

UNIVERSITÀ DEGLI STUDI DI UDINE
DIPARTIMENTO DI MATEMATICA E INFORMATICA
CORSO DI LAUREA IN TECNOLOGIE WEB E MULTIMEDIALI

TESI DI LAUREA

Verifica di proprietà locali su BRS

CANDIDATO:
Luca Geatti

RELATORE:
Prof. Marino Miculan

CO-RELATORE:
Dott. Marco Peressotti

Anno Accademico 2014-2015

Dipartimento di Matematica e Informatica
Università degli Studi di Udine
Via delle Scienze, 206
33100 Udine
Italia

Ai miei genitori

Indice

Introduzione	vii
1 Bigrafi e BRS	1
1.1 Definizione informale di Bigrafo	1
1.1.1 Esempio	2
1.2 Definizione formale di Bigrafo	5
1.2.1 Place Graph	5
1.2.2 Link Graph	6
1.2.3 Bigrafo	8
1.3 Operazioni sui Bigrafi	8
1.3.1 Traduzione di Supporto	9
1.3.2 Composizione	9
1.3.3 Giustapposizione	11
1.4 L' algebra dei bigrafi	12
1.4.1 Placing elementari	13
1.4.2 Linking elementari	13
1.4.3 Ioni	14
1.4.4 Forma normale discreta	15
1.5 Bigraphical Reactive Systems	16
1.5.1 Esempio	17
1.5.2 Regole di reazione parametriche	19
1.5.3 BRS	21
1.5.4 Esempio	21
2 Isomorfismo tra bigrafi	25
2.1 Esempio:	25
2.2 Formulazione del problema	26
2.3 Strategia di soluzione	27

2.3.1	Esempi	28
2.4	Vincoli	30
2.4.1	Vincoli per il place graph	30
2.4.2	Vincoli per il link graph	34
2.4.3	Vincoli di coerenza	38
2.5	Grafo degli stati	40
2.5.1	Esempio	42
2.6	Complessità	45
3	Model Checker per bigrafi	49
3.1	Model Checker	49
3.1.1	Generazione degli stati	50
3.2	Logica per i bigrafi	53
3.2.1	Sintassi	53
3.2.2	Semantica	54
3.3	Dettagli Implementativi	55
3.3.1	Property Matcher	56
3.3.2	Regole di Reazione con Proprietà	56
3.4	Esempi	57
3.4.1	Moltiplicazione	57
3.4.2	Router	58
4	Esempi	63
4.1	NFA	63
	Conclusioni	73
A	Notazione dei vari capitoli	75
A.1	Notazione della sezione 1.2	75
A.2	Notazione della sezione 1.4	75
A.3	Notazione della sezione ??	76
	Bibliografia	77

Elenco delle figure

1.1	Un semplice bigrafo.	2
1.2	Le due strutture ortogonali del bigrafo B.	2
1.3	Il bigrafo C.	4
1.4	Bigrafo C.	4
1.5	Un semplice bigrafo.	4
1.6	Bigrafo A.	5
1.7	Link Graph decomposto.	7
1.8	Esempio di bigrafo.	8
1.9	Placing elementari.	13
1.10	Linking elementari.	14
1.11	$K_{\vec{x}}$	14
1.12	Atomo e molecola discreti.	15
1.13	Esempio.	17
1.14	Prima regola di reazione	18
1.15	Seconda regola di reazione	18
1.16	Terza regola di reazione	19
1.17	Moltiplicazione tramite bigrafi	22
1.18	Caso ricorsivo	22
1.19	Caso Base	23
1.20	Match decomposto	24
1.21	Bigrafo finale	24
2.1	Bigrafi Isomorfi: $(4 * 2) = (2 * 4)$	28
2.2	Bigrafi non Isomorfi	29
2.3	Place Graph e Link Graph del bigrafo 2.2	29
2.4	Rete di flusso per l'isomorfismo tra place graphs.	30
2.5	Soluzione della rete di flusso	31
2.6	Esempio per il primo vincolo	32

2.7	Esempio per il secondo vincolo	33
2.8	Esempio per il vincolo sul flusso in uscita	33
2.9	Esempio per il vincolo sul flusso in entrata	34
2.10	Esempio di rete di flusso per il problema di isomorfismo tra link graphs.	35
2.11	Esempio per il primo vincolo.	36
2.12	Esempio per il secondo vincolo.	37
2.13	Esempio per i due vincoli sul flusso in uscita.	37
2.14	Esempio per i due vincoli sul flusso in entrata.	38
2.15	Esempio di grafo degli stati.	40
2.16	Grafo degli stati infinito.	41
2.17	Regola di inoltro tra router.	42
2.18	Bigrafo di partenza	43
2.19	Bigrafo dopo l'applicazione della regola R_0	44
2.20	Grafo degli stati infinito.	44
2.21	Grafo degli stati finito.	44
3.1	Grafo degli stati.	50
3.2	Esempio di generazione Breadth First.	51
3.3	Esempio di generazione random.	52
3.4	Regola di inoltro tra router.	56
3.5	Bigrafo per il numero 8	57
3.6	Model Checker.	58
3.7	Bigrafo di partenza	58
3.8	Regola di inoltro tra router.	59
3.9	Esempi di predicati	59
3.10	Grafo degli stati	60
3.11	Predicato con proprietà	61
4.1	Automa per il linguaggio $(a(a+b))^*$	63
4.2	Bigrafo per l'automa A	64
4.3	Bigrafo per la stringa "abaa"	65
4.4	Istanza del problema: la stringa "abaa" viene accettata dall'automa A?	66

4.5	Regola di reazione R_0	67
4.6	Bigrafo B	68
4.7	Grafo degli stati	68
4.8	Traccia d'esecuzione di MC_{big}	71

Introduzione

Il lavoro riportato in questa tesi nasce dal problema di verificare delle proprietà in un Sistema Reattivo Bigrafico (BRS). In particolare, si è studiato il modo di controllare questo sistema reattivo durante la sua evoluzione e dunque di fermare quest'ultima appena le proprietà desiderate siano state raggiunte. Questo tipo di verifica va sotto il nome di "Model Checking".

I Sistemi Reattivi Bigrafici (BRS) sono un nuovo formalismo con il quale si possono rappresentare sistemi distribuiti, di qualsiasi tipo essi siano: da un sistema di smartphones ad un sistema biologico. I BRS sono basati su un'importante struttura matematica: i bigrafi. Sono questi che permettono una facile trattazione dei vari "oggetti distribuiti" che compongono il mio sistema, e di come essi interagiscono tra di loro.

L'importanza dei bigrafi la si può riscontrare nella loro flessibilità: dando loro una certa "grammatica", è possibile rappresentare sistemi di qualsiasi dominio si voglia. Di recente i bigrafi sono stati usati per controllare droni [1], come anche per fornire un supporto alle decisioni di instradamento dei router [2].

Un altro punto di forza dei bigrafi sta nella loro capacità di evolversi, potendo così rappresentare lo stato del sistema anche quando questo cambia. Si ha così a disposizione un Sistema Reattivo Bigrafico.

Questa tesi tratta il problema di come poter sapere se un dato BRS rispetti certe proprietà. Per esempio: se rappresentiamo una rete con un BRS, ci possiamo chiedere se, dato uno stato iniziale in cui il pacchetto parte dal mittente A, esso arrivi o meno al destinatario B che si trova a vari router di distanza da A. Oppure, cambiando dominio del problema, ci possiamo domandare se, data una configurazione iniziale del gioco della vita, il giocatore X possa vincere ed entro quante mosse.

Nei precedenti due casi, le proprietà da verificare sono rispettivamente l'arrivo a destinazione del pacchetto e la condizione di vincita al gioco della vita.

Il problema affrontato in questa sede prescinde quindi dal particolare dominio del problema, ed offre una soluzione generale, cioè valida per qualsiasi BRS. Per fare questo, si sono dovute affrontare varie problematiche. Tra le più importanti figurano:

- quando due bigrafi sono uguali? Un BRS evolve senza memoria degli stati precedenti in cui si è trovato. Questo problema, in concreto, può potenzialmente causare evoluzioni infinite del BRS: per esempio, il pacchetto nella rete può girare all'infinito tra due router, perchè il BRS si "dimentica" da dove il pacchetto è arrivato.
- come rappresentare le proprietà da verificare nel BRS? In particolare, posso rappresentare con un solo formalismo vari tipi di proprietà, dall'arrivo a destinazione di un pacchetto alla condizione di vincita di un gioco? Il problema maggiore è il fatto che il modo per rappresentarle deve essere generale tanto quanto i BRS. In sostanza si è scelto un modo che astraesse ancora una volta dal dominio scelto.

La struttura della tesi rispetta dunque queste problematiche:

Nel capitolo 1 verranno presentate formalmente le nozioni di Bigrafo e di BRS. Con esse, verrà anche descritta un'algebra per creare nuovi bigrafi a partire da bigrafi base.

Nel capitolo 2 si affronta il primo dei due principali problemi, che va sotto il nome di "isomorfismo tra bigrafi". La risoluzione di questo problema ci permetterà di poter affermare quando due bigrafi sono uguali o meno, e quindi di evitare evoluzioni infinite del BRS.

Si affronterà nel capitolo 3 il secondo problema, cioè quello delle proprietà. Esse verranno espresse sul calcolatore tramite una semplice logica a predicati. Si potranno così esprimere tutte le proprietà desiderate, indipendentemente dal dominio del sistema. Grazie a queste proprietà, si arriverà all'implementazione di un Model Checker per i bigrafi.

Nel capitolo 4 verranno presentati alcuni esempi, presi da vari domini. Si potrà apprezzare l'importanza di avere un Model Checker e della semplicità con cui si possono esprimere le proprietà da verificare.

Infine (capitolo 5), si sono tratte le conclusioni sull'intero lavoro. Verranno presentate alternative per l'implementazione dell'isomorfismo e delle proprietà.

1

Bigrafi e BRS

In questo capitolo vengono presentate le descrizioni formali di bigrafo e di Sistema Reattivo Bigrafico. Si vedrà come l'importanza dei bigrafi risieda nel fatto di rappresentare contemporaneamente i concetti di *località* e *connessione*.

L'algebra dei bigrafi è stata per gran parte costruita sulla base della Teoria delle Categorie, che in questa sede non verrà introdotta. Le definizioni ed i teoremi sono stati presi da [1], a cui si rimanda per i dettagli sulla Teoria delle Categorie. Infine si rimanda all'Appendice A per la descrizione della terminologia usata.

1.1 Definizione informale di Bigrafo

L'idea fondamentale alla base della loro teoria, è che ogni bigrafo sia composto da due strutture del tutto *indipendenti* sullo *stesso* insieme di nodi. Queste due strutture si chiamano *Place Graph* e *Link Graph* e modellano rispettivamente la località e la connessione.

Nell'introduzione, si è accennato al fatto che i bigrafi sono flessibili e adatti a rappresentare ogni dominio. Questo è possibile grazie al concetto di *segnatura*, che è l'analogo ad una grammatica per un linguaggio.

Definizione 1 (Segnatura e Controllo). *Una segnatura è una coppia (K, ar) , dove K è un insieme di tipi di nodi chiamati controlli, e $ar : K \rightarrow \mathbb{N}$ è una mappa che associa ad ogni tipo di nodo (cioè ad ogni controllo) un numero naturale chiamato arietà.*

Quindi, dare una segnatura ad un bigrafo significa associare ad ogni nodo sia un tipo sia il suo numero di porte. L'equivalente grafico consiste nel disegnare nodi diversi con simboli diversi.

Notazione (Segnatura). *Da qui in avanti, una segnatura (K, ar) verrà indicata nel seguente modo:*

$$K = \{K_1 : a_1, \dots, K_n : a_n\}$$

dove ogni nodo di tipo (controllo) K_i ha arietà a_i .

1.1.1 Esempio

Diamo un primo esempio informale di bigrafo.

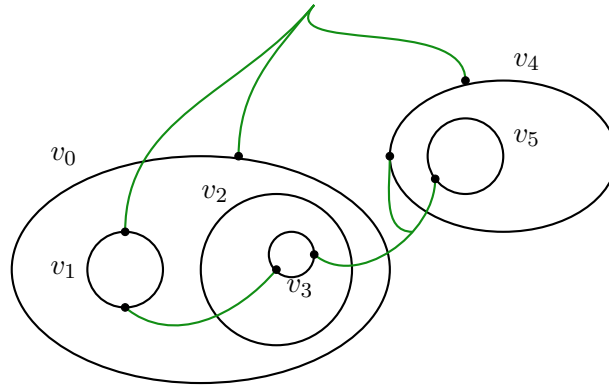


Figura 1.1: Un semplice bigrafo.

In figura 1.1 vediamo un bigrafo B , con una data segnatura. Si vede subito come ci siano dei controlli diversi. Per esempio, il nodo v_0 ha una sola porta mentre il nodo v_1 ne ha due. L'informazione che quest'ultimo sia contenuto in v_0 è rappresentata nel place graph di figura 1.2.a. Le interconnessioni dei vari nodi sono invece riportate nel rispettivo link graph di figura 1.2.b.

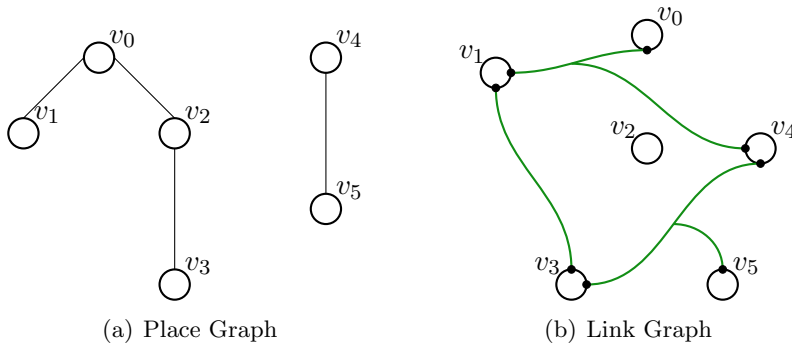


Figura 1.2: Le due strutture ortogonali del bigrafo B .

Un'importante caratteristica dei bigrafi e della loro algebra è la possibilità di essere composti, cioè di formare un nuovo bigrafo da due bigrafi di partenza. Questo è equivalente al problema di considerare un bigrafo *parte* di un altro. Si vedrà che questa operazione va sotto il nome di *composizione*. Se prendiamo il bigrafo B di cui sopra, allora è possibile scrivere un'equazione di questo tipo:

$$B = A \circ C$$

Per renderla possibile dobbiamo aggiungere struttura ai bigrafi. Si introducono quindi le interfacce interne ed esterne, sia per il place graph sia per il link graph:

- L'interfaccia esterna ed interna del place graph sono un numero naturale n che possiamo trattare come un ordinale: l'interfaccia n indica l'insieme $\{0, \dots, n-1\}$. Se l'interfaccia esterna è k , allora si dice che ci sono k radici. Se l'interfaccia interna è h , allora si dice che ci sono h siti.
- Per il link graph, invece, le interfacce sono *insiemi* di nomi, come per esempio $\{x, y\}$. Se un link graph ha un'interfaccia esterna del tipo $\{a, b, c\}$, allora diciamo che ci sono tre *outernames* chiamati a, b e c . Se l'interfaccia interna è del tipo $\{x, y\}$, allora diciamo che il bigrafo ha due *innername* chiamati x e y .

