ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1986
Seria: AUTOMATYKA z. 84 Nr kol. 894

Tomasz Szmuc
Akademia Górniczo-Hutnicza

DOWODZENIE POPRAWNOŚCI PROGRAMÓW STEROWANIA DYSKRETNYMI PROCESAMI

Streszczenie. W pracy rozważa się zagadnienie dowodzenia poprawności programów /systemów/ współbieżnych. Poprawność jest rozumiana jako relacja między procesem opisującym system współbieżny, a procesem specyfikującym wymagania. Operacje równoległego i sekwencyjnego połączenia procesów stanowią narzędzie dekompozycji. Relacja makrohomomorfizmu opisująca zależność między procesem, a jego strukturą dekompozycji jest wykorzystywana przy dowodzeniu poprawności.

1. Wprowadzenie i motywacje

Weryfikacja poprawności programów współbieżnych jest bardzo ważnym problemem pojawiającym się na etapie projektowania i implementacji oprogramowania systemów sterowania procesami dyskretnymi. W pracach [3,4] sformułowano zagadnienie poprawności programów /systemów/ współbieżnych. Proponowane podejście charakteryzują następujące założenia:

1. system współbieżny opisuje się jako sekwencyjny niedeterministyczny proces [4];
2. poprawność jest zdefiniowana jako pewna relacja między procesem opisującym system współbieżny a zadanymi wymaganiami, tzw. kryterium poprawności. Rozważa się poprawność systemu w sensie kryterium [3], co różni proponowane podejście względem dotychczas stosowanych.

Naturalnym kierunkiem dalszych działań, zmierzających do rozwiązania postawionego problemu, jest jego dekompozycja. W rozważanym przypadku dekompozycja może dotyczyć procesu opisującego system współbieżny, jak również procesu opisującego wymagania /tzw. proces kryterialny/. Zagadnienie to podejmuje niniejsza praca. Zdefiniowano w niej operacje równoległego i sekwencyjnego połączenia procesów. Stanowią one pewne uogólnienie rozważanych w [5] operacji. Następnie przedstawiono twierdzenia o reprezentacji dowolnego procesu dyskretnego za pomocą procesów elementarnych /jednostkowych/. Twierdzenia te znajdują zastosowanie przy dekompozycji procesu kryterialnego - dowodzenie elementarnych własności procesu. Dalszym pojęciem jest tzw. wyrażenie nad rodziną procesów, które stanowi poprawnie sformułowane wyrażenie, składające się z symboli procesów oraz symboli operacji połączeń /dopuszcza się użycie nawiasów/. Pojęcie to opisuje strukturę dekompozycji procesu i jest wykorzystywane przy dowodzeniu poprawności procesów.

Większość używanych oznaczeń jest zgodna z konwencją, przyjętą w poprzednich pracach. Dla dowolnej relacji $T \subseteq X \times Y$ będziemy pisać $T(x,y)$

jeśli element x jest w relacji T z elementem y. Jeśli $T \subseteq X \times Y$ jest relacją, to jej dziedzinę /przeciwdziedzinę/ oznaczać będziemy Dom T /Ran T/. Dla dowolnego $x \in$ Dom T będziemy definiować $T(x) = \{y \mid T(x,y)\}$ oraz odpowiednio, dla dowolnego $y \in$ Ran T : $T^{-1}(y) = \{x \mid T(x,y)\}$. Jeśli $A \subseteq X$, to obraz zbioru A względem relacji T oznaczać będziemy $T(A) = \bigcup_{x \in A} T(x)$, jeśli $B \subseteq Y$, to przeciwobrazem B względem tej relacji będzie odpowiednio zbiór $T^{-1}(B) = \bigcup_{y \in B} T^{-1}(y)$. Natomiast w przypadku, gdy T jest funkcją, będziemy pisać $T(x) = y$, gdzie y jest odpowiednim elementem przeciwdziedziny. Fakt ten będzie wynikał jednoznacznie z kontekstu i nie będzie prowadził do nieporozumień.

2. Pojęcia podstawowe

Podstawowym pojęciem używanym w pracy jest proces Pawlaka [1,2], który był wprowadzony w celu opisu działania komputera oraz był stosowany do badania własności programów /algorytmów/ deterministycznych. W naszych rozważaniach będziemy korzystać z procesu niedeterministycznego /relacyjnego/, którego będziemy używać do opisu badanego systemu współbieżnego [4], jak również do opisu wymagań poprawnościowych /proces kryterialny/.

