Quand des mathématiciens veulent ouvrir une porte...

Soit $n \geq 2$ un entier. On suppose que les "chiffres" utilisés sont $1, 2, \cdots, n$.
Le code initial choisi est appelé *la combinaison.*

Il existe des ensembles de codes qui permettent d'ouvrir la porte quelle que soit la combinaison choisie (par exemple, l'ensemble de tous les codes possibles). Un tel ensemble de codes sera dit *n-universel*, et on peut alors considérer un ensemble n-universel qui contient un nombre minimal, noté $f(n)$, de codes.
Par exemple, on a $f(2) = 2$ et $f(3) = 4$ (comme prouvé dans l'exercice).

Ce qui suit à pour objet de donner des évaluations plus ou moins précises de $f(n)$ par des arguments divers, et en tenant compte, ou pas, du niveau d'un candidat aux olympiades académiques. La dernière approche, de loin la plus efficace, peut être rendue élémentaire (il suffit d'alléger un peu le formalisme et raisonner modulo n plutôt que parler de $\mathbb{Z}/n\mathbb{Z}$ suffit amplement).

I - Où l'on n'utilise que des arguments olympiques.

Propriété 1. Pour tout $n \geq 2$, on a

$$f(n+1) \leq 2f(n).$$

Preuve.
On considère un ensemble n-universel S_n (et donc contenant $f(n)$ codes, les chiffres autorisés étant $1, 2, \cdots, n$). Pour les chiffres $1, 2, \cdots, n+1$, on construit alors l'ensemble S_{n+1} qui contient les $2f(n)$ codes suivants :
a) les $f(n)$ codes de S_n auxquels on ajoute à chacun $n+1$ à la fin ;
b) les $f(n)$ codes du a) en échangeant, pour chacun, les premiers et derniers chiffres (ainsi le $n+1$ passe au début).

Soit $C = a_1, a_2, \cdots, a_{n+1}$ la combinaison.
- Si $a_{n+1} \neq n+1$: il existe donc $k \leq n$ pour lequel $a_k = n+1$. Echangeons alors a_k par a_{n+1}, ce qui fournit une combinaison C' dont les n premiers chiffres forment une permutation de $1, 2, \cdots, n$. Puisque l'on part d'un ensemble n-universel, parmi nos $f(n)$ codes de S_n, il en existe un, disons c, qui ne coïncide en aucune place avec les n premiers chiffres de C' (il faut pouvoir ouvrir la porte pour une combinaison de longueur n formé par les n premiers chiffres de C'), et donc en aucune place avec les n premiers chiffres de C (puisque $a_k = n+1$ n'est pas un chiffre possible de c). Le code de longueur $n+1$ construit au a) à partir de c an lui ajoutant $n+1$ à la fin ne coïncide alors en aucune place avec C (puisque C ne se termine pas par $n+1$ dans le cas présent) et permet d'ouvrir la porte.

- Si $a_{n+1} = n+1$: les n premiers chiffres de C forment alors une permutation de $1, 2, \cdots, n$ et il doit exister un code c de S_n qui ne coïncide en aucune place avec ces n premiers chiffres de C. Si, conformément à la construction du b), on remplace le premier chiffre c_1 de c par $n+1$

et qu'on place c_1 à la fin de c, ce nouveau code de longueur $n+1$ ne coïncide en aucune place avec C, et permet donc d'ouvrir la porte.

Ainsi, l'ensemble S_{n+1} est $(n+1)$-universel. Par minimalité de $f(n+1)$, on a donc $f(n+1) \leq 2f(n)$.

Propriété 2. Pour tout $n \geq 3$, on a

$$f(n+1) \leq 2f(n-1).$$

Preuve.
Comme ci-dessus, notons $C = a_1, a_2, \cdots, a_{n+1}$ la combinaison lorsque les chiffres autorisés sont $1, 2, \cdots, n+1$.
Soit S_{n-1} un ensemble $(n-1)$-universel (les chiffres autorisés étant donc $1, 2, \cdots, n-1$).
On construit l'ensemble S_{n+1} qui contient les $2f(n-1)$ codes suivants :
a) tous les codes de S_{n-1} auxquels on ajoute à chacun n et $n+1$, dans cet ordre à la fin.
b) tous les codes de S_{n-1} auxquels on ajoute à chacun $n+1$ et n, dans cet ordre à la fin.

