Combien de fois faut-il battre un jeu de cartes ?

Ce texte est tiré d'un article de D. Bayer et P. Diaconis "Trailing the dovetail shuffle to its lair" Ann. Appl. Prob. 1992, vol 2, No 2, 294-313.

1 Introduction

La méthode la plus utilisée pour battre un paquet de cartes consiste à couper le paquet en deux, puis à mélanger les deux parties en alternant les cartes. J'appellerai ces deux opérations *la coupe* et *le mélange.*

Lorsqu'on suit la méthode rigoureusement, on coupe le paquet en deux parties égales et on alterne exactement les cartes de chaque partie. Si on fait ça avec un paquet de 32 cartes, en prenant soin de laisser toujours la première carte sur le dessus du paquet, on s'aperçoit qu'au bout de 5 battages de cartes, on est revenu dans la position intiale. La règle générale est que la carte en position k arrive en position $2k-1$ si $k \leq 16$ et en position $2k-32$ si $k \geq 17$. Par exemple voici les positions successives de la sixième carte : 6, 11, 21, 10, 19, 6. On est bien revenu en position initiale en 5 coups.

Plus généralement, avec un jeu de 2^n cartes, cette méthode permet de revenir dans la position initiale en n battages. Exercice : démontrer ce résultat ! (solution en annexe A).

Ce fait est à la base d'un tour de cartes spectaculaire, où le magicien retrouve une carte dans un paquet que tout le monde croit bien mélangé. Évidemment, pour arriver à couper un paquet *exactement* au milieu puis à le "mélanger" parfaitement et cela 5 fois de suite, il faut une dextérité hors du commun, et bien peu de personnes au monde sont capable d'exécuter ce tour.

En général, quand on bat un paquet, après la coupe les deux parties ne sont qu'approximativement égales et lors du mélange les deux paquets n'alternent pas exactement. Heureusement d'ailleurs, car le but de l'opération est que l'on ne puisse pas deviner la position des cartes une fois le paquet battu, même si on la connaissait avant. Cela nous amène à la question principale de l'exposé : combien de fois doit on battre le paquet pour qu'il soit bien mélangé ? L'intérêt de la question est évident, au moins pour les joueurs de cartes ou les patrons de casinos. En effet, si l'on ne bat pas assez les cartes, il reste dans le jeu un peu d'information provenant de la distribution précédente, que certains joueurs pourraient exploiter pour deviner les cartes, comme par exemple dans le tour de magie qui est expliqué plus bas. Évidemment, plus on bat les cartes et plus on lutte contre cet effet, mais d'un autre coté, si l'on bat les cartes pendant trop longtemps, cela ralentit le jeu (et donc diminue les gains du casino !), il est par conséquent utile de savoir à partir de combien de battages le jeu est suffisamment mélangé.

Pour répondre à cette question il faut disposer d'un modèle mathématique qui décrive la façon dont on bat les cartes, puis arriver à en faire une analyse assez précise. Le modèle dont il sera question ici a été proposé par les mathématiciens Gilbert et Shannon en 1955, et indépendamment par Reeds en 1981, et il a été testé par P. Diaconis qui a vérifié qu'il décrivait de façon réaliste le battage des cartes pratiqué par exemple dans les casinos.

2 Modèle probabiliste

2.1 La coupe

On dispose d'un paquet de n cartes, que l'on commence par couper en deux paquets de j et $n-j$ cartes, le nombre j étant choisi entre 0 et n, avec la loi *binomiale* c'est à dire que l'on a une probabilité $\frac{1}{2^n}\frac{n!}{k!(n-k)!}$ que j soit égal à k.

La formule du binôme nous dit que $\sum_{k=0}^{n} \frac{1}{2^n}\frac{n!}{k!(n-k)!} = 1$ donc la somme des probabilités fait bien 1. Si on trace le graphe de cette probabilité en fonction de k, on observe une courbe "en cloche", dont le maximum se situe en $n/2$, et dont la plus grande partie se trouve concentrée entre $n/2-\sqrt{n}$ et $n/2+\sqrt{n}$.

