

**Académie de Montpellier
Université de Montpellier II
Sciences et Techniques du Languedoc**

Diplôme d'Etudes Approfondies

"INFORMATIQUE"

PHYSIQUE ET CALCUL : L'EXEMPLE DU TEMPS

par

Pierre Laurent BOREL

Date de soutenance : le 26 Juin 1995

Membres du jury :

M. CHEIN
E. AHRONOVITZ
C. BOKSENBAUM
G. CARAUX
C. DONY
R. DUCOURNAU

J. FERRIE
O. GASCUEL
M. HABIB
D. HERIN
M. HUCARD
ML. MUGNIER

JF. PONS
A. PRELLER
J. QUINQUETON
MC. VILAREM

Tuteurs de stage : M. HABIB, P.REITZ, R. DUCOURNEAU

Invité : G. COHEN-SOLAL

Remerciements

Le présent travail a été réalisé dans le cadre des activités du LIRMM. Sans le soutien et l'aide que j'y ai trouvé, cette étude n'aurait pas pu se concrétiser. Je tiens donc à remercier :

M. Habib pour la confiance dont il a fait preuve en m'autorisant un sujet hors du commun,
M. Retz pour l'intérêt qu'il a porté à mon travail,
M. Sallantin pour l'apport de ses réflexions personnelles,
M. Cohen-Solal pour son regard de physicien,
M. Ducourneau pour ses critiques constructives,
M. Durand, de l'ENS Lyon pour son éclairage sur les automates cellulaires,
M. Papallardo du CREUFOP qui s'est préoccupé des problèmes d'intendance de la formation permanente.

Je remercie aussi :

l'ensemble des responsables du DEA informatique qui m'ont permis de concrétiser cette étude,
l'ensemble des camarades du DEA qui ont fait de cette année un bon souvenir.
l'ensemble des pionniers de la physique du calcul,
le monde des physiciens et celui des informaticiens,
et tous ceux que, malgré mes précautions, j'ai eu le tort d'oublier.

Table des matières

1. Information et physique.....	11
2. Matière	11
2.1 Physique, particules et systèmes formels	11
2.2 Mécanique quantique	12
2.3 Notation de Dirac	13
2.3.1 Espace de Hilbert	13
2.3.2 Bases de l'espace.....	13
2.3.3 Opérateurs	13
2.3.4 Evolution temporelle	14
3. Energie	14
3.1 Présentation.....	14
3.2 Entropie classique	14
3.3 Entropie statistique : lien matière énergie.....	14
4. Information	15
4.1 Les différentes théories de l'information	15
4.1.1 Shannon : entropie informatique (1949)	15
4.1.1.1 Définition statistique du contenu en information.....	15
4.1.1.2 Entropie informatique.....	15
4.1.1.3 Code préfixe.....	16
4.1.1.4 Codes optimaux.....	16
4.1.1.5 Irréversibilité	16
4.1.2 Kolmogorov : complexité algorithmique (1965)	17
4.1.2.1 Histoire	17
4.1.2.2 Définition.....	17
4.1.2.3 Notion de minoration	17
4.1.2.4 Complexité conditionnelle	18
4.1.2.5 A la recherche du minorant universel.....	18
4.1.2.6 C-incompressibilité.....	18
4.1.2.7 Complexité combinée.....	19
4.1.2.8 Entropie de Shannon et de Kolmogorov.....	19
4.1.2.9 Récapitulatif	19
4.1.3 Chaitin : complexité de préfixe (1966)	19
4.1.3.1 Présentation.....	19
4.1.3.2 Théorème d'invariance	20
4.1.3.3 Machine préfixe	20
4.1.3.4 Machine préfixe universelle	20
4.1.3.5 Variantes	21
4.1.3.6 Propriétés	21
4.1.3.7 Complexité réversible	21
4.1.4 Lloyd et Pagels : profondeur thermodynamique (1988).....	21
4.1.4.1 Idée	21
4.1.4.2 Profondeur d'un état	22
4.1.4.3 Profondeur thermodynamique.....	22
4.1.4.4 Génération d'entropie.....	22
4.1.4.5 Machines réversibles	22
4.1.4.6 Conséquences.....	23
4.1.4.7 Remarques.....	23
4.1.5 Bennett : profondeur logique (1988).....	23
4.1.5.1 Complexité, complexités	23
4.1.5.2 K-profondeur logique.....	24
4.1.5.3 Invariance.....	24
4.1.5.4 Propriétés	24
4.1.5.5 Intérêt	24
4.1.6 Zurek : distance informatique (1989)	25

4.1.6.1	Coût en information du calcul	25
4.1.6.2	Mise à jour	25
4.1.6.3	Distance informatique	25
4.2	Lien information-hasard	26
4.2.1	Chaitin : théorie algorithmique de l'information (1971)	26
4.2.1.1	Définition d'une chaîne aléatoire	26
4.2.1.2	Théorème d'incomplétude	26
4.2.1.3	Conséquences	27
5.	Temps	27
5.1	Questions de temps	27
5.2	Le temps à travers les âges	28
5.2.1	Le temps des grecs	28
5.2.2	Les temps médiévaux	28
5.2.3	Le temps des révolutions de la pensée	28
5.2.4	Les temps modernes	29
5.3	Les flèches du temps	29
5.3.1	Le problème de l'irréversibilité en physique	29
5.3.2	Irréversibilité fondamentale	29
5.3.3	Les formes de l'irréversibilité	30
5.4	Flèche statistique	30
5.4.1	Mathématiques et causalité	30
5.4.2	Inégalité de Bayes	31
5.5	Flèche thermodynamique	31
5.5.1	Carnot : thermodynamique macroscopique	31
5.5.1.1	Notion d'entropie	31
5.5.2	Boltzmann : thermodynamique statistique	32
5.5.2.1	Espace des phases	32
5.5.2.2	Entropie de Boltzmann	32
5.5.2.3	Mécanique quantique	33
5.5.2.4	Mécanique statistique et irréversibilité	33
5.5.3	Conclusion	33
5.6	Flèche radiative	34
5.6.1	Ondes et thermodynamique	34
5.6.2	Temps opaque	34
5.6.3	Ondes avancées acoustiques	34
5.6.4	Conclusion	34
5.7	Flèche informatique	34
5.7.1	Lien énergie et information	34
5.7.2	Maxwell : le démon (1871)	35
5.7.2.1	Le démon thermique	35
5.7.2.2	Démon de pression	36
5.7.3	Szilard : le moteur (1929)	36
5.7.3.1	Du démon au moteur	36
5.7.3.2	Fonctionnement du moteur	36
5.7.4	Landauer : dépense énergétique et calcul (1960)	38
5.7.4.1	Consommation des ordinateurs	38
5.7.4.2	Entropie thermodynamique et informatique	38
5.7.4.3	Bilan	39
5.7.5	Bennett : réversibilité logique du calcul (1973)	39
5.7.5.1	Histoire	39
5.7.5.2	Machines de Turing réversibles	39
5.7.5.3	Calcul réversible	39
5.7.5.4	Déchet et thermalisation	40
5.7.6	Fredkin, Toffoli : calcul et modèles balistiques (1981)	40
5.7.6.1	Objectif d'un modèle physique	40
5.7.6.2	Logique dissipative	40
5.7.6.3	Critères pour une logique conservative	41
5.7.6.4	Fil unitaire	41

5.7.6.5	Porte logique	41
5.7.6.6	Modélisation des fonctions logiques usuelles	42
5.7.6.7	Concrétisation physique	43
5.7.6.8	Porte réversible	43
5.7.6.9	Fonctions annexes	44
5.7.6.10	Bilan énergétique	44
5.7.6.11	Réseaux combinatoires	45
5.7.6.12	Conclusion	46
5.7.7	Bennett : modèle brownien (1982)	46
5.7.7.1	Intérêt	46
5.7.7.2	Constitution de machine de Turing, généralités	46
5.7.7.3	Le bit	47
5.7.7.4	La bande	47
5.7.7.5	La tête de lecture-écriture	48
5.7.7.6	La table de transitions	49
5.7.7.7	Fonctionnement	49
5.7.7.8	Lecture	49
5.7.7.9	Ecriture	49
5.7.7.10	Décalage	50
5.7.7.11	Changement d'état	50
5.7.7.12	Réversibilité physique et logique	50
5.7.8	Modèles quantiques	50
5.7.8.1	Recette	50
5.7.8.2	Machine quantique	51
5.7.8.3	Simulation de machines classiques	51
5.7.8.4	Simulation de machine universelle	51
5.7.8.5	Propriétés	52
5.7.8.6	Critiques	53
5.7.9	Bennett & Landauer : le nouveau démon (1988)	53
5.7.9.1	Retour du moteur de Szilard	53
5.7.9.2	Source froide	54
5.7.10	W.Porod & al : dissipation dans le calcul (1984)	55
5.7.10.1	Histoire	55
5.7.10.2	Les failles de l'interprétation classique	55
5.7.10.3	Origine vraie (pour PGFP) de la dissipation	55
5.7.10.4	Ce qu'en pense Bennett	56
5.7.10.5	Ce qu'en pense Toffoli	56
5.7.10.6	Ce qu'en pense Landauer	56
5.7.10.7	Réplique de Porod & al	57
5.7.11	Zurek : entropie physique (1989)	57
5.7.11.1	Hasard et complexité	57
5.7.11.2	Entropie algorithmique	58
5.7.11.3	Exemple du gaz de Boltzmann	58
5.7.11.4	Entropie physique	59
5.7.11.5	Démon de Maxwell	59
5.7.11.6	Discussion	60
5.7.11.7	Conclusion	60
5.7.12	Conclusion	60
5.7.12.1	Les formes de la réversibilité	60
5.7.12.2	Nature du temps	61
5.8	Flèche cosmologique	62
5.8.1	Organisation de l'Univers	62
5.8.2	Entropie objective et subjective	62
5.8.3	Entropie de l'Univers	62
5.8.4	Conclusion	62
5.9	Flèche quantique	63
5.9.1	Irréversibilité et mesure	63
5.9.2	Collision temporelle	63

5.9.3	Complémentarité.....	63
5.9.4	Exemple des fentes d'Young.....	64
5.9.5	Mesure non perturbatrice.....	64
5.9.6	Discussions sur la mesure.....	66
5.9.7	Rôle de l'environnement.....	66
5.9.8	Recouvrement de l'interférence.....	67
5.9.9	Causalité.....	67
5.9.10	Conclusion.....	68
5.10	Flèche microscopique.....	68
5.10.1	Symétries discrètes.....	68
5.10.2	Violation des symétries.....	69
5.10.3	Conséquence sur le temps.....	70
5.10.4	Intervention de modèles informatiques.....	70
5.10.5	Apport des autres modèles.....	71
5.10.6	Conclusion.....	71
5.11	Le temps en tant que grandeur fondamentale.....	71
5.11.1	Le temps tel qu'en lui-même.....	71
5.11.2	Systèmes dissipatifs.....	72
5.11.3	Evolution des systèmes.....	72
5.11.4	Temps et temps.....	72
5.11.5	Temps et simulation, des origines à nos jours.....	73
5.12	Conclusion sur le temps.....	73
6.	Applications.....	74
6.1	Preuve d'algorithme.....	74
6.1.1	objectif.....	74
6.1.2	terminologie.....	74
6.1.3	Principe.....	74
6.1.4	Schéma de preuve.....	75
6.1.5	Réécriture et écriture.....	76
6.1.5.1	Impératifs d'écriture.....	76
6.1.5.2	Instructions.....	76
6.1.5.3	structures.....	76
6.1.6	Piège à éviter.....	77
6.2	Exemple.....	77
6.2.1	Algorithmes de choix.....	77
6.2.2	Rappels sur les graphes.....	78
6.2.3	Présentation de MCS.....	78
6.2.4	Preuve par utilisation de la réversibilité.....	79
6.2.4.1	Procédure réversible.....	79
6.2.4.2	Terminaison de la procédure.....	79
6.2.4.3	Propriétés des résultats.....	79
6.2.4.4	Récédure.....	79
6.2.4.5	Preuve de la récédure.....	80
6.2.4.6	Conditions de réussite de la récédure.....	81
6.2.5	Conclusion.....	82
6.3	Conclusion sur l'approche.....	82
7.	Conclusion générale.....	83
8.	Références.....	84

1. Information et physique

La première activité d'observation scientifique a l'âge de l'homme moderne. Il y a 30 000 ans, il se trouvait déjà là pour graver dans les os les différents aspects de la lune. Dans la régularité des cycles diurnes et lunaires, il établissait le premier lien entre temps et espace. Certes, le caractère plus imprévisible de quelques "astres errants" au mouvement apparemment imprévisible troubla un peu ses observations pour aiguiller l'étude du ciel davantage vers la superstition que la connaissance.

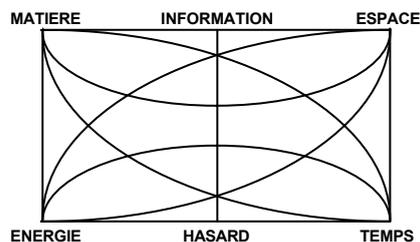
Quand il ne regardait pas en l'air et se contentait de son environnement directement accessible, la science ne le préoccupait pas tant que la technique. Notre ancêtre préhistorique qui cognait sur les pierres (ou autres) pour les façonner ne se préoccupait pas d'énergie cinétique. Pourtant il domestiquait la matière. Mais en cognant plus fort, il fit jaillir les premières étincelles d'énergie issues de son activité.

Il fallut attendre la Renaissance pour que l'on prenne conscience dans le monde occidental de l'intérêt d'une étude objective et chiffrée du Monde. La première vraie théorie scientifiquement établie a été celle de la chute des corps, relatant les liens entre matière et temps. Plus tard, les "machines à feu", c'est à dire les moteurs thermiques, ont fait ressentir le besoin d'une théorie de l'énergie. Ce sera la thermodynamique. Cette théorie sera la première à fournir à la dissymétrie passé-futur un support scientifiquement appréhendable en l'assimilant au sens de dégradation de l'énergie. Le temps sortait progressivement du simple constat pour former avec l'énergie, la matière et l'espace un ensemble interdépendant.

L'information quant à elle, n'intéressera pas le monde des sciences avant l'apparition des premiers systèmes de télécommunication. C'est dans ce cadre que naîtra la première théorie sur le sujet, due à Shannon. L'adaptation de ses idées aux contraintes liées au calcul sera une des bases des autres concepts liés à l'information.

Mais quel peut être l'intérêt d'étudier l'information en tant que matière première du monde physique, au même titre que la matière, l'énergie, le temps ? En fait il semble qu'elle a sa place au rang des notions fondamentales autour desquelles tournent l'ensemble des propos scientifiques. Nous pourrions ainsi nous construire un modèle mettant en scène 6 protagonistes. On les regroupe souvent 2 à 2. Temps avec espace, matière avec énergie. Et l'information, à quoi s'associe-t-elle ? Nous verrons qu'elle est intimement liée au sixième protagoniste non encore cité : le hasard.

Tous ces concepts furent étudiés chacun en son temps. Mais nos 6 notions sont beaucoup plus interdépendantes que ne le laisse entrevoir une telle opposition 2 à 2. Derrière elle se cachent des liens plus universaux, des relations de tout avec tout.



Nous essaierons de voir ce qu'il en est pour l'information. Nous interrogerons sur la réalité d'un éclairage que pourrait apporter les tentatives de définir objectivement l'information sur les autres notions de la physique.

Il semble ainsi a priori peu évident que la notion du temps puisse trouver quelque bénéfice de l'étude de l'information. Nous la prendrons donc comme exemple pour étudier la réalité des liens entre l'information et le reste. Après une brève présentation de quelques uns des autres protagonistes, nous nous attarderons donc sur les deux qui nous intéressent le plus : l'information et le temps.

2. Matière

2.1 Physique, particules et systèmes formels

Dans les années 60, plusieurs milliers de particules étaient nécessaires pour expliquer les phénomènes de la matière. Aujourd'hui, moins de 30 suffisent à décrire les mêmes phénomènes. Surtout, ces particules sont enfermées dans une classification et un ensemble de règles telles que l'existence de chacune est nécessaire.

- matière (fermions)

matière hadronique

quark u

quark t

quark c

quark d

quark b

quark s

matière leptonique

électron

muon

tau

neutrino e^-

neutrino μ^-

neutrino τ^-

- rayonnement (bosons)

photon (interaction électromagnétisme)

W^+ W^- Z^0 (interaction faible)

8 gluons (interaction forte)

boson de Higgs (électrofaible).

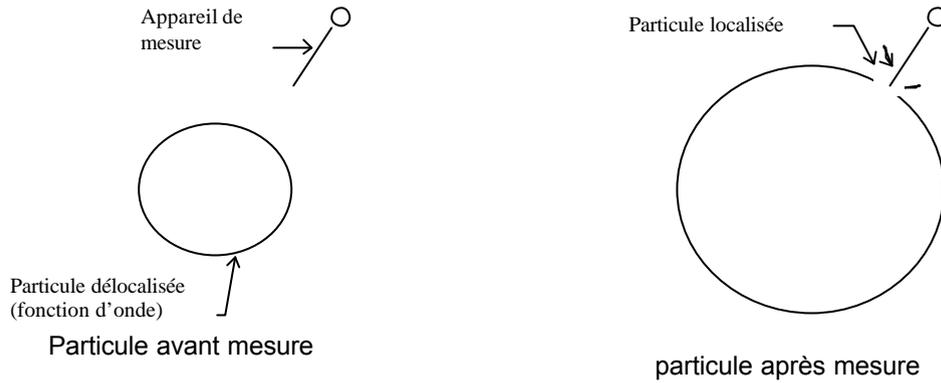
Retenons surtout que les mêmes phénomènes ont pu s'expliquer par un nombre de concepts réduit. D'une manière générale, on peut dire que le rôle de la science est d'essayer de trouver la description la plus succincte possible du monde qui puisse permettre de retrouver tous les résultats expérimentaux connus. Son activité s'apparente donc à un traitement de l'information qui, à partir de dérivations, chercherait le système formel minimal qui aurait pu les générer. Cet aspect des choses risque de nous intéresser par la suite.

2.2 Mécanique quantique

Certes tout n'est pas fini une fois que l'on a mis en évidence les particules élémentaires qui composent toute matière. Encore faut-il donner du liant à ces particules en trouvant les lois qui régissent leur comportement. La physique des particules ne va pas être abordée ici. Mais cette physique s'appuie sur des lois et un formalisme dont nous aurons besoin ultérieurement : les lois de la mécanique quantique.

La mécanique quantique attribue à chaque particule des propriétés à la fois continues et discontinues. Continues parce que tant qu'aucune mesure n'est effectuée sur le système, son comportement se décrit à l'aide d'une fonction d'onde étalée dans l'espace. Mais au moment de la mesure, le système apparaît comme constitué de particules ponctuelles.

Au regard des équations, on peut comparer une particule qui se déplace à un ballon qui gonfle. Mesurer la position de la particule revient à essayer de positionner une aiguille un peu n'importe où dans l'espace. A moment donné l'aiguille se retrouvera sur la surface du ballon qui se percera à cet endroit et à cet endroit seulement. Mais toute l'énergie contenue dans le ballon se manifestera instantanément au niveau du trou. Pour l'appareil de mesure, la particule est localisée à l'endroit où se trouvait la pointe au moment où l'échange d'énergie s'est manifesté. Seulement cette localisation a été "provoquée" par la mesure. Auparavant la particule était "délocalisée".



Plusieurs tentatives plus ou moins singulières d'interprétation de la délocalisation ont été données :

- l'interprétation de Costa de Beauregard, qui considère que la surface du ballon représente la position d'une même particule remontant dans le temps et explorant à "tour de rôle" toutes les trajectoires possibles,
- l'interprétation d'Everett qui considère que, au moment de la mesure, se créent autant d'univers parallèle qu'il existe de points sur le ballon, chaque univers manifestant une localisation différente de la particule,
- l'interprétation la plus prudente et la plus courante, dite interprétation de l'école de Copenhague, qui se contente de prendre en compte les faits et d'affirmer que la particule ne peut être entièrement décrite par des paramètres locaux avant mesure. Peu importe de savoir ce qu'est la surface du ballon en soi, l'important est de savoir ce qu'elle peut représenter pour des observateurs du monde macroscopique comme nous.

On ne sait pas où le ballon va percer, mais on sait que ce ne peut être que sur sa surface. Celle-ci matérialise donc une probabilité de localisation de la particule. En mécanique quantique, l'équivalent de la surface du ballon, c'est la fonction d'onde $\Psi(r,t)$. Il s'agit d'une fonction complexe. Le carré de son module $|\Psi(r,t)|^2$ donnera la probabilité pour que la particule soit localisée en un endroit donné, moyennant un facteur de normalisation qui permet de s'assurer que la somme des probabilités pour l'ensemble de l'espace est égale à l'unité. Pour que la normalisation soit possible il faut que Ψ soit une fonction de carré sommable, c'est à dire que l'intégrale $\int_{\mathbb{R}^3} |\Psi(x)|^2 dx$ soit finie.

2.3 Notation de Dirac

2.3.1 Espace de Hilbert

Il est envisageable d'assimiler une fonction $\Psi(x)$ à une combinaison linéaire de fonctions $\psi(x)$ donnant à l'ensemble des fonctions une structure d'espace vectoriel. Les fonctions de carré sommable peuvent ainsi être assimilées à un vecteur d'un espace \mathfrak{H} à nombre de dimensions pouvant atteindre l'infini et à coordonnées complexes : l'espace de Hilbert. Un vecteur ω de \mathfrak{H} est noté $|\omega\rangle$. Il représente l'état du système à un instant donné.

A chaque vecteur $|\omega\rangle$ on fait correspondre un vecteur dual $\langle\omega|$. Les coordonnées de $\langle\omega|$ sont les complexes conjuguées de celles de celles de $|\omega\rangle$.

L'espace de Hilbert est muni d'un produit scalaire. Le produit de 2 vecteurs $|\omega\rangle$ et $|\omega'\rangle$ se note $\langle\omega|\omega'\rangle$. Il se définit ainsi :

$$\langle\omega|\omega'\rangle = \int_{\mathbb{R}^3} \omega^*(x) \omega'(x) dx$$

analogue au produit scalaire classique si l'on assimile $\langle\omega|$ à un vecteur ligne et $|\omega'\rangle$ à un vecteur colonne.

L'ensemble des vecteurs représentant un même état d'un système sont colinéaires. Afin de prendre en compte l'interprétation probabiliste d'une fonction d'onde $\Psi(x)$, on lui attribuera un représentant normé $|\Psi\rangle$, c'est à dire tel que $\langle\Psi|\Psi\rangle = 1$.

2.3.2 Bases de l'espace

Il est possible de définir des ensembles de vecteurs discrets orthonormés de \mathfrak{X} en nombre fini ou infini mais dénombrable en posant que deux fonctions $u_i(x)$ et $u_j(x)$ doivent être telles que $\langle u_i | u_j \rangle = \delta_{ij}$ avec :

- $\delta_{ij} = 1$ si $i = j$
- $\delta_{ij} = 0$ sinon.

Mais il est également possible de définir des ensembles continus de vecteurs orthonormés de \mathfrak{X} . Les fonctions $u_\alpha(x)$ correspondantes sont cette fois indicées par un réel α . La condition d'orthonormalité devient $\langle u_\alpha | u_\beta \rangle = \delta(\alpha - \beta)$ où la fonction de Dirac $\delta(x)$ est construite pour que l'on ait :

- $\delta(x) = 0 \quad \forall x \neq 0$,
- $\delta(0) = +\infty$,
- $\int_{-\infty}^{+\infty} \delta(x) dx = 1$.

Une base orthonormée de l'espace de Hilbert est donc ainsi constituée d'un ensemble de vecteur orthonormaux à indices discrets ou continus. Pour la suite, nous ne les distinguerons pas. Ainsi nous noterons que la composante d'indice i d'un vecteur $|\omega\rangle$ vaut $\langle u_i | \omega \rangle$, que i soit réel ou entier. On note parfois $\langle e_i | \omega \rangle$.

2.3.3 Opérateurs

Si les vecteur de l'espace de Hilbert représentent les états d'un système, les opérateurs linéaires hermitiques que nous allons maintenant définir représentent les opérations de mesure possibles sur ces états.

Un opérateur linéaire défini sur \mathfrak{X} se représente par une matrice carrée Ω dont le nombre de lignes et colonnes peut être infini. L'application d'un opérateur Ω à un vecteur $|\omega\rangle$ se matérialise par le produit de la matrice et du vecteur correspondant et se note $\Omega |\omega\rangle$. Un élément Ω_{ij} de cette matrice vaut $\langle u_i | \Omega | u_j \rangle$ où u_i et u_j sont des vecteurs de la base. L'opérateur Ω est hermitique si $\langle u_i | \Omega | u_j \rangle = \langle u_j | \Omega | u_i \rangle^*$ (* représente la conjugaison complexe). L'élément $\Omega_{ij} = \langle u_i | \Omega | u_j \rangle$ se note parfois $\langle i | \Omega | j \rangle$.

On dit que ω , scalaire, et $|\omega\rangle$, vecteur de \mathfrak{X} , sont respectivement valeur propre et vecteur propre de l'opérateur Ω si l'on a $\Omega |\omega\rangle = \omega |\omega\rangle$. Les vecteurs propres d'un opérateur peuvent être en nombre infini. Ils forment une base de \mathfrak{X} . Les valeurs propres d'un opérateur hermitique sont toujours réelles.

Une grandeur physique observable est modélisée par un opérateur linéaire hermitique sur \mathfrak{X} . Chaque valeur propre représente un résultat de mesure possible. Chaque vecteur propre représente l'état du système après une mesure ayant donné pour résultat la valeur propre associée. L'ensemble des vecteurs propres associées à l'opérateur constitue une base orthonormée de \mathfrak{X} .

Dans cette base orthonormée, chacune des coordonnées d'un vecteur d'état normalisé représente la probabilité pour qu'une mesure donne pour résultat la valeur propre associée au vecteur propre définissant l'axe de la base considéré. Ainsi le système est dans un état $|\Psi\rangle$, la probabilité pour que le résultat de mesure soit ω (associée au vecteur propre $|\omega\rangle$) est :

$$|\langle \omega | \Psi \rangle|^2$$

2.3.4 Evolution temporelle

L'évolution du système entre les temps t_0 et t est décrite par un opérateur d'évolution temporelle $U(t_0, t)$. On a :

$$|\Psi(t)\rangle = U(t, t_0) |\Psi(t_0)\rangle$$

A partir d'une évolution en un temps infiniment bref, on définit l'opérateur constant H :

$$U(t, t+dt) = I - (i/\hbar) H dt$$

où I est l'opérateur identité. H est l'opérateur hamiltonien correspondant à l'énergie totale du système.

3. Energie

3.1 Présentation

La thermodynamique étudie l'énergie en général et la chaleur en particulier, qui en est considéré comme la forme la plus dégradée. Toute transformation d'une forme d'énergie en une autre s'accompagne d'une dissipation sous forme de chaleur et tout système tend donc à se dégrader. Cette tendance est matérialisée par l'évolution croissante d'une grandeur appelée entropie.

3.2 Entropie classique

L'entropie S , quotient de la chaleur par la température, se définit de manière différentielle par :

$$dS = dQ/T$$

dans laquelle Q représente la quantité de chaleur, et T la température.

3.3 Entropie statistique : lien matière énergie

Considérons un système thermodynamique à partir de la population de tous ses états possibles. Selon la précision que l'on s'accorde sur la position et la vitesse des particules qui composent le système, certains états sont différentiables d'autres non. Sur l'ensemble des états, certains seront caractérisés par les mêmes valeurs des grandeurs macroscopiques comme la température et la pression. Ces grandeurs sont vues comme des grandeurs statistiques moyennant l'énergie des particules du système. La notion d'entropie peut donc s'appuyer sur des bases statistiques établies sur l'ensemble des populations d'états possibles d'un système.

Soit Ω le nombre d'états différentiables accessibles à un système, on définit l'entropie de Boltzmann par

$$S = k \ln(\Omega)$$

où k est une constante. Au sein de cette interprétation, les caractéristiques de l'entropie classique se retrouvent sous forme de probabilités d'évolution. Si la température a tendance à s'homogénéiser, c'est que la population d'états correspondant à une température homogène est plus importante que celles correspondant à des températures hétérogène. Le système a donc plus de chances d'évoluer vers l'homogène.

Nous détaillerons plus tard les notions de thermodynamique.

4. Information

4.1 Les différentes théories de l'information

4.1.1 Shannon : entropie informatique (1949)

4.1.1.1 Définition statistique du contenu en information

Un processus qui tendrait à générer au hasard des caractères sur une feuille blanche est potentiellement capable de reproduire tout le savoir de l'Humanité ainsi qu'engendrer toutes les oeuvres de création littéraires possibles. Mais le nombre de pages de caractère représentant réellement une information serait extrêmement restreint par rapport au nombre de pages dans lesquelles on n'atteindrait même pas le niveau de la poésie libre contemporaine.

En outre, le processus aléatoire étant le même pour tout le monde, il serait impossible de distinguer les chef d'oeuvre des autres textes au sein du seul système formel constitué par le générateur. Le texte n'est que le support codé de l'information. Il n'est pas l'information elle-même. Il n'a de valeur que si un processus a généré ce texte suite à un codage d'information à partir de son contenu sémantique, et s'il est capable de retrouver ultérieurement cette sémantique par décodage.

En l'absence d'une connaissance du traitement qui a généré un code, peut-on néanmoins définir une notion de quantité d'information ? Si c'est le cas, il ne peut s'agir que d'une notion statistique. C'est d'ailleurs l'avis de Shannon qui cherche à traiter l'information comme la thermodynamique traite de

l'énergie. Il reprend les notions de thermodynamique statistique et l'applique au stockage et à la transmission d'information. L'idée de départ est de considérer que l'information mesure un degré d'organisation d'un système alors que l'entropie en mesurerait le désordre. Prenant en compte les notions statistiques rattachées à l'entropie, la richesse en information est caractérisée par l'existence d'un état peu probable.

Le niveau d'information I associé à un caractère x_k est d'autant plus élevé que sa probabilité d'apparition est faible. En prenant en considération la probabilité d'avoir un caractère $x = x_k$ à la sortie d'un canal connaissant les probabilités de sortie associées à chaque caractère possible, le niveau d'information se définit en nombre de bits par :

$$I(x=x_k) = -\log(p(x=x_k))$$

Cette définition est satisfaisante car elle est additive. L'intervention du logarithme permet d'affirmer que 2 pages de texte contiennent 2 fois plus d'information qu'une seule.

4.1.1.2 Entropie informatique

L'entropie H d'un canal véhiculant de l'information se calcule par la somme des états (sorties) possibles, d'une manière qui n'est pas sans rappeler celle par laquelle la thermodynamique statistique arrive à redécouvrir l'entropie S .

$$H(x) = -\sum(p(x=x_k) I(x=x_k)) = -\sum(p(x=x_k) \log(p(x=x_k)))$$

qui représente le nombre de bits permettant de décrire la sortie.

Quand une page est blanche, tous les contenus en caractère de la page sont potentiellement possibles. Quand un caractère s'imprime, l'espace des possibilités se restreint. Ce que mesure vraiment la quantité d'information est la réduction des possibles induites par l'apparition d'un caractère. Plus le niveau d'information I du caractère est élevé, plus donc le caractère est improbable, et plus sa présence réduit le nombre d'états possibles.

Notons dès à présent que la réduction de l'espace des possibles, c'est à dire la réduction du nombre de degrés de libertés du système, a un équivalent thermodynamique dont nous parlerons : la réduction de l'espace des phases, apparaissant dans toute opération irréversible, et génératrice d'entropie. Ici l'impression d'un caractère correspond bien à une opération fondamentalement irréversible. Entropie physique et thermodynamique sont donc construites sur le même schéma et entretiennent des liens plus profonds dont nous discuterons.

4.1.1.3 Code préfixe

la chaîne "000000" peut correspondre au code "0000" suivi du code "00", aussi bien que de "000" suivi de "000". Pour éviter la confusion lors des transmissions, on peut se servir, pour l'encodage de symboles, de codes préfixes conçus pour qu'aucun code de symbole ne soit le début d'un autre. Cette notion permet d'envisager l'unicité d'un décodage sans avoir à utiliser de caractère spécial pour la séparation, et autorise donc un traitement purement binaire.

4.1.1.4 Codes optimaux

Un moyen de réduire la quantité d'information nécessaire pour décrire une sortie est d'utiliser un code court (en nombre de bits) pour les caractères les plus fréquents et un code nécessairement plus long pour les autres. Dans le cas d'une transmission de caractères alphabétiques, un exemple typique est celui du morse dans lequel la lettre "e" est codée par un simple point (au détriment du monde arabe qui ne connaît pas cette lettre).

On peut imaginer qu'un codage ne cherche pas à véhiculer des caractères isolés mais des mots complets. On attribue ensuite à chaque mot un code dont la longueur est fonction de la probabilité d'apparition du mot. Le nombre de mots d'une langue étant plus réduit que le nombre de chaînes de caractère possibles, et les mots ayant des probabilités d'apparition très diverses, le code ainsi obtenu gagne encore en compacité.

On peut imaginer ensuite un codage de phrases entières afin de réduire encore la longueur du code. Il faut noter cependant que :

- la longueur des codes est proportionnelle au nombre chaînes utilisées comme alphabet de base, et ce nombre est a priori proportionnel à la longueur moyenne de ces chaînes de base. Aucun gain en compacité ne doit être apporté par cette seule raison,
- le gain à espérer en attribuant des codes courts aux chaînes fréquentes connaît un optimum dès lors que cette longueur de code est le reflet exact des probabilités d'apparition.

Il existe donc un codage optimal qui utilise au mieux les probabilités d'apparition de succession de caractères pour réduire la longueur du message transmis. Il correspond à un niveau de codage tel que les longueurs des codes reflètent exactement les probabilités d'apparition. Les codages optimaux permettent de transmettre une quantité d'information de la manière la plus brève possible mais suppose connue la probabilité d'apparition des symboles. C'est le désir de s'affranchir d'une telle connaissance a priori qui conduira à d'autres concepts comme la complexité de Kolmogorov, à partir de la même idée de compression de message.

4.1.1.5 Irréversibilité

L'extension des théories de Shannon du domaine des transmissions à celui du calcul fait encore l'objet de recherches.

Nous avons vu, dans notre exemple précédent, que chaque impression (irréversible) d'un caractère sur une feuille de sortie diminue de manière notable le nombre de sorties possibles que cette feuille peut contenir. Si l'on accepte d'étendre la théorie de Shannon en remplaçant la probabilité d'obtenir un caractère par la probabilité pour le système d'être dans un état mémoire par exemple, alors on constate que toute opération irréversible de calcul correspond à une diminution des états possibles du système.

Dans un calcul, l'opération fondamentalement irréversible est l'effacement d'une mémoire. Il correspond de même à une diminution des états possibles du système, donc à une diminution d'entropie au sens de Shannon. A l'encontre d'un système physique, l'entropie d'un système de calcul isolé (sans entrée-sortie) ne peut aller qu'en diminuant.

L'entropie constante est concevable. Nous verrons qu'il est possible de concevoir des machines de calcul réversibles à condition que celles-ci ne procèdent jamais à un effacement de valeurs. Ces machines effectueraient des transitions entre états équiprobables. Une telle machine ne pourrait jamais effectuer qu'un seul et même calcul alternativement dans un sens et dans l'autre. Mais l'ordinateur n'est pas un système isolé. La nécessité de fournir les données et d'observer les résultats font qu'un calculateur n'est jamais un système thermodynamiquement isolé au sens de Shannon.

Le calculateur étant en outre connecté à une source d'énergie, des liens entre entropie informatique et thermodynamique sont envisageables. Nous verrons si une consommation d'énergie est nécessaire et si elle rétablit une certaine universalité de la thermodynamique même dans ses extensions au monde de l'information, autrement dit si l'augmentation de l'entropie thermodynamique est le prix à payer d'une baisse informatique locale de l'entropie.

4.1.2 Kolmogorov : complexité algorithmique (1965)

4.1.2.1 Histoire

La machine de Turing, on s'en souvient, était partie de l'idée de modéliser un mathématicien au moyen d'une machine en reproduisant les activités de base afin de créer un modèle de calculabilité. La machine peut donc effectuer l'essentiel des tâches d'un mathématicien : lecture, changement d'état, écriture, effacement.

