Enabling conditions for interpolated rings

Fred Richman

Florida Atlantic University, Department of Mathematics
Boca Raton FL 33431
richman@fau.edu

Abstract. An *interpolated ring* is a particular kind of Brouwerian example in which the ring you are dealing with may be one of two given rings that are related by a homomorphism, often an inclusion. We are interested here in when all interpolated rings inherit some property common to the two given rings. An *enabling condition* is a condition on the homomorphism that guarantees that the property is inherited.

Keywords. Brouwerian counterexample, interpolated ring, intuitionistic algebra

1 Introduction

Let $\varphi : A \to B$ be a homomorphism of commutative rings. If P is any proposition, then the **P-interpolation** of φ is the disjoint union

$$C = A \cup \{b \in B : P\}$$

modulo the condition that $a = \varphi(a)$ for all $a \in A$ if P holds. If φ is the injection map $A \subset B$, then C is simply the union $A \cup \{b \in B : P\}$, which is a subring of B. This is the case of most interest when dealing with discrete rings. Interpolated rings are used to construct Brouwerian examples. For example, the interpolated rings of $\mathbf{Z} \subset \mathbf{Q}$ provide a Brouwerian example of a discrete ring C and a finitely generated ideal I of C for which the assertion "$1 \in I$ or $1 \notin I$" cannot be justified. If, in this example, P states that a certain binary sequence contains a 1, then C is countable.

Of course we need not restrict ourselves to rings. The same idea applies to other mathematical structures as well. Jesper Carlström pointed out that the P-interpolation C of the map $\varphi : \{0, 1\} \to \{0\}$, together with the natural map from $\{0, 1\}$ onto C is the Goodman-Myhill example showing that the axiom of choice implies the law of excluded middle [1].

2 A categorical formulation

We could define an **interpolated object** in a category $\mathcal{C}$ to be a functor F from the poset of propositions (or subsets of $\{0\}$) to $\mathcal{C}$ with the property that if G

Dagstuhl Seminar Proceedings 05021
Mathematics, Algorithms, Proofs
http://drops.dagstuhl.de/opus/volltexte/2006/279

is another such functor, with $F(\bot) = G(\bot)$ and $F(\top) = G(\top)$, then there is a unique natural transformation $\alpha : F \to G$ that is the identity on $F(\bot)$ and on $F(\top)$. This transformation α need not be an isomorphism. For example, set $G(P) = F(\neg\neg P)$.

Interpolated objects always exist in any category of (finitary) relational structures: rings, modules over a fixed ring, posets. Given a homomorphism $\varphi : A \to B$, define $F(\bot) = A$ and $F(\top) = B$ and $F(\bot \to \top) = \varphi$. Then let $C = F(P)$ be the disjoint union of A and $\{b \in B : P\}$, modulo $a = \varphi(a)$, and define φ on C in the obvious way. Set

$$\Gamma_C(c_1, \ldots, c_m) = \begin{cases} \Gamma_A(c_1, \ldots, c_m) & \text{if all } c_i \in A \\ \Gamma_B(\varphi c_1, \ldots, \varphi c_m) & \text{if } P. \end{cases}$$

3 Enabling and disabling conditions

Suppose we want to prove that any interpolated ring of $A \subset B$ is, say, a unique factorization domain. Then certainly A and B must be unique factorization domains. However, if the P-interpolation C of the pair $\mathbf{Z} \subset \mathbf{Q}$ were a unique factorization domain, then we could determine whether the element $2 \in C$ was a unit or not, so we could determine which of P or $\neg P$ holds. The problem here is that there are primes in $\mathbf{Z}$ that are not primes in $\mathbf{Q}$. The same problem arises, in a more substantial way, when interpolating the pair of polynomial rings $\mathbf{Q}[X^2] \subset \mathbf{Q}[X]$.

