Concurrent Systems

Nebenläufige Systeme

VII. Semaphore

Wolfgang Schröder-Preikschat

November 25, 2015

Outline

Preface

Fundamentals
  Classification
  Characteristics

Implementation
  Data Structures
  Functions
  Mutex

Summary

Subject Matter

- discussion on abstract concepts as to unilateral and multilateral synchronisation, thus, partial and mutual exclusion
  - with the general semaphore as a measure that supports both
  - while the binary semaphore was/is intended to support the latter, only
- comprehensive differentiation of semaphore and mutex
  - in terms of the mutual exclusion aspect only, computer science folklore is right in stating disparities between the general variant and a mutex
  - but one have to be much more precise and argue with caution as far as the binary alternative is concerned:

  Hint (Methods v. Implementation/Object)

  A binary semaphore is a valid implementation of one of the many “mutex methods”, but not that restrictive as a “mutex object” need to be.

- elaboration of various implementation aspects regarding both types of semaphore as well as mutex as an object
Concept for Cooperation and Communication

Definition (Binary Semaphore)

The semaphores are essentially non-negative integers; when only used to solve the mutual exclusion problem, the range of their values will even be restricted to “0” and “1”. [2, p. 28]

- Jumping-off point for sleeping lock (Ger. Schlafsperrre, [8, p. 9]) and, in particular, mutex (abbr. mutual exclusion)

Definition (General Semaphore)

It is the merit of [...] C. S. Scholten to have demonstrated a considerable field of applicability for semaphores that can also take on larger values. [2, p. 28]

- Also referred to as counting semaphore (Ger. zählender Semaphore)

Elementary Operations

Insensitive to the distinction between binary and general semaphore is the definition of two intrinsic primitives [1]:

- **P** abbr. for (Hol.) prolaag; a.k.a. down, wait, or acquire, resp.
  - decreases\(^1\) the value of the semaphore by 1:
    - i) iff the resulting value would be non-negative [2, p. 29]
    - ii) non-constraining [3, p. 345]
  - blocks the process iff the value is or was, resp., 0 before decrease
    - blocking processes are put on a waitlist associated with each semaphore

- **V** abbr. for (Hol.) verhoog; a.k.a. up, signal, or release, resp.
  - increases\(^1\) the value of the semaphore by 1
  - as the case may be, unblocks a process blocked on the semaphore
    - which process becomes unblocked is to be regarded as unspecified

Each primitive needs to be considered as an indivisible operation

Hint (Waitlist)

The queuing discipline rivals with planning decisions of the process scheduler and, thus, may be the cause of critical interference.

\(^1\)This does not only mean subtraction or addition, resp., in arithmetical terms.
multilateral synchronisation [5, p. 15] of interacting processes

- the critical section is considered as a non-preemptable reusable resource that needs to be allocated indivisibly to a process to be usable correctly
- in logical respect, the process having completed P on semaphore S is the only one being authorised to complete V on S

```c
semaphore_t mutex = {1};
{
    P(&mutex);
    /* critical section */
    V(&mutex);
}
```

- default value is, normally, 1
- block out only in the moment of a simultaneous process
- allow full bent, else
- in case of a default value of 0
- V must come before P

```
hint (Mutex (cf. p. 14/15))
```

A mutex is a binary semaphore that incorporates an explicit check for authorisation to release a critical section in the moment of V.

unilateral synchronisation [5, p. 15] of interacting processes

- used for availability control of entities of the following resource types:
  
  i. a consumable resource in the form of any data of any number
  ii. a reusable resource of limited number, e.g., a data store (buffer), any device

- typical for, but not limited to, producer/consumer systems

- also as noted previously [5, p. 15], this art of synchronisation means:
  
  logical
  
  - coordination as indicated by a particular “role playing”
  - e.g., in order to proceed, a “data consumer” depends on the data to be made available by a “data producer”

  conditional
  
  - coordination as indicated by a condition for making progress
  - e.g., in order to proceed, a “data producer” depends on the store available for data handling

- in the end, the data store will have to be deallocated and, thus, made available again by the “data consumer”

- from this it follows that P and V applied to the same semaphore S must have to be accomplishable by different processes, normally
- which makes the big difference to a binary semaphore or mutex, resp.