Se souvenant des travaux de Turing, Solomonoff (1960) eût l'idée de modéliser un physicien. Il considéra que ce dernier a pour fonction d'accumuler les données phénoménologiques sur le monde, et d'essayer de trouver un moyen de décrire les phénomènes de la manière la plus compacte possible.

Solomonoff inventa donc la notion de complexité algorithmique de l'information. La quantité absolue d'information d'une chaîne est donnée par la taille en bits du plus petit algorithme capable de la générer. Vers 1965 Kolmogorov et Chaitin développèrent ou réinventèrent cette notion.

La grande différence entre l'idée d'information selon Shannon et selon Solomonoff Chaitin Kolmogorov est que Shannon a besoin du hasard comme d'un préalable, alors que Solomonoff Chaitin et Kolmogorov, peuvent utiliser leur notion d'information pour définir le hasard.

4.1.2.2 Définition

Essayons de définir la complexité d'une donnée x par rapport à une méthode f à valeur entière [28]. Soient :

- $n(x)$ une représentation encodée numérique de x
- f une méthode à valeur entière

On note la complexité de x relativement à la méthode f :

$$C_f(x) = \min\{ |p| : f(p) = n(x) \}$$

en d'autres termes, la complexité de l'objet x relative à la méthode f est la plus petite longueur d'un programme p dont l'exécution par f donne le codage de x .

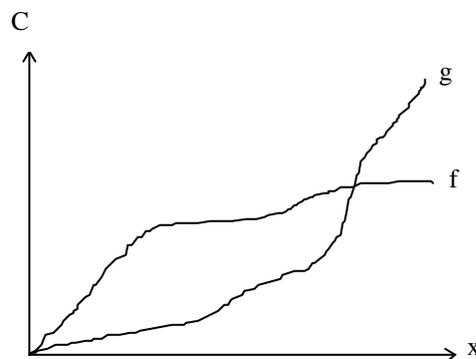
La notion de complexité est donc fortement dépendante de la méthode prise en compte.

4.1.2.3 Notion de minoration

Soient 2 méthodes f et g . f minorise g si il existe c tel que pour tout x on ait :

$$C_f(x) \leq C_g(x) + c$$

(toutes les descriptions par f sont plus courtes que par g à une constante près, indépendante de x)



2 méthodes peuvent se minorer mutuellement.

4.1.2.4 Complexité conditionnelle

Dans la notion de complexité définie précédemment, limitons nous au cas où les objets x sont des entiers naturels : $n(x) = x$.

Notons $\langle x, y \rangle$ une représentation codée des 2 objets x et y .

Définissons la complexité d'un objet x par rapport à une méthode ϕ connaissant y .

$$C_\phi(x|y) = \min\{ |p| : \phi(\langle y, p \rangle) = x \}$$

On notera la relation : $C_\phi(x) = C_\phi(y) + C_\phi(x|y)$ valable à un terme correctif près.

Si $y = \varepsilon$ on retrouve la définition inconditionnelle de la complexité.

4.1.2.5 A la recherche du minorant universel

Une méthode f est dite universelle si elle minorise toutes les autres. C'est le minorant de la notion de minoration.

Mais de telles méthodes existent-elles ? En d'autres termes le théorème suivant est-il vrai ?

théorème d'invariance : il existe une fonction minorante universelle

Prenons ϕ , la fonction calculée par une machine de Turing universelle (MTU). Soit n la donnée permettant à la MTU de simuler la machine calculant ϕ . On a :

$$\phi(\langle y, \langle n, p \rangle \rangle) = \phi(\langle y, p \rangle)$$

D'où :

$$C_{\phi}(x|y) \leq C_{\phi}(x) + c_{\phi}$$

où c_{ϕ} est une constante indépendante de x , représentant l'exécution de $\langle n, p \rangle$. On peut assimiler $\langle n, p \rangle$ au code généré par la compilation de p par n .

En d'autres termes, la méthode ϕ minorise toute méthode ϕ . ϕ est donc un minorant universel. La complexité de Kolmogorov notée $C(x)$ est la complexité pour une telle méthode universelle.

$$\begin{aligned} C(x|y) &= C_{\phi}(x|y) \\ C(x) &= C(x|\epsilon) \end{aligned}$$

4.1.2.6 C-incompressibilité

Quelle est la part de fonction compressibles ?

il existe 2^n chaînes de longueur n mais seulement $2^n - 1$ descriptions plus courtes. Une chaîne au moins de longueur n est incompressible.

de manière générale définissons la c -incompressibilité.

définition : x est c -incompressible si $C(x) \geq l(x) - c$. La complexité selon longueur se définit par $C(x||x)$.

Prenons le cas $c = 10$ par exemple. Pour les chaînes de longueur n :

le nombre de chaînes possibles est $2^n = 1024$

le nombre de descriptions de longueur $n-10$ est égal à $\sum_{i=1, n-11} 2^i = 2^{n-10} - 2$.

le rapport des 2 valeurs est ~ 1024

En d'autres termes, seule 1 chaîne sur 1000 peut se contracter de 10 caractères. La plupart des chaînes sont incompressibles ou peu compressibles.

4.1.2.7 Complexité combinée

La complexité combinée $C(x,y)$ est la complexité associée à la génération de 2 chaînes x et y en sortie d'une machine de Turing, avec un séparateur intermédiaire ou un autre moyen de les distinguer. Dans le cas de la complexité de Kolmogorov, les relations entre complexités simples de x et y et la complexité combinée de x,y font apparaître des termes logarithmiques qui rendront cette notion peu opérationnelle. Notons toutefois les propriétés suivantes, garanties à un terme près, fonction de la sensibilité de la machine à son contenu mémoire :

- $C(s,t) = C(t,s)$
- $C(s,t) = C(t) + C(s|t)$

4.1.2.8 Entropie de Shannon et de Kolmogorov

On peut définir la quantité d'information que x possède sur y par :

$$I_c(x : y) = C(y) - C(y|x)$$

A ce titre

$$I_c(x : x) = C(x) - C(x|x) = C(x) - 0 = C(x)$$

$C(x)$ définit donc la quantité d'information que x possède sur lui même.

$H(x)$ est l'entropie dont nous avons vu qu'elle représentait le nombre en moyenne suffisant de bits pour décrire une sortie x dans la théorie de Shannon. On a vu que dans cette dernière apparaissait la notion de code optimal, permettant de coder une sortie de la manière la plus brève possible connaissant a priori les probabilités d'apparition des caractères.

$C(x)$ est le nombre de bits minimal pour décrire algorithmiquement x .

Ces notions se ressemblent étrangement. On peut démontrer l'existence d'une relation explicite entre entropie stochastique et complexité algorithmique :

théorème : Soit $x = y_1y_2\dots y_m$, telle que y_i peut prendre un ensemble de configurations binaires notées k . Alors, à une constante additive près on a :

$$C(x) < m(H - \epsilon(m))$$

avec $H = \sum p_k \log(p_k)$ et $\epsilon(m) = 2^{r+1}l(m)/m$. $\epsilon(m)$ tend vers 0 quand m tend vers l'infini.

En d'autres termes, les 2 notions se rejoignent pour les chaînes de taille arbitrairement grandes. A ce moment, une chaîne peut apparaître comme étant constituée d'un ensemble de motifs de base aléatoirement distribués. Il en est ainsi par exemple d'une chaîne binaire comportant des "1" en proportion bien précise, 10% par exemple, mais distribués aléatoirement.

4.1.2.9 Récapitulatif

Nous avons pu définir de manière cohérente :

- la complexité de Kolmogorov $C(x)$
- la complexité conditionnelle $C(x|y)$
- la quantité d'information que x possède sur y : $I_c(x : y) = C(y) - C(y|x)$
- la complexité combinée $C(x,y)$ associée à la génération de 2 chaînes.

Bien d'autres notions sont construites à partir de cette idée, notamment la complexité généralisée, prenant en compte le caractère borné de certaines ressources comme la mémoire ou le temps.

4.1.3 Chaitin : complexité de préfixe (1966)

4.1.3.1 Présentation

L'analogie des codes préfixes de la théorie de Shannon est la complexité de préfixe, dérivée de la complexité algorithmique de Kolmogorov [9][11]. On ne prend en compte que les codes qui ne peuvent pas se retrouver être le début d'un autre code. La complexité de préfixe d'une chaîne x , notée $K(x)$, est la plus petite représentation possible de x telle que cette représentation ne peut pas être le début de la représentation d'une autre chaîne. En général, on notera x^* la représentation minimale de x . On a donc :

$$K(x) = |x^*|$$

4.1.3.2 Théorème d'invariance

Le théorème d'invariance se démontre pour $K(x)$ comme pour $C(x)$ dès lors que l'existence d'une machine préfixe universelle est assurée. La fonction préfixe exécutée par une telle machine doit pouvoir simuler toute fonction calculable préfixe. En d'autres termes Ψ_0 est telle que :

$$\forall \Psi \text{ fonction calculable préfixe } \exists c_\Psi \text{ constante} / \forall x, y \in \mathbb{N}, C_{\Psi_0}(x|y) \leq C_\Psi(x|y) + c_\Psi$$

On notera alors :

$$\begin{aligned} K(x|y) &= C_{\Psi_0}(x|y) \\ K(x) &= C_{\Psi_0}(x|\epsilon). \end{aligned}$$

4.1.3.3 Machine préfixe

Avant de construire une machine universelle, nous allons définir un modèle de machine préfixe à partir d'une machine de Turing à 3 bandes :

- 1 bande de données monodirectionnelle, à lecture seule.
- 1 bande résultat monodirectionnelle également, à écriture seule.
- 1 bande de travail bidirectionnelle, réinscriptible.

Les différentes opérations possibles sont les suivantes :

- recopie case bande données sur bande travail; déplacement bande de données
- écrire 0 ou 1 sur bande de travail
- déplacement dans un sens ou l'autre de la bande de travail
- écrire 0, 1 ou un séparateur sur la bande résultat; déplacement bande résultat
- arrêt
- éventuellement : consultation d'un oracle.

Nous imposons en outre à la bande de données de ne comporter que les caractères 0 et 1. Pas de séparateur ou de caractère de fin de chaîne prévu. L'exécution doit se terminer par elle-même et non par lecture d'un caractère spécial. Une fois l'arrêt obtenu, la partie de la bande de données effectivement lue lors de l'exécution représente le programme générant la sortie. L'ensemble de tels programmes possède nécessairement la propriété de préfixe. Si l'un contenait un autre comme préfixe, son exécution serait interrompue au moment où se serait terminé le programme qu'il possède en préfixe.

Sur un tel modèle de machine, la propriété de préfixe signifie donc que l'on impose aux programmes de se terminer par eux-mêmes. Il est possible de revenir ensuite au modèle de machine à 1 bande et de conserver cette conclusion.

C'est pourquoi la complexité de Chaitin est parfois appelée complexité pour programmes auto-délimités. Ces programmes incluent implicitement une information relative à sa propre longueur. Un programme auto-délimité peut se déduire d'un programme simple en ajoutant cette information. On peut en déduire que pour une chaîne s :

$$C(s) \leq K(s) \leq C(s) + C(C(s)) \leq C(s) + K(K(s)) \leq C(s) + \log_2(s)$$

à quelques termes d'erreurs près.

4.1.3.4 Machine préfixe universelle

Les machines préfixes constituent un ensemble infini dénombrable. Il est possible de concevoir une machine préfixe qui serait capable de simuler n'importe quelle autre au moyen d'un programme qui serait simplement encodé dans le nombre de zéros initial de la bande de données. Il suffirait que ce nombre corresponde au numéro de la machine préfixe à utiliser pour la suite du calcul. Un tel encodage serait conforme à la propriété de préfixe.

Cette possibilité est à la base du théorème d'invariance pour la notion de complexité de préfixe. La fonction calculée par une telle machine est en effet bien une fonction universelle ayant la propriété de préfixe et peut donc être assimilée à la fonction Ψ_0 , fonction universelle dont l'existence est nécessaire au théorème d'invariance.

4.1.3.5 Variantes

De même que pour C , nous pourrions définir pour K des notions dérivées comme :

- la complexité de préfixe conditionnelle $K(x|y)$, plus court programme préfixe générant x à partir de y ,
- la complexité combinée $K(x,y)$, plus court programme préfixe générant x et y avec un moyen de les distinguer
- (caractère séparateur par exemple),
- l'information mutuelle : $K(s:t) = K(s) + K(t) - K(s,t)$

Cette dernière notion mesure le degré d'indépendance de 2 chaînes. Si $K(t) = K(s,t)$ alors $K(s) = K(s:t)$, s est algorithmiquement redondant.

4.1.3.6 Propriétés

Les relations suivantes sont vraies à une légère dépendance près du comportement des machines à l'égard de leur contenu en information :

$$\begin{aligned}K(s,t) &= K(t,s) \\K(s,t) &= K(t) + K(s|(t,K(t))) \\K(s,t) &< K(s) + K(t)\end{aligned}$$

L'avant dernière relation est à rapprocher de son équivalent chez Kolmogorov : $C(s,t) = C(t) + C(s|t)$. Sans la connaissance de $K(t)$, l'équivalent brut ne serait vrai qu'à un terme logarithmique près.

A l'opposé, l'équivalent chez Kolmogorov de la dernière relation n'est garanti qu'à un terme logarithmique près. Ici, la condition d'arrêt implique que le programme a une connaissance de sa propre longueur, ce qui implique un nombre de bits fonction du logarithme de cette longueur. Les termes logarithmiques se trouvent donc implicitement présents dans la condition d'auto-délimitation.

Une des conséquences de cette dernière relation est que la complexité d'une chaîne n'a de signification que si elle se retrouve seule en sortie. Un algorithme très simple permet en effet de générer successivement toutes les chaînes possibles par ordre croissant de longueur. On rectifie donc la définition : la complexité d'une chaîne est le plus court programme permettant de la générer *et de ne générer qu'elle* avant de s'arrêter.

4.1.3.7 Complexité réversible

Nous pouvons dès à présent présenter la notion de complexité réversible qui se limite à des calculs de fonction bijective $x \leftrightarrow y$ permettant d'envisager l'existence d'une fonction réciproque. Nous verrons que cette bijectivité est toujours assurée lorsque le résultat comporte une copie de la donnée : $y = x, y'$.

Soient 2 algorithmes irréversibles, l'un calculant y à partir de x , l'autre calculant x à partir de y . Ils peuvent être combinés pour former un algorithme réversible calculant y à partir de x .

$$\exists i, j : \phi(x) = y \text{ et } \phi(y) = x \quad \Rightarrow \quad \exists k / \psi_k(x) = y$$

On démontre qu'il existe une machine de Turing préfixe universelle, et donc un équivalent au théorème d'invariance attaché à cette notion, ce qui permet de créer la notion de complexité de préfixe réversible $KR(x)$, la plus petite représentation réversible de x satisfaisant à la condition de préfixe.

4.1.4 Lloyd et Pagels : profondeur thermodynamique (1988)

4.1.4.1 Idée

autre tentative de mesurer le niveau d'organisation d'un système : la profondeur thermodynamique[29]. Bâtie sur l'idée que l'organisation doit faire apparaître une différence de complexité en fonction de l'échelle. Les objets parfaitement ordonnés ou parfaitement aléatoires ont une profondeur thermodynamique faible. Un objet et sa copie ont presque la même profondeur que l'objet seul, à l'algorithme de recopie près. Pour les systèmes aptes au calcul, la mesure de complexité calculatoire est un cas particulier.

On part de l'idée que la complexité doit correspondre à une semi-corrélation. En précisant les notions d'additivité et de continuité la mesure sera unique. il faut une définition :

- fonction de la probabilité d'arriver à un état
- proportionnelle au nombre de chemins d'accès à un état si ces chemins sont équiprobables
- additive : la mesure pour passer de b à d via c doit être celle pour passer de b à c + celle pour passer de c à d .

4.1.4.2 Profondeur d'un état

Si l'on prend en compte l'ensemble des trajectoires p permettant à un système d'arriver à un état, la complexité moyenne de l'état doit être proportionnelle à l'entropie de Shannon de l'ensemble des trajectoires permettant d'aboutir à cet état.

$$S = -\sum(p_i \ln(p_i))$$

La mesure de complexité d'un état macroscopique d accédé par le i° chemin possible est $-k \ln(p_i)$. où p_i est la probabilité associée au chemin. En prenant pour k la valeur de la constante de Boltzmann on définit la profondeur d'un état d par :

$$D(d) = -k \ln(p_i)$$

quantité d'information (au sens de Shannon) définissant le i° chemin d'accès à l'état d . Prenons l'exemple d'une porte logique ET. Il existe 3 possibilités d'obtenir une sortie FAUX. Si l'on admet que ces 3 possibilités sont équiprobables on aura $D(\text{faux}) = -k \ln(1/3) = k \ln(3)$. L'additivité de la notion permet de calculer la profondeur d'un état de sortie à la fin d'un calcul complexe.

On notera que lorsque le chemin pour parvenir à l'état de sortie est le chemin optimal (nécessitant le minimum d'information au sens de Shannon) la notion est analogue à celle de complexité algorithmique.

4.1.4.3 Profondeur thermodynamique

La profondeur thermodynamique étend la notion de profondeur d'état pour les systèmes macroscopiques dont le comportement est géré par un hamiltonien. La profondeur est alors proportionnelle à la différence entre l'entropie globale thermodynamique du système et l'entropie "fine", fonction du volume de l'espace des phases occupé par la trajectoire ayant accédé à l'état. On rappelle que l'espace des phases, dans lequel sont représentés par des points l'ensemble des états possibles d'un système, est divisé en cases de volume fini non nul dont la taille est fixée par les théories quantiques. Ces théories mettent en évidence le fait que deux états occupant la même case sont impossibles à distinguer. Une trajectoire dans l'espace des phases est donc bien associée à un volume. La profondeur thermodynamique est la différence entre :

- l'entropie de Boltzmann S , qui prend en compte l'ensemble des états accessibles du système,
- l'entropie "fine", qui ne prend en compte que les états accédés le long d'une trajectoire définissant une évolution du système.

La profondeur thermodynamique s'écrit donc :

$$D_T = S - S_0$$

4.1.4.4 Génération d'entropie

un calculateur peut effectuer 2 catégories d'opérations :

- de la copie, qui crée des corrélations ou information mutuelle
- des opérations logiques, séparant l'information encore utile de celle qui ne l'est plus, et générant de l'entropie.

L'entropie est artificiellement créée à un niveau élevé, car au niveau élémentaire, l'écrasement d'état n'existe pas. Ainsi dans le cas de la porte ET vu plus haut, le bit perdu après l'opération se retrouve dans la modification de la dynamique des électrons au sein d'un composant électronique. Cette information perdue se répercute dans une modification thermodynamique de l'environnement physique. Dans le cas de la porte ET, l'entropie générée est $k \ln(3)$.

4.1.4.5 Machines réversibles

Les systèmes calculatoires et les systèmes thermodynamiques se distinguent par le fait que le calcul réversible semble possible alors que la thermodynamique se fonde sur la notion d'irréversibilité. Le fait qu'il puisse exister des trajectoires de calcul réversibles n'engendrant pas d'entropie semble compromettre l'universalité de la notion de profondeur thermodynamique. En fait, l'existence d'une trajectoire réversible sur une moyenne effectuée sur l'ensemble des trajectoires possibles ne change pas grand chose. En outre, la trajectoire réversible nécessite un temps d'attente prohibitif et n'est pour cela jamais présente dans la nature.

4.1.4.6 Conséquences

La profondeur thermodynamique implique une relation entre la cosmologie et le caractère aléatoire de nombres dès lors qu'ils représentent l'état d'un système. Quand un système représente un état logique profond, l'état est thermodynamiquement profond. Vu le caractère fini de la profondeur thermodynamique de l'Univers, certains nombres très grands ne sont pas représentables. On en conclut à l'existence de nombres dont la description concise est inconnaissable dans notre univers, indistinguables de nombres

aléatoires. L'avenir de l'Univers pourrait les faire sortir de ce statut. De même, au début de l'Univers, π était aléatoire.

4.1.4.7 Remarques

Pour leurs inventeurs, l'intérêt de la profondeur thermodynamique est de s'appliquer à tout système, calculatoire ou non, en ayant des propriétés de base intéressantes : continuité, monotonie, additivité. La complexité de 2 systèmes identiques ne diffère de celle d'un seul système que par la complexité du système de copie.

Nécessitant la connaissance de toutes les trajectoires possibles pour accéder à un état, il s'agit d'une notion non effective.

4.1.5 Bennett : profondeur logique (1988)

4.1.5.1 Complexité, complexités

L'approche de Kolmogorov est-elle la seule possible pour définir la complexité ? Ce n'est pas l'avis de Charles Bennett qui propose de faire la distinction entre la complexité aléatoire de Kolmogorov et la complexité organisée dont il propose une définition à l'aide de sa notion de profondeur logique[15]. La complexité organisée tend à mesurer le niveau d'organisation d'un système et de cerner ce qui fait la différence entre un objet complexe et un être simple, qui sont tout aussi difficile à décrire entièrement.

Un orgue à tuyaux est un instrument extrêmement complexe dans ce sens qu'il comprend un grand nombre de pièces qui ont toutes une forme bien précise et un rôle bien précis. Les relations que ces pièces entretiennent entre elles sont telles que l'ensemble satisfait à une fonction évoluée : permettre la restitution d'un ensemble potentiellement infini (mais dénombrable) de créations musicales. Pourtant les plans de réalisation peuvent être relativement réduits. Tous les tuyaux se ressemblent et la description de l'ensemble se déduit à partir d'un nombre relativement restreint d'informations ajoutées à une description générale. De même pour les touches ou les valves, de sorte que l'ensemble des plans de la machine est relativement réduit.

Par contre, si l'on prend dans le détail la description de chaque nervure de boiserie, un orgue a une complexité au sens de Kolmogorov relativement élevée : la description est incompressible. Mais cette complexité ne met pas en évidence la différence d'organisation qui existe avec un tas de bois et de métal quelconques, tout aussi difficiles à décrire. Il existe une différence entre la description complète et la description effective.

La définition de la complexité organisée ne réside donc pas dans la taille d'une description. Peut-on la situer dans le temps de calcul d'un algorithme chargé de reconstruire l'objet à partir de sa description effective ? Probablement. Mais quelle description faut-il utiliser ? Celle permettant la reconstruction la plus rapide possible ? En informatique, aucun programme n'est plus rapide que celui n'effectuant aucun calcul parce que possédant la description la plus complète (le programme "Print" est le plus rapide pour régénérer une chaîne donnée). Cette proposition n'est donc pas satisfaisante.

Chaitin propose de prendre en compte le temps d'exécution à partir de la description la plus concise. On distingue donc :

- la complexité aléatoire de Kolmogorov : $K(s) = |s^*|$ = plus courte description effective de s
- la complexité organisée, déduite de la profondeur logique de Bennett : $P(s)$ = temps de calcul de s^* , programme minimal de s .

En d'autres termes, si l'orgue est un instrument complexe, c'est parce que sa construction demande un temps important et un nombre d'opérations importantes à partir des plans de l'instrument. Les objets peuvent se classer ainsi en :

- objets simples au sens de Kolmogorov et simples au sens de Chaitin, ex : 11111111111111
- objets simples au sens de Kolmogorov et complexes au sens de Chaitin, ex : 3,1415926535...
- objets complexes au sens de Kolmogorov et simples au sens de Chaitin, ex : tas de bois
- objets complexes au sens de Kolmogorov et complexes au sens de Chaitin, ex : orgue.

4.1.5.2 K-profondeur logique

De même que pour Kolmogorov on introduit la notion de c-incompressibilité, pour Chaitin on introduit la notion de k-profondeur logique.

Il est facile de comprendre qu'une description effective minimale peut introduire des temps de calcul très élevés alors qu'une description presque aussi courte peut permettre une exécution beaucoup plus rapide. Parmi les programmes produisant une chaîne s , prenons donc ceux dont la taille diffère au plus de k bits du programme minimal. Et parmi ces programmes prenons le plus rapide. Le temps d'exécution de ce programme définit la k-profondeur logique de la chaîne s .

La k-profondeur logique représente donc le temps d'exécution du plus rapide des programmes p produisant s tel que $(|p| - K(p) \leq k)$. Autrement dit, c'est le temps d'exécution du plus rapide des programmes k-incompressibles produisant s .

4.1.5.3 Invariance

pour la k-profondeur il existe un théorème d'invariance :

"pour 2 MTU rapides $\exists c /$ la k-profondeur pour l'une soit la même que la (k+c)-profondeur pour l'autre à une cte additive et une multiplicative près".

4.1.5.4 Propriétés

Bennett a montré que la notion de profondeur logique répond à la loi de croissance lente. Cette complexité ne peut augmenter que lentement (avec de possibles diminutions brusques). Cela semble être le cas dans la nature. L'organisation ne peut arriver qu'à vaincre lentement la tendance normale au désordre. Ainsi la complexité de l'être humain n'a pu apparaître qu'après quelques milliards d'années d'évolution d'un processus de sélection et d'évolution.

La distinction entre complexité organisée et complexité aléatoire permet de se poser la question de savoir à laquelle est le mieux attachée la notion physique d'entropie. Selon Delahaye [15], cette distinction permet d'envisager que l'augmentation d'entropie ne soit pas incompatible avec l'augmentation du degré d'organisation. La complexité organisée, autorisant la réversibilité, semble d'un rapport peu évident avec la thermodynamique, ne connaît pas le même destin que sa collègue aléatoire. "avec la conception de Bennett il n'y a aucune contradiction entre la seconde loi de la thermodynamique et l'augmentation de la complexité organisée dans l'Univers. Le monstre de la mort thermique, empêchant à terme toute vie et toute intelligence a disparu". l'optimisme peut être justifié mais apparemment prématuré tant que l'étude de liens entre complexité organisée et thermodynamique n'aura pas été approfondie.

4.1.5.5 Intérêt

Un système physique isolé évolue normalement vers le désordre. C'est une des interprétations possibles du second principe de la thermodynamique. Mais on constate qu'au sein de cette évolution normale des systèmes se forment des îlots de complexité que sont les êtres vivants. Au fil des générations ils semblent évoluer vers un degré d'organisation croissant. L'apparition locale de la complexité dans les systèmes est-elle une nécessité ? La formalisation de la notion de complexité organisée va permettre peut être de donner des éléments de réponse. D'autant que le principe de croissance lente semble se vérifier : il faut de nombreuses générations pour gagner un peu au niveau du degré d'organisation.

Mais les obstacles demeurent, car la notion de complexité organisée se heurte à un grand nombre de limitations "à la Gödel". La question de l'apparition du complexe est peut-être indécidable. Et même si elle est résolue, il ne faudra pas pour autant en conclure que celle du vivant ne posera plus de problèmes. Complexe et vivant sont encore deux notions non distinguées mathématiquement et qui semblent pourtant très différentes. Pourquoi l'évolution vers le complexe a-t-elle donné des hommes plutôt que des orgues ?

En fait, elle a aussi donné des orgues puisqu'elle a abouti à des êtres capables de les construire. Peu importe. Personne n'a eu l'idée d'inventer les bétarouffleurs mécaniques. La question est donc de savoir pourquoi la nature a inventé des hommes plutôt que des bétarouffleurs.

4.1.6 Zurek : distance informatique (1989)

4.1.6.1 Coût en information du calcul

Pour cerner le coût en information du calcul[48], considérons un calcul dont les données sont codées dans une chaîne initiale i , et dont le résultat est codée dans une chaîne finale f . Dans un tel calcul, f est moins riche en information que i . En effet, certaines opérations peuvent faire perdre de l'information (effacement ou écrasement de valeur...) alors qu'aucune n'en crée (un résultat de calcul ne recèle pas plus d'information que ses opérands).

On peut imaginer que, à chaque opération irréversible, on décide de stocker l'information normalement perdue : variables avant effacement, origines des branchements et autres. Ces informations dont une exécution normale se débarrasse sont considérées comme un déchet du calcul et notées $d(i,f)$. Il est possible à l'arrivée d'en réduire la taille éventuellement en s'appuyant sur la connaissance de f . Le coût du calcul $\delta S(i \rightarrow f)$ correspondra au nombre de bits qu'il sera finalement nécessaire d'effacer pour se retrouver dans l'état final. En d'autres on aura :

$$\delta S(i \rightarrow f) = K(d(i,f)|f).$$

Notons que le déchet permet de retrouver la donnée à partir du résultat. Il est donc toujours possible de concevoir un programme optimal $i|f$ permettant de retrouver i à partir de f . On a :

$$K(i|f) \leq \delta S(i \rightarrow f)$$

Notons que l'on a :

$$\delta S(i \rightarrow f) \leq |i|$$

Il est en effet toujours possible de transformer le déchet en une réplique de la donnée. Pour cela on duplique f , ce qui peut se faire sans déchet nouveau, et on se sert d'une des copies ainsi que du déchet pour reconstruire i . A la fin, il ne restera que f et i . Par ailleurs on a :

$$K(f) + \delta S(i \rightarrow f) \geq K(i) \Rightarrow \delta S(i \rightarrow f) \geq K(i) - K(f)$$

sinon, on pourrait coder i de manière plus courte que sa complexité, à partir de f^* et $(d(i,f)|f)^*$. L'égalité peut être atteinte lorsque i et f sont indépendants, par exemple dans le cas d'une remise à zéro d'une chaîne aléatoire. Retenons que le coût du calcul vaut a minima $K(i) - K(f)$.

4.1.6.2 Mise à jour

Imaginons que l'on veuille transformer une chaîne d en une chaîne r . Il peut s'agir par exemple d'une remise à jour d'un fichier. Pour cela on a besoin en entrée de d et de $r|d$. A la fin on aura r et un déchet qui permet le calcul inverse, soit $d|r$.

$$d, r|d \rightarrow r, d|r$$

$d|r$ doit être finalement effacé, alors que $r|d$ aura été fourni en plus au système. Il serait tentant de noter cette différence par une différence de signe algébrique et de noter la fluctuation de complexité par :

$$\delta K = K(d|r) - K(r|d)$$

en fait, cela laisse en entendre que l'acquisition d'information peut créer des corrélations et faire baisser la complexité ce qui n'est pas toujours le cas.

4.1.6.3 Distance informatique

Essayons une autre approche. Regardons ce que représente la quantité totale d'information à mettre en jeu pour transformer une chaîne d en une chaîne r . Cette quantité d'information se définit comme la somme de l'information à rajouter au départ et de l'information à retrancher à l'arrivée. Cette fois, on ne s'occupe plus de signe algébrique. On compte tous les échanges entre le calculateur et le milieu extérieur.

$$\Delta(d,r) = K(d|r) + K(r|d).$$

Cette grandeur possède toutes les propriétés nécessaires pour pouvoir être considérée comme une mesure. Elle est définie positive :

$$\Delta(d,r) \geq 0 \quad \forall d, \forall r$$

elle est symétrique :

$$\Delta(d,r) = \Delta(r,d) \quad \forall d, \forall r$$

elle répond à l'inégalité triangulaire :

$$\Delta(d,i) + \Delta(i,r) \geq \Delta(d,r) \quad \forall d, \forall i, \forall r$$

Δ est bien une distance et définit une métrique sur l'ensemble des chaînes binaires.

4.2 Lien information-hasard

4.2.1 Chaitin : théorie algorithmique de l'information (1971)

4.2.1.1 Définition d'une chaîne aléatoire

L'étude du lien entre information et hasard est la justification principale de la théorie de Kolmogorov.

Soient 2 chaînes

1111111111
1001011010

L'une de ces 2 chaînes est aléatoire. Laquelle ? La première ? Pourtant, par tirage au sort d'une succession de valeurs de bits, la seconde a exactement la même probabilité de sortir que la première. De sorte que si une chaîne était définie comme aléatoire par le seul fait qu'elle puisse être obtenue par tirage au sort, toutes les chaînes seraient aléatoires. Une telle définition serait sans intérêt. Ce que l'on cherche, c'est une définition utile, qui formalise l'idée intuitive selon laquelle les chiffres sont parfois agencés selon des motifs plus ou moins évidents qui permettraient éventuellement de parier sur les valeurs des chiffres suivants.

Inversement, nul doute qu'il est toujours possible d'imaginer une relation entre les chiffres d'une chaîne autorisant sa reconstruction ainsi que le pari sur les chiffres suivants. Si le seul critère distinguant les chaînes aléatoires des autres résidait dans l'absence de relations entre chiffres, aucune chaîne ne serait aléatoire. Mais on conçoit que la complexité des relations à trouver entre chiffres varie beaucoup selon la chaîne.

Après bien des réflexions, on en vient à l'idée de prendre en compte la complexité minimale qu'une relation doit avoir pour permettre de retrouver la chaîne. Dès lors qu'aucune relation entre chiffres ne peut décrire une chaîne de manière plus simple que la chaîne elle-même, la chaîne est aléatoire. C'est la complexité de Kolmogorov qui nous permet de formaliser cette idée. La chaîne est aléatoire si elle ne peut pas être générée par un programme plus court qu'elle-même, c'est à dire si sa complexité est égale à sa longueur [9].

Notons dès à présent qu'un programme minimal est une chaîne aléatoire, sinon il serait possible de trouver plus minimal en appliquant un algorithme de compression indépendant de la donnée, donc intégré à la constante.

4.2.1.2 Théorème d'incomplétude

Hilbert avait caressé un temps le rêve de pouvoir fonder les mathématiques à partir d'un système d'axiomes et de règles d'inférence, il aurait pu énumérer de manière automatique tous les théorèmes. Gödel est venu mettre fin à ses espoirs.

Gödel s'est appuyé sur le paradoxe du barbier qui est l'équivalent du paradoxe d'Epiménide " cette phrase est fausse". La version utilisée par Gödel est la suivante : "ce qu'affirme cette phrase ne peut pas être prouvé". Si le système formel dans lequel est construite cette affirmation n'arrive pas à la prouver il

est incomplet, s'il y arrive il est inconsistant. Gödel transpose les propriétés du système formel en propriétés des nombres entiers par un codage numérique du système et des preuves. L'incomplétude du système formel entraîne celle de l'arithmétique des entiers naturels. Le rêve de Hilbert restera un rêve.

Turing a repris sa version du paradoxe en montrant qu'il était impossible de concevoir un programme pouvant reconnaître les seuls programmes qui ne se reconnaissent pas eux mêmes. Ainsi il existe des fonctions incalculables.

Dans le cas de la complexité de Kolmogorov, le paradoxe qui nous intéresse est le paradoxe de Berry : "trouver le plus petit entier non définissable en moins de mots que n'en contient cette phrase". Il est évident qu'un tel nombre est défini par la précédente phrase elle même[10].

L'équivalent informatique du paradoxe de Berry est "trouver une chaîne de bits dont on peut prouver qu'elle est de complexité supérieure à ce programme". Nous allons nous en servir pour montrer qu'au sein d'un système formel, il est impossible de montrer qu'une chaîne donnée est de complexité supérieure à une valeur l donnée supérieure à la complexité du système formel.

Pour cela, on considère un programme dans lequel est encodé un axiome du système formel et les règles de dérivation. Il génère toutes les dérivations de l'axiome par ordre croissant de taille. Dès qu'il trouve une dérivation de complexité supérieure à l , il l'imprime et s'arrête.

Le programme constitue un codage de la chaîne trouvée. Excepté pour un nombre fini de valeurs de l , ce codage est par construction plus petit que la complexité de la chaîne, ce qui est impossible par définition de la complexité. Il existe donc des valeurs de l pour laquelle le programme correspondant ne peut exister.

4.2.1.3 Conséquences

Dans un système formel il est impossible de prouver qu'une chaîne est aléatoire par un programme de taille inférieure à lui. Un système formel de taille finie est donc nécessairement incomplet. On retrouve l'incomplétude de Gödel.

L'une des premières conséquences est que la complexité de Kolmogorov ne peut être déterminée dans le cas général (comment savoir qu'une chaîne est à son niveau minimal de description, donc aléatoire, si l'on ne dispose pas d'un programme de taille suffisante, ce qui ne peut intervenir que dans un nombre fini de cas ?)

