Words, Automata and Processus for Physics & Other Sciences

Gérard H. E. Duchamp
LIPN, *Université de Paris XIII, France*

Collaborators

***Mathematics* :**
Christophe Reutenauer, UQAM., *Montréal, Canada*
***Computer Science* :**
Eric Laugerotte, HatemHadj-Kacem, LIFAR, *Rouen, France*
***Physics* :**
Andrzej Horzela, *Instit. of Nucl. Phys., Krakow, Pologne*
Karol A. Penson, *LPTMC, Université de Paris VI, France*
Allan I. Solomon, *The Open University, United Kingdom*
Pawel Blasiak, *Instit. of Nucl. Phys., Krakow, Pologne*

JORCAD'08, Rouen, Sept 17 – 19, 2008

Content of talk

I : Solving a conjecture in operator theory by means of Automata (1997, Rouen)

II : Decomposing boolean functions with minimization theory (BFCA05, Rouen & +)

III : Solving the transfer coefficient problem in Quantum Theory (Katriel then Penson)

I : Solving a conjecture in operator theory (here NonCommutative Geometry) by means of Automata (1997, Rouen)

Un critère de rationalité
provenant de la géométrie non commutative

- À LA MÉMOIRE DE SCHÜTZENBERGER -

Gérard DUCHAMP* et Christophe REUTENAUER†

Abstract

We prove a conjecture of A. Connes, which gives a rationality criterion for elements of the closure of $\mathbb{C}\Gamma$ (Γ a free group) in the space of bounded operators in $l^2(\Gamma)$. We show that this criterion applies also to the ring of Malcev-Neumann series on Γ.

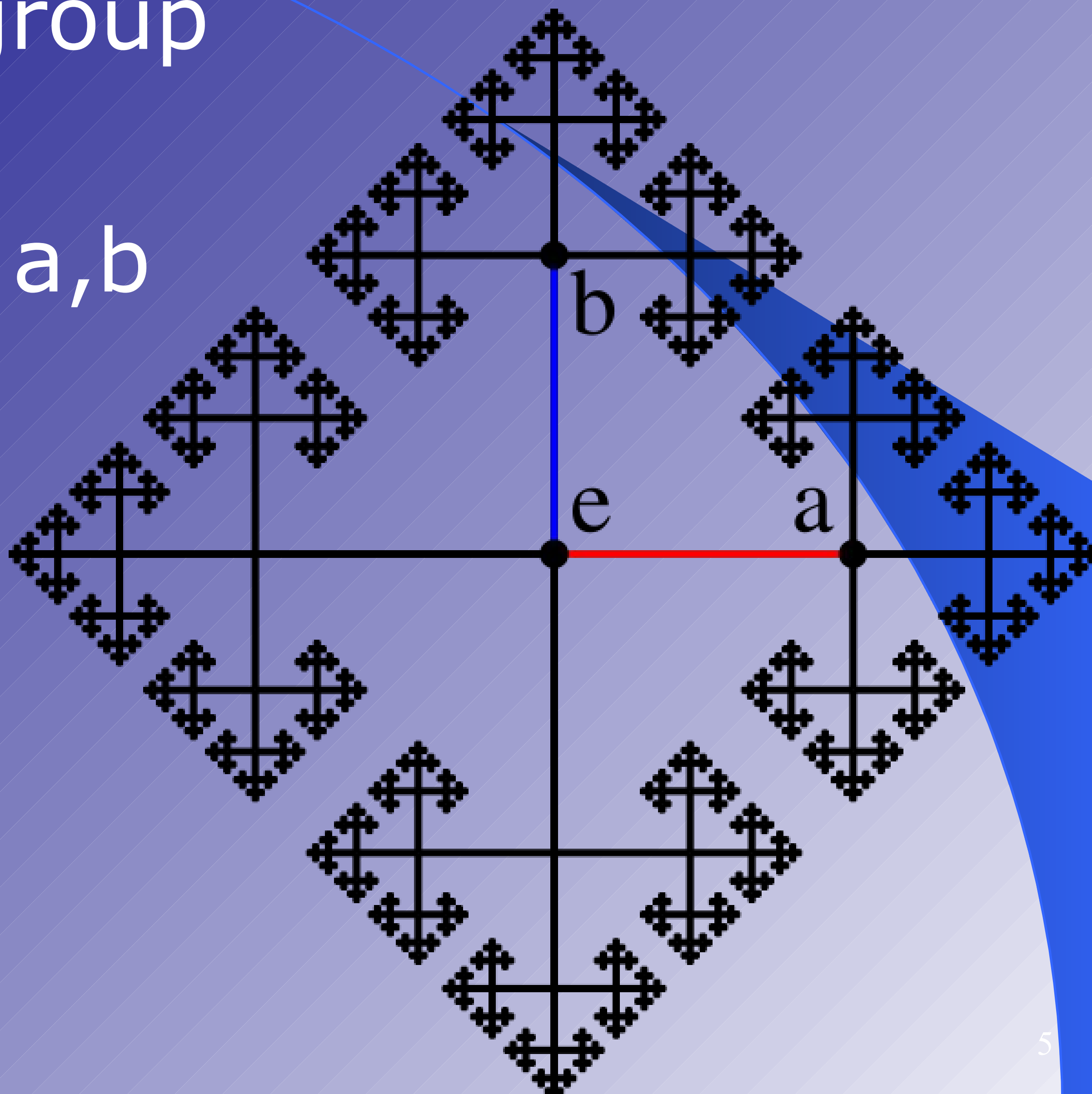
Publié dans Inventiones Mathematicae, **128** (1997)