Definicja 1. Procesem nazywamy czwórkę, $P = (S,B,F,T)$, gdzie:

S - zbiór /co najwyżej przeliczalny/ stanów procesu,

$B \subseteq S$ - zbiór stanów początkowych,

$F \subseteq S$ - zbiór stanów końcowych,

$T \subseteq S \times S$ - relacja przejścia oraz spełnione są warunki:

1. $B \subseteq$ Dom T ; 2. $F \cap$ Dom $T = \emptyset$.

Dowolny proces $P = (S,B,F,T)$ nazywamy:

1. procesem trywialnym wtw $S = F$ /w przeciwnym przypadku nietrywialnym/
2. procesem elementarnym wtw $S = B \cup F$;
3. procesem jednostkowym wtw P jest procesem elementarnym oraz

$$\text{card}(S) = \begin{cases} 1 & \text{jeśli } B = \emptyset \\ 2 & \text{w przeciwnym przypadku ;} \end{cases}$$

4. procesem spójnym wtw $(\forall s_1 \in S)(\exists s \in B)\ T^*(s,s_1)$, gdzie T^* oznacza przechodnie /T^+/ i zwrotne /T^0/ domknięcie relacji T.

Definicja 2. Niech będą dane procesy $P = (S,B,F,T)$, $P' = (S',B',F',T')$ oraz funkcja $h : S \longrightarrow S'$. Mówimy, że h jest homomorfizmem między procesami P,P' i zapisujemy $P \xrightarrow{h} P'$ wtw spełnione są warunki:

1. $h(\text{Dom } T) \subseteq \text{Dom } T'$;
2. $(\forall s \in \text{Dom } T)\ h(T(s)) \subseteq T'(h(s))$;
3. $h(B) \subseteq B' \wedge h(F) \subseteq F'$.

Definicja 3. Niech będzie dany proces $P = (S,B,F,T)$. Dowolny ciąg n /$n \geqslant 1$/ stanów procesu $sc(s_1,\cdot) = (s_1,s_2,\ldots)$ nazywamy semiobliczeniem wtw dla każdych dwóch kolejnych elementów s_i, s_{i+1} tego ciągu zachodzi $T(s_i,s_{i+1})$.

Semiobliczenie skończone, rozpoczynające się w stanie s_1, a kończące się w stanie s_n oznaczać będziemy $sc(s_1,s_n)$, natomiast semiobliczenie nieskończone - odpowiednio $sc(s_1,\infty)$. Zbiór wszystkich stanów tworzących semiobliczenie sc będziemy oznaczać $Z(sc)$.

Semiobliczenie $sc(s_1,\cdot)$ takie, że $s_1 \in B$ będziemy nazywać <u>obliczeniem</u> wtw $s_n \in P$ dla $sc(s_1,\cdot) = sc(s_1,s_n)$ lub jeśli semiobliczenie to jest nieskończone, tj. $sc(s_1,\cdot) = sc(s_1,\infty)$.

3. Poprawność procesu

Zagadnienie weryfikacji poprawności systemu programów można sprowadzić do badania, czy kolejność następowanie stanów charakterystycznych jest zgodna z zadaną wcześniej kolejnością [3]. Jak już wspomniano wcześniej modelem weryfikowanego systemu będzie proces sekwencyjny. Odpowiednią konstrukcję system współbieżny - proces sekwencyjny, opisujący jego zachowanie, można znaleźć w pracy [4].

Przed zdefiniowaniem poprawności wprowadzimy pojęcia semiobliczenia dolnego i górnego. Konstrukcja jest tu podobna jak w pracy [3], pojęcia będą nieco uproszczone, natomiast definicja poprawności równoważna względem pierwotnej.

