A Completeness Theorem for "Total Boolean Functions"

July 2008

Pierre Hyvernat,* pierre.hyvernat@univ-savoie.fr

Abstract. In [3], Christine Tasson introduces an algebraic notion of totality for a denotational model of linear logic. The notion of total boolean function is, in a way, quite intuitive. This note provides a positive answer to the question of completeness of the "boolean centroidal calculus" w.r.t. total boolean functions.

0. Introduction. Even though the question answered in this note has its roots in denotational semantics for the differential λ-calculus ([2] and [1], see also [4]), no background in proof-theory is necessary to understand the problem. In the end, it boils down to a question about a special kind of polynomials in $2n$ variables over an arbitrary field $\mathbf{k}$. This note is almost "self-contained", assuming only mild knowledge about polynomials and vector spaces (and a modicum about affine spaces).

The only exotic (??) technology is the following formula for counting monomials or multisets. The number of different monomials of degree d over n variables is usually denoted $\left(\!\!\binom{n}{d}\!\!\right)$. A simple counting argument shows that the number of monomials of degree *at most* d in n variables is $\left(\!\!\binom{n+1}{d}\!\!\right)$. A closed formula for $\left(\!\!\binom{n}{d}\!\!\right)$ in terms of the usual binomial coefficient is given by:

$$\left(\!\!\binom{n}{d}\!\!\right) \quad = \quad \binom{n+d-1}{n} \ .$$

Thus, the number of monomials of degree at most d in n variables is given by $\binom{n+d}{n}$.

1. Total boolean polynomials. The category of finite dimensional vector spaces give a denotational model for multiplicative additive linear logic. Adding the exponential is a non-trivial task and requires infinite dimensional spaces and thus, topology. Moreover, we need to find a subclass of spaces satisfying $E \simeq E^{**}$. Finiteness spaces (see [1]) give a solution. We won't need the details of this technology, but it is interesting to note that objects are topological vector spaces, and that morphisms (in the co-Kleisli category of the **!**-comonad) are "analytic functions", *i.e.* power series.

Of particular interest is the space $\mathbf{B}$ used to interpret the booleans: this is the vector space $\mathbf{k}^2$, where $\mathbf{k}$ is the ambient field. A morphism from $\mathbf{B}^n$ to $\mathbf{B}$ is a pair (P_1, P_2) of "finite" power series (polynomials) in $2n$ variables, where each pair (X_{2i-1}, X_{2i}) of variables corresponds to the i-th argument of the function.

A boolean value (a, b) is *total* if $a + b = 1$; and a pair of polynomials is *total* if it sends total values to total values. This means that a pair (P_1, P_2) of polynomials in $2n$ variables is total iff

$$a_1 + a_2 = 1,\ \ldots,\ a_{2n-1} + a_{2n} = 1 \quad \Rightarrow \quad P_1(a_1, \ldots, a_{2n}) + P_2(a_1, \ldots, a_{2n}) = 1 \ .$$

We first restrict our attention to the case of an infinite field $\mathbf{k}$: the above condition is then equivalent to the stronger condition (a pair of polynomials satisfying this condition is called *strongly total*)

$$(*) \quad P_1\big(X_1, 1-X_1, \ldots, X_{2n-1}, 1-X_{2n-1}\big) \ + \ P_2\big(X_1, 1-X_1, \ldots, X_{2n-1}, 1-X_{2n-1}\big) = 1 \ .$$

The proof of this is easy but interesting: refer to any algebra textbook ("Algebra" by Lang, corollary 1.7 in chapter IV for example) if you are in a hurry...

* Laboratoire de Mathématiques, Université de Savoie, 73376 Le Bourget-du-Lac Cedex, France

The constructions presented below also work for finite fields, but give a weaker result: see the remark at the end of section 5.

Lemma.