Cela modélise de façon raisonnable ce que peut faire un batteur de carte d'une adresse moyenne en essayant de couper le paquet en deux parties égales. Une autre raison de choisir cette distribution est la suivante : si on choisit une partie de $\{1,\dots,n\}$ au hasard, toutes les parties étant équiprobables, alors la probabilité de tirer une partie à k éléments est $\frac{1}{2^n}\frac{n!}{k!(n-k)!}$.

2.2 Le mélange

Ensuite, une fois que le paquet a été coupé, on mélange les deux parties de la façon suivante : supposons qu'il reste a_1 cartes dans le premier paquet et a_2 dans le second, alors on choisit la carte du dessous du premier paquet avec probabilité $\frac{a_1}{a_1+a_2}$, ou bien celle du second avec probabilité $\frac{a_2}{a_1+a_2}$, et on continue ainsi, avec a_1-1 cartes dans le premier et a_2 dans le second, ou bien a_1 dans le premier et a_2-1 dans le second suivant les cas, jusqu'à épuisement des deux paquets. Là encore ce choix semble raisonnable, car plus l'un des paquets est gros par rapport à l'autre, plus on a de chance de choisir la carte de ce paquet.
Exemple : Au départ, les deux tas contiennent respectivement $a_1 = j$ et $a_2 = n-j$ cartes. La probabilité de choisir la carte du premier tas est donc $\frac{j}{n}$, celle de prendre la carte du deuxième tas $\frac{n-j}{n}$. Supposons que nous ayons pris une carte du premier tas au premier coup. Les tas contiennent alors $j-1$ et $n-j$ cartes. La probabilité de reprendre la carte du dessous du premier tas est alors $\frac{j-1}{n-1}$, celle de prendre la carte du deuxième tas $\frac{n-j}{n-1}$. Et ainsi de suite.

2.3 Battages et permutations

On peut interpréter un battage de cartes comme une *permutation* du jeu de cartes. Dans la suite j'appellerai les cartes par des numéros $1, 2, 3, ..., n$, plutôt que par leurs valeurs faciales habituelles, avec trèfle, pique, etc..., car cela rend les arguments plus aisés à suivre, mais cela ne change rien à la nature des choses. Une permutation peut se représenter sous la forme (ici avec $n = 10$)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 6 & 7 & 1 & 2 & 8 & 3 & 9 & 4 & 10 \end{pmatrix}$$

La première ligne représente l'ordre des cartes avant le battage, et la seconde ligne l'ordre après battage. Pour un jeu de n cartes, il y a $n!$ permutations possibles. Pour un jeu de 52 cartes, on a ainsi 52! possibilités, soit :

$$80658175170943878571660636856403766975289505440883277824000000000000$$

un nombre gigantesque. Si on voulait écrire tous les ordre possibles d'un jeu de 52 cartes, non seulement cela prendrait des milliards d'années (au bas mot), mais il n'y aurait sans doute pas assez de matière dans l'univers pour le faire. Or, comme nous le verrons, un seul battage ne permet de réaliser que 2^n permutations, or ici :

$$2^{52} = 4503599627370496$$

un nombre très grand mais néanmoins beaucoup plus petit que 52!. Même avec 4 battages, on obtiendra moins de 2^{208} permutations, soit

$$411376139330301510538742295639337626245683966408394965837152256$$

ce qui est toujours beaucoup plus petit que 52! (environ 2 millions de fois plus petit).

Il faudra donc nécessairement plus de battages pour espérer obtenir une proportion satisfaisante de toutes les permutations possibles, et une distribution suffisamment aléatoire des cartes. Nous allons voir comment quantifier l'aléas contenu dans le résultat de plusieurs battages de cartes.

3 Répartition des configurations après m battages

3.1 Le théorème

Pour le moment je vais donner une formule explicite pour la probabilité d'obtenir une configuration π du paquet de cartes au bout de m battages. On suppose que dans la configuration initiale les cartes sont dans l'ordre $123...n$, alors la configuration π n'est autre que l'ordre des cartes obtenu après m battages. Dans l'énoncé le symbole C_p^q désigne le coefficient du binôme $\mathrm{C}_p^q = \dfrac{p!}{q!(p-q)!}$ si $q \leq p$, et vaut 0 sinon.