Les vrais générateurs de nombres aléatoires doivent donc avoir une taille infinie pour pouvoir générer des suites indéfinies de valeurs. Comme les modèles humains sont nécessairement limités (on a même vu que l'objet de la science est de créer les modèles les plus restreints possibles), les modèles physiques doivent nécessairement rencontrer le hasard quelque part, soit comme un élément fondamental des équations, soit comme une donnée irréductible des conditions aux limites.

Nombreux sont les exercices de probabilités pour débutants qui précisent dans leur énoncé une phrase du genre "on supposera que l'observateur ne fait pas de calculs... ". De fait, le hasard est considéré comme lié à un manque d'information sur le système. De tels énoncés sont irréalistes par le fait que certaines corrélations "non calculées" peuvent amener des résultats réels très éloignés de ceux estimés. Une connaissance plus grande du système aurait permis de meilleures prévisions. Mais aucune connaissance n'est suffisante pour que l'on puisse s'abstenir de faire appel au hasard. Autrement dit un énoncé de type : "on supposera que l'observateur est apte à effectuer tous les calculs nécessaires pour ne rien laisser au hasard" est un énoncé tout aussi irréaliste que le premier.

L'incertitude quantique découle-t-elle de cette nécessité ? Il y a une différence nette entre l'incertitude quantique et la notion de hasard tel que défini ici. Certes, il subsiste toujours une part d'aléatoire dans l'état d'un système. Mais rien n'interdit chez Kolmogorov de la réduire autant que l'on veut par une connaissance toujours plus grande du système. La mécanique quantique met en évidence une part incompressible d'incertitude due au fait que certaines connaissances sont mutuellement exclusives, la mesure de l'un agissant sur la valeur de l'autre. Le produit des deux grandeurs est donc affecté d'une

incertitude irréductible. Le hasard apparaît comme une brique fondamentale de l'Univers, au même titre que la matière et l'énergie.

5. Temps

5.1 Questions de temps

Pourquoi deux horloges synchronisées et placées côte à côte restent-elles synchronisées quels que soient les phénomènes physiques utilisés ? Pourquoi s'écoule-t-il toujours dans le même sens ? Existerait-il même sans cette caractéristique très spéciale qu'est l'irréversibilité ? Pourquoi cette différence entre un passé connaissable et non modifiable, et un avenir sans cesse remis en cause mais jamais connu d'avance ? Connaît-on tout du temps ? Existe-t-il dans des manifestations où on le pensait absent ? Connaît-on bien le temps ? En résumé qu'est-ce que le temps ?

Les questions de temps sont sans doute les plus troublantes que les humains se soient posées à travers les âges. Puisque tout est lié, peut être une partie des réponses se trouvent-elles dans les concepts manipulés pour définir l'information. Nous allons essayer de le savoir maintenant. Mais d'abord, un bref résumé de l'histoire.

5.2 Le temps à travers les âges

5.2.1 Le temps des grecs

Au commencement, le temps n'était pas infini. Ni dans un sens ni dans l'autre. Il était rond. Tout comme l'année faisait revenir régulièrement les mêmes saisons, une "grande année" devait pouvoir faire revenir les mêmes événements perpétuellement[12]. Le mythe de l'Eternel Retour était déjà explicité au 8^e siècle avant notre ère dans les poèmes d'Hérisode.

La circularité, reflet de la perfection divine dans le temps, le deviendra aussi dans l'espace avec Platon pour qui seul le mouvement circulaire était possible dans le domaine des dieux. Pourtant Platon croyait en une création de l'Univers. Comment la concilier avec une circularité du temps ? La création de l'Univers se fait hors du temps des hommes, tout simplement. Elle n'est pas un événement au sens "historique" du terme.

Aristote libéra le temps de sa circularité en le basant sur le mouvement. Il n'est que "le nombre du mouvement", et existe comme un moyen de les mesurer tous. A ce titre, il est unique pour tous. Cela permet de définir une notion absolue de la simultanéité. Plus tard, Bergson reliera de même temps et mouvement, considéré comme une "spatialisation du temps". Le temps d'Aristote est une grandeur infinie à la fois vers le passé et vers l'avenir, alors que l'espace était considéré comme limité à la sphère des fixes.

Si l'antiquité grecque se posa des questions sur la continuité de la matière, Aristote explicitera l'idée d'un temps continu et indéfiniment divisible. Par là, il réfutera les paradoxes de Zénon d'Elée, notamment le fameux paradoxe d'Achille et de la tortue, en affirmant qu'à une division infinie de l'espace correspondait une division infinie du temps, le rapport des deux pouvant être fini. Le paradoxe de Zénon est même pour lui une preuve de cette divisibilité infinie du temps. La mathématisation de cette idée correcte n'interviendra qu'au 17^e siècle.

5.2.2 Les temps médiévaux

L'Eternel retour n'a pas fini sa vie pour autant. Les philosophes arabes comme Avicenne et Ghalazi, rapporteurs des pensées d'Aristote, auront une conception plutôt Platonicienne.

Certains mettront en avant le christianisme comme base de la notion moderne de linéarité du temps. La "Rédemption Eternelle" fut pour certains la première loi de dissymétrie entre passé et avenir, incompatible avec l'Eternel retour, comme l'expliquera Saint Augustin qui réfléchit longuement à la question. "Si l'on ne me le demande pas, je crois savoir ce qu'est le temps. Mais si on me le demande, je ne le sais plus" écrivait-il. Pour Saint Augustin, "Avant le ciel et la Terre, il n'y avait pas de temps".

Au 12^e siècle le philosophe juif arabe Maïmonide approfondira une idée analogue en disant que le temps n'est qu'une manifestation de la matière et n'existe pas sans elle. Comment le temps existerait-il sans phénomènes susceptibles de marquer la durée ?

5.2.3 Le temps des révolutions de la pensée

Galilée fut le premier à faire intervenir le temps dans une théorie physique en notant la proportionnalité entre vitesse et temps de chute d'un corps. Cette idée n'était pas évidente et il a changé plusieurs fois sa vision des choses, affirmant successivement que la vitesse de chute d'un corps serait constante sans la poussée d'Archimède exercée par l'air, que la vitesse était proportionnelle à la distance parcourue, avant de la rendre proportionnelle au temps de chute.

Il faudra attendre l'époque moderne pour qu'une vision d'un temps absolu, inauguré par Newton, nous rende inacceptable l'idée d'une origine passée du temps. Newton formalisa le premier la notion physique du temps. "Le temps absolu vrai et mathématique, sans relation à rien d'extérieur, coule uniformément et s'appelle durée...". Temps absolu donc, comme pour Aristote. Il faudra un Einstein pour relativiser tout cela.

5.2.4 Les temps modernes

Les réflexions sur le temps ne font que commencer vraiment. L'"Eternel Retour" que l'on croyait révolu revient sans cesse. Des Kurt Gödel et des Stephen Hawking veulent le faire revivre. Un temps "cosmologique" veut se prendre pour le temps absolu newtonien au côté du temps relatif local d'Einstein. Le Big Bang veut faire ressortir l'Origine des temps de son néant.

Eternel retour ou pas, l'histoire est un perpétuel recommencement.

5.3 Les flèches du temps

5.3.1 Le problème de l'irréversibilité en physique

A l'heure actuelle, la quasi totalité des lois physiques fondamentales sont réversibles. C'est dire qu'un phénomène connaît toujours sa réciproque. Tout phénomène fondamental observé de près peut aussi bien se dérouler à l'endroit qu'à l'envers sans violer une loi physique. Ceci est vrai au point que l'on a longtemps postulé la symétrie passé-futur comme un principe fondamental de l'Univers.

Pourtant quand on observe un film en train de se dérouler à l'envers, il est très facile de se rendre compte que des choses anormales se produisent. Les ronds dans l'eau convergent pour forcer les cailloux à s'éjecter, les cheminées absorbent la fumée de l'atmosphère pour en façonner des bûches dont on fera des arbres qui iront nourrir la terre en rapetissant, les gens régurgitent la nourriture pour aller la vendre aux épiciers. On remarque immédiatement ces anomalies. Il se trouve pourtant que la succession d'événements que l'on observe a exactement les mêmes raisons de pouvoir se dérouler qu'une quelconque succession au sein d'un scénario "direct", car aucune loi physique ne serait violée dans ce monde à l'envers.

Paradoxe pourtant. Pendant très longtemps, le repérage du temps s'est effectué grâce à des phénomènes marqués par la flèche du temps[13]. Que ce soit la combustion progressive d'une mèche ou d'une bougie, ou l'écoulement de l'eau d'un clepsydre ou du sable d'un sablier. Or le gain fantastique en précision dans le repérage du temps est venu dès lors que l'on a utilisé les quelques rares phénomènes mécaniques parfaitement symétriques par renversement du temps, comme l'oscillation d'un pendule, d'un diapason ou d'atomes. Les phénomènes non marqués par la flèche du temps sont les meilleurs repères pour le temps.

Alors le temps peut-il se définir à partir d'autre chose ou est-il une donnée fondamentale ?

5.3.2 Irréversibilité fondamentale

L'idée que le temps est une donnée fondamentale peut s'exprimer selon des manières très différentes menant à des conclusions opposées.

L'une des manières de voir le temps comme fondamental, dont on ne peut cacher qu'elle est le parti-pris ici, est d'affirmer que le temps ne peut se définir autrement que par lui-même et qu'il est donc absent des

lois de la physique. Elles doivent donc toutes se retrouver réversibles. L'irréversibilité n'existe donc pas comme conséquence d'un caractère fondamental des lois élémentaires. Car chaque loi définirait sa propre flèche du temps. Le fait même que des horloges synchrones un temps restent synchrones par la suite indépendamment du phénomène physique utilisé montre bien que le temps se définit en dehors des lois, si ce n'est celle stipulant l'existence du temps lui-même. Sans le temps en elles, les lois de la physique doivent être réversibles. Les causes et les effets sont toujours à un niveau ou à un autre interchangeables.

Une autre manière de voir les choses est de considérer au contraire que l'irréversibilité doit se retrouver au niveau fondamental dans toutes les lois de la science. Le principal représentant de cette vision des choses est le spécialiste des milieux dissipatifs, le chimiste Ilya Prigogine[36]. Pour lui, l'irréversibilité doit se manifester dans toutes les lois physiques, alors que les lois connues sont pratiquement toutes symétriques par rapport au temps, et à toutes les échelles, et alors que les atomes ne semblent pas marqués par la dégradation entropique. Pour lui, tous les systèmes sont "chaotiques" quel que soit l'échelle d'observation. La réversibilité n'est qu'apparente.

Certains avaient pourtant déjà montré que l'irréversibilité macroscopique ne peut s'appuyer sur une réversibilité microscopique. C'est le cas d'hommes comme Kelvin, Goldschmidt et Zermelo qui avaient montré que l'irréversibilité ne pouvait se déduire de la mécanique. A l'époque, la réponse faite par Boltzman en 1877 mettait le point sur le fait que ce ne sont pas des lois d'évolution que naît l'irréversibilité, mais des conditions aux limites.

Nous discuterons plus en détail de cette approche

5.3.3 Les formes de l'irréversibilité.

Autre approche possible, le temps n'est pas posé comme fondamental, et on cherche à le déduire des autres phénomènes physiques. Le temps a ses propriétés propres, dont celle qui marque son existence même: l'irréversibilité. Eddington (qui mit en évidence la première preuve expérimentale de la relativité générale) inventa l'expression de "flèche du temps" pour caractériser cet aspect irréversible du temps macroscopique. D'où naît l'irréversibilité ? Existe-t-il une flèche ou des flèches du temps[25] ? On peut distinguer en effet au moins 6 formes de flèches du temps dont nous allons discuter :

- la flèche statistique,
- la flèche thermodynamique,
- la flèche radiative,
- la flèche informatique,
- la flèche cosmologique,
- la flèche quantique,
- la flèche microscopique.

Nous allons présenter chacune des ces définitions possibles du temps. Mais nous pensons que 6 flèches du temps, cela en fait 5 de trop. Il semble que le temps ne peut pas se définir de plusieurs manières différentes. De sorte que les différentes flèches doivent être en relation les unes avec les autres. Nous nous interrogerons pour savoir comment.

5.4 Flèche statistique

5.4.1 Mathématiques et causalité

Les mathématiques ignorent l'irréversibilité. Il est a priori toujours possible de plonger une relation simple pour en faire une relation d'équivalence. Par exemple la relation

droites parallèles => droites qui ne se coupent jamais

n'est pas une relation d'équivalence. Mais considérons maintenant la relation :

droites parallèles => droites coplanaires
droites qui ne se coupent jamais

nous avons une relation réversible dans le sens où la réciproque est vraie. On peut remplacer " \Rightarrow " par " \Leftrightarrow ". Le premier signe signifie donc que l'on a perdu de l'information entre le premier et le second membre de la relation. Le second que l'on est en présence d'une simple réécriture. On esquisse déjà la nature de la causalité pour un mathématicien : l'effet ne peut contenir plus d'information que la cause. Si l'on plonge la relation dans une loi dans laquelle l'information est intégralement conservée, l'effet et la cause sont interchangeables.

Dans la relation ci-dessus, si l'information qui nous intéresse est que les droites parallèles sont coplanaires, l'autre information constitue un déchet. Si on l'oublie, on perd la réversibilité. Notons que toute relation peut devenir une équivalence si l'on rajoute à droite une copie de ce qui se trouve à gauche, comme ci-dessous :

droites parallèles \Leftrightarrow droites coplanaires
droites parallèles

Dans de telles relations, on exclut l'existence de "causes finales". C'est à dire que chaque terme est influencé par ce qu'il a à sa gauche et influence ce qu'il a à sa droite. La valeur d'un terme ne peut résulter d'une combinaison de ce qui se produirait des deux côtés.

Le principe de causalité consiste à transposer dans le monde physique cette nature des mathématiques en assimilant cause, donnée et passé d'une part, et effet, résultat et futur d'autre part. Avec une telle assimilation, l'exclusion des "causes finales" prend son vrai sens, celui d'exclure des causes qui se situeraient temporellement après l'effet, au grand dam des devins et voyants en tous genres. La question de savoir si la distinction entre cause et effet peut s'appuyer sur autre chose que la distinction entre passé et futur sera revue. Dans la mesure où cette assimilation est postulée, l'outil mathématique est-il en mesure de mettre en évidence une dissymétrie temporelle ?

5.4.2 Inégalité de Bayes

Il existe pourtant une branche des mathématiques qui étudie les lois régissant les systèmes sur lesquels on ne dispose pas de toutes les informations. Il s'agit des probabilités. Elle vise à cerner les propriétés de l'information dont on ne dispose pas encore et à ce titre n'est pas astreinte à la remarque précédemment formulée concernant la dissymétrie induite par perte d'information.

Les probabilités sont un outil créé par l'homme et pour l'homme et qui a pour objectif de lui donner une certaine connaissance de ce qu'il ne connaît pas encore. A ce titre il n'y a donc rien de paradoxal à ce que les connaissances préalables influent sur le résultat. Par exemple, si l'on jette 2 dés non pipés, on a 1 chance sur 36 d'obtenir un double six. Mais si on jette les 2 dés l'un après l'autre, le résultat change à la vue du résultat du premier lancé.

- Si le premier dé donne un 6, les chances d'en avoir un double s'élèvent à 1 chance sur 6.
- Si le premier dé n'est pas un 6, les chances deviennent nulles.

La probabilité a donc été modifiée par la seule connaissance dont dispose l'expérimentateur. On peut dire que ce changement dans les valeurs probables est une opération irréversible. On ne peut revenir aux valeurs probables initiales sauf peut être en "oubliant" les résultats de l'observation.

L'un des fondateurs du calcul des probabilités, Bayes, découvrit une flèche du temps plus fondamentale dans le calcul des probabilités, en mettant en évidence une différence nette entre "prédiction" et "rétrodiction". En d'autres termes, en probabilités, conditions initiales et finales n'ont pas des propriétés symétriques. Il est permis de se donner des conditions initiales, correspondant à des solutions retardées, mais il est interdit de se donner des "conditions finales", correspondant à des "solutions avancées".

Reprenons l'exemple de notre lancé de dés. Appelons A l'événement qui consiste à avoir un premier dé à la valeur 6. Appelons B l'événement consistant à avoir un double 6. $P(B/A)$ est la probabilité liée à l'événement B connaissant A, $P(A/B)$ la probabilité d'avoir A connaissant B. Quelle relation entretiennent les 2 grandeurs ?

Dans notre cas, $P(B/A) = 1/6$. Que vaut $P(A/B)$? Quelle chance a-t-on d'avoir eu un simple 6 quand on en a un double ? On aimerait que $P(A/B)$ se déduise directement et sans autre information de $P(B/A)$ soit simple. Que l'une soit l'inverse de l'autre par exemple. Que $P(A/B)$ vaille 6. Mais que signifie une probabilité supérieure à 1 ? Elle n'a pas de signification reconnue. $P(A/B) = 1$. La probabilité liée au calcul inverse n'est pas l'inverse de celle liée au calcul direct. Les deux grandeurs semblent sans rapport simple.

$$P(B/A) \leftarrow ? \rightarrow P(A/B)$$

C'est à cause des dissymétries contenues dans les probabilités qu'un jeu de cartes que l'on bat évolue vers le désordre. C'est d'ailleurs tout l'intérêt de l'opération. Pourtant les lois de permutation des cartes dans un mélange ne sont pas marquées par la flèche du temps. La permutation de cartes est réversible. Ce paradoxe fut remarqué par les fondateurs même des probabilités, Pascal, Fermat et bien sur Bayes.

Nous vivons dans un monde où les probabilités sont majorées par 1. On n'imagine pas ce que pourrait être un monde dans lequel l'unité serait un minorant pour les probabilités. C'est pourtant bien ce que l'on observe quand on regarde un film à l'envers, monde dans lequel les conditions finales sont certaines quand les conditions initiales ne le sont pas. Un tel monde évolue vers un ordre croissant.

5.5 Flèche thermodynamique

5.5.1 Carnot : thermodynamique macroscopique

5.5.1.1 Notion d'entropie

La thermodynamique élaborée par Carnot fut la première théorie physique à fournir à la dissymétrie passé-futur un support scientifiquement appréhendable. Ceci par la mise en évidence d'une grandeur, l'entropie, notée S , qui ne peut que croître avec le temps. En fonction de la quantité de chaleur Q et de la température T elle se définit par :

$$dS = dQ/T$$

Lorsque un corps chaud est mis en contact avec un corps froid, la quantité de chaleur reçue par le corps froid est égale à la quantité de chaleur cédée par le corps chaud. Mais les températures étant différentes, l'entropie perdue par le corps chaud est plus faible que celle récupérée par le corps froid. Au total, l'ensemble des 2 corps aura une entropie plus grande après l'équilibre.

L'entropie ne peut qu'augmenter dans un système isolé. Cela signifie que températures, ainsi que pressions, ont tendance à s'homogénéiser. Un liquide ne bout ni ne gèle spontanément, un pneu ne se regonfle pas tout seul. Dans les machines thermiques, l'augmentation d'entropie est partiellement transformée en travail, mais elle ne peut être annulée.

L'entropie fait ainsi apparaître une dissymétrie entre passé et avenir : un phénomène n'est pas équivalent à son inverse temporel.

5.5.2 Boltzmann : thermodynamique statistique

5.5.2.1 Espace des phases

La thermodynamique statistique tel que définie par Boltzmann, tend à faire le lien entre matière et énergie, en interprétant l'énergie à partir du comportement microscopique de la matière. L'ensemble des états microscopiques possibles est très élevé. Mais beaucoup d'états sont énergétiquement (ergodiquement) équivalents, au regard des grandeurs macroscopiques comme température et pression. Le lien entre le monde microscopique et macroscopique met en jeu les statistiques.

L'état thermodynamique d'un système n'est entièrement défini que si l'on a une connaissance parfaite de la position et de la vitesse de toutes les particules, soit $6n$ données pour un système de n particules. On peut cependant envisager de décrire correctement un système en divisant le volume qu'il occupe en une multitude de cases et en notant pour chaque case la présence ou non d'une particule. Avec une telle représentation, le nombre de configurations possibles, ou nombre d'états accessibles, est très élevé

mais devient cependant fini. A partir de cette idée a été construite le concept plus élaboré d'espace des phases.

Si l'on considère un espace particulier à $6n$ dimensions, on peut définir dans cet espace l'état du système par la position d'un seul point, et l'évolution du système par une trajectoire. Un tel espace est l'espace des phases. Il pourra être divisé en cases dont la dimension sera fonction du degré de connaissance que l'on peut espérer obtenir sur les grandeurs. On admettra que deux états situés dans une même case sont indifférentiables. La connaissance de la case occupée par le système permettra de définir l'état dans lequel il se trouve. En mécanique classique aucune règle précise ne permet de choisir pour les cases une taille plutôt qu'une autre.

5.5.2.2 Entropie de Boltzmann

Ω est le nombre d'états différentiables (nombre de cases de l'espace des phases) accessibles à un système. A partir de Ω , l'entropie de Boltzmann se définit à partir de la relation :

$$S = k \ln(\Omega)$$

où k est une constante, appelée constante de Boltzmann. L'augmentation d'entropie est donc liée à une augmentation des degrés de liberté du système, caractérisée par une augmentation du volume de l'espace des phases qu'il peut occuper. Plus le nombre de degrés de liberté d'un système est élevé, plus le nombre de cases de l'espace des phases accessibles au système est élevé.

L'entropie statistique s'appuie sur le caractère indifférentiable d'un état au sein d'un ensemble de populations d'états occupables par un système. La notion s'appuie donc sur le fait que les grandeurs accessibles ne permettent pas une distinction complète de tous les états possibles. Par exemple, la température se contente d'une connaissance de l'énergie cinétique moyennée sur l'ensemble des particules. Les configurations caractérisées par la même moyenne ne se distinguent plus.

L'entropie statistique sous entend l'existence d'un lien entre une grandeur physique et la quantité d'information disponible. Le degré de précision avec lequel on cherche à étudier le système conditionne la taille des cases de l'espace des phases.

5.5.2.3 Mécanique quantique

La mécanique quantique permet de mieux définir l'espace des phases en fournissant un découpage limite naturel de cet espace. Ce découpage découle de l'existence d'une limite physique à la connaissance d'un système, donc d'une limite à la quantité d'information dont on peut disposer sur lui.

Il existe en physique des grandeurs dites croisées, qui sont telles que toute connaissance de l'une fait perdre de sa consistance à l'autre. Nous en avons parlé en étudiant les conséquences de l'incomplétude sur le hasard, et nous en reparlerons encore.

L'exemple type de grandeurs croisées est celui du couple position-vitesse d'une particule. Plus on connaît avec précision la position d'une particule, et moins on peut espérer connaître précisément sa vitesse. C'est l'une des relations d'incertitude d'Heisenberg, fondamentales en physique quantique. En vertu de ce principe, la division en cases de l'espace des phases n'est plus arbitraire. Chaque case peut en effet correspondre à un ensemble de configurations indiscernables au regard de la mécanique quantique.

Un autre point influe sur le décompte des états accessibles : l'indiscernabilité des molécules. Au niveau quantique rien ne permet de discerner 2 molécules de même nature. On ne change donc pas d'état en intervertissant 2 particules. On reste dans la même case.

En fait, en prenant en compte les limites imposées par la mécanique quantique sur la forme de l'espace des phases, l'entropie statistique permet de retrouver exactement les résultats de la thermodynamique classique.

Un processus de calcul devant par nature contraindre son évolution, on entrevoit que l'aptitude à calculer doit faire interagir l'outil de calcul avec les degrés de liberté du milieu dans lequel il travaille, milieu dans lequel il trouve l'origine de ses contraintes.

5.5.2.4 Mécanique statistique et irréversibilité

Le caractère croissant irréversible de l'entropie d'un système isolé est lié au fait que les états hétérogènes d'entropie faible sont moins nombreux que les états homogènes d'entropie élevée. Ainsi, si la température a tendance à s'homogénéiser dans un corps c'est parce que, à chaque étape, le nombre d'états voisins accessibles correspondant à une température plus homogène est plus élevé que les autres. Mais si l'on regarde dans le détail, toutes les cases de l'espace des phases sont équiprobables. Nous perdons alors la notion macroscopique de flèche du temps puisque, au niveau élémentaire, les particules sont impliquées dans des chocs élastiques, donc réversibles. L'irréversibilité n'apparaît qu'au niveau macroscopique, au même titre que la température ou la pression. La dissymétrie entre passé et futur est reportée à un autre niveau : l'irréversibilité des lois de la statistique, le reflet des inégalités de Bayes.

5.5.3 Conclusion

En étudiant les liens entre matière et énergie, nous avons eu besoin de faire appel à d'autres protagonistes comme le temps par exemple. Ceci nous confirme le fait que tout est lié et réciproquement.

La nature du passage du réversible microscopique à l'irréversible macroscopique semble se dessiner. Toutes les évolutions possibles d'un système à partir d'un état initial sont équiprobables. Mais sur l'ensemble des évolutions, certaines correspondent à des valeurs quasi-identiques des paramètres macroscopiques comme la température et la pression. Le système évoluera en température et pression vers les valeurs qui correspondent à la probabilité la plus élevée, c'est à dire celles correspondant au plus grand nombre de micro-états.

L'interprétation souvent formulée de l'entropie est qu'elle mesure le degré de désordre d'un système. Elle mesure plutôt la tendance d'un système macroscopique à évoluer vers son état le plus probable. En conséquence, une décroissance spontanée de l'entropie n'est pas impossible mais seulement hautement improbable car il existe beaucoup plus de façon pour un système de faire croître son entropie que pour la faire décroître. La flèche du temps thermodynamique n'est que la conséquence de l'introduction des lois de Bayes dans le système, par le biais d'une vision statistique des phénomènes. Van Der Waals le premier fit cette remarque en 1911. Elle était implicite chez Gibbs, l'un des fondateurs avec Maxwell et Boltzmann de la thermodynamique statistique.

Kelvin et d'autres ont montré que des lois irréversibles ne pouvaient découler de lois réversibles. Ici l'irréversibilité n'est pas dans les lois mais dans les conditions initiales. Ensuite, l'évolution est déterministe. Un système évoluant à contresens a autant de chance d'exister qu'un quelconque autre. mais les conditions initiales permettant une baisse d'entropie ne s'observent jamais en pratique. Y a-t-il une raison ? Ou les lois de la physique elles-mêmes cachent-elles une part d'irréversibilité ?

L'explication statistique constitue un progrès essentiel, mais elle n'est pas entièrement satisfaisante. Surtout par le fait qu'elle n'est qu'un constat de l'existence du temps. La probabilité de voir l'entropie diminuer est faible mais non nulle. Alors que le temps nous apparaît n'avoir aucune chance de s'écouler à l'envers.

5.6 Flèche radiative

5.6.1 Ondes et thermodynamique

Un équivalent au deuxième principe existe pour les ondes. On stipule en physique l'inexistence des ondes centripètes ou convergentes, dites encore "avancées". Cette règle ne découle pourtant pas des équations des ondes pour qui les potentiels avancés peuvent exister. Les solutions correspondantes sont tout simplement exclues comme étant physiquement inacceptables. L'observation montre que les ondes "retardées" correspondent à une dégradation de l'énergie.... Pourtant toutes les équations des formalismes ondulatoires sont réversibles !

Dans le cas des équations de Maxwell, l'habitude est ainsi prise d'écarter les solutions mettant en évidence des ondes électromagnétiques convergentes, alors que les équations ne les excluent pas a priori.

5.6.2 Temps opaque

Parmi les tentatives les plus surprenantes pour éliminer ce paradoxe, il faut noter celle de John Wheeler et Richard Feynman. Ils ont montré vers 1949 que les solutions avancées pouvaient être "effacées" par les solutions retardées à condition que celles-ci bénéficient d'une "opacité" des rayonnements vers le futur, caractérisant la certitude qu'ils soient tous absorbés un jour. Cette "opacité du futur" serait mesurable en comparant les consommations électriques d'une antenne émettrice face à l'espace libre et face à un matériau totalement absorbant. Une expérience tentée en 1973 par R.B.Partridge semble conclure que le futur est opaque... dans l'hypothèse où la théorie est bonne[27].

5.6.3 Ondes avancées acoustiques

Pour ce qui est des ondes acoustiques, on sait certes réaliser aujourd'hui des miroirs à ultrasons qui renversent l'histoire d'une onde pour la faire évoluer à l'envers. Mais ce retournement est imparfait et il s'agit de miroirs "actifs", c'est à dire consommant de l'énergie[19].

5.6.4 Conclusion

Il existe une connexion entre le principe de Carnot et celui des ondes retardées. Elle se formule mathématiquement dans des théories associant un formalisme ondulatoire et corpusculaire : la mécanique quantique. On peut raisonnablement penser que la flèche radiative est liée de manière suffisamment étroite à la flèche thermodynamique pour que l'on puisse considérer qu'il s'agit en fait de la même flèche.

5.7 Flèche informatique

5.7.1 Lien énergie et information

Dans son célèbre ouvrage "une brève histoire du temps"[22], Stephen Hawking considérait que le temps pouvait se définir à partir du sens de calcul des ordinateurs. Il affirmait que les ordinateurs "n'ont pas la mémoire du futur". Ils se souviennent du passé et calculent l'avenir ce qui introduit une dissymétrie. Mais le calcul est bien un moyen de prédire l'avenir et le résultat d'un calcul est bien une mémoire du futur. Il y a peut être davantage de symétries que de dissymétries. Notamment :

- la symétrie entre lecture d'une donnée et stockage d'un résultat,
- la symétrie du calcul lui-même lorsqu'il fait apparaître des opérations réversibles.

Il n'est pas évident que puisse exister une dissymétrie fondamentale permettant à coup sûr de distinguer une machine fonctionnant à l'endroit d'une machine fonctionnant à l'envers. Si l'on se limite à l'observation des échanges mémoire il semble même y avoir similitude parfaite entre une machine fonctionnant dans le sens du temps où à rebours. S'il y a moyen d'observer le calcul les choses sont sans doute plus complexes. Le déterminisme du calcul doit notamment être pris en compte. Celui-ci ne semble notamment pas garanti dans l'exécution inverse, car bien des jeux de données peuvent aboutir au même résultat. On peut donc s'interroger sur les points suivants :

- dans quelles conditions le déterminisme est conservé dans l'exécution inverse,
- que peut-on dire lorsqu'il ne l'est pas.

Si l'exécution directe autant qu'inverse d'un calcul sont toutes deux déterministes rien ne semble permettre de caractériser de manière absolue l'une par rapport à l'autre. En outre, il est envisageable que tout programme puisse être plongé dans un programme réversible, en conséquence directe de ce que nous avons dit sur les liens entre mathématiques et causalité.

Si le déterminisme n'est pas garanti, on peut s'attendre à ce que des notions statistiques de même nature que celles que l'on fait intervenir notamment en thermodynamique, jouent un rôle dans la définition du temps pour une machine de calcul.

On soupçonne donc l'existence de liens entre une possible flèche du temps définie par les ordinateurs, pas nécessairement celle de Stephen Hawking, et d'autres notions du temps comme celle de la thermodynamique. Nous allons essayer d'approfondir ces idées et voir si la science du calcul peut

éclairer le monde de la physique dans sa quête du temps, en abordant le riche domaine de la physique du calcul.

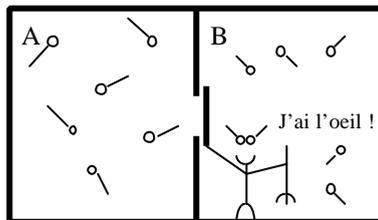
Historiquement, la physique du calcul est née de la considération inverse, celle de trouver les contraintes physiques qui devaient être imposées à un système afin qu'il puisse avoir des aptitudes au calcul. L'objectif était notamment de trouver une limite théorique à la consommation en énergie des ordinateurs.

5.7.2 Maxwell : le démon (1871)

5.7.2.1 Le démon thermique

A la fin du 19^e siècle, il n'était pas encore temps de se demander si un traitement automatisé de l'information pouvait jouer un rôle au sein des lois de la physique. Par contre, il semblait opportun de se poser des questions analogues concernant l'intervention, au sein des systèmes, de comportements intelligents. Une telle intervention peut-elle mettre en échec une loi fondamentale de la physique ? Dans le cas de la thermodynamique, le démon de Maxwell que nous allons maintenant étudier semblait apporter des arguments permettant d'étayer cette idée. Il semblait pouvoir réfuter la seconde loi de la thermodynamique qui veut qu'un système ne puisse évoluer que vers des états d'entropie croissante, la température d'un gaz dans une enceinte ne devant par exemple évoluer que vers l'homogénéisation. Cette loi paraissait pourtant tellement universelle qu'elle était considérée comme l'une des meilleures définitions possibles de la flèche du temps, de la dissymétrie entre passé et futur. Avec son démon, Maxwell posa sans le savoir l'une des bases de la physique du calcul[6].

Imaginons une enceinte contenant un gaz à température homogène. L'enceinte est divisée en 2 compartiments A et B au moyen d'une paroi percée d'un trou microscopique. Une vanne peut être manipulée sans frottements pour ouvrir ou fermer le trou. Imaginons alors qu'un petit démon soit capable d'observer le déplacement des molécules et qu'il ouvre la vanne chaque fois qu'une molécule rapide tend à passer de A vers B par le trou, ou à chaque fois qu'une molécule lente tend à passer de B vers A. Au bout d'un certain temps, la température de B aura augmenté et celle de A aura baissé. Une dissymétrie sera apparue qui pourra être utilisée pour faire fonctionner une machine thermique par exemple. Pourtant le démon n'a besoin de dépenser aucune énergie en apparence. Manipuler une vanne peut se faire sans dépenser de travail, et observer des molécules n'a aucune raison de nécessiter un apport d'énergie.



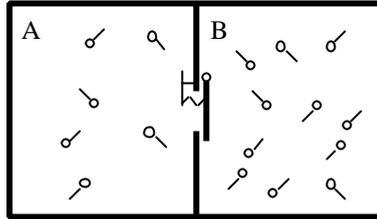
Maxwell croyait à la réalité du second principe de la thermodynamique. Il n'a pas su dire où pouvait se trouver une faille dans son raisonnement. Il a simplement pensé que l'observation de l'état individuel des molécules était impossible. En fait, l'intuition de Maxwell n'était pas la bonne. Elle aiguillera les futures recherches dans des fausses pistes notamment lorsque la mécanique quantique, qui étudie le comportement des particules, sembla confirmer la difficulté d'observer les molécules. Comme nous le verrons, c'est dans l'aptitude à traiter l'information que peut se trouver le moyen de redonner à la seconde loi de la thermodynamique son statut fondamental.

5.7.2.2 Démon de pression

Parmi les nombreuses variantes du démon de Maxwell, l'une des plus intéressantes est celle du démon de pression. L'être intelligent y est en effet remplacé par un automate. Le plus rudimentaire qui soit. Un clapet. Il ne s'agit alors plus de créer une différence de température mais une différence de pression.

Remplaçons la vanne située entre les compartiments A et B par une valve qui s'ouvre sous la pression des molécules tendant à passer de A vers B avant qu'un ressort ne la referme. Lorsqu'une molécule tend à passer de B vers A, la valve reste fermée. Au bout d'un certain temps, les molécules seront plus

nombreuses dans le compartiment B que dans le compartiment A. La pression en B sera donc plus grande. Une telle différence de pression pourrait alimenter un moteur. On transformerait ainsi de l'énergie thermique prélevée au milieu en travail en faisant l'économie d'une source froide. Ceci est contraire au second principe de la thermodynamique.



En fait, le démon de pression est condamné par les lois même de la thermodynamique qu'il prétendait réfuter. Le système ne peut fonctionner que si la valve se trouve à une température plus basse que le gaz. Une source froide est donc bien nécessaire. Sans cela, la vanne se retrouverait en équilibre thermique avec le gaz, et posséderait donc une énergie cinétique qui la ferait s'ouvrir et se refermer de manière aléatoire. Elle deviendrait donc inefficace.

Le démon de Maxwell semble donc résister à son automation. Apparemment, c'est donc bien l'aptitude au traitement intelligent qui serait à l'origine de son pouvoir.

5.7.3 Szilard : le moteur (1929)

5.7.3.1 Du démon au moteur

Léo Szilard, connu pour son opposition à l'utilisation de la bombe atomique dont il est le principal inventeur, étudia le problème du démon de Maxwell en donnant une définition plus théorisée de l'"être intelligent". Il s'agit d'un être :

- capable d'observer, donc d'effectuer des mesures sur l'état de son environnement,
- de traiter l'information qu'il retire de ses mesures pour décider d'un comportement
- d'agir en conséquence.

