

An addendum to JAW3

Document JAW3 was occupied with deriving “ $m \mathbf{gcd} p = 1$ ” as a suggested sufficient condition for

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

where m , n , and p are of type positive natural, and \sqsubseteq means “divides”. This document shows a different way to derive that condition, a way that allows us to simultaneously prove its sufficiency. Our investigation will be rabbit-free.

As in JAW3, we choose to exploit the fact that a natural is the product of a unique bag of primes. Letting

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

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

$$(1) \quad B.(x * y) = B.x \cup B.y \quad ,$$

$$(2) \quad B.(x \mathbf{gcd} y) = B.x \cap B.y \quad ,$$

$$(3) \quad x \sqsubseteq y \equiv B.x \subseteq B.y \quad ,$$

$$(4) \quad x = 1 \equiv B.x = \emptyset \quad ,$$

from which we conclude:

$$\begin{aligned} & (0) \\ = & \{ (3) , \text{twice} \} \\ & B.m \subseteq B.(n * p) \Rightarrow B.m \subseteq B.n \\ = & \{ (1) \} \\ & B.m \subseteq B.n \cup B.p \Rightarrow B.m \subseteq B.n \quad . \end{aligned}$$

Betting that the properties of the elements of these bags —in particular, primality— are irrelevant, we decide to investigate for arbitrary bags M , N , and P :

$$(5) \quad M \subseteq N \cup P \Rightarrow M \subseteq N \quad .$$

In JAW3, we translated (5) into a demonstrandum about sets, so that we could exploit predicate calculus. Here we stick with bags, and see what we can derive. Our first task is to analyze the subbag relation \subseteq .

With X and Y as sets, we can characterize the subset relation with the nice equivalence

$$X \subseteq Y \equiv [\chi.X \Rightarrow \chi.Y] \quad ,$$

where the function χ takes sets to their characteristic predicates. But with X and Y as bags, we are not as fortunate, because characteristic predicates do not fully capture baghood —we need to capture how many of each element is in a bag, as well—. To capture the subbag relation, I propose the sensible

$$(6) \quad X \subseteq Y \equiv \langle \forall e :: \#_e X \leq \#_e Y \rangle \quad ,$$

where e ranges over elements of the “domain of discourse” , and where $\#_e$ is the unary prefix operator defined by

$$\#_e X = \text{the number of occurrences of } e \text{ in } X \quad .$$

In practice, we replace

$$\langle \forall e :: \dots \#_e \dots \rangle$$

with the more convenient

$$[\dots \# \dots] \quad ,$$

leaving e implicit.

Besides (6) , we have the following nice properties of $\#$ —proofs again left to the reader— :

$$(7) \quad [\#(X \cup Y) = \#X + \#Y] \quad ,$$

$$(8) \quad [\#(X \cap Y) = \#X \mathbf{min} \#Y] \quad ,$$

$$(9) \quad [\#X = 0] \equiv X = \emptyset \quad .$$

Thus we calculate:

$$\begin{aligned} & (5) \\ & = \{ (6) , \text{twice} \} \\ & \quad [\#M \leq \#(N \cup P)] \Rightarrow [\#M \leq \#N] \\ & = \{ (7) \} \\ & \quad [\#M \leq \#N + \#P] \Rightarrow [\#M \leq \#N] \\ & \Leftarrow \{ \text{pred. calc., to simplify} \} \\ & \quad [\#M \leq \#N + \#P \Rightarrow \#M \leq \#N] \quad . \end{aligned}$$

Now this last formula is about naturals, and therefore we investigate —in an Interlude— the formula

$$(10) \quad a \leq b + c \Rightarrow a \leq b \quad ,$$

for arbitrary naturals a , b , and c .

Interlude. We seek some condition \mathbf{C} on a , b , and c implying (10). Which of a , b , and c must \mathbf{C} crucially depend on?

