



LA CHRONIQUE DE
GILLES DOWECK

EN MARS, MÉFIEZ-VOUS DE LA PARITÉ

Le « bit de parité » est une méthode simple de détection d'erreur dans un message. Un principe utilisé dans d'autres situations, mais qui n'est pas infallible !



À l'instar du bit de parité, les deux derniers chiffres du numéro de Sécurité sociale constituent une clé de contrôle pour détecter une erreur.

Il arrive qu'un canal de communication soit imparfait et que le message reçu par le destinataire soit un peu différent de celui envoyé par l'émetteur. Une façon de corriger de telles erreurs consiste à tripler chaque lettre et à envoyer, par exemple, le message «pppooouuurrrlllaaassccciieennncceee». Ainsi, quand une lettre est altérée lors de la transmission et que le message devient «pppooauurrrlllaaassccciieennncceee», il est facile de reconstituer le message original, car le triplet «ooo» est probablement une altération du triplet «ooo», qui exprime la lettre «o». Le message n'est durablement altéré, ou rendu indéchiffrable, que si deux lettres du même triplet sont simultanément altérées, par exemple si «ooo» est altéré en «oaa» ou en «oab».

Cette technique implique de tripler la taille des messages à transmettre. Une solution moins coûteuse consiste à simplement doubler chaque lettre: «ppooourrrllaassccciieennncce». Dans ce cas, il est impossible de corriger les erreurs, mais il est possible de les détecter: si, par

exemple, le message reçu est «ppoauurrrllaassccciieennncce», nous ne savons pas quelle était la deuxième lettre du message original, mais nous voyons qu'elle a été altérée et nous pouvons la redemander à l'expéditeur. À nouveau, le message n'est durablement altéré que si deux lettres du même couple sont altérées, si «oo» par exemple est altéré en «aa».

L'idée elle-même existe depuis la nuit des temps

Mais même cette seconde méthode augmente trop la taille des messages. Une méthode plus économique consiste à associer un nombre de 0 à 25 à chaque lettre de l'alphabet, à ajouter les nombres correspondant à chaque lettre du message, à prendre le reste de la division de

ce nombre par 26 et à associer une lettre à ce nombre.

Par exemple, avec le message «pourlascience», nous obtenons $15 + 14 + 20 + 17 + 11 + 0 + 18 + 2 + 8 + 4 + 13 + 2 + 4 = 128$, dont le reste de la division par 26 est 24, qui correspond à la lettre «y». Nous exprimons alors ce message en ajoutant cette unique lettre – dite «de parité» – à la fin: «pourlasciencey». Pour vérifier que le message n'a pas été altéré, le destinataire n'a qu'à ôter cette dernière lettre, faire lui-même le même calcul et vérifier qu'il obtient, lui aussi, la lettre «y». Si ce n'est pas le cas, par exemple s'il reçoit le message «paurlasciencey», il détectera l'erreur. Ajouter ainsi une seule lettre à un message de 13 lettres n'augmente sa longueur que de 8% et permet de détecter une erreur, sauf quand deux altérations simultanées se compensent. Cette méthode est souvent utilisée dans un système binaire (avec un alphabet de deux lettres) – d'où le nom de «lettre de parité» ou «bit de parité».

Cette notion de «code correcteur d'erreur», c'est-à-dire l'introduction d'une redondance dans un message afin de détecter d'éventuelles erreurs de transmission, est souvent attribuée à Claude Shannon, qui l'a théorisée en 1948. Mais l'idée elle-même existe depuis la nuit des temps. Par exemple, dans l'expression des dates, nous pourrions écrire «le 1^{er} mai 2019», mais nous écrivons souvent «le mercredi 1^{er} mai 2019», où le jour de la semaine «mercredi» est redondant. Mais si le message est altéré en «le mercredi 2 mai 2019», «le mercredi 1^{er} juin 2019» ou «le mercredi 1^{er} mai 2020», ce jour de la semaine nous permet de détecter l'erreur, car ces dates correspondent respectivement à un jeudi, un samedi et un vendredi.

