Modellezés UPPAAL-ban

Kockajáték mintafeladat és megoldása

dr. Bartha Tamás
BME Méréstechnika és Információs Rendszerek Tanszék

Tartalom

- A mintafeladat demonstrál néhány hasznos UPPAAL modellezési fogást:
  - Véletlen érték generálása és felhasználása
  - Atomi műveletek modellezése
  - Szinkron kommunikáció modellezése
    - Globális osztott változó használatával
    - Dedikált csatornatömbök alkalmazásával
  - Adatstruktúrák és függvények használata
  - Változók kezelése (állapottér csökkentése)
  - Temporális kifejezések írása modellellenőrzéshez

A feladat

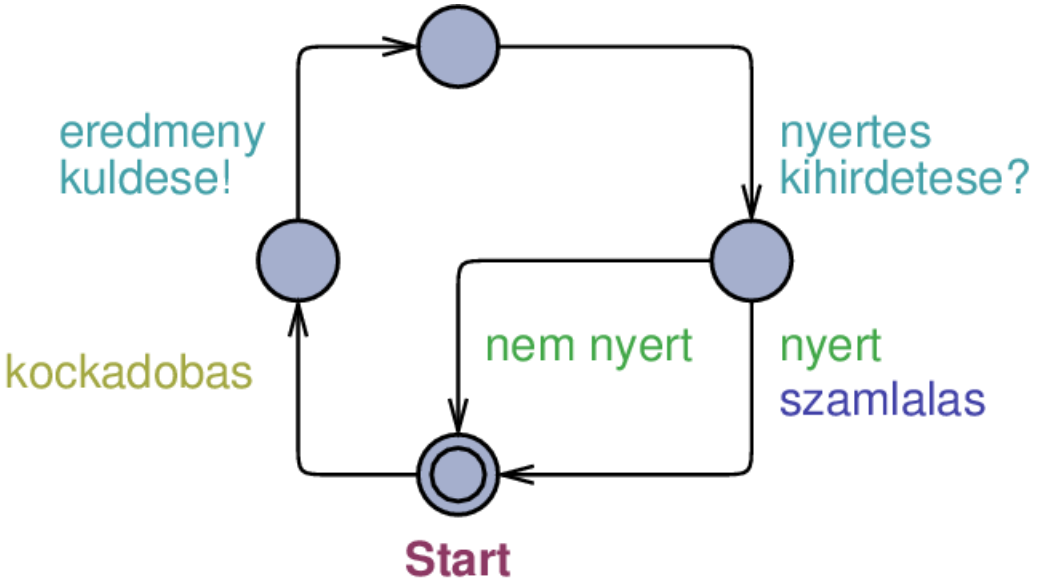
A feladat

- Kockadobálós játék
  - Szereplők: n játékos, 1 bíró
  - Minden játékos egy kockával egyszer dob
  - Közlik az eredményt a bíróval
  - A bíró
    - feljegyzi az eredményeket,
    - megkeresi a legnagyobbat,
    - kihirdeti a nyertest
  - A játékosok számlálják a nyeréseket

Mit kell megoldanunk?

- Véletlen érték generálása
- Kommunikáció
  - Értékek „továbbítása”
  - „Broadcast” kommunikáció
  - Csatornatömbök kezelése
- Adatszerkezetek
- Függvények
- Konkurencia és időzítés
- Modellellenőrzés

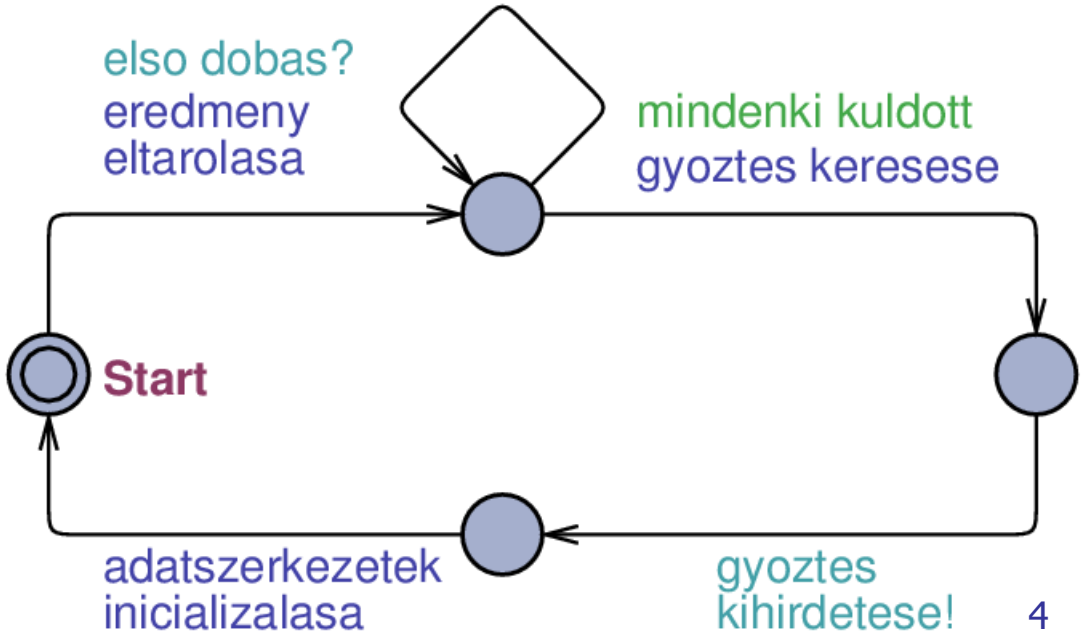
Szereplők és állapotok absztrakt modellje