1 Introduction

Soit X un alphabet et Γ, le groupe librement engendré par X. Pour une fonction à valeurs complexes quelconque $f : \Gamma \to \mathbb{C}$, on définit $||f||_2 = \sum_{g\in\Gamma} |f(g)|^2 \in [0, \infty]$ et $l^2(\Gamma) = \{f : \Gamma \to \mathbb{C}$ t.q. $||f||_2 < \infty\}$ muni de la base $(\epsilon_g)_{g\in\Gamma}$ et de la structure hilbertiennes habituelle

Beginning and end of the story

- The free group on two generators a,b



Beginning and end of the story (cont'd)

- This rationality criterion deals with rational closures

- Definition : X $\subseteq$ B (an associative algebra with unit), the rational closure of X is the smallest subalgebra containing X, closed by the (partially defined) operation x $\rightarrow$ x^(-1).
- Example X=A (a finite alphabet) and B=k<<A>> (here k is a field, can be extended). The rational closure of A is the set of (classical) rational functions.

Beginning and end of the story (cont'd)

- One can extend this rationality notion by considering the resolution of n x n linear systems → one obtains the notion of rational closure of order "n"

- Definition : $X \subseteq B$, then $(X)_n$ is the smallest subalgebra containing X and the coefficients of all its invertible n x n matrices.
- Obviously : $(X)_1 \subseteq (X)_2 \subseteq \ldots (X)_n \subseteq (X)_{n+1}$ and one defines $(X)_\infty$ as the union of all these closures.

Sketch of the setting

- Let Γ a free group with a finite number of generators.
- Define the algebra C[Γ] (C is here the field of complex numbers) as the space of functions Γ---> C with finite support and law given by the convolution product.
- Define a “big” algebra $C_r^*(\Gamma)$ (blackboard if needed).
- On the other hand, Connes defines a subalgebra $(C_r^*(\Gamma))_{fin}$ by a “finite rank” condition, remarks that $(C[\Gamma])_\infty \subseteq (C_r^*(\Gamma))_{fin}$ and conjecture that the reverse inclusion might hold.

Ingredients

----> the answer is YES and the proof uses the tools of Automata Theory in a crucial way

- Rational functions and Kleene-Schützenberger Theorem.
- Specializations
- Rational expressions
- Hadamard product
- Minimization theory

And (from group theory) Haagerup's inequality.

As a byproduct, one obtains an alternative proof of a theorem by G. Cauchon (Blackboard if needed)

II. Decomposing boolean functions with minimization theory (BFCA05, Rouen & +)

Boolean Functions: Cryptography and Applications BFCA'05
Fonctions Booléennes : Cryptographie & Applications

ON THE DECOMPOSITION OF BOOLEAN FUNCTIONS

Gérard H. E. Duchamp[1], Hatem Hadj Kacem[2] and Éric Laugerotte[2]

Abstract. The minimization of a weighted automaton given by its linear representation (λ, μ, γ) taking its letters in an alphabet A and its multiplicities in a (commutative or not)

