

Laboratorul 3

Responsabilități, contracte și invarianți — online

Analiza și Modelarea Sistemelor Software

Traian-Florin Șerbănuță

Ce proiectăm azi

Un depozit are 10 adaptoare de alimentare identice, pe care clienții le pot rezerva și ridica. Operatorul înregistrează cererile. **Rezervat nu înseamnă ridicat:** ce promite registrul când acceptă sau refuză o cerere?

Discutăm în plen pe Teams, apoi urmărim împreună **o analiză AI și o revizuire**, conduse de profesor.

Exemplu didactic. Schițele sunt facultative; nu predăm documente. Nu sunt necesare conturi AI pentru studenți.

Citatul zilei

> **„Precondiția obligă clientul; postcondiția obligă furnizorul.”**
>
> Original: “The precondition binds the client, the postcondition binds the supplier.”

— **Bertrand Meyer**

Sursa: Object-Oriented Software Construction, ediția a doua, „Using assertions”, p. 873

Ce luăm din cursurile 5–6

Responsabilitate: cine decide și cine poate modifica registrul?

Contract: precondiția (ce presupunem despre apel), condiția de succes (când reușim) și postcondițiile (ce întoarcem și ce păstrăm, la succes și la refuz).

Invariant: ce relații trebuie să fie adevărate în orice stare? O stare este **validă** dacă îi respectă pe toți.

Astăzi: **F** = bucăți fizic în depozit; **R** = suma cantităților rezervate activ; **D = F − R** = disponibil. „A activă(4)” înseamnă rezervarea A, activă, pentru 4 bucăți. Inițial avem 10 bucăți, fără reaprovizionare sau retururi; apelurile sunt secvențiale: fiecare începe după încheierea celui anterior.

Cine răspunde de modificarea registrului?

10–30 min · Predicții în chat, apoi explicații în ștafetă

Aceeași cerere vine din formular și din import.

Șase bucăți disponibile, două canale

Starea inițială I: F=10; A activă(4); identificatorul B nefolosit; R=4, D=6. **F** = fizic, **R** = rezervat activ, **D** = disponibil.

R2 (rezervare): rezervăm o cantitate întreagă pozitivă, cel mult egală cu D, cu un identificator nefolosit; R crește, D scade, F rămâne identic. Altfel refuzăm, fără modificări. **R5 (istoric și efect limitat):** formularul și importul folosesc aceleași reguli; celelalte rezervări se păstrează.

1. Individual: din I, scenariul S1 (**rezervă(B,6)**) și, independent, scenariul S2 (**rezervă(B,7)**) — ce rezultat și ce cantități rămân?
2. La semnal, predicțiile în chat. Un coleg propune verificări în fiecare canal; un coleg numit, operații ale unui registru comun, cu semnătura și rezultatele lor. Comparați dependențele.
3. Continuăm ștafeta cu alt coleg: cine împiedică importul să ocolească regula?

Enunțul complet: R1–R5 și scenariile S1–S7

Ce garantează operațiile?

30–55 min · Construim și explicăm contracte

Un refuz păstrează și cantitățile, și rezervările.

Contractul rezervării

Starea inițială I: F=10, A activă(4), identificatorul B nefolosit, R=4, D=6; F fizic, R rezervat activ, D disponibil.

R1 (context): cantitățile sunt numere întregi, identificatorii sunt nevizi, registrul este valid, iar apelurile sunt secvențiale. **R2 (rezervare):** pentru o cantitate q>0, un identificator nefolosit și q≤D, operația creează o rezervare activă nouă de q bucăți; F nu se modifică. Altfel refuză, fără modificări. **R5 (istoric și efect limitat):** celelalte rezervări se păstrează.

Un coleg formulează contractul în plen (precondiții, condiție de succes, postcondiții), iar un coleg numit verifică; apoi schimbați vorbitorii, cu obiecții în chat:

- scenariul S2 (**rezervă(B,7)**) și scenariul S7 (**rezervă(B,0)**), fiecare din I;
- succesul din scenariul S1 (**rezervă(B,6)**) și păstrarea lui A;
- relația **D = F − R** și lipsa cantităților negative: ajung ele singure?

Ridicarea nu mărește cantitatea disponibilă

Starea inițială I: F=10, A activă(4), R=4, D=6. F fizic, R rezervat activ, D disponibil.

R3 (ridicare) și R4 (anulare): numai o rezervare activă de q bucăți poate fi ridicată sau anulată; o marcăm ridicată, respectiv anulată. La ridicare, F și R scad cu q, iar D nu se modifică. La anulare, F rămâne, R scade cu q, iar D crește cu q. **R5 (istoric și efect limitat):** păstrăm identificatorul, cantitatea și celelalte rezervări; la refuz, tot registrul.

Un coleg explică scenariul S3 (**ridică(A)**), un coleg numit scenariul S4 (**anulează(A)**), **independent din I**. Alt coleg continuă ștafeta:

Scenariul S5: din I, **ridică(A)**, apoi **anulează(A)**. Ce rezultat și ce stare produce fiecare pas? De ce nu putem „reda” cele 4 bucăți?

O analiză AI, o revizuire împreună

55–80 min · Demonstrație condusă de profesor, discuție în plen

Prezicem răspunsul, îl verificăm, apoi decidem ce păstrăm.