- Si $a_n \notin \{n, n+1\}$ et $a_{n+1} \notin \{n, n+1\}$: il existe donc $p, q \leq n-1$ tels que $a_p = n$ et $a_q = n+1$. On considère alors le code C' formé à partir de C en échangeant a_p et a_n, ainsi que a_q et a_{n+1}. Les $n-1$ premiers chiffres de C' forment une permutation de $1, 2, \cdots, n-1$ et il existe donc un code $c = b_1, b_2, \cdots, b_{n-1}$ de S_{n-1} qui ne coïncide en aucune place avec les $n-1$ premiers chiffres de C'. En particulier, $b_i \neq a_i$ pour $i \neq p, q$. Comme $b_p < n$, on a aussi $b_p \neq a_p$. De même, $b_q \neq a_q = n+1$. Si l'on pose $b_n = n$ et $b_{n+1} = n+1$, on a donc $b_n \neq a_n$ et $b_{n+1} \neq a_{n+1}$, ce qui assure que le code de S_{n+1} construit à partir de c selon a) ne coïncide en aucune place avec C et permet d'ouvrir la porte.

- Si $a_n = n+1$ et $a_{n+1} = n$: on considère un code c de S_{n-1} qui ne coïncide en aucune place avec les $n-1$ premiers chiffres de C (qui forment une permutation de $1, 2, \cdots, n-1$). Le code de S_{n+1} formé à partir de c selon a) ne coïncide en aucune place avec C et permet donc d'ouvrir la porte.

- Si $a_n = n$ et $a_{n+1} = n+1$: on reprend le raisonnement ci-dessus, mais en complétant le code c de S_{n-1} selon b).

- Si $a_n = n$ et $a_{n+1} \neq n+1$: il existe donc $p \leq n-1$ tel que $a_p = n+1$. On considère à nouveau le code C' obtenu à partir de C en échangeant a_p et a_{n+1}. Les $n-1$ premier chiffres de C' forment une permutation de $1, 2, \cdots, n-1$ et il existe donc un code $c = b_1, b_2, \cdots, b_{n-1}$ de S_{n-1} qui ne coïncide en aucune place avec les $n-1$ premiers chiffres de C'. Selon b), en posant $b_n = n+1$ et $b_{n+1} = n$, on obtient ainsi un code de S_{n+1}. Comme ci-dessus, il est facile de vérifier que $b_i \neq a_i$ pour $i \neq p, n+1$, que $b_p < n < n+1 = a_p$ et que $b_{n+1} = n > a_{n+1}$. Ainsi, ce code permet d'ouvrir la porte.

- Si $a_p \neq n$ et $a_{n+1} = n+1$: le raisonnement est analogue à celui du cas précédent, mais en échangeant a_n et a_p, où $a_p = n$.

Ainsi, dans tous les cas, l'un des codes de S_{n+1} permet d'ouvrir la porte, ce qui prouve que S_{n+1} est $(n+1)$-universel. Par minimalité de $f(n+1)$, on a donc $f(n+1) \leq 2f(n-1)$.

Remarques. - Puisque $f(2) = 2$, on déduit facilement des deux propriétés que

$$f(n) \leq 2^{[\frac{n+1}{2}]}$$

où [..] désigne la partie entière.
Comme on le verra après cette majoration n'est franchement pas optimale.

- Si l'on revient aux questions posées, sans faire de constructions générales (juste $n = 3, 4, 5$) l'inégalité ci-dessus conduit toutefois à $f(3) \leq 4$ (et on a l'égalité dans ce cas), mais aussi $f(4) \leq 4$. Ainsi que $f(5) \leq 8$ et $f(6) \leq 8$.
Plus précisément, les codes $1, 2$ et $2, 1$ forment un ensemble 2-universel. Si on explicite les constructions ci-dessus, on trouve que :

Un ensemble 3-universel est formé par

$$1, 2, 3 \text{ et } 2, 1, 3 \text{ et } 3, 2, 1 \text{ et } 3, 1, 2.$$

Un ensemble 4-universel est formé par

$$1, 2, 3, 4 \text{ et } 2, 1, 3, 4 \text{ et } 1, 2, 4, 3 \text{ et } 2, 1, 4, 3.$$

