Journal of Universal Computer Science, vol. 6, no. 1 (2000), 194-200
submitted: 15/6/99, accepted: 2/11/99, appeared: 28/1/00

On Equational Craig Interpolation[1,2]

Grigore Roşu
(Department of Computer Science & Engineering, University of California,San Diego[3]
Email: grosu@cs.ucsd.edu.)

Joseph Goguen
(Department of Computer Science & Engineering, University of California, San Diego
Email: goguen@cs.ucsd.edu.)

Abstract: Generalizations of Craig interpolation are investigated for equational logic. Our approach is to do as much as possible at a categorical level, before drawing out the concrete implications.

1 Introduction

The Craig interpolation lemma is a well known fixture of first order logic [Cra57]. It says that, given sentences φ, ψ such that $\varphi \vdash \psi$, there is some sentence ρ, called an interpolant, such that $\varphi \vdash \rho$ and $\rho \vdash \psi$ where $|\rho| \subseteq |\varphi| \cap |\psi|$, where $|\alpha|$ denotes the set (or more precisely, the signature) of non-logical symbols in a sentence α. Part of the original motivation for this result came from the methodology of science, where the sentences[4] would be logical theories of (e.g.) physical phenomena. For a sample application, suppose that φ and ψ have no non-logical symbols in common and that ψ is not a tautology; then the interpolant must consist of only logical symbols, from which we conclude that $\varphi \vdash \psi$ is impossible. This implies[5] that a physical theory cannot be applied directly to yield results about a completely different domain. For applications of Craig interpolation to the relationship between module algebra and information hiding, the reader may see [BHK90, DGS93].

This paper focuses on Craig interpolation for equational logic. The situation here is perhaps a bit delicate. In fact, Craig interpolation does not hold for the usual formulation of equational logic, where sentences are simple equations. However, as pointed out in [RvG88, Rod91], it does hold if we add conjunction to equational logic, so that sentences are conjunctions of equations; this holds for both finite and infinite conjunctions. This paper takes a similar point of view, in which sentences may be arbitrary sets of equations, so that for us Craig interpolation says that if E_1 and E_2 are sets of Σ_1-equations and Σ_2-equations, respectively, such that $E_1 \models_{\Sigma_1 \cup \Sigma_2} E_2$, then there is a set of $(\Sigma_1 \cap \Sigma_2)$-equations I (called an *interpolant*) such that $E_1 \models_{\Sigma_1} I$ and $I \models_{\Sigma_2} E_2$.

[1] C. S. Calude and G. Ştefănescu (eds.). *Automata, Logic, and Computability. Special issue dedicated to Professor Sergiu Rudeanu Festschrift.*
[2] Supported by NSF grant CCR-9901002.
[3] Also Fundamentals of Computing, Faculty of Mathematics, University of Bucharest, Romania.
[4] These are generally conjunctions of finite sets of closed first order formulae.
[5] Provided that one accepts some form of logical positivism, which relatively few philosophers today are prepared to do.

We generalize this in two directions. First, we show that it holds for more general pushouts of signatures than those given by union and intersection, in fact, for those pushouts where the morphism with target Σ_2 is injective. A counter example is given showing that the result does not hold in general when that morphism is not injective. Second, we investigate different kinds of equations as sentences, and even more generally, formulae in universally quantified first order logic with equality. We show that the equations in E_1 can be conditional, and that the kind of equations in the interpolant is given by the kind of equations in E_2. For example, if E_2 contains universally quantified first order formulae[6] then the interpolant can contain only conditional equations, and if E_2 contains only unconditional equations then the interpolant can also contain only unconditional equations.

Inspired by the elegant work of Rodenburg [Rod91], we use Birkhoff axiomatizability results [Bir35] for equational logic. This paper first gives a categorical formulation and proof, and then instantiates that to obtain various forms of equational Craig interpolation. We assume a general familiarity with the basics of algebraic specification and category theory, for which see e.g. [GM96, Lan71, EM85].

