Homotopy Type Theory MPIM-Bonn 2016

Dependent Type Theories

Lecture 4. Computing the B-sets for C-systems $CC(\mathbf{RR})[\mathbf{LM}]$. The term C-systems of type theories.

By Vladimir Voevodsky

from Institute for Advanced Study in Princeton, NJ.

February, 2016

In the previous lecture we described two methods of constructing new C-systems from the existing ones.

In one method one starts with a C-system CC and a presheaf of sets F on the category underlying CC and constructs a new C-system $CC[F]$ that is called the F-extension of CC.

In another method one starts with a C-system CC and describes its B-sets $(B(CC), \widetilde{B}(CC))$ and the action of the B-system operations

$$pt, ft, \partial, T, \widetilde{T}, S, \widetilde{S}, \delta$$

on these sets. Then one uses a bijection between the pairs of subsets

$$B' \subset B(CC) \qquad \widetilde{B}' \subset \widetilde{B}(CC)$$

that are closed under these operations and C-subsystems CC' of CC.

Our goal in this lecture is to obtain the term C-systems of type theories with two kinds of judgements

$$\Gamma \triangleright Ok$$

$$\Gamma \triangleright o : T$$

as particular cases of our general constructions. As an application we will obtain the list of necessary and sufficient conditions that the sets of valid judgements of these two kinds have to satisfy in order for them to correspond to a type theory that has a term C-system.

We start with reminding the construction of a Lawvere theory from a monad **RR** on $Sets(U)$.

This construction can be factored into the composition of two construction - a very elementary "forgetting" construction from monads on $Sets(U)$ to relative monads on the functor $Jf : F \to Sets(U)$ followed by a construction of a Lawvere theory from a Jf-relative monad.

However, since we will not need the equivalence of categories result established in "Lawvere theories and Jf-relative monads" we may proceed directly from monads to Lawvere theories.

Let $\mathbf{RR} = (R, \eta, \mu)$ be a monad on $Sets(U)$. Let $F(\mathbf{RR})$ be the category whose set of objects is $\mathbf{N}$ and morphisms are given by

$$Mor(F(\mathbf{RR})) = \amalg_{m,n\in\mathbf{N}} Fun(stn(m), R(stn(n)))$$

Note that here again we can not use $\cup$ instead of $\amalg$ because the codomain function on the union will not be defined if $R(stn(n)) = R(stn(n'))$ for some $n \neq n'$. The identity morphisms are given by

$$Id_n = ((n, n), \eta(n))$$

and the composition by

$$((k, m), f) \circ ((m, n), g) = ((k, n), f \circ (R(g) \circ \mu(stn(n))))$$

The verification of the associativity and unity axioms is straightforward.

Lemma 1 *Let*

$$L_{\mathbf{RR},Ob} : Ob(F) \to Ob(F(\mathbf{RR}))$$

be the identity function and let

$$L_{\mathbf{RR},Mor} : Mor(F) \to Mor(F(\mathbf{RR}))$$

be the function given by

$$L_{\mathbf{RR},Mor}(f) = ((dom(f), codom(f)), f \circ \eta(n)).$$

Then $L_{\mathbf{RR}} = (L_{\mathbf{RR},Ob}, L_{\mathbf{RR},Mor})$ *is a functor that defines a Lawvere theory structure on* $F(\mathbf{RR})$*.*

For a detailed proof in the somewhat more general case of a relative monad see "Lawvere theories and Jf-relative monads".

Let us denote the C-system $LC(F(\mathbf{RR}), L)$ by $CC(\mathbf{RR})$ so that in particular, as a category

$$CC(\mathbf{RR}) = (F(\mathbf{RR}))^{op}.$$

We want to describe the B-sets and the B-system operations for the C-systems of the form $CC(\mathbf{RR})[\mathbf{LM}]$. Here, the notation $\mathbf{LM}$ for presheaves on $CC(\mathbf{RR})$ comes from the fact that such presheaves are precisely the left modules over the Jf-relative monad defined by $\mathbf{RR}$.

Unfortunately, in the ZF, the description that we will give and that we will use to establish the connection with the real world type theories does not extend to the more general case of C-systems $LC(T, L)[\mathbf{LM}]$.

The problem is due to the impossibility of constructing a Lawvere theory with

$$Mor(L(1), L(m)) = R(stn(m))$$

because the sets on the left hand side must be distinct for $m \neq m'$ while the sets on the right hand side may coincide for different m. This problem does not arise in the Univalent foundations and there one can make the computation a little more general.