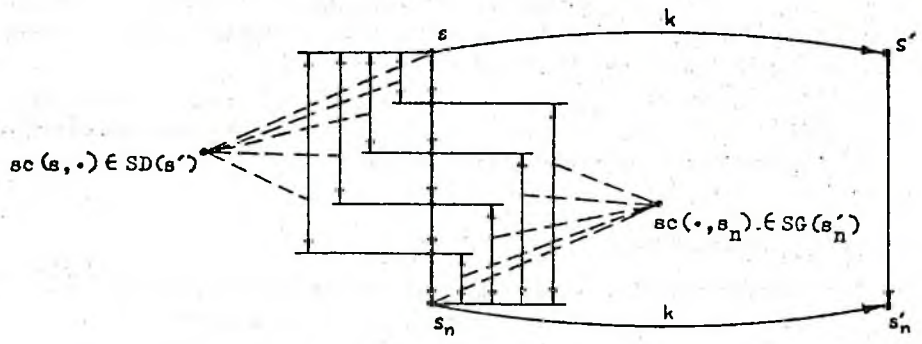
<u>Definicja 4</u>. Niech będą dane procesy $P = (S,B,F,T)$, $P' = (S',B',F',T')$ oraz relacja $k \subseteq S \times S'$. Dla dowolnych stanów s,s', takich że $k(s,s')$ definiujemy:

1. Semiobliczenie dolne, reprezentujące stan s' - dowolne semiobliczenie $sc(s,\cdot)$ spełniające warunek:
$$(\forall s_1 \in Z(sc(s,\cdot)))\ (\forall s_1' \in k(s_1))\ \neg T'(s',s_1')\ ,$$
2. Semiobliczenie górne, reprezentujące stan s' - dowolne semiobliczenie $sc(\cdot,s)$ takie, że:
$$(\forall s_1 \in Z(sc(\cdot,s)))\ (\forall s_1' \in k(s_1))\ \neg T'(s',s_1')\ .$$

Zbiór obliczeń dolnych /górnych/, reprezentujących stan $s' \in Ran\ k$ oznaczać będziemy $SD(s')$ /$SG(s')$/. Ilustracja graficzna pojęć przedstawionych w powyższej i poniższej definicji jest prezentowana na rys.1.

<u>Definicja 5</u>. Niech będą dane procesy $P = (S,B,F,T)$, $P' = (S',B',F',T')$ oraz relacja $k \subseteq S \times S'$. Mówimy, że proces P jest poprawny w sensie kryterium (P',k) wtw spełnione są warunki:

1. $\{s' \mid (\exists s \in B)\ (\exists sc(s,\cdot))\ sc(s,\cdot) \in SG(s')\} \subseteq B'$;
2. $\{s' \mid (\exists s \in F)\ (\exists sc(\cdot,s))\ sc(\cdot,s) \in SD(s')\} \subseteq F'$;
3. dla dowolnego $s_n' \in Ran\ k \cap Ran\ T'$ istnieje stan $s' \in Ran\ k$ i semiobliczenie $sc(s,s_n)$, takie że $T'(s',s_n')$ oraz spełniona jest koniunkcja:
$$sc(s,s_{n-1}) \in SD(s') \wedge sc(s_1,s_n) \in SG(s_n')\ ,$$
gdzie $sc(s,s_{n-1})$ /$sc(s_1,s_n)$/ oznacza semiobliczenie uzyskane z semiobliczenia $sc(s,s_n)$ po odłączeniu ostatniego /pierwszego/ elementu ciągu.



Rys.1.Interpretacja graficzna pojęć związanych z poprawnością
Fig.1.An illustration of notions related to the correctness

4. Dekompozycja procesu

W rozdziale definiuje się operacje równoległego i sekwencyjnego połączenia procesów. Operacje te bazują na mnogościowopodobnej sumie procesów [6,7]. Oznacza to, że wynikiem operacji połączenia jest suma łączonych procesów, natomiast rodzaj połączenia /równoległe lub sekwencyjne/ jest określony przez wzajemne położenie zbiorów stanów początkowych i końcowych łączonych procesów. Operacja sumy mnogościowopodobnej została zdefiniowana w pracy [6], poniżej podano nieformalny opis przeprowadzonej tam konstrukcji.

Dla dowolnych dwóch procesów, składników operacji sumy określa się odpowiadające im zbiory semiobliczeń i zbiory obliczeń. Następnie, poprzez sumowanie mnogościowopodobne, oblicza się sumy tych zbiorów, czyli określa się zbiór obliczeń, który można utworzyć z odpowiednich semiobliczeń obliczeń należących do zbiorów obliczeń procesów składowych oraz zbiór semiobliczeń, który można utworzyć z semiobliczeń należących do zbiorów semiobliczeń procesów składowych. Uzyskany w ten sposób zbiór obliczeń i zbiór semiobliczeń opisują proces, będący wynikiem sumowania. W konstrukcji tej korzysta się z faktu jednoznacznej reprezentacji procesu za pomocą zbioru obliczeń i zbioru semiobliczeń. Należy dodać, że dla procesów spójnych konstrukcja ta upraszcza się, gdyż każdy proces, należący do tej klasy, jest jednoznacznie reprezentowany za pomocą zbioru obliczeń [6]

Definicja 6. Niech będą dane procesy $P_1 = (S_1,B_1,F_1,T_1)$, $P_2 = (S_2,B_2,F_2,T_2)$ oraz $\overline{\cup}$ mnogościowopodobna suma procesów [9] opisana powyżej.