Un ensemble 5-universel est formé par

$$1, 2, 3, 4, 5 \text{ et } 2, 1, 3, 4, 5 \text{ et } 1, 2, 4, 3, 5 \text{ et } 2, 1, 4, 3, 5,$$

$$5, 2, 3, 4, 1 \text{ et } 5, 1, 3, 4, 2 \text{ et } 5, 2, 4, 3, 1 \text{ et } 5, 1, 4, 3, 2$$

Un ensemble 6-universel est formé par

$$1, 2, 3, 4, 5, 6 \text{ et } 2, 1, 3, 4, 5, 6 \text{ et } 1, 2, 4, 3, 5, 6 \text{ et } 2, 1, 4, 3, 5, 6,$$

$$1, 2, 3, 4, 6, 5 \text{ et } 2, 1, 3, 4, 6, 5 \text{ et } 1, 2, 4, 3, 6, 5 \text{ et } 2, 1, 4, 3, 6, 5.$$

II - Deux approches différentes sans préoccupation de niveau.

A - L'approche combinatoire (P. Bornsztein).

Moins efficace que celle qui sera présentée au B dans le cas présent, elle a tout de même le mérite de montrer l'efficacité de certains outils classiques, en particulier la méthode probabiliste découverte par Erdös.

Soit $n \geq 1$. Les chiffres autorisés sont $1, 2, \cdots, n$.
Soit c un code.
On note u_n le nombre de codes qui ne coïncident en aucune place avec c.

On prouve classiquement (voir le calcul du nombre de *dérangements*. Par exemple, on a facilement $u_1 = 0, u_2 = 1$ et $u_{n+2} = (n+1)(u_{n+1} + u_n)$ pour tout $n \geq 1$) que $u_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$ pour tout $n \geq 1$.
On note en particulier que u_n est indépendant de c (évident par symétrie des rôles entre les codes) et qu'asymptôtiquement $u_n \sim \frac{n!}{e}$.

Soit G un graphe fini simple et non orienté, à N sommets. On rappelle qu'un ensemble S de sommets est dit *dominant* si chaque sommet de G est dans S ou adjacent à un sommet de S.

Théorème (Arnautov, 1974).

Si le degré minimal dans G est $k > 1$ alors G contient un ensemble dominant qui ne contient pas plus de $N \times \frac{1 + \ln(k+1)}{k+1}$ sommets.

Preuve.
On considère une pièce qui fait Pile avec une probabilité $p = \frac{\ln(k+1)}{k+1}$.
On construit alors aléatoirement un ensemble A de sommets de G : pour chaque sommet x de G, indépendamment de ce qui a été décidé pour les autres, on lance la pièce. Le sommet x est choisi pour appartenir à A si et seulement si on a obtenu Pile au lancer qui le concerne. Ainsi, pour chaque sommet, la probabilité d'appartenir à A est p.
Une fois un tel ensemble A construit, on considère l'ensemble B des sommets de G qui ne sont ni dans A ni adjacents à un sommet de A. Il est clair que l'ensemble $S = A \cup B$ est un ensemble dominant de G. La question est de déterminer le nombre moyen d'éléments d'un tel ensemble.

Puisque chaque sommet de G appartient à A avec une probabilité p, indépendamment des autres, la variable aléatoire $|A|$ suit donc la loi binomiale de paramètres N et p. Ainsi, on a on a $E(|A|) = Np$.
La variable aléatoire $|B|$ est la somme de N variables de Bernoulli (chacune indiquant si le sommet associé est dans B ou pas). Or, le sommet x appartient à B si et seulement si x et aucun de ses voisins dans G n'appartiennent à A. Puisque x est de degré au moins k, cela se produit avec une probabilité qui ne dépasse pas $(1-p)^{k+1}$. De l'inégalité classique $1-p \leq e^{-p}$, on déduit que $(1-p)^{k+1} \leq e^{-p(k+1)}$. Par linéarité de l'espérance, il vient alors $E(|B|) \leq Ne^{-p(k+1)}$, puis $E(|A| + |B|) \leq Np + Ne^{-p(k+1)} = N \times \frac{1+\ln(k+1)}{k+1}$.

Puisque la valeur moyenne de $|A| + |B|$ ne dépasse pas $N \times \frac{1+\ln(k+1)}{k+1}$, c'est donc qu'il est réalisable, par une telle procédure aléatoire, d'obtenir un ensemble S dominant ne contenant pas plus de $N \times \frac{1+\ln(k+1)}{k+1}$ éléments, et donc qu'un tel ensemble S existe ! Cela conclut la preuve du théorème.