Consumable Resource

availability control

```c
semaphore_t data = {0};
void producer() {
    for (;;) {
        /* data released */
        V(&data);
    }
}
void consumer() {
    for (;;) {
        P(&data);
        /* data acquired */
    }
}
```

- usually, producer and consumer are different interacting processes
- in case of one and the same process, the number of a completed V must exceed the number of a completed P in order to prevent deadlock
- \#V > \#P, which implies a path V \rightarrow P (i.e., V “happens before” P)

Reusable Resource

availability control

```c
semaphore_t store = {N};
void producer() {
    for (;;) {
        P(&store);
        /* store acquired */
    }
}
void consumer() {
    for (;;) {
        P(&store);
        /* store released */
    }
}
```

- default value is N \geq 0
- P must block out only if there is no store
- V indicates more store

- calling sequence
- V must be actable independent of P
- in order to complete, P depends on V

- as to interacting processes in the line of producer and consumer, the same applies as mentioned before: \#V > \#P

- in other cases: \#V \leq \#P, must be completed by the same process
Semaphore v. Mutex I

**Hint**

Checking *authorisation* for release of a critical section in that very moment is improper for a general semaphore, optional for a binary semaphore, and may be demanded for a mutex (cf. p. 15).

- a *mutex object* ensures that the release of critical section CS will succeed only for the process having acquired CS
- by extending a binary semaphore, P will have to record and V will have to check ownership of CS
- improper
  - P and V on a *general semaphore* must be accomplishable in particular also by different processes
  - this is prevented by a mutex object—but not by a mutex
- optional
  - basically, a *binary semaphore* may be implemented by a general semaphore S, with \( S \leq 1 \) \( \Rightarrow \) never a mutex object
  - values \( S > 1 \) must be prevented either by the use pattern or by the implementation of \( P \) and \( V \)
- if *authorisation fails*, the process attempting to release CS should be aborted—in kernel mode, the computing system must be halted...

Semaphore v. Mutex II

**Hint (Computer Science Folklore)**

A semaphore can be released by any process.

- incomplete or rough, if not broad-bush, phrase that must be regarded with suspicion—one have to distinguish between semaphore types
  - strictly, essence of this phrase is requirement for a general semaphore
  - strictly as well, it is merely an option for a binary semaphore
    - in logical respect, a binary semaphore cannot be released by any process
    - in physical respect, this however is not a must for any implementation

**Hint (Computer Science Folklore)**

A mutex can be released only by the process having it acquired.

- a phrase that is slanted towards only one aspect as to the leastwise twofold non-uniform common understanding about a mutex:
  - a category of *methods* for ensuring mutual exclusion or
  - the *implementation* of one of these methods in terms of an object

---

Availability Control in Practice

**Hint (Bounded Buffer)**

A means of managing an unlimited number of consumable resources on the basis of a limited number of reusable resources.

```c
semaphore_t data = {0}, store = {N}; /* N > 0 */
void producer() {
  for (;;) {
    P(&store);
    /* store acquired */
    P(&data);
    /* data acquired */
    V(&data);
    /* data released */
    V(&store);
    /* store released */
  }
}
void consumer() {
  for (;;) {
    V(&data);
    /* data acquired */
    P(&store);
    /* store acquired */
    V(&data);
    /* data released */
    V(&store);
    /* store released */
  }
}
```

Indisputable classic in cooperation and communication of processes

- simply a merge of the semaphore use pattern discussed as before
- transverse application of \( P \) and \( V \) to a pair of general semaphores