Il concetto fondamentale delle interfacce è che servono per l'unione dei due bigrafi. Per esempio, prendendo il place graph, nell'operazione di composizione $A \circ C$, i siti di A dovranno *concordare* (vedremo una descrizione formale di questo concetto) con le radici di C. Per il link graph il concetto è lo stesso: gli innername di A dovranno unirsi con gli outernames di C.

Si consideri per esempio il bigrafo della figura 1.1. Se vogliamo trovare due bigrafi A e C tali che $B = A \circ C$, allora dobbiamo rispettare le condizioni con cui si può effettuare l'operazione di composizione. Le figure 1.3 e 1.5 rappresentano rispettivamente i due bigrafi C ed A. Si noti ancora una volta che le radici di C si *uniscono* ai siti di A, e gli outernames di C fanno lo stesso con gli innername di A.

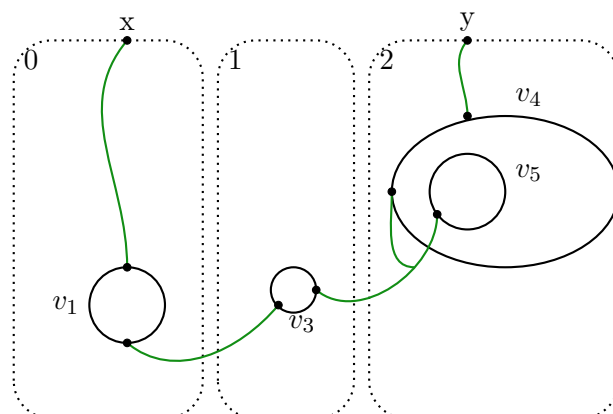


Figura 1.3: Il bigrafo C.

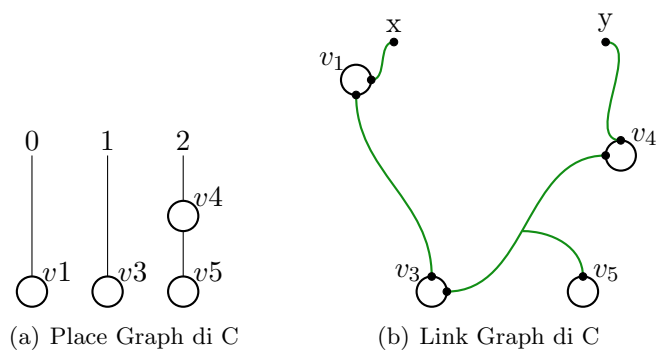


Figura 1.4: Bigrafo C.

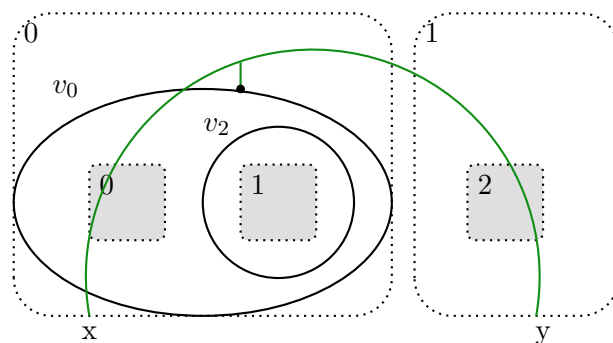


Figura 1.5: Un semplice bigrafo.

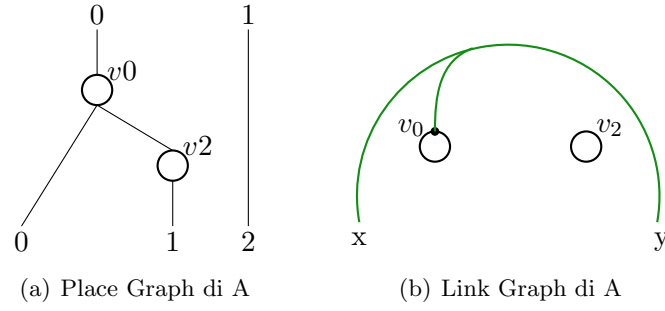


Figura 1.6: Bigrafo A.

1.2 Definizione formale di Bigrafo

Siamo ora pronti per definire separatamente i concetti di *Place Graph* e *Link Graph*. Quelli descritti, che noi chiameremo semplicemente bigrafi, in realtà si chiamano *concrete bigraphs*, per distinguerli da quelli astratti. In questa sede si tratterà solo di bigrafi concreti.

Si rimanda all'appendice A per la notazione usata.

1.2.1 Place Graph

Il place graph è una delle due strutture fondamentali di ogni bigrafo. E' una *foresta* e rappresenta l'informazione di *nesting*, ovvero quali nodi si trovano all'interno di altri. Come già notato in figura 1.2.a, le radici ed i siti sono *ordinati*, essendo essi rappresentati da un ordinale. In definitiva, quindi, il place graph è una foresta ordinata, in cui solo le radici ed i siti sono ordinati.

Definizione 2 (Place Graph). *Un place graph*

$$F = (V_F, ctrl_F, prnt_F) : m \rightarrow n$$

è una tripla avente un' interfaccia interna m ed un' interfaccia esterna n , entrambe ordinali finiti. Queste indicano rispettivamente i siti e le radici del place graph. F ha un insieme finito V_F di nodi, una control map $ctrl : V_F \rightarrow K$, e una parent map

$$prnt : m \uplus V_F \rightarrow V_F \uplus n$$

che è aciclica, cioè se $prnt_F^i(v) = v$ allora $i = 0$.

Questa definizione formale ricalca ciò che è già stato notato nell' esempio della sottosezione 1.1.1. Infatti, si noti che il place graph F ha m siti ed n radici, entrambi

ordinati, che costituiscono rispettivamente la sua interfaccia interna ed esterna. La funzione $ctrl_F$ associa ad ogni nodo un controllo, cioè un nome. Come già notato, l'equivalente grafico sta nel disegnare con simboli diversi nodi con controllo diverso. Infine, la funzione $prnt_F$ associa ad ogni nodo interno o sito il suo genitore, che può essere a sua volta un altro nodo interno o una radice. Questa funzione è di fondamentale importanza, in quanto è il cuore del place graph: rappresenta l'informazione di quali nodi si trovano all'interno di altri. E' *aciclica*, nel senso che n sue *composizioni* non porteranno mai al nodo di partenza. In formule:

$$prnt_F \circ prnt_F \circ \dots \circ prnt_F(v) \neq v$$

Questo è equivalente a dire che la struttura dati rappresentata dal place graph è una *foresta*.

1.2.2 Link Graph

La seconda struttura dati fondamentale è il link graph. Esso rappresenta l'informazione di *connessione* tra i nodi del bigrafo. E' un *ipergrafo*, infatti un arco può collegare due o più nodi.

Definizione 3 (Link Graph). *Un link graph*

$$F = (V_F, E_F, ctrl_F, link_F) : X \rightarrow Y$$

è una quadrupla avente un' interfaccia interna X ed una interfaccia esterna Y , chiamate rispettivamente gli *inner names* e *outer names* del link graph. F ha un insieme finito V_F di nodi e E_F di archi (edges), una control map $ctrl : V_F \rightarrow K$, e una link map:

$$link_F : X \uplus P_F \rightarrow E_F \uplus Y$$

dove $P_F = \{(v, i) \mid v \in V_F \wedge i \in ar(ctrl_F(v))\}$ è l'insieme delle porte di F . Quindi, (v, i) è l' i -esima porta del nodo v . Chiamiamo $X \uplus P_F$ i punti di F , mentre $E_F \uplus Y$ i suoi link.

Notiamo subito come alcune nozioni rimangono invariate dal place graph. Per esempio, V_F e $ctrl_F$ non cambiano. Si aggiungono però due concetti:

- E_F : è l'insieme di archi del link graph F . Sono oggetti del tutto indipendenti dai nodi.

- $link_F$: è la funzione che consente di creare l'*ipergrafo*.

Dalla definizione 1.1, sappiamo che un dato controllo ha un ben preciso numero di porte. La funzione $ar : K \rightarrow \mathbb{N}$ consente di calcolare il numero di porte di un dato controllo: $ar(ctrl_F(v))$ restituisce un numero naturale, che è il numero di porte del controllo del nodo v . Grazie alla funzione ar , nel link graph ci sleghiamo totalmente dal concetto di *nodo*, e siamo in grado di sostituirlo con il concetto di *porta*.

Introduciamo ora due concetti:

- l'insieme dei *punti* di F è l'insieme che comprende tutte le sue porte (P_F) e tutti i suoi inner names (X).
- l'insieme dei *link* di F è l'insieme che comprende tutti i suoi archi (edges) e tutti i suoi outer names (Y).

La funzione $link_F$ avrà come dominio l'insieme dei punti e come codominio l'insieme dei link. Possiamo quindi pensarla come è raffigurata in figura 1.7.b. La funzione $link_F$ è perciò quella che crea il vero e proprio ipergrafo: associa ad ogni punto *uno ed un solo* link. Sfruttando la *non-iniettività* della funzione possiamo creare l'ipergrafo.

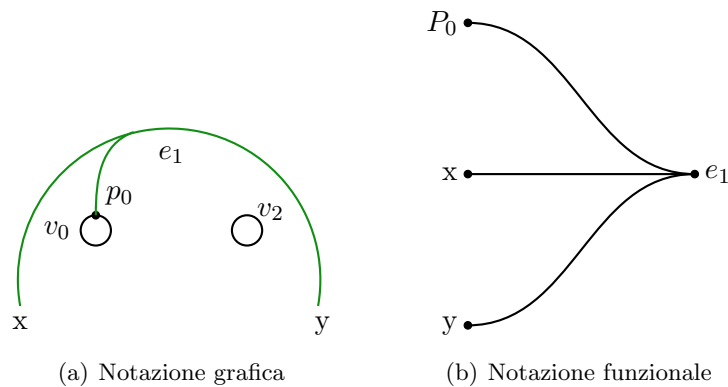


Figura 1.7: Link Graph decomposto.

In figura 1.7.a si vede il link graph nella sua notazione usuale, cioè con anche i nodi disegnati. Invece, in 1.7.b si vede la notazione sotto forma di funzione, dove si specifica dominio (p_0 , x e y) e codominio (e_1).

1.2.3 Bigrafo

Un bigrafo è semplicemente l'unione del place graph e del link graph. E' importante notare che esse condividono lo *stesso* insieme di nodi.

Definizione 4 (Bigrfo). *Un bigrafo*

$$F = (V_F, E_F, ctrl_F, prnt_F, link_F) : \langle n, X \rangle \rightarrow \langle m, Y \rangle$$

consiste in un place graph $F^P = (V_F, ctrl_F, prnt_F) : n \rightarrow m$ e in un link graph $F^L = (V_F, E_F, ctrl_F, link_F) : X \rightarrow Y$.

Notazione (Bigrfo). *Un bigrafo F viene spesso indicato tramite le sue interfacce:*

$$F = \langle n, X \rangle \rightarrow \langle m, Y \rangle$$

stando ad indicare che F ha n siti, X inner names, m radici e Y outer names.

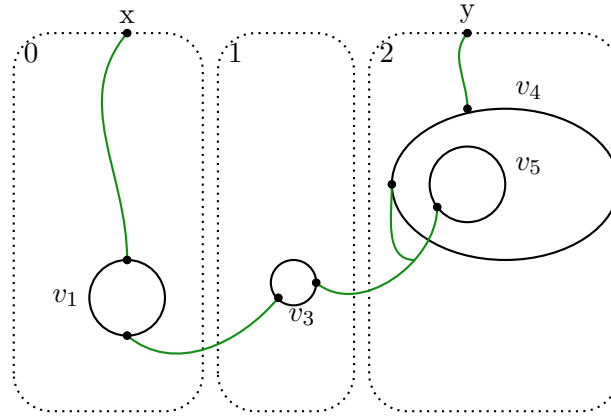


Figura 1.8: Esempio di bigrafo.

Il bigrafo della figura 1.8, rispettando la notazione, è scritto in questo modo:
 $F = \langle 0, \emptyset \rangle \rightarrow \langle 3, \{x, y\} \rangle$

1.3 Operazioni sui Bigrafi

Nelle sezioni precedenti, si è definita formalmente la nozione di bigrafo. Ora, si studiano le varie operazioni possibili, ovvero come ottenere un nuovo bigrafo da due bigrafi di partenza. Queste operazioni saranno utili per la prossima sezione, che tratterà dell'algebra dei bigrafi.

1.3.1 Traduzione di Supporto

La prima operazione tratta di come si può ottenere un nuovo bigrafo avendo a disposizione un solo bigrafo base e una funzione biettiva. Si dimostra che applicando tale biiezione ai nodi e archi del bigrafo di partenza si determina *unicamente* il bigrafo risultante.

Definizione 5 (Traduzione di Supporto). *Per ogni place graph, link graph e per ogni bigrafo è assegnato un insieme finito $|F|$, il suo supporto. Per un place graph, definiamo $|F| = V_F$, mentre per un link graph o un bigrafo definiamo $|F| = V_F \uplus E_F$. Per due bigrafi F e G , una traduzione di supporto $p : |F| \rightarrow |G|$ da F a G consiste in due biiezioni $p_V : V_F \rightarrow V_G$ and $p_E : E_F \rightarrow E_G$ che rispettano la struttura, nel seguente senso:*

- p preserva i controlli, cioè: $ctrl_G \circ p_V = ctrl_F$. Ne segue che p induce una biiezione sulle porte $p_P : P_F \rightarrow P_G$, definita da $p_P((v, i)) = (p_V(v), i)$.
- p modifica le mappe sulla struttura ($prnt$ e $link$) in questo modo:

$$\begin{aligned} prnt_G \circ (id_m \uplus p_V) &= (id_n \uplus p_V) \circ prnt_F \\ link_G \circ (id_X \uplus p_P) &= (id_Y \uplus p_E) \circ link_F \end{aligned}$$

Come detto prima, data la biiezione p e il bigrafo F , queste condizioni determinano unicamente G , che denotiamo con $p \cdot F$ e chiamiamo *traduzione di supporto di F tramite p* . Chiamiamo F e G *support equivalent* ($F \simeq G$) se esiste una tale traduzione di supporto.

Dati due bigrafi, il problema di trovare una traduzione di supporto tra i due è equivalente al problema di stabilire quando essi sono uguali. Per cui, da qui in seguito si userà il termine *traduzione di supporto* come sinonimo di *isomorfismo*.

Definizione 6 (Isomorfismo). *Due bigrafi F e G si dicono isomorfi se e solo se esiste una traduzione di supporto tra F e G , cioè se e solo se F e G sono support equivalent ($F \simeq G$).*

1.3.2 Composizione

L'operazione di *composizione* è denotata dal simbolo \circ e permette di scrivere equazioni del tipo $B = A \circ C$, come nell'esempio 1.1.1. La composizione necessita del

concetto di interfaccia: come già notato, l'interfaccia interna di A deve concordare con l'interfaccia esterna di C . Con una prima approssimazione, possiamo dire che C deve essere incluso *dentro* A .

