Projekt Coq

Jakub Dmitruk, Jakub Szcześniak

11 czerwca 2024

Projekt miał na celu zbadanie podstawowych własności dotyczących pojęcia największego wspólnego dzielnika, w szczególności implementację na dwa sposoby algorytmu Euklidesa służącego do obliczania tegoż oraz dowód poprawności tych implementacji. Na projekt składają się dwa pliki typu .v. Jeden z nich zawiera definicje, twierdzenia i algorytmy dotyczące liczb naturalnych, drugi dotyczące liczb całkowitych.

1 Definicja NWD

Definicja 1 *Dla dowolnych liczb naturalnych a oraz b ich NWD nazywamy liczbę naturalną c taką, że c jest dzielnikiem a oraz c jest dzielnikiem b oraz dla każdy inny wspólny dzielnik liczb a i b również jest dzielnikiem c.*

W naszym projekcie użyliśmy funkcji pomocniczej "divides" zdefiniowanej jako relację dwóch liczb, jeśli jedna jest dzielnikiem drugiej. Dzięki temu mogliśmy zastosować powyższą definicję do wprowadzenia funkcji "gcd_rel" jako relację trzech liczb a, b oraz d, kiedy d jest największym wspólnym dzielnikiem dwóch pozostałych.

2 Twierdzenie o kombinacji liniowej

Twierdzenie 1 *Niech d będzie największym wspólnym dzielnikiem liczb a i b. Wówczas dla każdej pary liczb naturalnych x i y liczba d jest dzielnikiem liczby* $x * a + y * b$.

Dowód 1 *Skoro d jest dzielnikiem a, to istnieje* k_1 *takie, że* $a = d*k_1$. *Podobnie istnieje* k_2 *takie, że* $b = d*k_2$. *Teraz łatwo zauważyć, że d jest dzielnikiem liczby* $x*a+y*b = x*k_1*d+y*k_2*d$. □

Dowód w Coq sprowadza się do rozbicia naszej wiedzy na czynniki pierwsze, w celu uzyskania bezpośredniego dostępu do liczb k_1 oraz k_2. Po podstawieniu ich w liczbie $x * a + y * b$ do końca dowodu potrzebujemy już tylko taktyki "ring", która wykorzystuje własność pierścienia do uproszczenia wyrażenia.

3 Algorytm Euklidesa

Algorithm 1: Algorytm Euklidesa

Data: Liczby naturalne a oraz b.
Result: Największy wspólny dzielnik liczb a oraz b.
1. Jeśli $a = 0$, to **return** b;
2. W przeciwnym wypadku wywołaj rekurencyjnie algorytm dla argumentów b $(mod\ a)$ oraz a;

Istnieje również drugie sformułowanie algorytmu Euklidesa.

Algorithm 2: Algorytm Euklidesa 2

Data: Liczby naturalne a oraz b.
Result: Największy wspólny dzielnik liczb a oraz b.
1. Jeśli $a = b$, to **return** b;
2. Jeśli $a > b$ wywołaj rekurencyjnie algorytm dla argumentów $a - b$ oraz b;
3. Jeśli $b > a$ wywołaj rekurencyjnie algorytm dla argumentów $b - a$ oraz a;

W języku Coq możliwe jest tylko użycie pierwszego sformułowania. Coq dopuszcza te rekurencje, dla których ma pewność, że nie będą nieskończone. Pierwsze sformułowanie jest poprawne jest poprawne, gdyż w każdym kroku zmniejsza się wartość zmiennej a. I tak też zapisany algorytm Euklidesa znalazł się w naszym projekcie. Algorytm 2 chociaż wymaga więcej iteracji, wydaje się być prostszy w obsłudze i implementacji. Jednak w tym przypadku nie da się przewidzieć, która zmienna będzie maleć w kolejnych krokach. Dlatego implementacja tego algorytmu w języku Coq nie jest możliwa.