Acknowledgement This paper is dedicated to Professor Sergiu Rudeanu. The first authour wishes to thank Professor Rudeanu for introducing him to Birkhoff axiomatizability at the University of Bucharest.

2 A Categorical Formulation

We formulate and prove the interpolation result categorically, in the spirit of the algebraic proof by Rodenburg [Rod91]. It is worth mentioning that there also exist constructive proofs of the classic equational interpolation in the literature, for example [RvG88, Pig74].

In this section, consider categories that distinguish two classes of morphisms, **S** and **H**, both including all identities. The morphisms in **S** can be thought as subobject inclusions and those in **H** as surjections[7]. To simplify the writing, we ambigously use the same symbols **S** and **H** for all categories. Given a class of objects $\mathcal{Q}$, $\mathbf{S}(\mathcal{Q})$ represents the class of objects which are sources of morphisms in **S** of target in $\mathcal{Q}$; it can be thought as closure under subobjects. Dually, $\mathbf{H}(\mathcal{Q})$ represents the class of objects which are targets of morphisms in **H** with source in $\mathcal{Q}$; it can be thought as closure under quotients. We adopt the usual notation $\mathbf{P}(\mathcal{Q})$ for closure under products. Let $\mathbf{HSP}(\mathcal{Q})$ be a shorthand for $\mathbf{H}(\mathbf{S}(\mathbf{P}(\mathcal{Q})))$, and similarly for $\mathbf{S}(\mathbf{P}(\mathcal{Q}))$, etc.

Definition 1. A functor $\mathcal{U}\colon \mathcal{C} \to \mathcal{D}$ is **H-source creating** iff for every morphism $D \to \mathcal{U}(C)$ in **H** there is an object $C' \in |\mathcal{C}|$ and a morphism $C' \to C$ in **H** such that $D = \mathcal{U}(C')$. Dually, $\mathcal{U}$ is **S-target creating** iff for every morphism $\mathcal{U}(C) \to D$ in **S** there is an object $C' \in |\mathcal{C}|$ and a morphism $C \to C'$ in **S** such that $D = \mathcal{U}(C')$.

[6] Note that these include the conditional equations.
[7] We adopt this notation for historical reasons.

Example 1. If $\varphi\colon \Sigma \to \Sigma'$ is an injective morphism of equational signatures, then the usual forgetful functor $\_\!\restriction_\varphi\colon \mathbf{Alg}_{\Sigma'} \to \mathbf{Alg}_{\Sigma}$ is both $\mathbf{H}$-target and $\mathbf{S}$-source creating, where $\mathbf{H}$ and $\mathbf{S}$ contain the surjective homomorphisms and inclusions, respectively.

The reader is referred to [Rod91] for a proof when φ is an inclusion of many-sorted signatures. It is realatively easy to see that no major changes appear when φ is injective and we only sketch the construction of C'. Given a Σ'-algebra C and a Σ-algebra D, then intuitively C' is obtained from C "expunging $C\!\restriction_\varphi$ and plugging in D instead". Technically, $C'_{s'}$ is D_s whenever $s' = \varphi(s)$, and $C_{s'}$ otherwise, for all sorts s' in Σ', and $C'_{\sigma'}$ is D_σ whenever $\sigma' = \varphi(\sigma)$. Suppose that there is some surjective morphism $e\colon D \to C\!\restriction_\varphi$; then for an operation σ' in $\Sigma'_{\varphi(s_1)\ldots\varphi(s_i)s'_{i+1}\ldots s'_k,s'}$ which is not in the image of φ, $C'_{\sigma'}(d_1,...,d_i,c_{i+1},...,c_k)$ is defined as $C_{\sigma'}(e_{s_1}(d_1),...,e_{s_i}(d_i),c_{i+1},...,c_k)$ if s' is not in the image of φ, and any element d in D_s with $e_s(d) = C_{\sigma'}(e_{s_1}(d_1),...,e_{s_i}(d_i),c_{i+1},...,c_k)$ if $s' = \varphi(s)$. On the other hand, if there is some inclusion morphism $C\!\restriction_\varphi \hookrightarrow D$ then $C'_{\sigma'}(d_1,...,d_i,c_{i+1},...,c_k)$ is defined as $C_{\sigma'}(c_1,...,c_i,c_{i+1},...,c_k)$ if $d_j = c_j \in C_{\varphi(s_j)}$ for all $1 \le j \le i$, and any element in $C'_{s'}$ otherwise. These constructions are not ambiguous, because φ is injective.