Should \mathbf{C} depend on a ? Most likely yes, because (10) is a formula of the form

$$(11) \quad R.(b+c) \Rightarrow R.b \quad ,$$

where the relation R depends on a . If \mathbf{C} did not depend on a , then \mathbf{C} would be a condition implying (10)/(11) for any a , which seems unlikely. However, in one case (11) is trivially satisfied for any a —indeed for any R —: when $b+c$ and b are the same natural; that is, when

$$\begin{aligned} & b+c=b \\ \equiv & \{ \text{algebra} \} \\ & c=0 \quad . \end{aligned}$$

Should \mathbf{C} depend on b ? Here the answer is not so clear, and we return to this question below.

Should \mathbf{C} depend on c ? As with a , the answer is most likely yes, since c is present in the left side of (10)/(11), but not the right. However, if \mathbf{C} did not depend on c , then with respect to \mathbf{C} , $b+c$ and b would be two arbitrary naturals. Thus in order to conclude (10)/(11) from \mathbf{C} , we would need R to hold for all naturals; in other words

$$\begin{aligned} & \langle \forall x :: R.x \rangle \\ \equiv & \{ \text{def of } R \} \\ & \langle \forall x :: a \leq x \rangle \\ \equiv & \{ \text{property of } 0 \} \\ & a=0 \quad . \end{aligned}$$

Now let us return to the question of whether \mathbf{C} should depend on b . Sometimes when we wish to find a sufficient condition for another involving a variable, we may be able to formulate that sufficient condition entirely in terms of the one variable. But given the shape of (10), it is unlikely that we could find a \mathbf{C} dependent on b , yet not on a and c ; in other words, it is unlikely that b can enter the picture without being related to a and c in some way.

Looking at a and c , however, we see that \mathbf{C} must depend on a , except given a certain condition on c , and that \mathbf{C} must depend on c , except given a certain condition on a . Thus these “certain” conditions are self-sufficient: By including both “certain” conditions in \mathbf{C} , we satisfy the requirement that \mathbf{C} be dependent on a and c , and b never enters the picture. Combining this observation with the desire to keep things simple, we conclude that \mathbf{C} is probably not crucially dependent on b .

Because we are trying to find a sufficient condition for (10), we would like \mathbf{C} to be as weak as possible, and so we combine the “certain” conditions $a = 0$ and $c = 0$ as weakly as possible; ie via disjunction. Thus we let

$$\mathbf{C} \equiv a = 0 \vee c = 0$$

be our sufficient condition for (10). (End of Interlude.)

With this in mind, we continue our derivation from before:

$$\begin{aligned} & M \subseteq N \cup P \Rightarrow M \subseteq N \\ \Leftarrow & \{ \text{see above} \} \\ & [\#M \leq \#N + \#P \Rightarrow \#M \leq \#N] \\ \Leftarrow & \{ (10) \Leftarrow \mathbf{C}, \text{ with } a, b, c := \#M, \#N, \#P \} \\ & [\#M = 0 \vee \#P = 0] \\ = & \{ \text{property of } \mathbf{min}, \text{ heading towards using (8)} \} \\ & [\#M \mathbf{min} \#P = 0] \\ = & \{ (8) \} \\ & [\#(M \cap P) = 0] \\ = & \{ (9) \} \\ & M \cap P = \emptyset \quad ; \end{aligned}$$

in other words,

$$(12) \quad (M \subseteq N \cup P \Rightarrow M \subseteq N) \Leftarrow M \cap P = \emptyset \quad .$$

This is delightful, and allows us to conclude our investigation thus:

$$\begin{aligned} & m \sqsubseteq n * p \Rightarrow m \sqsubseteq n \\ = & \{ \text{see first section} \} \\ & B.m \subseteq B.n \cup B.p \Rightarrow B.m \subseteq B.n \\ \Leftarrow & \{ (12), \text{ with } M, N, P := B.m, B.n, B.p \} \\ & B.m \cap B.p = \emptyset \\ = & \{ (2) \} \\ & B.(m \mathbf{gcd} p) = \emptyset \\ = & \{ (4) \} \\ & m \mathbf{gcd} p = 1 \quad . \end{aligned}$$

Santa Cruz, 13 December 2004

Jeremy Weissmann
11260 Overland Ave. #21A
Culver City, CA 90230
USA
jeremy@mathmeth.com