Below, mw = w.f (module action)

algorithm *suffix*
input the set S
a boolean function $f \in \mathcal{F}_n$
output a suffix set $P \subset S^*$
a set of relators R
$(P, Y, R) := (\emptyset, \{\varepsilon\}, \emptyset)$
while $Y \neq \emptyset$
do take $y \in Y$
if $my \notin \mathrm{span}(mp : p \in P)$
then $(P, Y) := (P \cup \{y\}, (Y - \{y\}) \cup yS)$
else there exits a relation $my = \sum_{p \in P} \alpha_p mp$
$(P, Y, R) := (P, (Y - \{y\}), R \cup \{y - \sum_{p \in P} \alpha_p p\})$
end_if
end_while
return(P, R)
end

The set P is a suffix set and the algorithm terminates. In fact, we show that the set P is suffix at each step of the algorithm. This is clear from the beginning when $P = \{\varepsilon\}$. Now, if $y \in Y \subseteq S^*$ is

This algorithm gives a complete description by generators and relations of the space M=k<S>.f. It provides

- A basis of M (precisely P.f)
- A complete set of relators in a normal form so that the computation be decidable.

For this reason, one can compute (if there are some) the true decompositions

$$M=M_1 \oplus M_2$$

where M_1, M_2 are stable by the actions of S. If there are no such decomposition, the setting gives an automatic proof (certificate) of undecomposability of M.

Applications :

- Boolean functions
- 0-Hecke algebra (forthcoming)

III. Transfer coefficient problem in Quantum Physics

Classical Fock space for bosons and q-ons

- Heisenberg-Weyl (two-dimensional) algebra is defined by two generators (a^+, a) which fulfill the relation

$$[a\,,\,a^+]=aa^+ - a^+a=1$$

- Known to have no (faithful) representation by bounded operators in a Banach space.

There are many « combinatorial » (faithful) representations by operators. The most famous one is the Bargmann-Fock representation

$$a \dashrightarrow d/dx\ ;\ a+ \dashrightarrow x$$

where a has degree -1 and a^+ has degree 1.

- These were bosons, there are also fermions. The relation for fermions is

$$aa^{+} + a^{+}a = 1$$

- This provides a framework for the q-analogue which is defined by

$$[a\,,\,a^{+}]_q = aa^{+} - qa^{+}a = 1$$

- For which Bargmann-Fock representation reads

$$a \dashrightarrow D_q \;;\; a+ \dashrightarrow x$$

where a has degree -1 and a^{+} has degree 1 and D_q is the (classical) q-derivative.

- For a faithful representation, one needs an infinite-dimensional space. The smallest, called Fock space, has a countable basis $(e_n)_{n\geq 0}$ (the actions are described below, each e_n is represented by a circled state « n »).

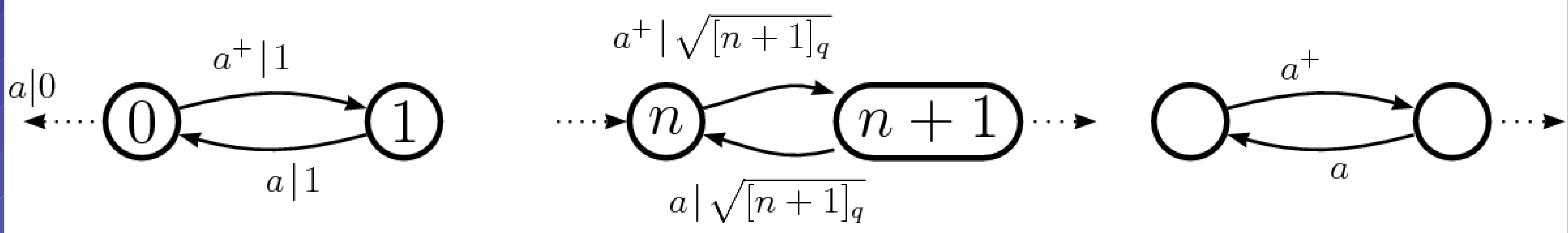


Figure 1: Classical Fock space

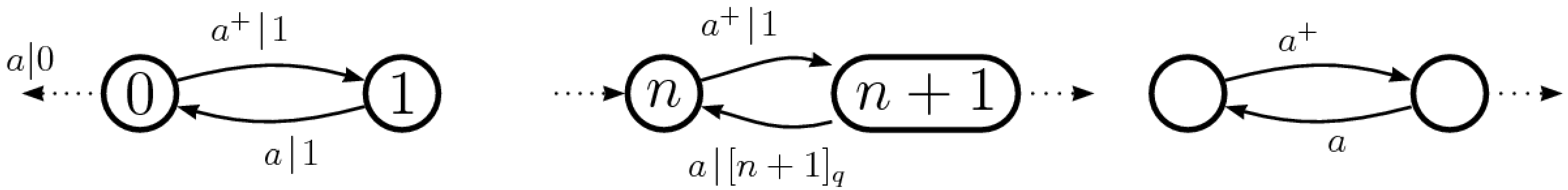


Figure 2: Bargman-Fock representation.
State "n" is z^n and $a^+ \to z$; $a \to D_q$ with $D_q(f) = \frac{f(qz)-f(z)}{z(q-1)}$