Now suppose we take $A \subset B$ to be unique factorization domains, and add the condition that every prime in A is also a prime in B. Then the P-interpolation C of $A \subset B$ is indeed a unique factorization domain. Given a nonzero element $c \in C$, either $c \in A$ or P. If $c \in A$, then either c is a unit in A, a prime in A or a product of primes in A. Because units and primes of A are also units and primes of B, the same alternatives hold in C. On the other hand, if P holds, then $C = B$ is a unique factorization domain.

Conversely, suppose some prime p in A is not a prime in B, so either p is a unit in B or p factors nontrivially in B. If C were a unique factorization domain, then we could determine whether or not p is a prime in C, so we could determine which of $\neg P$ or P holds. So if C were a unique factorization domain for all P, then the law of excluded middle would hold. That, of course, is the essence of a Brouwerian example.

We say that the condition that primes in A remain prime in B is an **enabling condition** for interpolating unique factorization domains. Note that this enabling condition has real classical content: it's not just something that necessarily holds from a classical point of view, but may not admit a constructive proof. Contrast this to the fact that, from a classical point of view, there are only two interpolated rings for $A \subset B$, and they are both unique factorization domains.

The condition that there is a prime in A that is not a prime in B is called a **disabling condition** for interpolating unique factorization domains.

Definition 1. *Let $\mathcal{C}$ be a class of rings. A condition on a homomorphism $\varphi : A \to B$ is said to be an* ***enabling condition*** *for interpolating rings of $\mathcal{C}$ if it implies that every interpolated ring of φ is in $\mathcal{C}$. It is called a* ***disabling condition*** *if, when it holds, and every interpolated ring of φ is in $\mathcal{C}$, then some omniscience principal (like the law of excluded middle) holds.*

Informally, we will say that an enabling condition is **exact** if the natural positive formulation of its classical negation is a disabling condition. That is the connection between the condition that primes in A remain prime in B, and the condition that there is a prime in A that is not a prime in B. The enabling conditions of most interest are the exact ones. An exact enabling condition for interpolating **discrete** rings is that the homomorphism φ be one-to-one. So if $\mathcal{C}$ consists of discrete rings, we will assume that φ is an inclusion.

We have shown that the property that every prime in A is a prime in B is an exact enabling condition for interpolating unique factorization domains. One instance of this is for the class $\mathcal{C}$ of factorial fields. The enabling condition is that A be algebraically closed in B. That's so because to say that a (discrete) field A is factorial is to say that $A[X]$ is a unique factorization domain, and primes are preserved in going from $A[X]$ to $B[X]$ if and only if A is algebraically closed in B.

> The pair consisting of an enabling condition and a disabling condition is somewhat analogous to Bishop's notion of a complemented set. Usually the corresponding disabling condition stands out: It is essentially a sort of strong negation that reduces to negation when dealing with propositions satisfying the law of excluded middle. We extend to more complicated formulas by $\neg (P \vee Q) = \neg P \wedge \neg Q$ and $\neg (P \wedge Q) = \neg P \vee \neg Q$. Quantifiers are negated analogously. Also $\neg (P \Rightarrow Q) = P \wedge \neg Q$, but there is a problem with implication in that the strong negation is not of order two. Maybe that's not important.
>
> The condition that φ be one-to-one provides an example of this problem. That condition says that $\varphi(x) = 0$ implies $x = 0$ for all x. The strong negation for that is that there exists x such that $\varphi(x) = 0$ and $x \neq 0$. But the negation of that negation is $\varphi(x) \neq 0$ or $x = 0$ for all x.

For an example using abelian groups instead of rings, let $\mathcal{C}_n$ be the class of abelian groups A such that nA **is detachable from** A, and let E_n be the property of a pair of abelian groups $A \subset B$ that $nA = A \cap nB$. (We say that A is *pure* in B if E_n holds for all n.) More generally, let E_n be the property of a homomorphism $\varphi : A \to B$ that $\varphi^{-1}(nB) = nA$. To show that E_n is an exact enabling condition for interpolating groups in $\mathcal{C}_n$, we have to show two things:

1. If $\varphi^{-1}(nB) = nA$, then every interpolated group C for φ has the property that nC is detachable from C.
2. If there exists $a \in \varphi^{-1}(nB)$ such that $a \notin nA$, and every interpolated group C for φ has the property that nC is detachable from C, then some omniscience principle holds.