Definition 2. Given two functors $\mathcal{V}\colon \mathcal{A}_1 \to \mathcal{A}$ and $\mathcal{U}\colon \mathcal{A}_2 \to \mathcal{A}$ and classes of objects $\mathcal{Q}_1 \subseteq |\mathcal{A}_1|$ and $\mathcal{Q}_2 \subseteq |\mathcal{A}_2|$, then a $(\mathcal{V},\mathcal{U})$**-interpolant for** $(\mathcal{Q}_1,\mathcal{Q}_2)$ (or simply an **interpolant** when $\mathcal{V},\mathcal{U},\mathcal{Q}_1$ and $\mathcal{Q}_2$ are clear from the context) is a class of objects $\mathcal{Q} \subseteq |\mathcal{A}|$ such that $\mathcal{V}(\mathcal{Q}_1) \subseteq \mathcal{Q}$ and $\mathcal{U}^{-1}(\mathcal{Q}) \subseteq \mathcal{Q}_2$.

Theorem 3. *Suppose that the following is a pullback in* $\mathbf{Cat}$

$$\begin{tikzcd}
& \mathcal{A}' \arrow[dl, "\mathcal{U}'"'] \arrow[dr, "\mathcal{V}'"] & \\
\mathcal{A}_1 \arrow[dr, "\mathcal{V}"'] & & \mathcal{A}_2 \arrow[dl, "\mathcal{U}"] \\
& \mathcal{A} &
\end{tikzcd}$$

such that $\mathcal{V}$ is product preserving and $\mathcal{U}$ is $\mathbf{S}$-target creating, and that $\mathcal{Q}_1 \subseteq |\mathcal{A}_1|$ and $\mathcal{Q}_2 \subseteq |\mathcal{A}_2|$ are classes of objects such that $\mathcal{Q}_1 = \mathbf{P}(\mathcal{Q}_1)$, $\mathcal{Q}_2 = \mathbf{S}(\mathcal{Q}_2)$ and $\mathcal{U}'^{-1}(\mathcal{Q}_1) \subseteq \mathcal{V}'^{-1}(\mathcal{Q}_2)$. Then

1. *$\mathcal{Q} = \mathbf{SP}(\mathcal{V}(\mathcal{Q}_1))$ is an interpolant; and*
2. *if in addition $\mathcal{Q}_2 = \mathbf{H}(\mathcal{Q}_2)$ and $\mathcal{U}$ is $\mathbf{H}$-source creating, then the class $\mathcal{Q} = \mathbf{HSP}(\mathcal{V}(\mathcal{Q}_1))$ is also an interpolant.*

Proof. Notice that $\mathcal{V}(\mathcal{Q}_1) \subseteq \mathcal{Q}$. Therefore $\mathbf{P}(\mathcal{V}(\mathcal{Q}_1)) = \mathcal{V}(\mathcal{Q}_1)$ because $\mathcal{V}$ is product preserving and $\mathcal{Q}_1$ is closed under products.

