

9. Problem wzajemnego wykluczania i sekcji krytycznej

9.1 Przeplot i współużywalność zasobów

Wyróżniamy dwa rodzaje zasobów:

1. Zasoby współużywalne - mogą być wykorzystane przez dowolną liczbę procesów.
2. Zasoby nie współużywalne - w danym odcinku czasu mogą być wykorzystane tylko przez jeden proces.

Przykład zasobu nie współużywalnego

- urządzenia wejścia / wyjścia.
- wspólny obszar pamięci.

Gdy kilka procesów czyta a przynajmniej jeden dokonuje zapisu wynik odczytu zależy może od sposobu realizacji przeplotu .

Przykład 1 – wątki korzystają ze zmiennej dzielonej

```
#include <pthread.h>
#include <stdlib.h>
#define NUM_THREADS 8

pthread_t tid[NUM_THREADS]; // Tablica identyfik.
watkow
static int x;

void kod(int num) {
    for(;;) {
        x = 0;
        x = x+1;
        printf(„watek: %d wartość: %d\n”,num,x);
    }
}

int main(int argc, char *argv[]){
    int i;
    // Tworzenie watkow -----
    for (i = 0; i < NUM_THREADS; i++)
        pthread_create(&tid[i], NULL, kod,(void *)
        (i+1));
    ...
}
```

Wątek1	Wątek 2	Wątek 3	x
x=0			0
x = x + 1			1
	x=0		0
		x=0	0
printf x			0
	x = x + 1		1
	printf x		1
		x = x + 1	2
		printf x	2

Możliwa realizacja przykładu 1 – każdy watek daje inny wynik

```
Watek 1 wartosc 0
Watek 2 wartosc 1
Watek 3 wartosc 2
```

Wyniki działania przykładu 1

Przykład 2 – Bank wpłaty i wypłaty – problem utraconej aktualizacji

```
void wypłata (int konto, int kwota) {
    int stan;
    stan = czytaj(konto);
    pisz(konto, stan - kwota);
}
```

```
void wpłata (int konto, int kwota) {
    int stan;
    stan = czytaj(konto);
    pisz(konto, stan + kwota);
}
```

```
stan konta 1 - 100
stan konta 2 - 200
stan konta 3 - 300
```

Transakcja 1

Przeniesienie 10 zł z konta 1 na 2

```
wypłata(1,10);
wplata(2,10);
```

Transakcja 2

Przeniesienie 20 zł z konta 3 na 2

```
wypłata(3,20);
wplata(2,20);
```

Po transakcjach powinno być:

stan konta 1 - 90

stan konta 2 - 230

stan konta 3 - 280

Proces 1	Proces 2	K1	K2	K3
		100	200	300
Czytaj(1)->100		100	200	300
Pisz(1,100-10)		90	200	300
	Czytaj(3)->300	90	200	300
	Pisz(3,300-20)	90	200	280
Czytaj(2)->200		90	200	280
	Czytaj(2)->200	90	200	280
	Pisz(2,200+20)	90	220	280
Pisz(2,200+10)		90	210	280
		90	210	280

Wynik:

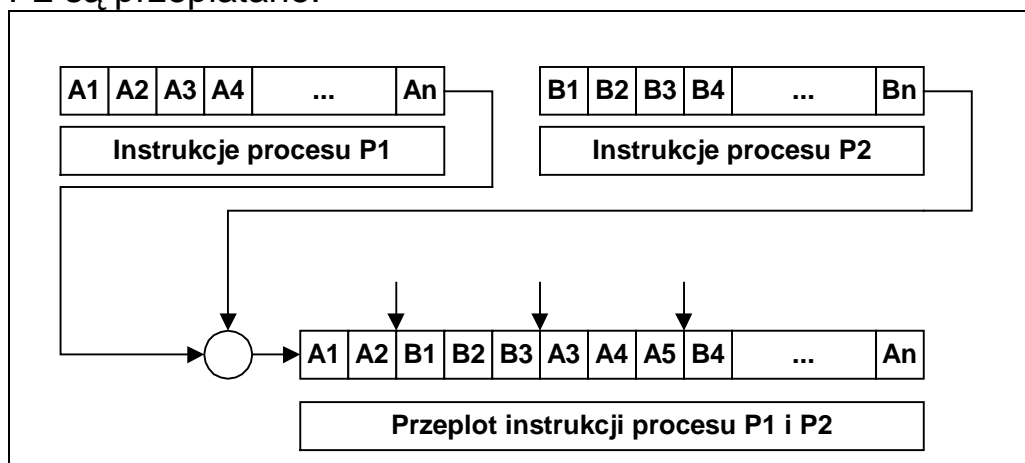
Z konta 2 znikło 10 zł

9.2 Problem wzajemnego wykluczania i warunki jego rozwiązania

Operacja atomowa

Sekwencja jednego lub wielu działań elementarnych które nie mogą być przerwane. Wykonuje się w całości albo wcale. Działania pośrednie nie mogą być obserwowane przez inny proces.

W poniższym przykładzie instrukcje atomowe kodu procesów P1 i P2 są przeplatane.



Instrukcje procesów P1 i P2 wykonywane w trybie przeplotu

- Nie możemy poczynić żadnych założeń dotyczących momentów przełączenia procesów P1 i P2
- W pewnych przypadkach nie da się określić wyniku działania powyższych procesów.

Wynik działania aplikacji współbieżnej nie może być uzależniony od sposobu przełączania procesów. Musi być prawidłowy dla wszystkich możliwych przeplotów.

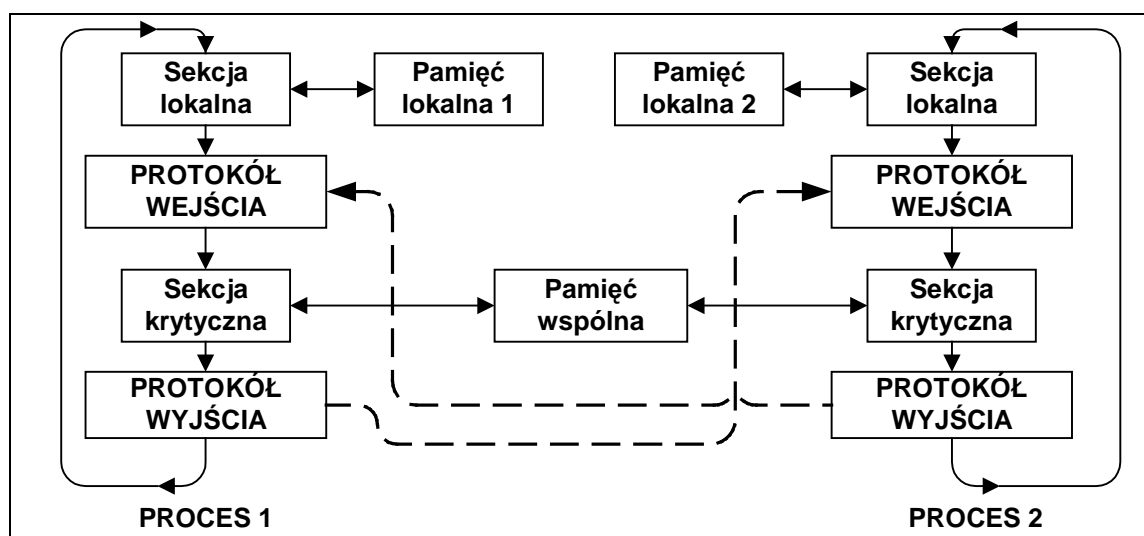
Gdy procesy współbieżne do wzajemnej komunikacji używają wspólnej pamięci, wyniki takiej komunikacji mogą okazać się przypadkowe. Prawidłowa komunikacja współbieżnych procesów przez wspólny obszar pamięci wymaga dotrzymania warunku wzajemnego wykluczania.

Wzajemne wykluczanie - wymaganie aby ciąg operacji na pewnym zasobie (zwykle pamięci) był wykonany w trybie wyłącznym przez tylko jeden z potencjalnie wielu procesów.

Sekcja krytyczna – ciąg operacji na pewnym zasobie (zwykle pamięci) który musi być wykonany w trybie wyłącznym przez tylko jeden z potencjalnie wielu procesów.