1. Proces $P = P_1 \overline{\cup} P_2$ jest uogólnionym równoległym połączeniem procesów

P_1 i P_2, $P = P_1 + P_2$ wtw $(F_1 \cap B_2) \cup (F_2 \cap B_1) = \emptyset$ lub $P_1 = P_2$.

2. Proces $P = P_1 \overline{\cup} P_2$ jest uogólnionym sekwencyjnym połączeniem procesów P_1 i P_2, $P = P_1 \cdot P_2$ wtw $F_1 \cap B_2 \neq \emptyset$.

Algebraiczne własności operacji połączeń są analizowane w pracy [7]. W niniejszej podane zostaną wyłącznie te, które są istotne z punktu widzenia dekompozycji.

Definicja 7. Niech $\mathcal{P}$ będzie zbiorem symboli procesów, należących do rodziny $\{P_i\}_{i \in I}$ /$I \subseteq \mathbb{N}$/, natomiast + oraz · symbolami operacji połączeń. Wyrażeniem /nad rodziną procesów/ nazywamy każde słowo E, które może być wygenerowane za pomocą następujących reguł:

1. $E = P_i$ dla każdego $P_i \in \mathcal{P}$;
2. jeśli E jest wyrażeniem, to następujące słowa są również wyrażeniami:

   a. (E); b. $P_i \square E$ lub $E \square P_i$ dla każdego $P_i \in \mathcal{P}$ oraz $\square \in \{+, \cdot\}$.

Wyrażenie, które jest skonstruowane z tych i tylko tych symboli procesów, które należą do $\mathcal{P}$, będziemy oznaczać $E(\mathcal{P})$. Mówimy, że proces P jest reprezentowany przez wyrażenie $E(\mathcal{P})$, $P = E(\mathcal{P})$ wtw P jest symbolem procesu, który jest wynikiem operacji połączeń specyfikowanych w wyrażeniu.

Twierdzenie 1. Dowolny proces P może być reprezentowany przez wyrażenie $E(\mathcal{P})$, gdzie $\mathcal{P}$ jest zbiorem symboli procesów elementarnych.

Twierdzenie 2. Dowolny proces P może być reprezentowany przez wyrażenie $E(\mathcal{P})$, gdzie $\mathcal{P}$ jest zbiorem symboli procesów jednostkowych.

Dowody powyższych stwierdzeń można znaleźć w pracy [5], gdzie zdefiniowano wprawdzie nieco inaczej operacje połączeń, lecz łatwo można wykazać, że dla procesów elementarnych /a tym samym i jednostkowych/ są one równoważne operacjom tu rozważanym.

5. Dekompozycja zagadnienia poprawności

Wyrażenie zdefiniowane w poprzednim rozdziale opisuje strukturę dekompozycji procesu. Struktura ta będzie określona poniżej za pomocą pojęcia procesu. Stąd specyfikacja na dwóch poziomach abstrakcji będzie realizowana za pomocą tego samego pojęcia. Umożliwi to zdefiniowanie relacji między tymi dwoma poziomami abstrakcji. Relacja ta, tzw. makrohomomorfizm, będzie wykorzystywana do dekompozycji problemu poprawności.

Proces opisujący wyrażenie /proces nad wyrażeniem/ będzie określony dla tzw. wyrażenie rozwiniętego [7]. Dowolne wyrażenie nazywamy rozwiniętym wtw jeśli składa się wyłącznie z symboli procesów i operacji połączeń /bez nawiasów/.

