Case Analysis, Variables and Parameters

Thierry Coquand

Preliminary version at October 22, 1998

1 Introduction

We explain how the formal description of the spectrum of a ring with its constructible topology, which is a boolean algebra associated to this ring, can be used to formalise the notion of case analysis with parameters. This notion is intuitively clear: for instance, we have an algebraic problem, like computing a Gröbner bases or solving a linear equation $mx + y = 1,\ x + my = 1$ that depends on a parameter m. According to some cases, here where $m^2 - 1 = 0$ or not, the problem has one, no or infinitely many solution. This notion of case analysis can be interpreted as working in a boolean model over a boolean algebra associated to the ring of parameters. This may be useful to structure some proofs and algorithms, like the one of computing a comprehensive Gröbner bases [BW91].

2 Spectrum of a Ring and Constructible Topology

We recall the construction of the spectrum of a ring [CC98].

Let A be a commutative ring. The relation $\mathcal{A} \vdash \mathcal{B}$ is defined to mean that the product of the elements of $\mathcal{B}$ belongs to the radical of the ideal generated by $\mathcal{A}$.

Theorem 2.1 *$\vdash$ is an entailment relation on A. It is the least entailment relation on A such that:*

- $\vdash 0$,
- $1 \vdash$,
- $x \vdash xy$,
- $xy \vdash x, y$,
- $x, y \vdash x + y$.

A point for this entailment relation is exactly a prime ideal of A.

We recall next the embedding of a distributive lattice in a boolean algebra [CC98].

Let D be a distributive lattice. We are interested in the following problem: to find a lattice map $i : D \to B$ from D in a boolean algebra B such that, if B' is any boolean algebra and $f : D \to B'$ any lattice map there exists a unique lattice map $f' : B \to B'$ such that $f'i = f$. We say that $B, i : D \to B$ is the boolean algebra *generated by* the distributive lattice D.

Let S be the set of elements $x \in D$ or $\bar{x}$ for $x \in D$. We define the relation $\vdash$ as follows: $x_i, \bar{y_j} \vdash z_k, \bar{t_l}$ iff $\wedge_i x_i \wedge \wedge_l t_l \leq \vee_j y_j \vee \vee_k z_k$ in D.

Theorem 2.2 *$\vdash$ is an entailment relation on S. If $B, i : S \to B$ is the distributive lattice generated by $S, \vdash$, then B is a boolean algebra, and $x \longmapsto i(x)$, $D \to B$ is the boolean algebra generated by D.*

Remark 2.1 If D is generated by an entailment relation $S_0, \vdash$ another entailment relation generating B is given by the set of elements $x \in S_0$ or $\bar{x}$ for $x \in S_0$ with the entailment relation: $x_i, \bar{y_j} \vdash z_k, \bar{t_l}$ iff $x_i, t_l \vdash y_j, z_k$ in S_0.

If we combine these two results, we get an entailment relation associated to any commutative ring A: the elements are of the form r or $\bar{r}$ for $r \in A$ and $x_i, \bar{y_j} \vdash z_k, \bar{t_l}$ iff the product of y_j, z_k belong to the radical of the ideal generated by x_i, t_l. The boolean algebra B associated to this entailment relation has a map $v : R \to B$ which is universal among the maps satisfying $v(ab) = v(a) \vee v(b)$ and $v(a)v(b) \leq v(a+b)$. In usual algebraic term, B is the boolean algebra associated to the spectrum of A for the constructible topology.

Remark 2.2 In the case $A = K[X_1, \ldots, X_n]$ where K is a decidable field, it follows from the existence of Gröbner bases [BW91] that B is a decidable boolean algebra.

3 Case Analysis

We explain how to use the previous results for case analysis, and in particular, how it can be used for computing "comprehensive Gröbner basis" [BW91]. This is based on the following result.

Theorem 3.1 *The map $A \times A \to B$, $(x, y) \longmapsto v(x - y)$ defines a boolean-valued equality on A, for which A is a decidable integral ring.*

This means that in the sense of the boolean model over B we can do "as if" A was a decidable integral ring.

Hence if we interpret intuitionistic proofs of existence in such a boolean model, we get a solution which covers all the possible cases for the parameters.

One example is for Gröbner's basis: we have a family of polynomials in

$$K[u_1, \ldots, u_n][X_1, \ldots, X_m]$$

and we want to compute its Gröbner's basis, looking at $u_1, \ldots, u_n$ as *parameters* and $X_1, \ldots, X_m$ as *variables*. We take $A = K[u_1, \ldots, u_n]$ and we work in the boolean model over B, $v : A \to B$. In this boolean model, A is an integral ring with a decidable equality, hence *in the sense of this model* there exists a Gröbner basis (see [CP98] for an intuitionistic description of such a model). When we look at what is such a basis "externally", we get a finite trees which covers all the possibilities for the parameters. The leaves of this tree are Gröbner bases in each possibilities. (Notice that in this case, B has a decidable equality.)

This is of course closely related to the dynamical algebra approach [CLR86].

References

[BW91] T. Becker and V. Weispfenning. *Gröbner Bases.* Springer-Verlag, 1991.

[CC98] J. Cederquist and Th. Coquand. Entailment relations and distributive lattices. *submitted*, 1998.

[CLR86] M. Coste, H. Lombardi, and M.F. Roy. Dynamical method in algebra: Effective nullstellensätze. *Preprint*, 1986.

[CP98] Th. Coquand and E. Palmgren. Intuitionistic choice and classical logic. *To appear in Archive for Mathematical Logic*, 1998.