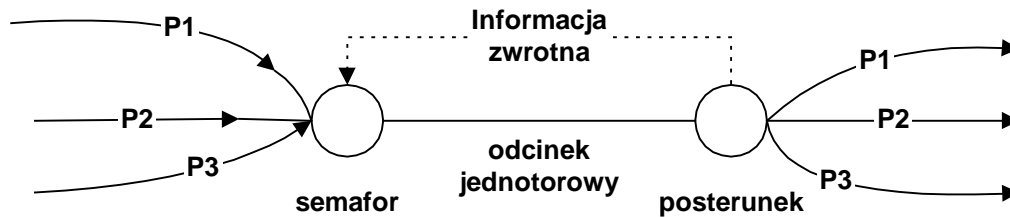
Przy wejściu do sekcji proces wykonuje **protokół wejścia** w którym sprawdza czy może wejść do sekcji krytycznej.

Po wyjściu z sekcji wykonuje **protokół wyjścia** aby poinformować inne procesy że opuścił już sekcję krytyczną i inny proces może ją zająć.



Model programowania z sekcją lokalną i sekcją krytyczną

W danej chwili w sekcji krytycznej może przebywać tylko jeden proces.



Na odcinku jednotorowym może przebywać tylko jeden pociąg

Rozwiązanie problemu wzajemnego wykluczania musi spełniać następujące warunki:

1. W sekcji krytycznej może być tylko jeden proces to znaczy instrukcje z sekcji krytycznej nie mogą być przeplatane.
2. Nie można czynić żadnych założeń co do względnych szybkości wykonywania procesów.
3. Proces może się zatrzymać w sekcji lokalnej nie może natomiast w sekcji krytycznej. Zatrzymanie procesu w sekcji lokalnej nie może blokować innym procesom wejścia do sekcji krytycznej.
4. Każdy z procesów musi w końcu wejść do sekcji krytycznej.

9.3 Niesystemowe metody wzajemnego wykluczania.

9.3.1 Blokowanie przerw

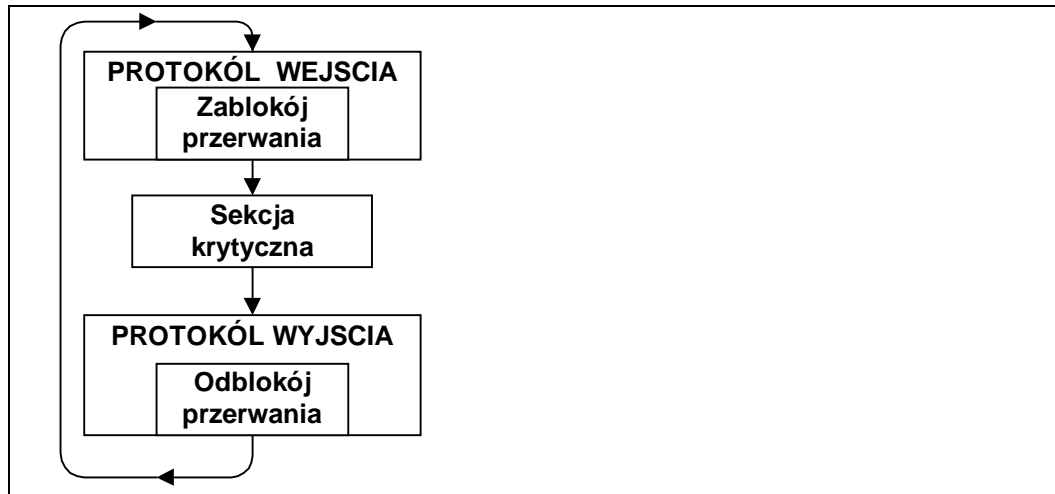
Metoda zapewnienia wzajemnego wykluczania poprzez blokowanie przerw opiera się na fakcie że proces może być przełączony przez:

1. Przerwanie które aktywuje procedurę szeregującą
2. Wywołanie wprost procedury szeregującej lub innego wywołania systemowego powodującego przełączenie procesów.