Mais il est un cas où cette méthode ne marche pas: le 25 mars 2019 est un lundi et le 25 février 2019 aussi, car le mois de février dure 28 jours, qui est un multiple de 7. Si nous nous trompons en notant un rendez-vous en mars, l'erreur ne sera pas détectée: en mars, méfiez-vous de la parité. ■

GILLES DOWECK est chercheur à l'Inria et membre du conseil scientifique de la Société informatique de France.

ABONNEZ-VOUS À POUR LA SCIENCE

3 FORMULES
AU CHOIX

	FORMULE DÉCOUVERTE	FORMULE PAPIER + HORS-SÉRIE	FORMULE INTÉGRALE
Le magazine papier (12 numéros par an)	✓	✓	✓
Le hors-série papier (4 numéros par an)		✓	✓
L'accès en ligne illimité à pourlascience.fr			✓
L'édition numérique du magazine (12 numéros par an)			✓
L'édition numérique du hors-série (4 numéros par an)			✓
L'accès aux archives numériques depuis 1996			✓
VOTRE TARIF D'ABONNEMENT	59€ Au lieu de 82,80€	79€ Au lieu de 114,40€	99€ Au lieu de 174,40€
	29 % de réduction *	31 % de réduction *	43 % de réduction *

BULLETIN D'ABONNEMENT

À renvoyer accompagné de votre règlement à :

Pour la Science – Service abonnements – 19 rue de l'Industrie – BP 90053 – 67402 Illkirch Cedex – email: pourlascience@abopress.fr

PAG19STD



**OUI, je m'abonne
pour 1 an à**
POUR LA SCIENCE

1 / Je choisis ma formule (merci de cocher)



**FORMULE
DÉCOUVERTE**

• 12 n° du magazine papier

59€

Au lieu de 82,80€

DIA59E



**FORMULE PAPIER
+ HORS SÉRIE**

• 12 n° du magazine papier
• 4 Hors-série papier

79€

Au lieu de 114,40€

PIA79E



**FORMULE
INTÉGRALE**

• 12 n° du magazine papier
• 4 Hors-série papier
• Accès illimité aux contenus en ligne

99€

Au lieu de 174,40€

IIA99E

2 / J'indique mes coordonnées

☐ M. ☐ Mme

Nom: Prénom:

Adresse:

Code postal: Ville:

Téléphone:

Email: (indispensable pour la formule intégrale)

.....@.....

J'accepte de recevoir les offres de Pour la Science

☐ OUI ☐ NON

3 / Je choisis mon mode de règlement

☐ Par chèque à l'ordre de Pour la Science

☐ Carte bancaire

N°:

Date d'expiration: Clé (Les 3 chiffres au dos de votre CB):

Signature obligatoire:

* Réduction par rapport au prix de vente en kiosque et l'accès aux archives numériques. Durée d'abonnement: 1 an. Délai de livraison: dans le mois suivant l'enregistrement de votre règlement. Offre valable jusqu'au 31/12/2019 en France métropolitaine uniquement. Pour un abonnement à l'étranger, merci de consulter notre site <https://boutique.pourlascience.fr>. Photos non contractuelles.

Les informations que nous collectons dans ce bulletin d'abonnement nous aident à personnaliser et à améliorer les services que nous vous proposons. Nous les utiliserons pour gérer votre accès à l'intégralité de nos services, traiter vos commandes et paiements, et vous faire part notamment par newsletters de nos offres commerciales moyennant le respect de vos choix en la matière. Le responsable du traitement est la société Pour la Science. Vos données personnelles ne seront pas conservées au-delà de la durée nécessaire à la finalité de leur traitement. Pour la Science ne commercialise ni ne loue vos données à caractère personnel à des tiers. Les données collectées sont exclusivement destinées à Pour la Science. Nous vous invitons à prendre connaissance de notre charte de protection des données personnelles à l'adresse suivante: <https://rebrand.ly/charte-donnees-pls>. Conformément à la réglementation applicable (et notamment au Règlement 2016/679/UE dit «RGPD») vous disposez des droits d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation de vos données personnelles. Pour exercer ces droits (ou nous poser toute question concernant le traitement de vos données personnelles), vous pouvez nous contacter par courriel à l'adresse protection-donnees@pourlascience.fr.