Théorème : *La probabilité pour que le paquet se trouve dans l'état π après m battages est égale à*

$$p_n(\pi) = \frac{1}{2^{mn}} \mathrm{C}^n_{2^m+n-r}$$

où r est le nombre de suites montantes dans π.

3.2 Un joli tour de cartes

3.2.1 Principe du tour

Pour comprendre l'énoncé du théorème il faut savoir ce qu'est une suite montante. Pour l'expliquer je vais décrire un tour de cartes inventé au début du siècle par les magiciens Williams et Jordan. Dans ce tour, le magicien tend un paquet de cartes à un spectateur, puis il tourne le dos au public et il demande au spectateur de battre deux fois le paquet, puis de le couper encore une fois, et de prendre la carte au dessus du paquet. Le spectateur note la valeur de la carte, puis il la remet où il veut dans le paquet et le rebat. Alors le magicien se retourne, étale les cartes devant lui, face dessus, et après les avoir intensément scrutées, désigne la carte que le spectateur avait sortie.

Comment fonctionne le tour ? Le magicien connaît l'ordre des cartes dans le paquet avant le battage, par exemple cet ordre est l'ordre naturel $1, 2, 3, ..., n$. L'idée de base est que battre trois fois le jeu laisse suffisamment de structures invariantes dans la distribution des cartes, ce qui est vrai si le nombre de cartes est suffisant (en général on prend un jeu de 52 cartes), et que l'on peut retrouver la carte du spectateur en comptant les suites montantes.

3.2.2 Suites montantes

Une suite montante est une sous-suite maximale constituée de nombres successifs. Toute permutation de $\{1, \ldots, n\}$ peut être décomposée de façon unique en une juxtaposition de suites montantes, par exemple si on considère la permutation de 16 chiffres

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 14 & 3 & 4 & 15 & 6 & 9 & 10 & 5 & 11 & 1 & 7 & 12 & 2 & 8 & 16 & 13 \end{pmatrix}$$

alors les sous-suites montantes sont : $(1, 2)$, $(3, 4, 5)$, $(6, 7; 8)$, $(9, 10, 11, 12, 13)$ et $(14, 15, 16)$. Pour trouver les suites montantes d'une permutation, on procède comme ceci : on commence par repérer la carte 1. Si la carte 2 est avant 1, alors (1) est une suite montante, sinon on cherche 3. Si 3 est avant 2, alors (1,2), est une suite montante, sinon on cherche 4, et ainsi de suite jusqu'à épuisement du paquet. Lorsqu'on bat une première fois les cartes qui sont dans la position initiale $123...n$, on obtient deux suites montantes $1, 2, ..., k$ et $k + 1, k + 2...n$, où k désigne le numéro de la carte où on a effectué la coupe (sauf dans le cas extrême où on a remis le paquet dans sa position initiale, auquel cas il y a une seule suite montante).

En général, au début, chaque battage multiplie par deux le nombre de suites montantes dans le paquet, donc au bout de 3 battages il y a 8 suites montantes, qui contiennent en moyenne 52/8= 6,5 cartes.

3.2.3 Explication du tour

La manipulation du spectateur, qui extrait une carte pour la replacer ailleurs, crée dans la plupart des cas une neuvième suite montante, qui consiste en cette unique carte. Le magicien n'a plus alors qu'à identifier les suites montantes dans le paquet pour trouver la carte recherchée (en fait l'analyse est un peu plus compliquée car on autorise le spectateur à faire une coupe supplémentaire mais j'ignore ici cette complication).

Le tour ne marche pas à tous les coups, c'est facile à voir, car une suite montante contenant une seule carte peut être créée par hasard lors des battages, ce qui peut tromper le magicien, ou bien le spectateur peut remettre la carte qu'il a choisie, à l'endroit où il l'a prise, ce qui détruit le principe du tour. Paradoxalement, en général le spectateur aura tendance, pour essayer d'embrouiller le magicien, à remettre la carte loin de l'endroit où il l'a prise, avec l'effet exactement inverse de celui recherché ! De même, plus il y a de cartes dans le jeu, plus il est rare qu'une suite montante à une seule carte soit créée, et donc plus le tour a de chances de marcher. Une simulation sur ordinateur a montré que, sur un million d'essais, avec un jeu de 52 cartes, le truc permet de deviner la bonne carte dans 84% des cas. Si on s'autorise une second essai en cas d'échec, alors le pourcentage de succès passe à 94%.