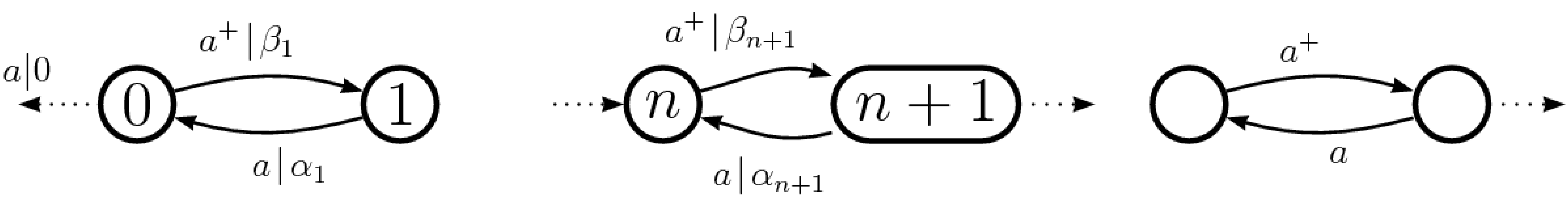


Figure 3: General setting: in order that the Fock space be bounded below, one must have $\alpha_0 = 0$.

- Physicists need to know the sum of all weights created when one passes from level « n » to level « m ». This problem has been called the « transfer packet problem » and is at once rephrased by combinatorists as the computation of a formal power series.

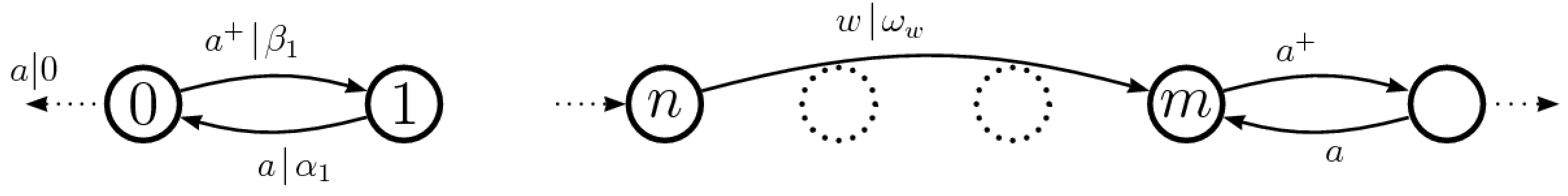
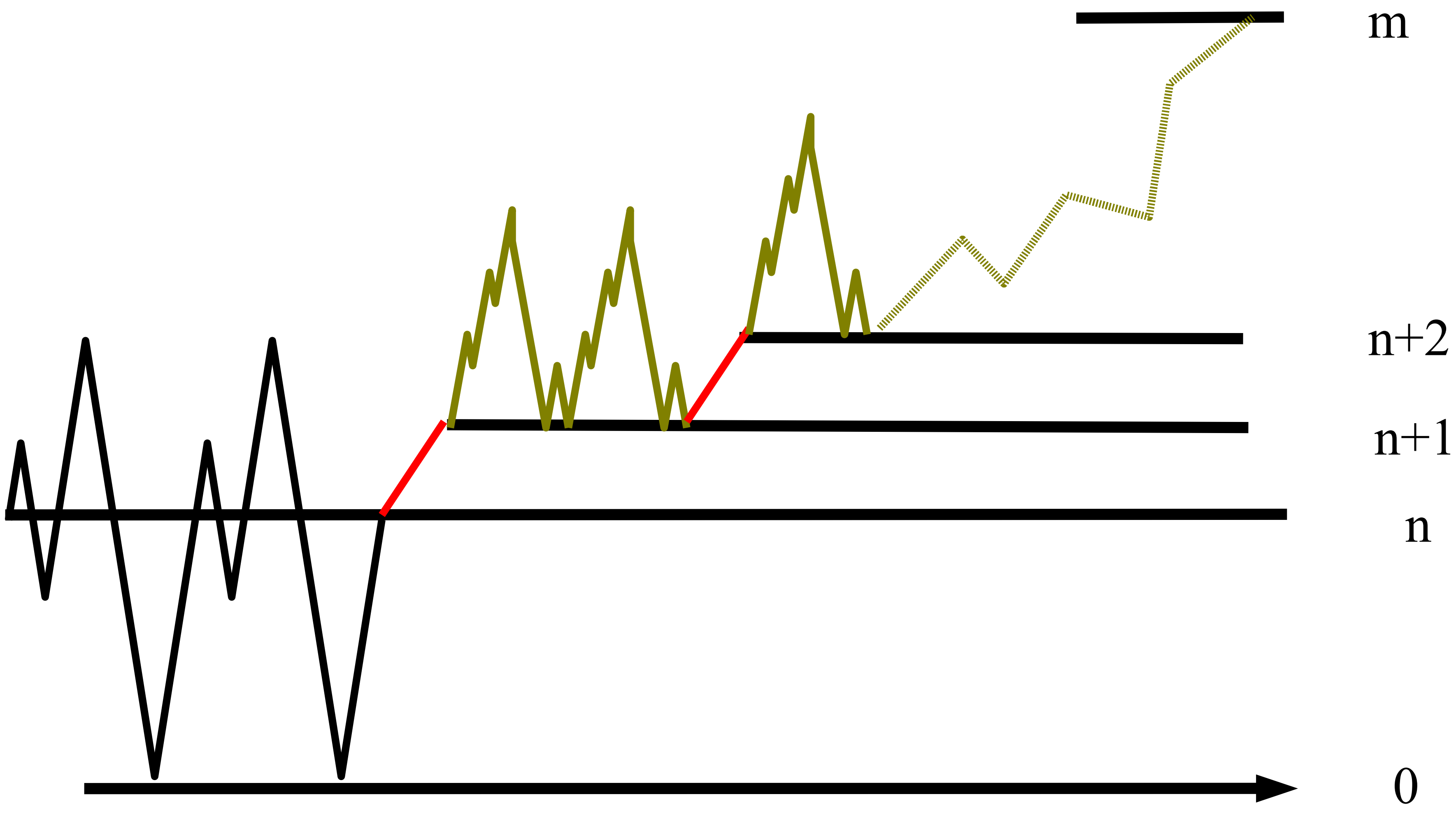