---

Hierarchic Placement

**“Uses” [4] Process Instances**

- the *standby position* of a process within \( P \) is passive, normally
  - “blocks the” or “unblocks a”, resp. (cf. p. 8), process means rescheduling
  - if so, both may also entail context switching—“may” because:
    - \( P \) — if no further process is ready to run, the *idle loop* becomes active
      - in that case, the blocking process likewise may fade to the *idle process*
    - \( V \) — if there is a waiting process, it will be set “ready to run” (cf. [9, p.28])
      - in that case, *priority violation* must be prevented (scheduling discipline!)
      - thus, the current process may defer to a prior-ranking one: context switch
- all this makes \( P \) and \( V \) programs of the operating system machine level
- \( P \) and \( V \) relies on *process management* of the operating system
  - one have to put the current process asleep and get a sleeping process up
  - in functional terms, however, \( P \) and \( V \) need not be system calls
  - in non-functional terms, \( P \) and \( V \) should be close to the *scheduler*
    - by settling \( P \) and \( V \) in the address space of the operating-system kernel or
    - by making scheduler functions available through “strawweight” system calls

---

If at least one of the processes on the waitlist is of higher-priority than the current process but will not become “ready to run” or allocated the processor.
Waitlist Association

- in order to aid ∨, processes blocked by P at a semaphore are entered on a waitlist in either logical or physical means
  - logical
    - to block, a blocked-on mark is stored in the process descriptor
      - constant (P) and variable but bounded above (V) run-time
    - to unblock, a process-table walk looks for that mark
  - physical
    - to block, the process descriptor joins a queue data structure
    - to unblock, a process descriptor is removed from that structure
    - variable but bounded above (P) and constant (V) run-time
    - additional queue attribute of the semaphore data structure

- desirable is to have the waitlist queuing discipline in compliance with the process scheduling discipline: freedom of interference
  - a characteristic by means of which priority violation will be prevented
  - usually, this excludes straightforward queuing disciplines such as FCFS

Hint (Process-Table Walk—Conformance to Scheduling)

Part of the scheduler, lookup function to locate a process descriptor on the basis of the blocked-on mark as search key.

Indivisible Operation I

- in the absence of simultaneous processes, the implementation of a semaphore could be as simple as follows:

```c
void prolaag(s semaphore_t *sema)
{ atomic *sema = { if (!claim(sema)) /* at the moment, unavailable */
    sleep(&sema->wand);
}

void verhoog(s semaphore_t *sema)
{ if (unban(sema)) /* as from now, available */
    rouse(&sema->wand);
}
```

- whereat claim decreases and unban increases the value of the semaphore according to binary or general, resp., characteristic

but, assuming that the presence of simultaneous processes is possible, this implementation shows a race condition ~ lost wakeup

- while going to sleep, i.e. being “sleepy”, the process gets delayed
- but in good faith of a sleeper, the “sleepy” process may be missed

Shallows Implementation

- protection of the P/V pair against simultaneous processes sharing a semaphore follows either the blocking or non-blocking paradigm
  - blocking
    - inhibit FLIH, postpone SLIH, or lock process
    - problem-specific construction of an enter/leave pair coming right up next in this lecture (cf. p. 22ff.)
  - non-blocking
    - fall back on the elementary operations of the ISA level
    - problem-specific construction of P and V coming up as a case study in the context of LEC 10/11

- more detailed analysis of the “atomic” version of P reveals another problem: overtaking of an aroused process
  - upon return from sleep a formerly blocked process may complete P by mistake, joining a process in the critical section to be protected by P
  - note that completion of V also opens the door for any process, not only for a process having been blocked at the semaphore
  - aroused processes will have to retry claiming if a while

- not least, concurrency had to be constricted to no more than what is absolutely necessary: reflect on claim/sleep and unban/rouse

- as a process will have to block inside a critical section, deregulation of protection is indispensable for the period the process is blocked

Deadlock Prevention

Provided that protection of the critical section on the P side is not deregulated, the V side will never complete and, thus, will never cause unblocking of a process:

- the right location for deregulation is sleep
- after the process was marked sleeping

5 abbr. for first- or second-level interrupt handling, resp.
Semaphore Data Type

```c
typedef volatile struct semaphore {
    int gate;        /* value: binary or general */
    wand_t wand;     /* protective shield */
} semaphore_t;
```