3.3 Démonstration du théorème

Voyons maintenant comment on démontre le Théorème. Tout d'abord, examinons de plus près ce qui se passe après un seul battage.

Supposons que la coupe ait produit deux tas de j et $n-j$ cartes, numérotés 1 et 2. Ceci se produit avec la probabilité $\dfrac{1}{2^n}\dfrac{n!}{j!(n-j)!}$.

Pour effectuer le mélange on choisit chaque carte successivement dans l'un des deux paquets. Les choix successifs sont notés $i_1, i_2, ..., i_n$, où à chaque fois $i_k \in \{1,2\}$ désigne l'un des deux paquets. La probabilité d'un tel mélange est

$$\frac{x_1}{n}\frac{x_2}{n-1}\cdots\frac{x_{n-1}}{2}\frac{x_n}{1}$$

où x_k désigne le nombre de cartes qui restent dans le i_k^{eme} paquet à la k^{eme} étape.

Exemple : La probabilité de tirer toues les cartes du premier tas, puis toues celles du secont est

$$\frac{j}{n}\frac{j-1}{n-1}\cdots\frac{1}{n-j+1}\frac{n-j}{n-j}\cdots\frac{1}{1}$$

On voit facilement que, quel que soit le mélange, les nombres $j, j-1, j-2, ..., 1$ et $n-j, n-j-1, ..., 1$ apparaissent chacun une fois au numérateur, donc le produit ne dépend pas de la suite des i_k, et vaut $\dfrac{j!(n-j)!}{n!}$.

Finalement, tous les résultats possibles avec une coupe au niveau j sont donc équiprobables, de probabilité :

$$\frac{1}{2^n}\frac{n!}{j!(n-j)!}\frac{j!(n-j)!}{n!} = \frac{1}{2^n}$$

Ce résultat donne une autre justification au choix de la loi binomiale pour j : il conduit à l'équiprobabilité de tous les choix possibles, indépendamment de la taille des paquets après la coupe.

Il est possible que l'on obtienne la même permutation avec des nombres j_1 et j_2 différents. En fait cela ne peut se produire que si la permutation obtenue est la permutation identique :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \end{pmatrix}$$

et cela peut se produire exactement une fois pour chaque valeur de j. En effet, dans tous les autres cas, les deux suites montantes obtenues à l'issue de ce mélange sont, on l'a vu, de la forme $1, 2, \ldots, j$ et $j+1, \ldots, n$. C'est-à-dire qu'elles caractérisent l'entier j.

Si nous résumons ce que nous avons obtenu, nous voyons que chaque permutation avec 2 suites montantes peut être réalisée avec probabilité $\frac{1}{2^n}$, alors que la permutation identique, qui a une seule suite montante peut-être réalisée une fois pour chaque valeur de j $(0 \leq j \leq n)$, ce qui fait qu'elle apparaît avec la probabilité $\frac{(n+1)}{2^n}$.

On vérifie bien ainsi le Théorème dans le cas $m = 1$: dans ce cas, les seules valeurs possibles de r sont $r = 1$ et $r = 2$.

L'analyse du cas général est un peu plus compliquée. On remarque que l'on peut faire d'abord toutes les coupes avant de faire les mélanges, sans changer la probabilité finale de tirer une permutation donnée. Pour cela, après la première coupe, au lieu de mélanger les deux paquets, recoupons les chacun en deux parties, puis encore les quatre paquets obtenus en deux parties, etc... et cela m fois en tout, de sorte que l'on a obtenu 2^m parties. Rappelons que ces parties peuvent être éventuellement vides ! Alors on mélange ces parties de sorte que chacune des façons de faire le mélange a la même probabilité $\frac{1}{2^{nm}}$ (la démonstration du cas $m = 1$ se transpose, voir l´annexe B). On remarque aussi que le nombre de suites montantes après m battages est d'au plus 2^m.

