Volume of multiplicative formulas and provability

François Métayer*

Abstract

In [Met], we introduced a homological condition of correctness for paired-graphs. As an application of this result, we establish here new conditions of provability in multiplicative linear logic, by defining the volume of a formula. We also extend the complexity results of [Kan] and [LW] to abstract graphs.

1 Introduction

This paper introduces a correspondance between modules with a given border (see sect.2) and subspaces of an euclidian space, in such a way that the correct pasting of two modules M_1 and M_2 along their common border can be expressed by an equation

$$\mathrm{a}(X_1, X_2^{\perp}) = \lambda$$

Here X_i denotes the subspace associated with M_i, a is a geometrical invariant of a pair of subspaces, and λ is a constant depending on M_1 and M_2 as separate modules, not on the way they are pasted together.

Since this interpretation stems from the homological correctness criterion we introduced in [Met], we first recall the main definitions and results of this paper. Let G be a graph. A *pair* of G is a pair of edges having a unique vertex in common. A *paired-graph* (pg) is an ordered pair $(G, \mathcal{P})$ where G is a

*Équipe de Logique, Université Paris VII–CNRS, 45-55, 5ème étage, 2 place Jussieu 75251 PARIS Cedex 05 FRANCE. e-mail: metayer@logique.jussieu.fr

graph and $\mathcal{P} = \mathcal{P}(G)$ is a set of mutually disjoint pairs of G. The motivation for considering this notion is that proof-structures in multiplicative linear logic (see [Gir1]) can be seen as pg's, where pairs correspond to *par*-links. We denote by $\mathcal{V}(G)$ (resp. $\mathcal{E}(G)$) the set of vertices (resp. edges) of G. We call an edge a *paired-edge* if it belongs to a pair, and a *free* edge otherwise. Now a *morphism* $f : G \longrightarrow G'$ is a map $\mathcal{V}(G) \longrightarrow \mathcal{V}(G')$, $x \mapsto x'$, such that, if uv is a free edge, $u'v'$ is free, or $u' = v'$, and, if $\{uw, vw\}$ is a pair, then $\{u'w', v'w'\}$ is a pair, or $u' = v' = w'$. Abstract proof-nets can be defined in this setting: let G_1, G_2 be pg's, $u \in \mathcal{V}(G_1)$, $v \in \mathcal{V}(G_2)$. We denote by $\mathrm{t}(G_1, G_2, u, v) = G_1 \coprod G_2 / u \sim v$ the graph obtained by identifying u and v in the disjoint reunion of G_1 and G_2. Likewise, if G is a pg with distinct vertices u and v, we denote by $\mathrm{p}(G, u, v)$ the graph obtained by adjoining a new vertex w, and a new pair $\{uw, vw\}$ (fig.1).

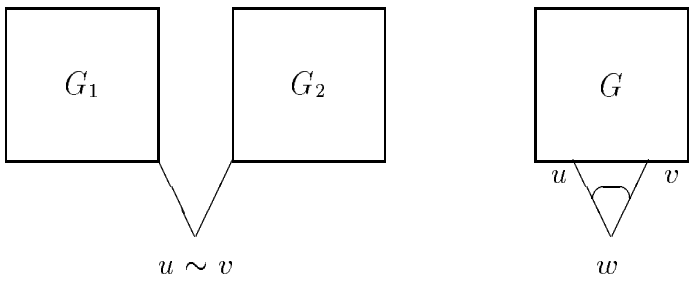

fig.1

The smallest class of pg's containing trees (connected, acyclic graphs, without pairs), and closed by t and p is the class of *proof-nets*. The starting point of [Met] is the following remark: a paired-graph G, just like an ordinary one, gives rise to a complex of abelian groups:

$$0 \quad \longrightarrow \quad C_1(G) \quad \xrightarrow{\partial} \quad C_0(G) \quad \xrightarrow{\epsilon} \quad \mathbf{Z} \quad \longrightarrow \quad 0$$

where $C_0(G) = \mathbf{Z}[\mathcal{V}(G)]$ and $C_1(G)$ is the subgroup of $\mathbf{Z}[\mathcal{E}(G)]$ generated by the free edges and the elements $e + e^*$ where e runs over paired edges. ∂ is the restriction to $C_1(G)$ of the boundary morphism defined by $\partial(uv) = v - u$, and ϵ is the *augmentation* morphism defined by $\epsilon(u) = 1$ for each vertex u. Notice that edges have to be oriented in order to define ∂. The only requirement is that, in each pair, both edges point towards their common vertex, or both in the opposite direction. Since $\epsilon\partial = 0$ we can define homology groups $H_0(G) = \ker\epsilon / \operatorname{im}\partial$ and $H_1(G) = \ker\partial$. Morphisms have been defined such that each $f : G \longrightarrow G'$ determines morphisms of groups $f^i_* : H_i(G) \longrightarrow H_i(G')$, for

