

Enabling conditions for interpolated rings

Fred Richman
Florida Atlantic University

23 February 2005

Let $\varphi : A \rightarrow B$ 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 $\varphi(a) = a$ 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 in $\mathbf{Z} \subset \mathbf{Q}$ 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 $\varphi : \{0, 1\} \rightarrow \{0\}$, together with the natural map from $\{0, 1\}$ to C is the Goodman-Myhill example showing that the axiom of choice implies the law of excluded middle [1].

1 A categorical formulation

An **interpolated object** in a category \mathcal{C} is a functor F from the poset of propositions (or subsets of $\{0\}$) to \mathcal{C} with the property that if G is another such functor, with $F(\perp) = G(\perp)$ and $F(\top) = G(\top)$, then there is a unique natural transformation $\alpha : F \rightarrow G$ that is the identity on $F(\perp)$ 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 $\varphi : A \rightarrow B$, define $F(P)$ with $F(\perp) = A$ and $F(\top) = B$ and $F(\perp \rightarrow \top) = \varphi$. Let $F(P)$ 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

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

which can be written as

$$(c_1, \dots, c_m \in A) \wedge \Gamma_A(c_1, \dots, c_m) \vee P \wedge \Gamma_B(\varphi c_1, \dots, \varphi c_m).$$

We get a unique middle vertical map

$$\begin{array}{ccccc} A & \longrightarrow & F(P) & \longrightarrow & C \\ & \searrow & \downarrow & \nearrow & \\ & & G(P) & & \end{array}$$

2 Enabling and disabling conditions

Unique factorization domains. Suppose we want to prove that any interpolated ring in $A \subset B$ 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 $\varphi : A \rightarrow B$ 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 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 $\varphi : A \rightarrow B$ that $\varphi^{-1}(nB) = nA$. To show that E_n is an exact enabling condition for interpolating groups in \mathcal{C} , 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 $a \notin nA$. In the latter case, P cannot hold lest $C = B$ in which case $a \in nC$.

3 Classes closed under interpolation

Noetherian rings (ACC) are closed under interpolation, that is, they require no enabling condition. Suppose $I_1 \subset I_2 \subset \dots$ is a chain of finitely generated ideals. Using countable choice we can construct a sequence of finitely enumerable sets $G_1 \subset G_2 \subset \dots$ 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 pairs (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.

Swedish Noetherian rings are coherent, strongly discrete rings whose finitely generated ideals are well founded under reverse inclusion [2]. We will show that this class of rings is also closed under interpolation, that is, they require no enabling condition.

Suppose $A \subset B$ are Swedish Noetherian, and C is an interpolated ring. We want to show that if I is a finitely generated ideal of C , then $IB \cap C = I$. Either $I = I_0C$ 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 $I = I_0C$, 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, $c \in I_0B \cap A = I_0 \subset I$.

So 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 $I \subset J$. Presumably that makes it well founded under reverse inclusion. I guess that's what the following argument proves.

Suppose $U \subset V$ where V is well founded. Let $S \subset U$ be hereditary in U . Let

$$T = \{v \in V : v \in U \Rightarrow v \in S\},$$

the largest subset of V whose intersection with U is contained in S . That is, it is $U \rightarrow S$ as in Heyting algebras. We want to show that T is an hereditary subset of V , hence equal to V . Suppose $x \in V$ and $v \in T$ for all $v < x$. We want to show that if $x \in U$, then $x \in S$ because that will show that $x \in T$. So suppose $x \in U$. As S is hereditary in U , and $v \in T$ for all $v < x$, we have $v \in S$ for all $v < x$ with $v \in U$. Thus $x \in S$.

There is a large class of rings which require no enabling condition. Thierry says it works for “geometric statements” and gives the reference [7]. I haven’t looked at that yet; I will try to do that soon. Meanwhile, here is what I came up with.

A functorial predicate in the category of rings (say) is a functor from the category of set maps $\{1, 2, \dots, n\} \rightarrow A$ to propositions. It is an **interpolating predicate** if

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

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

Equality of polynomials is an interpolating predicate. Also $a^m = 0$ for some m . 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 $\forall x : q(x) \Rightarrow \exists y p(x, y)$, where q and p are functorial predicates and q is interpolating, is closed under interpolation. Here x and y represent some 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 phenomenon:

- **Bezout rings.** For all x, y , there exist s, t, u, v such that $x = u(sx + ty)$ and $y = v(sx + ty)$.
- **Fields.** For all x there exists y such that if $x \neq 0$, then $xy = 1$.
- **Flat R -modules.** For all $a_1, \dots, a_m \in C$ and $r_1, \dots, r_m \in R$, if $\sum r_i a_i = 0$, then there exist $b_1, \dots, b_n \in C$ 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 $x_1, \dots, x_m \in C$, there exists n and $a_1, \dots, a_m \in C$ such that

$$p(a_1x_1, \dots, a_mx_m, x_1^n, \dots, x_m^n) = 0,$$

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

4 Examples of enabling conditions

Seidenberg's Condition P . This is a condition on a field k that is required for primary decomposition of finitely generated ideals in polynomial rings over k (see [5]). One formulation of this condition 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, \dots, 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 $c_0 \in Bc_1 + \dots + Bc_n$. In the latter, we test to see if $c_0 \in Ac_1 + \dots + Ac_n$. If not, then $c_0 \notin I$ because $Ac_1 + \dots + Ac_n$ 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 $C \rightarrow C$ 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 $C^n \rightarrow C$ is finitely generated. We may assume that the generators of C^n go into A , giving us a map $A^n \rightarrow A$ which when tensored with C gives our map $C^n \rightarrow C$.

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

The exact condition we need is that if the sequence $0 \rightarrow K \rightarrow A^n \rightarrow A$, so is the sequence $0 \rightarrow BK \rightarrow B^n \rightarrow B$. Now K is the relation module of a_1, \dots, a_n over A and we want BK to be the relation module of a_1, \dots, 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 $b_i = \sum_j \beta_j q_{ij}$. Looks like flat. So how does the disabling bit go? Suppose we have a B -relation $\sum b_i a_i = 0$ on a_1, \dots, a_n with $(b_1, \dots, b_n) \notin BK$. Now the C -relations on a_1, \dots, 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 $(b_1, \dots, b_n) \in BK$.

Lower Krull dimension. For $\dim R > n$, there doesn't seem to be a pretty 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 $\dim B > 0$. Poor. Comparable prime ideals don't collapse, or something. Is this one of those going-up going-down kinds of things?

5 What is a UFD?

The issue is whether principal ideals are detachable. That 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 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 (presumably by the unwritten proof of [5, Theorem IV.2.3]).

What would an interpolated-rings counterexample look like? The en-

abling 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 .

6 Working in the topos $\cdot \rightarrow \cdot$

Looks like you should be able to interpret all this in the topos $\cdot \rightarrow \cdot$, which is essentially a simple Kripke model. A class of rings would be given by a sentence, and we would look for (external) conditions on φ that would assure that the sentence was (internally) true for $A \xrightarrow{\varphi} B$. “True” meaning has truth value $1 \rightarrow 1$. Discrete is the sentence $\forall_{x,y}(x = y \vee \neg x = y)$. How do we assign a truth value to that? You look at its value in A and its value in B , from inside out? How do you interpret the variables x and y ?

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.
- [7] WRAITH, GAVIN, *Proceedings of the International Congress of Mathematics*, Helsinki, 1978, 330–337.