Definizione 7 (Composizione). *Si trattano separatamente i casi del place graph e del link graph:*

- Place Graph: Se $F : k \rightarrow m$ e $G : m \rightarrow n$ sono due place graph con supporti disgiunti ($|F| \# |G|$), la loro composizione

$$G \circ F = (V, ctrl, prnt) : k \rightarrow n$$

ha i nodi $V = V_F \uplus V_G$ e la control map $ctrl = ctrl_F \uplus ctrl_G$. La sua parent map $prnt$ è definita come segue: se $w \in k \uplus V_F \uplus V_G$ è un sito o un nodo di $G \circ F$, allora :

$$prnt(w) \stackrel{def}{=} \begin{cases} prnt_F(w), & \text{se } w \in k \uplus V_F \wedge prnt_F(w) \in V_F \\ prnt_G(j), & \text{se } w \in k \uplus V_F \wedge prnt_F(w) = j \in m \\ prnt_G(w), & \text{se } w \in V_G \end{cases}$$

Il place graph identità su m è $id_m \stackrel{def}{=} (\emptyset, \emptyset, id_m) : m \rightarrow m$

Si noti come l'unione delle due interfacce (quella esterna di A e quella interna di B) sia modellata dalla seconda riga. In particolare, $prnt_F(w) = j$ sta ad indicare che j è una radice di F e w è uno dei suoi figli. Dato che j è una radice, essa sarà un intero nell'insieme $\{0, \dots, m-1\}$, e dovrà quindi appartenere anche all'interfaccia interna di G , dove j sarà un sito. La parent map di $G \circ F$ su w sarà quella di G sul suo sito j . Quindi la seconda riga modella la seguente azione: mantengo la parent map per tutti i nodi interni dei due bigrafi, e al momento dell'unione delle due interfacce unisco la radice i -esima di F con il sito i -esimo di G , per ogni $i \in \{0, \dots, m-1\}$.

- Link Graph: Se $F : X \rightarrow Y$ e $G : Y \rightarrow Z$ sono due link graph con supporti disgiunti ($|F| \# |G|$), la loro composizione

$$G \circ F = (V, E, ctrl, link) : X \rightarrow Z$$

ha $V = V_F \uplus V_G$, $E = E_F \uplus E_G$, $ctrl = ctrl_F \uplus ctrl_G$ e la sua link map $link$ è definita come segue: se $q \in X \uplus P_F \uplus P_G$ è un punto di $G \circ F$, allora

$$link(q) \stackrel{def}{=} \begin{cases} link_F(q), & \text{se } q \in X \uplus P_F \wedge link_F(q) \in E_F \\ link_G(y), & \text{se } q \in X \uplus P_F \wedge link_F(q) = y \in Y \\ link_G(q), & \text{se } q \in P_G \end{cases}$$

Il link graph identità su X è $id_X \stackrel{def}{=} (\emptyset, \emptyset, \emptyset, id_X) : X \rightarrow X$. Anche qui, si noti come la seconda riga modella l'unione tra le interfacce. In particolare, se $link_F(q) = y$ e $y \in Y$, si ha che il punto q del bigrafo F è collegato al suo outer name y . Dato che Y è anche l'interfaccia interna di G , si ha che y è un inner name di G . La seconda riga quindi rappresenta l'unione tra gli outernames di F e gli inner names di G che hanno lo stesso nome.

- Bigrafo: Se $F : I \rightarrow J$ e $G : J \rightarrow K$ sono due bigrafi con supporti disgiunti ($|F| \# |G|$), la loro composizione

$$G \circ F \stackrel{def}{=} \langle G_P \circ F_P, G_L \circ F_L \rangle : I \rightarrow K$$

ed il bigrafo identità su $I = \langle m, X \rangle$ è $\langle id_m, id_x \rangle$.

Si noti come l'operazione di composizione *unisca* le interfacce dei due bigrafi, creando un unico bigrafo risultato, cioè un' unica funzione *prnt* ed un' unica funzione *link*.

1.3.3 Giustapposizione

Si definisce ora un' altra operazione per creare un bigrafo da altri due base. Si chiama *giustapposizione* e consiste nell'affiancare un bigrafo ad un altro. Questa operazione è possibile solo se i due bigrafi sono *disgiunti*. Spesso viene anche chiamata *prodotto*.

Definizione 8 (Bigrafi disgiunti). *Due place graphs $F_i (i = 0, 1)$ sono disgiunti se $|F_0| \# |F_1|$. Due link graph $F_i : X_i \rightarrow Y_i$ sono disgiunti se $X_0 \# X_1$, $Y_0 \# Y_1$ e $|F_0| \# |F_1|$. Due bigrafi $F_i (i = 0, 1)$ sono disgiunti se $F_0^P \# F_1^P$ e $F_0^L \# F_1^L$.*

L'operazione di giustapposizione è monoidale, cioè è associativa ed ha un unità. Si definiranno quindi le proprietà dell'operazione e le sue unità.

Definizione 9 (Giustapposizione). *Definiamo separatamente i casi del place graph e del link graph:*

- Place Graph: la giustapposizione di due interfacce $m_i (i = 0, 1)$ è $m_0 + m_1$ e l'unità è 0 . Se $F_i = (V_i, ctrl_i, prnt_i) : m_i \rightarrow n_i$ sono place graphs disgiunti ($i = 0, 1$), la loro giustapposizione $F_0 \otimes F_1 : m_0 + m_1 \rightarrow n_0 + n_1$ è data da:

$$F_0 \otimes F_1 = (V_0 \uplus V_1, ctrl_0 \uplus ctrl_1, prnt_0 \uplus prnt'_1),$$

dove $prnt'_1(m_0 + i) = n_0 + j$ ogni volta che $prnt_1(i) = j$.

Informalmente, affianco due place graph avendo come risultato una foresta. Le radici aumenteranno quindi di numero. Per questo motivo è necessaria la funzione $prnt'_1$: supponiamo che F_0 abbia due radici e F_1 una sola. I nodi figli diretti di F_1 non possono più puntare alle loro vecchie radici, per esempio la radice 0, perchè ora essa è la radice di F_0 . La parent map di F_1 dovrà quindi venire traslata in questo modo: tutti i nodi di F_1 che puntano alla sua radice 0, ora punteranno alla nuova radice $0 + 2 = 2$. Questo è quello che fa la funzione $prnt'_1$.

- Link Graph: la giustapposizione di due interfaccie disgiunte di due link graph è $X_0 \uplus X_1$ e l'unità è \emptyset . Se $F_i = (V_i, E_i, ctrl_i, link_i) : X_i \rightarrow Y_i$ sono due link graph disgiunti ($i = 0, 1$), la loro giustapposizione $F_0 \otimes F_1 : X_0 \uplus X_1 \rightarrow Y_0 \uplus Y_1$ è data da

$$F_0 \otimes F_1 = (V_0 \uplus V_1, E_0 \uplus E_1, ctrl_0 \uplus ctrl_1, link_0 \uplus link_1)$$

- Bigrafi: la giustapposizione di due interfacce disgiunte $I_i = \langle m_i, X_i \rangle (i = 0, 1)$ è $\langle m_0 + m_1, X_0 \uplus X_1 \rangle$ e l'unità è $\varepsilon = \langle 0, \emptyset \rangle$. Se $F_i : I_i \rightarrow J_i$ sono bigrafi disgiunti ($i = 0, 1$), la loro giustapposizione $F_0 \otimes F_1 : I_0 \otimes I_1 \rightarrow J_0 \otimes J_1$ è data da:

$$F_0 \otimes F_1 = \langle F_0^P \otimes F_1^P, F_0^L \otimes F_1^L \rangle$$

Tutte queste tre operazioni saranno utili per definire l'algebra dei bigrafi della prossima sezione.

1.4 L' algebra dei bigrafi

In questa sezione verrà illustrato come poter ottenere nuovi bigrafi da bigrafi base tramite le operazioni di composizione, identità e prodotto (giustapposizione). Si definisce quindi una vera e propria *algebra* per la teoria dei bigrafi, in cui si dimostra che ogni bigrafo può essere derivato da alcuni bigrafi base. Si incomincia nelle prime tre sezioni ad illustrare i bigrafi base su cui si appoggerà l'algebra, ovvero placing, linking e ioni. Infine, si enuncia un importante risultato che è la decomponibilità di ogni bigrafo in una sua forma normale.

Si rimanda all' appendice A per i dettagli sulla notazione usata.

1.4.1 Placing elementari

Definizione 10 (Placing, Permutazioni, Merge). *Un bigrafo senza nodi e senza link viene detto placing (\emptyset). Un placing che è biiettivo dai siti alle radici è detto permutazione (π). Un placing sono una radice e n siti è denotata da $merge_n$.*

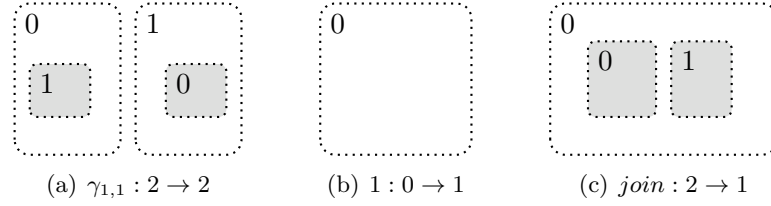


Figura 1.9: Placing elementari.

Un placing ha quindi solo siti e radici.

Il risultato importante è che si può ottenere qualsiasi *placing* dai tre *placing elementari* di figura 1.9, tramite le operazioni di composizione, identità e prodotto. In particolare:

- ogni permutazione π può essere ottenuta dalla simmetria elementare $\gamma_{1,1}$. Per esempio, se si vuole ottenere la permutazione di ordine 3 (π_3), allora si può scrivere la seguente equazione: $\pi_3 = (\gamma_{1,1} \circ \gamma_{1,1}) \otimes id_1$.
- ogni placing \emptyset (e quindi anche ogni merge) può essere ottenuto dai tre placing elementari $\gamma_{1,1}$, 1 e $join$. Per esempio: $merge_0 = 1$ e $merge_{n+1} = join \circ (id_1 \otimes merge_n)$.

1.4.2 Linking elementari

Definizione 11 (Linking, Sostituzioni, Chiusure). *Un bigrafo senza nodi e senza places è detto linking (δ). Una sostituzione (σ) è il prodotto tra sostituzioni elementari (??). Una sostituzione biiettiva è detta rinomina (α). Una chiusura è il prodotto tra chiusure elementari(??).*

Un linking ha solo inner names e outer names.

Il risultato importante è che ogni *linking* può essere generato tramite composizione, prodotto e identità a partire dai due *linking elementari* di figura ??: sostituzioni elementari y/X e chiusure elementari $/x : x \rightarrow \varepsilon$.

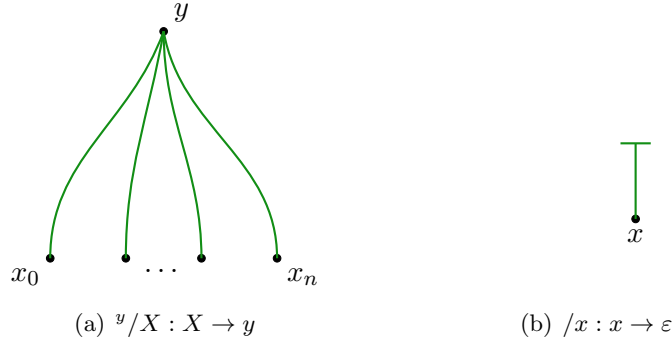
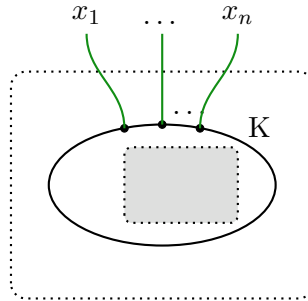


Figura 1.10: Linking elementari.

1.4.3 Ioni

Si descrive un altro tipo di bigrafo base: questa volta esso contiene nodi, a differenza dei placing e dei linking.

Definizione 12 (Ione). *Per ogni controllo $K : n$, il bigrafo $K_{\vec{x}} : 1 \rightarrow \langle 1, \{\vec{x}\} \rangle$ avente un singolo nodo di tipo K le cui porte sono collegate biettivamente con n distinti nomi \vec{x} , è chiamato un ione discreto.*

Figura 1.11: $K_{\vec{x}}$.

Riassumendo, i tre tipi di *bigrafi elementari* sono i placing, i linking e gli ioni. Tramite questi possiamo esprimere algebricamente ogni bigrafo in termini di composizione, prodotto e identità. Per esempio:

- per formare un atomo (vedi definizione 14) usiamo la composizione tra un ione ed un placing (1.12.a).
- per formare una molecola (vedi definizione 15) usiamo anche qui la composizione tra un ione e un bigrafo discreto, ottenuto a sua volta ricorsivamente usando solo placing, linking e ioni (1.12.b).

Definizione 13 (Bigrafo Discreto). *Un bigrafo si dice discreto se non ha link chiusi e la sua link map è biiettiva.*

Definizione 14 (Atomo). *Se il sito di un K -ione viene riempito dal placing $1 : 1 \rightarrow 0$ (vedi 1.9.b), il risultato è un atomo discreto $K_{\vec{x}} \circ 1$.*

Definizione 15 (Molecola). *Se il sito di un K -ione viene riempito da un bigrafo discreto $G : I \rightarrow \langle 1, Y \rangle$, il risultato è una molecola discreta $(K_{\vec{x}} \otimes id_Y) \circ G$.*

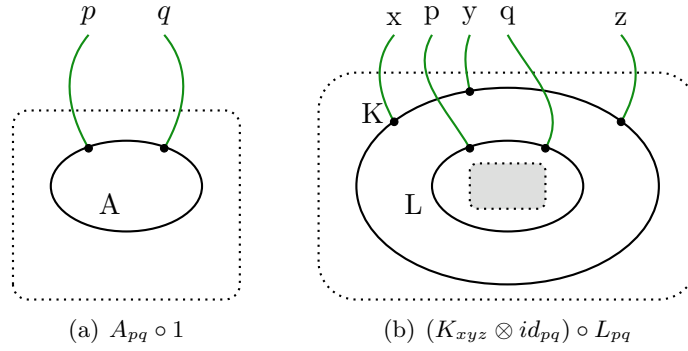


Figura 1.12: Atomo e molecola discreti.

Teorema 1. *Ogni bigrafo può essere costruito a partire da placing elementari, linking elementari e ioni tramite le tre operazioni di composizione, identità e giustapposizione.*

1.4.4 Forma normale discreta

Si è ora arrivati al risultato principale: la scomponibilità di ogni bigrafo in più bigrafi base. Per descrivere questo enunciato, sono necessarie le definizioni di *bigrafo discreto* (definizione 13) e di *bigrafo primo*.