Among the presheaves that we will consider will be the presheaf given by the formulas:

$$RR_{Ob}(n) = R(stn(n))$$

and

$$RR_{Mor}((m,n),f) = R(f)\circ\mu(n)$$

It is easy to construct an isomorphism $(RR_{Ob}, RR_{Mor}) \rightarrow Yo(L(1))$ where $Yo(L(1))$ is the presheaf represented by $L(1) = 1$. However this isomorphism is not an identity due to the fact that

$$Yo(L(1))(L(n)) = Mor_{CC(R)}(L(n), L(1)) =$$

$$\{((1,n),f)\,|\,f\in Fun(stn(1), R(stn(n)))\}$$

and this set is not equal to the set $RR(n) = R(stn(n))$.

Let

$$B(\mathbf{RR}, \mathbf{LM}) = \coprod_{n \in \mathbf{N}} LM(0) \times \ldots \times LM(n-1)$$

and

$$\widetilde{B}(\mathbf{RR}, \mathbf{LM}) = \coprod_{n \in \mathbf{N}} LM(0) \times \ldots \times LM(n) \times RR(n)$$

Then, by construction,

$$B(CC(\mathbf{RR})[\mathbf{LM}]) = B(\mathbf{RR}, \mathbf{LM})$$

In the next few slides we will construct a bijection

$$mb_{\mathbf{RR},\mathbf{LM}} : \widetilde{B}(CC(\mathbf{RR})[\mathbf{LM}]) \to \widetilde{B}(\mathbf{RR}, \mathbf{LM})$$

Then we will compute the operations on $(B(\mathbf{RR}, \mathbf{LM}), \widetilde{B}(\mathbf{RR}, \mathbf{LM}))$ obtained by transport of the B-system operations for $CC(\mathbf{RR})[\mathbf{LM}]$ through the pair of bijections $(Id, mb_{\mathbf{RR},\mathbf{LM}})$.

Pairs of subsets invariant under these operations in

$$(B(\mathbf{RR}, \mathbf{LM}), \widetilde{B}(\mathbf{RR}, \mathbf{LM}))$$

will correspond to C-subsystems of $CC(\mathbf{RR})[\mathbf{LM}]$ through the composition of two bijections - the bijection $(B', \widetilde{B}') \mapsto (B', mb^{-1}(\widetilde{B}'))$ followed by the bijection of the C-subsystems theorem.

Recall, that by the definition of a Lawvere theory the square

$$\begin{array}{ccc} L(n+1) & \xrightarrow{L(ii_1^{n,1})} & L(1) \\ {\scriptstyle L(ii_0^{n,1})}\downarrow & & \downarrow \\ L(n) & \longrightarrow & L(0) \end{array}$$

is a pull-back square in $CC(\mathbf{RR}) = (F(\mathbf{RR}))^{op}$.

Therefore, by a general lemma about pull-back squares and taking into account that $L(0)$ is a final object we see that the mapping

$$s \mapsto s \circ L(ii_1^{n,1})$$

is a bijection from the sections of $L(ii_0^{n,1})$ to morphisms $L(n) \to L(1)$. Since the morphism $L(ii_0^{n,1})$ is, by construction, $p_{L(n+1)}$ we obtain a bijection from sections of $p_{L(n+1)}$ to $Mor_{CC(\mathbf{RR})}(L(n), L(1))$. Let us denote this bijection b_1.

Next we have

$$Mor_{CC(\mathbf{RR})}(L(n), L(1)) = \{((1,n), f) \mid f \in Fun(stn(1), R(stn(n)))\} =$$
$$\{((1,n), f) \mid f \in Fun(stn(1), RR(n))\}$$

Let

$$b_2 : Mor_{CC(\mathbf{RR})}(L(n), L(1)) \to RR(n)$$

be "the obvious bijection", i.e., the bijection given in the forward direction by

$$b_2((1,n), f) = f(0)$$

Then $ss \mapsto b_2(b_1(ss))$ gives us a bijection from the subset of $Mor(CC(\mathbf{RR}))$ that consists of sections of p_{n+1} to $RR(n)$.