On voit alors que ce procédé donne le même résultat que celui correspondant à faire m battages successifs. Maintenant, pour une permutation donnée, il faut calculer de combien de façons elle peut être réalisée avec ce procédé et multiplier par $\frac{1}{2^{nm}}$ pour obtenir sa probabilité d'apparaître. Quand on a effectué les m coupes on se retrouve avec 2^m paquets, chacun étant constitué de cartes qui se suivent. Cela revient en fait à avoir choisi les $2^m - 1$ positions où se trouvent les coupures entres les 2^m paquets. Supposons que les r suites montantes de la permutation que l'on veut obtenir soient données, par exemple $(1, 2, .., k_1); (k_1 + 1, ..., k_2); ...; (k_{r-1}+1, ..., n)$, alors nécessairement, on doit avoir coupé les paquets entre k_j et k_{j+1}. Cela fait $r-1$ coupes qui sont déterminées. Il reste alors $2^m - r$ coupes à effectuer, et on peut les faire où on veut dans $n+1$ positions. Une fois cela fait, on pourra retrouver la permutation voulue au moment du mélange, d'une seule façon. Cela fait en tout $\mathrm{C}^n_{2^m+n-r}$ possibilités, d'après le

Lemme : *Il y a* C_{p+q-1}^{p-1} *façons de placer* q *objets dans* p *cases (les objets sont indistinguables, et on peut en mettre plusieurs dans chaque case).*

La démonstration du lemme est simple : si j'appelle $a_1, a_2, \ldots, a_p$ le nombre d'objets dans les cases $1, 2, ..., p$, alors $\{a_1+1, a_1+a_2+2, \ldots, a_1+...+a_{p-1}+p-1\}$ forme un sous-ensemble à $p-1$ éléments de $\{1, 2, 3, \ldots, p+q-1\}$. Nous avons q objets au total, donc $a_1 + ... + a_p = q$, c'est-à-dire $a_p = q - (a_1 + ... + a_{p-1})$, et la connaisance des entiers $a_1, \ldots, a_{p-1}$ caractérise le placement des objets. On obtient ainsi une bijection entre les façons de placer q objets dans p cases et les sous-ensembles à $p-1$ éléments de $\{1, 2, 3, \ldots, p+q-1\}$, dont le nombre est C_{p+q-1}^{p-1}.

4 Vers une répartition homogène

Une fois le Théorème démontré, comment résoudre notre problème initial ? On voit que lorsque m tend vers l'infini alors $\dfrac{\mathrm{C}_{2^m+n-r}^{n}}{2^{nm}}$ tend vers $1/n!$, *i.e.* toutes les répartitions deviennent équiprobables, ce qui correspond bien à l'idée intuitive que plus l'on bat les cartes, plus le paquet devient aléatoire. Il faut maintenant quantifier cette intuition. Une manière de le faire consiste à introduire la quantité

$$\mathrm{Q}_m = \frac{1}{2} \sum_{\pi} |p_m(\pi) - \frac{1}{n!}|$$

qui mesure la distance entre la probabilité uniforme et la probabilité réalisée par m battages de cartes. Cette quantité est toujours comprise entre 0 et 1. Si elle est proche de 1, cela signifie que les probabilités p_m se concentrent sur un petit nombre de configurations. Plus cette quantité est petite, plus la répartition est “aléatoire”. En utilisant le Théorème 1, on voit que

$$\mathrm{Q}_m = \frac{1}{2} \sum_{r} \mathrm{A}_{n,r} \left| \frac{\mathrm{C}_{2^m+n-r}^{n}}{2^{nm}} - \frac{1}{n!} \right|$$

où $\mathrm{A}_{n,r}$ désigne le nombre permutations avec r suites montantes. On ne connaît pas d'expression explicite simple de ces nombres, mais on connaît des algorithmes permettant de les calculer, et des formules approchées lorsque n est grand. À l'aide de cela, Bayer et Diaconis ont montré que si $m = \dfrac{3}{2}\log_2 n + x$, alors