Definizione 16 (Bigrafo primo). *Un bigrafo si dice primo se non ha inner names ed ha un' interfaccia esterna unaria. Esso prende la segue forma: $m \rightarrow \langle X \rangle$.*

Un importante esempio di bigrafo primo è $merge_n : n \rightarrow 1$, dove $n \geq 0$. L'assenza di inner names nei bigrafi primi è fondamentale: essa assicura che ci sia una ed una sola decomposizione di ogni bigrafo in linking e primi discreti, come segue:

Proposizione 1 (Forma normale discreta). *Ogni bigrafo $G : \langle m, X \rangle \rightarrow \langle n, Z \rangle$ può essere espresso univocamente, con al più una rinomina su Y , come:*

$$G = (id_n \otimes \lambda) \circ D$$

dove $\lambda : Y \rightarrow Z$ è un *linking* e $D : \langle m, X \rangle \rightarrow \langle n, Y \rangle$ è un *bigrafo discreto*. Inoltre, ogni *bigrafo discreto* D può essere fattorizzato univocamente, con al più una permutazione dei siti di ogni fattore, come

$$D = \alpha \otimes ((P_0 \otimes \cdots \otimes P_{n-1}) \circ \pi)$$

dove α è una *rinomina*, ogni P_i è *primo e discreto*, e π è una *permutazione di tutti i siti*.

Questa proposizione è cruciale per dimostrare la completezza della teoria algebrica dei bigrafi, che risulta quindi sia corretta che completa.

1.5 Bigraphical Reactive Systems

Uno degli aspetti fondamentali di un bigrafo è la sua capacità di evolversi sulla base di regole ben precise. Un BRS (Bigraphical Reactive System) consente di fare evolvere lo stato di un sistema (bigrafo iniziale) e di dedurre nuove informazioni con specifiche regole di reazione. Un BRS costituisce quindi la *dinamica* dei bigrafi.

La definizione di un BRS richiede prima la definizione di altri concetti, come quello delle *occorrenza* e di *regola di reazione parametrica*.

Definizione 17 (Occorrenza). *Un bigrafo F occorre in un bigrafo G se l'equazione $G = C_1 \circ (F \otimes id_I) \circ C_0$ esiste per qualche interfaccia I e per qualche bigrafo C_0 e C_1 .*

L'identità id_I è importante: consente a C_1 di avere figli in C_0 e in F , e consente a C_0 e C_1 di condividere link che non riguardano F .

Il secondo concetto importante è quello di *regola di reazione*.

Definizione 18 (Regola di reazione). *Una regola di reazione è della forma*

$$R \rightarrow R'$$

dove R si dice essere il *redex della regola*, cioè il *pattern da trovare e cambiare nel bigrafo a cui si applica la regola*, e R' è il *reactum*, cioè il *pattern che andrà a sostituire il redex*.

Redex e reactum sono entrambi bigrafi, e possono occorrere (secondo la definizione 17) nel bigrafo a cui si applica la regola di reazione. Le regole di reazione possono coinvolgere sia il link graph sia il place graph, come si può vedere da questo esempio.

1.5.1 Esempio

Nella figura 1.13, è rappresentato un bigrafo che indica lo stato di un ambiente. Esso è formato da due costruzioni B (buildings), da quattro stanze R (rooms), da cinque agenti A e da quattro computer C. Il bigrafo ha le seguente segnatura: $K = \{A : 2, B : 1, C : 2, R : 0\}$.

Il bigrafo rappresenta lo stato dell' ambiente, in cui i cinque agenti A stanno tenendo una video conferenza: gli agenti che stanno partecipando sono collegati dal link e_0 . Ogni agente che vuole partecipare deve essere collegato ad un computer. A sua volta i vari computer di una stessa costruzione sono collegati insieme, formando una LAN.

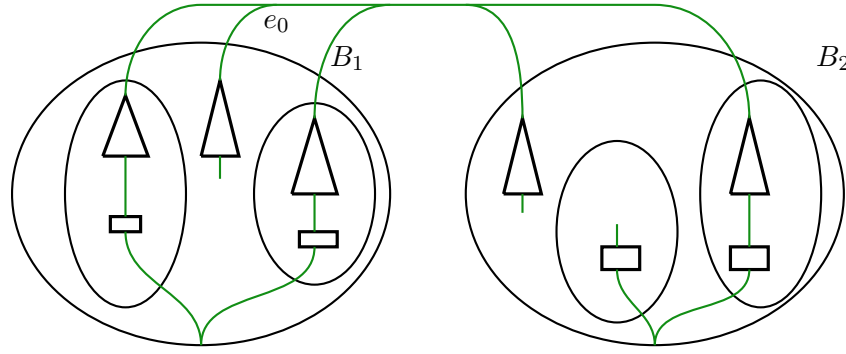


Figura 1.13: Esempio.

Alcune regole di reazione possono essere quelle delle figure 1.14, 1.15, 1.16. Esse agiscono sul bigrafo di partenza (figura 1.13) e sono così definite:

- La prima è la più semplice: un agente può lasciare la video chiamata. Il redex è la parte a sinistra della regola e può matchare qualsiasi agent. I due outernome del redex indicano che le porte dell' agent devono essere collegate (prima dello scatto della regola) a zero o più porte. Se l'agent è collegato ad altri in una videochiamata, egli verrà disconnesso, mantenendo però attivo il collegamento al computer: questa informazione è espressa dal reactum, la parte destra della regola.
- La seconda regola prevede di matchare solo gli agent che non sono collegati a nessun computer e che si trova nella loro stessa stanza. Il reactum prevede che l'agent si ricollegli a un tale computer. Se ci sono più computer nella stanza, la regola non si esprime su quale computer l' agent si debba ricollegare. Si noti

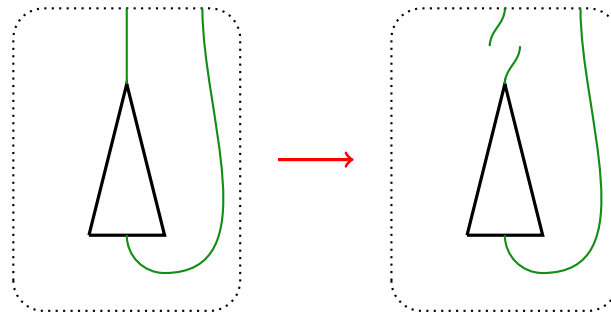


Figura 1.14: Prima regola di reazione

un' importante dettaglio: agent e computer si trovano sotto la stessa radice, e quindi la regola scatta solo se essi si trovano dentro la stessa stanza, o dentro entrambi dentro lo stesso building.

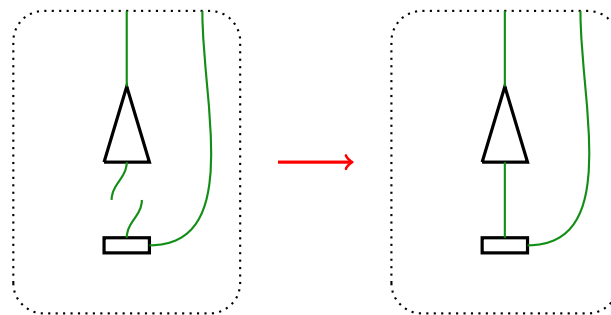


Figura 1.15: Seconda regola di reazione

- Mentre le prime due regole modificavano solamente il link graph, questa terza regola agisce anche sul place graph. Essa prevede lo spostamento di un agent in una stanza. Si noti ancora una volta che l' agent e la stanza si trovano sotto la stessa radice. Questo implica che se assumiamo che ogni stanza sia dentro una costruzione (building), allora questa regola scatta se e solo se l'agent si trova nella stesso building della stanza. In altre parole, non è possibile che un agent fuori da un building entri direttamente in una stanza. Infine, si noti il sito presente sia nel redex che nel reactum: esso rappresenta i parametri della regola. Dentro questo sito ci possono essere altri computer o altri agent. Se si togliesse tale sito dal redex, allora la regola scatterebbe solo se in tale stanza non ci fossero nè computer nè agenti, cioè solo se fosse vuota.

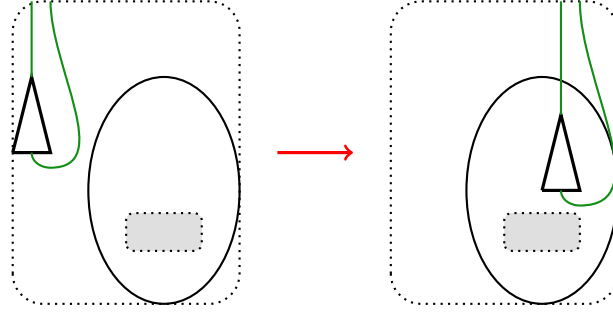


Figura 1.16: Terza regola di reazione

1.5.2 Regole di reazione parametriche

Definizione 19 (Matching). *Il problema di trovare una o più occorrenze di un redex R all'interno di un bigrafo B si chiama matching. Nel caso in cui un match venga trovato, esso viene denotato tramite la seguente equazione:*

$$B = C \circ (R \otimes id_I) \circ D$$

dove C è detto il contesto e D sono i parametri del match.

I bigrafi e la loro teoria ereditano ed estendono molte caratteristiche del CCS (*Calculus of Communicating Systems*). Una di queste è la possibilità di isolare le zone che possono evolversi, cioè determinare quali nodi del bigrafo possono essere soggetti al processo di matching. Introduciamo quindi la nozione di *segnatura dinamica*.

Definizione 20 (Segnatura dinamica). *Una segnatura è dinamica se assegna ad ogni controllo K uno stato nell'insieme $\{\text{attivo}, \text{passivo}\}$. Diciamo che un K -nodo è attivo se il suo controllo è assegnato allo stato attivo; lo stesso vale per lo stato passivo.*

Un bigrafo $G : \langle m, X \rangle \rightarrow \langle n, Y \rangle$ è attivo su $i \in m$ se ogni nodo antenato del sito i è attivo. Un bigrafo G si dice attivo, se è attivo su ogni sito.

Prima di scattare, una regola di reazione necessita del processo di matching, che trova l'occorrenza del redex della regola nel bigrafo. L'occorrenza sarà della forma $B = C \circ (R \otimes id_I) \circ D$. Se il contesto C è attivo, allora la regola scatta, sostituendo l'occorrenza del redex con il reactum. Altrimenti, la regola non scatta. In questo senso si riesce ad isolare parti del sistema che non si vogliono fare evolvere.

Si fornisce ora una definizione precisa di *regola di reazione*. Si tenga a mente l'esempio 1.5.1, in cui si presta particolare attenzione alla sostituzione del redex con il reactum.

Definizione 21 (Regola di reazione). *Una regola di reazione $R \rightarrow R'$, dove il redex R e il reactum R' hanno la stessa interfaccia, è una trasformazione che, se applicata al bigrafo B , produce un nuovo bigrafo B' secondo questa relazione:*

$$B : C \circ (R \otimes id_I) \circ D \quad \rightarrow \quad B' : C \circ (R' \otimes id_I) \circ D$$

dove il contesto C è attivo.

Si noti che questa definizione richiede che R e R' abbiano la stessa interfaccia. Questo è in genere un vincolo troppo forte, che obbliga il progettista a scrivere regole di reazione limitative. Per esempio, non potrei copiare il contenuto, perchè i siti del reactum sarebbero uno in più di quelli del redex, rendendo la loro interfaccia interna diversa. Per indebolire questo vincolo, introduciamo il concetto di *mappa di istanziazione* che porterà al concetto di *regole di reazione parametriche*.

Definizione 22 (Mappa di istanziazione). *Siano $\langle m, X \rangle$ e $\langle m', X \rangle$ le interfacce interne rispettivamente di R e R' . Una mappa di istanziazione è una funzione $\eta : m \rightarrow m'$ che mappa siti di R' in siti di R .*

Definizione 23 (Regola di riscrittura parametrica). *Una regola di reazione parametrica è una tripla della forma:*

$$(R : m \rightarrow I, R' : m' \rightarrow I, \eta)$$

dove R e R' sono rispettivamente il redex e il reactum della regola. Questa volta devono concordare solo sull'interfaccia esterna e sugli inner names.

La regola di reazione parametrica, se applicata al bigrafo B , produce la reazione:

$$B = C \circ (R \otimes id_I) \circ D \quad \rightarrow \quad B' = C \circ (R' \otimes id_I) \circ \bar{\eta}(D)$$

in cui la funzione $\bar{\eta}$ è definita come segue:

sia $g : \langle m, X \rangle$ un bigrafo la cui FND è $g = \lambda \circ (d_0 \otimes \cdots \otimes d_{m-1})$, allora

$$\bar{\eta}(g) = \lambda \circ (d'_0 || \cdots || d'_{m-1})$$

dove $d'_i \simeq d_{\eta(i)}$

1.5.3 BRS

Si sono date tutte le nozioni necessarie per definire formalmente la dinamica di un bigrafo. Essa è costituita da un BRS (*bigraphical reactive system*), che fa evolvere il bigrafo di partenza sulla base di regole ben precise, contenute al suo interno. Ogni BRS è costituito da una segnatura e da un insieme di regole: risulta quindi essere un sistema deduttivo, perchè composto rispettivamente da sintassi e semantica.

Definizione 24 (BRS). *Un sistema reattivo bigrafico (BRS) è definito attraverso una coppia (K, R) , dove K è una segnatura e R è un insieme di regole di reazione, e si indica con $BG(K, R)$.*

L'insieme delle regole R è chiuso rispetto all'equivalenza sul supporto: se $R \simeq S$ e $R' \simeq S'$ e $(R, R', \eta) \in R$ per un certo η , allora $(S, S', \eta) \in R$.

Si indichi ora con $B \rightarrow *B'$ il fatto che il bigrafo B' sia raggiungibile da B con zero o più regole di reazione. Si dimostra che, dato un bigrafo B la cui segnatura è K , il BRS denotato da $BG(K, R)$ computa ogni bigrafo B' tale che $B \rightarrow *B'$. Se si considerano quindi tutti i possibili B' , si ha l'insieme di tutti i possibili stati in cui il sistema B può evolversi secondo le regole R .

1.5.4 Esempio

Vediamo ora un ultimo esempio, in cui si useranno le regole di reazione parametriche. Si vuole rappresentare l'operazione di moltiplicazione tramite i bigrafi. Incominciamo con la segnatura: ci sono tre controlli

- *Mul*, che rappresenta l'operazione di moltiplicazione. Ha arietà 0. Attivo.
- *Num*, che rappresenta il numero, anch'esso 0 porte. Passivo.
- *One*, rappresenta l'unità, con arietà 0. Passivo.

L'idea principale è che il nodo *mul* contiene due numeri, cioè due nodi *num*, che saranno quelli che dovranno essere moltiplicati. Si può anche optare per una versione ricorsiva, permettendo al nodo *mul* di contenere anche altri nodi *mul*. Infine, ogni numero è rappresentato come unione di varie unità. Per esempio, il numero 4 verrà rappresentato tramite il nodo *num* contenente quattro nodi *one*.

Se vogliamo operare la moltiplicazione fra 4 e 2, allora il bigrafo equivalente sarà quello di figura 1.17.