On considère alors le graphe G dont les sommets sont les codes, deux reliés par une arête si et seulement s'ils ne coïncident en aucune place. Il y a donc $n!$ sommets, chacun de degré u_n. De plus, un code x permet d'ouvrir la porte si et seulement si la combinaison est un code adjacent à x dans G.
Trouver un ensemble S dominant pour G revient alors à déterminer un ensemble de codes qui permettent d'ouvrir la porte quelle que soit la combinaison du moment qu'elle n'est pas dans S.

Or, si l'on connaît l'ensemble S, pour chaque sommet x dans S, il suffit de choisir un sommet de G adjacent à x. Cela ajoute au plus $|S|$ nouveaux codes qui, avec ceux qui sont dans S, permettent cette fois d'ouvrir la porte dans tous les cas. On comprend alors l'intérêt qu'on peut avoir à trouver un ensemble dominant qui contiendrait le moins possible d'éléments.
Or, d'après le théorème ci-dessus, G possède justement un ensemble S dominant qui ne contient pas plus de $s = n! \times \dfrac{1+\ln(u_n+1)}{u_n+1}$ éléments.
Bon, évidemment, dit comme ça, cela ne semble pas super impressionnant, mais si on se souvient que $u_n \sim \frac{n!}{e}$ et qu'on utilise la formule de Stirling, on voit facilement que $s \sim en\ln(n)$.
Ainsi, on peut assurer l'ouverture de la porte en au plus $2s$ essais (et donc que $f(n) \leq 2s$), avec $2s \sim 2en\ln(n)$.

Cette borne, sous-quadratique, rend celle du I un peu dérisoire...

B - L'approche algébrique (V. Jugé).

Soit $n \geq 2$ un entier et $\mathfrak{S}_n$ l'ensemble des permutations de $\mathbb{Z}/n\mathbb{Z}$. Ainsi $f(n)$ est le cardinal minimal d'un ensemble $E \subseteq \mathfrak{S}_n$ tel que

$$\forall \sigma \in \mathfrak{S}_n, \exists \tau \in E, \forall i \in \mathbb{Z}/n\mathbb{Z}, \sigma(i) \neq \tau(i).$$

Si x est un réel, on note $\lfloor x \rfloor$ la partie entière de x, et $\lceil x \rceil$ le plus petit entier supérieur ou égal à x.

Propriété 3. Pour tout $n \geq 2$, on a

$$f(n) \leq n \text{ si } n \text{ est pair, et } f(n) \leq \lfloor 3n/2 \rfloor \text{ si } n \text{ est impair.}$$

Preuve.
Pour tout $k \in \{1, \ldots, n\}$, on pose $T_k : i \mapsto k+i$. Ensuite, pour tout $\ell \in \{1, \ldots, \lceil n/2 \rceil\}$, on pose

$$\begin{array}{rlll} U_\ell : & 2\ell - 1 & \mapsto 2\ell \\ & 2\ell & \mapsto 2\ell - 1 \\ & i & \mapsto i \text{ si } i \notin \{2\ell-1, 2\ell\}. \end{array}$$

Soit $\sigma \in \mathfrak{S}_n$ une permutation. On dit qu'un ensemble $S \subseteq \mathfrak{S}_n$ est σ-aveugle s'il existe $\tau \in S$ tel que $\sigma(i) \neq \tau(i)$ pour tout $i \in \mathbb{Z}/n\mathbb{Z}$. On pose alors $E = \{T_k : 1 \leq k < n\}$ et $F = \{U_\ell : 1 \leq \ell \leq \lceil n/2 \rceil\}$.

Supposons d'abord que n est pair et que $E \cup \{T_n\}$ n'est pas σ-aveugle. Alors, pour tout $k \in \mathbb{Z}$, il existe $i \in \mathbb{Z}/n\mathbb{Z}$ tel que $\sigma(i) = k + i$ et, par principe des tiroirs, i est nécessairement unique. Par conséquent,

$$\frac{n(n+1)}{2} \equiv \sum_{i=1}^{n} i \equiv \sum_{i=1}^{n} \sigma(i) \equiv \left(\sum_{i=1}^{n} i\right) + \left(\sum_{k=1}^{n} k\right) \equiv n(n+1) \equiv 0 \pmod{n},$$

et donc $\frac{n+1}{2} \in \mathbb{Z}$, ce qui est impossible car n est pair. C'est pourquoi $f(n) \leq n$ si n est pair.