On sait qu'il est en théorie possible d'agir sans dépense d'énergie comme c'est le cas pour les opérations demandées au démon : ouverture et fermeture réversibles d'une vanne en l'absence de frottements. Szilard, convaincu de la réalité du second principe, essaya de démontrer que l'une des deux autres opérations nécessitait une dépense énergétique. Pour cela, il conçut une machine, le "moteur de Szilard", employant un démon de Maxwell automatisé au moyen de capteurs de position et d'une mémoire informatique. Il étudia la consommation d'un tel moteur et conclut bien à une dépense d'énergie au cours d'un cycle de fonctionnement. Son étude ne permit pas de discerner l'origine de la dépense d'énergie.

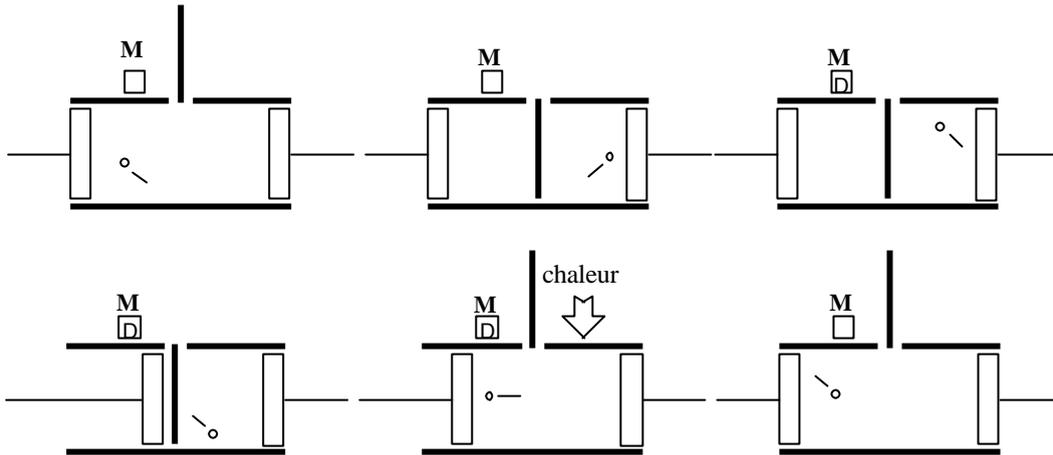
5.7.3.2 Fonctionnement du moteur

Le moteur transforme l'énergie thermique du milieu en travail sans avoir besoin de la source froide ordinairement indispensable à toute machine thermique. Il exploite l'énergie thermique captée de l'environnement extérieur par une seule molécule. Il est constitué :

- d'un cylindre pouvant être divisé en deux au moyen d'une paroi amovible actionnable sans frottements.
 - d'une particule s'agitant dans le cylindre sous l'action de l'énergie fournie par le milieu.
 - de 2 pistons, situés de part et d'autre du cylindre, et chargé de récupérer l'éventuel travail que pourrait fournir la machine.
- d'un système de mesure permettant de savoir laquelle des deux moitiés du cylindre est occupé par la particule lorsque la paroi est baissée.
- d'une mémoire conservant le résultat de la mesure. Elle peut comporter 3 états : gauche, droite, et indéterminé.

Le cycle est le suivant :

1. au départ la paroi est relevée et les pistons tirés au maximum pour laisser le plus grand degré de liberté à la molécule.
2. la paroi est baissée et la molécule bloquée dans l'une des deux moitiés.
3. le système détermine la moitié occupée et initialise la mémoire en conséquence.
4. on pousse sans frottement le piston situé du côté non occupé par la molécule. Aucune consommation d'énergie puisque, outre l'absence de frottements, le piston se heurte à une pression nulle.
5. on retire la paroi, autorisant une exploitation de l'énergie que la particule retire du milieu pour pousser le piston et retirer de l'énergie.
6. on efface la mémoire pour se retrouver dans les conditions initiales



Apparemment, le système retire de l'énergie du milieu sans contrepartie entropique. Pourtant, le nombre d'états accessibles différentiables par le système évolue au cours du cycle :

- Dans les étapes 1, 2, 3, 4 et 6, 2 phases sont possibles selon la moitié occupée par la molécule. Dans ces étapes, soit la mémoire est vide, soit son contenu est corrélé avec la position de la particule.
- Etape 5, 4 phases possibles selon l'état mémoire et la position de la molécule, les 2 valeurs étant décorrélées.

Le volume de l'espace des phases connaît donc une fluctuation d'un facteur 2. Celle-ci doit amener une consommation d'énergie de :

$$kT \ln(2)$$

où T représente la température absolue et k la constante de Boltzmann définie en thermodynamique statistique. Mais où se situe la consommation d'énergie ? Elle ne vient pas du mouvement mécanique des parois ou des pistons. Elle ne peut venir que de la mesure ou de la mémorisation. Léo Szilard avait une préférence pour la seconde explication mais n'a pas su argumenter son idée. Hélas, la théorie naissante de la mesure allait faire croire à tort à une nécessaire consommation liée à la mesure de la position de la particule.

En effet, au sein d'une enceinte close où la température est homogène, règne un rayonnement uniforme dans lequel une particule ne se distingue pas de son milieu. Pour connaître sa position il est donc nécessaire de "éclairer", introduisant dans le système une source d'entropie. Mais cette explication ne semble pas être la bonne origine de la consommation d'énergie. Nous verrons que l'on peut envisager de repérer la position d'une particule sans l'éclairer.

Le moteur de Szilard constitue une évolution nette du problème du démon de Maxwell. En remplaçant l'être intelligent par un automate et en jugeant les deux approches équivalentes, Szilard se rallie implicitement à la thèse de Church-Turing. La réponse au problème posé par Szilard ne sera cherchée que par de purs physiciens pendant longtemps. Il faudra attendre que se développe une science propre

de l'information pour que l'on puisse entrevoir une réponse exacte (qui fait néanmoins encore l'objet de controverses).

5.7.4 Landauer : dépense énergétique et calcul (1960)

5.7.4.1 Consommation des ordinateurs

Les premiers ordinateurs avaient une consommation d'énergie importante. Aujourd'hui encore, les problèmes de refroidissement des circuits électroniques sont cruciaux. Il est donc légitime de se demander si l'acte de calculer nécessite intrinsèquement un besoin de consommation d'énergie.

Dans les années 60, l'opinion générale était que le moteur de Szilard dissipait de l'énergie à cause de l'acte de mesure. Comme toute opération logique sur un bit nécessite une part de mesure, on concluait avec Von Neumann qu'une quantité d'énergie $kT \ln(2)$ était dissipée à chaque opération logique. Ainsi la recopie d'une zone mémoire nécessite la "mesure" de l'état mémoire à recopier. De fait, une telle recopie doit consommer une quantité d'énergie proportionnelle au nombre de bits.

Tournant crucial. Landauer, animé initialement du désir de démontrer rigoureusement l'existence d'une telle consommation théorique constata que la démonstration lui échappait pour toute une série d'opérations parmi lesquelles la recopie mémoire. On n'augmente pas dans ce cas le contenu global en information du système et aucune contrepartie énergétique n'apparaît nécessaire. Par contre une opération faisant baisser le contenu en information génère de la dissipation.

C'est ainsi qu'un effacement d'un bit de mémoire dissipe nécessairement de l'énergie si ce bit était porteur d'information (donnée ou résultat de calcul) et que cette information ne peut plus être retrouvée avec les données restantes. L'effacement d'un bit aléatoire peut ne rien consommer, de même que l'effacement d'un bit redondant, corrélé à un autre. En d'autres termes, l'effacement est dissipatif s'il est irréversible. Landauer montra de manière générale que les opérations réversibles peuvent ne pas consommer d'énergie.

Evidemment, ceci n'est vrai que si l'on sait exploiter le contenu en information des chaînes. Une procédure qui effacerait tout type de chaîne dissiperait autant d'énergie pour une chaîne riche en information que pour une autre. Simplement, dès lors que le contenu d'une chaîne à effacer est corrélé avec le reste de l'information en mémoire, il est possible d'exploiter ces corrélations pour diminuer la dissipation lors de l'effacement.

Le raisonnement de Landauer s'appuie sur le fait qu'un traitement informatique nécessite un phénomène physique support : champ ou courant électrique, champ magnétique.... Toute modification d'un état logique du système se répercute donc sur le système physique support. Ainsi un effacement d'une zone mémoire de n bits amène une réduction des états logiques du système. De 2^n états possibles on passe à 1 seul état. Ceci correspond à une diminution de l'espace des phases, donc à une diminution d'entropie informatique au sens de Shannon. L'entropie globale de l'ensemble calculateur + milieu ne pouvant qu'augmenter, le calculateur dissipe donc nécessairement de l'énergie vers son milieu.

5.7.4.2 Entropie thermodynamique et informatique

Ainsi, toute opération irréversible de calcul s'accompagne nécessairement d'une modification du nombre d'états accessibles du système physique, et donc de son entropie. En vertu de telles considérations, il existe une limite d'énergie en deçà de laquelle tout traitement d'un bit d'information est impossible. Cette limite vaut encore :

$$k T \ln(2)$$

A température ambiante, cela représente $2,87 \times 10^{-21}$ joules.

La relativité restreinte d'Einstein nous apprend par ailleurs que toute fluctuation d'énergie s'accompagne d'une fluctuation de masse selon l'équation

$$E = mc^2$$

On peut donc dire qu'un bit d'information a une masse de :

$$k T \ln(2)/c^2$$

soit $3,19 \cdot 10^{-38}$ kilogrammes à température ambiante, soit un centième d'électron volt. Mieux vaut donc acheter ses disquettes informatiques non formatées car elles sont plus légères dans la poche (encore qu'il faille prendre en compte l'état thermodynamique de la carte bleue à puce).

5.7.4.3 Bilan

A ce stade de l'histoire, il apparaît que les opérations réversibles autorisent toute une procédure permettant leur exécution sans dépense d'énergie. Il peut être jugé surprenant de voir que la recopie d'une zone mémoire, du fait qu'elle génère des corrélations et non des réductions d'états, peut s'effectuer gratuitement. A noter que l'inverse temporel d'une telle recopie apparaît comme un effacement d'une copie excédentaire. Tout effacement d'information n'est donc pas dissipatif. Seules les informations qui sont perdues de l'information le sont.

Malgré tout, l'irréversibilité semble une nécessité pour le calcul réel. Toute porte logique amène une réduction d'état génératrice d'entropie puisque de l'information est perdue : 2 bits n'en redonnent qu'un. La non dissipation semble à ce stade bien théorique.

5.7.5 Bennett : réversibilité logique du calcul (1973)

5.7.5.1 Histoire

Les travaux de Landauer semblaient inefficaces dans la mesure où les calculs réels font appel à des opérations logiques nécessairement irréversibles. Par amusement, Landauer réussit cependant à écrire un algorithme réversible permettant de tester la divisibilité d'un nombre par un autre. Cet algorithme était constitué de 2 parties : la première effectuait les calculs mais générait des résultats parasites (quotient et reste), la seconde réussissait à effacer les résultats parasites de manière réversible sans écrasement d'état. Landauer approfondira alors l'idée que tout calcul peut être rendu réversible à condition de générer un déchet parasite[5][7].

5.7.5.2 Machines de Turing réversibles

Un calcul peut toujours être rendu réversible à condition qu'il y ait moyen, à chaque étape, de récupérer les données suffisantes permettant d'effectuer l'étape dans le sens inverse. Par exemple ne pas effacer les valeurs intermédiaires d'une variable mais les stocker dans une pile, conserver à chaque branchement dans un programme l'adresse d'où l'on est parti... Il est ainsi possible de transformer tout calcul irréversible en calcul réversible mais générant un déchet constitué de données excédentaires indésirables.

Les algorithmes ordinaires ont pour objectif de supprimer dans un jeu de données les informations latentes qui ne nous intéressent pas pour ne garder à la fin que l'information que l'on recherche. Un calculateur réversible fonctionnera sur un principe différent, il effectuera un tri dans les informations présentes dans le jeu de données. Le résultat sera l'information cherchée, le déchet contiendra en puissance l'ensemble des autres informations accessibles à partir de ce même jeu.

5.7.5.3 Calcul réversible

Soit à vouloir calculer S à partir de E. Si ce calcul est effectué sur une machine réversible, il générera un déchet d. On sait que l'effacement irréversible d'un tel déchet d doit générer de l'entropie. Comment exploiter le contenu en information de ce déchet pour rendre l'effacement réversible ?

Pour cela effectuons un calcul en plusieurs étapes.

- 1 - calcul direct :E → S , d
- 2 - recopie du résultat :S , d → S , S , d
- 3 - calcul inverse à partir d'un résultat et du déchet :S , S , d → S , E

au total on aura $E \rightarrow S$; E. Le seul déchet final sera une copie des données. Tout calcul peut être donc rendu réversible si les données se retrouvent dans le résultat. Dans le cas où la correspondance entre les entrées possibles et les sorties possibles est biunivoque (bijection), tout déchet peut être éliminé, comme nous allons le voir.

Considérons les 2 machines M1 et i qui permettent le calcul mutuel de E et de S

$$\begin{aligned} E &\xrightarrow{d} S \\ S &\xrightarrow{i} E \end{aligned}$$

Créons des versions réversibles de ces machines

$$\begin{aligned} E &\xrightarrow{dr} S, d & S, d &\xrightarrow{dr} E \\ S &\xrightarrow{ir} E, d' & E, d' &\xrightarrow{ir} S \end{aligned}$$

Maintenant, suivons une procédure en 7 étapes.

1	calcul de S :.....	E	\xrightarrow{dr}	S, d
2	recopie du résultat :.....	S, d	\rightarrow	S, S, d
3	régénération de la donnée :.....	S, S, d	\xrightarrow{dr}	S, E
4	échange donnée - résultat :.....	S, E	\rightarrow	E, S
5	calcul inverse de E :.....	E, S	\xrightarrow{ir}	E, E, d'
6	effacement réversible d'une copie excédentaire :.....	E, E, d'	\rightarrow	E, d'
7	calcul de S :.....	E, d'	\xrightarrow{ir}	S

Au total, $E \rightarrow S$ sans déchets. On généralise donc le résultat trouvé pour la recopie, en fait toute relation biunivoque peut être réalisée sans dissipation.

5.7.5.4 Déchet et thermalisation

En conclusion, toute relation biunivoque peut être réalisée sans consommation d'énergie. Pour les autres, une consommation peut être consécutive à l'effacement d'un déchet. Ce dernier peut généralement se limiter à une réplique des données.

A noter que les données d'une machine de Turing ne se limitent pas aux variables nécessaires à la suite du calcul. La machine possède en elle même une réserve infinie de constantes constituées par les cases vides de la bande de travail. On pourrait imaginer que le travail de la machine consiste à transformer une suite de 0 parfaitement ordonnés, donc à basse entropie, en un déchet de complexité plus élevée, donc d'entropie plus grande. L'aptitude au calcul aurait pour contrepartie une telle "thermalisation" de l'information, qui se concrétisera au moment de l'effacement par une thermalisation réelle. Quant à la source de constantes, nécessaire en plus des données, elle peut être assimilée à un "carburant". Caractérisée par une complexité de Kolmogorov faible, elle joue le rôle du carburant de machine thermique, c'est à dire une source de faible entropie. Elle se transformera en déchet aléatoire de complexité élevée.

5.7.6 Fredkin, Toffoli : calcul et modèles balistiques (1981)

5.7.6.1 Objectif d'un modèle physique

Les travaux de Fredkin se sont déroulés dans un premier temps en parallèle à ceux de Bennett et ont abouti aux mêmes conclusions, mais en donnant un aspect plus intuitif aux réflexions par l'utilisation d'un modèle inspiré de la physique[45]. Ce modèle a pour objectif apparent de montrer le caractère effectif du calcul réversible. Mais Fredkin avait cependant une intention secrète exactement inverse : montrer que les lois de la physique sont conformes aux lois du calcul. Quelles que soient les lois par lesquelles le monde réel relie les causes aux effets, ces lois doivent se soumettre aux principales contraintes du calcul. Certaines sont déjà pressenties chez Turing :

- propagation de l'information à vitesse finie
- un système physique fini ne peut contenir qu'une quantité d'information finie.
- les fonctions logiques primitives universelles sont réalisables par des dispositifs physiques réels.

5.7.6.2 Logique dissipative

Lorsque les caractéristiques d'un système sont entièrement spécifiées, son évolution est parfaitement réversible et déterministe. Sur le plan microscopique il en est ainsi de tout système physique, qu'il soit

classique ou quantique. Nous discuterons ultérieurement du caractère irréversible de la transition d'un système quantique à un système classique au moyen d'une opération de mesure. Mais les deux mondes classiques et quantiques sont tous les deux déterministes chacun dans son domaine.

A noter que le sens donné ici au mot réversibilité n'implique pas nécessairement que l'on parie sur une invariance des lois par renversement de temps. Réversible signifie que le déroulement inverse est déterministe, même avec des lois légèrement différentes. Précaution utile car la physique contemporaine semble mettre en évidence une dissymétrie fondamentale de l'axe des temps dont nous parlerons en abordant la flèche microscopique.

Lorsque la spécification d'un système est incomplète, l'étude de son évolution fait intervenir des lois régies par la statistique. On peut ainsi étudier le caractère hautement probable de l'évolution du système, mais pas son évolution certaine. Cette nature de quasi-loi confère à la statistique un caractère d'irréversibilité. Les systèmes macroscopiques, impossibles à spécifier dans le détail, sont principalement concernés par cette notion de l'irréversibilité.

Ainsi les lois du calcul s'appuient-elles sur des fonctions logiques irréversibles comme la porte logique ET, qui après exécution efface les traces de son passé. Ceci a des répercussions sur l'état du milieu. Il est dit qu'une telle perte d'information équivaut à un transfert d'énergie de l'ordre de $kT \ln(2)$ vers le milieu dès lors que l'on persiste à ne pas vouloir connaître plus en détail son état.

En pratique, l'ordre de grandeur de la consommation réelle est de l'ordre de 10^8 fois plus élevé au mieux. L'idéal d'un transfert thermique à sens unique de l'outil de calcul vers l'environnement n'est jamais réalisé. La pénétration de l'énergie thermique dans le système rendrait le résultat du calcul très aléatoire si le système n'encodait pas le signal de manière très redondante afin de filtrer la partie non déterministe du comportement du système. Mais cela nécessite une régénération permanente de la partie du signal perdu. La consommation ne doit donc que très peu à l'irréversibilité. Dans les machines actuelles le calcul réversible est simulé par des opérateurs irréversibles.

Quant à la consommation théorique, il s'agit de voir si elle n'est pas remise en cause par une reconsidération des études précédentes au regard des lois microscopiques et non plus de l'état macroscopique du système. En outre, on peut se demander s'il n'existe pas d'espoir de voir un modèle physique réel répondre aux critères du calcul non dissipatif.

5.7.6.3 Critères pour une logique conservative

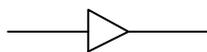
Outre les 3 contraintes déjà présentés que doit satisfaire le modèle pour répondre à son objectif, les principales contraintes auxquelles il doit obéir concernent la mémorisation, la transmission et le traitement de signaux discrets :

- Pas de distinction entre mémorisation et transmission d'information.
- Primitives réversibles.
- Duplication de résultat intermédiaire réalisable à partir des seules primitives de base.
- Le système de calcul doit mettre en évidence au moins une grandeur conservative. De telles grandeurs sont nécessaires dans les systèmes réversibles. Ainsi l'étude thermodynamique d'un gaz est déterministe dès lors que l'on prend en compte l'état individuel de toutes les particules dont le nombre est constant.
- La géométrie de l'espace est localement euclidienne (l'exemple typique de géométrie non euclidienne est celle de certains jeux de type "Pacman" dans lequel un objet qui sort de l'écran par un bord, rentre par le bord opposé).

Une logique répondant à ces critères a pu être construite à partir de 2 primitives : le fil unitaire et la porte logique de Fredkin.

5.7.6.4 Fil unitaire

Il s'agit d'un fil transmettant un signal d'une de ses extrémités à l'autre en un temps exactement unité.

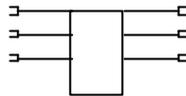


L'état du fil au temps t est celui de son entrée. Il est égal à l'état de la sortie au temps $t+1$. Lorsque les deux extrémités sont confondues, on mémorise un état en permanence.

Le dispositif est conservatif pour le nombre de 0 et 1 fournis au départ.

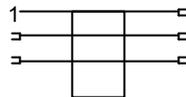
5.7.6.5 Porte logique

La seule et unique porte logique est la porte de Fredkin. Elle a autant d'entrées que de sorties, soit 3 de chaque. Certaines sorties fourniront le résultat du traitement souhaité, d'autres représenteront le déchet généré pour rendre le calcul réversible. La porte est conservatrice. On retrouve en sortie autant de 1 et de 0 qu'il y en avait en entrée. Voici sa représentation :

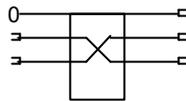


notons que la représentation est parfaitement symétrique Et voici comment la porte fonctionne :

- Si la première entrée est à l'état 1, les 2 autres sont directement recopiées sur les 2 sorties correspondantes.



- Si la première entrée est à 0, il y a également recopie des 2 autres entrées, mais cette fois après inversion.



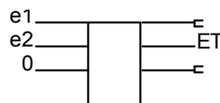
Le temps de traversée d'une porte est supposé nul, il revient aux fils unitaires de mémoriser les délais.

Dans un circuit, le nombre de degrés de liberté correspond au nombre N de fils unitaires car chaque fil est dans un état indépendant de celui des autres. Le nombre N_1 de fils unitaire à l'état 1 représente une grandeur additive. Sa valeur pour le système complet correspond à la somme des valeurs pour chaque portion. N_1 se conserve en cours de calcul (considérations identiques pour N_0 , le nombre de fils à l'état 0).

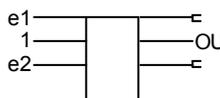
5.7.6.6 Modélisation des fonctions logiques usuelles

Toutes les fonctions logiques peuvent être modélisées à l'aide des deux dispositifs décrits. Comme certaines des fonctions modélisables ne sont pas réversibles, on en conclut que l'on modélise en fait des fonctions plus puissantes dans lesquelles sont plongées les fonctions à modéliser. En conséquence, le dispositif générera, en plus du résultat cherché, les bits de déchet.

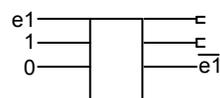
Voici la fonction ET :



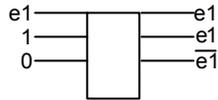
la fonction OU :



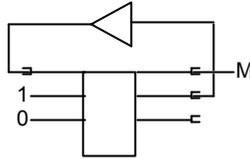
l'inverseur logique :



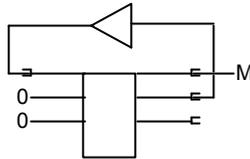
et le duplicateur :



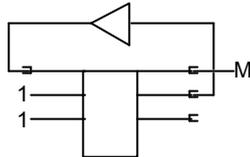
Un exemple de circuit composite : la bascule. Ici, elle conserve indéfiniment son état. Le fil unitaire mémorise l'état précédent. La porte permet de régénérer en permanence cet état sur la sortie M.



Ici, la bascule est forcée à 0, qui sera l'état du fil à l'étape suivante.



Ici, la bascule est forcée à 1.



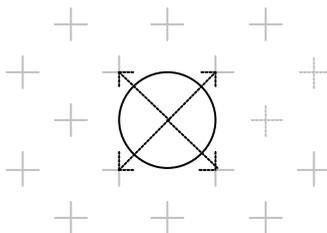
5.7.6.7. Concrétisation physique

A ce stade nous savons qu'il est possible de concevoir des systèmes réversibles capables de calculs universels. Toute logique peut en effet être modélisée par la logique conservative à condition d'avoir des 0 et 1 disponibles à volonté en constantes et de consentir à récupérer un déchet. Les modèles de machine de Turing réversibles répondent à ces contraintes par la disponibilité d'une bande de longueur infinie, qui sert à la fois comme source de constantes 0 et comme réservoir de déchets finaux.

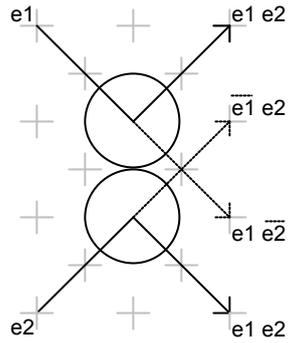
mais les machines de Turing autant que les portes de Fredkin sont des êtres pour l'instant purement mathématiques. Nous allons essayer de leur faire franchir un cap supplémentaire en essayant de voir si les lois de la physique sont compatibles avec leur existence. Dans la logique de Fredkin, le modèle des boules de billard va nous permettre d'avancer.

5.7.6.8. Porte réversible

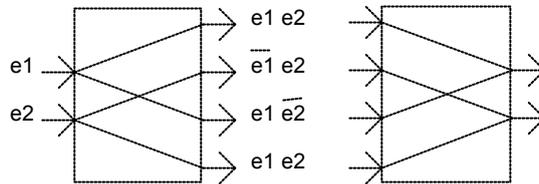
Le jeu se joue sur une grille de pas unité avec des billes de rayon $1/\sqrt{2}$. Au temps initial, toutes les billes sont sur un point de grille. Chaque bille peut parcourir en une unité de temps une distance équivalente au pas de grille dans une direction parmi 4 possibles.



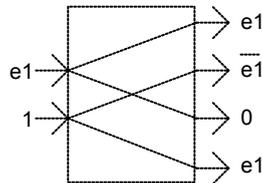
L'opération logique fondamentale est l'"interaction", résultant du choc de 2 billes.



Elle est réversible car l'inversion du sens de parcours des billes permet de retrouver de façon déterministe l'état initial à partir de l'état final. La porte logique et son inverse seront représentés symboliquement comme suit :



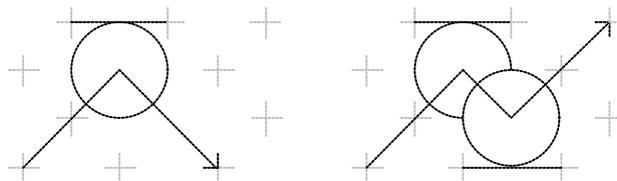
On obtient donc directement la fonction ET. La fonction NON et la duplication se déduisent directement :

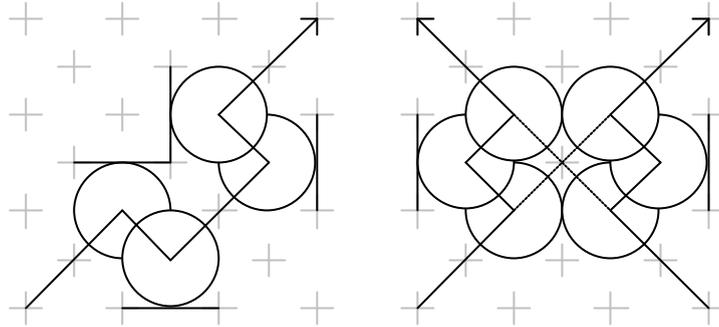


En combinant le tout, on peut obtenir un NAND, la porte est donc bien universelle en plus d'être réversible.

5.7.6.9 Fonctions annexes

Pour que notre porte logique puisse être réellement employée au sein d'un système logique complet, il nous faut nous prémunir des problèmes d'acheminement du signal de porte en porte. Pour cela nous nous aiderons de miroirs plans destinés à assurer les fonctions d'acheminement et les fonctions dérivées : déviation, décalage latéral, délai et croisement (nous restons dans un espace plan euclidien).





Ce qu'il est important de noter, c'est que de tels dispositifs peuvent modéliser une porte de Fredkin. Ainsi l'interaction, qui n'est pas conservative (2 entrées et 4 sorties), peut simuler la logique conservative. Nous pourrions donc continuer à raisonner en logique conservative en ayant à l'idée qu'un modèle physique réel est envisageable pour la concrétiser.

5.7.6.10 Bilan énergétique

Nous avons vu que la logique réversible était possible moyennant une source de constantes disponibles à tout moment et la récupération de déchets pouvant apparaître également à tout moment. Il est opportun de se poser la question de savoir si l'un et l'autre ne peuvent pas atteindre des tailles arbitrairement élevées. L'effacement des déchets correspondant à un rejet thermique, ne risque-t-on pas de perdre tout le bénéfice énergétique obtenu ?

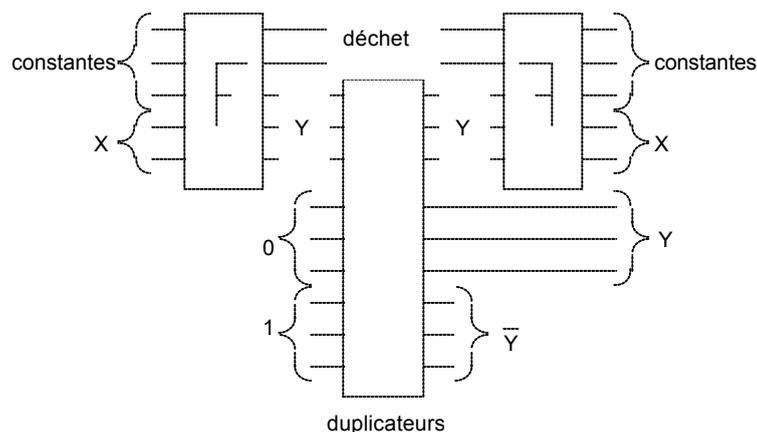
Le nombre de portes croît généralement de manière exponentielle par rapport au nombre d'entrées. Ceci est dû au fait que la plupart des fonctions logiques complexes sont "aléatoires" dans ce sens qu'elles ne sont pas plus performantes que l'examen d'une table exhaustive de correspondances entre les entrées possibles et les sorties possibles. De fait, le déchet est censé augmenter en taille de manière également exponentielle, puisque chaque porte génère un déchet. Il est donc légitime de croire qu'une autre approche permettrait de rendre la croissance moins abrupte, par exemple linéaire. Nous allons voir qu'en fait le déchet peut non seulement avoir la même taille que les données mais peut en être une copie exacte.

5.7.6.11 Réseaux combinatoires

Il est envisageable d'effacer le déchet par un procédé analogue à celui utilisé par Bennett à savoir un traitement en 3 étapes :

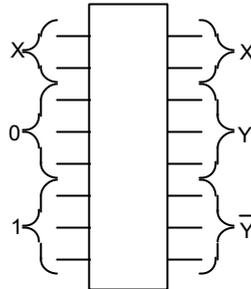
- calcul avec déchet
- duplication du résultat
- régénération des données à partir d'un résultat et du déchet.

Le réseau de calcul à billes étant réversible comme l'est la porte de Fredkin, le schéma global est le suivant :



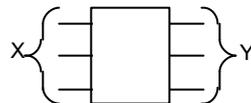
On voit qu'un dispositif "espion" se charge de réarranger un série de 0 et de 1 pour qu'ils soient l'image du résultat et de son complémentaire.

Une étude plus poussée permettrait de montrer que, moyennant une fonction d'espionnage moins localisée, il est toujours possible de diminuer la taille des constantes autres que celles nécessaires à l'espionnage lui même. Le système global serait à la limite équivalent à :



Mais cette limite ne peut être obtenue qu'au prix de l'élaboration d'une fonction logique spécifique, devant gérer ses propres déchets, et généralement non décomposable en portes élémentaires. L'idée est de réutiliser le déchet généré à un endroit comme constante pour un autre.

Le nombre de constantes peut encore se réduire. A la limite, si la fonction est bijective (réciproque déterministe) et conservative (autant de 1 dans la donnée que dans le résultat, idem pour les 0), on se passe totalement de constantes et de déchets.



La dissipation n'a donc rien à voir avec le nombre de portes.

5.7.6.12 Conclusion

Après Fredkin, le calcul non dissipatif sort du modèle purement mathématique en exhibant des réalisations physiques. L'intérêt pratique de telles réalisations semble toutefois limité à l'aide à la réflexion, ce qui est déjà beaucoup. Mais l'idéalisation physique est poussée à son extrême. Les billes doivent avoir un diamètre parfaitement défini, les chocs doivent être parfaitement élastiques, et les miroirs parfaitement orientés. Le système doit être totalement isolé de toute perturbation extérieure. Les seules fluctuations gravitationnelles engendrées par les mouvements des atmosphères de planètes proches suffiraient à fausser le calcul au bout d'une centaine de collisions. Le système évoluerait vers un gaz de billes au comportement aléatoire. On peut améliorer les choses avec des boules carrées (!) mais les modes de résonance de telles boules seraient difficiles à maîtriser.

Outre l'utilisation de chocs élastiques, les portes de Fredkin peuvent être construites à partir d'un inverseur mécanique actionné par le passage d'une bille dans l'entrée de commande. Mais cette bille devrait alors subir des frottements qui compromettraient la réversibilité. Ces frottements peuvent être rendus arbitrairement faibles en ralentissant la vitesse de la bille. La réversibilité absolue ne serait obtenue qu'avec une vitesse nulle des billes et un temps de calcul infini.

A partir de là, l'ensemble des modèles qui seront étudiés se classeront principalement en 3 catégories :

- les modèles "browniens" qui, à l'image de l'inverseur mécanique décrit à l'instant, résistent à l'agitation thermique, voire exploitent cette agitation, mais ne peuvent être parfaitement réversibles que pour un temps de calcul infini,
- les modèles balistiques, comme celui des billes, pouvant calculer en temps fini mais qui sont des idéalizations et ne peuvent en pratique fonctionner car la moindre agitation thermique fausse le résultat,
- la classe des modèles quantiques, qui essaient de concilier temps fini et résistance à l'environnement en s'appuyant sur des phénomènes mis en évidence dans le comportement de particules élémentaires.

Après avoir étudié un modèle ballistique, nous allons regarder un représentant de chacune des 2 autres catégories.

5.7.7 Bennett : modèle brownien (1982)

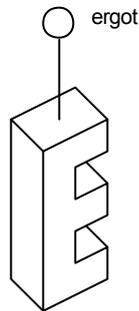
5.7.7.1 Intérêt

Les modèles browniens sont venus après les modèles balistiques[7]. Ils cherchaient à répondre à certaines critiques de ces derniers. Premier modèle brownien, le modèle de Bennett permet d'éclairer la distinction existant entre réversibilité physique et réversibilité logique. Sa machine en effet n'exige pas de génération de déchets, elle n'exige pas une précision infinie dans le dimensionnement des pièces, elle résiste à l'agitation thermique et elle exploite même cette agitation pour fonctionner. En contrepartie, son temps de calcul peut être arbitrairement long.

5.7.7.2 Constitution de machine de Turing, généralités

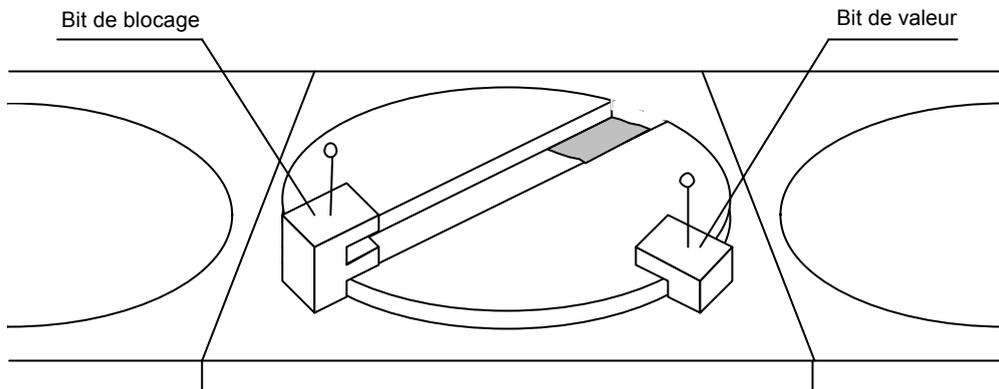
Toutes les pièces sont emboîtées sans frottements. Aucune pression n'est exercée par un ressort. L'agitation thermique est la vraie force motrice de cette machine. Elle peut faire évoluer le système dans un sens comme dans l'autre. Aucun rôle n'est joué par le poids des pièces.