- The purpose of “wand” (Ger. "Zauberstab") is to safeguard the semaphore operations in various respects.
  - Protect P and V against simultaneous processes.
  - Give leeway for protection variants (cf. p. 20).
- A wand that takes care of mutual exclusion techniques as presented in the previous lecture could be the following:

```c
typedef volatile struct wand {
    lock_t clue;    /* protects P or V, resp. */
    event_t wait;   /* list of sleeping processes */
} wand_t;
```

- Becoming acquainted with other wands is content of future lectures...

Acquire and Release Semaphore

```c
void prolaag(semaphore_t *sema) {
    enter(&sema->wand);     /* avert overlapped P or V */
    while (!claim(sema))    /* acquire semaphore */
    sleep(&sema->wand);    /* await wakeup signal */
    leave(&sema->wand);    /* allow P or V */
}
```

```c
void verhoog(semaphore_t *sema) {
    enter(&sema->wand);    /* avert overlapped P or V */
    if (unban(sema))        /* release semaphore */
        rouse(&sema->wand);    /* cause wakeup signal */
    else                    /* no sleeping process... */
        leave(&sema->wand);    /* allow P or V */
}
```

- Exercise caution in the analysis of these program statements:
  - 3–4: Takes care of the overtaking-problem as to aroused processes.
  - 10–11: In case of (i) logical waitlist and (ii) strict binary semaphore, the search for sleeping processes happens unconditionally.
  - In that particular case, there is no direct indication of sleepers.

Load/store-based implementation for a binary semaphore:

```c
inline bool claim(semaphore_t *sema) {
    return (sema->gate == 0) ? false : (sema->gate = 1);
}
```

```c
inline bool unban(semaphore_t *sema) {
    return !(sema->gate = 0);
}
```

Enumetor-based implementation for a general semaphore:

```c
inline bool claim(semaphore_t *sema) {
    return (sema->gate-- > 0);
}
```

```c
inline bool unban(semaphore_t *sema) {
    return (sema->gate++ < 0);
}
```

- Note that both variants are sensitive to simultaneous processes.
- Use within a safeguarded program section is assumed.

P and V Safeguarded Mutual Exclusion

```c
void prolaag(semaphore_t *sema) {
    enter(&sema->wand);     /* avert overlapped P or V */
    while (!claim(sema))    /* acquire semaphore */
    sleep(&sema->wand);    /* await wakeup signal */
    leave(&sema->wand);    /* allow P or V */
}
```
inline void sleep(wand_t *wand) {
    catch(&wand->wait); /* disclose process to V */
    leave(wand); /* allow P or V */
    coast(); /* take a break */
    enter(wand); /* apply for return to P */
}

inline void rouse(wand_t *wand) {
    leave(wand); /* allow P or V */
    cause(&wand->wait); /* signal end of break */
}

constrict concurrency to no more than what is absolutely necessary:
- endorse interest of the current process of upcoming dormancy
- transition to dormant state: rescheduling, context switch or idleness
- apply for return to safeguarded P
- dormant processes could be available, deregulate V safeguard
- annulment of dormant state: rescheduling, context switch

Semaphore Gatekeeper
- as there is no single solution to protect P and V adequately, the wand attribute symbolises intention to application orientation
- depending on the mode of operation or use case, the wand acts differently
- assuming that processing elements are not multiplexed [7, p.5], then:

    inline void enter(wand_t *wand) {
        lock(&wand->clue);
    }

    inline void leave(wand_t *wand) {
        unlock(&wand->clue);
    }

- wand capability depends on the “type of exclusion” in relation to the required characteristics of the operating system machine level:
  - scheduler
  - partial
  - processor multiplexing
  - mutual
  - processor multiplication

- combination of both is optional, not mandatory, and problem-specific
- depends on the degree of parallelism (a) allowed for by the application use case and (b) made possible by the ISA level
Extents of Critical Section

Binary Semaphore devoid of Waitlist

let the sequence of instructions within $P$ be as follows:

1. point at semaphore
2. address is blocked-on mark
3. apply for $P$ protection
4. unoccupied, take $S_B$
5. occupied, $S_B$ already taken
6. point at process structure
7. define blocked-on mark
8. deregulate $P$ protection
9. fall asleep, dream about $V$

release of a mutex by an unauthorised process is a serious matter

presumably, the non-sequential program contains a software fault (bug)

returning an error code is no option, as one cannot rely on error checking

any other than “raising a non-maskable exception” is a botch job...