1. Hence $\mathcal{Q} = \mathbf{S}(\mathcal{V}(\mathcal{Q}_1))$. Let $A \in \mathcal{U}^{-1}(\mathcal{Q})$ and let A_1 be an object in $\mathcal{Q}_1$ such that there is a morphism $\mathcal{U}(A) \hookrightarrow \mathcal{V}(A_1)$ in $\mathbf{S}$. Since $\mathcal{U}$ is $\mathbf{S}$-target creating, there are an object $A_2 \in |\mathcal{A}_2|$ such that $\mathcal{U}(A_2) = \mathcal{V}(A_1)$ and a morphism $A \hookrightarrow A_2$ in $\mathbf{S}$. By the pullback property in $\mathbf{Cat}$, there is an object $A' \in |\mathcal{A}'|$ such that $\mathcal{U}'(A') = A_1$

and $\mathcal{V}'(A') = A_2$. Since $\mathcal{U}'^{-1}(\mathcal{Q}_1) \subseteq \mathcal{V}'^{-1}(\mathcal{Q}_2)$, we get that $A_2 \in \mathcal{Q}_2$, and since $\mathcal{Q}_2 = \mathbf{S}(\mathcal{Q}_2)$, we get that $A \in \mathcal{Q}_2$.

2. Hence $\mathcal{Q} = \mathbf{HS}(\mathcal{V}(\mathcal{Q}_1))$. Let $A \in \mathcal{U}^{-1}(\mathcal{Q})$. Then there are some objects $A_1 \in \mathcal{Q}_1$, $B \in |\mathcal{A}|$ and morphisms $B \hookrightarrow \mathcal{V}(A_1)$ in $\mathbf{S}$ and $B \to \mathcal{U}(A)$ in $\mathbf{H}$. Since $\mathcal{U}$ is $\mathbf{H}$-source creating and $\mathbf{S}$-target creating, there are objects $B', A_2 \in |\mathcal{A}_2|$ such that $\mathcal{U}(B') = B$, $\mathcal{U}(A_2) = \mathcal{V}(A_1)$ and morphisms $B' \to A$ in $\mathbf{H}$ and $B' \hookrightarrow A_2$ in $\mathbf{S}$. By the pullback property in $\mathbf{Cat}$, there is an object $A' \in |\mathcal{A}'|$ such that $\mathcal{U}'(A') = A_1$ and $\mathcal{V}'(A') = A_2$. Since $\mathcal{U}'^{-1}(\mathcal{Q}_1) \subseteq \mathcal{V}'^{-1}(\mathcal{Q}_2)$, we get that $A_2 \in \mathcal{Q}_2$, and since $\mathcal{Q}_2 = \mathbf{S}(\mathcal{Q}_2) = \mathbf{H}(\mathcal{Q}_2)$, we get that $A \in \mathcal{Q}_2$.

Therefore $\mathcal{U}^{-1}(\mathcal{Q}) \subseteq \mathcal{Q}_2$, and so $\mathcal{Q}$ is an interpolant.

3 Down to the Real World

A natural generalization of the Craig interpolation result for any pushout

$$\begin{tikzcd}
& \Sigma' & \\
\Sigma_1 \arrow[ur, "\varphi'"] & & \Sigma_2 \arrow[ul, "\psi'"'] \\
& \Sigma \arrow[ul, "\psi"] \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

of signatures would be

> Given a set of Σ_1-equations E_1 and a set of Σ_2-equations E_2 such that $\varphi'(E_1) \models_{\Sigma'} \psi'(E_2)$, then there is a set of Σ-equations I (called *interpolant*) such that $E_1 \models_{\Sigma_1} \psi(I)$ and $\varphi(I) \models_{\Sigma_2} E_2$.

Unfortunately, this is not true! The following counter-example shows that in general it does not hold when φ is not injective.

Example 2. Let all the signatures involved contain one sort S and the indicated unary operations $\Sigma = \{a, b\colon S \to S\}$, $\Sigma_1 = \{a, b, c\colon S \to S\}$, $\Sigma_2 = \{d\colon S \to S\}$, $\Sigma' = \{d, c\colon S \to S\}$; also let $E_1 = \{(\forall x)\ b(x) = c(a(x)), (\forall x)\ a(b(x)) = c(b(x))\}$ and $E_2 = \{(\forall x)\ d(d(x)) = d(x)\}$, let ψ, ψ' be inclusions, and let φ and φ' both take a and b to d. It is easy to see that the four morphisms form a pushout and that $\varphi'(E_1) \models_{\Sigma'} \psi'(E_2)$. We claim there is no interpolant for this pushout of signatures since any interpolant would contain only Σ-equations which are consequences of E_1, that is, equations involving only operations a and b which can be deduced from E_1. But notice that there are no such equations except identities (equations $(\forall X)\ t = t$) because there is no way to get rid of c. Therefore there is no interpolant.