$i = 1, 2$, making H_i a functor from paired-graphs to abelian groups. As an example, the reader may check that if $\mathcal{V}(G) = \{u, v, w\}$, $\mathcal{E}(G) = \{uw, vw, uv\}$ and $\mathcal{P}(G) = \{\{uw, vw\}\}$, then $H_1(G) = 0$ and $H_0(G) = \mathbf{Z}/2\mathbf{Z}$ (fig.2).

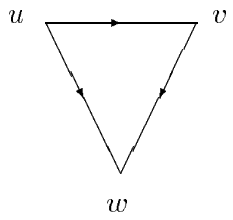

fig.2

The relevance of this homology lies in the fact that it characterizes proof-nets among arbitrary paired-graphs, as shown by the main result of [Met]:

Theorem 1.1 *G is a proofnet if and only if $H_1(G) = 0$ and* card $H_0(G) = 2^p$, *where $p =$* card $\mathcal{P}(G)$.

It should be pointed out that, for *each* graph G, not necessarily a proof-net, satisfying $H_1(G) = 0$ and $H_0(G)$ finite, the cardinal of $H_0(G)$ cannot be greater than $2^{\text{card}\,\mathcal{P}(G)}$. Finally, if G is a paired-graph and K a subgraph of G we may define *relative homology groups* $H_i(G, F)$ for $i = 1, 2$, as usual: with the above notations, we denote by $C_i(G, K)$ the factor group $C_i(G)/C_i(K)$. Now ∂ induces $\overline{\partial}$:

$$0 \quad \longrightarrow \quad C_1(G, K) \quad \xrightarrow{\overline{\partial}} \quad C_0(G, K) \quad \longrightarrow \quad 0$$

so that $H_0(G, K) = C_0(G, K)/\operatorname{im}\overline{\partial}$ and $H_1(G, K) = \ker\overline{\partial}$.

2 Modules

Let M, N, and F be paired-graphs, and $F \xrightarrow{m} M$, $F \xrightarrow{n} N$ be injective morphisms. $M *_F N$ is defined, up to isomorphism, by the following pushout diagram:

$$\begin{array}{ccc} F & \xrightarrow{m} & M \\ \downarrow n & & \downarrow i \\ N & \xrightarrow{j} & M *_F N \end{array}$$

We only consider the case where (1) $M \cap N = F$ (as subgraphs of $M *_F N$) and (2) F is a set of vertices. As in [Tro], we say that M and N are

connectable along F if $M *_F N$ is a proofnet (fig.3). We are asking under which conditions two graphs M and N are connectable.

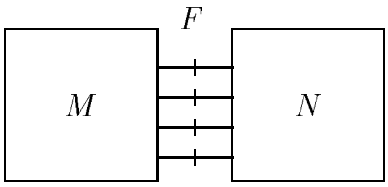

fig.3

In fact, we can restrict our attention to *modules*, in the following sense:

Definition 2.1 *A* module *is an ordered pair (M, F) where M is a graph and F is a subgraph of M consisting of vertices only, such that $H_1(M) = 0$ and $H_0(M, F)$ is a finite group. We call F the* border *of the module.*

It should be noticed that 2.1 is not strictly equivalent with the definition of [Tro] but it is better suited to our homological approach. Now the above injections m and n give rise to morphisms

$$H_0(F) \xrightarrow{m_*} H_0(M)$$

and

$$H_0(F) \xrightarrow{n_*} H_0(N)$$

If F has $k+1$ vertices, we get $H_0(F) \cong \mathbf{Z}^k$ and a Mayer-Vietoris exact sequence

$$0 \longrightarrow \mathbf{Z}^k \xrightarrow{\phi} H_0(M) \oplus H_0(N) \xrightarrow{i_*+j_*} H_0(G) \longrightarrow 0 \qquad (1)$$