Gdy żaden z powyższych czynników nie zachodzi procesy nie mogą być przełączane.

Metoda ochrony sekcji krytycznej poprzez blokowanie przerwania opiera się na następujących zasadach:

1. Protokół wejścia do sekcji – następuje zablokowanie przerwania.
2. Protokół wyjścia z sekcji – następuje odblokowanie przerwania.
3. Wewnątrz sekcji krytycznej nie wolno używać wywołań systemowych mogących spowodować przełączenie procesów.



Ochrona sekcji krytycznej przez blokowanie przerwania

Wady metody:

1. Przełączanie wszystkich procesów jest zablokowane.
2. System nie reaguje na zdarzenia zewnętrzne co może spowodować utratę danych.
3. Skuteczne w maszynach jednoprocessorowych

Zastosowanie metody:

Wewnątrz systemu operacyjnego do ochrony wewnętrznych sekcji krytycznych.

9.3.2 Metoda zmiennej blokującej (nieprawidłowa)

Operacje atomowe:

W większości procesorów operacje zapisu i odczytu bajtu, krótkiego słowa (2 bajty), słowa (4 bajty) są operacjami atomowymi.

W procesorach Intel 486 następujące operacje odczytu i zapisu są operacjami atomowymi:

- Bajt
- Krótkie słowo (2 bajty) gdy jest wyrównane do granicy 16 bitów
- Słowo (4 bajty) gdy jest wyrównane do granicy 32 bitów

W procesorach Pentium dodatkowo

- Podwójne słowo (8 bajty) gdy jest wyrównane do granicy 64 bitów

Metoda polega na użyciu zmiennej o nazwie lock.

Gdy zmienna lock = 0 sekcja jest wolna, gdy lock = 1 sekcja jest zajęta.

Proces przy wejściu testuje wartość tej zmiennej. Gdy wynosi ona 1 to czeka, gdy zmieni się na 0 wchodzi do sekcji ustawiając wartość zmiennej lock na 1.

```
int lock = 0;

do {
    sekcja_lokalna;
    // Protokół wejścia
    while(lock != 0) (* czekanie aktywne *);
    lock = 1;
    sekcja_krytyczna;
    lock = 0; // Protokół wyjścia
} while(1);
```

Kompilator może przetłumaczyć powyższy kod w następujący sposób:

```
CHECK:  MOV AL, lock
        TEST AL,AL
        JNZ CHECK ←
        MOV lock, 1
            sekcja_krytyczna
        MOV lock, 0
```


Proces 1	Proces 2	lock
MOV AL, lock		0
TEST AL,AL		
Przełączenie kontekstu z P1 na P2		
	MOV AL, lock	0
	TEST AL,AL	0
	JNZ CHECK	
Przełączenie kontekstu z P2 na P1		
JNZ CHECK		0
MOV lock, 1		1
Przełączenie kontekstu z P1 na P2		
P1 w sekcji krytycznej	MOV lock, 1	1
	P2 w sekcji krytycznej	1

Metoda jest niepoprawna, gdyż operacja testowania wartości zmiennej lock i ustawiania jej na 1 może być przerwana (nie jest niepodzielna).

Dodatkową wadą metody jest angażowanie procesora w procedurze aktywnego czekania.

9.4 Wykorzystania wsparcia sprzętowego do ochrony sekcji krytycznej

Uwaga:

Do zapewnienia wzajemnego wykluczania należy dysponować atomową operacją: **czytaj – modyfikuj – zapisz**

Wiele mikroprocesorów zawiera instrukcje wspierające sprzętowo wzajemne wykluczanie. Są to instrukcje typu

1. **TAS** - sprawdź i przypisz - (*ang. TAS -Test And Set*)
2. **CAS** - porównaj i zamień – (*ang. Compare And Swap*)

Pozwalają one wykonać kilka operacji w sposób nieprzerywalny.

9.5 Sprzętowe wspomaganie wzajemnego wykluczania w procesorach IA-32

W mikroprocesorach IA32 sprzętową ochronę sekcji krytycznej wspomagają instrukcje XCHG (zamień) i CMPXCHG (porównaj i zamień).