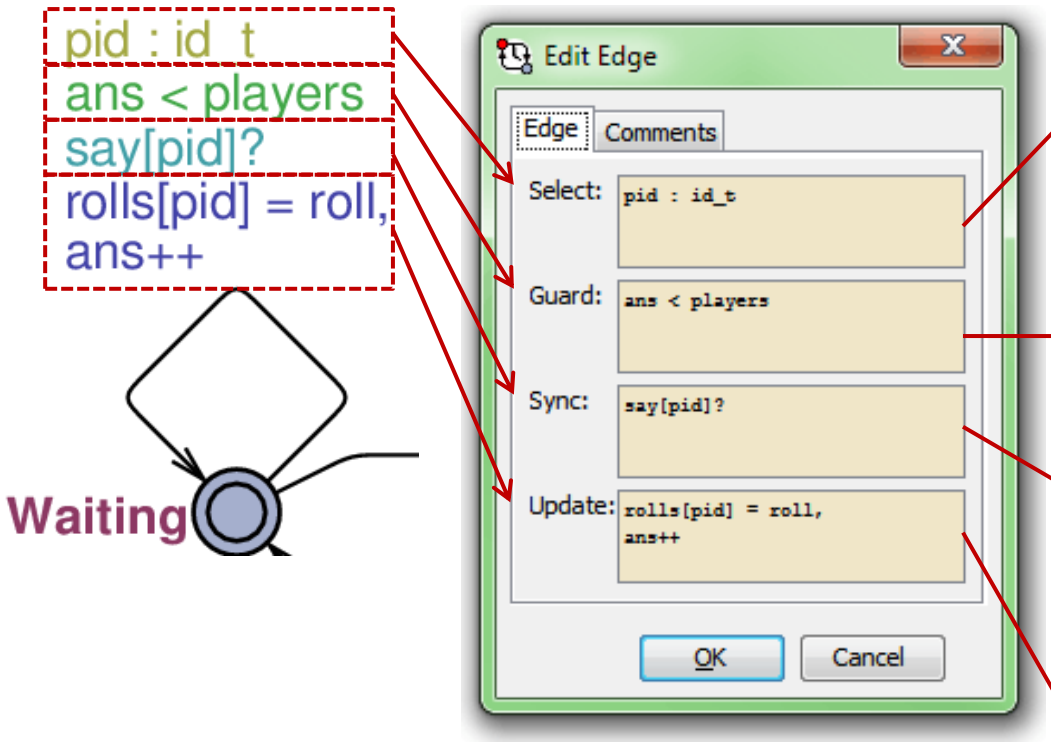
Játékos

Bíró

amig mindenki el nem kuldi:
kovetkezo dobas?
eredmeny eltarolasa



Modellezési kitérő: az élekhez rendelt kifejezések



- Az élek esetén a szekciók kiértékelési sorrendje:
  Select » Sync » Guard » Update

- Selection
  - Nemdeterminisztikus választás egy változó értékkészletéből
- Guard
  - Engedélyező feltétel (logikai kifejezés)
- Synchronization
  - Szinkronizáció adott csatornán megfelelő processz „párok” között
- Update
  - Állapotváltás esetén kiértékelt kifejezés (mellékhatása is lehet)

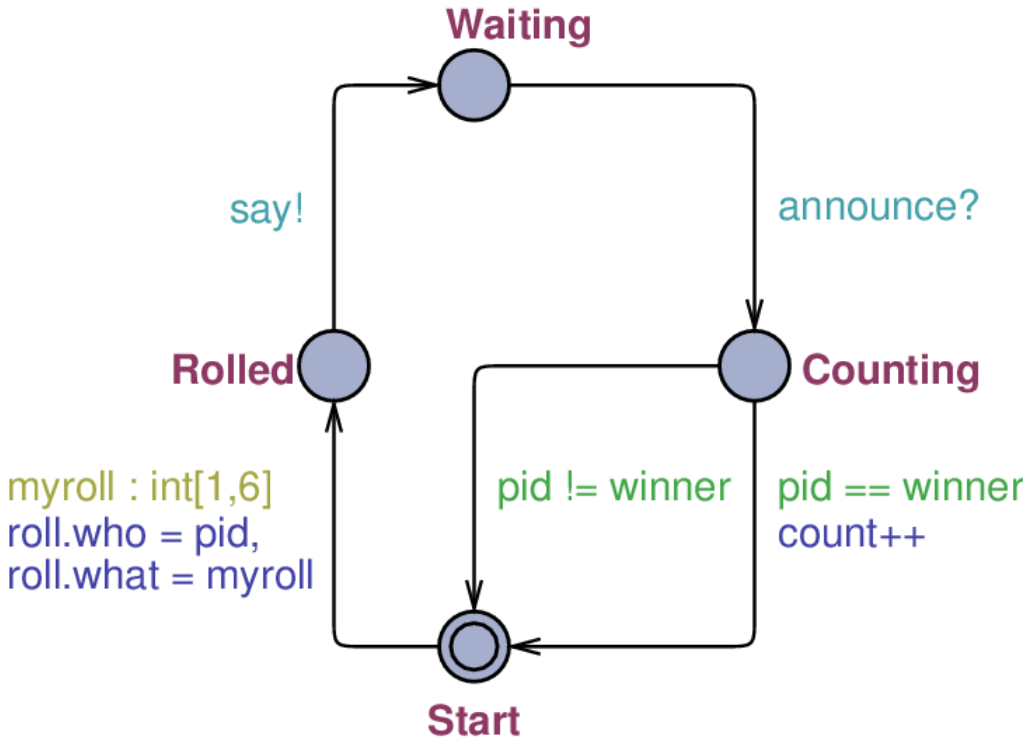
Modellezés: A rendszer és egy játékos

Rendszer:

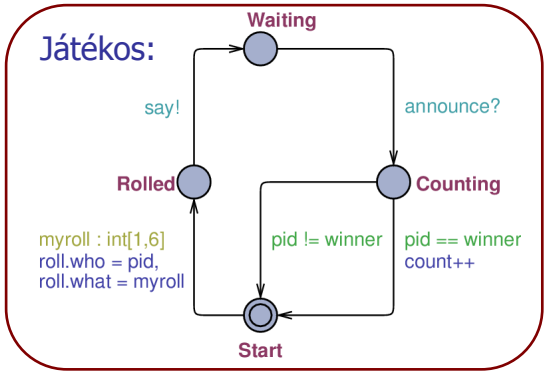
```
system Player, Referee;

const int players = 3;
const int wins = 10;

typedef int[0,players-1] id_t;
typedef int[0,6] dice_t;
struct {
  id_t who;
  dice_t what;
} roll;

id_t winner;
chan say;
broadcast chan announce;
```