5.7.7.3 Le bit



Le bit est matérialisé par une pièce métallique en forme de E. Les 2 encoches de la pièce autorisent 2 positionnements au sein du mécanisme, une position haute et une position basse représentant les 2 valeurs possibles du bit. La pièce est surmontée d'un ergot permettant à la valeur qu'il représente d'être lue. L'ergot fournit également une prise au bras manipulateur qui sera chargé de modifier cette valeur.

5.7.7.4 La bande

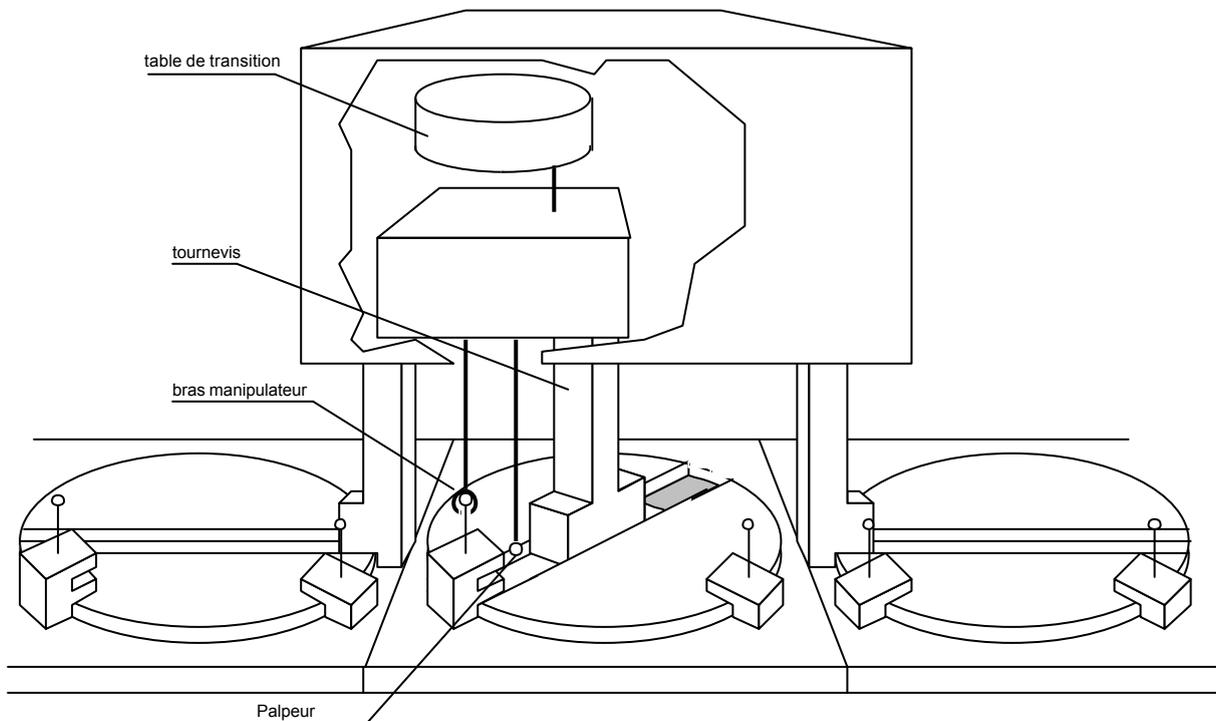


La bande est constituée par une succession de disques sur lesquels viennent s'enclencher les bits. Chaque disque comporte une fente. La valeur d'un bit ne peut être modifiée que lorsque cette fente est correctement orientée face au bit à modifier.

En fait chaque case comporte au moins 2 bits.

- le ou les bits de valeur représentant le symbole présent sur la case de la bande,
- un bit de blocage, qui par un mécanisme particulier va permettre de bloquer l'un des disques adjacents et de débloquer l'autre, avant translation de la tête de lecture-écriture.

5.7.7.5 La tête de lecture-écriture



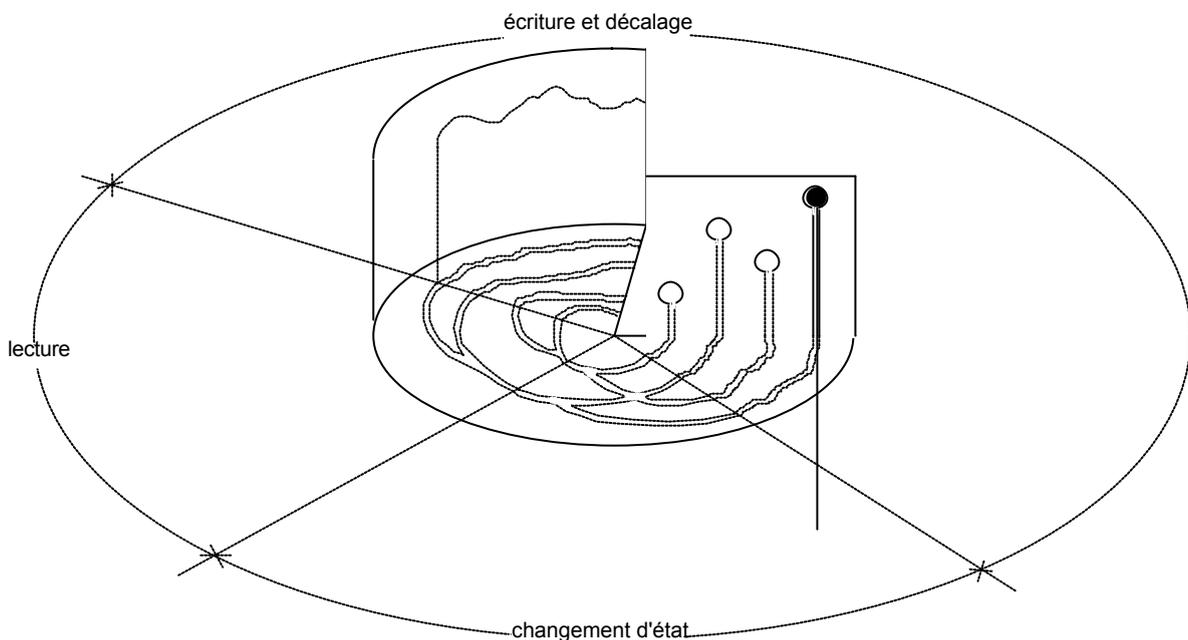
La tête elle-même est constituée :

- d'un berceau qui soutient la tête, et bloque les 2 disques adjacents,
- d'un tournevis qui oriente le disque en cours de traitement,
- d'un palpeur dont les trajectoires possibles sont contraintes par la présence des ergots des bits,
- d'un bras manipulateur qui pourra modifier les bits et faire translater la tête en faisant prise sur un ergot de bit,
- de la tête elle-même contenant l'ensemble des mécanismes ainsi que la table de transitions.

A tout moment :

- le bit de blocage d'un disque situé à gauche de la tête bloque le disque situé à sa gauche,
- le bit de blocage d'un disque situé à droite de la tête bloque le disque situé à sa droite,
- les disques immédiatement adjacents à la tête sont bloqués par la tête elle-même,
- le disque sur lequel se trouve la tête est débloqué.

5.7.7.6 La table de transitions



La table de transitions est matérialisée par une came rotative très élaborée, dans laquelle se déplace la tête d'une tige sonde. Chaque sillon a une forme complexe aussi bien latéralement qu'en profondeur. La table comporte 3 secteurs :

- Le secteur de lecture. En début de ce secteur, on trouve autant de sillons que d'états possibles pour le système. Pour chacun de ces sillons on trouve ensuite un embranchement correspondant aux diverses valeurs possibles du caractère à lire sur la case où se trouve la tête.
- Le secteur écriture et décalage dans lequel se trouvent encodées les instructions de manipulation du tournevis et du bras manipulateur.
- Le secteur de changement d'état, dans lequel s'entrecroisent les sillons afin de transiter d'un état à l'autre.

5.7.7.7 Fonctionnement

La machine effectue les opérations classiques fondamentales des machines de Turing :

- lecture
- écriture
- décalage
- changement d'état.

Pour plus de clarté, nous allons examiner les opérations se succédant dans le sens direct, celui aboutissant au résultat cherché. Mais tout est réalisable dans le sens inverse.

5.7.7.8 Lecture

La tête se trouvant au dessus d'une case, le palpeur effectue un mouvement qui répond aux contraintes de la tige sonde dans la came. Lorsque cette dernière se trouve à un embranchement, le palpeur peut emprunter plusieurs voies possibles. Elles sont toutes explorées à tour de rôle au hasard. Mais pour chaque embranchement, l'une des voies mènera le palpeur dans une trajectoire bloquée par la présence d'un ergot de bit, et l'autre sera libre. C'est ainsi que la valeur du bit sera lue.

5.7.7.9 Ecriture

La tête sonde étant engagée dans une branche de sillon fonction de la valeur de bit lue par le palpeur, elle trouvera dans la trajectoire de ce sillon les informations aiguillant l'évolution des mécanismes complexes commandant le bras manipulateur et le tournevis. Ceci afin de changer la valeur des bits.

5.7.7.10 Décalage

La suite de l'exploration du sillon fera rentrer le mécanisme dans la phase de décalage de la tête. Selon la nature du décalage, les mécanismes de la tête positionneront le bit de blocage afin de débloquent l'un des disques adjacents. Seul le berceau, encore engagé dans la fente, empêchera un mouvement intempestif du disque suivant avant que la tête ne s'y positionne. Le transfert vers la case suivante se fait sous l'action du bras manipulateur qui agrippe pour ce faire l'un des ergots de bit et s'en sert comme prise pour évoluer.

5.7.7.11 Changement d'état

Dans la dernière partie de sa rotation, la table d'état aiguillera la tige sonde sur un sillon correspondant à l'état suivant à donner à la tête.

5.7.7.12 Réversibilité physique et logique

Tous les mouvements étant réversibles, la machine effectue une marche aléatoire dans un sens et dans l'autre. Elle explore toutes les voies et si l'une est sans issue, bloquée par un ergot de bit, la machine rebrousse chemin. On voit donc que la réversibilité ici est physique. C'est à dire que la machine peut fonctionner indifféremment à l'endroit ou à l'envers. Si l'on présente un film montrant le fonctionnement de la machine, nul ne saurait dire si le film se déroule dans le sens correct.

Il est à noter que la machine ne nécessite nullement une programmation en logique réversible, même si celle-ci est hautement recommandée. En effet, lorsqu'une opération logique n'a pas d'inverse déterministe, la machine explore simplement à tour de rôle toutes les hypothèses sur l'état antérieur des variables. Ainsi lors de l'effacement irréversible d'un bit on supposera à tour de rôle que la valeur antérieure était 1 puis 0. Lors de l'effacement d'une variable le nombre de branches inverse à explorer est très grand. Ce nombre croît de manière exponentielle avec le nombre de variables.

Avec ce principe, on peut retrouver tous les jeux de données possibles qui fournissent le même résultat que le jeu de données fourni. Par contre, un seul résultat pourra être atteint. Compte tenu du nombre quasi infini de branches à explorer lorsque l'on évolue dans le sens inverse de la normale, la programmation en logique réversible permet d'atteindre plus sûrement le résultat dans un délai néanmoins non garanti.

Pour être sûr que la machine évolue vers le résultat on peut rajouter une légère force motrice contraignant le sens du parcours de la table d'état. Mais dès lors la réversibilité n'est plus qu'approchée. Et qui dit force dit travail, donc dissipation. Ce qui est important est que cette force peut être arbitrairement faible et la dissipation n'est pas astreinte à dépasser un quelconque minimum théorique.

5.7.8 Modèles quantiques

5.7.8.1 Recette

La mécanique classique n'est qu'une approximation. Dans son comportement rigoureux, le monde physique semble plutôt répondre au formalisme de la mécanique quantique. En utilisant les équations mises en évidence dans l'étude de la matière fondamentale, on espère pouvoir concilier temps de calcul

fini et résistance aux perturbations. Tout le problème consiste à construire un espace de configurations, un état initial et un opérateur d'évolution donnant à l'ensemble des propriétés aptes à faire évoluer l'ensemble dans la voie du calcul par la simple application du formalisme quantique. Ces modèles ont l'aspect d'un tas d'équations, censées modéliser un système physique, mais on ne sait pas nécessairement lequel.

Certains ont tout de même essayé de se préoccuper de la nature des phénomènes physiques réels à employer. Feynmann par exemple utilise une population de spin de particules. Mais son modèle n'est pas programmable au sens classique du terme. Il faut un système par type de calcul désiré. Le système créé est un système idéalisé pour un calcul donné. Ont été également étudiés des dispositifs comme les jonctions Josephson qui exploitent les propriétés de la supraconduction, l'une des rares manifestations macroscopiques du caractère quantique de la matière.

D'autres motivations existent pour la recherche des modèles quantiques. Les propriétés des machines de Turing s'appuient sur une conception classique de l'Univers. Elles exploitent l'idée que tout peut être décrit par des nombres tous connaissables. Ceci est faux dans la pratique et l'on est donc en droit de s'attendre à ce que la prise en compte des propriétés du monde quantique fasse évoluer la théorie des modèles informatiques. Notamment, la modélisation du hasard pur pourrait être possible, alors qu'elle est simulée avec les limites que l'on sait dans les modèles classiques.

5.7.8.2 Machine quantique

L'exemple de modèle quantique présenté ici est celui de David Deutsch[16]. On retrouve dans un tel modèle les 2 composantes classiques d'une machine de Turing : un processeur fini et une mémoire de taille arbitrairement élevée. Le pas de calcul est de durée constante Δt , et met en jeu une quantité finie de mémoire à chaque fois. Le vecteur d'état à l'instant t est de la forme :

$$|\Psi(t)\rangle = |x; n; m\rangle$$

dans lequel

- x est une variable discrète donnant la position de la tête de lecture,
- $n = \{n_i, i \in 0, 1 \dots M-1\}$ représente M variables d'état modélisant le processeur,
- $m = \{m_j, j \in Z\}$ représente une infinité de variables modélisant la mémoire et valant 0 ou 1.

L'évolution du système pendant la durée élémentaire T est décrit par un opérateur U constant. On a :

$$\forall k \in Z, |\Psi(k \Delta t)\rangle = U^k |\Psi(0)\rangle$$

l'état initial est décrit par le programme localisé dans un nombre fini de bits de mémoire, les autres paramètres étant nuls :

$$|\Psi(0)\rangle = \sum_i \lambda_i |0; 0; m\rangle$$

$$\sum_i |\lambda_i|^2 = 1 \text{ (normalisation)}$$

où seul un nombre fini de λ_i sont non nuls. La description de la fonction U contient tout le secret de la machine. On a :

$$\langle x'; n'; m' | U | x; n; m \rangle = (\delta_{x',x+1} U^+(n',m'_x|n,m_x) + \delta_{x',x-1} U^-(n',m'_x|n,m_x)) \prod_{y \neq x} \delta_{m_y, m'_y}$$

qui fait intervenir 2 applications U^+ et U^- , associées aux 2 déplacements possibles de la tête. Le terme produit Π permet de ne sélectionner qu'un bit dans la mémoire de travail, celui correspondant à la position de la tête.

Durant le calcul, aucune réduction ne doit être induite par une opération de mesure, l'observation du résultat devant n'intervenir qu'à la fin des opérations. Il est donc nécessaire de réserver dans la mémoire un bit n_0 , pouvant être mesuré sans perturber la valeur du reste du contenu mémoire, et qui sera positionné à 1 à la fin du calcul.

L'évolution du calcul est déterministe et réversible. Le choix des applications U et U est arbitraire. Chaque choix constitue un modèle machine différent.

5.7.8.3 Simulation de machines classiques

Les machines de Turing réversibles classiques peuvent être modélisées par des applications :

$$U^+(n', m'_x | n, m_x) = 1/2 \delta_{h', A(n, m_x)} \delta_{m', B(n, m_x)} (1 + C(n, m_x))$$

$$U^-(n', m'_x | n, m_x) = 1/2 \delta_{h', A(n, m_x)} \delta_{m', B(n, m_x)} (1 - C(n, m_x))$$

les fonctions A, B et C ayant des domaines respectifs de Z^{2M} , Z^2 et $\{-1, 1\}$. En d'autres termes, après chaque étape, on se retrouve nécessairement dans un état de base, et non dans un état superposé. Le caractère déterministe est assuré par le caractère biunivoque quel que soit x de la relation :

$$(n, m_x) \leftrightarrow A(n, m_x), B(n, m_x), C(n, m_x)$$

pour toutes les valeurs de m_x .

5.7.8.4 Simulation de machine universelle

Les fonctions A, B et C pouvant prendre toute forme, toute machine peut être simulée. Il est et notamment possible de simuler une machine de Turing universelle, elle-même capable de simuler toutes les autres machines de Turing. La machine calcule f(i) à partir du programme p(f) de la fonction f et de la donnée i. Le reste de la mémoire se retrouve à 0 sauf le bit de fin d'exécution. Pour une exécution en n pas de calcul sur la machine universelle simulée on a :

$$U^n | 0 ; 0 \dots 0 ; p(f), i, 0 \dots 0 \rangle = | 0 ; 1, 0 \dots 0 ; p(f), i, f(i), 0 \dots 0 \rangle.$$

La recherche des fonctions A, B et C permettant d'aboutir à ce résultat ne sera pas entreprise ici. Afin de cerner les propriétés d'une machine de ce type, on s'impose de pouvoir distinguer les variables mises en jeu en peut considérer que la mémoire est divisée en une infinité dénombrable de collections de bits. Par exemple, la collection i sera constituée des bits de rang égaux aux puissances du i^o nombre premier. Ceci ne fait pas perdre à la machine son caractère universel.

Pour toute fonction récursive f et toute paire d'entier a et b, il existe un programme p(f, a, b) appliquant f au contenu de a et le stockant dans b. Afin de conserver la réversibilité, le contenu de b n'est pas écrasé, la nouvelle valeur est combinée à l'ancienne au moyen de ou exclusifs :

$$\begin{array}{cccccc} \text{collection 1} & \text{collect. a} & \text{collect. b} & \text{collection 1} & \text{collect. a} & \text{collect. b} \\ | p(f, a, b) & , \dots , i & , \dots , j & \rangle \rightarrow | p(f, a, b) & , \dots , i & , \dots , j \oplus f(i) & \rangle \end{array}$$

Propriété : si une fonction récursive g est bijective, il existe un programme $\phi(g, a)$ qui remplace tout entier i de la collection a par g(i), et laisse inchangé le reste de la mémoire. En d'autres termes :

$$\begin{array}{cccccc} \text{collection 1} & \text{collection a} & & \text{collection 1} & \text{collection a} & \\ | \phi(g, a) & , \dots , i & , \dots & | \phi(g, a) & , \dots , g(i) & , \dots & \rangle \end{array}$$

Ceci se montre en construisant la fonction par 4 applications successives de la fonction p comme montré ci-dessous.

$$\begin{array}{cccccc} \text{collection 1} & \text{coll. a} & \text{coll. b} & \text{collection 1} & \text{coll. a} & \text{coll. b} \\ | p(g, a, b) & , \dots , i & , \dots , 0 & \rangle \rightarrow | p(g, a, b) & , \dots , i & , \dots , g(i) & \rangle \\ | p(g^{-1}, b, a) & , \dots , i & , \dots , g(i) & \rangle \rightarrow | p(g^{-1}, b, a) & , \dots , i \oplus g^{-1}(g(i)) = 0 & , \dots , g(i) & \rangle \\ | p(l, b, a) & , \dots , 0 & , \dots , g(i) & \rangle \rightarrow | p(l, b, a) & , \dots , g(i) & , \dots , g(i) & \rangle \\ | p(l, a, b) & , \dots , g(i) & , \dots , g(i) & \rangle \rightarrow | p(l, 2, 3) & , \dots , g(i) & , \dots , 0 & \rangle \end{array}$$

5.7.8.5 Propriétés

Une machine quantique comme celle décrite ici ne se contente pas de simuler une machine universelle au sens classique du terme. Elle peut simuler tout système, classique ou quantique. La machine

quantique peut admettre un nouvelle classe de programmes dans laquelle il est possible d'exploiter certaines propriétés quantiques comme la possibilité pour un bit de se retrouver dans un état superposé. Pour cela on ajoute aux opérations habituelles des machines de Turing 8 opérations supplémentaires qui résument l'ensemble des manipulations de base possibles sur un vecteur d'un espace de Hilbert à 2 dimensions, représentant un bit unique d'information :

$$V_0 = V_4^{-1} = \begin{vmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{vmatrix} \quad V_1 = V_5^{-1} = \begin{vmatrix} \cos\alpha & i \sin\alpha \\ i \sin\alpha & \cos\alpha \end{vmatrix} \quad V_2 = V_6^{-1} = \begin{vmatrix} e^{i\alpha} & 0 \\ 0 & 1 \end{vmatrix} \quad V_3 = V_7^{-1} = \begin{vmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{vmatrix}$$

opérations auxquelles correspondent les 8 programmes $\phi(V_i, a)$ exécutant V_i sur le premier bit de a . Les opérations peuvent se combiner par concaténation des programmes. Sur l'exemple d'un bit j de la collection 2 pouvant prendre les valeurs 0 ou 1 on a :

$$|\phi(V_i, 2), j\rangle = \sum_{k \in \{0,1\}} \langle k | V_i | j \rangle |\phi(V_i, 2), k\rangle$$

En exploitant les fonctions décrites ci-dessous, il est possible de simuler non seulement le comportement des machines de Turing classiques universelles ou non, mais tout système physique notamment quantique. Il est possible entre autres de générer au moyen d'un programme très court des nombres parfaitement aléatoires. Remarquons cependant que si le nombre est aléatoire, la machine n'est pas capable de le prouver. On suppose vraie au départ et de manière rigoureuse l'interprétation habituelle qui veut que le hasard pur décide de la valeur mesurée parmi les valeurs possibles. En d'autres termes, la mécanique quantique est modélisée par la mécanique classique. Il ne s'agit donc pas de la faire émerger d'un niveau d'abstraction plus fondamental.

L'une des plus surprenante propriétés des machines quantiques est leur possible utilisation pour tester certaines hypothèses de la théorie quantique, notamment la réalité des univers parallèles décrits par Everett et dont nous avons parlé en présentant la mécanique quantique. Vu que les divers univers restent corrélés tant qu'il n'y a pas mesure, autant profiter de la situation pour effectuer un calcul en parallèle sur l'ensemble des univers disponibles, réduisant d'autant le temps de calcul. Si, en fin d'exécution, la machine a bien trouvé le résultat, c'est que le modèle d'Everett est vrai. Au passage on aura effectué une infinité de calculs en simultané, et donné une réalité concrète aux fameuses "machines à oracle" qui en théorie de la complexité peuvent faire abstraction du temps de calcul d'une fonction.

5.7.8.6 Critiques

Les modèles quantiques n'échappent pas aux critiques. Ce sont des idéalizations par équations mathématiques. Les problèmes habituels des systèmes physiques, thermalisation, sensibilité à l'environnement, sont évacués par le seul fait que l'on ne se préoccupe généralement pas de donner aux équations un système physique dont elles seraient la modélisation. Néanmoins il n'est pas exclu que de tels systèmes physiques puissent exister et qu'ils donnent au calcul des pouvoirs nouveaux. Certains algorithmes pourraient changer de classe, des NP-complets devenant polynomiaux par exemple. Il pourrait être possible de coder 2 bits d'information dans un seul, et le système d'encryptage infaillible pourrait enfin voir le jour.

Et puis même si les modèles quantiques ne sont pas les plus réalistes, ce sont les plus amusants.

5.7.9 Bennett & Landauer : le nouveau démon (1988)

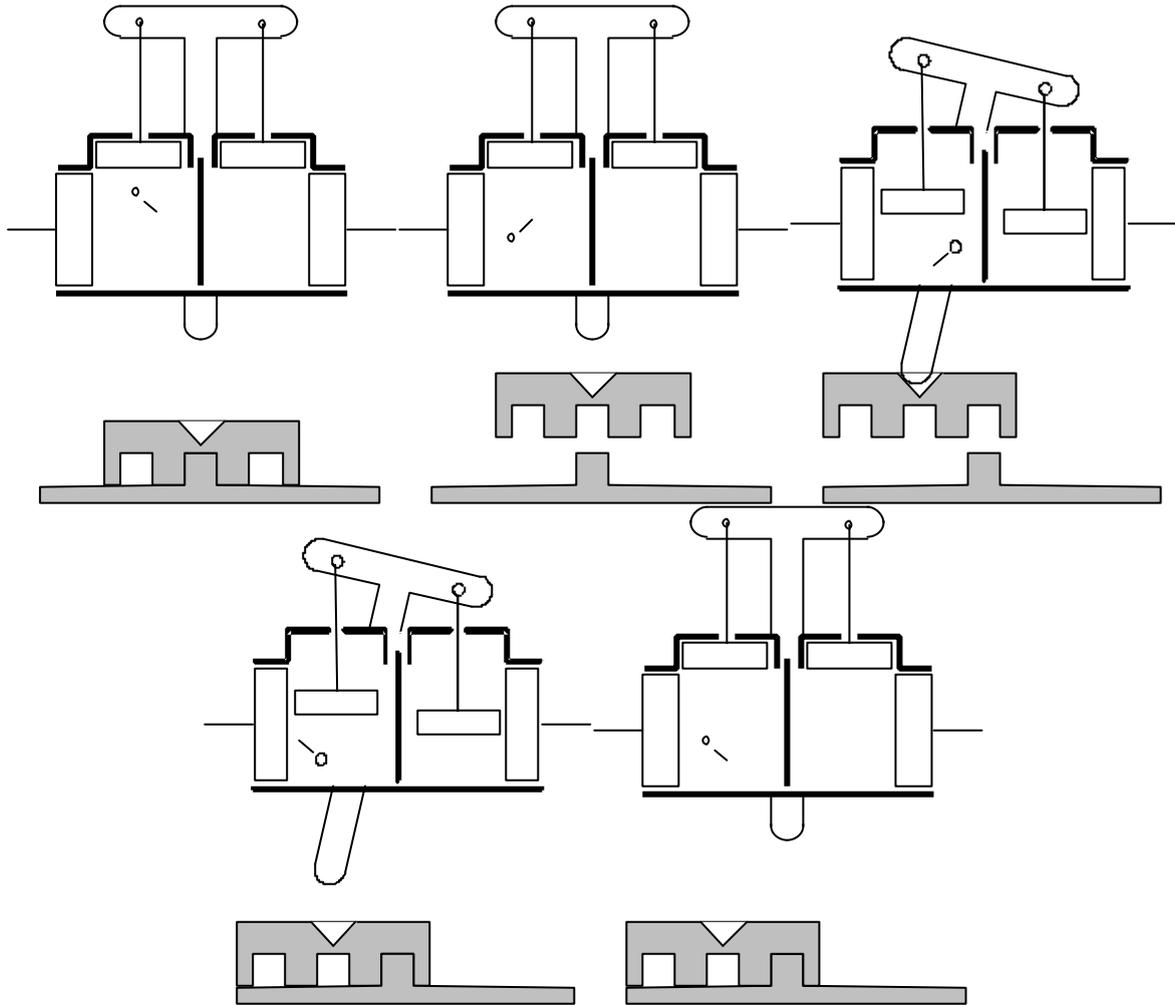
5.7.9.1 Retour du moteur de Szilard

L'évolution des connaissances a permis de mieux cerner le problème du démon de Maxwell. Nous savons depuis Szilard qu'une consommation d'énergie se produit dans le cycle du moteur qui porte son nom, mais nous ne savons pas encore en localiser l'origine.

En 1956, Brillouin et Gabor crurent comprendre que cette génération d'entropie venait de l'énergie nécessaire pour "éclairer" les particules. Un éclairage semblait indispensable pour pouvoir discerner une particule du fond de rayonnement existant dans l'enceinte de par la température homogène de cette dernière. L'évolution des connaissances permet de fournir de sérieux arguments permettant d'innocenter l'acte de mesure. Il est possible de connaître la position de la particule sans l'éclairer et sans dépenser

d'énergie. Plusieurs modèles existent. Nous allons en présenter un s'adaptant au cas du moteur de Szilard[6].

Il s'agit de connaître la position de la particule sans l'éclairer. Il suffit pour cela de mesurer de manière réversible la différence de pression entre les 2 moitiés du cylindre. Pour ce faire, on rajoute 2 pistons de mesure supplémentaires. La différence de pression entre les 2 parties fera basculer un fléau qui déplacera une clef à 3 positions. Le fléau peut être ensuite repositionné. La molécule restitue pour ce faire le travail que la baisse du piston de mesure lui avait fournie.



Le détail des opérations est le suivant.

1. Au départ la clef à 3 positions est verrouillée sur la position intermédiaire.
2. Déplacement de la clef pour son déverrouillage.
3. Descente du fléau qui, par la différence de pression, s'incline et déplace la clef. La baisse du piston fournit de l'énergie à la molécule
4. Déplacement de la clef qui se verrouille en fonction de la position de la molécule
5. Remontée du fléau sous l'action mécanique de la particule qui restitue l'énergie précédemment fournie.

A la fin, sans dépense d'énergie, la position de la clef aura mesuré la position de la particule. Toutes les opérations sont réversibles et le bilan énergétique final est nul.

En conclusion, la dépense d'énergie dans le moteur de Szilard peut ne pas être localisée dans la mesure. Elle ne peut plus se situer que dans le nécessaire effacement de l'information en mémoire, effacement requis par le retour aux conditions initiales à la fin d'un cycle.

5.7.9.2 Source froide

Dans le moteur de Szilard, la source froide réside dans le nécessaire refroidissement de la mémoire. Quel que soit le phénomène physique utilisé pour la concrétiser, l'énergie nécessairement dissipée lors de l'effacement ne doit pas donner au support physique du bit un niveau d'énergie supérieur aux barrières de potentiel permettant de distinguer les états mémoire. Sans cela, cette dernière aura un comportement comparable à celui de la valve du démon de pression. Ainsi, dans un circuit électronique par exemple, l'énergie d'origine thermique des électrons doit rester faible face à l'énergie mise en jeu pour donner une signification logique au mouvement des électrons.

Dans le système que nous venons d'étudier, le fait que la clé soit opérée sans frottements sous entend que sa position ne peut être verrouillée et qu'aucune barrière d'énergie n'existe entre les états. En d'autres termes, la seule agitation thermique suffit à donner un mouvement aléatoire à la clé, effaçant la mémoire à la première occasion. Le principe de mesure présenté sous entend donc que la clé est à température nulle alors que l'énergie thermique est employée par ailleurs pour faire fonctionner le moteur. D'autres systèmes de mesure non perturbatifs sont proposés par Bennett notamment, qui exploite les propriétés d'un domaine magnétique[7], mais ils n'échappent pas non plus aux critiques de cet ordre.

Le seul moyen de mesurer à température non nulle consisterait à rompre partiellement l'irréversibilité. Dans le système que nous venons d'étudier, cela se ferait au moyen de frottements dans les déplacements de la clé et du cadre, nécessitant des forces non nulles pour les mouvoir. La source froide serait alors clairement le milieu dans lequel se dissipe l'énergie dégagée par frottement. Reste à savoir si la dissipation ainsi engendrée est astreinte à devoir dépasser un minimum théorique. L'avis général est que de tels frottements peuvent être arbitrairement faibles. Mais 4 chercheurs ne sont pas de cet avis.

5.7.10 W.Porod & al : dissipation dans le calcul (1984)

5.7.10.1 Histoire

Les choses allaient bon train dans les recherches sur le calcul réversible quand un courrier portant 4 signatures proposa une nette remise en cause des données établies[35]. En gros, le lien entre irréversibilité et dissipation, implicitement accepté par tous, était remis en cause. Les auteurs sont collectivement désignées par Porod & al ou PGFP dans la littérature. Voici leurs arguments.

5.7.10.2 Les failles de l'interprétation classique

Une consommation de $kT \ln(2)$ par bit est généralement considérée comme le minimum théorique d'énergie à consommer pour le traitement d'un bit de données. Originellement les causes de cette consommation furent attribuées aux contraintes qu'impose la nécessité de distinguer le signal du bruit thermique dans la transmission de l'information entre portes logiques. Le signal doit être plus énergétique que le bruit et l'énergie du signal doit bien nécessiter une consommation. Cette interprétation, apparemment due à Von Neumann, dérive des théories de Shannon sur la transmission d'information sur canal bruité. Bien que jamais mise en défaut, PGFP estime qu'elle a été délaissée.

Landauer a ensuite essayé de localiser la consommation d'énergie dans les opérations réduisant l'espace des phases. Cela semblait être vrai pour toutes les opérations logiques binaires de base écrasant plusieurs états en 1 seul. On a cru alors pouvoir plonger ces opérations logiques dans des opérations conservatives comme celles effectuées par les portes de Fredkin pour que la consommation soit éliminée à ce stade. Furent donc conçus des modèles de machine dits réversibles remplissant en théorie cette condition. La seule consommation d'énergie était induite par l'effacement irréversible de bits de déchets en fin de parcours. Chaque effacement de bit effectuée alors un écrasement de 2 états possibles en 1 seul.

Mais PGFP fait remarquer que toute opération effectuée sur un bit est conservative, de type 1:1, du point de vue du bit lui même. De la sorte, aucun argument lié à l'entropie ne nécessite une quelconque dissipation lors de son effacement. En outre, Landauer fait apparaître une distinction entre bits aléatoires et bits calculés. Seuls l'effacement des premiers devraient être dissipatifs. Mais pour la tête d'une

machine de Turing, tout bit est aléatoire. Tout changement d'état d'un bit est réversible et tout effacement d'une chaîne aléatoire peut être programmé. De 2 choses l'une donc, où toute opération 1:1 est dissipative, où elle ne l'est pas. Dans les 2 cas, la réversibilité ne change rien.

Parmi les modèles de machines réversibles on peut noter :

- que les modèles balistiques genre ordinateur à billes font une totale abstraction du bruit thermique alors que la moindre agitation fausse totalement les calculs.
- que les machines browniennes ne sont pas vraiment réversibles puisqu'elles fonctionnent en présence d'une force "arbitrairement faible", et donc amenant une dissipation d'énergie apparemment réductible à volonté. Une dissipation nulle, si elle est possible ce qui reste à démontrer, ne peut apparaître qu'avec un temps de calcul infini.

Il serait bon de regarder de plus près le rôle que peut jouer le bruit thermique mis de côté depuis un certain temps dans les explications généralement admises, alors que les failles des modèles réversibles semblent en découler.

5.7.10.3 Origine vraie (pour PGFP) de la dissipation

L'ordinateur procède par cycles constitués de 2 types d'opérations : lecture et interprétation. Toute lecture de bande par une machine de Turing est une opération de mesure. Après celle-ci, l'état du système n'a pas le droit d'évoluer librement. Les étapes successives de mesure et d'évolution forcent le système dans une trajectoire qui n'est pas celle qu'il suivrait s'il répondait aux seules lois de la thermodynamique. Il est donc nécessaire que le système soit maintenu loin de l'équilibre thermique. C'est la nécessité de lutter contre la thermalisation du processus qui est à l'origine de la consommation.

Le fonctionnement d'une machine de calcul s'apparente alors à un moteur mu par un démon de Maxwell. La mesure effectuée par le démon autorise une évolution du système hors de son évolution thermodynamique normale. Mais un prix énergétique doit être payé. Si le système de mesure est en équilibre thermique avec son milieu il ne peut effectuer de mesure sur lui.

En résumé, la consommation vient du fait qu'il faut forcer le système à obéir aux lois de la logique et non à celles de la thermodynamique. Plus un système est proche de l'équilibre thermique, moins il peut calculer, et réciproquement. On est conforme à l'interprétation standard, au sein des théories de l'information de Shannon, basées sur les contraintes liées à la transmission sur canal bruité. Par elle, la valeur classique de $kT \ln(2)$ est retrouvée.

5.7.10.4 Ce qu'en pense Bennett

Pour PGFP la consommation résulte

- de la nécessité de distinguer le signal du bruit dans son parcours dans le calculateur,
- de la nécessité de lui faire choisir l'état suivant correct parmi les successeurs possibles, ce malgré le bruit thermique,
- de la nécessité de maintenir l'intégrité des systèmes aptes à mémoriser un état par une structure éloignée de l'équilibre mais qui en est séparé par une barrière d'énergie (domaines magnétiques d'une bande par ex)

PGFP semble dans le vrai pour le premier et troisième point, mais se trompe sur le second.