Take a sledgehammer to crack a nut...

Given the concept of a binary semaphore, implementation of a mutex is straightforward and, absolutely, no black magic:

- a mutex data structure is composed of two parts:
  - a binary semaphore used to actually protect the critical section and
  - a handle that uniquely identifies the process having acquired the mutex
- given such a structure, let the following two functions be defined:
  - acquire – performs the $P$ and registers the current process as owner
  - release – conditionally unregisters the owner and performs the $V$

a corresponding data type may be laid out as follows:

```
typedef volatile struct mutex {
    semaphore_t sema; /* binary semaphore */
    process_t *link; /* owning process or 0 */
} mutex_t;
```

At kernel level, the handle is the pointer to the process descriptor of the process instance. At user level, it is the process identification.

Outline

Preface
Fundamentals
Classification
Characteristics
Implementation
Data Structures
Functions
Mutex
Summary
Résumé

fundamental concept for cooperation and communication

- binary and general/counting semaphore, intrinsic primitives P and V
- correlation to unilateral and multilateral synchronisation
- differentiation as to mutex (methods v. implementation/object):

Hint

A binary semaphore is a valid implementation of one of the many “mutex methods”, but not that restrictive as a “mutex object” need to be.

- hierarchic placement at operating system machine level
- characteristics important in functional and non-functional terms
  - logical or physical waitlist, conformance to the scheduling discipline
  - deregulation of the protection of P against simultaneous processes
  - further shallows such as overtaking of unblocked processes in P:

Hint

Constrict concurrency to no more than what is absolutely necessary.

- not least, basic approaches and sketches of an implementation...

Reference List I


Reference List II


Semaphore v. Mutex III

Commonalities and differences as to their possible internal states.

- general semaphore $S_g$:
  - positive: $N > 0$ processes will complete $P(S_g)$ without blocking
  - zero: $P(S_g)$ will block the running process on the waitlist of $S_g$
  - negative: $P(S_g)$ will block the running process on the waitlist of $S_g$  $|N|$ processes are blocked on the waitlist of $S_g$

- binary semaphore $S_b$:
  - not taken: exactly one process will complete $P(S_b)$ without blocking
    - the very process becomes logical owner of $S_b$
  - taken: $P(S_b)$ will block the running process on the waitlist of $S_b$
    - $V(S_b)$ should be performed only by the logical owner of $S_b$

- mutex object $M$: let $A$ be acquire and let $R$ be release
  - not owned: exactly one process will complete $A(M)$ without blocking
    - the very process becomes physical owner of $M$
  - owned: $A(M)$ will block the running process on the waitlist of $M$
    - $R(M)$ can succeed only for the physical owner of $M$
Idle State

- principle pattern of a scheduler function to block a process
- called by coast (cf. p. 25) and other functions to pause computation

```c
void block() {
    process_t *next, *self = being(ONESELF);

    while (!(next = elect(hoard(READY))))
        relax(); /* no ready to run... */

    if (next != self) { /* must relinquish */
        self->state = BLOCKED; /* vacate processor */
        seize(next); /* resume elected */
    }

    self->state = RUNNING; /* occupy processor */
}
```

- choose next process to be dispatched to the processor
- ready list is empty, so the running process fades to the idle process
- as the case may be, the running process may be allowed to continue:
  - i. the idle/running process found itself ready-to-run on the ready list or
  - ii. the running process, sent to sleep due to $P$, was roused due to $V$ (p. 25)