To show (1), let C be the P-interpolation of φ and let $c \in C$. Either $c \in A$ or P holds. If $c \in A$, then either $\varphi(c) \in nB$, in which case $c \in nA$, hence $c \in nC$, or $\varphi(c) \notin nB$, in which case $c \notin nC$. If P holds, then C is isomorphic to B, so nC is detachable from C.

To show (2), suppose that there exists $a \in \varphi^{-1}(nB)$ such that $a \notin nA$. Suppose also that the P-interpolated group C of φ has the property that nC is detachable from C. Then, as an element of C, either $a \in nC$ or $a \notin nC$. In the former case, $a = nc$ for some element of C. Either $c \in A$ or P holds, but c cannot be in A because $a \notin nA$, so P holds. In the latter case, P cannot hold lest $C = B$ in which case $a \in nC$.

4 Classes closed under interpolation

There are many cases where no enabling condition is necessary. In such a case we say that the class of rings is closed under interpolation. In what follows, C denotes the P-interpolation of $A \to B$.

Noetherian rings (ACC) are closed under interpolation, that is, they require no enabling condition. Suppose $I_1 \subset I_2 \subset \cdots$ is a chain of finitely generated ideals. Using countable choice we can construct a sequence of finitely enumerable sets $G_1 \subset G_2 \subset \cdots$ such that G_n generates I_n, and an ascending binary sequence λ_n such that if $\lambda_n = 0$, then $G_n \subset A$, while if $\lambda_n = 1$, then P holds. Let J_n be the ideal in A generated by G_n if $\lambda_n = 0$, and $J_n = A$ if $\lambda_n = 1$. To eliminate countable choice, use the ascending tree condition [6] instead of ACC. Look at the tree of triples (G, n, λ), where G is a finitely enumerable set of generators of I_n and $\lambda \in \{0, 1\}$ is such that if $\lambda = 0$, then $G \subset A$ and if $\lambda = 1$, then P holds. Set $(G, n, \lambda) < (G', n+1, \lambda')$ if $G \subset G'$ and $\lambda \leq \lambda'$. At the node (G, n, λ) we attach the ideal of A generated by G, if $\lambda = 0$, and A if $\lambda = 1$. The same thing can be done starting with a tree of finitely generated ideals instead of a chain.

We now consider a certain kind of class of rings that requires no enabling condition. A functorial n-ary predicate in the category of rings (say) is a functor Γ from the category of set maps $\{1, 2, \ldots, n\} \to A$ to propositions. The functor Γ is an **interpolating predicate** if

$$\Gamma_C(a_1, \ldots, a_n) \Rightarrow \Gamma_A(a_1, \ldots, a_n) \vee P$$

whenever $a_1, \ldots, a_n \in A$. (Is that automatic?)

For a fixed polynomial f in $\mathbf{Z}[X_1, \ldots, X_n]$, the predicate $f(a_1, \ldots, a_n) = 0$ is interpolating. So is the predicate "a is nilpotent". For modules over a fixed ring R, the predicate $\exists r \neq 0 : ra = 0$ is interpolating.

A class that is specified by a statement of the form $\forall \mathbf{x} : q(\mathbf{x}) \Rightarrow \exists \mathbf{y}\, p(\mathbf{x}, \mathbf{y})$, where q and p are functorial predicates and q is interpolating, is closed under interpolation. Here each of $\mathbf{x}$ and $\mathbf{y}$ represent a number of variables that range over elements, or finite sets of elements, of the structures in question. These are the only such variables in the statement.