Figure 4: The transfer packet problem

Change of level



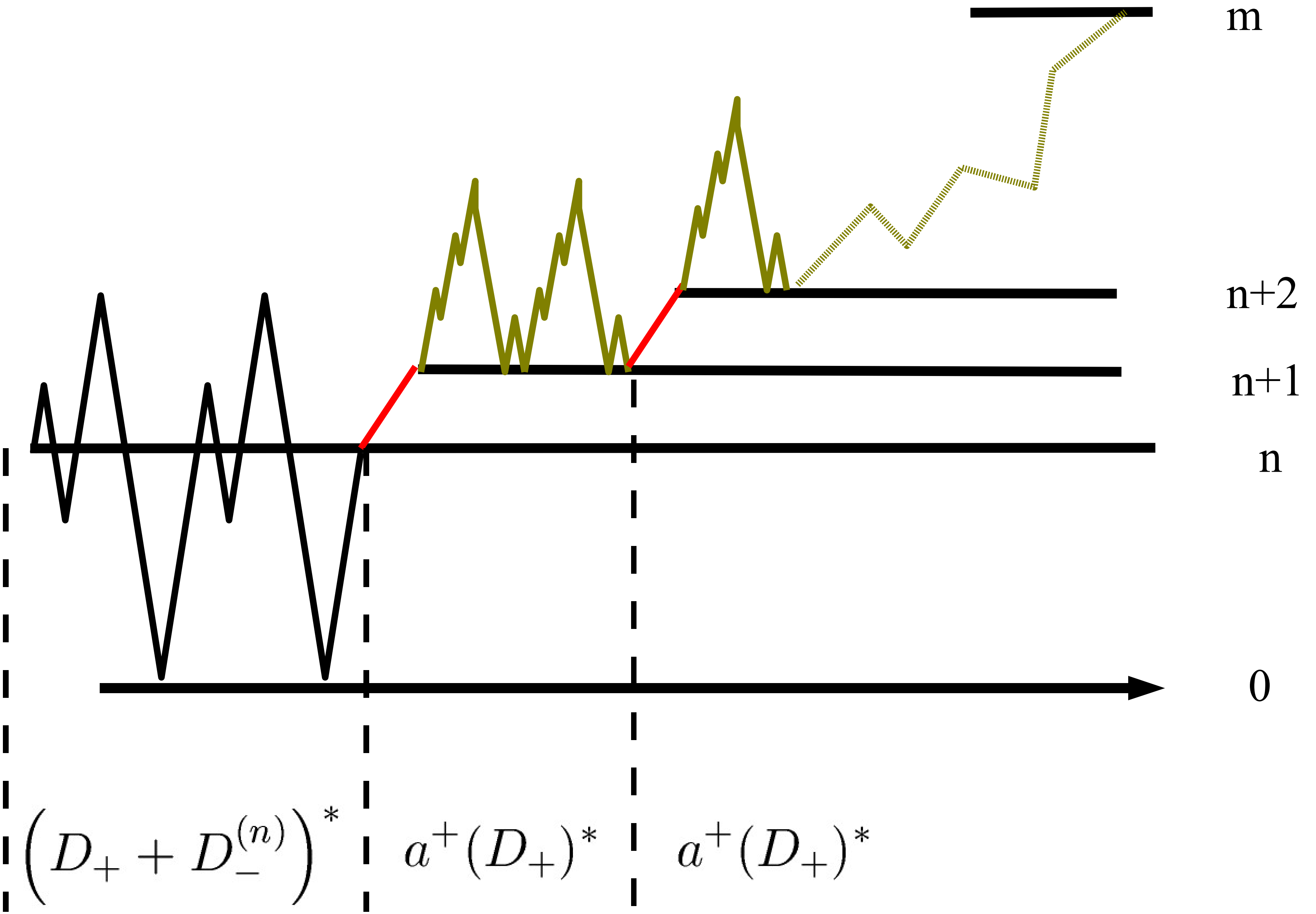
- The set of words which allow to pass from level « n » to level « m » in « i » steps is clearly.