Játékos:

```
Player(id_t  pid)

int[0,wins] count = 0;
```



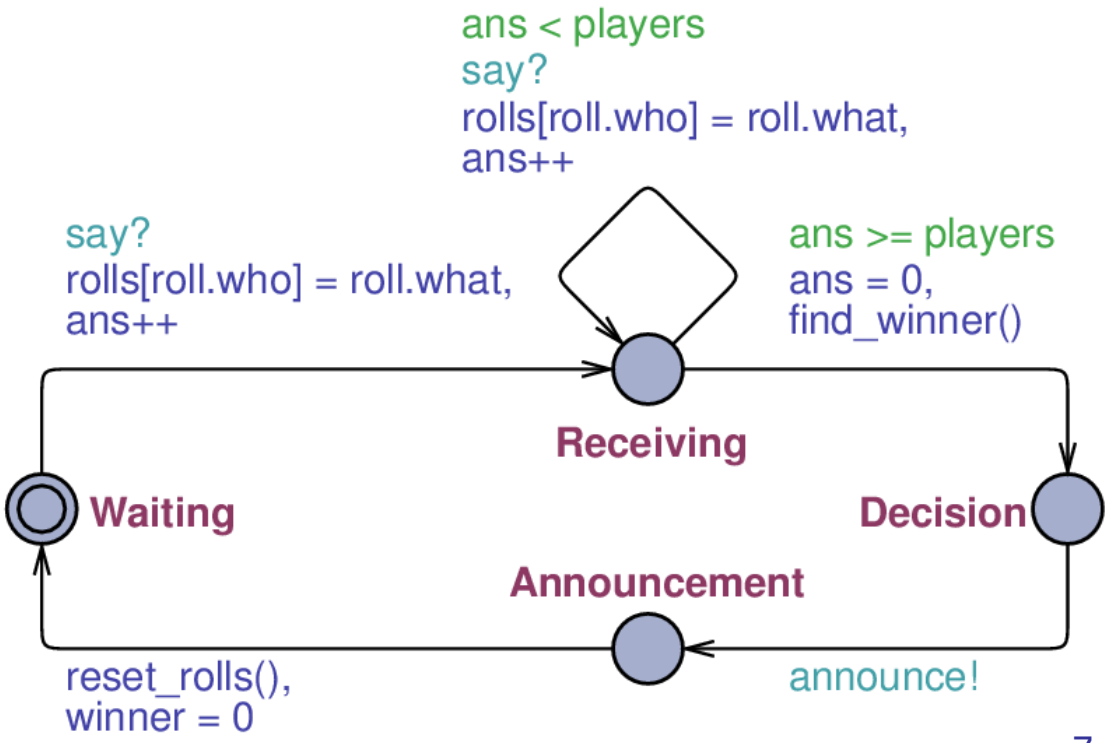
Modellezés: A bíró



Bíró:

```
int [0,players] ans = 0;
dice_t rolls[id_t];
dice_t best = 0;

void find_winner() {
  int[0,players] i;

  for (i = 0; i < players; i++) {
    if (rolls[i] > best) {
      best = rolls[i];
      winner = i;
    }
  }
  best = 0;
}
```

```
void reset_rolls() {
  int[0,players] i;

  for (i = 0; i < players; i++) rolls[i] = 0;
}
```



Ellenőrizzük a működést! (dice_roll_1)

- Mindig van győztes a játékban
  - Mindig van olyan játékos, aki maximális számú alkalommal nyer

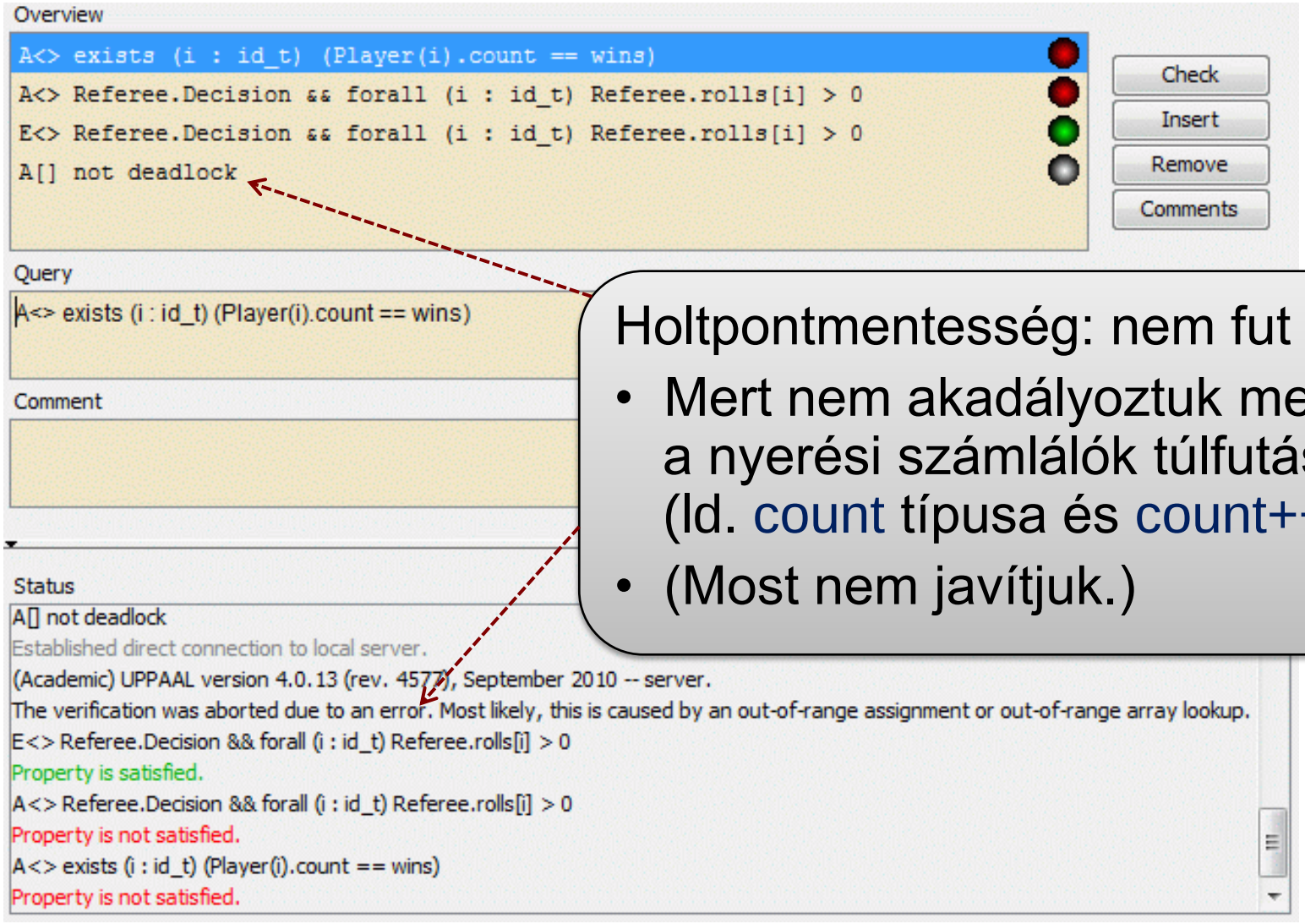
    A<> exists (i : id_t) (Player(i).count == wins)
- A bíró csak akkor hoz döntést, ha minden játékos dobott
  - Ez legalább egyszer megtörténik:

    E<> Referee.Decision && forall (i : id_t) (Referee.rolls[i] > 0)
  - Ez minden lehetséges úton bekövetkezik:

    A<> Referee.Decision && forall (i : id_t) (Referee.rolls[i] > 0)
- A rendszerben nincs holtpont
  - Nincs olyan állapot, amelyből ne vezetne ki olyan engedélyezett állapotátmenet, amellyel egy következő állapotba léphetünk

    A[] not deadlock

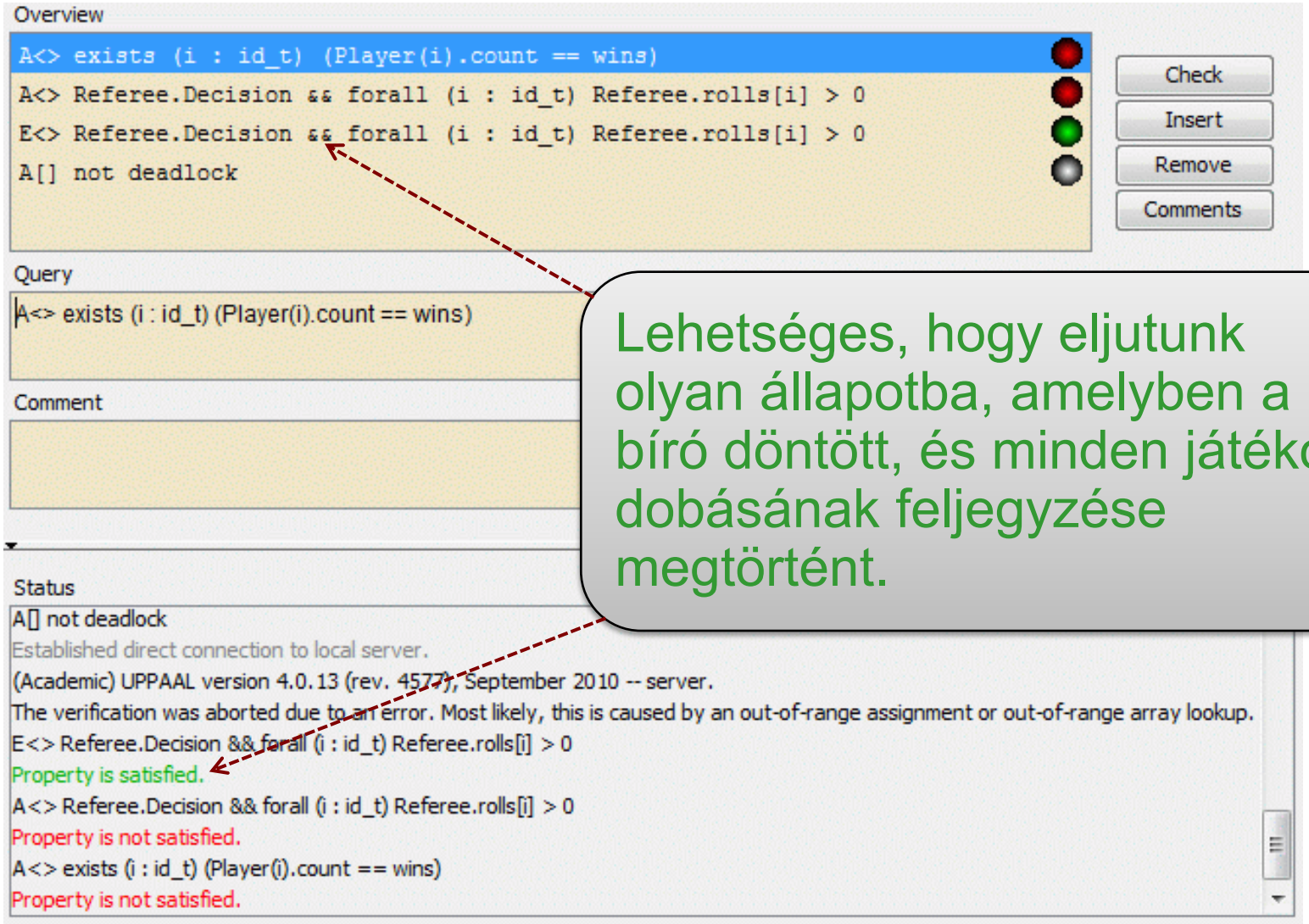
Ellenőrizzük a működést! (dice_roll_1)



Holtpontmentesség: nem fut le.