Here are some specific examples of this kind of class:

– **Bezout rings**. For all x, y, there exist s, t, u, v such that $x = u\,(sx + ty)$ and $y = v\,(sx + ty)$. Here $q = \top$ while $\mathbf{x} = (x, y)$ and $\mathbf{y} = (s, t, u, v)$.
– **Fields**. For all x there exists y such that if $x \neq 0$, then $xy = 1$.
– **Flat R-modules**. For all $a_1, \ldots, a_m \in C$ and $r_1, \ldots, r_m \in R$, if $\sum r_i a_i = 0$, then there exist $b_1, \ldots, b_n \in C$ and $t_{ij} \in R$ such that $a_i = \sum t_{ij} b_j$ and $\sum r_i t_{ij} = 0$.
– **Local rings**. For all x, there exists s such that either $sx = 1$ or $s\,(1 - x) = 1$.
– **Upper Krull dimension** m. That is, $\dim C \leq m$. For all $x_1, \ldots, x_m \in C$, there exists n and $a_1, \ldots, a_m \in C$ such that

$$p\,(a_1 x_1, \ldots, a_m x_m, x_1^n, \ldots, x_m^n) = 0,$$

where p is a polynomial with integer coefficients (see [3]).

5 Examples of enabling conditions

In this section we examine a few properties of rings together with their enabling conditions.

Seidenberg's Condition P. This is a property of a field k that is required for primary decomposition of finitely generated ideals in polynomial rings over k (see [5]). One formulation of this property is that if p is a prime that is equal to 0 in k, then any finitely generated k^p-subspace of k is finite-dimensional. The exact enabling condition is that A^p-independent subsets of A are also independent over B^p. That's the same as saying that B is separable over A (see [4, 198–201]). If the independent subset in question consists of two elements, then we get the condition $B^p \cap A = A^p$, as in our abelian groups example. The disabling condition is that there exists a finite subset of A that is independent over A^p but dependent over B^p.

Strongly discrete. Every finitely generated ideal is detachable. The enabling condition is that every ideal of A is contracted. In fact, if I is the ideal of the P-interpolation C that is generated by $c_1, \ldots, c_n$, and $c_0 \in C$, then either P holds or all the c_i are in A. In the former case we test to see if $c_0 \in Bc_1 + \cdots + Bc_n$. In the latter, we test to see if $c_0 \in Ac_1 + \cdots + Ac_n$. If not, then $c_0 \notin I$ because $Ac_1 + \cdots + Ac_n$ is contracted. The disabling condition is that there is a finitely generated ideal I of A such that $BI \cap A$ contains an element a that is not in I. In that case, $a \in CI$ if and only if P.

Coherent. Every finitely generated ideal is finitely presented. The example of a noncoherent ring in [5] is the P-interpolated ring C between the ring $k[X, Y]/(X, Y)^2$ and the subring $k[X]$. Map $C \to C$ by taking 1 to X and suppose the kernel of this map is finitely generated. Note that $XY = 0$ in B. If the generators of the kernel involve Y, then P holds. If not, then $\neg P$ holds.

The enabling condition here is that B be a flat A-module. To see that this enables coherence, we have to show that the kernel of any map $C^n \to C$ is finitely generated. We may assume that the generators of C^n go into A, giving us a map $A^n \to A$ which when tensored with C gives our map $C^n \to C$. If B

is flat over A, then C is flat over A (from the general theorem) so the kernel of $C^n \to C$ is finitely generated.

The exact condition we need is that if the sequence $0 \to K \to A^n \to A$, so is the sequence $0 \to BK \to B^n \to B$. Now K is the relation module of $a_1, \ldots, a_n$ over A and we want BK to be the relation module of $a_1, \ldots, a_n$ over B. That says that if $\sum b_i a_i = 0$, then we can find elements $q_{ij} \in A$ such that $\sum_i q_{ij} a_i = 0$ and $b_i = \sum_j \beta_j q_{ij}$. This is the definition of flatness. How does the disabling part go? Suppose we have a B-relation $\sum b_i a_i = 0$ on $a_1, \ldots, a_n$ with $(b_1, \ldots, b_n) \notin BK$. Now the C-relations on $a_1, \ldots, a_n$ are finitely generated. Either the generators are all A-relations, or P holds. If the generators are all A-relations (that is, in K), then P cannot hold because if it did, then C would be B and $(b_1, \ldots, b_n) \in BK$.