Les études précédentes ont clairement montré qu'une machine évoluant sans faire varier la taille de l'espace des phases est concevable. Si localement certaines opérations peuvent apparaître comme des écrasements d'états ou au contraire des éclatements d'états, l'évolution globale est de type 1:1. Les modèles browniens ou balistiques ont montré que le forçage de l'état suivant ne se fait pas de manière dissipative. Dans les modèles browniens par exemple, la transformation de l'information est réversible comme l'est une machine de Carnot qui pourtant ne fonctionne jamais à l'équilibre.

5.7.10.5 Ce qu'en pense Toffoli

La réduction par 2 du volume de l'espace des phases, et la dissipation qui lui est associée, n'est en fait induite que par les portes de type 2:1 réalisant les fonctions classiques. Dès lors que des portes logiques réversibles existent, la dissipation d'un bit d'information par porte logique n'est pas nécessitée par la thermodynamique. Seul le nombre global d'entrées et de sorties est à prendre en compte.

Outre cette consommation globale, il y a bien une consommation par porte logique, nécessité par le besoin de régénérer le signal perturbé par le bruit thermique. La régénération n'a pas à intervenir nécessairement après chaque porte, mais c'est là qu'elle est le plus économique en énergie. On obtient bien une consommation proportionnelle au nombre de portes et à la température. Mais la constante de proportionnalité peut être arbitrairement faible et ne dépend que de notre savoir faire technique. PGFP se trompe quand il situe là l'origine du minimum théorique de consommation.

5.7.10.6 Ce qu'en pense Landauer

Ton vigoureux chez Landauer qui met en avant plusieurs points.

Les étapes dissipatives du calcul sont celles qui perdent de l'information et n'ont pas d'inverse logique unique. Mais toute fonction irréversible peut être plongée dans une fonction réversible plus complexe. Bennett a mis en évidence la réalisation pratique de telles fonctions. Ces modèles sont critiqués mais leurs failles ne sont pas vraiment cernées par PGFP.

Shannon prévoit bien une énergie minimale pour transmettre un bit sur canal bruité, mais cette énergie n'est pas nécessairement dissipée, elle peut survivre jusqu'à destruction de l'information. Ceci a bien été déjà étudié. L'interprétation de Shannon n'a donc pas été rejeté d'emblée.

Prendre le point de vue du bit c'est oublier qu'ils ne sont rien par eux même. Tout n'existe que par les interactions qu'ils ont entre eux. Les lois régissant les bits ne sont pas linéaires, ils sont interdépendants.

Toutes les correspondances dans un système clos sont bien sûr de type 1:1, si tous les degrés de liberté sont autorisés. Cette propriété n'est pas propre au bit. Elle est sous-jacente à toutes les descriptions des systèmes physiques, qui, pour nombre d'entre eux, n'en sont pas moins dissipatifs.

PGFP considère que chaque étape de calcul comporte l'équivalent d'une mesure dissipative. Tout couplage de système n'est pas nécessairement une mesure et n'implique pas forcément dissipation.

5.7.10.7 Réplique de Porod & al

La réplique de PGFP à l'ensemble des critiques qui leur sont faites n'est pas moins vigoureuse. Il leur apparaît que les différents intervenants s'accordent sur le fait qu'il existe 2 sources de dissipation dans un calculateur :

- l'effacement d'information
- la lutte contre le bruit thermique.

Mais le calcul réversible prétend savoir s'affranchir de ces deux sources. Or s'affranchir de la première est inutile car l'effacement n'est pas dissipatif, et s'affranchir de la seconde est impossible.

L'idée selon laquelle l'effacement d'un bit correspond à une restriction de l'espace des phases ignore la distinction entre l'état logique et l'état physique d'un système. Seul un écrasement de plusieurs états *physiques* dans un seul est dissipatif. Les machines de Bennett se basant sur la réversibilité logique n'apportent rien au calcul non dissipatif.

Le problème du bruit thermique est éludé dans la plupart des modèles qui le considèrent comme réductible à volonté par le savoir faire technique. Les différents modèles de calcul non dissipatif ignorent le bruit thermique ou s'en affranchissent par construction. Par exemple, la machine brownienne de Bennett prend en compte le bruit thermique et l'exploite, mais elle ne peut fonctionner qu'en présence d'une force "arbitrairement faible" qui rompt la réversibilité et génère de la dissipation. On ne s'affranchit de cette dernière qu'à vitesse de calcul nulle. La dissipation disparaît en même temps que l'aptitude au calcul. La réversibilité en temps d'exécution fini n'a jamais été démontrée.

La mesure est requise après chaque traitement de bit. La théorie de l'information met en évidence une dissipation associée à toute mesure dès lors que le système de mesure est assujéti au bruit thermique. Il n'y a certes pas mesure par le seul fait que 2 systèmes sont couplés, mais par le fait que de l'information transite de l'un à l'autre et y reste. Pour cela, les 2 systèmes ne peuvent constituer un

ensemble isolé, mais un ensemble en contact avec une source thermique extérieure. Il en est de même pour l'effacement.

Il y a incohérence à prétendre d'une part que la lecture n'est pas dissipative et d'autre part que l'effacement de mémoire l'est. L'effacement d'un bit peut s'effectuer sans écrasement d'états en lisant la valeur du bit et en effectuant la correspondance 1:1 adéquate.

En résumé, beaucoup de points prétendument démontrés sont postulés dans les différentes critiques des arguments proposés. Il vaut mieux ne pas rejeter a priori la possibilité d'une dissymétrie fondamentale de l'axe du temps.

5.7.11 Zurek : entropie physique (1989)

5.7.11.1 Hasard et complexité

On rappelle que l'entropie de Boltzmann S se définit par, $S=k \ln(\Omega)$. où Ω représente le nombre d'états accessibles du système. Une des difficultés conceptuelles réside dans le fait que cette notion dépend du niveau de connaissance que l'on possède sur le système. Si l'on dispose d'une connaissance complète, l'évolution possible est unique et il n'y a donc pas de variation du nombre d'états accessibles, donc pas de variation d'entropie. C'est la méconnaissance que l'on a d'un état qui permet de mettre en jeu des notions probabilistes. Il est paradoxal que cette description modélise bien la réalité des phénomènes, alors qu'elle semble introduire une part d'arbitraire dans la notion d'aléatoire...

Les nouveaux concepts liés à l'information peuvent-ils nous permettre d'y voir plus clair ? La complexité de Kolmogorov jetant un nouvel éclairage les liens existant entre information et hasard, est-il possible de l'employer pour donner un sens nouveau à l'entropie ? Il appartient à Zurek d'avoir étudié la question dans le détail[46].

5.7.11.2 Entropie algorithmique

La description numérique complète d'un système thermodynamique nécessite une certaine quantité d'information. Comme celle-ci est en grande partie inaccessible, on essaie de la caractériser, notamment par son entropie de Shannon. Dans cette notion d'entropie, les probabilités jouent un rôle analogue à celui qu'elles ont dans les notions plus classiques de l'entropie comme celle de Boltzmann. Simplement ces probabilités s'appliquent cette fois aux descriptions binaires du système.

Mais l'entropie de Shannon n'est pas la seule manière de caractériser une chaîne binaire. La complexité de Kolmogorov en est une autre. Elle a cette particularité de ne pas faire intervenir les probabilités mais au contraire de servir de définition au hasard. Peut-on espérer par elle s'affranchir du côté subjectif que les probabilités confèrent à la thermodynamique ? L'idée de Zurek est de faire jouer à la complexité de Kolmogorov le rôle que l'on a fait jouer jusqu'à présent à l'entropie de Shannon. Le hasard y est donc introduit par le biais de la définition que cette notion permet de donner d'une chaîne aléatoire.

L'énumération de Ω états distincts accessibles nécessite $\log_2(\Omega)$ bits d'information. La complexité de Kolmogorov d'une description numérique s du micro-état d'un système est $K(s) = \log_2(s)$ si s est aléatoire. Le rapprochement avec Boltzmann se dessine déjà.

5.7.11.3 Exemple du gaz de Boltzmann

Un exemple peut nous convaincre que le remplacement de l'entropie de Shannon par celle de Kolmogorov est envisageable. Certes, on peut s'interroger sur le gain réel dû au remplacement de probabilités inconnues par une grandeur incalculable. Mais si la complexité de Kolmogorov d'une chaîne ne peut être connue exactement, elle peut être parfois estimée avec une bonne précision.

Afin de s'en convaincre, nous allons nous appuyer sur l'exemple d'un gaz de Boltzmann constitué de N particules dans une enceinte à D dimensions de volume V . Nous chercherons à estimer la taille d'une description minimale en cernant la nature des informations nécessaires à la description complète d'un micro-état du système.

Pour décrire totalement le micro-état du système, il nous faut coder la position et la vitesse de chaque particule. En fait, il est d'usage de prendre plutôt en compte l'impulsion p que la vitesse v , l'impulsion

ayant un caractère conservatif. Rappelons que $p = mv$ où m est la masse de la particule. La relation entre l'impulsion et la température est $|p| = (mkT)^{1/2}$. L'enceinte est divisée en cases de telle façon que l'on ait une chance raisonnablement élevée de n'avoir qu'une particule par case.

- Soit Δx la dimension spatiale d'une case. Son volume Δv est égale à Δx^D . Le nombre de cases remplissant l'espace est $V/\Delta v$. Préciser la case occupée par une particule demande donc $\log_2(V/\Delta v)$ bits.
- Soit Δp la dimension d'une case de l'espace des phases sur un axe des impulsions. La détermination totale de l'impulsion correspond à une valeur parmi $(p/\Delta p)^D = mkT^{D/2}/\Delta p^D$. Ce qui correspond à un contenu en information de $D/2 \log_2(mkT/\Delta p^2)$.
- Les particules sont indiscernables. La prise en compte de cette donnée permet de réduire la taille moyenne des représentations relatives aux positions en codant pour un axe non pas les coordonnées de chaque particule mais les différences de coordonnées entre particules dans l'ordre où elles apparaissent sur l'axe sans se soucier de l'identité de chaque particule. Les autres coordonnées de chaque particule seront notées normalement. Ainsi l'inversion de position de 2 particules deviendra insensible. En moyenne, sur l'axe considéré, les nombres à coder seront N fois plus petits. D'où une économie de bits.

Tous calculs faits, on retrouve à un terme d'erreur près l'expression de Sackur Tetrode de l'entropie d'un gaz parfait :

$$K = N(\log_2(V/N\Delta v) + D/2 \log_2(mkT/\Delta p^2))$$

En d'autres termes, l'utilisation d'une notion indécidable nous permet de retrouver comme approximation un résultat connu. L'idée d'utiliser la complexité algorithmique semble donc défendable. Néanmoins, la subjectivité de l'entropie statistique n'a pas disparu, car la division de l'espace en cellules reste arbitraire dans sa contrepartie algorithmique. Il semble cependant possible de limiter cette subjectivité en demandant au programme minimal d'inclure des informations relatives au maillage pris en compte de l'espace des phases. Dès lors, la subjectivité est reléguée à un rang analogue à celui du choix d'une machine de Turing particulière.

5.7.11.4 Entropie physique

Est-il possible de trouver une définition de l'entropie permettant de s'affranchir de la subjectivité ?

L'importance à accorder au hasard dans la caractérisation d'un système dépend du niveau de connaissance dont on dispose sur lui. La notion d'entropie semble pourtant ne pas souffrir l'arbitraire tant elle prédit avec précision l'évolution des systèmes thermodynamiques. On peut s'interroger sur ce que mesure vraiment l'entropie. Boltzmann et Maxwell la soupçonnaient déjà d'être une mesure de l'ignorance. Szilard établit un lien plus étroit à partir du démon de Maxwell. Reprenant ces idées, on peut conjecturer une définition de l'entropie qui ne doit plus grand chose au hasard : l'entropie physique.

Soit d une chaîne décrivant un système thermodynamique avec un certain degré de précision. L'entropie physique S est considéré comme la somme de 2 contributions :

- $K(d)$, représentation la plus concise de la description des données connues du système,
- H_d , entropie au sens de Shannon des informations manquantes pour obtenir une description complète du système.

$$S_d = H_d + K(d) = -\sum p_{k|d} \log_2 p_{k|d} + K(d)$$

Dans l'exemple précédent, on opposait une étude se basant sur une notion classique statistique de l'entropie, et une autre étude du même cas s'appuyant sur une description complète du système et l'entropie algorithmique associée. Le premier cas correspond à $S_d = H_d$ avec $K(d) = 0$, le second à $S_d = K(d)$ avec $H_d = 0$. La notion est donc à première vue cohérente avec les notions déjà envisagées pour définir l'entropie. Elle est en outre conforme aux intuitions déjà manifestées de caractériser l'entropie comme étant une somme entre l'inconnu et le connu.

Afin de mieux se convaincre, nous ferons appel à des machines de Turing associées à un mécanisme de mesure. A chaque mesure :

- les probabilités conditionnelles des états sont changées, amenant une diminution de H_d ,
- la quantité d'information disponible sur la bande augmente, amenant une augmentation de $K(d)$.

Si le système est à l'équilibre, sa description est incompressible. Dans ce cas, on démontre que la compensation est parfaite et que S_d reste constant. Il s'agit d'un résultat idéal s'appuyant sur l'idée que la compression de données peut se réaliser de manière réversible. Cela est vrai seulement si la chaîne comprimée est connue d'avance... L'incalculabilité d'une telle chaîne modère un peu ce résultat.

Si par contre on est loin de l'équilibre (état inhomogène), une acquisition d'information peut ne pas faire augmenter notablement la complexité algorithmique, voire la faire diminuer. Dès lors, une mesure se manifeste par une diminution de S_d suivant de près celle de H_d .

5.7.11.5 Démon de Maxwell

Nous allons nous inspirer du moteur de Szilard pour concevoir un système thermodynamique dont l'évolution pourrait être dirigée par un automate pouvant acquérir et mémoriser des données sur le système. L'énergie fournie après transition d'un état initial vers un état final se décomposera en :

- ΔW^+ liée à l'évolution de l'entropie statistique au sens de Shannon. Elle correspond à l'entropie au sens thermodynamique classique et sa valeur est fixée par les lois classiques : $\Delta W^+ = T (H_f - H_i)$
- ΔW^- liée à la mise à jour des mémoires évoluant entre l'état initial et final d'un contenu i vers un contenu f . Nous allons discuter de sa valeur. Nous allons nous appuyer sur les propriétés connues de la complexité algorithmique.

$$\begin{aligned} K(f,i) &= K(f) + K(i|f^*) &= K(f) + K(i | (f,K(f))) \\ \implies K(f,i) - K(f) &= K(i | (f,K(f))) \\ \implies K(i,f) - K(f) &= K(i | (f,K(f))) \\ \implies K(i) - K(f) &= K(i | (f,K(f))) \quad \text{car } i \text{ permet de calculer } f, \text{ d'où } K(i,f) = K(i) \end{aligned}$$

Pour calculer de manière réversible i à partir de f^* on a besoin d'un complément d'information $i|f^*$, dont la longueur (1^o ligne du calcul) est égale à $K(i | (f,K(f)))$, terme lui même égal à $K(i) - K(f)$. C'est le nombre de bits à effacer pour passer du contenu f au contenu i en information de la mémoire. L'entropie générée dans le calcul inverse (calcul de f d'après i) s'en déduit immédiatement : $\Delta W^- = K(f) - K(i)$.

L'énergie totale fournie par le système vaut :

$$\Delta W = \Delta W^+ + \Delta W^- = T (H_f - H_i) + T (K_f - K_i) = T (S_f - S_i)$$

La définition que l'on vient de se donner de S , entropie physique, répond donc aux propriétés d'une entropie. On est dans le cas où les transformations sont supposées réversibles. La génération d'une chaîne à partir de son programme minimal n'est pas normalement réversible, puisque l'inverse est indécidable. L'information manquante pour permettre l'inversion n'est ni plus ni moins que la chaîne minimale elle même, supposée donc connue alors même que l'on cherche à la calculer. Vu cela, le rendement réel sera donc plus faible, ΔW représente l'énergie maximale extractible.

5.7.11.6 Discussion

Entropie algorithmique et physique sont des mesures correctes du désordre pour un système vu de l'extérieur, démon de Maxwell compris. Mais l'entropie physique est nécessaire pour suivre l'extraction d'énergie du point de vue du démon observateur. Comme la connaissance d'un système est généralement très faible, l'entropie statistique au sens de Boltzmann-Gibbs-Shannon est très proche de l'entropie physique. Mais l'entropie physique permet de prendre en compte l'existence d'un éventuel démon et sa contribution au processus d'extraction de l'énergie. Parallèlement, le théorème d'incomplétude de Gödel apparaît comme l'une des raisons de l'inaccessibilité du rendement optimal des machines thermiques.

Dans le cas de la mécanique quantique, la définition des entropies est similaire. Le choix de la base de l'espace de Hilbert qui caractérise un système quantique devient analogue au choix du maillage de l'espace des phases. Le principal contraste réside dans la nature de la notion de mesure.

5.7.11.7 Conclusion

Les regards successifs sur le problème de l'entropie ont associé aléatoire et probabilités, oubliant l'approche algorithmique. Parallèlement à cela, la physique du calcul s'occupait des contraintes physiques imposées aux ordinateurs. Il a fallu attendre aujourd'hui pour avoir l'idée de faire l'inverse et de réfléchir aux contraintes que la science du calcul impose aux systèmes physiques. Se basant sur la définition algorithmique de l'aléatoire, la notion d'entropie physique est indispensable pour comprendre le rôle du démon de Maxwell de son propre point de vue.

Le démon peut être simulé par un automate

- mesurant de manière réversible,
- calculant comme une machine universelle,
- pouvant choisir des stratégies d'optimisation pour extraire de l'énergie.

L'entropie physique a permis de donner un support théorique à une idée ancienne : considérer l'entropie comme une somme de ce qui est connu et de ce qui est inconnu d'un système.

En incluant la nécessité pour les algorithmes minimaux de contenir la définition du maillage, le caractère subjectif de ce dernier est remis en cause. La taille du maillage est contrainte par le niveau d'information qu'il doit fournir d'une part, et la nécessité d'être décrit brièvement de l'autre. En fait, la subjectivité ne disparaît pas vraiment. Elle réside alors dans les caractéristiques de la MTU à utiliser.

5.7.12 Conclusion

5.7.12.1 Les formes de la réversibilité

La réversibilité, cette aptitude pour un système à rendre interchangeables les données et les résultats peut revêtir plusieurs aspects.

- déterministe
- indéterministe
- asymétrique

Nous avons démontré que l'exécution inverse d'un programme était possible et de manière déterministe grâce à la collecte dans un déchet des informations normalement perdues lors de l'exécution directe. Ce type de réversibilité s'applique aux systèmes fermés n'échangeant avec l'extérieur ni information ni énergie. Dans un tel système isolé, les études entreprises jusqu'ici permettent d'affirmer que la quantité d'information est constante, au même titre que la quantité d'énergie. Si l'on considère le système calculateur + environnement, le déchet se retrouve en fait dans le micro-état de l'environnement. A chaque effacement de valeur, l'énergie thermique dissipée génère des corrélations dans les mouvements des atomes agités par la chaleur, corrélations qui contiennent l'information perdue.

L'exécution inverse est néanmoins possible, mais de manière non déterministe, si aucun déchet n'a été généré lors de l'exécution directe. Retrouver les données en faisant fonctionner le système de calcul à l'envers est dès lors un processus aléatoire affecté d'une probabilité de succès qui décroît de manière exponentielle avec le nombre d'étapes irréversibles. Dans l'évaluation de ces chances, on fait intervenir des considérations analogues à celles de la thermodynamique statistique ou de l'entropie de Shannon. Notons que si une grandeur peut prendre un nombre infini de valeurs, son effacement réduit à zéro les probabilités d'exécution inverse. Ceux qui cherchent dans la physique du calcul des modèles pour la physique concluent ainsi que la réversibilité physique implique que toutes les grandeurs du monde physique sont quantifiées et ne peuvent prendre qu'un nombre fini de valeurs.

Enfin, on peut prendre en compte l'existence d'une réversibilité non symétrique, rendant possible l'exécution inverse mais avec des lois légèrement différentes, c'est à dire avec une machine différente de celle qui a été utilisée dans le calcul direct. On peut considérer que là aussi le cas déterministe et non déterministe peuvent exister. De l'idée originale de réversibilité on n'a conservé que l'interchangeabilité données-résultats.

5.7.12.2 Nature du temps

N'en déplaise à Stephen Hawking, les ordinateurs ne définissent pas la flèche du temps. Les machines de Turing réversibles en sont la preuve. Quand on observe une telle machine, il est impossible de savoir si elle fonctionne à l'endroit où à l'envers.

La présente étude semble compléter celle liant la flèche du temps et la thermodynamique. Les systèmes physiques évoluent vers les états les plus probables, ces derniers étant caractérisés par des descriptions binaires minimales plus longues, correspondant à une entropie informatique plus élevée. Ceci est cohérent avec le fait que les longues descriptions possibles sont nécessairement plus nombreuses que les descriptions courtes. La flèche du temps informatique est donc une réplique de la flèche thermodynamique, qui est elle-même le reflet des inégalités de Bayes dans les organes de calcul lorsqu'une opération irréversible surgit.

Depuis longtemps les physiciens présentaient que l'entropie ressemble à une mesure du désordre, mais sans pouvoir définir au juste ce qu'est le désordre. Car sur le plan microscopique toutes les configurations d'un système se valent et sont équiprobables. Aujourd'hui nous en savons un peu plus. Le désordre est lié à la longueur des descriptions minimales. Un système est d'autant plus désordonné que sa description est peu compressible. Ceci est clairement formalisé notamment dans la notion d'entropie physique de Zurek. Pour l'informaticien l'effet le plus marquant des inégalités de Bayes se manifeste donc par le fait que les systèmes évoluent préférentiellement vers les configurations dont les représentations minimales vont croissant, pour finir par l'état homogène dont la description est incompressible.

En fait la différence entre travail et chaleur, deux formes de l'énergie, est de nature informatique. Le travail devient chaleur dès lors que la description des mouvements mécaniques des atomes devient trop complexe pour être connue. La transformation inéluctable du travail en chaleur traduit le fait qu'un système devient de plus en plus complexe à décrire et qu'à moment donné sa description doit faire intervenir des grandeurs statistiques.

L'informatique peut cependant nous donner un éclairage supplémentaire. En effet, en raison de ce lien entre entropie et information, Boltzman fit remarquer que le temps biologique perçu par les êtres vivants devait suivre le mouvement d'entropie croissante. En d'autres termes, notre cerveau, système calculatoire, ne perçoit jamais de baisse d'entropie car la conscience que nous avons des choses, assujettie aux exigences de l'entropie informatique de notre cerveau, ne peut aller que dans le sens de l'entropie croissante. On peut en conclure que la probabilité que notre cerveau perçoive le temps à l'envers est infinitésimale mais non nulle...

Donc l'axe du temps peut être fondamentalement symétrique, les inégalités de Bayes le rendent dissymétrique dès lors que l'on approxime son contenu en information. Plus un système est homogène, plus la description de son micro-état est complexe, moins elle est connaissable dans le détail, plus la statistique rentre en jeu, plus elle se perd au milieu d'autres configurations présentant les mêmes valeurs des grandeurs statistiques, plus Bayes intervient. Mais la dissymétrie ainsi induite est la même pour les systèmes physiques et pour notre conscience, raison pour laquelle nous ne percevons pas le monde à l'envers.

Bien après Boltzmann, N.Wiener fit remarquer qu'aucune communication n'était possible entre des êtres vivants dans 2 milieux dont l'entropie évolue en sens opposé. Si une conversation entre 2 personnes de chacun des 2 mondes était tentée elle serait très confuse. Chacun percevrait les réponses de l'autre lui parvenir avant que les questions soient posées... Mais, de manière fondamentale, aucun signal ne peut être échangé. Pour chaque monde, l'autre ne peut émettre de signaux mais seulement les absorber.

Comme ce qui vient d'être dit est vrai pour n'importe quel signal porteur d'information, certains, comme le physicien anglais Frank Russel Stannard[40], concluent que deux mondes vivant des évolutions entropiques inversées peuvent coexister au même endroit, s'interpénétrer, et s'ignorer totalement sans existence possible d'une quelconque influence de l'un sur l'autre.

5.8 Flèche cosmologique

5.8.1 Organisation de l'Univers

Le refroidissement de la matière est proportionnel au carré du rayon de l'univers, alors que le refroidissement des rayonnements est proportionnel au rayon simple. Ces écarts dans le refroidissement sont les sources de négentropie générant les hétérogénéités que sont les galaxies, étoiles et planètes. Il existe donc un lien entre l'évolution entropique ou "informatrice" et l'expansion de l'univers pour les structures à grande échelle. Cette implication pourrait-elle se retrouver dans tous les phénomènes entropiques, y compris sur les structures les plus fines[13] ?

5.8.2 Entropie objective et subjective

Déjà en 1914 le statisticien Emile Borel, au nom si célèbre, remarquait que l'entropie n'est pas liée à l'apparition de désordre ou à la perte d'information, mais plutôt au changement d'échelle à partir de laquelle celles-ci peuvent être appréhendées. Ainsi l'équilibre thermique entre 2 corps ne crée pas une température homogène, car le système est toujours aussi inhomogène au niveau des molécules qui peuvent conserver la même diversité dans leurs énergies cinétiques que celles qu'elles avaient avant équilibre. L'entropie diminue la finesse des inhomogénéités sans les détruire. Borel estima que lorsque le degré de finesse atteint une certaine valeur, les irrégularités peuvent alors réellement disparaître et voir la véritable cause de la création d'entropie qui, auparavant, n'est créée que pour l'observateur pouvant accéder à un niveau de finesse donné.

Mais quel peut être le mécanisme destructeur des petites inhomogénéités ? Emile Borel pensa que les fluctuations gravifiques dues aux mouvements des masses de l'Univers peuvent former le mécanisme recherché. En 1935, Arthur Eddington suggéra que ce couplage entre petits systèmes et Univers pourrait résulter du mouvement d'expansion de ce dernier. L'idée n'est pas morte puisqu'aujourd'hui l'américain David Layzer les reprend.

5.8.3 Entropie de l'Univers

S'il existe un lien entre expansion de l'Univers et entropie, peut-on envisager ce qui se produira lorsque l'Univers engagera une éventuelle recontraction ? Les rôles des conditions initiales et finales des systèmes seront ils inversés ? Stephen Hawking, encore lui, affirma un temps (!) que dans une telle situation, l'entropie évoluerait naturellement en sens inverse du sens actuel, et qu'en conséquence les êtres vivants et toutes les machines de calcul percevraient le temps à l'envers. Stephen Hawking est revenu sur cette vision des choses. L'Univers peut se contracter et son entropie continuer à croître. Comme le fit remarquer entre autres l'un de ses collaborateurs Roger Penrose[34], le "Big crunch" par lequel se terminera peut être notre Univers ne sera pas l'inverse temporel du big bang. S'il doit avoir un terme, l'Univers finira dans un état entropique différent de celui qui lui a fait voir le jour (!).

5.8.4 Conclusion

Le statut de flèche du temps est peut être prématuré en ce qui concerne la flèche cosmologique. Rien ne l'oblige apparemment à coïncider avec les autres flèches. Si l'Univers se contractait au lieu de se dilater, il est probable que nos horloges ne s'en rendraient pas compte.

5.9 Flèche quantique

5.9.1 Irréversibilité et mesure

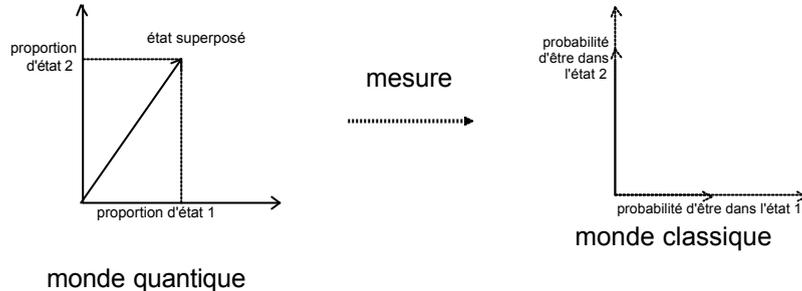
On rappelle que l'état d'un système quantique est représenté par un vecteur, appelé vecteur d'état, dans un espace de Hilbert. La grandeur à mesurer est représentée par un opérateur matriciel dont les vecteurs propres définissent une base d'un sous espace.

La mesure d'une grandeur physique joue un rôle particulier, celui de permettre la transition entre 2 mondes :

- un monde quantique dans lequel les systèmes physiques peuvent être dans une combinaison de plusieurs états,
- un monde classique dans lequel l'état d'un système est unique.

Les proportions d'états de la combinaison quantique représentent les probabilités de se retrouver dans l'un ou l'autre des états physiques possibles.

L'opération de mesure revient à remplacer le vecteur d'état par l'un des vecteur propres qui définissent la base. La valeur propre correspondante représentera la valeur mesurée. Il y a donc autant de résultats de mesure possible que de vecteurs propres pour l'opérateur de mesure considéré. Avant mesure, la projection du vecteur d'état sur l'axe défini par un vecteur propre représente la probabilité associée au résultat de mesure correspondant.



Le comportement des systèmes dans chacun des deux mondes quantique et classique est parfaitement déterministe et la réversibilité est concevable. Tout se complique lors de la transition d'un monde à l'autre. Durant la mesure, il se produit donc une "réduction d'état" consécutive à la perte des coordonnées du vecteur d'état, qui ne peuvent être retrouvées par la seule connaissance du résultat de la mesure. Correspondant à une perte d'information, la réduction est bien une opération fondamentalement irréversible.

5.9.2 Collision temporelle

Eddington a, dès le début de la mécanique quantique, fait remarquer que si l'évolution d'un système est décrite par l'équation de Schrödinger Ψ , son complexe conjugué Ψ^* représentait lui l'évolution du même système vers le passé. De sorte que la probabilité $|\Psi|^2 = \Psi \Psi^*$ pourrait s'interpréter comme une rencontre entre deux temps, l'un issu du passé l'autre de l'avenir. En fait cela signifie que la probabilité définie par l'équation de Schrödinger est symétrique par rapport au temps.

5.9.3 Complémentarité

On serait tenté de croire que la réduction de fonction d'onde n'est que l'analogie de ce que l'on rencontre en probabilités lorsque l'on acquiert de l'information sur le système étudié, et dont nous avons déjà parlé dans la flèche statistique. Ce qu'il est important de comprendre, c'est que la description probabiliste antérieure à la mesure n'est pas le reflet de notre ignorance, mais bien, jusqu'à nouvel ordre, une description complète du système. Le changement s'opérant à la mesure est donc un changement physique réel et irréversible de la nature de l'objet mesuré.

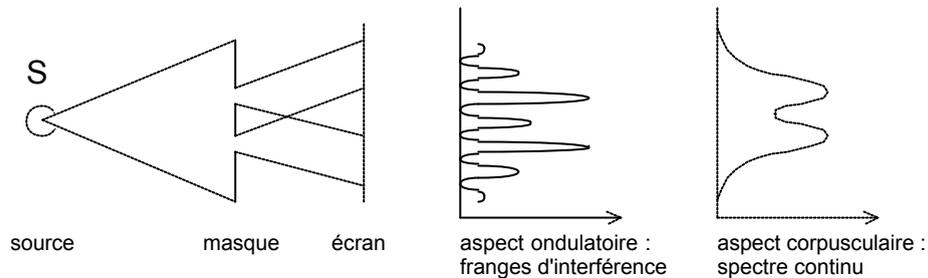
Nous avons déjà parlé de l'une des conséquences de ce changement irréversible. Elle amène l'existence de grandeurs dites complémentaires, qui sont telles qu'il est impossible de connaître simultanément les valeurs prises par l'une et par l'autre. La mesure effectuée pour une grandeur, en écrasant le vecteur d'état sur un axe, perd les informations qui auraient permis de connaître la valeur qu'avait l'autre grandeur avant mesure. Mathématiquement cela se produit à chaque fois que les 2 opérateurs correspondant aux 2 grandeurs à mesurer sont représentées par 2 matrices qui ne commutent pas entre elles.

C'est le cas des opérateurs donnant la position et l'impulsion d'une particule. La mesure de l'impulsion, en faisant perdre à la particule la possibilité de connaître la position, va lui faire perdre son comportement corpusculaire pour mettre en évidence des propriétés délocalisées ondulatoires. Une particule nous apparaît dès lors tantôt comme un corpuscule, tantôt comme une onde, jamais pleinement comme les deux à la fois, elle n'est en fait ni l'une ni l'autre. L'exemple de l'expérience des fentes d'Young va "éclairer" ce propos.

5.9.4 Exemple des fentes d'Young

Soit une source de lumière éclairant un masque avec deux fentes. Derrière le masque se trouve un écran. On observe les figures que forment la lumière sur l'écran. De deux choses l'une

- La lumière est une onde. C'est dire qu'elle est délocalisée. Cette onde se propage jusqu'au masque. De l'autre côté, chacune des deux fentes sera perçue comme une source ondulatoire. Ce qui se produit alors est conforme aux phénomènes issus du battement de deux ondes. Sur l'écran se formeront des franges d'interférence.
- La lumière est constituée de corpuscules. Chaque corpuscule passe soit par une fente soit par l'autre. Au total, sur l'écran, on verra pour chaque trou la superposition du flux lumineux issu de chaque fente ce qui produira une figure continue avec deux pics.



que se passe-t-il quand on réalise l'expérience ? On observe bien les franges d'interférence, mais constitués d'impacts localisés. Les franges représentent les répartitions statistiques d'impacts de particules : les photons. Ce qu'il est important de noter, c'est que le phénomène persiste même quand l'intensité de la lumière est si faible qu'elle correspond à un envoi de photons un par un. Autrement dit, durant tout le parcours entre le masque et l'écran, le photon "connaît" l'existence des deux chemins pour interférer avec lui même. Il est dans une superposition des états correspondant aux deux chemins possibles jusqu'à ce que l'impact sur la pellicule "mesure" une position parfaitement localisée.

Tant que l'on ne cherche pas à observer le photon en tant que particule, la lumière se comporte comme une onde et fait apparaître des phénomènes d'interférence. Dès lors que l'on ajoute un dispositif destiné à localiser la particule en essayant de savoir par quelle fente passe chacune d'elle, on perd la notion ondulatoire et on obtient sur l'écran un spectre continu. Le caractère complémentaire de l'impulsion et de la position est quantifié dans une des relations d'incertitude d'Heisenberg :

$$\delta x \delta p \geq \hbar/2$$

où δx est l'incertitude sur la position, δp l'incertitude sur l'impulsion, et \hbar une constante fondamentale.

L'interprétation habituelle situe l'origine de la complémentarité dans le fait que pour connaître la position de la particule il est nécessaire de l'éclairer, et que cet éclairage perturbe sa position. C'est donc les moyens mis en oeuvre pour mesurer la position des particules qui effacent les franges d'interférence en perturbant les trajectoires. La mesure de la position perturbe la mesure de l'impulsion. Cette interprétation est incomplète comme nous le verrons.

La relation d'Heisenberg est vraie pour les particules autres que celles de la lumière. Que ce soit un flux d'électrons ou de noyaux atomiques, une source formera normalement sur un écran des franges d'interférence correspondant à la répartition statistique des particules. Chacune sera passée par un trou de l'écran en connaissant l'existence de l'autre.

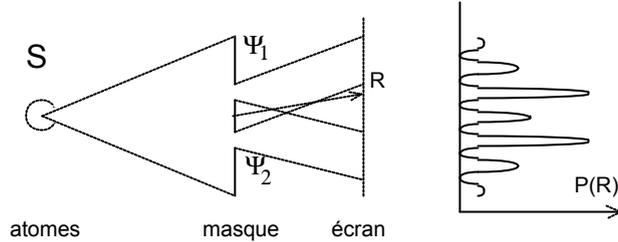
5.9.5 Mesure non perturbatrice

Récemment ont cependant été mis en évidence des moyens de connaître la fente empruntée par une particule sans pour autant perturber sa trajectoire[38][39]. La mesure devient non perturbatrice. Que deviendraient les franges d'interférence si une telle mesure s'effectuait ? Subsisteraient-elles ? D'après la théorie, les franges disparaîtraient aussi sûrement que si la trajectoire avait été perturbée. La complémentarité des grandeurs quantiques serait donc un phénomène beaucoup plus fondamental.