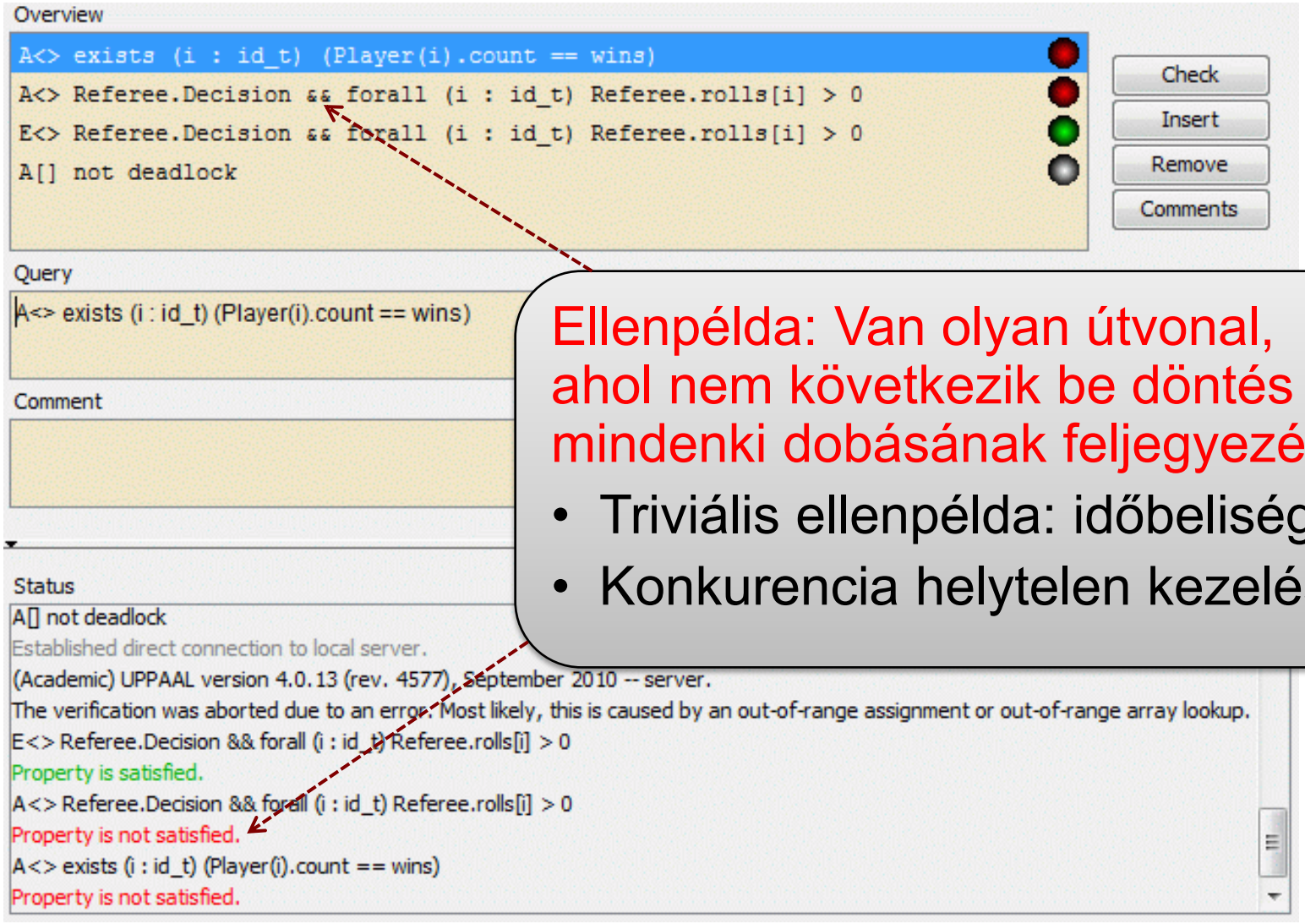
- Mert nem akadályoztuk meg a nyerési számlálók túlfutását (ld. count típusa és count++).
- (Most nem javítjuk.)

Ellenőrizzük a működést! (dice_roll_1)



Lehetséges, hogy eljutunk olyan állapotba, amelyben a bíró döntött, és minden játékos dobásának feljegyzése megtörtént.

Ellenőrizzük a működést! (dice_roll_1)

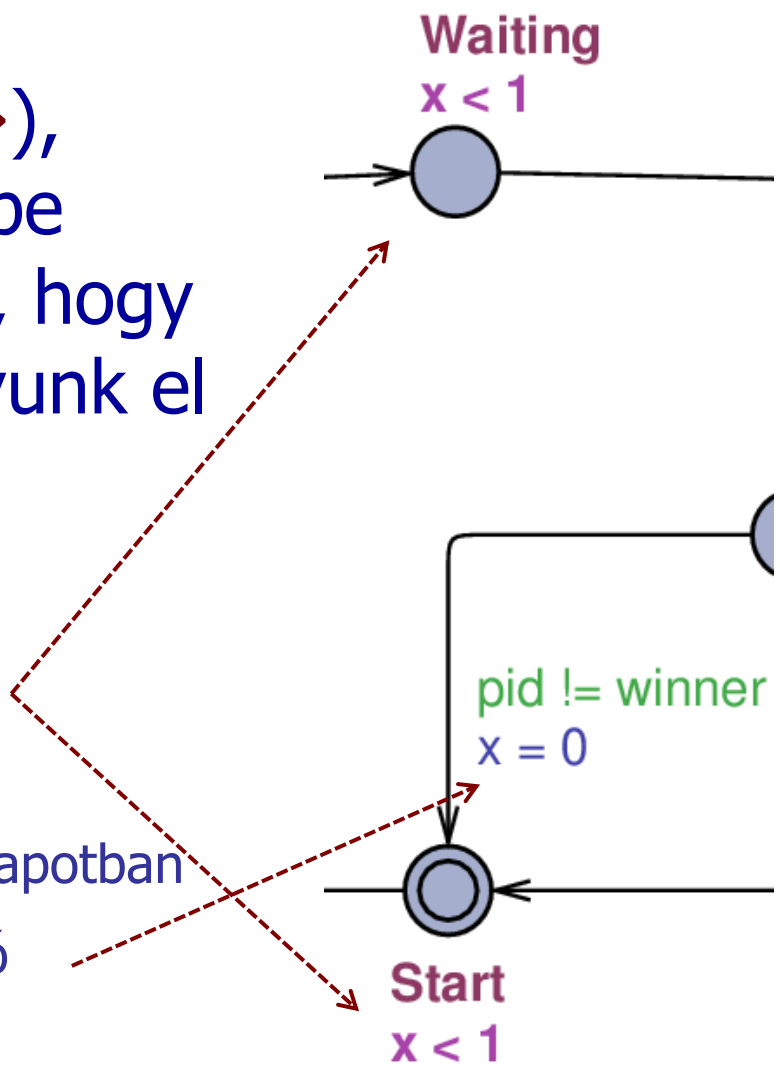


Ellenpélda: Van olyan útvonal, ahol nem következik be döntés és mindenki dobásának feljegyezése