By using the homological correctness criterion of [Met], we can show:

Proposition 2.2 *Let (M, F) and (N, F) be two modules, and π_M (resp. π_N) the number of pairs in M (resp. N). They are connectable if and only if*

$$\operatorname{card} H_0(M, F) \times \operatorname{card} H_0(N, F) \times [H_0(F) : \ker m_* \oplus \ker n_*] = 2^{\pi_M + \pi_N} \qquad (2)$$

Notice that (2) implicitely contains the conditions: $\ker m_* \cap \ker n_* = 0$ and: $\operatorname{rank}(\ker m_* \oplus \ker n_*) = \operatorname{rank} H_0(F)$.

To each multiplicative formula A we associate as usual a binary tree M, which can be seen as a paired-graph where pairs represent the *par* connectives of A. The vertices of M correspond to the subformulas: in particular, vertices of degree 1 are associated to the atomic subformulas, and form a subgraph F. There is a unique vertex of degree 2, which is associated to the whole formula and is the *root* of M. Then (M, F) is a module. Such an M will be called a *graph of formula* (gf). The number of vertices in the border F is the *size* of M and will be denoted by τ_M. Clearly, if A is provable, then $\tau_M = 2k$.

Let M be a gf of size $2k$. It is called *provable* if and only if we can obtain a proofnet by adjoining k disjoint edges having their vertices in F. In other words, if N_k denotes the graph of k disjoint edges, M is provable if and only if there is an injection $n : F \longrightarrow N_k$ such that (M, F) and (N_k, F) are connectable. As a consequence of the finiteness of $[H_0(F) : \ker m_* \oplus \ker n_*]$ in (2), we find again a well-known condition of provability:

Proposition 2.3 *If M is provable, $\tau_M = 2\pi_M$.*

Before we turn to more interesting conditions, we briefly investigate the complexity of the decision problem for gf's.

3 Complexity

We sketch here the proof of the following result:

Theorem 3.1 *The decision problem for graphs of formulas is NP-complete.*

Kanovich has proved NP-completeness for the full propositional fragment of multiplicative linear logic [Kan], and the same is true for the neutral fragment, as shown by Lincoln and Winkler [LW]. We reduce our problem to the latter in two steps.

Step 1: encoding of the neutrals in the fragment L(a), whose formulas are builded with literals a and $a^\perp$ only. We translate neutrals in L(a) as follows:

- $1^\circ = a \wp a^\perp$ and $\perp^\circ = a \otimes a^\perp$.
- For all formulas A and B, $(A \wp B)^\circ = A^\circ \wp B^\circ$ and $(A \otimes B)^\circ = A^\circ \otimes B^\circ$.
- For each sequent $\Gamma = A_1, \ldots, A_p$, $\Gamma^\circ = A_1^\circ, \ldots, A_p^\circ$.

Then

Lemma 3.2 *The translation $A \longrightarrow A^\circ$ is sound and faithful.*

Step 2: encoding of $\mathrm{L}(a)$ in (abstract) gf's.

For each formula $A \in \mathrm{L}(a)$, we denote its graph by M_A. Let $B = (a \wp a) \wp (a \wp a)$ and $A^* = A[B/a; B^\perp/a^\perp]$. Then we define $T_A = M_{A^*}$. Recall that a formula is *balanced* if it has the same number of occurences of a and $a^\perp$. We can prove

Lemma 3.3 *A balanced formula A is provable in $\mathrm{L}(a)$ if and only if the gf T_A is provable.*

Proof. Suppose first that A is provable (hence balanced). Then A^* is provable, as well as its gf, which is precisely T_A.

Suppose conversely that A is a balanced formula such that $T = T_A$ is provable.

If $M = M_A$, $\tau_M = 2k$ hence $\tau_T = 8k$. Let $F^1 = F_{8k}$ be the border of T and $N^1 = N_{4k}$. By hypothesis, there is an injection $F^1 \xrightarrow{n} N^1$ such that $G = T *_{F^1} N^1$ is a proofnet.