- *Strongly total polynomials form an affine subspace of* $\mathbf{k}[X_1,\ldots,X_{2n}] \times \mathbf{k}[X_1,\ldots,X_{2n}]$;
- *total polynomials form an affine subspace of* $\mathbf{k}[X_1,\ldots,X_{2n}] \times \mathbf{k}[X_1,\ldots,X_{2n}]$.

2. The centroidal calculus for boolean functions. The centroidal calculus produces pairs of polynomials (P_1, P_2) using

- constants: $\mathtt{T} := (1,0)$ and $\mathtt{F} := (0,1)$;
- pairs of variables: (X_1, X_2);
- $\mathtt{if}\ (P_1,P_2)\ \mathtt{then}\ (Q_1,Q_2)\ \mathtt{else}\ (R_1,R_2) := (P_1Q_1 + P_2R_1\ ,\ P_1Q_2 + P_2R_2)$;
- affine combinations: $\sum_{i=1}^n \alpha_i (P_{i,1}, P_{i,2})$ where $\sum_{i=1}^n \alpha_i = 1$.

A pair of polynomials is *centroidal* if it is generated by the above operations.

Lemma. *Centroidal polynomials form an affine subspace of* $\mathbf{k}[X_1,\ldots,X_{2n}] \times \mathbf{k}[X_1,\ldots,X_{2n}]$.

A note on terminology: "affine calculus" would be a much better name than "centroidal calculus"; but in the context of linear logic, this would lead to endless confusion.

The following proposition answers the natural question that was raised by Christine Tasson and Thomas Ehrhard:

Proposition. *Suppose the field* $\mathbf{k}$ *is infinite; then the spaces of centroidal polynomials and of total polynomials coincide.*

That centroidal polynomials are total is a direct consequence of their definition: all centroidal polynomials are in fact *strongly total*, in the sense of $(*)$. The rest of this note is devoted to the converse.

3. Tips and tricks for centroidal polynomials. Here is a collection of recipes for constructing centroidal polynomials:

- $(\alpha, 1-\alpha) := \alpha\,\mathtt{T} + (1-\alpha)\,\mathtt{F}$;
- $\neg(P_1,P_2) = (P_2,P_1) := \mathtt{if}\ (P_1,P_2)\ \mathtt{then}\ \mathtt{F}\ \mathtt{else}\ \mathtt{T}$;
- $(P_1,P_2) * (Q_1,Q_2) = (P_1Q_1\ ,\ P_1Q_2 + P_2) := \mathtt{if}\ (P_1,P_2)\ \mathtt{then}\ (Q_1,Q_2)\ \mathtt{else}\ \mathtt{F}$;*
- $(P_1,P_2)^+ = (P_1 + P_2\ ,\ 0) := \mathtt{if}\ (P_1,P_2)\ \mathtt{then}\ \mathtt{T}\ \mathtt{else}\ \mathtt{T}$;
- $\pi_1(P_1,P_2) = (P_1\ ,\ 1-P_1) := \mathtt{F} + (P_1,P_2)^+ - \neg(P_1,P_2)$.

Using those, we can get more complex centroidal polynomials:

(a) suppose P_1 is *any polynomial*; we can always get a centroidal term (P_1,P_2) for some polynomial P_2:
  - using "$\_ * \_$", we can get any monomial $(M,\ldots)$,
  - if M is such a monomial, α its coefficient in P_1 and m the total number of monomials in P_1, $(m\alpha M,\ldots) = \mathtt{if}\ (m\alpha, 1-m\alpha)\ \mathtt{then}\ (M,\ldots)\ \mathtt{else}\ \mathtt{F}$,
  - we can then sum those monomials using coefficients $1/m$ to get $(P_1,\ldots)$.

(b) If $(P_1, 0)$ is centroidal and if Q_1 is *any polynomial*, then $\big((P_1-1)Q_1, 1\big)$ is centroidal:
  - thanks to the previous point, we can obtain (Q_1,Q_2) for some Q_2,
  - $\big((P_1-1)Q_1, 1\big) = \big((Q_1,Q_2) * (P_1,0)\big) + \mathtt{F} - (Q_1,Q_2)$.