- Triviális ellenpélda: időbeliség
- Konkurencia helytelen kezelése

Triviális ellenpélda kiküszöbölése: időzítés

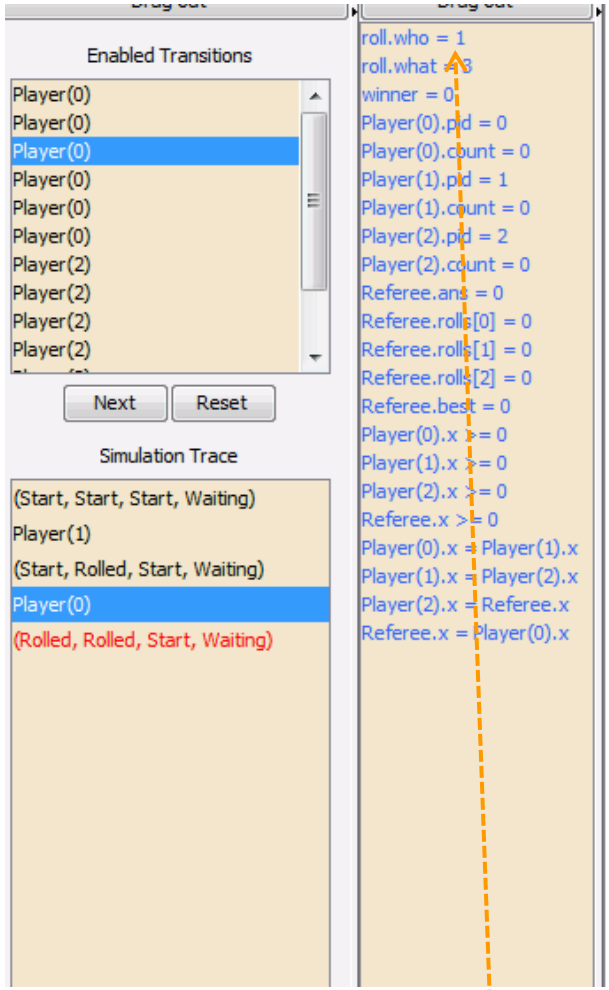
- Ha az összes lehetséges lefutást vizsgáljuk (pl. A<>), akkor az UPPAAL figyelembe veszi azt a lehetőséget is, hogy egy állapotot sosem hagyunk el
- Megoldás:
  - Óraváltozó bevezetése
    - Invariáns előírása
    - Legfeljebb 1 időegységig tartózkodhatunk az adott állapotban
    - Gondoskodunk az óraváltozó inicializálásáról

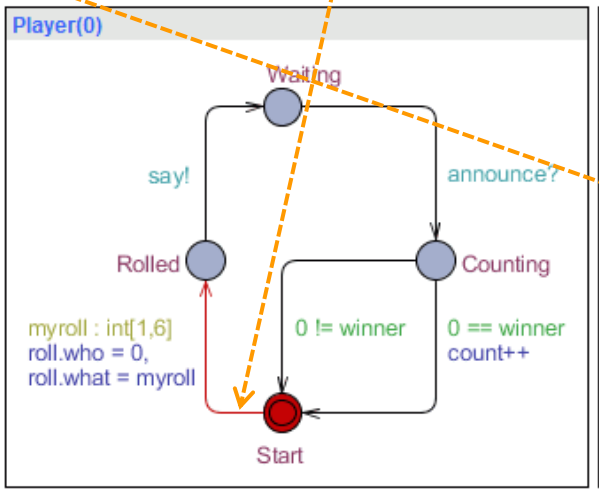


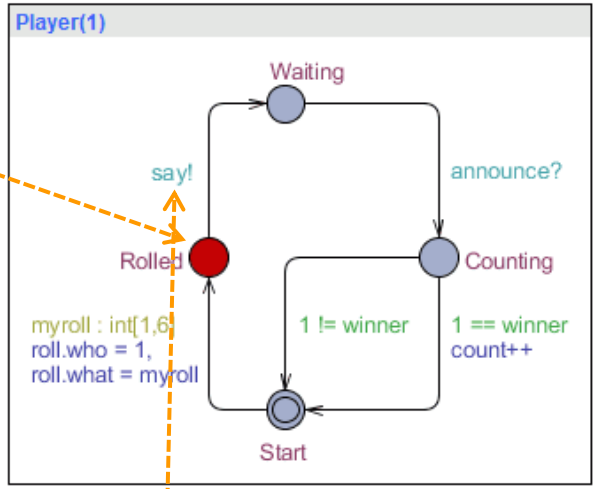
Konkurens működés - mi a baj?