4 Dowód poprawności algorytmu

Twierdzenie 2 $NWD(a, b) = NWD(b \ mod \ a, a)$

Dowód 2 *Niech* $d := NWD(a, b)$. *Wówczas wiemy, że* d *jest dzielnikiem* a *oraz* d *jest dzielnikiem* b, *czyli istnieją takie* s *oraz* t, *że* $a = s * d$, $a\ b = t * d$. *Ponadto niech* $r := b \ mod \ a$, *czyli dla pewnego* p *mamy* $b = a * p + r$. *Zatem*

$$r = b - a * p = t * d - s * d * p = (t - s * p) * d.$$

Wobec tego d *jest również dzielnikiem* r. □

Twierdzenie 3 *Algorytm Euklidesa poprawnie oblicza największy wspólny dzielnik i zawsze się zakończy.*

Dowód 3 *Dzięki poprzedniemu twierdzeniu prosta indukcja po* a *dowodzi poprawności algorytmu. Również dzięki temu, że wartość* a *maleje w każdym kroku, mamy gwarancję, że algorytm zawsze się zakończy.* □

Ten wydawałoby się prosty dowód okazał się dla nas przeszkodą nie do przeskoczenia. Prawdopodobnie głównym problemem było rozpisanie w sposób operatywny funkcji "mod", jednak ze względu na finalne niepowodzenie trudno wskazać jednoznaczną przyczynę.

5 Bonus

Nie udało nam się udowodnić poprawności algorytmu Euklidesa, jednak w ramach własnej inwencji twórczej sformułowaliśmy i udowodniliśmy całą masę lematów dotyczących własności NWD, które potencjalnie byłyby użyteczne dla tego dowodu.

Twierdzenie 4 $NWD(a, b) = NWD(b, a)$

Twierdzenie 5 $NWD(a, 0) = a$

Twierdzenie 6 $NWD(a, -b) = NWD(b, a)$

Twierdzenie 7 $NWD(a, b) = -NWD(b, a)$

Matematycznie dowody tych twierdzeń są natychmiastowymi wnioskami, natomiast w języku Coq składa się na nie ciąg oparty na wbudowanej serii twierdzeń "Z.divide" reprezentującej własności podzielności dla liczb całkowitych. Szczegóły dowodów i użycia tychże twierdzeń znajdują się w kodzie naszego projektu.

Twierdzenie 8 *Dla każdej trójki liczb całkowitych a, b, d oraz q, jeśli d dzieli a oraz d dzieli b, to d dzieli również liczbę $a - q * b$.*

Dowód 4 *Skoro d dzieli a, to istnieje liczba k_1 taka, że $a = k_1 * d$. Podobnie, Skoro d dzieli b, to istnieje liczba k_2 taka, że $b = k_2 * d$. Zatem istnieje liczba $k_1 - q * k_2$, którą możemy podstawić do definicji podzielności w tezie. Zastosowanie własności rozdzielności mnożenia względem odejmowania kończy dowód.* □

Warto zauważyć, że rozdzielność mnożenia względem odejmowania jest własnością pierścieni. Zatem za zastosowanie jej w języku Coq odpowiada taktyka "ring".

6 Algorytm Euklidesa w semantyce relacyjnej

Algorytm Euklidesa można zapisać nie tylko jako funkcję rekurencyjną, ale też relację trzech liczb naturalnych. Reprezentuje go typ "euclid" postaci "nat -¿ nat -¿ nat -¿ Prop" o trzech konstruktorach:

1. Dla każdego a liczby a a a są w relacji "euclid". Odowiada to temu, że dla dwóch takich samych liczb, ich NWD jest im równe i taką wartość zwraca algorytm Euklidesa.

2. Dla każdych liczb a, b, z, jeśli $a < b$ i liczby $a, (b - a)$ oraz z są w relacji "euclid", to również liczby a, b, z są w tej relacji. Odpowiada to krokowi algorytmu Euklidesa z wersji 2 w przypadku $a < b$.

3. Dla każdych liczb a, b, z, jeśli $b < a$ i liczby $(a - b), b$ oraz z są w relacji "euclid", to również liczby a, b, z są w tej relacji. Odpowiada to krokowi algorytmu Euklidesa z wersji 2 w przypadku $b < a$.

7 Dowód terminancji

Twierdzenie 9 *Dla każdej pary liczb naturalnych $a > 0$ oraz $b > 0$ istnieje liczba naturalna z taka, że liczby a, b oraz z są w relacji "euclid".*

W języku matematyki dowód tego twierdzenia wydaje się być prostym wnioskiem. Niestety, zapisanie go w języku Coq jest już dużo większym wyzwaniem, któremu nie sprostaliśmy.

Spis treści