* This operation is neither commutative nor associative!

(c) If (P_1, P_2) is centroidal and if Q_1 is *any polynomial*, then $(P_1+Q_1\,,\,P_2-Q_1)$ is also centroidal: $(P_1+Q_1\,,\,P_2-Q_1) = (P_1,P_2)+(Q_1+Q_2,0)-(Q_2,Q_1)$

The last point implies in particular that it is equivalent to show that (P_1,P_2) is centroidal and to show that $(P_1+P_2,0)$ is centroidal.

4. An interesting vector space. Write $\mathbf{k}[X_1,\dots,X_n]_d$ for the vector space of polynomials of degree at most d. The operator $\varphi : \mathbf{k}[X_1,\dots,X_{2n}]_d \to \mathbf{k}[X_1,\dots,X_n]_d$ with

$$\varphi \quad : \quad P(X_1,\dots,X_{2n}) \;\mapsto\; P(X_1, 1-X_1,\dots,X_n,1-X_n)$$

is linear and surjective. Since the dimension of $\mathbf{k}[X_1,\dots,X_n]_d$ is $\binom{n+d}{n}$, we get

$$\dim\big(\ker(\varphi)\big) \quad = \quad \binom{2n+d}{2n} - \binom{n+d}{n}\ .$$

It is easy to see that the following polynomials are all in the kernel of φ:

$$\Big((X_1+X_2)^{i_1}\times\ldots\times(X_{2n-1}+X_{2n})^{i_n}-1\Big)\times X_1^{j_1}\times\ldots\times X_{2n-1}^{j_n}$$

where $(\sum_k i_k)+(\sum_k j_k)\le d$ and at least one of the i_k is non zero.

Lemma. *The above polynomials are linearly independent.*

Proof: suppose $\sum\alpha_k P_k = 0$ where each P_k is one of the above vectors. We show that the coefficient of any $\big((X_1+X_2)^{i_1}\dots(X_{2n-1}+X_{2n})^{i_n}-1\big)X_1^{j_1}\dots X_{2n-1}^{j_n}$ is zero by induction on $\sum_k j_k$.

- If $\sum_k j_k = 0$: since the linear combination is zero, this implies that the global coefficient of each monomial is zero. Since $(X_1+X_2)^{i_1}\dots(X_{2n-1}+X_{2n})^{i_n}-1$ is the only polynomial contributing to the monomial $X_2^{i_1}\dots X_{2n}^{i_n}$, its coefficient must be zero.
- The polynomial $\big((X_1+X_2)^{i_1}\dots(X_{2n-1}+X_{2n})^{i_n}-1\big)X_1^{j_1}\dots X_{2n-1}^{j_n}$ is the only polynomial contributing to $X_2^{i_1}\dots X_{2n}^{i_n}X_1^{j_1}\dots X_{2n-1}^{j_n}$ because, by induction hypothesis, all the polynomials with fewer X_{2k-1}'s have zero for coefficient. This implies that the above coefficient is also zero...

∎

Corollary. *The above polynomials form a basis for* $\ker(\varphi)$.

Proof: the number of those polynomials is exactly $\binom{2n+d}{2n}-\binom{n+d}{n}$:

- the first term accounts for the polynomials with $(\sum_k i_k)+(\sum_k j_k)\le d$,
- the second term removes the polynomials where all the i_k's are zero.

We have a family of $\binom{2n+d}{2n}-\binom{n+d}{n}$ linearly independent polynomials in a space of the same dimension: they necessarily form a basis.

∎

5. Back to total polynomials. Abusing our terminology, we say that a single polynomial P is total [resp. centroidal] if the pair $(P,0)$ is total [resp. centroidal].