Definicja 8. Niech będzie dane wyrażenie rozwinięte $E(\mathcal{P})$, reprezentujące proces P. Procesem nad wyrażeniem E nazywamy czwórkę $P_E = (S_E, B_E, F_E, T_E)$, gdzie:

$S_E = \mathcal{P}$ - zbiór symboli procesów wyrażenia E ,

$B_E \subseteq S_E$ - zbiór tych wszystkich symboli procesów P_i , przy których po ich lewej stronie występuje znak + lub nie występuje żaden znak, natomiast po prawej stronie znajduje się znak · oraz spełniony jest warunek: $S_i \cap B \neq \emptyset$,

$F_E \subseteq S_E$ - zbiór tych wszystkich symboli procesów P_i , przy których po ich prawej stronie występuje znak + lub nie znajduje się żaden znak oraz spełniony jest warunek: $S_i \cap P \neq \emptyset$,

$T_E \subseteq S_E \times S_E$ - relacja określona następująco:

$T_E(P_i, P_j)$ wtw w wyrażeniu E występuje zapis $P_i \cdot P_j$.

Konstrukcja przeprowadzona w pracy [7] prowadzi do stwierdzenia, że wszystkie rozwinięcia dowolnego wyrażenia są równoważne /reprezentują ten sam proces/. Będziemy korzystać z tego faktu, oznaczając przez P_E proces reprezentujący dowolne wyrażenie E . Należy zauważyć, że dla dowolnego wyrażenia istnieje dokładnie jeden proces określony jak wyżej.

Definicja 9. Niech będą dane procesy P, P' , wyrażenie $E(\mathcal{P})$ reprezentujące proces P oraz funkcja $h : \mathcal{P} \longrightarrow S'$.

1. Mówimy, że procesy P, P' są makrohomomorficzne wtw h jest homomorfizmem procesu P_E w proces P' , $P_E \xrightarrow{h} P'$.
2. Relacją makrohomomorfizmu będziemy nazywać relację $k \subseteq S \times S'$ określoną za pomocą warunków:
   a. $k(s,s') \Longrightarrow (\exists P_i \in \mathcal{P})\ (s \in S_i \wedge h(P_i) = s')$;
   b. dla dowolnych $(P_i, P_j) \in T_E$ oraz dla każdego $s \in F_i \cap B_j$ spełnione są warunki:
      (i) $\neg k(s, h(P_i))$ jeśli P_i jest procesem nietrywialnym,
      (ii) $\neg k(s, h(P_j))$ jeśli P_i jest procesem trywialnym.
   c. dla dowolnych $(P_i, P_j) \in T_E^+$, takich że $B_i \cap P_j \neq \emptyset$ spełniony jest warunek:
      $(\forall s \in B_i \cap P_j)\ \neg k(s, h(P_j))$.

   Jeśli k jest makrohomomorfizmem procesu P w proces P' , to fakt ten będziemy zapisywać $P \xrightarrow{k} P'$.

W pracy [8] udowodniono szereg twierdzeń pokazujących własności relacji makrohomomorfizmu. Niżej podane zostaną najważniejsze z nich. Ze względu na brak miejsca twierdzenia te będą cytowane bez dowodu. We wspomnianej pracy podano również szczegółową interpretację warunków przedstawionych w powyższej definicji.

Twierdzenie 3. Jeśli dane są procesy P, P' oraz homomorfizm h , $P \xrightarrow{h} P'$, to istnieje również makrohomomorfizm k procesu P w proces P'.

Twierdzenie 4. Niech $\{P_i\}_{i \in I}$, $\{P'_j\}_{j \in J}$ będą rodzinami procesów oraz $\{k_i\}_{i \in I}$ zbiorem makrohomomorfizmów spełniających warunek:

$(\forall i \in I)\ P_i \xrightarrow{k_i} h(P_i)$, gdzie $h : \mathcal{P} \longrightarrow \mathcal{P}'$.

Jeśli proces P jest reprezentowany przez wyrażenie $E(\mathcal{P})$ /nad rodziną

$\{P_i\}_{i \in I}$/, proces P' jest reprezentowany przez wyrażenie $E'(P')$ /nad rodziną $\{P'_j\}_{j \in J}$/ oraz h jest homomorfizmem $P_E \xrightarrow{h} P_{E'}$, to istnieje makrohomomorfizm $P \xrightarrow{k} P'$.

Z twierdzenia 3 wynika, że makrohomomorfizm jest pewnym uogólnieniem homomorfizmu. Nieformalnie mówiąc jest to homomorfizm określony z dokładnością do dekompozycji procesu P na procesy składowe. W przypadku, gdy jest to dekompozycja na procesy jednostkowe i trywialne, wówczas makrohomomorfizm staje się homomorfizmem /por. dowód twierdzenia 3 w pracy [8]/. Natomiast twierdzenie 4 pokazuje sposób dekompozycji procesów makrohomomorficznych. Oznacza to, że istnienie makrohomomorfizmu między procesami P, P' może być wykazane przez dekompozycję tych procesów na procesy składowe oraz dowodzenie odpowiednich makrohomomorfizmów między tymi procesami składowymi. Warunek specyfikowany w tezie twierdzenia określa zależności, które muszą być spełnione przez makrohomomorfizmy składowe.