$$\mathrm{Q}_m = \sqrt{\frac{2}{\pi}} \int_0^{\frac{2^{-x}}{4\sqrt{3}}} e^{-t^2/2}\, dt + r_n \qquad (*)$$

où r_n est un reste qui tend vers 0 quand n tend vers l'infini. On voit que Q_m est proche de 1 lorsque $x << 0$ et proche de 0 lorsque $x >> 0$ (on peut donner des valeurs numériques précises, par exemple en regardant dans une table de la loi de Gauss). La conclusion est qu'il faut environ un peu plus que $\dfrac{3}{2}\log_2 n$ battages pour bien mélanger un jeu de n cartes. Lorsque $n = 52$, ce qui est le cas le plus fréquent dans les applications, on peut calculer précisément Q_m en fonction de m et on obtient les valeurs (avec 3 décimales)

$$\mathrm{Q}_1 = 1.000,\ \mathrm{Q}_2 = 1.000,\ \mathrm{Q}_3 = 1.000,\ \mathrm{Q}_4 = 1.000,\ \mathrm{Q}_5 = 0.924,$$
$$\mathrm{Q}_6 = 0.614,\ \mathrm{Q}_7 = 0.334,\ \mathrm{Q}_8 = 0.167,\ \mathrm{Q}_9 = 0.085,\ \mathrm{Q}_{10} = 0.043$$

On voit que la distance reste pratiquement à son maximum jusqu'à 5 battages, puis elle se met à décroître rapidement, et en pratique, avec 8 battages on obtient un brassage des cartes suffisant pour que la donnée de la distribution avant battage soit inutilisable par les joueurs. Notez que les valeurs de $\mathrm{Q}_7, \mathrm{Q}_8, \mathrm{Q}_9, \mathrm{Q}_{10}$ forment approximativement une suite géométrique de raison 1/2, ce qui est en accord avec la formule approchée $(*)$.

Annexe A : Solution de l'exercice

Terminons par une solution à l'exercice. On numérote les cartes de 0 à $2^n - 1$, et on écrit leur numéro en notation binaire, chaque numéro est donc une suite de n chiffres égaux à 0 ou 1. On vérifie facilement que la transformation de "battage parfait" consiste à faire une *permutation circulaire* de ces n chiffres, par exemple si on prend la sixième carte d'un jeu de 64 cartes, on écrit 5 en binaire (on a commencé par 0 !), soit 000101, et les positions successives seront, en notation binaire, 001010, 010100, 101000, 010001, 100010 et enfin 000101. Il est clair qu'avec une permutation circulaire, on revient sur ses pas en n étapes, et l'exercice est résolu.

Annexe B : Probabilité après m coupes

Comme annoncé lors de la démonstration du théorème, une fois les m coupes déterminées, chaque mélange possible a la même probabilité $1/2^{nm}$.
Pour démontrer ce résultat, il nous faut d'abord trouver la probabilité d'obtenir toutes les coupes effectuées aux endroits correspondants. Or, faire m coupes successives, c'est couper le paquet de cartes en 2 parties, puis les deux parties chacune en 2, et ainsi de suite. Au total, nous avons 2^m tas de cartes, séparés par $2^m - 1$ coupes, donc. Notons $j_1 \geq j_2 \geq \ldots \geq j_{2^m-1}$ les positions de ces coupes. Notons enfin $j_0 = n$ et $j_{2^m} = 0$. Nous allons montrer par récurrence sur l'entier m que la probabilité d'une telle coupe s'écrit :

$$p_1\left(j_1, \ldots, j_{2^m-1}\right) = \frac{1}{2^{nm}} \prod_{i=1}^{2^m-1} \frac{j_{i-1}!}{j_i!\,(j_{i-1}-j_i)!} = \frac{n!}{2^{nm} \prod\limits_{i=1}^{2^m} (j_{i-1}-j_i)!}$$