Thus $2\pi_T = \tau_T = 8k$ but $\pi_M = \pi_T - 3k = k$ hence $H_0(M) \cong \mathbf{Z}^k$. On the other hand $G = M *_F N$ where F is the border of M and $N = G \setminus M$, which is obtained by pasting together N^1 with k copies of M_B and k copies of $M_B^\perp$ along F^1. If we now chose a switching σ *of* N we know that $G^\sigma = M *_F N^\sigma$ is again a proofnet. By (1) we get

$$\mathrm{rank}(H_0(M)) + \mathrm{rank}(H_0(N^\sigma)) = \mathrm{rank}(H_0(F)) = 2k - 1$$

hence also $\mathrm{rank}(H_0(N^\sigma)) = k - 1$. Then N^σ is an ordinary graph having k connected components.

Now the vertices of F^1 are distibuted in sets of four vertices, according to the graphs M_B or $M_B^\perp$ where they belong. We denote these sets by

$$X_i = \{a_{i1}, a_{i2}, a_{i3}, a_{i4}\} \quad \text{for} \quad i = 1, \ldots, k$$

$$Y_j = \{a_{j1}^\perp, a_{j2}^\perp, a_{j3}^\perp, a_{j4}^\perp\} \quad \text{for} \quad j = 1, \ldots, k$$

where X_i (resp. Y_j) is the border of $M_i \cong M_B$ (resp. $M_j^\perp \cong M_B^\perp$). s_i (resp. $s_j^\perp$) will be the root of M_i (resp. $M_j^\perp$).

Let $X = \bigcup_i X_i$ and $Y = \bigcup_i Y_i$. The edges of N^1 induce a partition of $X \cup Y$ in pairs. Two vertices of Y cannot belong to the same pair, otherwise G has a cycle in contradiction with $H_1(G) = 0$.

By $\mathrm{card}(X) = \mathrm{card}(Y) = 4k$, all pairs consist of a vertex of X and a vertex of Y. This gives a bijective mapping $\phi : X \longrightarrow Y$. Consider now $\Phi : \{1, \ldots, k\} \longrightarrow \mathcal{P}(\{1, \ldots, k\})$ which associates to each index i the set $\{j / \phi^\bullet(X_i) \cap Y_j \neq \emptyset\}$. Let I be any subset of $\{1, \ldots, k\}$, we verify that

$$\mathrm{card}(\bigcup_{i \in I} \Phi(i)) \geq \mathrm{card}(I)$$

Indeed, if $C = \bigcup_{i\in I} \Phi(i)$:

$$\phi^\bullet(\bigcup_{i\in I} X_i) \subset \bigcup_{j\in C} Y_j$$

Since X_i and Y_j are pairwise disjoint sets of four elements and ϕ is bijective, the cardinals in the above inclusion are respectively $4 \times \mathrm{card}(I)$ and $4 \times \mathrm{card}(C)$. This proves the inequality.

Now the wedding lemma (see [Hal, p.48]) applies, giving an injective—hence bijective—ψ from $\{1,\ldots,k\}$ in itself such that, for all i, $\psi(i) \in \Phi(i)$. We can chose in each X_i a vertex x_i such that $\phi(x_i) \in Y_{\psi(i)}$. Take in each M_i the switching connecting s_i to x_i (in M_i). It induces a switching σ_0 of N such that for all $i \in \{1,\ldots,k\}$, s_i and $s^\perp_{\psi(i)}$ are in the same connected component of N^{σ_0}. But this graph has k connected components; each one can be replaced by a unique edge $s_i s^\perp_{\psi(i)}$ (fig.4). The result is a proof of A. $\diamond$

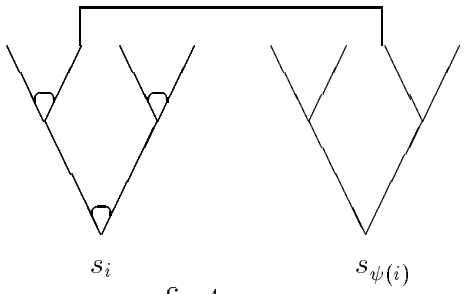

fig.4

We get 3.1 as an immediate consequence. The problem belongs to NP: given (M,F) of size $2k$ and $F \xrightarrow{n} N_k$, the correctness of $M *_F N_k$ is decidable in polynomial time (in k). As regards completeness, the composition of the two translations $A \longrightarrow A^\circ \longrightarrow T_{A^\circ}$ reduces polynomially the decision problem for neutrals to the problem for gf's. But the former is already NP-complete.