W cytowanej już pracy dowodzi się również równoważności między relacją poprawności a odpowiednim makrohomomorfizmem. Twierdzenie to jest prawdziwe dla dowolnej dekompozycji, spełniającej warunki:

- każdy proces jest dekomponowany na procesy spójne lub trywialne,
- dowolne połączenie sekwencyjne $P_1 \cdot P_2$ jest określone dla procesów spełniających warunek $(S_1 \setminus (B_1 \cup F_1)) \cap (S_2 \setminus (B_2 \cup P_2)) = \emptyset$.

Twierdzenie 5. Niech będą dane procesy P, P' oraz relacja $k \subseteq S \times S'$. Proces P jest poprawny w sensie kryterium (P', k) wtw $P \xrightarrow{k_1} P'$, gdzie $k_1 \subseteq S \times S'$ jest relacją określoną następująco:

$$k_1(s, s') \text{ wtw } \begin{cases} (\exists sc \in SD(s') \cup SG(s'))\ s \in Z(sc) & \text{jeśli } s' \in B' \cup \overline{\text{Ran } T'}, \\ (\exists sc \in SD(s'))\ s \in Z(sc) & \text{w przeciwnym przypadku,} \end{cases}$$

przy czym zbiory $SD(s')$, $SG(s')$ są określone za pomocą relacji k, natomiast $\text{Ran } T' = S' \setminus \text{Ran } T'$.

Powyższe twierdzenie umożliwia sprowadzenie problemu poprawności procesu do badania istnienia odpowiedniego makrohomomorfizmu. Implikuje to postępowanie, w którym wyróżnić można dwa następujące etapy:

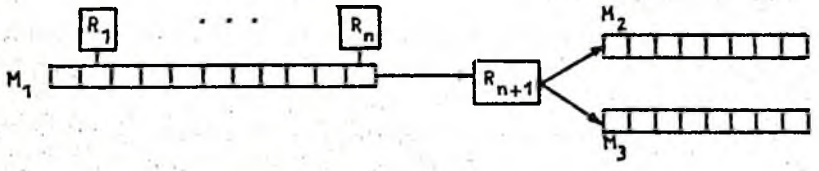
1. Konstruowanie rodziny procesów $\{P_i\}_{i \in I}$ oraz wyrażenia $E(P)$.
2. Badanie istnienia homomorfizmu $P_E \xrightarrow{h} P'$.

Czynności wymienione w punkcie 1 związane są z agregacją stanów weryfikowanego procesu i mogą być realizowane, jak to pokazano w dowodzie twierdzenia 5 /zamieszczonego w pracy [8]/. W punkcie 2 określono natomiast działanie na poziomie makro: badanie homomorfizmu między procesami P_E, P'.

6. Poprawność systemu sterowania robotami

Rozważmy kompleks złożony z robotów $R_1, \ldots, R_n, R_{n+1}$ zainstalowanych odpowiednio przy taśmie montażowej M_1 oraz korzystających z taśm - magazynów M_2, M_3 /rys. 2/. Roboty $R_1 - R_n$ realizują montaż wyrobów rozmieszczonych w pojemnikach taśmy montażowej M_1. Robot R_{n+1} bada stan

wykonanych wyrobów i przenosi prawidłowo wykonane na taśmę - magazyn M_2, zaś nieprawidłowo złożone na taśmę - magazyn M_3.