Swedish Noetherian rings are coherent, strongly discrete rings whose finitely generated ideals are well founded under reverse inclusion [2]. (I am indebted to Peter Schuster for this terminology, although I'm not sure he expected me to take it seriously.) So part of the enabling condition is that every ideal of A is contracted and that B is a flat A-module. We will show that no further enabling condition is required to get the well foundedness.

Suppose $A \subset B$ are Swedish Noetherian, that every ideal of A is contracted, and that C is the P-interpolated ring. We want to show that if I is a finitely generated ideal of C, then $IB \cap C = I$. Either $I = I_0 C$ for some finitely generated ideal I_0 of A, or P holds. If P holds, then $C = B$ so $IB \cap C = I \cap B = I$. If $I = I_0 C$, suppose $\sum g_i b_i = c \in C$ where the g_i are a finite number of generators of I_0 and $b_i \in B$. Either $c \in A$ or P holds. In the second case, $\sum g_i b_i \in I$. In the first case, $c \in I_0 B \cap A = I_0 \subset I$.

Thus the poset of finitely generated ideals of C is embedded in the poset of finitely generated ideals of B, that is, $IB \subset JB$ if and only if $I \subset J$. So the former poset is also well founded under reverse inclusion.

Lower Krull dimension. For $\dim R > n$, there doesn't seem to be a pretty enabling condition. That $\dim R > 0$ needs an enabling condition is illustrated by the inclusion $\mathbf{Z} \subset \mathbf{Q}[X]$. The problem in this example is that the witnessing element for $\dim A > 0$ need not (in fact, cannot) be a witness that $\dim B > 0$. The property in question is that there exists $x \in R$ such that $1 \notin Rx + (0 : x^\infty)$. Alternatively, $(1 + rx)\, x^n \neq 0$ for all r and n, that is, $x^n \notin Rx^{n+1}$. An enabling condition is that some witness to the fact that $\dim A > 0$ must also witness the fact that $\dim B > 0$. That is not a particularly attractive or enlightening condition. Perhaps one could formulate a more interesting enabling condition, even if it is not exact.

6 What is a UFD?

One unexpected outcome of this investigation was the discovery that the treatment of unique factorization domains in [5] is flawed. The issue is whether principal ideals are detachable, which is not required by the definition in [5]. Equivalently, given two primes, either they are associates or not. Clearly the latter is implied by the former. The converse is reasonably clear also, but a little fussy. Should this condition be included in the definition of a UFD or, alternatively, is it a consequence of the weaker definition of a UFD in [5]?

In [5, Theorem IV.2.3] it is claimed without proof that every UFD is a bounded GCD-domain. In a UFD that is a GCD-domain, the condition above holds because, given primes p and q, one simply checks to see if $\gcd(p, q)$ is a unit or not. Conversely, if the condition holds, then the UFD is a GCD-domain for the usual reason.

What would an interpolated-rings counterexample look like? The enabling condition for a UFD is that primes in A remain primes in B. The disabling condition for principal ideals being detachable is that some element of B is in the quotient field of A but not in A. It seems to be a nontrivial classical question whether these two conditions are compatible.

References

1. Goodman, Nelson, and John Myhill, Choice implies excluded middle, *Zeit. Math. Logik Grundlagen Math*, **24** (1978), 461
2. Jacobsson, Carl, and Clas Löfwall, Standard bases for general coefficient rings and a new constructive proof of Hilbert's basis theorem, *J. Symbolic Comput.*, **12** (1991) 337–371.
3. Lombardi, Henri, Dimension de Krull, Nullstellensätze et évaluation dynamique, *Math. Zeit.* **242** (2002) 23–46.
4. Matsumura, Hideyuki, *Commutative ring theory*, Cambridge University Press 1986
5. Mines, Ray, Fred Richman, and Wim Ruitenburg, *A course in constructive mathematics*, Springer 1988.
6. Richman, Fred, The ascending tree condition: constructive algebra without countable choice, *Communications in Algebra*, **31** (2003), 1993–2002.