Progettazione di un Pianificatore di Treni senza Deadlock: Un Approccio di Controllo del Modello

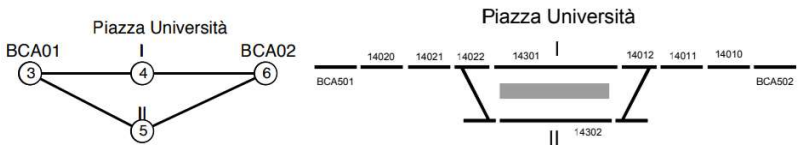
Astratto.
In questo articolo presentiamo l'approccio utilizzato nella progettazione di il kernel di programmazione di un sistema di supervisione automatica dei treni (ATS). È stato realizzato un modello formale del tracciato ferroviario e del servizio previsto utilizzato per individuare tutte le possibili sezioni critiche del tracciato ferroviario in quale potrebbe verificarsi un deadlock. Per ogni sezione critica, la prevenzione di il verificarsi di situazioni di stallo si ottiene vincolando l'insieme dei treni permesso di occupare queste sezioni contemporaneamente. L'identificazione di le sezioni critiche e la verifica della correttezza della logica utilizzato dall'ATS viene effettuato sfruttando una verifica di model checking framework sviluppato localmente presso l'ISTI e basato sullo strumento UMC.

1. Introduzione

La tendenza attuale nella progettazione dei sistemi ferroviari metropolitani è quella di fornire piattaforme completamente automatizzate, dove i treni si muovono in modalità driverless, e sono monitorati da un componente centralizzato, normalmente chiamato Automatic Train Supervision sistem (ATS).
Il ruolo principale di un sistema ATS è quello di coordinare automaticamente l'avanzamento dei treni.
In assenza di ritardi, un ATS garantisce una perfetta aderenza agli orari previsti.
In presenza di ritardi, il sistema ATS deve effettuare le corrette scelte di programmazione dei treni al fine di garantire che ogni treno arrivi comunque a destinazione.
In particolare, ciò significa che l'ATS dovrebbe necessariamente evitare il verificarsi di situazioni di deadlock, cioè situazioni in cui un gruppo di treni si bloccano a vicenda impedendo in tal modo il completamento delle loro missioni.
Il progetto italiano "Train Control Enhancement via Information Technology" (TRACE-IT) è un progetto finanziato dalla Regione Toscana che vede la collaborazione di un partner industriale attivo nel campo del segnalamento ferroviario e partner accademici tra cui l'ISTI Istituto Nazionale Ricerca Consiglio.
Uno degli obiettivi del progetto TRACE-IT è la progettazione, lo sviluppo e la sperimentazione di un sistema di controllo dei treni basato sulle comunicazioni (CBTC) [1] basato sul recente standard europeo ERTMS/ETCS Baseline 3 (BL3).
ISTI è coinvolto nella specifica e nello sviluppo dell'ATS componente del sistema CBTC, e questo compito include lo sviluppo di un prototipo dimostrabile di un sistema ATS per un layout di scalo ferroviario semplice ma non banale e un piano di servizio semplice ma non banale.
Il nostro approccio parte dalla costruzione di un modello formale del tracciato ferroviario e del servizio previsto.
Eseguendo un model checking esaustivo del sistema, identifichiamo tutte le possibili sezioni critiche del tracciato ferroviario in quale il dato insieme di treni in corsa potrebbe portare alla generazione di situazioni di stallo.
Per ogni tratta critica, la prevenzione degli stalli è realizzata in modo semplice ma efficace, vincolando l'insieme dei treni autorizzati ad occupare la tratta contemporaneamente.
Il kernel di schedulazione dell'ATS è progettato per tenere conto di queste informazioni durante l'esecuzione delle sue scelte di schedulazione.
La correttezza complessiva del comportamento dell'ATS in presenza di ritardi viene infine verificata dimostrando che il progetto adottato garantisce l'assenza di deadlock del tracciato supervisionato.
La verifica formale dello scalo ferroviario completo viene eseguita scomponendolo in più regioni, che vengono analizzate separatamente, e dimostrando che la scomposizione adottata consente di estendere i risultati al layout completo.
La modellazione e verifica del sistema è stata effettuata utilizzando il framework UMC sviluppato presso ISTI.
UMC è una verifica astratta, al volo, basata su eventi di stato ambiente che lavora su macchine a stati simili a UML [2, 3].