Now we give a sufficient condition, namely that φ is injective.

Corollary 4. *Given a pushout of equational signatures as above with φ injective, given a set of conditional Σ_1-equations E_1 and a set of universally quantified first order Σ_2-formulae E_2 such that $\varphi'(E_1) \models_{\Sigma'} \psi'(E_2)$, then*

1. *there is a set of conditional Σ-equations I such that $E_1 \models_{\Sigma_1} \psi(I)$ and $\varphi(I) \models_{\Sigma_2} E_2$; and*
2. *if E_2 contains only unconditional Σ_2-equations then I can be taken to also contain only unconditional Σ-equations.*

Proof. We use Theorem 3 as follows:

– The pushout of equational signatures translates to the following pullback of categories of algebras:

$$\begin{tikzcd} & \mathbf{Alg}_{\Sigma'} \arrow[dl, "\upharpoonright_{\varphi'}"'] \arrow[dr, "\upharpoonright_{\psi'}"] & \\ \mathbf{Alg}_{\Sigma_1} \arrow[dr, "\upharpoonright_{\psi}"'] & & \mathbf{Alg}_{\Sigma_2} \arrow[dl, "\upharpoonright_{\varphi}"] \\ & \mathbf{Alg}_{\Sigma} & \end{tikzcd}$$

– $\_\upharpoonright_\psi$ is product preserving, because it is a right adjoint.
– By Example 1, $\_\upharpoonright_\varphi$ is both **S**-target and **H**-source creating.
– Let $\mathcal{Q}_1$ and $\mathcal{Q}_2$ be the classes of algebras satisfying E_1 and E_2, respectively. Then $\mathcal{Q}_1$ is closed under products. On the other hand, it is known that $\mathcal{Q}_2$ is closed under subalgebras; moreover, if E_2 contains only unconditional Σ_2-equations, then $\mathcal{Q}_2$ is additionally closed under quotients.

The rest follows from the well known fact (Birkhoff [Bir35]) that quasivarieties and varieties can be defined by conditional and unconditional equations, respectively.

Notice that if E_2 contains only unconditional equations and is finite, then by the equational completeness the interpolant can be taken to be also finite. An important special case is when the pushout is given by union and intersection of signatures, and all morphisms are inclusions (special injections). We reformulate Corollary 4 for this situation:

Corollary 5. *Given signatures Σ_1 and Σ_2, a set of conditional Σ_1 equations E_1 and a set of universally quatified first order Σ_2-formulae E_2 such that $E_1 \models_{\Sigma_1 \cup \Sigma_2} E_2$, then*

1. *there is a set of conditional $(\Sigma_1 \cap \Sigma_2)$-equations I such that $E_1 \models_{\Sigma_1} I$ and $I \models_{\Sigma_2} E_2$; and*
2. *if E_2 contains only unconditional Σ_2-equations then I can be taken to also contain only [unconditional] $(\Sigma_1 \cap \Sigma_2)$-equations.*

If in addition we add the (unnecessary) condition that E_1 contains only unconditional equations, then we obtain the (usual) equational interpolation:

Corollary 6. *If E_1 and E_2 are sets of unconditional Σ_1-equations and Σ_2-equations, respectively, such that $E_1 \models_{\Sigma_1 \cup \Sigma_2} E_2$, then there is a set of unconditional $(\Sigma_1 \cap \Sigma_2)$-equations I such that $E_1 \models_{\Sigma_1} I$ and $I \models_{\Sigma_2} E_2$*

See [DGS93] for a detailed study of this and closely related formulations at the level of institutions [GB92], using inclusion systems for union and intersection of signatures.

