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 2\(n\) variables over an arbitrary field \(k\). 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 multi-
sets. The number of different monomials of degree \(d\) over \(n\) variables is usually denoted \(\binom{n}{d}\). A
simple counting argument shows that the number of monomials of degree at most \(d\) in \(n\) vari-
ables is \(\binom{n+1}{d}\). A closed formula for \(\binom{n}{d}\) in terms of the usual binomial coefficient is given
by:
\[
\binom{n}{d} = \binom{n + d - 1}{n}.
\]
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 \(B\) used to interpret the booleans: this is the vector
space \(k^2\), where \(k\) is the ambient field. A morphism from \(B^n\) to \(B\) 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 if
\[
a_1 + a_2 = 1, \ldots, a_{2n-1} + a_{2n} = 1 \quad \Rightarrow \quad P_1(a_1, \ldots, a_{2n}) + P_2(a_1, \ldots, a_{2n}) = 1.
\]
We first restrict our attention to the case of an infinite field \(k\): the above condition is then
equivalent to the stronger condition (a pair of polynomials satisfying this condition is called
strongly total)
\[
(*) \quad P_1 (X_1, 1 - X_1, \ldots, X_{2n-1}, 1 - X_{2n-1}) + P_2 (X_1, 1 - X_1, \ldots, X_{2n-1}, 1 - X_{2n-1}) = 1.
\]
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 $k[X_1, \ldots, X_{2n}] \times k[X_1, \ldots, X_{2n}]$;
- total polynomials form an affine subspace of $k[X_1, \ldots, X_{2n}] \times k[X_1, \ldots, X_{2n}]$.

2. **The centroidal calculus for boolean functions.** The centroidal calculus produces pairs of polynomials $(P_1, P_2)$ using
- constants: $T := (1, 0)$ and $F := (0, 1)$;
- pairs of variables: $(X_1, X_2)$;
- if $(P_1, P_2)$ then $(Q_1, Q_2)$ else $(R_1, R_2) := (P_1 Q_1 + P_2 R_1, P_1 Q_2 + P_2 R_2)$;
- 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 $k[X_1, \ldots, X_{2n}] \times k[X_1, \ldots, X_{2n}]$.

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 $k$ 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 $(\ast)$. 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:

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

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, $\alpha$ its coefficient in $P_1$ and $m$ the total number of monomials in $P_1$, $(m \alpha M, \ldots) := \text{if } (m \alpha, 1 - m \alpha) \text{ then } (M, \ldots) \text{ else } F$,
- we can then sum those monomials using coefficients $1/m$ to get $(P_1, \ldots)$.

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

\(^*\) 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: $(P_1 + Q_1, P_2 - Q_1) = (P_1, P_2) + (Q_1, Q_2) = (Q_2, Q_1)$

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 $k[X_1, \ldots, X_n]_d$ for the vector space of polynomials of degree at most $d$. The operator $\varphi : k[X_1, \ldots, X_n]_d \to k[X_1, \ldots, X_n]_d$ with

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

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

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

It is easy to see that the following polynomials are all in the kernel of $\varphi$:

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

where $(\sum_k i_k) + (\sum_k j_k) \leq d$ 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 $((X_1 + X_2)^{i_1} \ldots (X_{2n-1} + X_{2n})^{i_n} - 1) X_1^{j_1} \ldots X_{2n-1}^{j_n}$ is zero by induction on $\sum_k i_k$.

- If $\sum_k j_k = 0$: since the linear combination is zero, this implies that the global coefficient of each monomial is zero. Since $(X_1 + X_2)^{i_1} \ldots (X_{2n-1} + X_{2n})^{i_n} - 1$ is the only polynomial contributing to the monomial $X_1^{j_1} \ldots X_{2n-1}^{j_n}$, its coefficient must be zero.

- The polynomial $((X_1 + X_2)^{i_1} \ldots (X_{2n-1} + X_{2n})^{i_n} - 1) X_1^{j_1} \ldots X_{2n-1}^{j_n}$ is the only polynomial contributing to $X_1^{j_1} \ldots X_{2n-1}^{j_n}$ 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 $\sum_k i_k + \sum_k j_k \leq d$;

- 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:

$$1 + \left( (X_1 + X_2)^{i_1} \times \ldots \times (X_{2n-1} + X_{2n})^{i_n} - 1 \right) \times X_1^{j_1} \times \ldots \times X_{2n-1}^{j_n}$$
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 \((X_1 + X_2)^{i_1} \ldots (X_{2n-1} + X_{2n})^{i_n}\) is also centroidal (using the “\(\cdot *\)” operation); we can find a centroidal \((X_1^{i_1} \ldots X_{2n-1}^{i_n}, Q)\) and apply point \((b)\) of section 3 to obtain

\[
\left( ((X_1 + X_2)^{i_1} \ldots (X_{2n-1} + X_{2n})^{i_n} - 1) X_1^{i_1} \ldots X_{2n-1}^{i_n}, 1 \right)
\]

The “\(\cdot ^*\)” 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

\[
1 + X_1 (X_1 + 1) (X_2 + 2) \ldots (X_2 + l)
\]

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:

\[
P \lor Q := \text{if } P \text{ then } T \text{ else } Q = (P_1 + P_2 Q_1, P_2 Q_2).
\]

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

\[
P \lor Q := \frac{1}{2} \text{ if } P \text{ then } T \text{ else } Q + \frac{1}{2} \text{ if } Q \text{ then } T \text{ else } P.
\]

This “or” is indeed commutative, and \(F\) is neutral; but we do not have \((P_1, P_2) \lor T = T\).

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

\[
P \lor Q := \text{if } P \text{ then } T \text{ else } Q + \text{if } Q \text{ then } T \text{ else } P
= (P_1 + Q_1 - P_1 Q_1, P_2 Q_2)
\]

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]):

\[
P | Q = (P_1 + Q_1, P_2 Q_2)
\]

but which is unfortunately not total.

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

\[
\begin{align*}
1/2, 1/2 \lor_1 1/2, 1/2 &= (1,0) \\
1/2, 1/2 \lor_2 1/2, 1/2 &= (0,1)
\end{align*}
\]
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

\[ G(X_1, X_2, Y_1, Y_2, Z_1, Z_2) = (X_1Y_2 + Y_1Z_2 + Z_1X_2, X_1Y_1Z_1 + X_2Y_2Z_2) \]

in Lefschetz totality spaces. It is trivial matter to check that this function is total. Here is one example of stable but non-sequential function; and it can be shown to have polynomial

\[
\begin{align*}
& \text{Expressing the corresponding polynomial in the basis given in section 5 seems to yield an even bigger centroidal expression:} \\
& X_1Y_2 + Y_1Z_2 + Z_1X_2 + X_1Y_1Z_1 + X_2Y_2Z_2 = \\
& \quad \left((X_1 + X_2)(Y_1 + Y_2)(Z_1 + Z_2)\right) \\
& \quad - \left((X_1 + X_2)(Y_1 + Y_2) - 1\right)Z_1 + 1 \\
& \quad - \left((X_1 + X_2)(Z_1 + Z_2) - 1\right)Y_1 + 1 \\
& \quad - \left((Y_1 + Y_2)(Z_1 + Z_2) - 1\right)X_1 + 1 \\
& \quad + \left((X_1 + X_2) - 1\right)Z_1 + 1 \\
& \quad + \left((Y_1 + Y_2) - 1\right)X_1 + 1 \\
& \quad + \left((Z_1 + Z_2) - 1\right)Y_1 + 1
\end{align*}
\]

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

References