2 Il modello iniziale del sistema

In UMC un sistema è descritto come un insieme di macchine a stati simili a UML comunicanti.
Nel nostro caso particolare il nucleo del sistema ATS è modellato da un'unica macchina a stati che ha uno status locale che descrive l'andamento attuale dei treni nello scalo ferroviario e che effettua le opportune scelte di schedulazione tra i treni in base alla struttura delle loro missioni.
Al nostro livello di analisi gli elementi base oggetto della programmazione sono la richiesta di itinerari, dove un itinerario è costituito dalla sequenza di circuiti di binario che devono essere percorsi per arrivare ad una banchina di stazione da un varco esterno, o per partendo da una banchina di una stazione in una direzione specifica verso un punto di uscita esterno.



(a) Visualizzazione livello itinerario (b) Vista a livello del circuito di binario

Fig. 1: Vista a livello di itinerario e circuito di binario di una stazione

In Figura 1 è mostrata la corrispondenza tra questi due livelli di astrazione del sistema.
Si noti che a livello di gestione dell'interlocking siamo interessati alla vista più dettagliata basata sul circuito di binario perché abbiamo a che fare con l'impostazione dei segnali e la commutazione degli scambi per la preparazione dei percorsi richiesti.

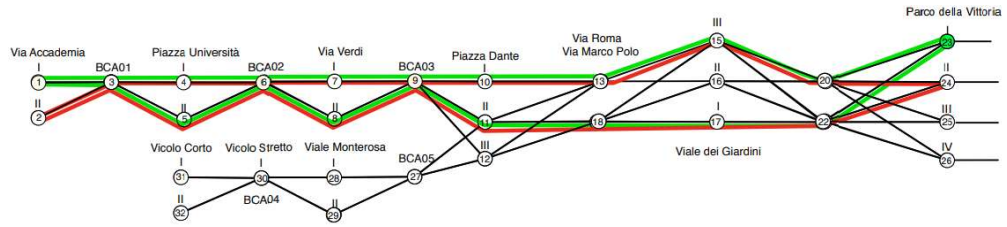


Fig. 2: Il layout dello scalo e le missioni per i treni della linea verde e rossa

Nel nostro caso, la mappa complessiva dello scalo ferroviario che descrive i vari marciapiedi di stazione interconnessi e i punti di ingresso/uscita di stazione (endpoint di itinerario) è mostrata in Figura 2.
Data la nostra mappa, la missione di un treno può essere vista come una sequenza di punti finali dell'itinerario.
Nel nostro caso il servizio è costituito da 8 treni che iniziano la loro missione nei punti estremi del tracciato e percorrono l'intero tracciato in una direzione.
Ad esempio le missioni dei quattro treni che erogano il servizio green-line e red-line mostrati in Figura 2, sono rappresentate dai seguenti dati:

Green1: [1,3,4,6,7,9,10,13,15,20,23] *Green2*: [23,22,17,18,11,9,5,8,6,5,3, 1]
Red1: [2,3,4,6,7,8,10,13,15,20,24] *Red2*: [24,22,17,18,11,9,5,8,6,5,3, 2]

Inizialmente, per scoprire tutte le possibili situazioni di stallo di base, i treni possono spostarsi da un punto all'altro solo se il punto di destinazione non è occupato.
Dato l'insieme delle missioni dei treni, e dato il loro attuale punto di avanzamento, il modello può dedurre quali treni hanno la libertà di avanzare e calcolare tutti i possibili stati successivi del sistema.
L'analisi iniziale del modello, anche con solo i 4 treni mostrati sopra, rivela immediatamente che si verificano deadlock in 4 sezioni del layout:

a) Nella sezione lineare [1-3] quando occupata da *Green1* e *Green2*.
b) Nella sezione lineare [2-3] quando occupata da *Red1* e *Red2*.
c) Nella sezione circolare [3-4-6-5] quando occupata da tutti e quattro i treni.
d) Nella sezione circolare [6-7-9-8] quando occupata da tutti e quattro i treni.

3 Introduzione alle sezioni critiche

Per ogni caso di stallo individuato al passaggio precedente possiamo costruire una contromisura per evitarlo associando una "sezione critica" all'insieme di punti su cui si è verificato lo stallo e vincolando contemporaneamente l'insieme dei treni autorizzati ad occuparlo .
Ad esempio, rispetto ai 4 casi di deadlock mostrati prima possiamo impostare il seguente insieme di sezioni/vincoli critici:

a) Tratta A=[1-3] : al massimo 1 dei treni *Green1* e *Green2*.
b) Tratta B=[2-3] : al massimo 1 dei treni *Red1* e *Red2*.
c) Sezione C=[3-4-6-5] : al massimo 3 di tutti e quattro i treni.
d) Sezione D=[6-7-9-8] : al massimo 3 dei quattro treni.