Rys.2. Kompleks współpracujących robotów

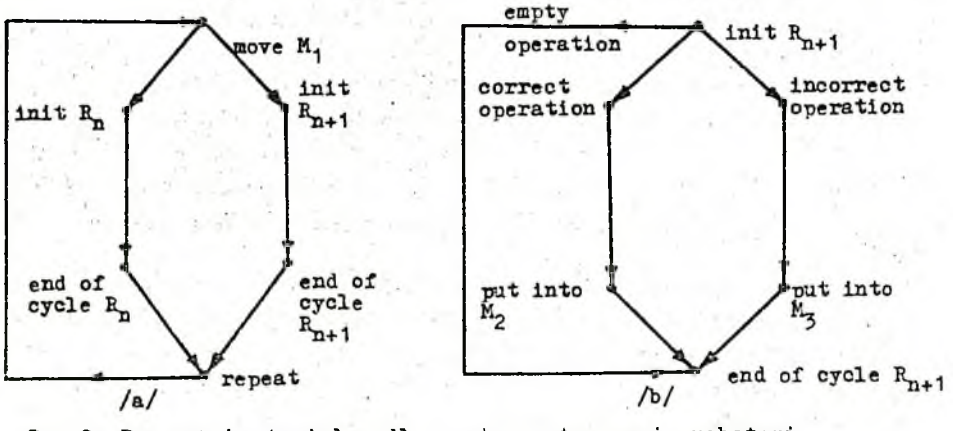
Fig.2. Cooperating robots

Taśma M_1 przesuwa się o jeden krok po wykonaniu cyklu wszystkich robotów. Taśmy M_2 i M_3 przesuwają się o jeden krok po każdorazowym przeniesieniu na nie odpowiedniego wyrobu.

Procesy kryterialne zdefiniujemy dla następujących warstw abstrakcji:

- współdziałanie robotów R_n, R_{n+1} /rys. 3 a/,
- sterowanie robotem R_{n+1} - rys. 3.b.

Stan procesu kryterialnego specyfikowany jest przez operację, której wykonanie rozpoczyna się w danym stanie, a jej zakończenie powoduje przejście do następnego stanu.



Rys.3. Procesy kryterialne dla systemu sterowania robotami

Fig.3. Criteria processes for control of robots

Zauważmy, że postępując podobnie można zdefiniować procesy kryterialne, odpowiadające niższym warstwom abstrakcji, np. sterowanie ramieniem robota. Uzyskujemy tym samym szereg makrohomomorficznych procesów, opisujących coraz to niższe warstwy systemu. Stąd przedstawiony formalizm znajduje zastosowanie na etapie projektowania systemu: podział na warstwy abstrakcji, projektowanie mechanizmów synchronizacji itp. Należy podkreślić, że poszczególne warstwy są opisane za pomocą tego samego modelu, jak również zależności między warstwami są precyzyjnie określone /twierdzenie 4/, co jest bardzo ważne w zagadnieniach projektowania niezawodnego opro-

gramowania.

Przejdźmy teraz do zagadnień weryfikacji poprawności. Wyrażenia reprezentujące odpowiednie procesy kryterialne dla problemów współdziałania robotów oraz sterowania pojedynczym robotem przedstawiono niżej. Odpowiednie operacje zapisano w skrócie za pomocą dwóch symboli, indeksy specyfikują natomiast obiekty, które są argumentami operacji. Za pomocą symboli primowanych oznaczono odpowiednie wyrażenia rozwinięte. Wyrażenia opisujące procesy kryterialne:

- system współdziałających robotów:

$$E_1 = MV_1 \cdot (IN_n \cdot EN_n + IN_{n+1} \cdot EN_{n+1}) \cdot RP \quad ,$$

$$E_1' = MV_1 \cdot IN_n \cdot EN_n \cdot RP + MV_1 \cdot IN_{n+1} \cdot EN_{n+1} \cdot RP \quad ;$$

- pojedynczy robot:

$$E_2 = IN \cdot (EM + CO \cdot PT_2 + IC \cdot PT_3) \cdot EN \quad ,$$

$$E_2' = IN \cdot EM \cdot EN + IN \cdot CO \cdot PT_2 \cdot EN + IN \cdot IC \cdot PT_3 \cdot EN \quad .$$

Zauważmy, że w rozważanych przypadkach wyrażenia opisujące procesy kryterialne są proste - stąd zagadnienie poszukiwania homomorfizmu /etap 2 dowodzenia poprawności/ nie powinno sprawiać kłopotu. Trudniejsza wydaje się realizacja etapu 1, zauważmy jednak, że rozbicie na warstwy abstrakcji znacznie upraszcza ten problem.