We saw in section 3 that it is sufficient to show that all the total P are centroidal. Since the space of total polynomials is just the affine space $1+\ker(\varphi)$, the following polynomials form a basis for the space of total polynomials:

$$1\;+\;\Big((X_1+X_2)^{i_1}\times\ldots\times(X_{2n-1}+X_{2n})^{i_n}-1\Big)\times X_1^{j_1}\times\ldots\times X_{2n-1}^{j_n}$$

We thus only need to show that each element in this basis is indeed centroidal.

Each $(X_1+X_2,0)$ is centroidal, so that each $(X_1+X_2)^{i_1}\dots(X_{2n-1}+X_{2n})^{i_n}$ is also centroidal (using the "$\_*\_$" operation); we can find a centroidal $\big(X_1^{j_1}\dots X_{2n-1}^{j_n}\,,\,Q\big)$ and apply point *(b)* of section 3 to obtain

$$\Big(\big((X_1+X_2)^{i_1}\dots(X_{2n-1}+X_{2n})^{i_n}-1\big)X_1^{j_1}\dots X_{2n-1}^{j_n}\ ,\ 1\Big)$$

The "$\_^+$" operation allows to conclude the proof of the proposition.

Everything we've done so far also apply to finite fields, but the result we obtain is

Proposition. *Suppose the field* **k** *is finite; then the space of centroidal polynomials is exactly the space of "strongly total" polynomials (see* $(*)$ *in section 1). This space is a strict subspace of the space of total polynomials.*

Proof: we only need to show that centroidal polynomials are a strict subspace of total polynomials. Take the polynomial $1+X(X+1)(X+2)\dots(X+l)$ where $l+1$ is the cardinality of the field. This polynomial is total but not strongly total: it thus can't be encoded in the centroidal calculus.

∎

6. Some examples: the "parallel" or and Gustave's function. In order to write smaller formulas, we occasionally use a single letter P to denote a pair (P_1,P_2) of polynomials.

Using the usual encoding with the "`if`" primitive, the usual "or" function is easily programmed in the centroidal calculus:

$$P\vee Q \quad := \quad \texttt{if}\ P\ \texttt{then T else}\ Q = \big(P_1+P_2Q_1\ ,\ P_2Q_2\big)\ .$$

However, this function is not commutative: in general, $(P_1,P_2)\vee(Q_1,Q_2)$ is not the same as $(Q_1,Q_2)\vee(P_1,P_2)$, except for total values. To get a commutative version, one needs to use sums:

$$P\vee Q \quad := \quad \frac{1}{2}\ \texttt{if}\ P\ \texttt{then T else}\ Q\ +\ \frac{1}{2}\ \texttt{if}\ Q\ \texttt{then T else}\ P\ .$$

This "or" is indeed commutative, and `F` is neutral; but we do not have $(P_1,P_2)\vee\texttt{T}=\texttt{T}$.

The simplest really well-behaved "or" function seems to be the following:

$$\begin{aligned} P\vee Q \quad := & \quad\ \ \texttt{if}\ P\ \texttt{then T else}\ Q \\ & \quad +\texttt{if}\ Q\ \texttt{then T else}\ P \\ & \quad -\texttt{if}\ P\ \texttt{then}\ \big(\texttt{if}\ Q\ \texttt{then T else T}\big)\ \texttt{else}\ Q \\ = & \quad \big(P_1+Q_1-P_1Q_1\ ,\ P_2Q_2\big) \end{aligned}$$

This "or" function is commutative, has `F` as a neutral element and `T` as an absorbent element. It is the closest one can get to the real "parallel-or" which should be (see [3]):

$$P\parallel Q \quad = \quad \big(P_1+Q_1\ ,\ P_2Q_2\big)$$

but which is unfortunately not total.