4 Volume of modules and formulas

The complexity result we have just proved opposes a simple characterization of provable gf's. It is however possible to improve 2.3, as we shall see. Let (M,F) be a module, with $F = \{s_1,\ldots,s_l\}$ and $F \xrightarrow{m} M$ the inclusion morphism. Recall that $H_0(F) \cong \mathbf{Z}^{l-1}$, and if rank $H_0(M) = p$, then $\ker m_* \cong \mathbf{Z}^r$ where $r = l - 1 - p$.

Now $A = (s_1, \ldots, s_l)$ can be seen as the canonical basis of $E = \mathbf{R}^l$ so that $H_0(F)$ becomes a discrete subgroup of the hyperplane:

$$L : \quad x_1 + \cdots + x_l = 0$$

If $e_i = s_i - s_l$, then $\mathcal{B} = (e_i)_{1 \leq i \leq l-1}$ is a basis of L. If we provide E with its canonical (w.r.t A) scalar product $\langle , \rangle$, the *volume* of a family of vectors $v_1, \ldots, v_p$ is well defined: it will be denoted by $\|v_1, \ldots, v_p\|$ (see [Ber]). In particular, if $(m_1, \ldots, m_r)$ is a $\mathbf{Z}$-basis of $\ker m_*$, $\|m_1, \ldots, m_r\|$ only depends on M and F, so that we may define:

Definition 4.1 *The* volume *of M, denoted by $\|M\|$ is the volume of any* $\mathbf{Z}$*-basis of* $\ker m_*$.

Let M_1 and M_2 be two modules with common border $F = \{s_1, \ldots, s_l\}$ and $F \xrightarrow{m^i} M_i$ the inclusion morphism. Let $p_i = \pi_{M_i}$ and $d_i = \mathrm{card}(H_0(M_i, F))$. By 2.2 M_1 and M_2 are connectable if and only if

$$[H_0(F) : \ker m^1_* \oplus \ker m^2_*] = \frac{2^{p_1+p_2}}{d_1 d_2} \tag{3}$$

If $(m^1_1, \ldots, m^1_{r_1})$ and $(m^2_1, \ldots, m^2_{r_2})$ are $\mathbf{Z}$-bases of $\ker m^1_*$ and $\ker m^2_*$ respectively, then $r_1 + r_2 = l - 1$ and the left member of (3) is

$$\left|\det_{\mathcal{B}}(m^1_1, \ldots, m^1_{r_1}, m^2_1, \ldots, m^2_{r_2})\right| = \frac{\|m^1_1, \ldots, m^1_{r_1}, m^2_1, \ldots, m^2_{r_2}\|}{\|\mathcal{B}\|}$$

and we may rewrite (3) as

$$\|m^1_1, \ldots, m^1_{r_1}, m^2_1, \ldots, m^2_{r_2}\| = \frac{2^{p_1+p_2}\sqrt{l}}{d_1 d_2}$$

On the other hand

$$\|m^1_1, \ldots, m^1_{r_1}, m^2_1, \ldots, m^2_{r_2}\| = \mathrm{a}\,\|M_1\|\|M_2\|$$

where a only depends on the vector spaces X_1 and X_2 generated in L by $\ker m^1_*$ and $\ker m^1_*$ respectively.

The precise value of a is defined as follows: if Y and Z are subspaces of an euclidian space and if p_Y denotes the orthogonal projector on Y, we may consider $p_Y \circ p_Z$ as an endomorphism u of Y—by restriction to Y. Then $\det u \geq 0$ and if

$$\mathrm{a}(Y, Z) = \sqrt{\det u}$$

we have

$$\mathrm{a} = \mathrm{a}(X_1, X_2^\perp) = \mathrm{a}(X_2, X_1^\perp)$$

Thus, with the above notations

Theorem 4.2 *The correctness of $M_1 *_F M_2$ is expressed by an equation:*

$$\mathrm{a}(X_1, X_2^\perp) = \lambda$$

where λ only depends on M_1 and M_2 separately.