Le protocole proposé consiste à travailler avec des noyaux d'atomes. Les fentes d'Young sont matérialisées par 2 cavités résonnantes. Chaque atome est excité par un laser avant de pénétrer dans

l'une des deux cavités. Là, il se désexcite en émettant un photon. On démontre que cette émission ne perturbe pas suffisamment la trajectoire pour permettre à elle seule d'affecter l'existence éventuelle de franges d'interférence sur l'écran.

Dans un premier temps, on ne s'occupe ni de laser, ni de cavités résonnantes ni de mesure.



On se retrouve donc dans le cas où les franges d'interférence existent. Voyons comment le formalisme de la mécanique quantique met en évidence l'existence de ces franges. La fonction d'onde Ψ décrivant le déplacement du centre de gravité des atomes est la somme de 2 termes Ψ_1 et Ψ_2 . On a :

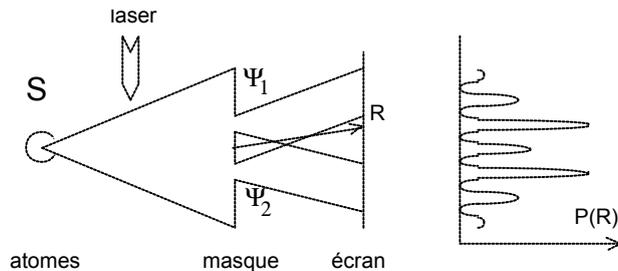
$$\Psi(r) = 1/\sqrt{2} (\Psi_1(r) + \Psi_2(r))$$

Ceci formalise le fait que $\Psi(r)$ est un état superposé. Le facteur $1/\sqrt{2}$ ramène la norme du vecteur superposé à 1. La probabilité associée à la présence du photon est :

$$P(r) = |\Psi(r)|^2 = 1/2 (|\Psi_1(r)|^2 + |\Psi_2(r)|^2 + \Psi_1(r)^* \Psi_2(r) + \Psi_2(r)^* \Psi_1(r))$$

Le terme en italique fait apparaître le battement à la base de l'existence des franges d'interférence.

Dans un deuxième temps, on met le laser en route pour faire en sorte que l'atome sème un photon sur son chemin. L'information sur le chemin n'est pas disponible puisque l'on ne s'occupe toujours pas des cavités résonnantes.



L'état interne de l'atome est noté $|e\rangle$. Le vecteur d'état peut s'écrire :

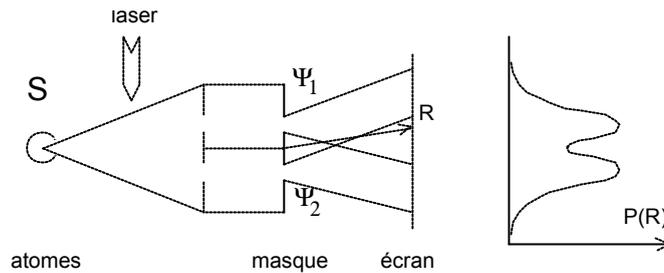
$$\Psi(r) = 1/\sqrt{2} (\Psi_1(r) + \Psi_2(r)) |e\rangle$$

et la densité de probabilité :

$$P(r) = 1/2 (|\Psi_1|^2 + |\Psi_2|^2 + \Psi_1^* \Psi_2 + \Psi_2^* \Psi_1) \langle e | e \rangle$$

le laser n'a donc pas supprimé les interférences.

Dans un troisième temps, on met en place les cavités résonnantes. L'état correspondant à un photon qui se retrouve dans la cavité 1 est noté $|1,0\rangle$. L'état correspondant à un photon laissé dans la cavité 2 est noté $|0,1\rangle$. L'état de l'atome après émission est noté $|f\rangle$.



La fonction d'onde est :

$$\Psi(r) = 1/\sqrt{2} (\Psi_1(r) | 1,0 \rangle + \Psi_2(r) | 0,1 \rangle) | f \rangle$$

La densité de probabilité est :

$$\begin{aligned} P(r) &= 1/2 (|\Psi_1|^2 + |\Psi_2|^2 + \Psi_1^* \Psi_2 \langle 1,0 | 0,1 \rangle + \Psi_2^* \Psi_1 \langle 0,1 | 1,0 \rangle) \langle f | f \rangle \\ &= 1/2 (|\Psi_1|^2 + |\Psi_2|^2) \end{aligned}$$

car les termes $\langle 1,0 | 0,1 \rangle$ et $\langle 0,1 | 1,0 \rangle$ tendent vers 0. Les franges d'interférence disparaissent donc, et ce sans que la cause se situe dans une perturbation de la trajectoire. La cause se situe ailleurs. Elle est la manifestation de l'un des phénomènes les plus curieux du monde quantique, la non séparabilité. L'atome reste en effet corrélé au photon émis dans la cavité, quelle que soit la distance qui l'en sépare, et jusqu'à l'impact sur l'écran. Sans prise en compte de ce phénomène, l'interprétation habituelle des relations d'incertitude d'Heisenberg est insuffisante pour tout décrire.

5.9.6 Discussions sur la mesure

Tel que présenté, le statut de la mesure en mécanique quantique est mal déterminé. L'appareil de mesure est effectivement considéré comme un appareil macroscopique répondant aux lois du monde classique. La réduction de fonction d'onde a donc un statut hybride d'appareillage macroscopique agissant sur un système quantique.

On peut essayer de considérer que l'appareil de mesure a un comportement qui peut lui-même être décrit par la mécanique quantique. Soit donc à vouloir effectuer une mesure sur un système quantique régi par une fonction d'onde Ψ_s . L'appareil de mesure est lui-même un système considéré sous son aspect quantique et géré par sa fonction d'onde Ψ_a . Après interaction, le système global sera régi par sa fonction d'onde $\Psi = \Psi_s \Psi_a$ et restera dans cet état puisque rien ne vient mesurer le système de mesure lui-même. Il s'agit d'un état quantique, donc constitué d'une superposition des états correspondant aux différents résultats de mesure que peut fournir l'appareil. Il est assez gênant, quand on pose une question, d'obtenir une superposition de toutes les réponses possibles.

On peut donc rajouter un appareil destiné à mesurer le système appareil + système quantique. Mais le même raisonnement s'applique. On peut rajouter autant d'appareils se mesurant à la chaîne sans résoudre le problème. C'est d'ailleurs ce que l'on fait en pratique jusqu'à l'appareil ultime à nos yeux : l'observateur régi lui aussi par son vecteur d'état. En fin de compte, l'observateur, à l'instar du reste de l'appareillage et du système quantique, se retrouvera dans tous ses états, ce qui n'est jamais agréable. Certains se vengent en cherchant à faire vivre avant eux à d'innocents représentants de la race féline le sort qui leur est destiné (!).

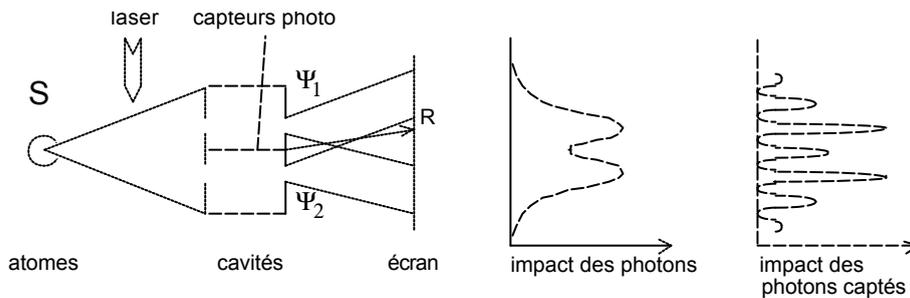
5.9.7 Rôle de l'environnement

Un dernier laron a été oublié dans notre histoire : l'environnement du système physique et de l'appareillage de mesure. W Zurek a démontré que si l'on définit un hamiltonien de l'interaction avec l'environnement, cette interaction apparaît comme responsable de la suppression des états superposés[47][48]. Seuls les états purs correspondant aux valeurs pouvant être mesurées subsistent, dès lors que l'on néglige les degrés de liberté de l'environnement qui ne sont jamais observés.

D'après Zurek, un système est classique ou quantique selon que l'on prend en compte ou non l'environnement. Un système classique est ouvert et dissipe vers l'environnement, un système quantique est isolé. Ce qui est irréversible c'est la rentrée dans le système physique. La mesure signifie que l'on fait désormais partie intégrante du système et non plus de l'environnement. En toute rigueur, le monde classique n'est qu'une apparence. Car les états superposés ne disparaissent pas totalement. Ils deviennent infinitésimaux. En d'autres termes, le chat de Schrödinger, même vivant, reste un petit peu mort quand même.

5.9.8 Recouvrement de l'interférence

Le discours précédent sous entend que lorsque deux grandeurs physiques sont complémentaires, la connaissance de l'une amène les informations relatives à l'autre à se dissiper dans l'environnement. Il est parfois possible en effectuant une mesure sur l'environnement de retrouver les informations perdues, mais toujours au prix de la perte de celles dont on disposait déjà. Une illustration de ce propos va être discutée. Elle réside dans la suite à donner à l'expérience de mesure non perturbatrice décrite précédemment. Si l'on ouvre la séparation entre les 2 cavités après le passage de la particule, on perd l'information relative au chemin suivi par la particule. On ne retrouve pas directement les franges d'interférence, mais il est possible de récupérer des informations susceptibles de les reconstruire. Pour cela, on place un mur de détection photo électrique à la place de la paroi enlevée. L'adaptation de la fonction d'onde du photon à la cavité après enlèvement de la séparation peut amener la cellule à capter le photon ou non.



Les photons captés sont répartis sur l'écran selon des motifs qui reconstituent les franges d'interférence disparues. Ceci nous montre que, après mesure d'une grandeur, il est parfois possible de changer d'avis et de mesurer la grandeur complémentaire à la condition nécessaire d'oublier le résultat de la mesure première.

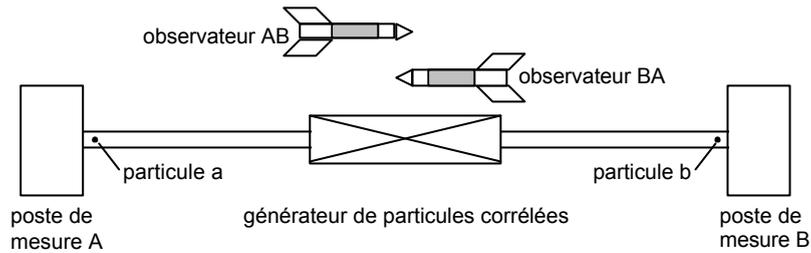
5.9.9 Causalité

Dans nos expériences de mesure non perturbatrice, nous avons dit qu'un atome qui a traversé la cavité reste corrélé avec le photon qu'il y a émis quel que soit la distance qui l'en sépare. Ce phénomène est connu sous le nom de paradoxe EPR [18] et a été mis en évidence expérimentalement[1]. Nous n'entrerons pas dans les détails mais il a été observé que dans un système de 2 particules distantes, le résultat de la mesure effectuée sur l'une est influencé par la nature de la mesure effectuée sur l'autre. Cette influence semble instantanée. Pour autant, on n'est pas en contradiction avec la relativité car cette influence apparemment instantanée au sein du système quantique ne peut être récupérée par deux objets classiques pour communiquer entre eux à une vitesse supérieure à la lumière. Mais, la relativité pourrait avoir un autre mot à dire dans cette histoire[34].

Imaginons 2 postes de mesure A et B contenant 2 particules corrélées a et b et les appareils de mesure associés. Imaginons 2 observateurs se déplaçant à vitesse relativiste :

- le premier entre A et B
- le second entre B et A.

Ils sont tous les deux à mi-chemin.



Le premier observateur verra que la particule b influence la particule a, le second que la particule a influence la particule b. Les causalités seront inversées pour l'un et l'autre des observateurs. La notion de causalité n'apparaît pas absolue mais relative. De par la réversibilité fondamentale des phénomènes, la flèche du temps semble être la seule possibilité de définir cause et effet. Les causes finales ont vécu.

5.9.10 Conclusion

Le lien entre l'irréversibilité quantique et les autres flèches étudiées jusqu'à présent est peu évident à établir, pourtant il semble bien qu'il l'est désormais. La nature de l'irréversibilité est ici la même qu'ailleurs, et due au fait que l'on ne cherche pas à connaître le micro-état de l'environnement du système de mesure, environnement qui contient les informations perdues. On peut donc considérer que la réduction de fonction d'onde pourrait être rendue réversible à condition de prendre a minima en compte l'entropie informatique de l'appareil de mesure considéré comme système de traitement de l'information, entropie elle-même liée à celle que le calculateur rejettera dans l'environnement.

Un processus de mesure quantique est donc un processus comme un autre, si l'on était capable d'inverser conditions initiales et finales le phénomène de réduction pourrait se dérouler à l'envers. Outre le fait que la probabilité associée est très faible, ce déroulement à l'envers ne pourrait s'effectuer qu'au prix d'un effacement des résultats de mesure. Il y a une raison bien simple pour laquelle la réduction de fonction d'onde nous paraît irréversible, c'est que si elle se déroulait à l'envers, elle effacerait toute connaissance que l'on a pu avoir du phénomène direct.

Reprenons l'exemple du lancer de dés dont nous avons parlé en présentant les inégalités de Bayes. Nous nous sommes posés la question de savoir ce que pourrait signifier une probabilité supérieure à 1, notamment une probabilité égale à 6. En fonctionnant à l'envers, c'est à dire en partant d'un double six pour en obtenir un simple par "déjet" d'un dé, le nombre 6 représente le nombre de configurations dont on a pu partir pour aboutir au simple 6, si l'on considère que le "déjet" d'un dé implique le fait d'oublier quelle était sa valeur.

En d'autres termes, 6 représente le nombre de configurations initiales possibles sur le nombre de configurations finales obtenues, compte tenu du fait que l'on a perdu de l'information entre temps. En d'autres termes, on a remplacé un niveau de probabilité par un niveau de certitude. Peut-être une nouvelle branche des statistiques, incluant non seulement l'acquisition de données mais aussi leur oubli, pourrait-elle apporter des éclairages nouveaux sur la réduction de fonction d'onde ainsi que sur la thermodynamique.

5.10 Flèche microscopique

5.10.1 Symétries discrètes

Dans les années 40, On considèrait en physique 3 symétries discrètes fondamentales[21].

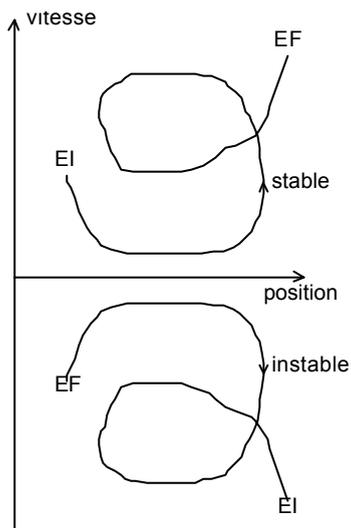
- P ou symétrie de parité, par qui l'Univers serait le même après interversion de la gauche et de la droite.
- C ou symétrie de charge, qui prétend qu'un échange des charges + et - serait sans effet observable.
- T ou symétrie temporelle, affirmant que rien ne change quand on intervertit passé et futur.

La symétrie P signifie que la gauche et la droite n'ont pas d'existence intrinsèque. Chacune n'existe que par opposition à l'autre. Une conséquence de cela est qu'il serait impossible d'indiquer par radio à des habitants d'une planète lointaine que nous avons le coeur à gauche et le foie à droite. Nous pourrions seulement leur signifier que tous les hommes ont le coeur d'un même côté et le foie de l'autre.

La symétrie C signifie que le positif et le négatif n'existent de même que par opposition l'un à l'autre. Les notions de pôle nord et sud magnétiques découlent directement de celles de charges électriques et ne sont pas davantage absolues.

Quant à T, on constate que toutes les lois physiques microscopiques sont réversibles, identiques pour décrire l'évolution d'un système dans le sens du temps ou dans le sens inverse. L'irréversibilité n'est pas dans les lois mais dans les conditions aux limites. Ce sont elles qui font émerger l'irréversible du réversible. C'est la nature de ce passage du réversible microscopique à l'irréversible macroscopique qui a longtemps été la seule base des réflexions sur la nature du temps.

Remarquons notamment que dans l'espace des phases, pour tout point caractérisant un état devant évoluer normalement dans le sens de l'entropie croissante, il existe un point destiné à évoluer dans le sens opposé. Il s'agit du point correspondant aux mêmes coordonnées spatiales des particules, et à des vitesses exactement opposées. Autrement dit, le volume de l'espace des phases occupé par des configurations devant évoluer à contre temps est égal à celui occupé par les configurations plus orthodoxes. Mais au sein de l'espace des phases, certaines places sont plus chères que d'autres. Notamment, alors que les trajectoires allant dans le sens du temps ont des chances de présenter un certain niveau de stabilité (un point initial légèrement différent amènera à des configurations finales voisines) ces chances sont sûrement plus minces pour les trajectoires inverses qui se comporte de manière cahotique (le moindre écart dans le point de départ amène des configurations très différentes à l'arrivée).



5.10.2 Violation des symétries

Coup de théâtre fin des années 50. La physique s'intéresse depuis peu à une force de la nature jusque là ignorée, l'interaction faible, responsable de certains phénomènes de radioactivité. Cette force intervient dans la désintégration d'une particule, le méson K. Comme toute particule, elle est caractérisée entre autres par sa parité, qui doit être globalement conservée dans les produits de désintégration. Oui mais voilà. La particule peut se désintégrer soit en 2, soit en 3 mésons π . La parité n'étant pas la même dans les 2 cas, celle du méson ne serait de fait pas conservée dans l'un ou l'autre cas. Ceci bien sûr dans l'hypothèse où il n'existe qu'un seul méson K, ce qui n'était pas à l'époque établi. 2 physiciens, Yang et Lee, imaginèrent des expériences pouvant trancher la question de la conservation de parité. L'une de ces expériences fut tentée par une physicienne, Mme Wu (Yang, Lee, Wu, tout ce beau monde est bien entendu californien) et apporta une réponse nette : un électron a plus de chance d'être éjectée du pôle sud que du pôle nord d'un atome de cobalt 60. Vu dans un miroir, l'expérience montrerait les électrons s'éjectant préférentiellement du pôle nord (le nord et le sud s'inversent dans un miroir, mais pas le + et le -). Il y a donc une distinction absolue entre la gauche et la droite.

Il semble donc possible de communiquer à une planète lointaine que nous avons le coeur à gauche. Il suffirait de décrire l'expérience de Mme Wu, de définir ainsi les pôles nord et sud magnétiques, et de décrire ensuite une expérience relative au comportement d'un aimant face à un courant électrique. Le déplacement du conducteur permettrait de distinguer la gauche de la droite... à condition que les extraterrestres travaillent avec les mêmes électrons que nous. Si nous communiquons avec un monde d'antimatière, les informations que nous leur envoyons les guideront vers des notions de gauche et de droite erronées. Il semble donc que si la seule symétrie P est violée, par contre, la conjugaison des symétries C et P est conservée. Autrement dit, si l'on inverse simultanément la gauche et la droite d'une part, le + et le - de l'autre, on obtient un monde impossible à discerner de celui dont on est parti. C'est d'ailleurs ce que l'on pensait au début des années 60.

Nouveau coup de théâtre en 1964. On s'intéresse de nouveau aux mésons K mais cette fois en se préoccupant de leur charge, ainsi que de celles des produits de désintégration. Fitch et Conin montrent que le K neutre peut se désintégrer en 2 mésons π de charge opposée. Lorsque cela survient, il n'y a pas conservation de CP.

5.10.3 Conséquence sur le temps

Les conséquences sont considérables. En effet, les théories actuelles rendent obligatoire la conservation de la conjugaison globale PCT. Autrement dit, en effectuant simultanément les 3 opérations de symétrie, on aboutit à des phénomènes physiques répondant aux mêmes lois physiques que celles du système de départ. Comme la symétrie CP est violée, pour rétablir l'équilibre global, il faut que la symétrie T ne soit pas conservée.

Il y aurait donc une distinction absolue entre passé et avenir à l'échelle fondamentale. L'un ne pourrait se déduire simplement par opposition à l'autre. Le problème est qu'aucune autre définition du temps ne semble découler de la violation du CP.

Noter que la violation directe de la symétrie T n'a jamais pu être mise en évidence directement. Les efforts expérimentaux actuels concluent que cette violation est inférieure à 1% dans le cas de l'interaction faible[32][37]. Aucune violation d'une quelconque des 3 symétries n'a encore été mise en évidence pour les autres forces fondamentales de l'Univers.

Le phénomène de violation de symétrie est actuellement un des plus grands mystères de la mécanique quantique, sans doute beaucoup plus que l'existence d'états superposés ou celle de corrélations entre particules distantes du type paradoxe EPR.

L'existence d'une violation de symétrie fondamentale vient jouer les troubles faits, surtout parce qu'elle semble n'avoir aucun rapport avec les autres phénomènes marqués par la flèche du temps. Il semble opportun de chercher ce rapport s'il existe. Pour cela l'informatique semble encore pouvoir jouer un rôle majeur.

5.10.4 Intervention de modèles informatiques

La première idée d'apport de l'informatique pourrait résider dans les modèles d'automates cellulaires, par lesquels on essaie depuis un certain temps de faire émerger des lois de la physique pour leur trouver une base plus fondamentale[50].

On rappelle qu'un automate cellulaire est un modèle du monde physique dans lequel l'espace est rempli par un maillage rectangulaire régulier, chaque noeud du maillage est occupé par un automate qui s'informe de l'état dans lequel se trouvent les automates voisins et qui, en fonction de cela, modifiera son propre état au top d'horloge suivant. Un des exemples les plus connus d'automates cellulaires est le modèle du jeu de la vie. On dispose de cases sur lesquelles se trouvent des pions. A l'étape suivante, des pions seront enlevés ou rajoutés sur chaque case en fonction du nombre de pions situés sur les cases adjacentes.

La théorie des automates cellulaires ne sera pas détaillée mais certains points pourraient nous intéresser, notamment les problèmes de réversibilité et de localité dans ces modèles, problèmes déjà très étudiés. Ici, il nous intéresse de savoir si la violation des symétries discrètes fondamentales peut trouver un modèle qui lui soit équivalent. L'état de l'art sur la question peut être résumé dans un courrier

électronique échangé avec M. Bruno Durand, de l'Ecole Normale Supérieure de Lyon, courrier reproduit intégralement ici.

suite à notre rencontre au Zimm, voici ma question.

Il existe plusieurs façons de définir la flèche du temps, entre autres :

- le sens de l'entropie thermodynamique croissante
- la réduction irréversible de fonction d'onde
- la violation de symétrie temporelle à l'échelon fondamental

Il se pourrait que la réduction de fonction d'onde puisse être plongée dans une opération réversible en prenant en compte l'entropie informelle du système de mesure considéré comme outil de traitement d'information. Par contre, la violation de symétrie temporelle \mathcal{T} semble avoir un statut à part. Elle est liée à la violation de symétrie de parité \mathcal{P} (la gauche n'est pas équivalente à la droite).

Est-on réfléchi, notamment dans les modèles d'automates cellulaires, à la possibilité de faire émerger la violation de symétrie \mathcal{P} de données plus fondamentales ?

Cher Pierre Boud.

Je suis presque sûr que non n'a été fait sur le sujet. Je vous demanderai à d'autres gens lors d'une conférence la semaine prochaine et vous tiendrai au courant si j'ai du nouveau. Je pense que vous pouvez vous pencher sur le sujet, vous serez forcément original. Cependant ça risque d'être assez dur.

Vous pouvez avoir une idée de ce qui a été fait comme simulation sur Masac sur Netscape (<http://www.santafe.edu/~horng>). Faites vous aider par quelqu'un du Zimm si vous ne connaissez pas. Tous les théoriciens devraient savoir comment cela se manipule. DE toute façon, il y a un peu de tout sur ce sujet, quelques succès, quelques fois moins succès.

Tenez-moi au courant si vous faites quelque chose

Bon courage

5.10.5 Apport des autres modèles

Depuis l'échange de ce courrier, la réflexion a légèrement progressé, mais à partir d'un autre modèle, celui de la machine de Turing réversible brownienne. Il s'agissait de partir de l'espoir de pouvoir construire une machine à la fois réversible et comportant un niveau de symétrie tel que, par simple réflexion dans un miroir, on obtienne la machine exécutant la fonction réciproque. L'inversion de l'espace se reflétant d'une certaine façon dans l'inversion du temps. Mais cette approche se heurte à une difficulté majeure.

La réflexion dans un miroir d'une machine de Turing réversible ne donne pas exactement la machine que l'on aurait conçue pour exécuter la fonction inverse. L'exécution directe et inverse est assez différente.

- Dans l'exécution directe, la valeur du bit est lue puis les opérations correspondantes de changement de valeur et de déplacement sont effectuées.
- Dans l'exécution inverse, on effectue d'abord les opérations de changement de valeur et de déplacement, puis on vérifie que la valeur de bit est compatible avec le travail effectué.

Or les opérations de changement de valeur et déplacement d'une part, de lecture d'autre part, ne sont pas les symétries temporelles l'une de l'autre. Peut-il en être autrement ?

Il y a donc une dissymétrie fondamentale. Mais l'important est que le système formel ne peut pas accéder à cette dissymétrie. Aucun programme ne peut savoir dans quel sens s'effectue son exécution.

Car du point de vue du programme, la machine reste bien parfaitement réversible. La dissymétrie ne se trouve pas dans le programme.

Le fond de la violation du CP est d'affirmer le contraire, et de dire que le programme peut savoir dans quel sens il s'exécute...

5.10.6 Conclusion

La flèche du temps microscopique est sans doute celle qui reste le plus à étudier. Il est raisonnable de penser que les modèles informatiques peuvent apporter leur contribution à la compréhension du problème. Si l'on peut concevoir de récupérer les résultats des études de réversibilité déjà entrepris pour les modèles d'automates cellulaires, il est également envisageable que d'autres modèles informatiques puissent donner leur apport.

5.11 Le temps en tant que grandeur fondamentale

5.11.1 Le temps tel qu'en lui-même

Les différentes flèches du temps précédemment étudiées n'ont pas empêché certains de considérer le temps comme étant une donnée fondamentale, dont l'existence se situe en amont de toutes les flèches étudiées jusqu'ici.

5.11.2 Systèmes dissipatifs

Comment faire émerger la flèche du temps des lois symétriques de la Nature ? La science des structures dissipatives (structures hors de l'équilibre) peut apporter un élément de réponse dans la mesure où elle fait apparaître des tendances à l'auto-organisation dans des systèmes censés évoluer vers le désordre. Certaines propriétés des systèmes loin de l'équilibre et cherchant donc à en trouver un font intervenir une dissymétrie temporelle qui ne semble pas pouvoir émerger d'approximations sur des lois réversibles, comme le fait l'entropie.

L'idée de base est de donner à la notion fondamentale de trajectoire, apparemment déterministe, une nature fondamentalement probabiliste. Dès lors la flèche du temps statistique se retrouve également être une flèche fondamentale. Pour cela il convient de modifier et compléter les théories de la dynamique tant classiques que quantiques.

5.11.3 Evolution des systèmes

Lorsque l'on essaye de décrire l'évolution d'un système deux approches sont possibles:

- l'approche déterministe, s'efforçant de décrire la trajectoire du point qui définit le système au sein de l'espace des phases. Cela nécessite une connaissance de la position du système avec une précision infinie. Dans le cas de systèmes instables où des points voisins de l'espace des phases aboutissent à des évolutions très divergentes l'approche est irréaliste.
- l'approche probabiliste, cherchant à décrire l'évolution de la distribution de probabilités associées à la présence du point au sein de l'espace des phases.

Ces deux approches peuvent se déduire l'une de l'autre pour des systèmes très simples. Mais dès qu'interviennent des interactions entre composantes du système, l'approche déterministe aboutit à des systèmes non intégrables alors que l'approche probabiliste reste possible. Elle est de fait utilisée pour les systèmes caotiques dans lesquels les interactions créent des résonances entre les degrés de liberté du système.

Pour éclaircir cela, définissons un système à partir de l'opérateur liant l'état du système à l'état précédent. Cet opérateur est entièrement défini par ses valeurs propres et ses vecteurs propres. Tant que les vecteurs propres représentent des termes normaux, réguliers, intégrables, il y a équivalence entre la distribution de probabilité obtenue et le comportement décrit en termes de trajectoires. Notamment, dans le cas d'une particule isolée, la trajectoire est retrouvée au point où les interférences entre les différentes ondes planes décrites par la famille des vecteurs propres sont constructives. La trajectoire n'est plus élémentaire dans cette approche mais déduite de l'étude des domaines de probabilité.

Mais il peut arriver que les vecteurs propres ne correspondent pas tous à des fonctions normales (comme la fonction de Dirac dont seul le produit avec une fonction normale donne une fonction normale).

Nous avons alors un spectre régulier, et un spectre singulier. Le vecteur propre n'est alors plus décrit dans l'espace de Hilbert. Cette situation peut notamment être induite par l'existence d'interactions persistantes, associées à des probabilités délocalisées, alors que les interactions transitoires sont associées à des probabilités localisées. Lorsque l'on cherche à intégrer, le spectre singulier peut faire apparaître des termes divergents vers le passé et amortis vers le futur, et introduire ainsi une brisure dans la symétrie temporelle qui n'apparaît pas dans l'étude newtonnienne des trajectoires.

En mécanique quantique, la nécessité de sortir de l'espace de Hilbert et de retrouver des solutions dissymétriques par rapport au temps résulte de l'existence de parties continues dans le spectre de vecteurs propres, liées notamment à l'existence de champs. La dissymétrie temporelle émerge ainsi malgré le caractère réversible de l'équation de Schrödinger. Une telle approche, selon leurs défenseurs, arrive à reconstruire le phénomène de réduction de fonction d'onde propre à la flèche du temps quantique. L'élimination des solutions à « ondes avancées » dans les phénomènes radiatifs s'obtient pareillement. Des simulations informatiques semblent confirmer ces affirmations. Nous nous interrogerons sur la validité de la simulation informatique qui semble avoir été très employée pour étayer le modèle présenté ici.

5.11.4 Temps et temps

En fait le temps ici n'est pas introduit au sein des lois de la physique mais en amont de ces lois, comme un principe de base. En conséquence directe, l'irréversibilité ne doit pas exister dans la formulation des lois fondamentales de la physique, car elle n'est qu'héritée d'une loi encore plus fondamentale dont elles constituent une surcouche. Chaque loi réintroduirait une flèche du temps distincte s'il n'en était ainsi. Les lois de la physique doivent donc être fondamentalement symétriques en elles-mêmes. Le caractère symétrique peut donc être un critère de validité pour une loi qui ne fait pas intervenir la loi probabiliste fondatrice de la dissymétrie temporelle. En cherchant l'irréversibilité partout, on l'a peut être chassée de partout.

Pourtant, l'entropie semble pouvoir faire émerger la flèche du temps de la symétrie des lois physiques. Ceci sans prendre en compte les mécanismes nouveaux proposés par Prigogine. Qu'est-ce qui fait mourir cette première flèche dans l'approche de Prigogine ? Ne risque-t-on pas d'introduire une double flèche du temps ? Il est nécessaire de faire que l'une des émergences se déduise de l'autre. En fait l'un comme l'autre font émerger le temps d'une même matière première: l'incertitude. Mais elle intervient à des niveaux différents. Celle-ci est une brique fondamentale pour Prigogine. Elle est indissolublement liée à l'observation pour les interprétations faisant intervenir l'entropie classique. La notion de trajectoire est inexistante pour Prigogine, et inaccessible pour les tenants de l'entropie. Dans les deux cas, les lois de la statistique permettent néanmoins de connaître des valeurs probabilistes sur l'évolution des systèmes. L'approche proposée par Prigogine signifie que les interactions persistantes sont « dissipatives » plutôt que « concentratives ». Pourquoi ? N'est-ce pas simplement parce qu'il existe davantage de moyens de dissiper que de concentrer ? N'est-ce pas toujours le hasard qui mène le jeu ?

Il a été envisagé que la réduction de fonction d'onde intervenait du fait de la relation avec l'environnement, notamment celui induit par l'appareil de mesure, ici on considère que l'appareil de mesure amène le système à briser la symétrie temporelle de par les interactions qu'il induit. Il a été dit également que le temps était perçu à la condition que la flèche entropique de nos cerveaux soit la même que celle du milieu. Ici on considère que la mesure n'est possible que si l'appareil de mesure brise la symétrie temporelle de la même façon que le système mesuré le fait, et qu'ils partagent une même flèche du temps. Avec des approches différentes, on retrouve des points assez semblables, notamment sur l'importance de l'introduction des lois de probabilité. Et un problème reste toujours en suspens : celui de la violation du CP, qui semble toujours vouloir faire bande à part dans les différentes définitions possibles du temps.

5.11.5 Temps et simulation. des origines à nos jours.

L'existence du temps a-t-elle précédé celle de l'Univers ? Que signifierait d'ailleurs sans cela le terme « précéder » ? Les philosophes anciens avançaient déjà que le temps n'existait pas sans phénomène pour le mesurer ou le constater, donc il n'existe pas sans la matière. Mais plus fondamentalement la question n'est peut-être pas une question physique puisque la flèche du temps est incluse dans l'outil scientifique lui-même par le biais de la flèche mathématique, et que sans cela aucune formulation physique ne nous est accessible. Pour les mêmes raisons les simulations informatiques ne sont que

moyennement satisfaisantes dans la mesure où l'outil de calcul est marqué par la flèche du temps. Dans un cas comme dans l'autre il s'agit d'étudier un temps à l'aide d'un autre temps, un « méta temps » qui n'est pas expliqué lui-même. On retrouve la notion d' « ensemble d'ensembles » qui chez Gödel a donné naissance au théorème d'incomplétude. De manière inavouée, le temps est donc posé comme existant au départ, assujéti à des lois mais n'en émergeant pas. Le temps émerge d'un « méta-temps » d'existence admise.

5.12 Conclusion sur le temps

L'approche que nous avons proposée ici n'a pas eu pour ambition d'expliquer le temps, car il existe déjà dans les outils que l'on prétend pouvoir utiliser pour cela, et nous fait rentrer de fait dans les problèmes de l'auto-référence. Il s'est agi simplement ici de réfléchir sur les moyens de supprimer les incohérences pouvant exister entre divers phénomènes fondamentalement marqués par le temps, en préjugant que l'information, qui est sans doute la donnée la plus fondamentale de la science, pouvait, étudiée en tant que telle, aider à éclaircir certaines notions. Cette approche semble avoir été fructueuse sur plusieurs points :

- les phénomènes d'irréversibilité peuvent pour l'essentiel s'expliquer sans faire appel à une dissymétrie fondamentale des lois physiques,
- ces divers phénomènes semblent en fait la manifestation sous diverses formes d'un seul et même, induit par le caractère statistique des comportements lui-même induit par une perte de l'information relative à une connaissance incomplète, à un niveau ou un autre du micro-état d'un système.

Des flèches du temps étudiées jusqu'à présent, la plupart semble n'être que le reflet dans la physique des inégalités de Bayes. Cela semble vrai également pour les phénomènes quantiques de réduction de fonction d'onde. L'asymétrie des lois de la statistique est-elle la clé de tout ? D'où vient cette asymétrie ? Que pourrait réellement signifier une probabilité supérieure à 1 ?

Sur ce dernier point une suggestion a été faite, celle de considérer qu'une telle probabilité s'appliquerait au nombre d'états initiaux possibles compatibles avec un état final, compte tenu que les traces de l'état initial disparaissent jusque dans nos mémoires. Un tel concept est peut-être encore à affiner, son intérêt à étudier. Apporterait-elle un éclairage nouveau sur la dissymétrie temporelle ?

Reste la dissymétrie fondamentale de l'axe du temps mis en évidence dans la violation du CP. Le problème n'est pas tant qu'une telle dissymétrie existe, mais le fait qu'elle ne se relie pas aux autres manifestations de l'existence du temps. Quel est son rôle véritable ? Doit-on se résoudre à avoir deux définitions distinctes de la flèche du temps ?