From the definitions one computes that elements of $\widetilde{B}(CC(\mathbf{RR})[\mathbf{LM}])$ are iterated pairs of the form

$$(((n, ft(\Gamma)), (n+1, \Gamma)), ss)$$

where $\Gamma \in LM(0) \times \ldots \times LM(n)$ and ss is a section of p_{n+1}. We define $mb_{\mathbf{RR},\mathbf{LM}}$ as the function

$$mb_{\mathbf{RR},\mathbf{LM}} : \widetilde{B}(CC(\mathbf{RR})[\mathbf{LM}]) \to \widetilde{B}(\mathbf{RR}, \mathbf{LM})$$

given by the formula

$$mb_{\mathbf{RR},\mathbf{LM}}(((n, ft(\Gamma)), (n+1, \Gamma)), ss) = (n, (\Gamma, b_2(b_1(ss))))$$

Knowing that b_1 and b_2 are bijections one proves easily that $mb_{\mathbf{RR},\mathbf{LM}}$ is a bijection.

Let me remind that we have

$$B(\mathbf{RR},\mathbf{LM}) = \coprod_{n\in\mathbf{N}} LM(0)\times\ldots\times LM(n-1)$$

$$\widetilde{B}(\mathbf{RR},\mathbf{LM}) = \coprod_{n\in\mathbf{N}} LM(0)\times\ldots\times LM(n)\times RR(n)$$

Let us describe the operations $ft, \partial, T, \widetilde{T}, S, \widetilde{S}, \delta$ on these two sets. I will not provide the actual computation that can be found in "C-system of a module over a Jf-relative monad" but will only describe the answer.

For ft and ∂ we have

$$ft(n,(T_0,\ldots,T_{n-2},T_{n-1})) = (max(n-1,0),(T_0,\ldots,T_{n-2}))$$

and

$$\partial(n,(T_0,\ldots,T_n,r)) = (n+1,(T_0,\ldots,T_n))$$

For $E \in LM(m)$ and $f : m \to n$ in F we write $f(E)$ instead of $LM_{Mor}(L(f))(E)$.

This agreement applies in particular to the presheaf **RR** so that for $r \in RR(m)$ and $f : m \to n$ in F we write $f(r)$ instead of $RR_{Mor}(L(f))(r)$

For $n \in \mathbf{N}$ and $i = 0, \ldots, n-1$, let $x_i^n \in RR(n) = R(stn(n))$ be the element given by $x_i^n = \eta(n)(i)$. When n is clear from the context we will write x_i instead of x_i^n.

We will need two series of morphisms in F.

For $m, i \in \mathbf{N}$,

$$\iota_m^i : stn(m) \to stn(m+i)$$

of the form $(fun\, x \Rightarrow x)$ and for $m \in \mathbf{N}$ and $0 \leq i \leq m$

$$\partial_m^i : stn(m) \to stn(m+1)$$

which is the increasing inclusion that does not take the value i.

The last ingredient that we need are operations $\theta^{\mathbf{LM}}_{m,n}$ of the form

$$\theta^{\mathbf{LM}}_{m,n} : RR(m) \times LM(n) \to LM(n-1)$$

defined for all $n, m \in \mathbf{N}$ such that $n > m$.

To define these operations we will use the representation of morphisms in $CC(\mathbf{RR})$ in the form of sequences $(r_0, \ldots, r_{m-1})$ where $r_i \in RR(n)$. Such a sequence defines an element in $Fun(stn(m), RR(n))$ and therefore a morphism $n \to m$ in $CC(\mathbf{RR})$.

For example, the sequence $(x^n_0, \ldots, x^n_{n-1})$ represents the morphism

$$((n, n), \eta(n))$$

i.e., the identity morphism of n.

The operation

$$\theta^{\mathbf{LM}}_{m,n} : RR(m) \times LM(n) \to LM(n-1)$$

is given by the formula:

$$\theta^{LM}_{m,n}(r, E) = LM_{Mor}(x_0, \ldots, x_{m-1}, \iota^{n-m-1}_m(r), x_m, \ldots, x_{n-2})(E)$$

The sequence

$$(x_0, \ldots, x_{m-1}, \iota^{n-m-1}_m(r), x_m, \ldots, x_{n-2})$$

has n terms that belong to $RR(n-1)$ and so represents an element in $Mor_{CC(\mathbf{RR})}(n-1, n)$. We apply to it LM_{Mor} obtaining a function $LM(n) \to LM(n-1)$ and act by it on E.

We will usually write θ instead of $\theta^{LM}_{m,n}$ because the arguments LM, m and n can be inferred from the remaining two arguments.