Instrukcja Zamień

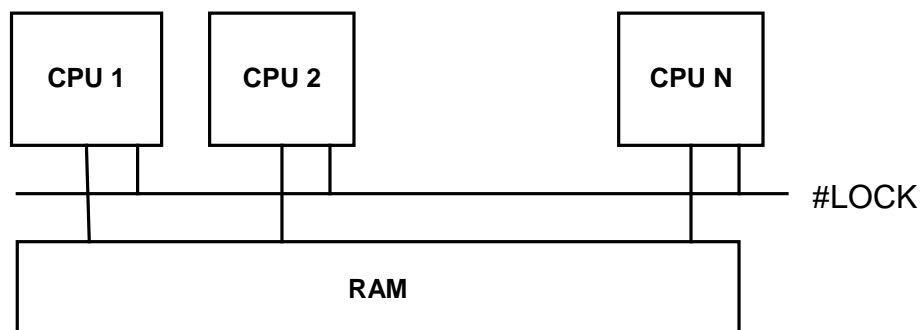
XCHG mem, reg

Działanie:

1. Instrukcja powoduje niepodzielną wymianę zawartości komórki **mem** i rejestru **reg**.
2. Na czas wykonania instrukcji dostęp do pamięci operacyjnej jest blokowany, dla kontrolera pamięci wystawiany jest sygnał LOCK. Uniemożliwia to dostęp do pamięci innym procesorom (gdy system jest wieloprocessorowy).

Blokowanie magistrali:

Procesory Pentium mogą być używane w systemach wieloprocesorowych. Stąd potrzeba blokowania dostępu do pamięci na czas wykonania krytycznych operacji. Architektura IA-32 przewiduje do tego celu sygnał LOCK#.



Rys. 9-1 Sprzętowy sygnał #LOCK blokuje dostęp do pamięci dzielonej.

Gdy sygnał LOCK# jest aktywny dostęp do pamięci przez inne procesory lub moduły aktywne jest zablokowany.

W asemblerze dla procesorów Intel używany jest przedrostek LOCK. Powoduje on zablokowanie dostępu do magistrali na czas wykonania bieżącej instrukcji.

Dla pewnych instrukcji sygnał LOCK# jest aktywowany automatycznie:

- Instrukcja XCHG gdy jeden z operandów odnosi się do pamięci.
- Przy przełączaniu zadań (bit Busy w deskrytorze TSS)
- Przy aktualizacji deskrytorów segmentów.
- Przy aktualizacji katalogu stron i tablicy stron.
- Podczas przerwania, gdy kontroler przerwania przesyła do procesora numer przerwania.

9.6 Wirujące blokady (ang. *Spinlock*)

W oparciu o instrukcję XCHG i zmienną lock można zaimplementować procedurę ochrony sekcji krytycznej - tak zwaną wirującą blokadę.

lock:	dd 0	# 1 - sekcja zajęta # 0 - sekcja wolna
spin_lock:	# Zajmij blokadę	# Zajmij blokadę
CHECK:	MOV EAX,1	# ustaw rejestr EAX na 1
	XCHG EAX ,[lock]	# wymien niepodzielnie # EAX i zmienna lock
	TEST EAX, EAX	# testuj zawartość EAX
	JNZ CHECK	# ustaw to flagę ZF # skocz do CHECK gdy # sekcja była zajęta
	RET	# zakończ procedurę
spin_unlock:	# Zwolnij blokadę	# zwolnij blokadę
	MOV EAX,0	# ustaw rejestr EAX na 0
	XCHG EAX ,[lock]	# wymien niepodzielnie # EAX i zmienna lock
	RET	# zakończ procedurę

Przykład 9-1 Wykorzystanie instrukcji XCHG do implementacji procedur ochrony sekcji krytycznej

Wadą metod jest użycie aktywnego czekania co powoduje niepotrzebną stratę mocy procesora.

Własności:

W systemach jednoprocessorowych i tak musi dojść do przełączenia wątku, bo kto miałby zmienić wartość testowanej zmiennej? Tak więc, nie opłaca się stosować wirujących blokad w systemie jednoprocessorowym.