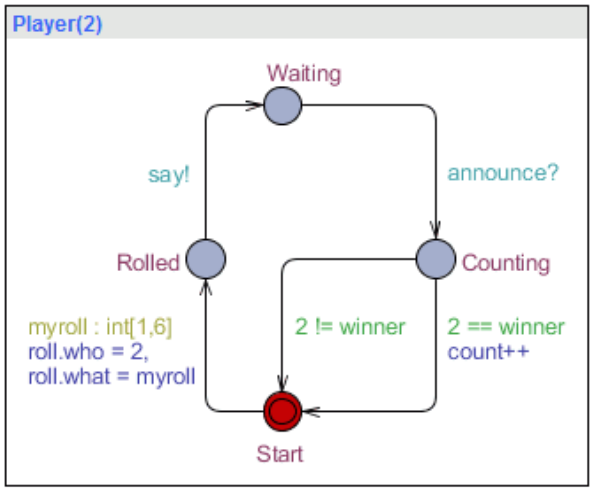
Player(1) kockával dobott

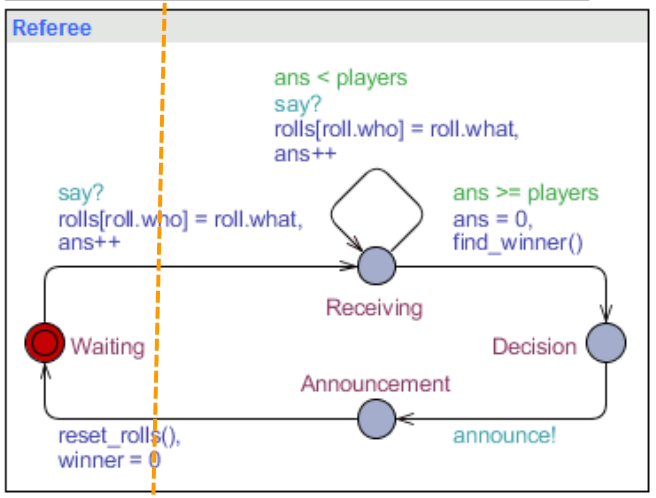
Player(0) kockával dob







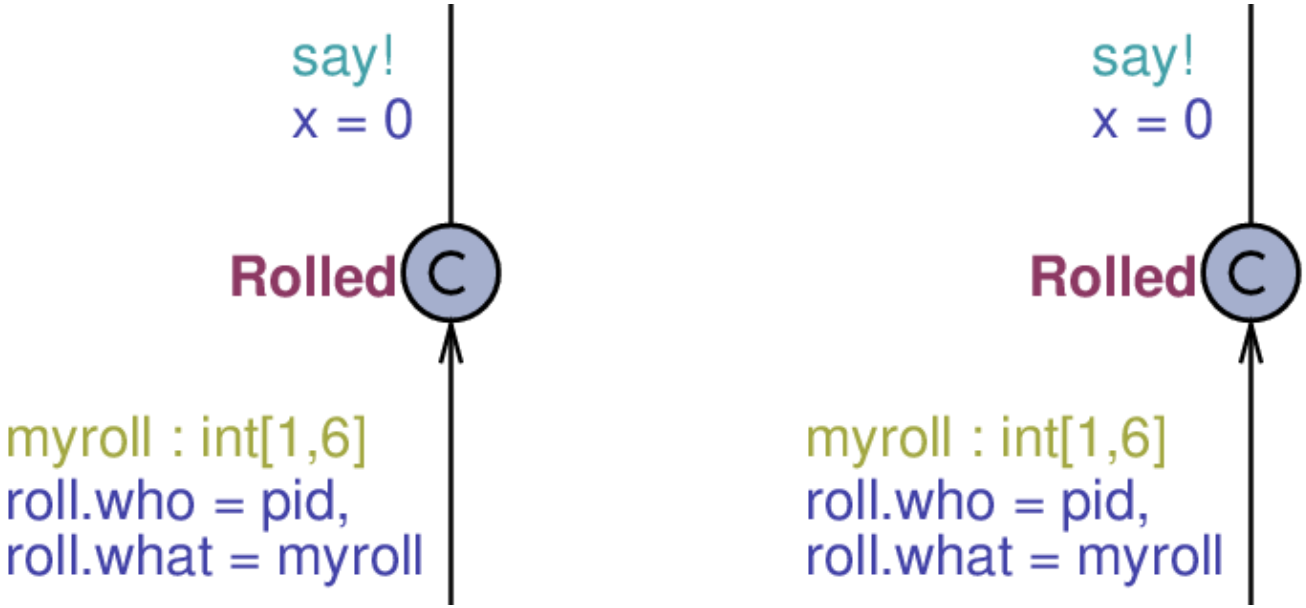




Player(0) felülírja a megosztott változót

Player(1) hibásan „küldi el”

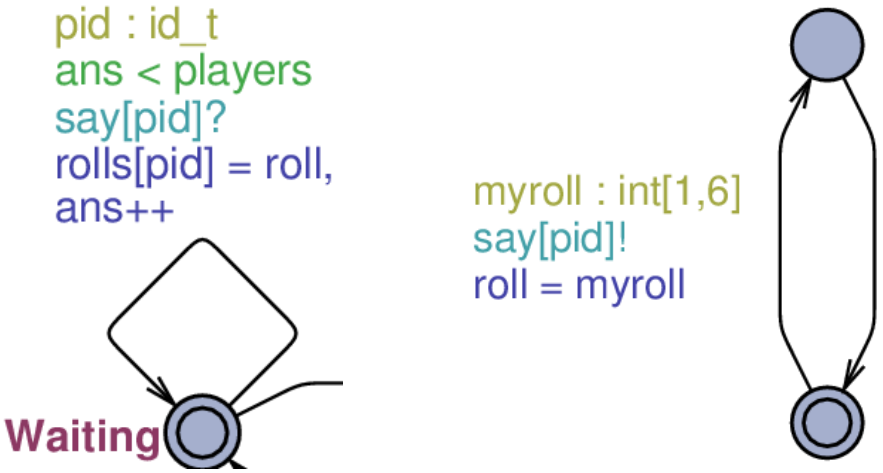
Nem kívánt konkurencia elkerülése (dice_roll_1.1)



- Probléma: Átlapolódhat (konkurens) az egyes játékosokra:
  - A dobás eredményének rögzítése (roll közös változó feltöltése)
  - A bíróval való közlés (say! átmenet)
- Megoldás:
  - Konkurencia megszüntetése: „committed” állapot bevezetése (a „committed” állapotból azonnal tovább kell lépnünk)

Speciális lehetőségek (dice_roll_2)

- Csatornatömbök használata
  - A fogadó folyamat egy Select konstrukcióval „egyszerre” az összes csatornát figyeli
  - A csatorna azonosító felhasználható az Update szekcióban!