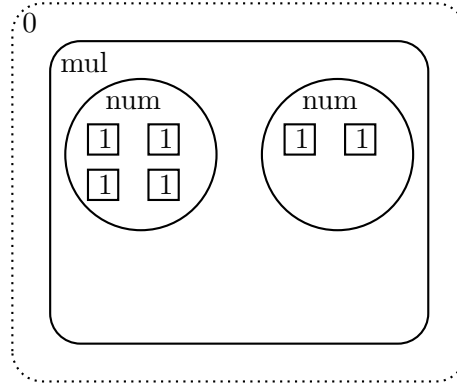


Figura 1.17: Moltiplicazione tramite bigrafi

Per eseguire la moltiplicazione si usano solamente due regole di reazione, ma in maniera *ricorsiva*. Esse ricalcano nel formalismo dei bigrafi questa semplice operazione: $a * b = (a - 1) * b + b$. Distinguiamo quindi fra caso ricorsivo e caso base.

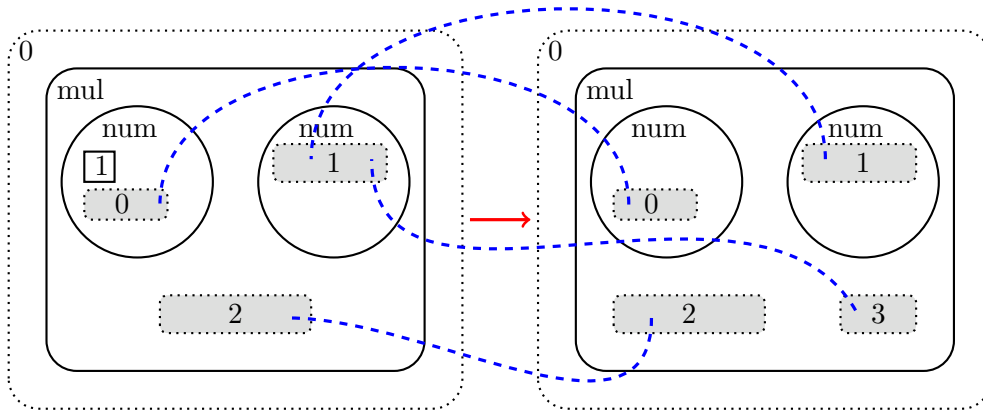


Figura 1.18: Caso ricorsivo

La regola del caso ricorsivo mette bene in evidenza l'importanza delle regole parametriche. Un sito del redex (1) viene copiato in una regione diversa, cioè dentro *mul*. Questo ci consente di *copiare* tutto il contenuto del secondo nodo *num* dentro il nodo *mul*. Infatti, il contenuto di *mul* al di fuori dei nodi *num* rappresenta la somma (+*b*) dell'uguaglianza $a * b = (a - 1) * b + b$.

Si noti che questa regola va applicata ricorsivamente fino a quando il primo nodo *num* ha contenuto vuoto, cioè fino a quando il caso base è applicabile.

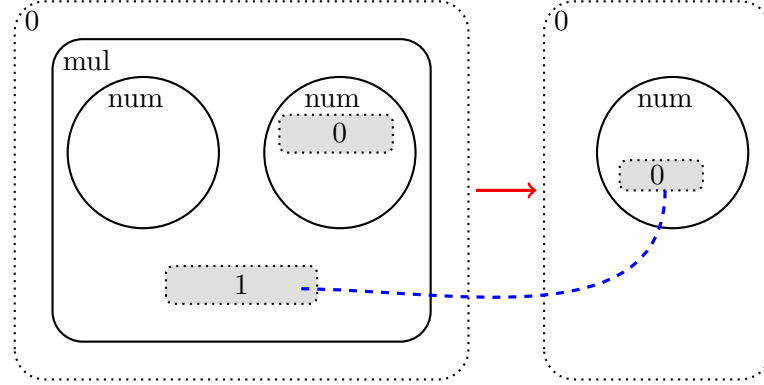


Figura 1.19: Caso Base

Il caso base copia il contenuto di *mul* dentro un nuovo nodo *num*, che rappresenta il risultato della moltiplicazione. Nell'aritmetica classica, per risolvere ricorsivamente la moltiplicazione $2 * 4$ si operano questi passi:

$$\begin{aligned}
 result &= 4 * 2 = (4 - 1) * 2 + 2 = 3 * 2 + 2 && \text{(caso ricorsivo)} \\
 3 * 2 &= (3 - 1) * 2 + 2 = 2 * 2 + 2 && \text{(caso ricorsivo)} \\
 2 * 2 &= (2 - 1) * 2 + 2 = 1 * 2 + 2 && \text{(caso ricorsivo)} \\
 1 * 2 &= (1 - 1) * 2 + 2 = 0 * 2 + 2 = 2 && \text{(caso base)}
 \end{aligned}$$

Seguendo la catena di uguaglianze, si trova che il risultato finale della moltiplicazione è:

$$result = 4 * 2 = (((0 * 2 + 2) + 2) + 2) + 2 = 2 + 2 + 2 + 2 = 8.$$

Vediamo ora l'applicazione della prima regola ricorsiva sul bigrafo di partenza (figura 1.17). La prima operazione da eseguire è trovare l'occorrenza del redex nel bigrafo, che formalmente significa rispettare l'equazione $B = C \circ (R \otimes id_I) \circ D$, dove C è il contesto, R è il redex e D sono i parametri. Dato che tutti e tre sono bigrafi, possiamo disegnarli, come è stato fatto in figura 1.20.

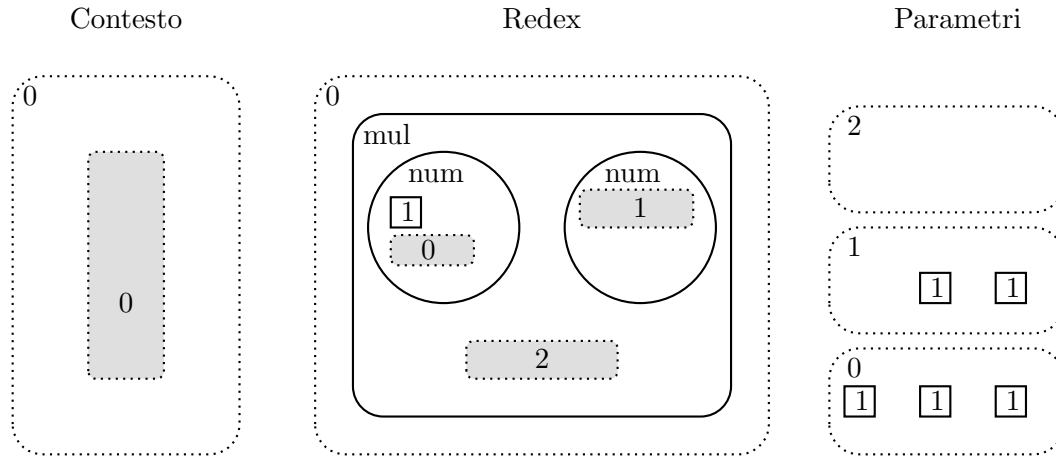


Figura 1.20: Match decomposto

Il bigrafo finale, dopo 3 applicazioni della regola ricorsiva ed una della regola base, sarà quello di figura 1.21.

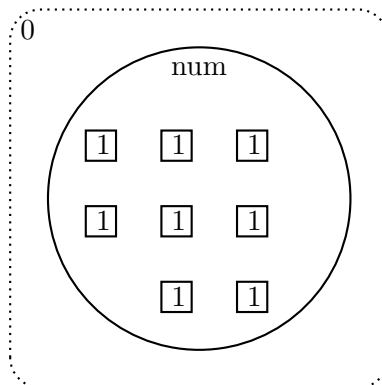


Figura 1.21: Bigrafo finale

L'implementazione di questo esempio si può trovare in ??.

Questo esempio mostra bene come le regole di reazione che formano il BRS rappresentano la semantica del sistema. Per evitare di sprecare memoria sul calcolatore, è necessario progettare con cura la signature e l'insieme di regole del BRS. Nell'esempio di cui sopra, le regole erano soltanto due e potevano essere applicate ricorsivamente. Questo è preferibile ad avere k regole e applicarle una dopo l'altra, appunto a causa dello spreco di memoria che si otterrebbe.

Isomorfismo tra bigrafi

Si è visto nel precedente capitolo come un bigrafo sia capace di evolversi all'interno di un BRS. In alcune situazioni, si vuole evitare evoluzioni infinite di un bigrafo, perchè per esempio porterebbero sempre a stati uguali fra di loro.

Per tenere traccia all'istante t_k di tutti gli stati precedentemente assunti da un BRS $(t_0 \dots t_{k-1})$, si è costruita una struttura dati a grafo, dove ogni nodo è uno stato, cioè un bigrafo: si chiamerà questo grafo “*grafo degli stati*”. Se un BRS parte dallo stato S_0 , è possibile che dopo K regole di reazione lo stato S_k sia uguale allo stato iniziale S_0 . Questo significa che S_0 e S_k hanno la stessa *semantica*, cioè rappresentano lo stesso stato del sistema. Per cui, nel grafo degli stati, essi dovranno essere lo stesso medesimo nodo.

Questo è equivalente a scrivere: “se lo stato S_k è stato ottenuto da S_{k-1} tramite la regola R e S_k e S_0 sono isomorfi, allora da S_{k-1} si ottiene S_0 ”

$$\text{se } S_{k-1} \xrightarrow{R} S_k \text{ e } S_k \simeq S_0 \quad \text{allora } S_{k-1} \xrightarrow{R} S_0$$

Capire quando due bigrafi sono isomorfi e quindi *semanticamente equivalenti* è di fondamentale importanza se si vogliono evitare i così detti *loop* fra regole: per evitare che fra S_i e S_{i+1} si continuino ad applicare sempre le due stesse regole R_1 e R_2 all'infinito, devo capire che:

- da S_i , tramite la regola R_1 , ottengo un bigrafo isomorfo a S_{i+1}
- da S_{i+1} , tramite la regola R_2 , ottengo un bigrafo isomorfo a S_i

Questo concetto verrà chiarito con gli esempi sottostanti.

2.1 Esempio:

Si prenda l'esempio di una rete modellata tramite un bigrafo: si vuole fare in modo che, dato un pacchetto iniziale che ha come mittente l'host A, esso arrivi al destina-

tario B. Ci saranno quindi delle regole di reazione per i router, che permetteranno di inoltrare i pacchetti verso le sue interfacce di uscita. Poichè, utilizzando i soli bigrafi, servirebbero troppe regole di reazione per modellare il fatto che se il destinatario è X allora l'interfaccia di uscita del pacchetto è la numero N, si può pensare di inoltrare il pacchetto verso tutte le uscite in modo non deterministico. Così facendo, il pacchetto arriverà sicuramente al destinatario. I problemi sono ora due:

- il pacchetto arriverà a destinatari non corretti. Si può introdurre una regola di reazione che elimini dall'host ogni pacchetto che non ha come destinatario l'host stesso.
- se prendiamo il k -esimo router R_k , allora il pacchetto ritornerà al $(k-1)$ -esimo router R_{k-1} , che a sua volta lo inoltrerà verso tutte le sue interfacce, e quindi anche nuovamente verso R_k . Si ha così un ciclo infinito di pacchetti tra R_k e R_{k-1} .

In questa sede si tratterà il secondo di questi problemi, che ha un'apparentemente semplice soluzione: capire quando due bigrafi sono uguali. In questo esempio, è facile capire che per risolvere il problema basta verificare se gli stati S_{k+i} e S_{k-1} sono uguali: se S_k è il bigrafo in cui il pacchetto è nel router R_k , allora si applica la regola di inoltro e si generano tanti stati $(S_{k+1} \dots S_{k+j})$ quanti sono i router vicini a R_k ; tra di questi ci sarà anche R_{k-1} . Quindi, se supponiamo che nello stato S_{k+i} il pacchetto torni indietro al router R_{k-1} , allora il problema è capire che S_{k+i} è uguale a S_{k-1} , cioè verificare che i due bigrafi siano isomorfi. In questo modo si sa che dallo stato S_{k-1} non si dovrà più applicare la regola di inoltro verso S_k , perchè questo causerebbe un ciclo infinito.

2.2 Formulazione del problema

Si è visto che il termine isomorfismo ci aiuta a capire quando due bigrafi sono uguali. Riportiamo di nuovo la sua definizione formale (6):

Definizione 25 (Isomorfismo). *Due bigrafi F e G si dicono isomorfi se e solo se esiste una traduzione di supporto tra F e G , cioè se e solo se F e G sono support equivalent ($F \simeq G$).*

Il problema consiste quindi nel trovare una funzione biettiva che ha come dominio i nodi e gli archi del primo bigrafo, come codominio quelli del secondo bigrafo e che

ne rispetti la struttura del primo. Come già visto, tale funzione si chiama *traduzione di supporto*.

Si noti come la traduzione di supporto consenta di ritenere isomorfi due bigrafi che sono uguali *modulo permutazione*: tale funzione può infatti operare una permutazione sui nomi dei nodi e degli archi, così come sugli inner names e outer names. In altre parole, non c'è nessun vincolo sui nomi, ma solo sulla struttura del bigrafo. Si capirà meglio questo concetto negli esempi che seguiranno.

2.3 Strategia di soluzione

Dal punto di vista teorico, si è trattato questo problema come una *rete di flusso*: esse consentono di specificare in modo molto preciso delle condizioni sulla *struttura* dei grafi. Qui l'obiettivo è trovare una traduzione di supporto, che conservi la struttura e sia biettiva: quest'ultima caratteristica per esempio può essere espressa come il fatto che ogni nodo del primo bigrafo deve essere associato ad uno ed un solo nodo del secondo bigrafo. Tramite la rete di flusso, si può specificare questa condizione dicendo che il flusso in uscita da ogni nodo deve essere esattamente 1. Questo è un primo esempio del motivo per cui si è scelta una rete di flusso per la modellizzazione.

Si è scelto di trattare questo problema tramite la programmazione a vincoli. Questo paradigma permette di rappresentare al calcolatore un sistema di equazioni, che esso risolverà. Le equazioni saranno i vincoli che la rete di flusso dovrà rispettare. Nel nostro caso, ci basterà capire se esiste una soluzione al sistema, e non ci interessa sapere quali sono le sue soluzioni. Tutte le equazioni scritte sono lineari, con la conseguenza che si avrà un sistema lineare: questo permette di abbassare la complessità dell'algoritmo.

Si è usata la libreria Java *Choco vs 3.3.1* per esprimere tutti i vincoli.

Si è precedentemente visto che ogni bigrafo è formato da due strutture ortogonali e totalmente indipendenti, il place graph ed il link graph. Il problema dell'isomorfismo verrà quindi trattato separatamente per le due strutture: ci saranno dei vincoli solamente per il place graph, ed altri solamente per il link graph. Infine, gli ultimi vincoli serviranno per conciliare le due soluzioni: si vedrà che senza di questi il calcolatore riconoscerà come uguali due bigrafi che hanno lo stesso link graph e lo stesso place graph modulo permutazione ma che non sono isomorfi (figura 2.2).