Są one stosowane gdy:

- W systemach wieloprocessorowych SMP. Czas oczekiwania jest mniejszy niż czas przełączenia wątku i nie opłaca się wyłączać wątku.
- W systemach wieloprocessorowych SMP – blokada przerwań tu nie wystarczy.
- Gdy nie ma innych metod – np. brak systemu operacyjnego.

Wady:

- Zajmują czas procesora – czekanie aktywne
- Brak mechanizmów zapewniających uczciwość (może wystąpić zagłodzenie)
- Brak mechanizmów zapewniających bezpieczeństwo (można czekać w nieskończoność)

9.7 Wirujące blokady w standardzie POSIX

```
#include <pthread.h>
```

Inicjacja wirującej blokady:

```
int pthread_spin_init( pthread_spinlock_t *
  spinner, int pshared )
```

Gdzie:

spinner	blokada
pshared	Flaga: PTHREAD_PROCESS_SHARED PTHREAD_PROCESS_PRIVATE

Gdzie:

PTHREAD_PROCESS_SHARED blokada może być używana
przez wątki różnych procesów

PTHREAD_PROCESS_PRIVATE blokada może być używana
przez wątki jednego procesu

Funkcja inicjalizuje zasoby potrzebne do działania wirującej blokady i pozostawia ją w stanie otwartym.

Zajęcie blokady:

```
int pthread_spin_lock( pthread_spinlock_t *
  spinner )
```

Funkcja próbuje zająć blokadę. Gdy jest ona wolna to zostaje zajęta. Gdy jest zajęta to wątek jest blokowany do czasu aż blokada nie zostanie zwolniona.

Zwolnienie blokady:

```
int pthread_spin_unlock( pthread_spinlock_t * sp)
```

Funkcja zdejmuję blokadę *sp*. Gdy jakieś wątki oczekują na zdjęcie blokady jeden z nich (nie jest specyfikowane który) będzie odblokowany.

Warunkowe zajęcie blokady:

```
int pthread_spin_trylock(pthread_spinlock_t *sp )
```

Funkcja próbuje zająć blokadę sp. Gdy jest ona wolna to zostaje zajęta. Gdy jest zajęta to funkcja zwraca kod błędu EBUSY i wątek nie jest blokowany.

Funkcja zwraca:

EOK - gdy udało się zająć blokadę
EBUSY - gdy blokada jest zajęta

Skasowanie blokady:

```
pthread_spin_destroy( pthread_spinlock_t * sp)
```

Funkcja kasuje blokadę sp. Gdy jakieś wątki oczekują na zdjęcie blokady, będą one odblokowane.

9.8 Systemowe metody zapewnienia wzajemnego wykluczania

Niesystemowe metody stosowane są rzadko i ich znaczenie jest raczej teoretyczne.

Powody:

1. Prawie zawsze tworzymy aplikacje działające w środowisku systemu operacyjnego który z reguły dostarcza mechanizmów zapewnienia wzajemnego wykluczania.
2. Realizacja metod wzajemnego wykluczania polega na zawieszeniu pewnych procesów a wznowieniu innych. System operacyjny w naturalny sposób zapewnia takie mechanizmy. Proces zawieszony nie wykonuje czekania aktywnego a zatem nie zużywa czasu procesora.
3. Metody systemowe są znacznie prostsze i powiązane z innymi mechanizmami i zabezpieczeniami. Przykładowo awaryjne zakończenie się procesu w sekcji krytycznej odblokowuje tę sekcję. Można też narzucić maksymalny limit czasowy oczekiwania na wejście do sekcji krytycznej (*ang. Timeout*).

Systemowe metody zapewnienia wzajemnego wykluczania – przykłady:

- Semaforey POSIX,
- Muteksy POSIX,
- Monitory

Z niesystemowych metod wzajemnego wykluczania praktycznie stosowane są metody:

1. Wirujące blokady (*ang. Spin Locks*) wykorzystujące sprzętowe wsparcie w postaci instrukcji sprawdź i przypisz oraz zamień. Stosuje się je do synchronizacji wątków ze względu na mały narzut operacji systemowych.
2. Blokowanie przerwań – do ochrony wewnętrznych sekcji krytycznych systemu operacyjnego.