Le résultat est vrai pour $m = 1$: la relation précédente s'écrit alors :

$$p_1\left(j_1\right) = \frac{1}{2^n} \frac{n!}{j_1!\,(n-j_1)!}$$

C'est bien la probabilité obtenue par la loi binomiale que nous avons supposée pour toute coupe.
Supposons le résultat vrai pour un entier m donné. Pour passer à $m+1$, on effectue 2^m coupes supplémentaires (on coupe chaque tas de carte existant en deux parties). Cela revient à choisir des entiers $(k_i)_{1 \leq i \leq 2^m}$ vérifiant :

$$\forall i \leq 2^m, \quad j_i \leq k_i \leq j_{i-1}$$

Or, toujours dans le modèle utilisé où la loi d'une coupe est la loi binomiale, pour chaque indice i la probabilité du choix k_i est :

$$\frac{1}{2^{j_{i-1}-j_i}}\frac{(j_{i-1}-j_i)!}{(j_{i-1}-k_i)!\,(k_i-j_i)!}$$

Pour obtenir la probabilité de nos 2^m choix, il faut multiplier ces probabilités. Et comme nous avons préalablement choisi les 2^m-1 premières coupes (les entiers j_i), dont la probabilité nous est donné par l'hypothèse de récurrence, on obtient la probabilité :

$$\frac{n!}{2^{nm}\prod\limits_{i=1}^{2^m}(j_{i-1}-j_i)!}\prod_{i=1}^{2^m}\frac{1}{2^{j_{i-1}-j_i}}.\frac{(j_{i-1}-j_i)!}{(j_{i-1}-k_i)!\,(k_i-j_i)!}$$

Soit, comme $\prod\limits_{i=1}^{2^m}\frac{1}{2^{j_{i-1}-j_i}}=\frac{1}{2^{j_0-j_{2^m}}}=\frac{1}{2^n}$,

$$p_1\left(k_1,j_1,\ldots,j_{2^m-1},k_{2^m}\right)=\frac{n!}{2^{n(m+1)}\prod\limits_{i=1}^{2^m}(j_{i-1}-k_i)!\,(k_i-j_i)!}$$

Il suffit alors de renommer les entiers $k_1\geq j_1\geq\ldots\geq j_{2^m-1}\geq k_{2^m}$ pour obtenir le résultat à l'ordre $m+1$ avec la formulation annoncée. On conclue par le principe de récurrence que notre propriété est vraie à tout ordre.

Pour ce qui est de la deuxième partie du raisonnement, c'est-à-dire une fois les 2^m-1 coupes effectuées, c'est beaucoup plus simple : la démonstration du cas $m=1$ se transpose telle quelle.
Soit en effet $a_1,\ldots,a_{2^m}$ les nombres de cartes respectifs des 2^m tas. On choisit alors la carte du dessous du tas numéro i avec la probabilité $\frac{a_i}{\sum\limits_{i=1}^{2^m}a_i}$.
Pour la deuxième étape, on recommence le procédé avec des tas de respectivement $a_1,\ldots,a_i-1,\ldots,a_{2^m}$ cartes. Et ainsi de suite. Pour obtenir la probabilité du mélange, on fait alors le produit de tous ces termes. Et, comme pour le cas $m-1$, on retrouve au numérateur tous les facteurs de $\prod\limits_{i=1}^{2^m}a_i!$ dans le désordre, et au dénominateur, dans l'ordre décroissant, les facteurs de $n!$. Soit une probabilité pour un mélange donné M de :

$$p_2\left(\mathrm{M}\right)=\frac{\prod\limits_{i=1}^{2^m}a_i!}{n!}$$

Enfin, le tas de carte numéro i est constitué des cartes situées au départ entre les deux coupes et j_{i-1} et j_i. Donc $a_i=j_{i-1}-j_i$, et l'on obtient :

$$p_2\left(\mathrm{M}\right)=\frac{\prod\limits_{i=1}^{2^m}(j_{i-1}-j_i)!}{n!}$$

La probabilité d'obtenir les coupes en $j_1,\ldots,j_{2^m-1}$ puis le mélange M est donc :

$$p_1\left(j_1,\ldots,j_{2^m-1}\right)p_2\left(\mathrm{M}\right)=\frac{1}{2^{nm}}$$