La definizione di isomorfismo vista precedentemente può far credere che esso sia un termine puramente sintattico, cioè che riguardi solamente la struttura dei due bigrafi. L'isomorfismo è invece un'operazione che riguarda anche la semantica: due bigrafi strutturalmente uguali sono due bigrafi semanticamente equivalenti (figura 2.1).

2.3.1 Esempi

Non è sempre banale capire quando due bigrafi sono isomorfi. Si forniscono quindi alcuni esempi per acquisire familiarità con questo concetto.

Il primo riprende il bigrafo di figura 1.17 per la moltiplicazione tra numeri naturali. Si vuole mostrare che, semanticamente, l'operazione $2 * 4$ è equivalente all'operazione $4 * 2$. In altre parole, non importa l'ordine dei nodi.

Incominciamo notando che i due link graph sono isomorfi, perchè non hanno archi e presentano lo stesso numero di nodi. Prendiamo ora in esame il place graph: se si ritorna alla sua definizione, si nota subito come i due place graph siano uguali perchè i nodi interni non sono ordinati.

Il fatto di dimostrare che i due bigrafi sono isomorfi e semanticamente equivalenti, dimostra che la proprietà commutativa della moltiplicazione vale anche nella sua versione bigrafica.

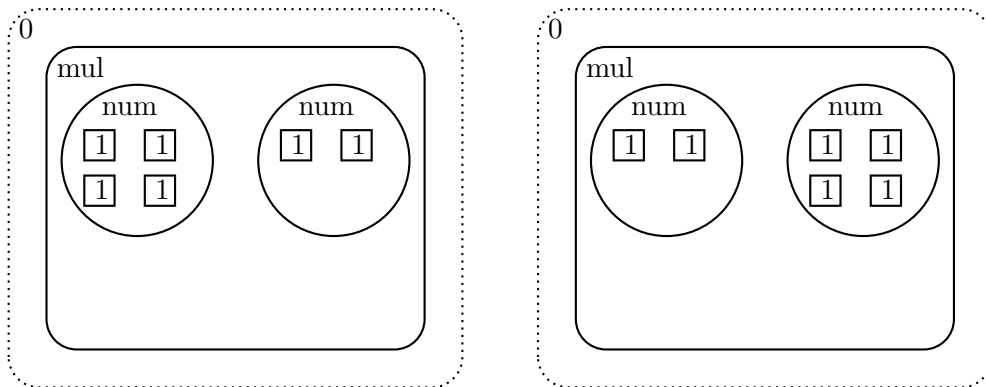


Figura 2.1: Bigrafi Isomorfi: $(4 * 2) = (2 * 4)$

Presentiamo un altro esempio, questa volta su un caso negativo. Si è specificato che per risolvere il problema si trattano separatamente i casi del place graph e del link graph: questo approccio però necessita di avere dei vincoli di “coerenza” che uniscano le due soluzioni. Senza questi vincoli, si può incorrere nel seguente problema.

Si considerino i due bigrafi di figura 2.2 e i loro relativi place graph e link graph (figura 2.3). Si nota subito che i due bigrafi *non* sono isomorfi. Prendendo però i due place graph ci si accerta che essi lo sono. Lo stesso vale per i due link graph: sono entrambi formati da tre nodi, in cui c'è solamente un edge che collega il cerchio ad un quadrato.

I casi separati del link graph e del place graph sembrano quindi suggerire che i due bigrafi siano isomorfi, mentre si vede subito che non è così. Quello che non abbiamo considerato sono appunto i *vincoli di coerenza*, che informalmente dicono che il quadrato collegato al cerchio (nel primo link graph) deve essere quello che contiene un altro quadrato (nel primo place graph). Aggiunta questa condizione, si nota che le due soluzioni sono *incompatibili*, avendo quindi che i due bigrafi *non* sono isomorfi.

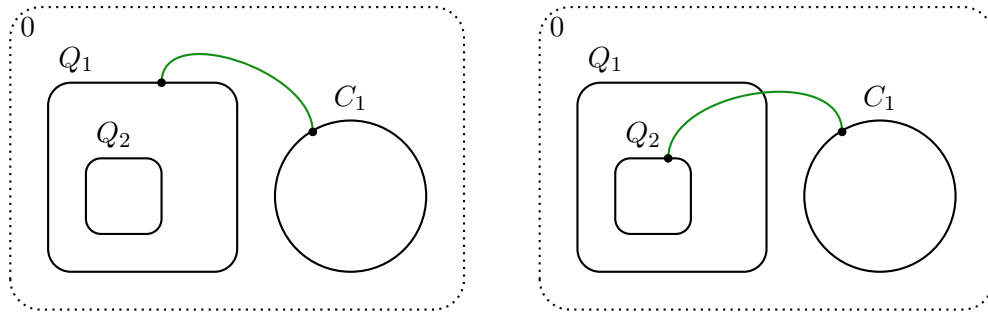


Figura 2.2: Bigrafi non Isomorfi

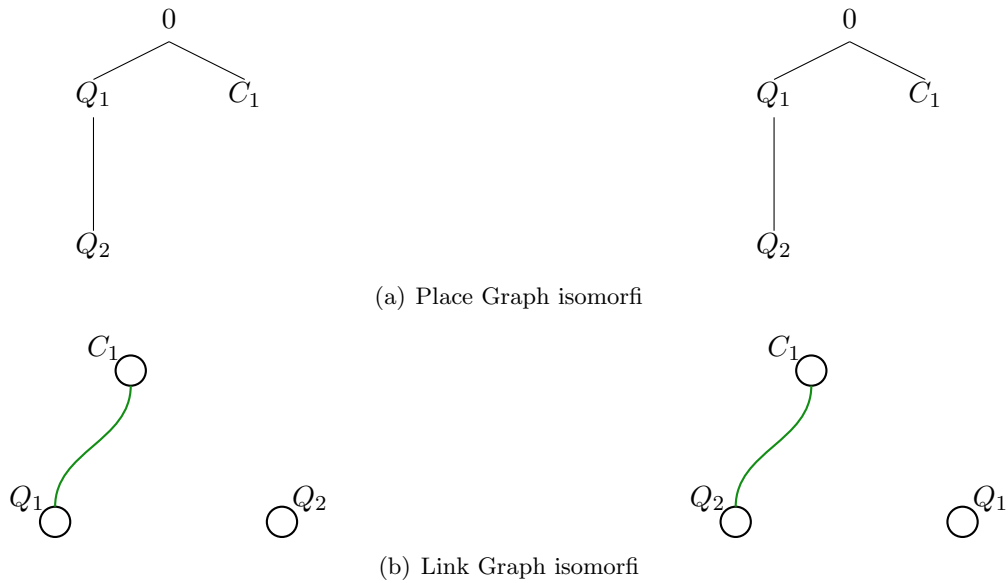


Figura 2.3: Place Graph e Link Graph del bigrafo 2.2

2.4 Vincoli

In questa sezione si presentano le equazioni necessarie per risolvere il problema dell'isomorfismo. Come già anticipato, si lavorerà sulle *reti di flusso*, che sono grafi orientati pesati. Distinguiamo le equazioni per il place graph, per il link graph e per la così detta coerenza.

2.4.1 Vincoli per il place graph

L'isomorfismo tra place graphs è un isomorfismo tra foreste. Si vuole infatti vedere quando la prima foresta è isomorfa alla seconda, a meno di permutazioni delle radici e dei siti. Una rete di flusso per questo problema è quella in figura 2.4.

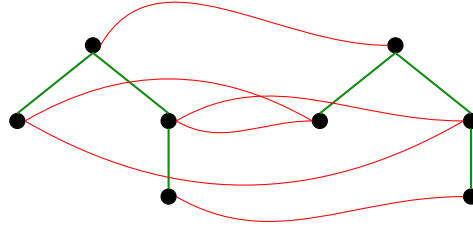


Figura 2.4: Rete di flusso per l'isomorfismo tra place graphs.

Alle due foreste (cioè ai due place graph, costituiti da archi di colore verde), che chiameremo P_F e P_G , si sono aggiunti altri archi (quelli rossi) *solamente* tra nodi della stessa altezza, creando così un grafo. Questa è la vera e propria rete di flusso per il problema dell'isomorfismo tra place graph. Ogni arco rosso è *orientato*, perchè va dai nodi della prima foresta ai nodi della seconda, e *pesato*, perchè gli è assegnato un numero naturale $p \in \{0, 1\}$.

Nell'implementazione, trattata tramite la programmazione a vincoli, ogni arco rosso è una variabile. L'insieme delle variabili per il place graph sarà quindi:

$$M_{d,m,n} \in \{0, 1\} \quad \begin{array}{l} 0 \leq d \leq \text{depth} \\ m \in P_F^d \\ n \in P_G^d \end{array}$$

dove depth è l'altezza massima della prima foresta, e P_F^d e P_G^d indicano l'insieme di nodi/radici/siti che si trovano all'altezza d rispettivamente nel place graph P_F e P_G . In altre parole, creo una variabile che può assumere valore 0 o 1 per ogni coppia di

nodì (a, b) che si trovano sulla stessa altezza, dove a appartiene al primo place graph mentre b al secondo.

I vincoli dovranno essere tali che, dopo l'esecuzione del sistema sul calcolatore, le variabili che assumeranno il valore 1 saranno quelle che *formeranno* la vera e propria traduzione di supporto. Ovvero:

Proposizione 2. *La variabile $M_{d,m,n}$ assumerà il valore 1 se e solo se esiste una traduzione di supporto ρ tale che $\rho(m) = n$.*

Tutte le altre variabili dovranno assumere il valore 0. Un altro modo di vedere la soluzione è questa: la funzione di traduzione di supporto sarà definita da tutte e sole le variabili con valore 1. Infine:

Terminologia. *Quando la variabile $M_{d,m,n} = 1$ diremo che m e n costituiscono un match.*

Nell'esempio di figura 2.4, la soluzione esiste ed è definita come in figura 2.5, dove i numeri sopra le variabili (archi rossi) indicano i valori che esse hanno assunto dopo la risoluzione del sistema di equazioni.

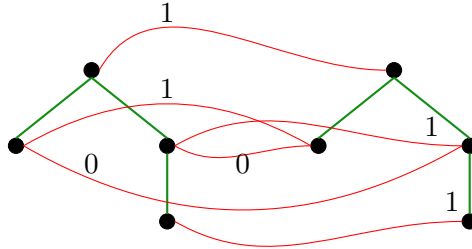


Figura 2.5: Soluzione della rete di flusso

Riassumendo, dobbiamo tradurre in vincoli il fatto che la funzione di traduzione di supporto sia biiettiva e che conservi la struttura del place graph P_F . Distingueremo quindi in vincoli di flusso, che serviranno per il primo problema, e in vincoli strutturali, per il secondo.

Incominciamo con i **vincoli strutturali**: si è adottata una versione ricorsiva per i vincoli. Distinguiamo quindi in caso base e passo ricorsivo.

- *Caso Base*: due nodi della stessa altezza che hanno un numero diverso di figli *non* possono costituire un match. In formule:

$$\begin{aligned}
M_{d,m,n} = 0 \quad & \text{se } |prnt_F^{-1}(m)| \neq |prnt_G^{-1}(n)| \\
& \forall d \leq depth - 1 \\
& \forall m \in P_F^d \text{ e } n \in P_G^d
\end{aligned}$$

Nella figura sottostante, si vede subito che la variabile $M_{0,r_0,r_0} = 0$ perchè $prnt_F^{-1}(r_0) = 1 \neq 2 = prnt_G^{-1}(r_0)$.

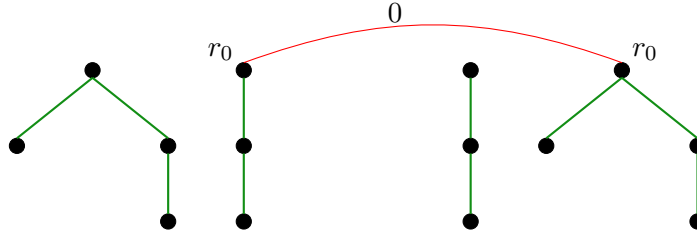


Figura 2.6: Esempio per il primo vincolo

Si noti che questo vincolo viene applicato a tutti i nodi tranne ai siti, come specificato dalla condizione $\forall d \leq depth - 1$.

- *Caso Ricorsivo*: se due nodi alla stessa altezza *non* costituiscono un match, allora neanche i loro figli lo fanno. In formule:

$$\begin{aligned}
M_{d,m,n} \leq M_{d-1,prnt(m),prnt(n)} \quad & \forall d \geq 1 \\
& \forall m \in P_F^d \\
& \forall n \in P_G^d
\end{aligned}$$

Questo vincolo modella la seguente implicazione:

$$M_{d-1,prnt(m),prnt(n)} = 0 \quad \Rightarrow \quad M_{d,m,n} = 0$$

Esso costituisce il caso ricorsivo perchè vale per tutti i nodi tranne le radici, e le radici sono ricoperte dal caso base. Si veda la figura 2.7: la variabile $M_{1,n_1,n_2} = 0$ perchè dalla figura 2.6 sappiamo che $M_{0,r_0,r_0} = 0$ e perchè $prnt_F(n_1) = r_0$ e $prnt_G(n_2) = r_0$. Lo stesso ragionamento vale per la variabile M_{1,n_1,n_3} .

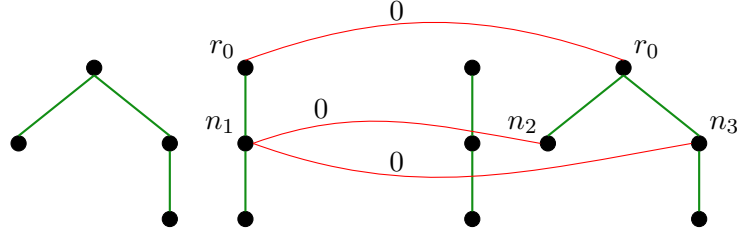


Figura 2.7: Esempio per il secondo vincolo

Questi vincoli non sono però sufficienti per determinare un isomorfismo tra i due place graph P_F e P_G . In particolare, la traduzione di supporto deve essere biettiva, cioè associare un nodo/radice/sito di P_F ad uno ed un solo nodo/radice/sito di P_G . Si sono quindi aggiunti i **vincoli di flusso**.

- *Flusso in uscita*: il flusso totale in uscita da ogni nodo deve essere esattamente pari a 1.

Notazione. Questo vincolo lo indicheremo con la notazione: $\delta^+(m) = 1$, dove $m \in P_F^d$.

Esso si traduce nel fatto che la somma di tutte le variabili in uscita da ogni nodo/radice/sito di P_F deve essere 1, ovvero: ogni nodo di F può costituire un match solamente con uno ed un solo altro nodo di G . In formule:

$$\sum_n M_{d,m,n} = 1 \quad \begin{array}{l} 0 \leq d \leq \text{depth} \\ m \in P_F^d \\ n \in P_G^d \end{array}$$

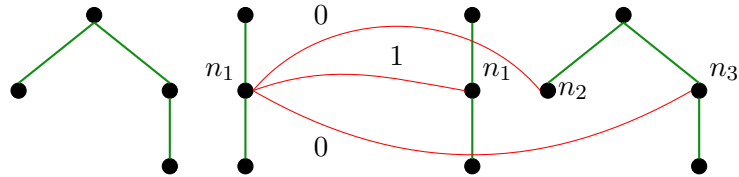


Figura 2.8: Esempio per il vincolo sul flusso in uscita

In figura 2.8 si può vedere come la somma degli archi in uscita dal nodo n_1 sia 1, ovvero: $M_{1,n_1,n_1} + M_{1,n_1,n_2} + M_{1,n_1,n_3} = 1$.