$$W_k^{(i)} = \left\{ w \in \{a, a^+\}^* \middle| \pi_e(w) = k \text{ and } |w| = i \right\}$$

$$\text{with } k = m - n \text{ and } \pi_e(w) = |w|_{a^+} - |w|_a.$$

- The weight associated with this packet and the desired generating series are then

$$e_n.W_{m-n}^{(i)} = \omega_{n\to m}^{(i)}\, e_m \ ; \ T_{n\to n+k} := \sum_{i\geq 0} t^i \omega_{n\to n+k}^{(i)}$$


m
n+2
n+1
n
0
$\left(D_+ + D_-^{(n)}\right)^*$
$a^+(D_+)^*$
$a^+(D_+)^*$

The following selfreproducing formulas can be considered as noncommutative continued fraction expansions of the involved “D” codes

$$D_+ = a^+\left(D_+\right)^* a \ ; \ \ D_-^{(n)} = a\left(D_-^{(n-1)}\right)^* a^+ \ ; \ \ D_-^{(0)} = \emptyset$$

Using a bit of analysis to extend the right action of the words to series of words and the representation

a ---> ?.ta ; a+ ---> ?.ta+

We get

$$T_{n\to n}[t] = \frac{1}{1 - \frac{t^2\alpha_{n+1}\beta_{n+1}}{1-\frac{t^2\alpha_{n+2}\beta_{n+2}}{1-\cdots}} - \frac{t^2\alpha_n\beta_n}{1-\frac{t^2\alpha_{n-1}\beta_{n-1}}{1-\cdots}}}$$

And, if one allows only the positive loops

$$T^{+}_{n\to n}[t] = \frac{1}{1 - \frac{t^2\alpha_{n+1}\beta_{n+1}}{1-\frac{t^2\alpha_{n+2}\beta_{n+2}}{1-\cdots}}}$$

Which solves, with two cases, the problem of the transfer packet.

Concluding remarks and future

i) We have solved the problem of packet of monoidal actions on a "level" space by means of the theory of codes and a bit of operator analysis → this can be extended to more than two operators/

ii) In general, Hopf algebras of physics which are non-commutative are free on some alphabet (often, of diagrams) and computation on its Sweedler's dual (which is the biggest available for finite comultiplications) and we have seen that they can be performed via rational expressions.

Concluding remarks and future (cont'd)

iii) Kleene-Schützenberger's theorem still works in the general case (infinite alphabet) up to a slight modification. This will allow the development of a calculus in the general (i. e. out of the free) case.

Thank You