Analiza: ce îi cerem și ce verificăm?

Instrucțiunea trimisă: „[...] formulează contractele operațiilor rezerva, ridica și anuleaza: precondiții, condiții de succes, efecte, refuzuri și invarianți. Calculează S2, S3 și S5. [...]”

Reguli: rezervarea reușește numai cu un identificator nefolosit și $0<q\leq D$; ridicarea și anularea, numai pentru o rezervare activă; altfel refuz, fără modificări. Ridicarea scade F și R cu q; anularea, doar R.

Din I (F=10, A activă(4), R=4, D=F−R=6): scenariul S2 (**rezervă(B,7)**); scenariul S3 (**ridică(A)**); scenariul S5 (**ridică(A)**, apoi **anulează(A)**). **Predicție în chat, la semnal:** ce rezultate așteptăm?

Analiza: ce îi cerem și ce verificăm?

Instrucțiunea trimisă: „[...] formulează contractele operațiilor rezerva, ridica și anuleaza: precondiții, condiții de succes, efecte, refuzuri și invarianți. Calculează S2, S3 și S5. [...]”

Reguli: rezervarea reușește numai cu un identificator nefolosit și $0<q\leq D$; ridicarea și anularea, numai pentru o rezervare activă; altfel refuz, fără modificări. Ridicarea scade F și R cu q; anularea, doar R.

Din I (F=10, A activă(4), R=4, D=F−R=6): scenariul S2 (**rezervă(B,7)**); scenariul S3 (**ridică(A)**); scenariul S5 (**ridică(A)**, apoi **anulează(A)**). **Predicție în chat, la semnal:** ce rezultate așteptăm?

Analistul AI — Claude Haiku 4.5, captură din 27 octombrie 2026; fragmente din contractul rezervă:

> **Precondiții:** id ≠ 0; id nu apare deja în registru; q > 0; D ≥ q
>
> **Refuz:** Orice precondițiune încălcată ⇒ stare neschimbată

Revizuirea: o observație trebuie justificată

Evaluatorul (agent AI de revizuire) — Claude Haiku 4.5, captură din 27 octombrie 2026; context nou, cu enunțul, sarcina și propunerea integrală; fragmente:

> **3. Efect asupra altor rezervări** Propunerea nu enumeră explicit “alte rezervări rămân neschimbate”. […]
>
> **Concluzie:** Propunerea e substantiv corectă. […] Nu sunt remedieri logice necesare.

Reguli: R5 (istoric și efect limitat) cere ca o operație să nu modifice alte rezervări. Identificatorul nefolosit, $q>0$ și $q \leq D$ decid succesul rezervării; altfel operația refuză, iar întregul registru rămâne identic.

În chat, la semnal, apoi pe rând: observația 3 este susținută de R5? Ce nu a verificat evaluatorul AI la „Precondiții: … $D \geq q$”?

Capturile pregătite: instrucțiunile reale și răspunsurile integrale

Decizia comună asupra propunerii

Păstrăm sau corectăm numai cu justificare:

Întrebare	Reper pentru decizie
Cine modifică registrul?	Aceleași operații pentru formular și import.
Ce decide succesul?	Identificator nefolosit, $q>0$, $q \leq D$: împreună, condiția de succes, cu refuz promis.
Ce înseamnă refuz?	Întregul registru identic, inclusiv istoricul.
Ce păstrăm la succes?	Celelalte rezervări, integral; identificatorul și cantitatea celei vizate.

Un coleg explică o afirmație acceptată; alt coleg o verifică printr-un exemplu. Nu este obligatoriu să găsim o eroare.

Verificăm explicația altor colegi

80–100 min · Explicații și verificări în plen, încheiere

Poate altcineva aplica exact contractul nostru?

Două rezervări, două operații succesive

Starea de pornire (după scenariul S1): F=10; A activă(4), B activă(6); R=10, D=0. F fizic, R rezervat activ, D disponibil.

Reguli: pentru o rezervare activă de q bucăți, anularea scade R cu q, fără modificarea lui F; ridicarea scade F și R cu q; D=F−R. Păstrăm identificatorul, cantitatea și celelalte rezervări; la refuz, întregul registru.

1. Executăm **anulează(A)**, apoi **ridică(B)**. Ce cantități și ce rezervări avem după fiecare pas?
2. Un voluntar explică în plen; un coleg numit verifică primul păstrarea rezervării neatinse de operație. Ceilalți pot formula obiecții în chat.
3. Alt coleg explică o ramură separată, imediat după anularea lui A, ca în scenariul S6 (reutilizarea lui A), dar din această stare: **rezervă(A,2)**. **Identificatorul nu se reutilizează.** Ce se păstrează la refuz?

Ce putem explica acum?

Un exemplu din discuția voastră pentru fiecare întrebare:

- Cine asigură respectarea regulii și ce dependență evită copierea ei?
- Ce promite un refuz, dincolo de mesaj?
- Ce relație dintre cantități este un invariant?
- Ce au confirmat sau au corectat analiza și revizuirea comună?

Repere: ambele canale aplică aceleași reguli prin operațiile registrului; un refuz lasă registrul identic; $D=F-R\geq 0$ este un invariant; fiecare operație păstrează celelalte rezervări.