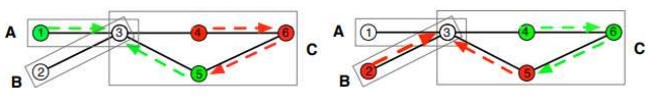


Fig. 3: Situazioni di stallo sulla composizione delle sezioni critiche di base

Una seconda versione del modello del nostro sistema può ora essere costruita prendendo in considerazione l'insieme delle sezioni critiche scoperte e arricchendo le definizioni delle missioni con le informazioni da quali sezioni critiche stiamo entrando/uscendo
quando ci spostiamo da un punto al successivo.
In questo modo il nostro modello ATS, prima di consentire l'avanzamento del treno, può prima verificare se il movimento del treno violerebbe il limite di qualche sezione critica.
Rispetto ai nostri 4 treni sul layout mostrato in Figura 2, la strategia ATS è descritta dai seguenti dati:

Sezioni: [A init 1 max 1,B init 1 max 1,C init 0 max 3,D init 0 max 3]
Verde1: [1,[C+],3,[A-],4,[D+],6,[C-],7,9,[D-],10,13,15,20,23]
Verde2: [23,22,17,18,11,[D+],9,5,8,[C+],6,[D-],5,[A+],3,[C-],1]
Rosso1: [2,[C+],3,[B-],4,[D+],6,[C-],7,9,[D-],10,13,15,20,24]
Rosso2: [24,22,17,18,11,[D+],9,5,8,[C+],6,[D-],5,[B+],3,[C-],2]

4 Sezioni critiche semplici e composite

Qualora si abbiano sezioni critiche che si sovrappongono parzialmente (condividendo alcuni punti comuni del layout), l'introduzione delle regole per l'inserimento di una sezione può introdurre ulteriori casi di deadlock non originariamente presenti nel sistema.
Pertanto sono necessari ulteriori cicli di controllo del modello per completare l'analisi del sistema.
Nel caso di 4 treni nel layout di Figura 2 il model checking rivela le nuove situazioni di stallo illustrate in Figura 3.
Si noti che nel caso sinistro il treno *Green2* non può uscire dalla sezione critica C perché non può entrare nella sezione critica A, e il treno *Green1* non può uscire dalla sezione critica A perché non può entrare nella sezione critica C.
Per risolvere queste situazioni possiamo introdurre un'ulteriore sezione critica composita E sui punti *[1-2-3-4-6-5]*, che può contenere al massimo 3 dei treni *Green1, Green2, Red1, Red2*.[1]
Al termine di questi ulteriori cicli di model checking la situazione è diventata come mostrato di seguito:

[1] In alternativa, possiamo aggiungere due sezioni aggiuntive e criteri di uscita più ottimizzati. Ciò consentirebbe di ottenere un modello anche privo di falsi positivi.

Sezioni: [A init 1 max 1,B init 1 max 1,C init 0 max 3,D init 0 max 3,E init 0 max 3]
Verde1:[1,[C+],3,[A-],4,[D+],6,[C-,E-],7,9,[D-],10,13,15,20,23]
Verde2:[23,22,17,18,11,[D+],9,5,8,[C+,E+],6,[D-],5,[A+],3,[C-],1]
Rosso1:[2,[C+],3,B-],4,[D+],6,[C-,E-],7,9,D-],10,13,15,20,24]
Rosso2:[24,22,17,18,11,[D+],9,5,8,[C+,E+],6,[D-],5,[B+],3,[C-],2]

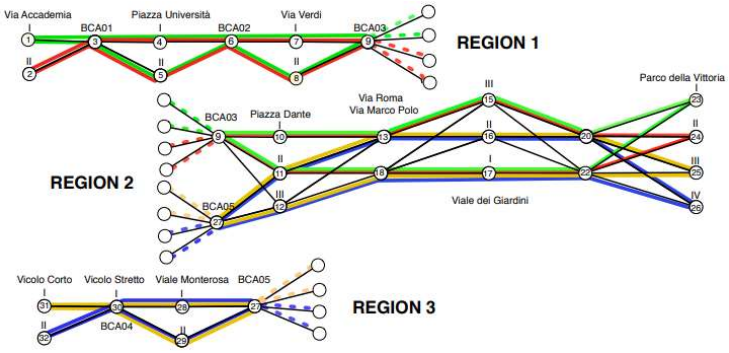


Fig. 4: Le tre regioni che suddividono l'intero layout

Una verifica finale del modello con 4 treni conferma che il trac è ora privo di deadlock e quindi che queste definizioni di sezione e dati di missione estesi possono essere utilizzati in sicurezza dall'ATS per la programmazione dei treni.

