

An investigation, via JAW0 and JAW2

In JAW0 , I asked when we could conclude:

$$(0) \quad m \sqsubseteq n * p \Rightarrow m \sqsubseteq n \quad ,$$

where \sqsubseteq means “divides” , and wrote of being “hit in the face” by the famous lemma from number theory which says that (0) follows from:

$$(1) \quad m \mathbf{gcd} p = 1 \quad .$$

Being familiar with Edsger Dijkstra’s struggles in EWD1313 , I was in no hurry to tackle a calculational proof of $(0) \Leftarrow (1)$. (In fact, it would be several months before I attempted such a proof: see JAW9 and JAW10 .) But it seemed worthwhile to explore how one might derive the condition (1) if one were not “hit in the face” by it. Thus I decided to investigate (0) and see what I could derive from it. What follows is a recreation of that investigation, warts and all!

Where to begin? This observation from JAW2 seemed like a reasonable guideline:

“About natural numbers we know really only two interesting things: first, that the set of natural numbers is well-founded [...], and second, that positive natural numbers are products of unique finite bags of primes.” .

Because there are several variables in (0) , and because **gcd** has more to do with prime factorization than well-foundedness, I opted for the prime decomposition approach.

This approach is actually a rather nice choice, because it gives us a nice way to translate the operators \sqsubseteq , **gcd** , and $*$ into bag terminology. Let:

$$B.x = \text{the bag of primes in the decomposition of } x \quad .$$

Then we have such lovely theorems as —proofs left to the reader— :

$$\begin{aligned} B.(x * y) &= B.x \cup B.y \\ B.(x \mathbf{gcd} y) &= B.x \cap B.y \\ x \sqsubseteq y &\equiv B.x \subseteq B.y \quad , \end{aligned}$$

and so we may translate (0) as the equivalent:

$$B.m \subseteq B.n \cup B.p \Rightarrow B.m \subseteq B.n \quad .$$

Now that the entire theorem was phrased in terms of bags, I conjectured that the primality of their elements would be irrelevant. Thus I decided to investigate for arbitrary bags M , N , and P :

$$(2) \quad M \subseteq N \cup P \Rightarrow M \subseteq N \quad .$$

However, no sooner than I had written down (2) , I realized that I had no idea what to do with it! I knew that sets could be represented by characteristic predicates:

$$y \in X \equiv (X).y \quad ,$$

which puts all the calculational power of the predicate calculus at one's disposal. But characteristic predicates don't suffice for bags: We need to capture not only whether an element is in a bag, but also how many copies of that element are in it. Bags are much more flexible than sets because they allow for multiple elements with the same value, but it is precisely this flexibility that complicates a demonstrandum about bags.

Thus, I opted to change (2) into a demonstrandum about sets X , Y , and Z :

$$X \subseteq Y \cup Z \Rightarrow X \subseteq Y \quad ,$$

and then immediately eliminated sets in favor of their characteristic predicates, which I also called X , Y , and Z :

$$(3) \quad [X \Rightarrow Y \vee Z] \Rightarrow [X \Rightarrow Y] \quad .$$

Now I could start to manipulate (3) , using predicate calculus:

$$\begin{aligned} & [X \Rightarrow Y \vee Z] \Rightarrow [X \Rightarrow Y] \\ \equiv & \quad \{ \text{predicate calculus, to homogenize} \} \\ & [\neg X \vee Y \vee Z] \Rightarrow [\neg X \vee Y] \\ \Leftarrow & \quad \{ \text{predicate calculus, to bring the terms together} \} \\ & [\neg X \vee Y \vee Z \Rightarrow \neg X \vee Y] \\ \equiv & \quad \{ \text{predicate calculus, to simplify} \} \\ & [Z \Rightarrow \neg X \vee Y] \\ \equiv & \quad \{ \text{predicate calculus, preparing to translate} \} \\ & [X \wedge Z \Rightarrow Y] \quad . \end{aligned}$$

To summarize: $[X \wedge Z \Rightarrow Y]$ is a sufficient condition for (3) .

But is the bag analogue $M \cap P \subseteq N$ a sufficient condition for (2) ? The answer is no. For example, if we let $M, N, P := \{\bullet, \bullet\}, \{\bullet\}, \{\bullet\}$, we easily see that the condition is **true** , while (2) is **false** .

So we have to choose a stronger condition. To this end I returned to the predicate condition $[X \wedge Z \Rightarrow Y]$, and superhomogenized it as:

$$(4) \quad [\neg X \vee Y \vee \neg Z] \quad .$$

The simplest way I saw to choose a stronger condition was to select a proper subset of the disjoined predicates in (4) . Which ones? Some choices were obviously unhelpful. I couldn't take just one predicate, because I didn't know how to translate something like $[\neg X]$ or $[Y]$ back into bag terminology. Also, $[\neg X \vee Y]$ is an uninteresting choice, because it trivially implies (3) .

Only two choices remained:

$$[\neg X \vee \neg Z] \quad \text{and} \quad [\neg Z \vee Y] \quad .$$

In set notation, these correspond to:

$$X \cap Z = \emptyset \quad \text{and} \quad Z \subseteq Y \quad ,$$

and in bag notation:

$$M \cap P = \emptyset \quad \text{and} \quad P \subseteq N \quad .$$

The instantiation $M, N, P := \{\bullet, \bullet\}, \{\bullet\}, \{\bullet\}$ rules out the latter condition, so we are left with the former:

$$(5) \quad M \cap P = \emptyset \quad .$$

And as the reader can check, if we translate (5) from bag notation back into the language of natural numbers, we get $m \mathbf{gcd} p = 1$, which is precisely the condition we had hoped to derive.

* *

 *

Postlude. At the beginning of this document, I wrote: “I was in no hurry to tackle a calculational proof of $(0) \Leftarrow (1)$.” . In the meantime, I attempted a calculational proof of the bag correlate $(2) \Leftarrow (5)$. My efforts were more than a little frustrating, and the reader should consider himself fortunate that at the last minute I excised all the paragraphs devoted to this proof, and kept the focus of the document on the design of the sufficient conditions (1) and (5) ! (**End of Postlude.**)

Santa Cruz, 19 November 2004 / Revised: NYC, 26-27 December 2010

Jeremy Weissmann
jeremy@mathmeth.com