We are now ready to describe the action of the operations $T, \widetilde{T}, S, \widetilde{S}$ on the sets $B = B(\mathbf{RR}, \mathbf{LM})$, $\widetilde{B} = \widetilde{B}(\mathbf{RR}, \mathbf{LM})$

Theorem 2 *Operation* T *is defined on the set of pairs* $(m,\Gamma),(n,\Gamma')$ *in* B *where* $\Gamma=(T_0,\dots,T_{m-2},T)$, $\Gamma'=(T_0,\dots,T_{n-1})$ *with* $n>m-1$ *and* $m>0$. *It takes values in* B *and is given by*

$$T((m,\Gamma),(n,\Gamma'))=$$

$$(n+1,(T_0,\dots,T_{m-2},T,\partial_{m-1}^{m-1}(T_{m-1}),\dots,\partial_{n-1}^{m-1}(T_{n-1})))$$

Operation $\widetilde{T}$ *is defined on the set of pairs* $(m,\Gamma)\in B$, $(n,(\Gamma',s))\in\widetilde{B}$ *where* $\Gamma=(T_0,\dots,T_{m-2},T)$, $\Gamma'=(T_0,\dots,T_{n-1})$ *with* $n+1>m-1$ *and* $m>0$. *It takes values in* $\widetilde{B}$ *and is given by*

$$\widetilde{T}((m,\Gamma),(n,(\Gamma',s)))=(n+1,(T((m,\Gamma),(n,\Gamma')),\partial_n^{m-1}(s)))$$

Operation S *is defined on the set of pairs* $(m,(\Gamma,r))\in\widetilde{B}$, $(n,\Gamma')\in B$ *where* $\Gamma=(T_0,\dots,T_m)$, $\Gamma'=(T_0,\dots,T_{n-1})$ *such that* $n-1>m$. *It takes values in* B *and is given by*

$$S((m,(\Gamma,r)),(n,\Gamma'))=$$

$$(n-1,(T_0,\dots,T_{m-1},\theta(r,T_{m+1}),\theta(r,T_{m+2}),\dots,\theta(r,T_{n-1})))$$

Operation $\widetilde{S}$ *is defined on the set of pairs* $(m,(\Gamma,r)),(n,(\Gamma',s))\in\widetilde{B}$ *where* $\Gamma=(T_0,\dots,T_m)$, $\Gamma'=(T_0,\dots,T_n)$ *such that* $n>m$. *It takes values in* $\widetilde{B}$ *and is given by*

$$\widetilde{S}((m,(\Gamma,r)),(n,(\Gamma',s)))=(n-1,(S((m,(\Gamma,r)),(n+1,\Gamma'))),\theta(r,s))$$

Operation δ *is defined on the subset of* (m, Γ) *in* B *such that* $m > 0$*. It takes values in* $\widetilde{B}$ *and is given by*

$$\delta(m, \Gamma) = (m, (T((m, \Gamma), (m, \Gamma)), x_{m-1}))$$

Let us consider now the following special case. Define a binding arity as a sequence $(n_1, \ldots, n_d)$ of natural numbers. Let BAr be the set of binding arities. Define a binding signature as a pair $\Sigma = (Op, Ar)$ where Op is a set whose elements are called operations and $Ar : Op \to BAr$ is a function.

For any binding signature Σ and any universe U one can construct a monad $\mathbf{RR}_\Sigma$ on $Sets(U)$. The value of the object part of this monad on a set X is the set of "α-equivalence classes of expressions under Σ with free variables from X". The functor and the monad structures on $\mathbf{RR}_\Sigma$ is given by "capture free substitution".

There is very interesting and non-trivial theory of such monads with the main references being the foundational 1999 paper by Fiore, Plotkin and Turi and the 2007 and 2010 papers by Hirschowitz and Maggesi.

I will illustrate these concepts on examples since we have no time to go into the mathematical construction of $\mathbf{RR}_\Sigma$.

The first group of examples arises when all the arities are of the form $(0, \ldots, 0)$. Such arities are called algebraic. Then Σ can be viewed as the usual algebraic signature where the arity of an operation is the number of 0's in its binding arity. Given such a Σ and a set X one defines the set of expressions under Σ with variables from X in a usual way. For example one can define $\mathbf{RR}_\Sigma(X)$ as the free structure on the set of generators X with the set of operations Op where $P \in Op$ is an operation with d variables where d is the number of 0's in $Ar(P)$.