- *Flusso in entrata*: il flusso totale in entrata da ogni nodo deve essere esattamente pari a 1.

Esso è equivalente a dire che la somma di tutte le variabili in entrata da ogni nodo/radice/sito di P_G deve essere 1. In altre parole: ogni nodo di G può costituire un match solamente con uno ed un solo altro nodo di F . In formule:

In figura 2.9, è stato espresso il vincolo che il flusso in entrata verso il nodo n_1 deve essere 1, cioè: $M_{1,n_1,n_1} + M_{1,n_2,n_1} + M_{1,n_3,n_1} = 1$.

2.4.2 Vincoli per il link graph

Sulla base di queste osservazioni, possiamo costruire la *rete di flusso* per questo problema nel seguente modo: innanzitutto chiamiamo i due link graph rispettivamente L_F e L_G , e le loro funzioni come $link_F$ e $link_G$ (definite dagli archi verdi di figura 2.10). Possiamo collegare tutti gli elementi del dominio di $link_F$ a tutti gli elementi del dominio di $link_G$, creando così archi *orientati*, perchè vanno da punti

di L_F a punti di L_G , e *pesati*, perchè possono assumere un valore $p \in \{0, 1\}$. Infine, facciamo lo stesso con i loro Handle: colleghiamo tutti gli elementi del codominio di $link_F$ a tutti gli elementi del codominio di $link_G$.

Si è così creata la rete di flusso in figura 2.10, dove D_X (con $X \in \{F, G\}$) indica il dominio di $link_X$ e C_X il suo codominio.

Per chiarezza visiva, si sono omessi alcuni archi rossi, ma si deve immaginare che ogni elemento di D_F abbiamo tre archi verso ognuno degli elementi di D_G . Lo stesso vale per C_F .

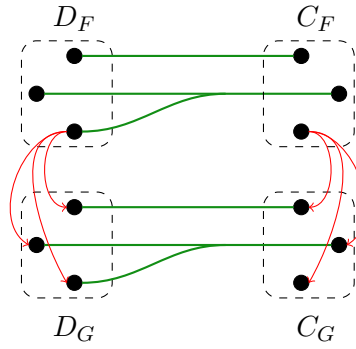


Figura 2.10: Esempio di rete di flusso per il problema di isomorfismo tra link graphs.

Incominciamo quindi con definire le variabili del sistema di equazioni:

$$\begin{aligned} x_{h,h'} &\in \{0, 1\} & h &\in C_F = Y_F \uplus E_F \\ & & h' &\in C_G = Y_G \uplus E_G \\ y_{p,p'} &\in \{0, 1\} & p &\in D_F = X_F \uplus P_F \\ & & p' &\in D_G = X_G \uplus P_G \end{aligned}$$

Si sono distinte le variabili che vanno dal dominio D_F a D_G , che vengono chiamate y , da quelle che vanno dal codominio C_F a C_G , chiamate x . Le soluzioni del sistema hanno lo stesso significato che avevano nel place graph: dopo l'esecuzione, le variabili che assumeranno il valore 1 saranno solamente quelle che costituiranno la vera e propria traduzione di supporto. Quindi, anche per questo problema, valgono la proposizione 2 e la notazione 2.4.1.

I vincoli che si devono scegliere hanno il compito di “costituire” la funzione di traduzione di supporto, e devono quindi assicurare che essa sia biettiva e che mantenga la struttura del primo link graph. Perciò, anche in questo caso, distinguiamo in *vincoli di flusso*, per il primo problema, e in *vincoli strutturali*, per il secondo.

Incominciamo con il definire i **vincoli strutturali**. Essi hanno il compito di definire una funzione che va dal primo link graph al secondo, che sia in grado di mantenere la struttura del primo. In altre parole, devono controllare che le due strutture siano *compatibili*. I vincoli strutturali fanno riferimento al caso negativo, cioè descrivono nel sistema quando due punti o due handle *non* possono costituire un match. Da qui i due vincoli:

- *Primo vincolo strutturale*: due handles (il primo di L_F e il secondo di L_G) che hanno un numero diverso di pre-immagini *non* possono costituire un match. In altre parole: se l'handle h è immagine di due punti ma l'handle h' lo è di uno solo, allora h e h' non possono essere associati. In formule:

$$\begin{aligned} x_{h,h'} &= 0 & |link_F^{-1}(h)| &\neq |link_G^{-1}(h')| \\ h &\in C_F = Y_F \uplus E_F \\ h' &\in C_G = Y_G \uplus E_G \end{aligned}$$

In figura 2.11, si può vedere come la variabile x_{h_3,h_1} sia vincolata ad assumere il valore 0, infatti: $|link_F^{-1}(h_3)| = 0$ ma $|link_G^{-1}(h_1)| = 1$, quindi $x_{h_3,h_1} = 0$.

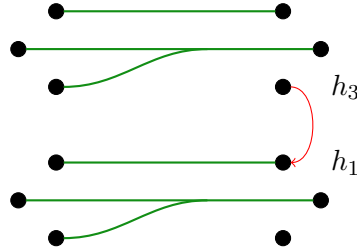


Figura 2.11: Esempio per il primo vincolo.

- *Secondo vincolo strutturale*: se due handles ($h \in C_F$ e $h' \in C_G$) non costituiscono un match, allora neanche i punti che hanno h e h' come immagine lo fanno. Questo vincolo modella la seguente implicazione:

$$x_{h,h'} = 0 \quad \Rightarrow \quad y_{p,p'} = 0$$

dove $p \in link_F^{-1}(h)$ e $p' \in link_G^{-1}(h')$. Esso può essere tradotto tramite la seguente equazione.

$$\begin{aligned} y_{p,p'} &\leq x_{link_F(p),link_G(p')} & p &\in D_F = X_F \uplus P_F \\ & & p' &\in D_G = X_G \uplus P_G \end{aligned}$$

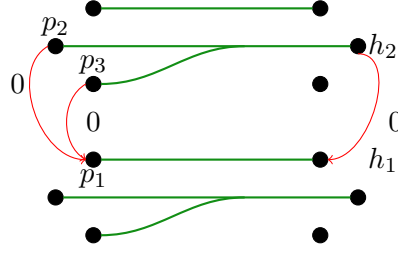


Figura 2.12: Esempio per il secondo vincolo.

Si noti che questa equazione equivale all'implicazione precedente: se $x = 0$, allora deve per forza essere che anche $y = 0$.

In figura 2.12, si può vedere un esempio per questo vincolo. Dal primo vincolo sappiamo che $x_{h_2, h_1} = 0$ perchè $|link_F^{-1}(h_2)| = 2$ mentre $|link_G^{-1}(h_1)| = 1$. Aggiungendo il vincolo appena descritto, ricaviamo quindi che $y_{p_2, p_1} = 0$ e $y_{p_3, p_1} = 0$. Infatti, si vede subito che i punti p_2 e p_3 non possono costituire un match con p_1 .

Descriviamo adesso i **vincoli di flusso**, che consentono di avere una funzione biiettiva. Il caso è analogo a quello per il place graph e la notazione rimane la stessa.

- *Flusso in uscita:*

- $\delta^+(p) = 1$: Dobbiamo assicurare che ogni punto di D_F sia associato ad uno e un solo punto di D_G , che si traduce in questa equazione:

$$\sum_{p'} y_{p, p'} = 1 \quad p \in X_F \uplus P_F \quad p' \in X_G \uplus P_G$$

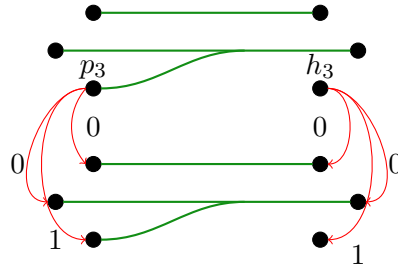


Figura 2.13: Esempio per i due vincoli sul flusso in uscita.

- $\delta^+(h) = 1$: E' l'analogo del caso precedente. Ogni handle di C_F deve essere associato ad uno e un solo handle di C_G . La rispettiva equazione è:

$$\sum_{h'} y_{h,h'} = 1 \quad h \in Y_F \uplus E_F \quad p' \in Y_F \uplus E_F$$

La figura 2.13 mostra un esempio di questi due vincoli.

- *Flusso in entrata:*

- $\delta^-(p') = 1$: ogni punto di D_G può essere associato ad uno e un solo punto di D_F . In formule:

$$\sum_p y_{p,p'} = 1 \quad p \in X_F \uplus P_F \quad p' \in X_G \uplus P_G$$

- $\delta^-(h') = 1$: ogni handle di C_G può essere associato ad uno e un solo handle di C_F . In formule:

$$\sum_h y_{h,h'} = 1 \quad h \in Y_F \uplus E_F \quad p' \in Y_G \uplus E_G$$

La figura 2.14 mostra un esempio per questi due vincoli.

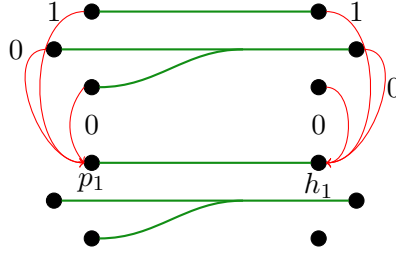


Figura 2.14: Esempio per i due vincoli sul flusso in entrata.

Si noti che i quattro vincoli di flusso assicurano la iniettività e la suriettività della funzione di traduzione di supporto, rendendola quindi *biiettiva*.

2.4.3 Vincoli di coerenza

Nella sottosezione 2.3.1, dedicata ad alcuni esempi, la figura 2.2 mostrava due bigrafi che, pur avendo i place graphs ed i link graphs isomorfi, *non* erano tali. Questo perchè il sistema di equazioni non era completo: non bastano cioè i vincoli visti fino ad ora, e bisogna integrarli con dei **vincoli di coerenza** che sono dedicati all'unione delle due soluzioni.

Nell'esempio citato, si era già notato informalmente che il quadrato collegato al cerchio nel primo link graph deve essere quello più esterno nel primo place graph. Diamo ora le definizioni formali di questi vincoli:

- *Primo vincolo di coerenza*: due porte costituiscono un match nei due link graphs *se e solo se* i rispettivi nodi lo fanno nei due place graphs e le due porte hanno lo stesso indice. In formule:

$$\begin{aligned}
 y_{p,p'} &= M_{d,m,m'} & p &= (m, i) & p' &= (m', i) \\
 & & p &\in P_F & p' &\in P_G \\
 & & m &\in V_F & m' &\in V_G \\
 & & i &\in \mathbb{N}
 \end{aligned}$$

In altre parole, se due nodi m e m' non costituiscono un match nei due place graphs, allora neanche le loro porte lo fanno. D'altra parte, se m e m' costituiscono un match, cioè $M_{d,m,m'} = 1$, allora le porte con lo stesso indice devono costituire un match: $y_{p,p'} = 1$.

- *Secondo vincolo di coerenza*: due porte con indici diversi non possono costituire un match. In formule:

$$\begin{aligned}
 y_{p,p'} &= 0 & p &= (m, i) & p' &= (m', i) \\
 & & p &\in P_F & p' &\in P_G \\
 & & m &\in V_F & m' &\in V_G \\
 & & i, i' &\in \mathbb{N} & i &\neq i'
 \end{aligned}$$

- *Terzo vincolo di coerenza*: se due punti sono di tipo diverso, cioè il primo è una porta e il secondo un inner name, allora essi non possono costituire un match.

$$y_{p,p'} = 0 \quad p \in P_F \quad p' \in X_G$$

Banalmente, vale anche il caso speculare, dove il primo punto è un inner name mentre il secondo è una porta:

$$y_{p,p'} = 0 \quad p \in X_F \quad p' \in P_G$$

- *Quarto vincolo di coerenza*: se due handles sono di tipo diverso, cioè il primo è un arco e il secondo un outername, allora essi non possono costituire un match.

$$y_{h,h'} = 0 \quad h \in E_F \quad h' \in Y_G$$

Il caso speculare, dove il primo handle è un outer name name mentre il secondo è un arco, è dato dalla formula:

$$y_{h,h'} = 0 \quad h \in Y_F \quad h' \in E_G$$

- *Quinto vincolo di coerenza*: un nodo può costituire un match solo con un altro nodo. Lo stesso vale per le radici e per i siti. Perciò, è impossibile per esempio che esista una variabile con valore 1 da una radice verso un nodo. I vincoli che coprono tutti i possibili casi sono:

$$\begin{array}{ll}
 M_{d,a,b} = 0 & \text{se} \quad a \in n \quad b \in V_G \\
 \text{oppure se} & a \in n \quad b \in m \\
 \text{oppure se} & a \in m \quad b \in V_G \\
 \text{oppure se} & a \in m \quad b \in n \\
 \text{oppure se} & a \in V_F \quad b \in m \\
 \text{oppure se} & a \in V_F \quad b \in n
 \end{array}$$

- *Sesto vincolo di coerenza*: due nodi con controlli diversi non possono costituire un match. Per esempio, in figura 2.2 il quadrato più grande del primo bigrafo non può essere associato con il cerchio del secondo.

$$M_{d,a,b} = 0 \quad ctrl_F(a) \neq ctrl_G(b)$$

2.5 Grafo degli stati

Sono stati elencati tutti i vincoli necessari per determinare l'isomorfismo tra bigrafi. Si è già visto che l'utilità di sapere quando due bigrafi sono uguali risiede nel fatto che è possibile fermare l'esecuzione del BRS, evitando così cicli infiniti tra due bigrafi uguali. Per memorizzare tutti gli stati assunti da un BRS durante la sua evoluzione, si è creato il *grafo degli stati*: è una struttura dati a grafo dove ogni nodo è a sua volta un bigrafo.

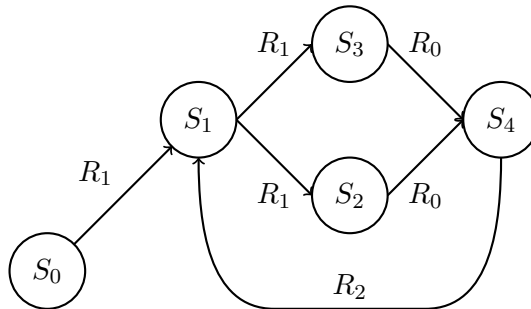


Figura 2.15: Esempio di grafo degli stati.

Come si può vedere dalla figura 2.15, ogni nodo è etichettato con la stringa S_i , perchè si tratta di uno stato, cioè di un bigrafo. All'interno di un BRS, abbiamo visto che un bigrafo può evolversi tramite le regole di reazione, motivo per cui ogni arco orientato del grafo degli stati è etichettato con il nome della regola che ha portato dal primo stato al secondo. Nell'esempio di cui sopra, dal bigrafo iniziale S_0 si passa a S_1 tramite la regola R_1 .