Les différents aspects évoqués sont-ils bien là pour dire que le temps n'est qu'une illusion, comme le dira Einstein ? Le débat est-il clos ?

Bien d'autres questions n'ont pas été abordées dans le cadre de cette étude. Peut-on concevoir des modèles où le temps aurait plusieurs dimensions ? Le modèle d'Everett n'en est-il pas déjà un (noter que la pluridimensionnalité temporelle est proposée dans la théorie des supercordes qui cherche à expliquer globalement toutes les lois de la physique) ? Qu'en est-il des violations de la causalité que semblent mettre en évidence la théorie de la relativité [41] ?

Cela fait bien d'autres sujets d'étude pour lesquels les théories de l'information pourraient aussi jouer leur rôle. Car avant que la matière soit constituée de quarks et de photons, elle est constituée d'objets communicants. La nature de ces objets nous importe, mais les phénomènes qui peuvent régir les échanges d'information entre eux sont omniprésents.

Ainsi on se souvient du paradoxe des jumeaux, présent dans les équations de la relativité restreinte, et qui veut qu'un voyageur effectuant à grande vitesse un aller-retour sur une planète lointaine vieillisse moins vite qu'une personne restée à terre. Pour expliquer ce qui se passe, Langevin, qui a découvert ce paradoxe, l'a expliqué en imaginant ce qui se produirait sur un canal de communication reliant les 2 personnages durant tout le parcours. Aujourd'hui, certains pensent avoir réussi à faire émerger la relativité restreinte de données plus fondamentales mises en évidence dans les modèles d'automates cellulaires.

A l'avenir, le temps devra compter avec l'information.

6. Applications

6.1 Preuve d'algorithme

6.1.1 objectif

L'ensemble des discussions développées ici semblent être un pur jeu de l'esprit, ce qui n'est d'ailleurs déjà pas si mal. La suite de ce discours a pour objet de montrer qu'il n'est pas exclu de trouver des applications. Ici nous allons envisager l'exemple de la preuve d'algorithme. L'idée est de dire que puisqu'un calcul réversible est possible, il revient au même de prouver un algorithme qu'il fonctionne à l'endroit ou qu'il fonctionne à l'envers. En réécrivant certains algorithmes de manière réversible et en raisonnant sur l'exécution inverse on peut notablement simplifier certaines preuves.

6.1.2 terminologie

Nous avons vu qu'il est toujours possible de "plonger" un algorithme irréversible dans un algorithme réversible à condition de générer un déchet. Cet algorithme va pour nous se présenter sous deux formes :

- la procédure, algorithme normal, qui essaie de calculer un résultat à partir de données,
- ce que nous appellerons la récédure, et qui a pour fonction de retrouver les données à partir du résultat.

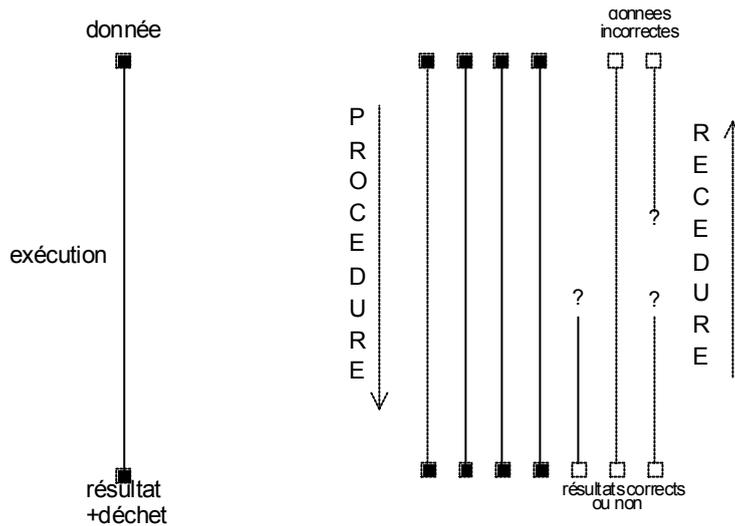
Afin d'éviter les confusions, les termes de données et résultats que nous emploierons à présent se rapporteront toujours à la procédure. Un résultat est donc calculé par une procédure et fourni à une récédure. Une donnée est fournie à la procédure et calculée par la récédure.

6.1.3 Principe

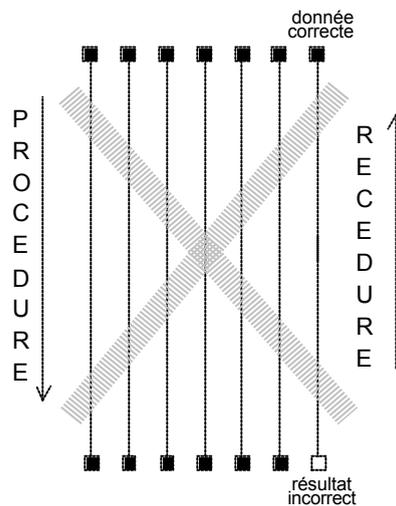
L'idée est de considérer que toute exécution finie de la procédure a pour image une exécution également finie de la récédure. Il est donc envisageable de récupérer une preuve de la récédure pour prouver la procédure, en partant de l'idée que toute exécution de l'algorithme non prouvé est le reflet d'une exécution de l'algorithme prouvé.

Précisons bien. Il ne suffit pas de prouver la récédure. Il faut montrer que cette preuve est liée au fait que la procédure remplit correctement son rôle. En d'autres termes, la récédure, si elle se termine, génère un jeu de données correct à la condition qu'on lui ait fourni un résultat correct, et uniquement dans ce cas. Ce doit être une condition nécessaire. Dès lors, la récédure étant prouvée, la procédure peut dès lors être considérée comme telle.

Le schéma ci-dessous résume toutes les situations que l'on peut rencontrer avec un algorithme correct. On voit que, dans la mesure où l'on ne demande pas à une procédure d'accéder à toutes les solutions possibles, certaines de ces solutions ne sont pas nécessairement connectées à des jeux de données corrects.



Le seul cas à exclure est présenté ci-dessous. Dès lors qu'un seul résultat incorrect peut donner un jeu de données correct après exécution de la récédure, l'algorithme est faux.



On voit donc que cette approche fonctionne dans les deux sens (!), et peut démontrer la justesse comme la fausseté d'une procédure.

6.1.4 Schéma de preuve

Le schéma de preuve global est le suivant.

1. réécrire la procédure de manière réversible (avec génération de déchet au besoin).
2. En ce qui concerne la procédure, montrer simplement qu'elle se termine dès lors que le jeu de données est correct.
3. Eventuellement il est permis de démontrer certaines propriétés des résultats générés.
4. Ecrire la récédure associée. Cela implique le respect de règles permettant de garantir l'obtention d'un algorithme équivalent à l'inverse temporel de l'autre.
5. Prouver la récédure. Elle doit bien arriver à retrouver des données correctes pour la procédure à partir de résultats de cette dernière. La preuve de la récédure peut être plus facile que celle de la

récedure, dans la mesure où certains invariants de procédure peuvent nécessiter la connaissance de l'avenir ... difficile quand celui-ci est incertain (examen de toutes les éventualités). La preuve peut se limiter aux cas où les résultats fournis à la récédure présentent les propriétés démontrés éventuellement en 3.

- 6. Mettre en évidence le fait que la récédure n'aboutit que si les résultats qu'on lui a fournis possèdent la propriété à démontrer, celle qu'est censé donner la procédure à ses résultats. Cela doit être une condition nécessaire.

6.1.5 Réécriture et écriture

6.1.5.1 Impératifs d'écriture

L'écriture d'une récédure nécessite au préalable la réécriture de la procédure sous forme réversible, c'est à dire sous une forme qui n'efface jamais de valeurs et n'effectue jamais de branchements avec perte de l'origine. Le premier point concerne la réécriture des instructions. Le second, celui des structures de contrôle. Les algorithmes réécrits sont normalement plus complexes que l'algorithme original. Il s'agit donc de savoir si la complexité ainsi surajoutée peut être compensée par la simplification espérée de la preuve.

6.1.5.2 Instructions

L'instruction

$$x = A$$

mettant en jeu une variable x et une expression A où x est absente, rend une procédure irréversible dans la mesure où elle permet d'effacer la dernière trace d'une valeur significative, impossible à redéfinir à coup sûr lors d'une exécution inverse. Par contre, l'instruction

$$x = x + A$$

est réversible. Dans une récédure elle sera remplacée par $x = x - A$. Si l'on remplace la variable x par une pile, l'opération

$$X.\text{Empile}(A)$$

peut être utilisé comme un équivalent réversible de l'affectation, l'opération inverse étant le dépileage. Mais le contenu de la pile à l'arrivée de la procédure devra faire partie des hypothèses de départ de la récédure. Il est un constituant du déchet.

En résumé les écritures des instructions des procédures et récédures à partir de l'algorithme original suivent les principales règles suivantes :

algorithme	procédure	récédure
$x = A$	$X.\text{Empile}(A)$	$X.\text{Dépile}(A)$
$x = x + A$	$x = x + A$	$x = x - A$
$x = x - A$	$x = x - A$	$x = x + A$
$x = x * A$	$x = x * A$	$x = x / A$
$x = x / A$	$x = x / A$	$x = x * A$

6.1.5.3 structures

Un bloc d'instruction S de la procédure sera remplacé dans la récédure par un bloc S^{-1} comprenant les instructions réciproques et dans l'ordre inverse. Le remplacement des structures sera la principale source de complexification des algorithmes. Mais dans certains cas, des structures simples pourront être l'équivalent de structures plus complexes. Quelques exemples de remplacement de structures.

Dans les exemples ci-dessous les instructions entre accolades {} peuvent correspondre à un ensemble d'instructions équivalentes. Les intructions entre parenthèses () correspondent à des tests qui doivent être vrais pour que la suite du programme s'exécute.

structure	procédure	récedure
boucle	{variable test ← état initial} Tant que variable test ≠ état final S Fin tant que	{variable test ← état final} répéter S ⁻¹ jusqu'à variable test = état initial
choix multiple dans le cas général La réversibilité rend utile l'adjonction d'une variable mémorisant le résultat du test rendu vrai. La programmation structurée permettrait de s'en passer mais pas simplement. La valeur de la variable ajoutée fera partie du déchet accompagnant le résultat.	Si test 1 vrai Alors SA variable = valeur 1 Sinon si test 2 vrai alors SB variable = valeur 2 : : Sinon SX Fin si	Si variable = valeur 1 alors SA ⁻¹ (test 1 vrai) Sinon si variable = valeur 2 alors SB ⁻¹ (test 2 vrai) : : Sinon SX ¹ Fin si
choix multiple, cas particulier si les résultats des tests ne sont pas modifiables par un bloc instruction, une structure équivalente sans variable déchet pourra être obtenu	Si test 1 vrai Alors SA Sinon si test 2 vrai alors SB : : Sinon SX Fin si	Si test 1 vrai Alors SA ⁻¹ Sinon si test 2 vrai Alors SB ⁻¹ : : Sinon SX ¹ Fin si
alternative Cas particulier du choix, elle nous montre un moyen d'éliminer la variable de déchet.	Si test vrai Alors SA Sinon SB Fin si	SB ⁻¹ Si test vrai alors SB SA ⁻¹ (test vrai)

6.1.6 Piège à éviter

Tout s'appuie sur le fait que procédure et récedure sont un même algorithme qui bénéficie d'une symétrie de l'axe des temps. De fait, ce qui est prouvé pour l'un peut être considéré comme hypothèse pour l'autre. Mais si un tel va-et-vient est permis, il s'agit de bien séquencer les opérations. A chaque instant, la démonstration d'une propriété ne doit s'appuyer que sur ce qui a été démontré antérieurement. Cela semble une évidence mais le fait de travailler sur 2 types d'exécution à la fois, dont l'une ne suit pas le sens normal de la causalité peut mener à des confusions.

6.2 Exemple

6.2.1 Algorithmes de choix

L'habitude pour un système physique est d'évoluer vers le désordre, simplement parce que ce dernier peut se manifester sous un plus grand nombre de formes. L'habitude pour une procédure est d'évoluer à l'inverse du monde physique pour retrouver un monde ordonné contenant un niveau d'information réduit à la réponse cherchée. Il s'ensuit que généralement l'exécution d'une procédure est déterministe, menant vers un état unique, alors qu'une exécution inversée de celle-ci serait indéterministe. Ainsi l'exécution d'un tri ne laisse pas de place au hasard. A l'inverse, un algorithme qui mettrait du désordre dans un ensemble de n fiches aurait n! résultats possibles (si l'on admet que l'ordre est un "désordre particulier"). le rôle d'un algorithme est donc souvent d'aller à l'encontre des lois de la nature, et de la tendance naturelle des systèmes physiques au désordre.

Certains algorithmes ne répondent pourtant pas à cette habitude :

- la procédure est non déterministe (existence d'une instruction de type "choisir...")
- la récedure associée est déterministe.

Le fait que la récédure soit déterministe permet d'assurer que la preuve passant par l'approche proposée ici sera probablement plus facile. Ce type d'algorithme est donc le candidat idéal pour monter l'intérêt de l'approche présentée ici.

6.2.2 Rappels sur les graphes

Avant de présenter l'algorithme qui nous servira d'exemple, voici quelques rappels.

On appelle graphe triangulé un graphe dont tous les cycles de longueur ≥ 4 ont une corde. En particulier un arbre est un graphe triangulé... sans cycles.

La propriété est héréditaire. Quand on supprime un sommet à un graphe triangulé, le graphe restant est triangulé.

On appelle sommet simpliciel un sommet dont le voisinage est une clique.

Un ordre d'élimination simpliciel est un ordre d'élimination des sommets tel que à tout moment le sommet éliminé est simpliciel pour le sous graphe restant. Un ordre d'élimination simpliciel est parfait si il inclut tous les sommets du graphe.

Pour un graphe G, les 3 propriétés suivantes sont équivalentes :

- G est triangulé,
- G admet un ordre parfait d'élimination simpliciel,
- tout séparateur minimal de 2 sommets (+ petit sous graphe dont la suppression isole les sommets l'un de l'autre) est une clique.

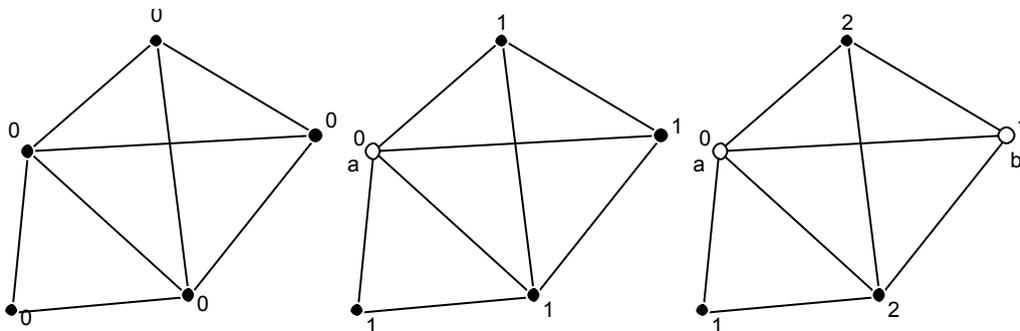
Son objectif est de créer un ordre d'élimination simpliciel dans un graphe triangulé.

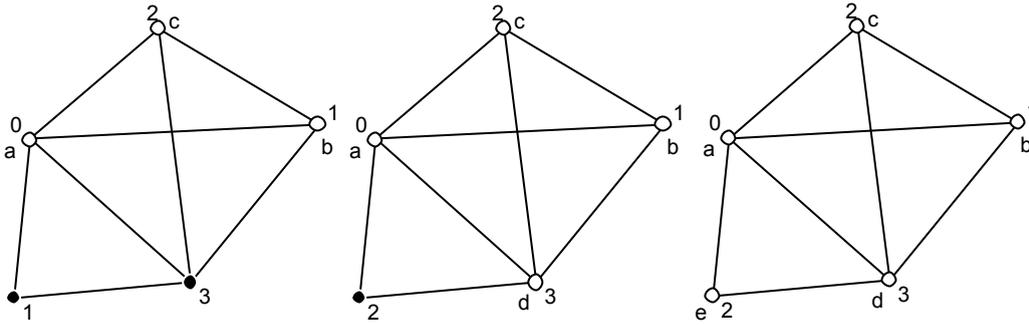
6.2.3 Présentation de MCS

Un représentant type des algorithmes de choix pour présenter notre démarche est l'algorithme Maximal Cardinality Search. Son objectif est de trouver un ordre d'élimination simpliciel parfait pour un graphe triangulé.

- L'algorithme est le suivant :
- au départ associer la marque 0 à tous les sommets,
- choisir un sommet,
- augmenter de 1 la marque de tous les sommets voisins non précédemment choisis,
- choisir l'un des sommets restants de plus grande marque et revenir au point précédent tant qu'il reste des sommets non choisis.

L'ordre inverse des sommets choisis est un ordre d'élimination simpliciel. Voici un exemple d'exécution.





L'ordre inverse des choix (edcba) est un ordre d'élimination simpliciel.

Malgré la simplicité de l'algorithme, les premières tentatives de preuve ont abouti à des constructions très laborieuses et complexes. Nous allons essayer de construire une preuve simple en utilisant la réversibilité.

6.2.4 Preuve par utilisation de la réversibilité

6.2.4.1 Procédure réversible

Essayons d'écrire la procédure MCS de manière réversible.

Données :
un graphe triangulé dont chaque sommet est associé à une marque initialisée à 0.
Résultat :
une pile contenant un ordre d'élimination simpliciel pour le graphe.
Algorithme :
tant qu'il existe des sommets non empilés faire
 choisir un sommet non empilé x de marque maxi
 faire + 1 aux marques des sommets voisins non empilés
 empiler x
fin tant que

6.2.4.2 Terminaison de la procédure

Il est trivial de constater que la procédure se termine car chaque sommet est examiné une et une seule fois. Le sommet à examiner est pris parmi ceux qui ont le plus de voisins déjà empilés. On ne voit pas comment aucun sommet ne pourrait répondre à cette caractéristique.

Au départ la marque d'un sommet est nulle. Celle-ci augmente de 1 à chaque fois qu'un de ses voisins est empilé, et ce jusqu'à ce que le sommet lui-même soit empilé. A tout moment la marque du sommet indique le nombre de voisins empilés avant lui, ceux qui sont en dessous de lui dans la pile.

6.2.4.3 Propriétés des résultats

Le fait que le sommet à examiner soit pris parmi les voisins déjà empilés s'il en existe assure que chaque composante connexe du graphe de départ sera traité en totalité avant de passer à la suivante. Aucune composante connexe ne donnera même passagèrement naissance à deux composantes dans la pile. On verra que ce ne sera pas nécessairement le cas pour le sous graphe dépilé : le sous graphe empilé peut provisoirement en partager une composante connexe en plusieurs parties.

6.2.4.4 Récédure

Voici maintenant la récédure MCS écrite de manière réversible. La signification de la marque, démontrée dans la procédure, est prise comme hypothèse ici.

Données :
une pile contenant un ordre d'élimination simpliciel pour un graphe triangulé.
le graphe triangulé lui-même, chaque sommet est valué par le nombre de voisins qui sont empilés sous lui.
Résultat :
le même graphe dont tous les sommets sont valués à 0
algorithme :
répéter
dépiler le sommet x
faire - 1 aux marques des voisins dépilés de x
(vérifier que x a une marque maxi pour les sommets dépilés)
jusqu'à (pile vide)

Il serait tentant de donner une sémantique à l'algorithme de la récédure. Son objectif serait de vérifier qu'un ordre d'élimination est simpliciel, le fait étant acquis dès lors que l'algorithme se termine. Mais il n'est pas question pour nous de démontrer que la récédure atteint un tel objectif. Ceci pour une raison simple, c'est que rien ne garantit que tous les ordres simpliciels réussiront le test de l'algorithme. Le fait qu'un ordre soit simpliciel doit être une condition nécessaire pour terminer l'algorithme. Si l'on en faisait en outre une condition suffisante, on sous entendrait que tout ordre simpliciel sur un graphe peut être découvert par la procédure, ce qui n'est pas garanti.

6.2.4.5 Preuve de la récédure

Regardons dans le détail la récédure

- *La pile contient un ordre d'élimination simpliciel pour le sous graphe qu'elle contient.*

vrai par hypothèse au départ, reste vrai par héritage après chaque dépilage d'un sommet.

- *La marque d'un sommet correspond au nombre de voisins qui sont en dessous de lui dans la pile (on admet qu'un sommet dépilé est "plus haut" que la tête de pile).*

Vrai par hypothèse au départ. Reste vrai évidemment pour les sommets encore dans la pile puisque tout y est constant. Reste vrai aussi pour les sommets qui sont dépilés puisqu'à chaque dépilage d'un voisin la marque est décrémentée, le nouveau sommet dépilé n'étant plus au dessous.

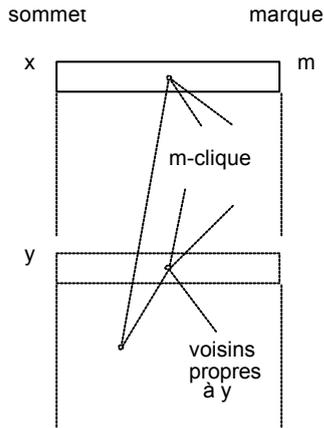
Pour un sommet dépilé la marque est donc égale aux nombre de voisins encore dans la pile. Cet élément garantit la satisfaction de la conclusion : toutes les marques seront strictement nulles une fois la pile vide.

- *Condition imposée par la construction de la récédure : la marque d'un sommet dépilé est maximale pour les sommets déjà dépilés.*

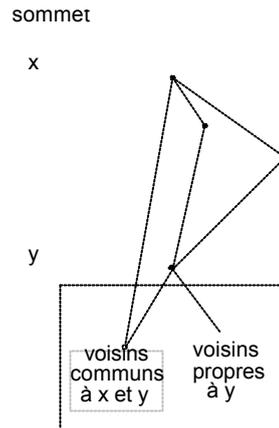
Soit un sommet x de marque m quand il est en tête de la pile. A ce moment, x est simpliciel. Tous ses voisins situés dans la pile forment une m-clique. Soit y l'un de ces voisins. Tous les autres voisins de x sont donc aussi voisins de y par définition d'une clique. Par contre y peut avoir des voisins propres. Lorsque x et y seront dépilés tous deux, à tout moment la pile pourra contenir :

- des voisins communs à x et y
- des voisins propres à y
- mais pas de voisins propres à x.

La marque de y sera donc alors toujours supérieure à celle de x, ou égale si y n'a plus de voisins propres dans la pile. Par transitivité, tout sommet dépilé a une marque supérieure ou égale à celle de tout sommet dépilé avant lui auquel il est relié par un chemin. Au dépilage, un sommet a donc nécessairement la plus grande marque de la composante connexe à laquelle il fait partie dans le sous graphe dépilé



y fait partie de la m-clique à laquelle est reliée x. Tous les voisins de x sont donc aussi voisins de y. Mais y peut avoir des voisins propres.



Lorsque x et y seront dépilés, la pile contiendra des voisins communs à x et y, des voisins propres à y, mais pas de voisins propres à x. La marque de y sera supérieure à celle de x du nombre de sommets propres à y.

Cette condition n'est pas tout à fait celle que l'on souhaite, puisque l'on a demandé une marque supérieure à celle de tous les sommets dépilés. Mais au fait, n'avons nous pas pris une condition trop restrictive au départ ? S'il en était ainsi, récédure et procédure pourraient être réécrits ainsi :

Récédure :

algorithme :

répéter

dépiler le sommet x

faire - 1 aux marques des voisins dépilés de x

(vérifier que la marque de x est maxi dans sa composante connexe du sous graphe dépilé)

jusqu'à (pile vide)

Procédure :

algorithme :

tant qu'il existe des sommets non empilés faire

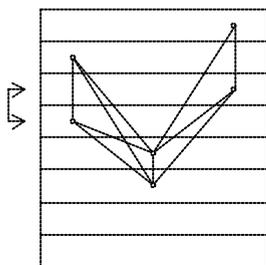
choisir x de marque maxi dans sa composante connexe du sous graphe dépilé

faire + 1 aux marques des sommets voisins non empilés

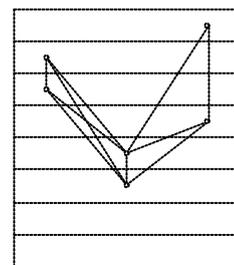
empiler x

fin tant que

l'exemple ci-dessous montre en tous cas que la procédure initiale ne voit pas tout. Il montre que le sous graphe dépilé peut un temps présenter plusieurs composantes connexes pour une composante du graphe complet.



l'ordre empilé est correct mais l'algorithme de départ aurait imposé un ordre inversant les 2 éléments indiqués



L'ordre tel que généré par la procédure initiale. On voit que dès les 2 premiers sommets empilés, le sous graphe dépilé comprend 2 composantes connexes.

6.2.4.6 Conditions de réussite de la récédure

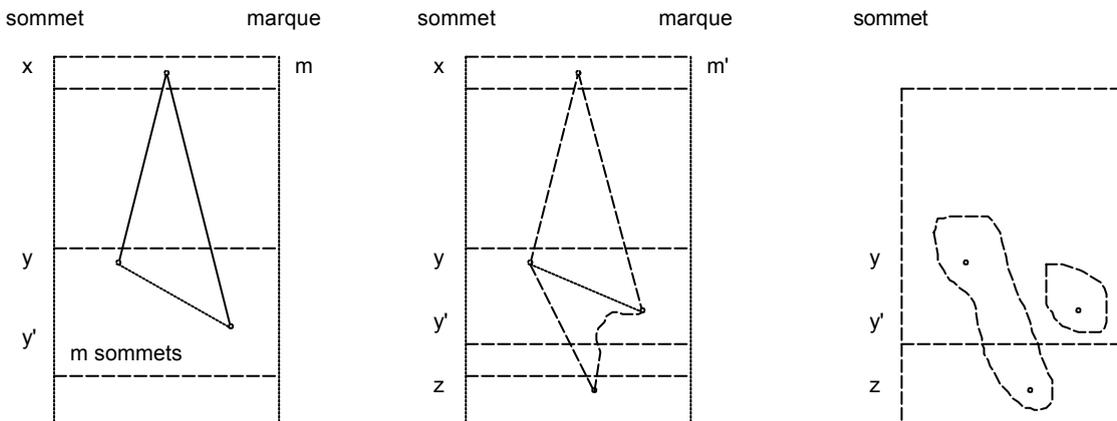
Voyons ce qu'il advient si le contenu de la pile ne représente pas un schéma d'élimination simpliciel d'un graphe triangulé.

Dans ce cas il arrivera un moment où le sommet x de marque m situé en haut de pile ne sera pas relié à une m -clique. Mettons qu'il soit relié à une m -clique à laquelle il manque 1 ou plusieurs arcs... Appelons y et y' les 2 sommets de l'un de ces arcs manquants. Le sommet y est le plus élevé des deux dans la pile.

- Soit y n'est relié à rien d'autre qu'à d'autres sommets de la "clique incomplète",
- Soit y est relié à d'autres sommets.

Dans le premier cas, la marque au défilage de y sera inférieure à celle du sommet x , et l'exécution sera rejetée par le test. Dans le cas où y est relié à d'autres sommets, prenons z l'un de ces sommets.

- S'il en existe, tout cycle $y'x y z \dots y'$ est de longueur ≥ 4 , la corde $x z$ n'existant pas (z n'est pas l'un des m voisins de x , sinon on revient au cas précédent), la corde $y y'$ n'existant pas non plus, et le chemin $z y'$ ayant nécessairement une longueur supérieure à l'unité. Donc le graphe n'est pas triangulé. On est contraire aux hypothèses.
- Si un tel cycle n'existe pas, $y'xyz$ est le seul chemin reliant y' et z . Quand x sera défilé y' et z seront dans 2 composantes connexes distinctes du sous graphe empilé. On a vu dans les propriétés des résultats de la procédure que l'ordre d'élimination généré par cette dernière était tel qu'aucune composante connexe ne peut donner même passagèrement naissance à deux composantes distinctes dans la pile. La situation présentée ici ne pouvant être générée par la procédure, elle n'a pas à être examinée pour la récédure.



L'arc yy' manque. Si y n'est relié à aucun autre sommet que les voisins de x , sa marque au défilage sera inférieure à celle de x

Si y est relié à un autre sommet z , le cycle $xyzy'x$ s'il existe est de longueur ≥ 4

Si aucun chemin zy' n'existe, le graphe contenu dans la pile sera constitué de 2 composantes connexes, une contenant y et z , l'autre contenant y'

6.2.5 Conclusion

Toute exécution correcte de la procédure est l'inverse d'une exécution correcte de la récédure. Comme l'exécution de cette dernière n'est correcte que si la procédure atteint son objectif (création d'un ordre d'élimination simpliciel), on montre donc que la procédure construit effectivement un tel ordre.

6.3 Conclusion sur l'approche

Il peut sembler choquant de travailler simultanément sur 2 algorithmes en considérant que ce qui est prouvé pour l'un peut être considéré comme admis pour l'autre. Pourtant la cohérence de l'ensemble est conservée. Il ne s'agit pas vraiment de 2 algorithmes mais du même. Seule la flèche du temps est modifiée. Or celle-ci n'a pas d'importance. Le regard physique sur la réversibilité permet de s'en convaincre.

La preuve d'algorithme n'est présentée ici que comme un exemple d'applications possibles de l'étude de la réversibilité dans les systèmes de calcul. L'approche peut être affinée notamment en rendant plus strictes les règles de construction des récédures à partir des procédures. L'algorithme MCS semblait idéalement conçu pour démontrer l'intérêt de cette approche car l'écriture des procédures et récédures associées est facile.

L'approche proposée peut être la base d'une nouvelle manière de concevoir un algorithme de type :

construire X

On peut commencer par écrire :

détruire X

noter tout ce qui se passe à l'exécution pour pouvoir écrire :

ne détruire que X

et finalement écrire l'algorithme inverse.

7. Conclusion générale

Les apports de l'informatique à la physique pure peuvent être encore très nombreux. Notamment les modèles des automates cellulaires pourraient éclairer certaines lois de la cosmologie. Même le problème du temps pourrait recevoir des nouveaux éclairages. Notamment sur la possibilité ou non d'existence de "boucles de genre temps", conformes à la relativité générale, mais totalement contraire au bon sens puisque contraire à la causalité. Il est caractéristique de constater que certains noms, comme ceux de Zurek et de Feynmann, se retrouvent aussi bien dans les articles de physique quantique que dans la physique du calcul. Il y a là un domaine encore très important à étudier : celui de l'émergence des lois physiques à partir de données plus fondamentales lié à ce qui est peut-être le plus fondamental des constituants du monde physique : l'information.

Comme c'est souvent le cas, l'amorce d'applications semble possible. Nous avons présenté ici l'exemple de la preuve informatique. Cette voie pourrait être approfondie et il serait intéressant de l'étendre peut être aux problèmes de complexité et décidabilité, en étudiant de près ce que deviennent les propriétés d'un algorithme pour son inverse temporel.

8. Références

- [1] Aspect 1976, "experimental tests of realistic local theories", Phys. Rev. Letters vol 47 n°7 p 460-463
- [2] Barjavel, "Le voyageur imprudent".
- [3] Bennett 1973, "Logical Reversibility of computation", IBM journal of r&d Nov 73 p 525, 532
- [4] Bennett 1982, "The thermodynamics of computation", Int. J of Theoret. Physics vol 21 n° 12 p 905-939
- [5] Bennett 1984, "Thermodynamically reversible computation", Phys. Rev. Letters vol 53 n°12 p 1202
- [6] Bennett 1988, "Démons, machines et thermodynamique", Pour La Science janvier p 91-97.
- [7] Bennett 1988, "Notes on the history of reversible computation", IBM journal of r&d vol 32 1° Jan 88
- [8] Bennett Landauer 1985, "Les limites physiques du calcul", Pour La Science Septembre.
- [9] Chaitin 1977, "Algorithmic information theory", IBM journal of r&d Juillet
- [10] Chaitin 1992, "Information theoretic incompleteness", applied math. & computation 52 p 83-101
- [11] Chaitin 1975, "Randomness and mathematical proof", Scientific American n° 232 p 47-52
- [12] Costa de Beauregard 1963, "Le second principe de la science du temps", éditions du Seuil.
- [13] Costa de Beauregard, "Temps physique", Encyclopaedia Universalis.
- [14] Costa de Beauregard 1988, "Le temps déployé", éditions Le Rocher.
- [15] Delahaye 1994, "Information, complexité, hasard", éditions Hermes
- [16] Deutsch 1985, "Church-Turing & universal quantum computer", Proc. R. Soc. Lon vol A 400 97-117
- [17] Deutsch Lockwood 1994, "The quantum physics of Time Travel", Scientific American Mars
- [18] Einstein Podolsky Rosen 1935, "quantum-mechanical description complete ?" Phys. Rev. vol 47 p 777-780
- [19] Fink, "Le retournement des ondes acoustiques", La Recherche n°264.
- [20] Fredkin 1982, "Conservative logic", Int. J of Theoret. Physics vol 21 n°3/4 p 219-253
- [21] Gardner 1985, "L'Univers ambidextre", éditions du Seuil
- [22] Hawking, "Une brève histoire du temps".
- [23] Hofstadter "Gödel Escher Bach, les brins d'une guirlande éternelle".
- [24] Kari 1990, "Reversibility of 2D cellular automata is undecidable, Physica D45 1990 379
- [25] Klein Spiro 1994, "Le temps et sa flèche", éditions Frontières
- [26] Kolmogorov 1983, "combinatorial foundations of information theory", Russian math surveys 38:4 p 29-40
- [27] Lestienne, "Les fils du temps".
- [28] Li Vitany 1993, "Introduction to Kolmogorov complexity and its applications", éditions Springer-Verlag
- [29] Lloyd Pagels 1988, "complexity as thermodynamic depth", annals of physics 188 p 186-213
- [30] Maddox 1994, "Times machines still over horizon", Nature 10 Février .
- [31] Margolus 1984, "physics like models of computation", Physica D 10 81-95
- [32] Oversch 1969, "Experiments in time reversal", Scientific American p 89-101
- [33] Parrochia 1994, "cosmologie de l'information", éditions Hermes
- [34] Penrose, "Pensée, ordinateurs et lois de la physique"
- [35] Porod.W Grondin Ferry Porod.G 1984, "dissipation in computation", Phys. Rev. Letters vol 52 N° 3 p 232
- [36] Prigogine, "La fin des certitudes", Odile Jacob 1996
- [37] Sachs 1987, "The physics of time reversal", The university of chicago press
- [38] Scully, Drühl 1982, "Quantum eraser", Physical Review vol 25 N° 4 p 2208-2213
- [39] Scully, Engelbert, Walther 1991, "Quantum optical test of complementarity", Nature vol 351 p 111-116
- [40] Stannard 1966, "Symmetry of time axis", Nature p 693-695.
- [41] Stewart 1994, "Le voyage dans le temps", Pour La Science n°197 et 198 (mars-avril).
- [42] Svozil 1990, "constructive chaos by cellular automata", Physica D 45 420-427
- [43] Svozil 1990, "chaos, automates cellulaires et flèche du temps", Physica D 45 p420
- [44] Tipler 1986, "Cosmological limits of computation", Int. J of Theoret. Physics vol 25 n° 6 p 617-661
- [45] Toffoli 1982, "Physics and computation", Int. J of Theoret. Physics vol 21 n° 3/4 p 165-175
- [46] Zurek, "Algorithmic randomness and physical entropy", Physical review A vol 40 n°8 p 4731-4751
- [47] Zurek 1981, "Pointer basis of quantum apparatus", Physical Review D vol 24 p 1516-1525
- [48] Zurek 1982, "Environment induced superselection rules", Physical Review D vol 26 p 1862-1880
- [49] Zurek 1989, "Thermodynamic cost of computation", Nature vol 341 p 119-124
- [50] Zurek 1990, "Complexity, entropy and the physics of information", éditions Addison Wesley

[51] Zwirn 1992, "Du quantique au classique", Pour la science n° 182 p 38-46