4 Summary and Future Work

Generalizations of equational Craig interpolation are investigated in the present paper. We look both at more general pushouts of signatures than the union intersection ones, and at different kinds of sentence, including unconditional and conditional equations, and universally quantified first order formulae.

A first result is that equational Craig interpolation can be generalized to any pushout of signatures for which the morphism with target Σ_2 is injective, and that the result does not hold in general if that morphism is not injective.

A second result is that the kind of equation in E_1 does not influence the kind of equation in the interpolant; actually the only requirement for the sentences in E_1 is that they generate classes of models that are closed under products, which means the door is open to generalize the result even further.

A third result is that even if E_2 contains formulae more complex than conditional equations, namely, universally quantified first order formulae, the interpolant can still contain only conditional equations; actually only closure under submodels is required for the class of models of E_2.

Another result is that if E_2 contains only unconditional equations, then the interpolant can also contain only unconditional equations even if E_1 might contain conditional equations or other sentences generating classes of models closed under products.

We think an interesting direction for further research would be to dualize the results of this paper to coalgebra. The fact that our main technique was the Birkhoff axiomatizability, which also holds for coalgebra and coequations [Gum98] supports the feasibility of this project.

The methodological approach of this paper may also be of interest, in that we avoid the details of equational logic until the end, by using a very general categorical formulation. Although this paper has mainly discussed the case of unsorted equational logic, it is an advantage of our apporach that it applies equally well to many other forms of equational logic that have been developed, such as the many sorted and various order sorted variants [GD94], and indeed, to non-equational logics.

References

[BHK90] Jan Bergstra, Jan Heering, and Paul Klint. Module algebra. *Journal of the Association for Computing Machinery*, 37(2):335–372, 1990.

[Bir35] Garrett Birkhoff. On the structure of abstract algebras. *Proceedings of the Cambridge Philosophical Society*, 31:433–454, 1935.

[Cra57] W. Craig. Linear reasoning. a new form of the herbrand-gentzen theorem. *Journal of Symbolic Logic*, 22:250–268, 1957.

[DGS93] Răzvan Diaconescu, Joseph Goguen, and Petros Stefaneas. Logical support for modularization. In Gerard Huet and Gordon Plotkin, editors, *Logical Environments*, pages 83–130. Cambridge, 1993.

[EM85] Hartmut Ehrig and Bernd Mahr. *Fundamentals of Algebraic Specification 1: Equations and Initial Semantics*. Springer, 1985. EATCS Monographs on Theoretical Computer Science, Volume 6.

[GB92] Joseph Goguen and Rod Burstall. Institutions: Abstract model theory for specification and programming. *Journal of the Association for Computing Machinery*, 39(1):95–146, January 1992.

[GD94] Joseph Goguen and Răzvan Diaconescu. An Oxford survey of order sorted algebra. *Mathematical Structures in Computer Science*, 4:363–392, 1994.

[GM96] Joseph Goguen and Grant Malcolm. *Algebraic Semantics of Imperative Programs.* MIT, 1996.

[Gum98] H. Peter Gumm. Equational and implicational classes of coalgebras. extended abstract. In *The 4th International Seminar on Relational Methods in Logic, Algebra and Computer Science.*, 1998. Warsaw.

[Lan71] Saunders Mac Lane. *Categories for the Working Mathematician.* Springer, 1971.

[Pig74] Don Pigozzi. The join of equational thories. *Colloquium Mathematicum*, 30:15–25, 1974.

[Rod91] Pieter Hendrik Rodenburg. A simple algebraic proof of the equational interpolation theorem. *Algebra Universalis*, 28:48–51, 1991.

[RvG88] Pieter Hendrik Rodenburg and Rob van Glabbeek. An interpolation theorem in equational logic. Technical Report CS-R8838, CWI, 1988.