Exercise: with the above "or", we have $\big(1/2\,,1/2\big)\vee\big(1/2\,,1/2\big)=\big(3/4\,,1/4\big)$. Design two other "or" functions which are truly commutative, have $(1,0)$ for absorbent element and $(0,1)$ for neutral element such that:

- $\big(1/2\,,1/2\big)\vee_1\big(1/2\,,1/2\big)=(1,0)$
- $\big(1/2\,,1/2\big)\vee_2\big(1/2\,,1/2\big)=(0,1)$

Gerard Berry's "Gustave function" is a ternary boolean function. It is the first and simplest example of stable but non-sequential function; and it can be shown to have polynomial

$$G(X_1, X_2, Y_1, Y_2, Z_1, Z_2) \quad = \quad \big(X_1Y_2 + Y_1Z_2 + Z_1X_2\ ,\ X_1Y_1Z_1 + X_2Y_2Z_2\big)$$

in Lefschetz totality spaces. It is trivial matter to check that this function is total. Here is one way to obtain it in the centroidal calculus:

- $P := (X * Y) * Z;$ $\qquad = \big(X_1Y_1Z_1\ ,\ X_2{+}X_1Y_2{+}X_1Y_1Z_2\big)$
- $Q := (\neg X * \neg Z) * \neg Y;$ $\qquad = \big(X_2Y_2Z_2\ ,\ X_1{+}X_2Z_1{+}X_2Y_1Z_2\big)$
- $R := \pi_1(Y * \neg Z);$ $\qquad = \big(Y_1Z_2\ ,\ 1{-}Y_1Z_2\big)$
- $S := \pi_1(X) + \neg X - \mathtt{T};$ $\qquad = \big(X_1{+}X_2{-}1\ ,\ 1\big)$
- $U :=$ `if` R `then` S `else` $\mathtt{T}$; $\qquad = \big(Z_2Y_1(X_1{+}X_2{-}1)\ ,\ 1\big)$
- $V :=$ `if` U `then` $\mathtt{T}$ `else` $\neg(X^+)$; $\qquad = \big(Z_2Y_1(X_1{+}X_2{-}1)\ ,\ X_1{+}X_2\big)$
- $H := P + Q - \neg(V^+);$ $\qquad = \big(X_1Y_1Z_1{+}X_2Y_2Z_2\ ,\ X_1Y_2{+}Y_1Z_2{+}Z_1X_2\big)$
- $G := \neg H.$

Expressing the corresponding polynomial in the basis given in section 5 seems to yield an even bigger centroidal expression:

$$\begin{aligned} X_1Y_2 + Y_1Z_2 + Z_1X_2 + X_1Y_1Z_1 + X_2Y_2Z_2 \quad = \quad & \Big((X_1+X_2)(Y_1+Y_2)(Z_1+Z_2)\Big) \\ & - \Big(\big((X_1+X_2)(Y_1+Y_2)-1\big)Z_1+1\Big) \\ & - \Big(\big((X_1+X_2)(Z_1+Z_2)-1\big)Y_1+1\Big) \\ & - \Big(\big((Y_1+Y_2)(Z_1+Z_2)-1\big)X_1+1\Big) \\ & + \Big(\big((X_1+X_2)-1\big)Z_1+1\Big) \\ & + \Big(\big((Y_1+Y_2)-1\big)X_1+1\Big) \\ & + \Big(\big((Z_1+Z_2)-1\big)Y_1+1\Big) \end{aligned}$$

where each basic polynomial can be expressed in the centroidal calculus using the recipes from section 3.

References

[1] Thomas Ehrhard, "Finiteness Spaces". *Mathematical Structures in Computer Science*, 15(04):615646, 2005.

[2] Thomas Ehrhard and Laurent Regnier, "The Differential λ-calculus". *Theoretical Computer Science*, 309:141, 2003.

[3] Christine Tasson, "Totality in an Algebraic Setting". Unpublished, 2008.

[4] Lionel Vaux, "On Linear Combinations of λ-Terms". *Lecture Notes in Computer Science, Term Rewriting and Applications*, 4533:374, 2007. See also [5]

[5] Lionel Vaux, "Algebraic λ-calculus". Submitted, 2008.