5 Partizionamento del modello completo

In realtà, il nostro sistema è più complesso di quello che abbiamo analizzato finora.
Abbiamo altri 4 treni che si muovono lungo il servizio di linea gialla e linea blu, con 8 treni che potrebbero occupare contemporaneamente il lato destro del tracciato.
Il nostro model checker non è in grado di eseguire un'analisi esaustiva dell'intera rete, quindi dobbiamo suddividere il layout complessivo in sottoregioni da analizzare separatamente.
Ad esempio possiamo partizionare il sistema come mostrato in Figura 4. L'analisi della regione 1 è stata mostrata sopra e ha permesso l'introduzione di 6 sezioni critiche.
L'analisi della regione 3 è simile alla precedente, e porta all'introduzione di ulteriori 5 sezioni critiche.
L'analisi della regione 2 è più complessa, essendo più grande e con 8 treni al suo interno. Tuttavia rivela altre due sezioni circolari in cui potrebbe verificarsi un deadlock (mostrato nella Figura 5).
Dopo l'introduzione delle opportune sezioni critiche anche la regione 2 può essere dimostrata priva di deadlock (la verifica richiede l'analisi di 1.636.498 stati).
In generale non è vero che l'analisi separata delle singole regioni in cui un layout è partizionato riveli effettivamente tutti i possibili deadlock dell'intero sistema.
Per questo è necessario che la partizione adottata non tagli (nascondendola all'analisi) alcuna sezione critica che si sovrapponga a due regioni.
Nel nostro caso questa proprietà del partizionamento è garantita da due fatti.
In primo luogo, l'insieme dei punti di confine in comune tra ciascuna regione e il suo "mondo esterno" è costituito da un unico punto.
Ciò garantisce che la partizione non tagli alcuna sezione critica circolare, perché ciò avrebbe creato almeno due punti nel confine.
In secondo luogo, il punto di confine (unico) non appartiene a una sezione critica in ciascun lato del confine.
Infatti, se ciò fosse accaduto, avrebbe potuto portare ad una sezione critica composita non scoperta composta dall'unione delle due sezioni critiche confinanti delle due regioni.

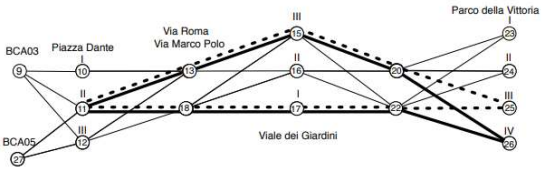


Fig. 5: Due sezioni critiche nella regione 2

6. Conclusioni

Lo sviluppo di soluzioni al problema dell'elusione dello stallo nella programmazione dei treni è un compito complesso e ancora aperto.
Molti studi sono stati condotti in materia a partire dai primi anni '80, ma la maggior parte di essi sono relativi al normale tracciato ferroviario, e non al caso particolare dei sistemi metropolitani driverless.
I sistemi automatici di metropolitana infatti possono esprimere alcune proprietà originali, ad es. la difficoltà dell'impossibilità di cambiare la missione di un treno, che rende il problema alquanto diverso, ad esempio, dalla programmazione dei treni merci per i quali l'unica informazione veramente rilevante è la destinazione finale del treno.
I metodi formali sono stati ampiamente e con successo utilizzati nel contesto ferroviario [4], ma di solito sono applicati solo ai loro componenti critici per la sicurezza.
L'ATS, nonostante la sua rilevanza funzionale, non è considerato un componente critico per la sicurezza e non siamo a conoscenza di altre esperienze nella sua progettazione formale.
Il progetto nell'ambito del quale è stato condotto questo studio è ancora in corso e l'attuale prototipo di ATS è in fase di sviluppo.
Ci sono molte direzioni in cui questo lavoro potrebbe procedere.
Ad esempio, sarebbe interessante vedere se la fase di model checking per il rilevamento di regioni critiche potrebbe essere inclusa come parte del comportamento ATS invece di essere eseguita in una precedente fase di preconfigurazione.
Ciò consentirebbe, se necessario, di effettuare in modo automatico e sicuro anche il cambio dinamico dell'itinerario dei treni.
Attualmente i dati rilevati dal controllore modello devono essere analizzati manualmente e i dati di configurazione ATS devono essere creati manualmente e questa attività potrebbe essere fonte di errori.
È possibile immaginare invece che i dati di configurazione dell'ATS siano generati automaticamente anche dai risultati del model check del sistema.