Supposons maintenant que n est impair et que E n'est pas σ-aveugle. Pour tout $k \in \{1, \dots, n-1\}$, soit i_k le plus petit élément de $\{1, \dots, n\}$ tel que $\sigma(i_k) = i_k + k$. Enfin, soit i_∞ l'unique élément de $\{1, \dots, n\} \setminus \{i_1, \dots, i_{n-1}\}$. Alors $\frac{n+1}{2} \in \mathbb{Z}$, donc

$$0 \equiv \frac{n(n+1)}{2} \equiv \sum_{i=1}^{n} i \equiv \sum_{i=1}^{n} \sigma(i) \equiv \left(\sum_{i=1}^{n} i\right) + \left(\sum_{k=1}^{n-1} k\right) + (\sigma(i_\infty) - i_\infty) \equiv n^2 + (\sigma(i_\infty) - i_\infty) \pmod{n},$$

ce qui montre que $\sigma(i_\infty) = i_\infty$ et donc que $E \cup \{T_n\}$ n'est pas σ-aveugle non plus : pour tout $k \in \mathbb{Z}$, il existe en fait un unique $i_k \in \mathbb{Z}/n\mathbb{Z}$ tel que $\sigma(i_k) = k + i_k$.

Soit $\ell \in \{1, \dots, \lceil n/2 \rceil\}$ tel que $i_0 \in \{2\ell - 1, 2\ell\}$, et soit $i_0' = U_\ell(i_0) = 4\ell - 1 - i_0$, Alors $\sigma(i_0) = i_0 \neq i_0' = U_\ell(i_0)$ et $\sigma(i_0') \neq i_0 = U_\ell(i_0')$. De surcroît, pour $j \notin \{2\ell - 1, 2\ell\}$, on a également $\sigma(j) \neq j = U_\ell(j)$. Donc $\{U_\ell\}$ et $E \cup F$ sont σ-aveugles. C'est pourquoi $f(n) \leq \lfloor 3n/2 \rfloor$ si n est impair.

Propriété 4. Pour tout $n \geq 2$, on a

$$\lfloor n/2 \rfloor < f(n).$$

Preuve.
En effet, soit $E = \{P_1, \dots, P_m\} \subseteq \mathfrak{S}_n$ un ensemble de cardinal $m \leq \lfloor n/2 \rfloor$. On construit des suites $a_1, \dots, a_m$ et $b_1, \dots, b_m$ comme suit : pour tout $k \in \{1, \dots, m\}$, on choisit $a_k \in \mathbb{Z}/n\mathbb{Z} \setminus \{a_1, \dots, a_{k-1}\}$ et $b_k \in \mathbb{Z}/n\mathbb{Z} \setminus \{b_1, \dots, b_{k-1}\}$ tels que $P_k(a_k) = b_k$. Notons que c'est toujours possible, puisque

$$|\mathbb{Z}/n\mathbb{Z}| - |\{a_1, \dots, a_{k-1}\}| - |\{b_1, \dots, b_{k-1}\}| = n - 2(k-1) > n - 2m \geq 0.$$

On choisit alors une permutation $\sigma \in \mathfrak{S}_n$ telle que $\sigma : a_k \mapsto b_k$ pour $k \in \{1, \dots, m\}$. Il est alors clair que $\sigma(a_k) = P_k(a_k)$ pour tout $k \in \{1, \dots, m\}$. cela montre bien que E n'est pas un des ensembles recherchés, et donc que $f(n) > \lfloor n/2 \rfloor$.

Remarques. On en déduit que $f(5) \leq 7$ et $f(6) \leq 6$. En particulier :

- Un ensemble 5-universel est formé par les quatre permutations circulaires de $1, 2, 3, 4, 5$ autres que $1, 2, 3, 4, 5$, auxquelles on ajoute les trois codes

$$2, 1, 3, 4, 5 \text{ et } 1, 2, 4, 3, 5 \text{ et } 5, 2, 3, 4, 1.$$

- Un ensemble 6-universel est formé par les 6 permutations circulaires de $1, 2, 3, 4, 5, 6$.

Pour finir, notons que nous n'avons pas trouvé d'argument pour prouver que $f(n)$ est une fonction croissante de n, même si le contraire serait surprenant.