We now apply the previous results to the particular case of formulas. Here $M_1 = M$ is a gf of size $l = 2k$ and $M_2 = N_k = N$. Then $p_1 = \pi_M$—and we may suppose that $p_1 = k$ by 2.3—$p_2 = 0$, $d_1 = 2^h$ and $d_2 = 1$. We also denote $m = m_1$, $n = m_2$, $X_1 = X$ and $X_2 = Y$.

A few calculations show that, with the above notations,

Proposition 4.3 *A gf (M, F) is provable if and only if there is an $n : F \longrightarrow N$ such that*

$$\mathrm{a}(X_1, X_2^\perp)\|M\| = (\sqrt{2})^{k-2h+1}\sqrt{k} \tag{4}$$

Any bound $\mathrm{a}(X, Y^\perp) \leq A$ independent of n gives a necessary condition of provability for M of the form:

$$\|M\| \geq \frac{(\sqrt{2})^{k-2h+1}\sqrt{k}}{A}$$

Consider for instance

$$A = (((a \wp (a \otimes a)) \otimes a) \wp (a \otimes a)) \wp (((a^\perp \wp a^\perp) \wp (a^\perp \wp a^\perp)) \otimes (a^\perp \otimes a^\perp))$$

For $M = M_A$, according to 4.1, $\|M\| = 4\sqrt{33}$. Now formulas of the form $\Phi' \wp \Phi''$ where Φ' (resp. Φ'') has k atoms of type a (resp. $a^\perp$) verify

$$\mathrm{a}(X, Y^\perp) \leq \left(\frac{1}{\sqrt{2}}\right)^{k-1}$$

Thus M can be provable only if

$$\|M\| \geq 2^{k-h}\sqrt{k}$$

but here $k = 6$ and $h = 2$, so that $2^{k-h}\sqrt{k} = 16\sqrt{6} > 4\sqrt{33}$. Hence M is not provable, although it satisfies $\tau_M = 2\pi_M$.

Let us examine more generally the problem of finding a proof of a given gf M of size $2k$, if it exists. In the euclidian space L, M defines a subspace X generated by $\ker m_*$. Each partition p of F in pairs determines an injection $n^p : F \longrightarrow N_k$, and consequently a subspace Y^p generated by $\ker n^p$. Now every correct choice (i.e. giving an actual proof) *maximizes* $\mathrm{a}(X^\perp, Y^p)$ over all possible p's. Therefore, the decision problem for M amounts to calculate

$$\max_p \mathrm{a}(X^\perp, Y^p)$$

and verify that this maximum satisfies (4) in 4.3.

The group S_{2k} of permutations of F can be seen as the subgroup A_{2k-1} (see [Hum, p.5]) of isometries of L generated by the reflections associated to tranpositions of vertices. It acts transitively on the above set of subspaces Y^p. If we chose an arbitrary $Y_0 = Y^p$, we must solve the optimization problem for

$$g \mapsto \mathrm{a}(X^\perp, gY_0)$$

over A_{2k-1}. We may then ask if there is any *small* set of generators of A_{2k-1} for which successive approximations provide the right answer, at least for a wide class of formulas.

References

[Ber] M.Berger *Géométrie, vol.2.* (Cedic/Nathan 1977)

[Dan] V.Danos *La Logique Linéaire appliquée à l'étude de certains processus de normalisation.* (Thèse de Doctorat, Université Paris VII, 1990)

[DR] V.Danos & L.Régnier *The structure of multiplicatives.* (Arch. Math.Logic 28, 1990)

[Gir1] J.Y.Girard *Linear Logic.* (Theor.Comput.Sci.50, 1987)

[Gir2] J.Y.Girard *Quantifiers in Linear Logic II.* (Prépublications Université Paris VII 19, 1991)

[Hal] P.J.Hall *Combinatorial Theory.* (Wiley, 1986)

[Hum] J.E.Humphreys *Reflection groups and Coxeter groups.* (Cambridge, 1990)

[Kan] M.I.Kanovich *The multiplicative fragment of Linear Logic is NP-complete.* (TR X-91-14 University of Amsterdam, 1991)

[LW] P.Lincoln & T.Winkler *Constant only Multiplicative Linear Logic is NP-complete.* (1992)

[Met] F.Métayer *Homology of proof-nets.* (Arch.Math.Logic 33, 1994)

[Tro] A.S.Troelstra *Lectures on linear logic.* (CSLI, 1992)