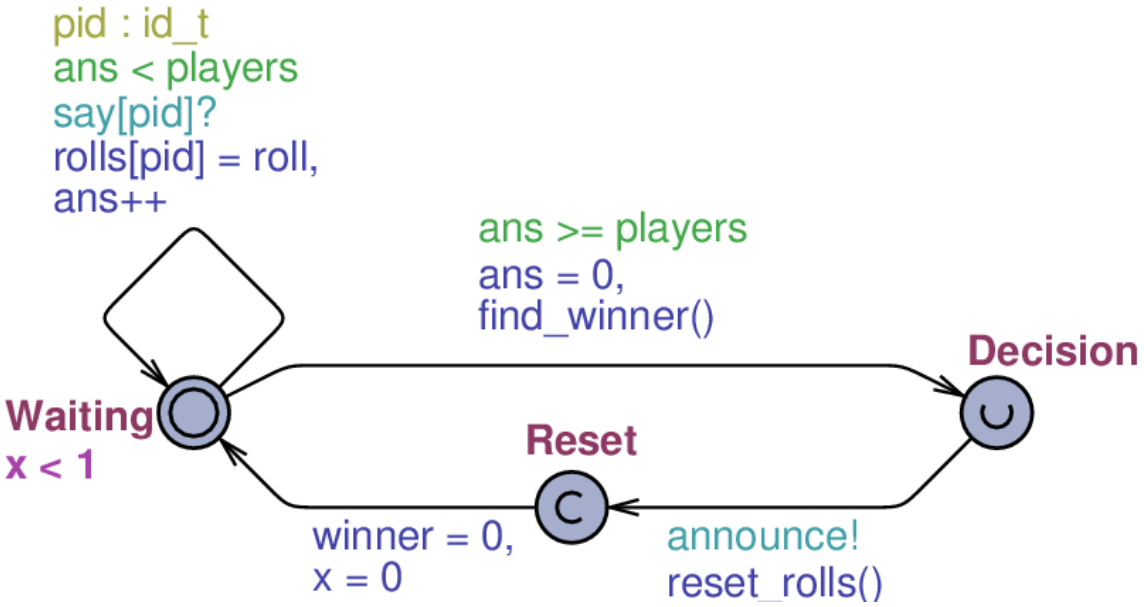


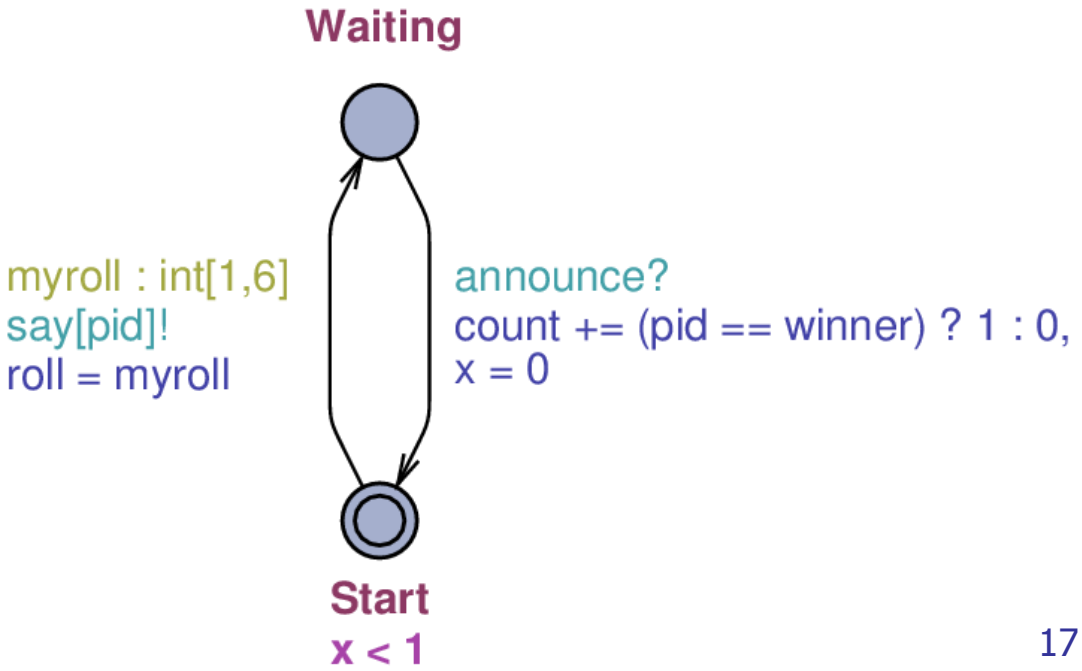
- Iterátorok alkalmazása

```
void reset_rolls() {
  for (i : id_t) rolls[i] = 0;
}

void find_winner() {
  for (i : id_t) {
    if (rolls[i] > best) {
      best = rolls[i];
      winner = i;
    }
  }
  best = 0;
}
```

További egyszerűsítési lehetőségek

- Csatornatömbök használata: válaszok gyűjtése egy állapotban
- „?” operátor alkalmazása
- Reset állapot „committed”





További modellezési tippek, tanácsok

- Az élek esetén a szekciók kiértékelési sorrendje:
  Select » Sync » Guard » Update
  - Szinkronizáló élek esetén a küldő Update-ja a fogadóé előtt fut le
  - Nem tesztelhetünk a fogadóban egy szinkronizáló él által beállított globális változót (a küldőnél előbb kell beállítanunk, pl. előző élen)
  - Nem „védhetünk meg” Guard-dal egy Sync-ben levő változót (pl. csatornatömb esetén)
- A függvények működésének ellenőrzése nehézkes
  - Nincs lehetőség nyomkövetésre (a belső működés szimulációjával)
  - Próbáljunk a fejlesztés során kis lépésekben haladni, és szimulációval, verifikációval gyakran ellenőrizni

További modellezési tippek, tanácsok

- Az A<> q tulajdonság használata esetén ki kell zárnunk a triviális ellenpéldát
  - Óraváltozók használatával
  - „Urgent” állapot beállításával
  - Emlékezzünk a „leads to” p --> q szemantikájára: A[] (p imply A<> q)
- Ne felejtsük el az óraváltozókat megfelelően inicializálni
- A csatorna-, vagy automataszintű prioritások használata
  - Az UPPAAL modellellenőrzője nem támogatja (pl. a holtpontot sem tudja ellenőrizni)
  - Ezek a modellezési elemek lehetőleg kerülendők