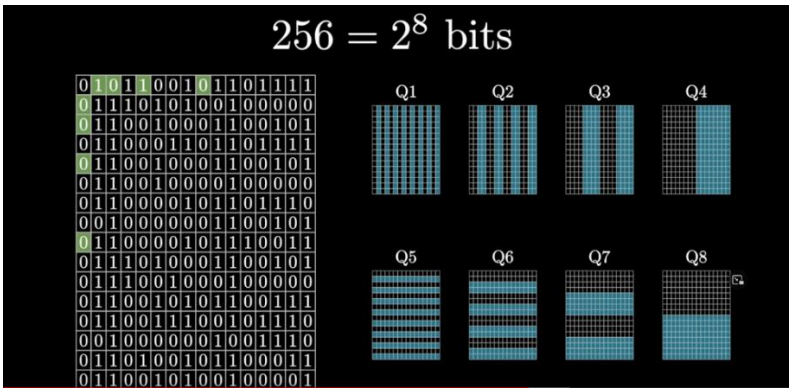

Figure extraite de la vidéo de 3blue1brown : « How to send a self-correcting message (Hamming codes) »

Dans l'illustration ci-dessus, les colonnes et lignes en bleu correspondant aux questions Q1 à Q8 permettent d'identifier la position du bit erroné.

4. Quel est le pourcentage de redondance dans le cas du message de 256 bits ?
5. *Question pour les professeurs.*
   On note n la taille du message en bits. Exprimer le pourcentage de redondance en fonction de n puis déterminer la limite du pourcentage de redondance lorsque n tend vers l'infini.

Pour finir, il existe des codes correcteurs permettant d'identifier et corriger plus d'une erreur, en voici quelques-uns : codes de Reed-Muller, codes de Goppa, codes de Reed-Solomon...

Notebook

Pour ceux qui le souhaitent, un notebook en python complémentaire est disponible sur Capytale.
Code : 14e4-1368591

https://capytale2.ac-paris.fr/web/c/14e4-1368591

Podcasts recommandés

https://www.radiofrance.fr/franceculture/podcasts/la-methode-scientifique/ada-lovelace-la-grande-ordinatrice-5403084

https://www.radiofrance.fr/franceinter/podcasts/affaires-sensibles/affaires-sensibles-du-mercredi-21-decembre-2022-1824884

Correction :

1. $a = 1 \quad b = 1 \quad c = 0 \quad d = 1$
2. $\frac{4}{15} \times 100 \approx 27\ \%$
3. $\frac{12}{23} \times 100 \approx 52\ \%$
4. $\frac{8}{256} \times 100 \approx 3\%$
5. On admettra que pour un message de n bits, le pourcentage de redondance sera équivalent à

$$\frac{\log_2 n}{2^n} = \frac{\ln n}{2^n \ln 10}$$

Ainsi la limite du pourcentage de redondance est de 0 lorsque n tend vers l'infini.

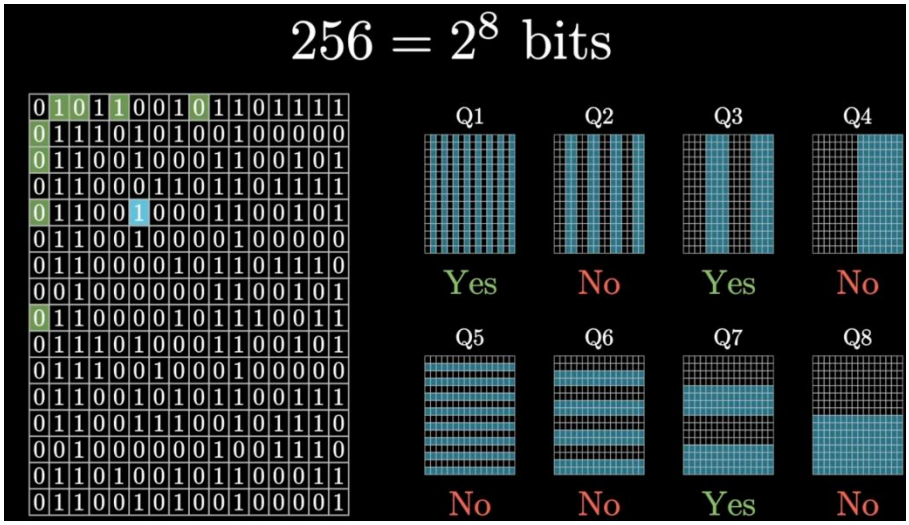

Figure 9 Illustration de la position du bit erroné.
Position 69 du tableau : écriture binaire 01000101
Cette écriture binaire peut être trouvée avec Q8 Q7 Q6 Q5 Q4 Q3 Q2 Q1 et la correspondance Yes=1 et No = 0.
Extrait de la vidéo de 3blue1brown : « How to send a self-correcting message (Hamming codes) »