7. Zakończenie

Przedstawiona koncepcja opisu poprawności oraz zaproponowana metoda weryfikacji wydają się być szczególnie przydatne w zagadnieniach związanych z implementacją systemów sterowania dyskretnymi procesami. W systemach tych cel jest zazwyczaj precyzyjnie określony, stąd procesowy opis tego celu może stanowić kryterium poprawności na najwyższym poziomie abstrakcji opisu systemu. Dokonując następnie uszczegółowienia pojęcia stanu możemy przechodzić na niższe warstwy abstrakcji [3,4,7]. Każde dwie warstwy są połączone relacją makrohomomorfizmu. Badanie poprawności systemu odbywa się warstwami, z zachowaniem warunków specyfikowanych w twierdzeniu 4.

LITERATURA

[1] Bartol W., Raś Z., Skowron A.: Theory of Computing Systems, Banach Center Publications, Vol. 2, PWN 1977 /red. Mazurkiewicz A., Pawlak Z./

[2] Pawlak Z.: Maszyny programowane. Algorytmy, nr 10, 1969, 5-19.

[3] Szmuc T.: Procesowy opis zagadnienia poprawności systemów współbieżnych. Elektrotechnika, t. 4, z. 4, 1985, 427-438.

[4] Szmuc T.: Poprawność systemu procesów. Elektrotechnika, t. 4, z. 4, 1985, 439-454.

[5] Szmuc T.: Połączenia i dekompozycja procesów dyskretnych. Zeszyty Naukowe AGH, Automatyka, z. 39, 1985, 47-55.

[6] Szmuc T.: Uogólnione operacje na zbiorach obliczeń. Elektrotechnika, t. 5, z. 1, 1986 /w druku/.

[7] Szmuc T.: Uogólnione połączenia procesów. Elektrotechnika, t. 5, z. 1, 1986 /w druku/.

[8] Szmuc T.: Dowodzenie poprawności procesu przez dekompozycję. Elektrotechnika, t. 5, z. 2, 1986 /w druku/.

Recenzent: Dr hab.inż.Mirosław Zaborowski

Wpłynęło do Redakcji do 1986.04.30

ДОКАЗЫВАНИЕ КОРЕКТНОСТИ ПРОГРАММ УПРАВЛЕНИЯ ДИСКРЕТНЫМИ ПРОЦЕССАМИ

Р е з ю м е

В работе рассматривается доказывание корректности параллельных программ (систем) . Корректность определяется как отношение между последовательными процессами , изображающими параллельную систему и т.н. критериальным процессом , специфицирующим требования. Процесс Павляка является моделью последовательного процесса. Проверка корректности реализуется как при помощи разложения процесса , описывающего проверяемую систему так и разложения критериального процесса. С этой целью определяются операции параллельного и последовательного соединения процессов.Следущее понятие это выражение над семейством процессов, которое состоит из символов процессов символов операции соединений.Это понятие описывает структуру разложения процесса.Эта структура описана дальше при помощи понятия процесса , когда процесс над выражением определяется. Таким образом спецификация на двух уровнях абстракции реализуется при помощи такого же понятия. Следовательно определение отношения между этими уровнями возможно.Это отношение- т.н. макрогомоморфизм, используется для доказывания корректности. В работе представлены утверждения, описывающие разложение проверки корректности и даже описывающие эквивалентность отношения корктности и макрогомоморфизма. Таким образом проверка корректности сводится к исследованию соответствующих выражений , описывающих проверяемый и критериальный процессы. Результаты формальных исследований представлены на примере системы управления роботами.

PROVING OF CORRECTNESS OF DISCRETE PROCESSES CONTROL PROGRAMS

S u m m a r y

In the paper ,a correctness proving of parallel programs /system / is concidered.The correctness is defined by a relation between a sequen - tial process describing parallel system and so-called criterion process specifying correctness requirements. Nondeterministic Pawlaks process is chosen as a process model.The correctness proving is realized by a decom- position of a verified process as well of a criterion one.The parallel and sequential composition operations are define in order to obtain decomposi- tion tools. An expression over a family of processes is defined further on. It is a well formed expression that consist of processes symbols and of symbols of the composition operations.This notion describes a structure of a process decomposition.The structure is described by means of the pro- cess notion ,when a process over an expression is defined.Hence ,any two levels of abstration are specified using the same notion. Thus, a relation between the two description levels can be defined. This relation ,so-called macrohomomorphism is applied for proving the correctness.In the paper ,the the theorems specifying a decomposition of the correctness problem , and describing an equivalence between the correctness relation and macrohomo - morphism are present. It results from the conciderations that the correct- ness proving may be reduced to a comparison of corresponding expressions representing a verified process and a criterion. The result of the formal investigations are illustrated using an example of system of cooperating robots.