The monad in this case is the well-known monad of free algebraic structures under a given signature.

The second group of examples is obtained from the single sorted predicate logic theory without function symbols. Then one has quantifiers $\forall$ and $\exists$, operations $\vee$, $\wedge$, $\neg$ and $\Rightarrow$ and a set Pr of predicates with a function $A : Pr \to \mathbf{N}$ giving the number of arguments for a predicate (this needs to be encoded in the ZF but we will ignore this step of the construction).

Formulas in this theory with variables in all free occurrences being from a set X and considered up to the equivalence relation generated by renaming of bound variables form a set $\mathbf{RR}_\Sigma(X)$ and using properly defined substitution one can make these sets into a monad. The binding signature in this case is given by $Op = \{\forall, \exists, \vee, \wedge, \neg, \Rightarrow\} \cup Pr$ with the arities being

$$Ar(\forall) = (1) \quad Ar(\exists) = (1)$$

$$Ar(\vee) = (0,0) \quad Ar(\wedge) = (0,0) \quad Ar(\neg) = (0) \quad Ar(\Rightarrow) = (0,0)$$

$$\text{for } P \in Pr, \quad Ar(P) = (0,\ldots,0) \text{ where the number of 0's is } A(P)$$

The binding signature of the Martin-Lof type theory MLTT78 described in the paper "Constructive mathematics and computer programming" contains 3 operations with the signature $(1, 0)$, one operation with signature (1), one operation with signature $(0, 2)$, one with $(0, 1, 1)$, one with $(0, 0, 2)$, one with $(0, 3)$ and many, including some infinite series, algebraic operations. See p. 158 of the "Constructive mathematics" paper.

For such monads, since the monad structure is given by actual substitution, our abstract formulas specialize into a much more familiar form. Here is how operations T and S look like in the case $\mathbf{RR} = \mathbf{RR}_\Sigma$ and $\mathbf{LM} = \mathbf{RR}$.

First we need to express ι^i_m, ∂^i_m and $\theta_{m,n}$ in terms of substitutions. We consider $RR(m) = R_\Sigma(stn(m))$, i.e., expressions with free variables being natural numbers $0, \dots, m-1$. This is a little inconvenient for presentation and we will write x_i instead of i. Then

$$x^n_i = x_i \in RR(n)$$

$$\iota^i_n(E) = E, \text{ the same expression considered as an element of } RR(n+i).$$

$$\partial^i_n(E) = E[x_{i+1}/x_i, x_{i+2}/x_{i+1}, \dots, x_n/x_{n-1}]$$

$$\theta_{i,n}(r, E) = E[r/x_i, x_i/x_{i+1}, \dots, x_{n-2}/x_{n-1}]$$

Elements of $B(\mathbf{RR}, \mathbf{RR})$ are pairs $(n, (T_0, \ldots, T_{n-1}))$ where T_i is an expression in variables $x_0, \ldots, x_{i-1}$. They can be written as

$$(T_0, \ldots, T_{n-1})\, Ok$$

Elements of $\widetilde{B}(\mathbf{RR}, \mathbf{RR})$ are pairs $(n, (T_0, \ldots, T_n, r))$ where T_i is an expression in variables $x_0, \ldots, x_{i-1}$ and r is an expression in variables $(x_0, \ldots, x_{n-1})$. They can be written as

$$(T_0, \ldots, T_{n-1} \rhd r : T_n)$$

The actions of T and $\widetilde{T}$ produce an insertion of one additional T-expression with the shift of numbers of variables in the following expressions. This is known in the type theory as *weakening*.

The actions of S and $\widetilde{S}$ produce the removal of one T-expression followed by the replacement of one of the variables in the following expressions by the r-argument of the operation and a shift of numbers of variables. This is known in type theory as the *substitution operation*.

The action of δ takes $(T_0, \ldots, T_n)\,Ok$ to $(T_0, \ldots, T_n \rhd x_n : T_n)$.

We conclude that any pair of sets of sequences of the form $(T_0, \ldots, T_{n-1})$ and $(T_0, \ldots, T_n \rhd r : T_n)$ that is closed under truncation (this is the ft), removal of r (this is ∂), weakening, substitution and contains elements of the form $(T_0, \ldots, T_n \rhd x_n : T_n)$ defines a C-system.

When these subsets are the subsets of valid judgements of a type theory the C-system that one obtains is called the term C-system of the type theory.