Si noti un aspetto molto importante: da S_0 a S_1 la regola R_1 ha generato un solo nuovo stato. Questo vuol dire che il redex di R_1 ha una sola occorrenza in S_0 , ed essa è stata sostituita dal reactum di R_1 , creando così lo stato S_1 . Però, se prendiamo in considerazione quest'ultimo stato, si vede che ora la regola R_1 porta a due nuovi stati. Questo perchè in S_1 ci sono due occorrenze del redex di R_1 , che vengono sostituite dal suo reactum, creando rispettivamente i due nuovi stati S_2 e S_3 . In altre parole: una regola di reazione può generare un diverso numero di stati a seconda del bigrafo a cui è applicata.

Infine, si presti attenzione all'arco tra S_4 e S_1 . Il significato è il seguente: applico la regola R_2 al bigrafo S_4 , generando un nuovo stato S_5 . Esso è però isomorfo a S_1 , cioè: S_1 e S_5 hanno la stessa *semantica*, per cui collego S_4 a S_1 . Se non ci fossimo accorti di questa proprietà, allora avremmo continuato ad applicare le regole R_0 , R_1 e R_2 all'*infinito*, generando sempre nuovi stati, come in figura 2.16. Ora invece, dato che ci siamo accorti che da S_4 siamo ritornati ad S_1 , non applichiamo più nessuna regola, avendo quindi un grafo degli stati *finito*, cioè quello di figura 2.15.

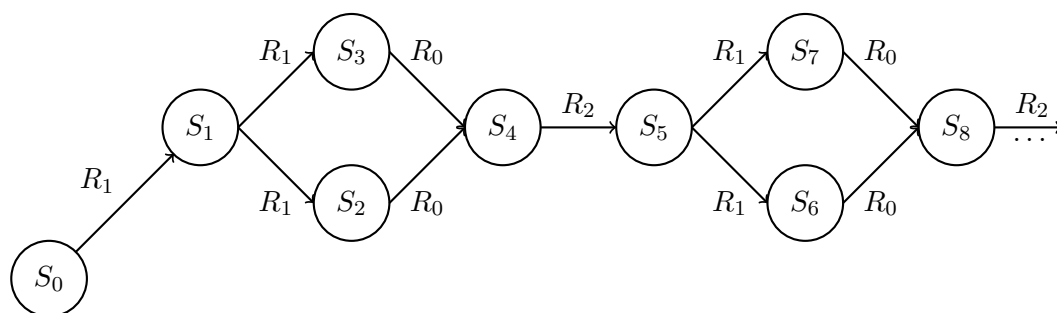


Figura 2.16: Grafo degli stati infinito.

2.5.1 Esempio

In questa sottosezione, viene fornito un esempio concreto di grafo degli stati, con particolare attenzione al problema dell'evoluzione infinita. Si riprende l'esempio della rete della sottosezione 2.5.1. L'implementazione la si può trovare in [...].

Si introduce solo la segnatura del pacchetto, del router e del dominio: $K = \{\text{pacchetto} : 2, \text{router} : 2, \text{dominio} : 0\}$. Chiameremo rispettivamente *Encap* e *Decap* le regole per l'incapsulamento e il decapsulamento dei pacchetto nei vari strati, per esempio da Http a Tcp, o da Ip a Ethernet. Ci concentriamo sulla regola di inoltra tra router, che è quella in figura 2.17.

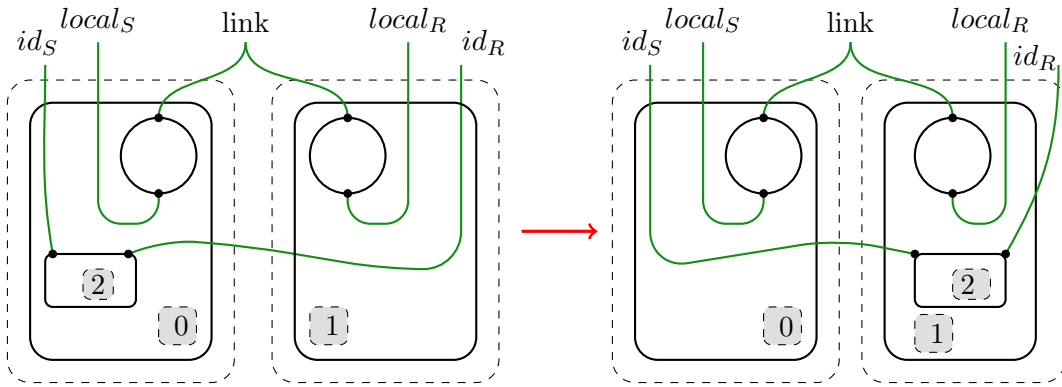


Figura 2.17: Regola di inoltra tra router.

La regola è molto semplice. Innanzitutto, incominciamo con i vari controlli. Figli diretti delle due radici sono i due rettangoli: essi sono i domini di cui fanno parte i due router. Questi ultimi, a loro volta, sono disegnati come circonferenze con due porte: la prima collegata a “*link*” e la seconda a “*Local*”. Infine, il pacchetto è rappresentato da un rettangolo, anch’esso con due porte: la prima, che è quella più a sinistra, è collegata al mittente, mentre la seconda al destinatario.

Passiamo ora a definire il ruolo degli outername. “*Link*” è l’outernome dedicato alla connessione tra router: se un terzo router volesse collegarsi a questi due, allora dovrebbe collegare (nel vero senso della parola) la sua porta superiore con l’outernome “*link*”. Si ricordi quanto detto nella sottosezione 2.5.1: i router inoltrano non deterministicamente ogni pacchetto verso tutte le sue interfacce. Se tre router sono collegati all’outernome “*link*”, allora uno di questi inoltra il pacchetto verso tutti gli altri due. Per cui “*link*” rappresenta l’insieme di tutte le interfacce di un router.

Gli outernome “*Local_S*” e “*Local_R*” sono a disposizione solamente per gli host del dominio corrente. Per esempio, a “*Local_S*” (che sta per *Local Sender*) si possono

collegare solo gli host del dominio in cui si trova il primo router. Nella regola di figura 2.17, questi host vengono inglobati dal sito numero 0. Il medesimo discorso vale per “ $Local_R$ ”.

Il pacchetto è collegato a due outername. Il primo, quello più a sinistra, è “ id_S ” ($id\ Sender$), mentre il secondo è “ id_R ” ($id\ Receiver$). Nella realtà, questi due outername saranno gli identificativi del mittente e del destinatario. Se per esempio il pacchetto in questione è IP, allora id_S sarà l’indirizzo IP del mittente, mentre id_R quello del destinatario.

Infine, si noti anche il sito numero 2: si trova dentro il pacchetto e permette di astrarre al tipo di pacchetto. Per esempio: se è un pacchetto IP, allora è probabile che abbia incapsulato al suo interno un pacchetto TCP, che a sua volta contiene un pacchetto HTTP. Onde evitare di scrivere regole ad hoc per ogni tipo di pacchetto, si introduce il sito numero 2, così che la regola trovi un’occorrenza (e quindi scatti) per qualsiasi tipo di pacchetto.

Vediamo ora un esempio reale, proposto in figura 2.18. Siano D_S e D_R i domini rispettivamente del mittente (sender) e del destinatario (receiver). Indicheremo con il triangolo il controllo per un host. Quindi h_1 e h_2 saranno rispettivamente all’interno di D_S e D_R . Lo stesso vale per i router, cioè R_S e R_R . Supponiamo che il pacchetto sia di tipo IP, e che h_1 sia collegato per esempio a 158.110.3.46, e h_2 a 158.110.144.31. Infine, per quanto detto prima a proposito di “ $Local_S$ ” e “ $Local_R$ ”, alla porta inferiore di R_S si collegherà h_1 , mentre a quella di R_R si collegherà id_2 .

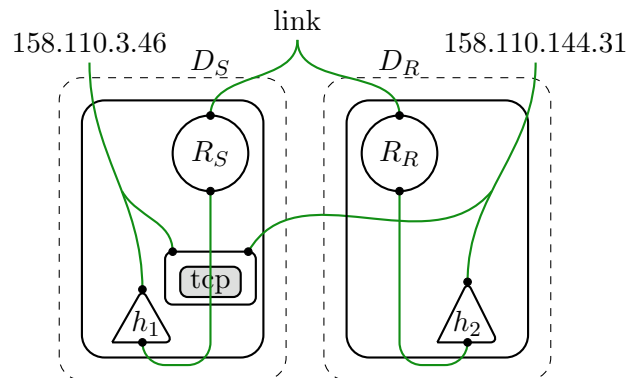


Figura 2.18: Bigrafo di partenza

Chiamiamo il bigrafo della figura 2.18 come S_0 , cioè lo stato iniziale del grafo degli stati. Il nostro BRS è formato da una sola regola, cioè quella di figura 2.17, che chiameremo R_0 . Si noti come il redex di R_0 trovi una ed una sola occorrenza in S_0 , e quindi genererà un solo stato, ovvero S_1 , dove il pacchetto si è spostato in

D_R , arrivando a destinazione. Si può vedere questo risultato nel bigrafo di figura 2.19, che sarà quindi S_1 .

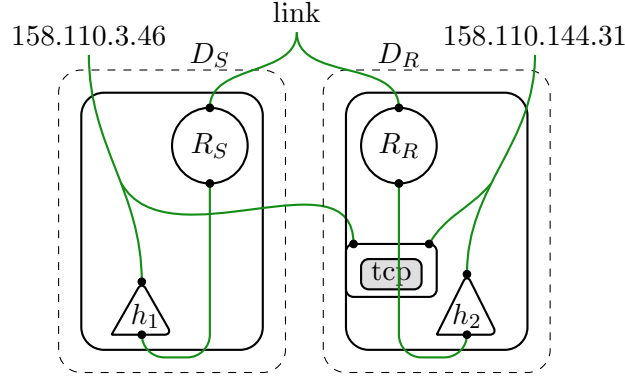


Figura 2.19: Bigrafo dopo l'applicazione della regola R_0

Di per sè, il BRS si dimentica degli stati precedenti, in questo caso S_0 . Per cui, da S_1 scatterebbe di nuovo la regola R_0 , creando lo stato S_2 . A sua volta, da S_2 , eseguirebbe di nuovo R_0 e causerebbe così un'esecuzione infinita, dando luogo al grafo degli stati in figura 2.20.

Grazie all'isomorfismo tra bigrafi, riusciamo a collegare lo stato S_1 a S_0 . Poichè da S_1 tramite la regola R_0 viene creato lo stato S_2 , siamo ora in grado non doverlo più memorizzare, in quanto è uguale (o meglio, è semanticamente equivalente) allo stato S_0 . Per cui, ritrovandoci di nuovo in S_0 , sappiamo che non dobbiamo applicare più nessuna regola, pena un'esecuzione infinita del BRS. Tramite l'isomorfismo, si è potuto generare il *grafo degli stati* della figura 2.21.

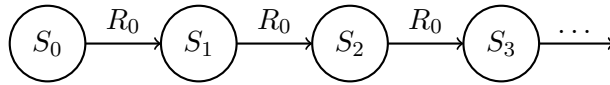


Figura 2.20: Grafo degli stati infinito.

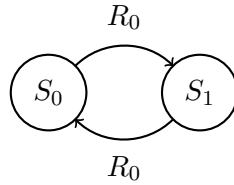


Figura 2.21: Grafo degli stati finito.

2.6 Complessità

Il problema dell'isomorfismo tra bigrafi, come si è visto, è stato affrontato tramite il *constraint programming*. Si è scelta questa tecnica per i seguenti motivi:

- la programmazione a vincoli consente di ridurre notevolmente il tempo di sviluppo dell'algoritmo e il numero di errori.
- il motore che risolve il sistema di equazioni (in questo caso *Choco vs 3.3.1*) è di solito soggetto a molti test, ed è quindi affidabile. C'è anche la possibilità di imporre delle euristiche che migliorano notevolmente le prestazioni, rendendolo quindi anche efficiente.
- il motore può venire considerato come una *black box*, astraendosi quindi alla sua implementazioni interna, che può per esempio venire cambiata o migliorata nel tempo, evitando di affliggere il software che lo usa.

Stabilire la complessità del problema dell'isomorfismo tra bigrafi è molto importante, perchè relazionandolo con altri problemi è possibile trovare un algoritmo efficiente per risolverlo. Facciamo un esempio: ipotizziamo che il problema dell'isomorfismo tra bigrafi (che chiameremo P_{big}) si trovi nella classe C , e che il problema P_c sia *completo* rispetto a questa classe. Per definizione di *completezza*, ogni istanza di ogni problema appartenente alla classe C , quindi anche ogni istanza di P_{big} , può essere tradotta (cioè *ridotta*) con una certa complessità al problema P_c .

L'importanza di questa considerazione risiede in questo fatto: se si riesce a scoprire un algoritmo che operi in tempo polinomiale per risolvere il problema P_c allora tutti i problemi della classe C , incluso P_{big} , sarebbero risolvibili in tempo polinomiale.

Si dimostrerà il seguente risultato:

Teorema 2 (Complessità di P_{big}). *Il problema dell'isomorfismo tra bigrafi è GI-completo.*

Corollario 1. *Il problema dell'isomorfismo tra bigrafi è **equivalente** al problema dell'isomorfismo tra grafi.*

Dimostrazione. *Per dimostrare l'equivalenza, procederemo in due direzioni: nella prima dimostreremo che esiste una riduzione in tempo polinomiale da P_{graph} a P_{big} , cioè che ogni istanza del problema P_{graph} può venire tradotta in un'istanza del*

problema P_{big} . Invece, nella seconda direzione, faremo l'inverso. Si dimostreranno quindi che esistono le seguenti riduzioni:

$$\begin{cases} P_{graph} \leq P_{big} \\ P_{big} \leq P_{graph} \end{cases}$$

- $P_{graph} \leq P_{big}$:

Dando una particolare segnatura al bigrafo, ogni termine del π -Calcolo può essere tradotto in un bigrafo, quindi si ha che ogni istanza del problema π -SC (π Structural Conguence), che controlla quando due termini sono equivalenti, può essere tradotta in tempo polinomiale in un'istanza del problema P_{big} , che controlla quando due bigrafi sono isomorfi. Questa è una Karp-riduzione dal problema P_{π} a P_{big} . In [...] si dimostra che il problema di congruenza tra termini del π -Calcolo, cioè π -SC, è equivalente al problema dell'isomorfismo tra grafi, P_{graph} . Quindi, abbiamo trovato una riduzione che traduce ogni istanza del problema di isomorfismo tra grafi in un'istanza del problema di isomorfismo tra bigrafi.

- $P_{big} \leq P_{graph}$:

Procediamo ora con la seconda parte della dimostrazione: vogliamo dimostrare che ogni istanza del problema P_{graph} può venire tradotta in tempo polinomiale in un'istanza del problema P_{big} . Si è visto nell'introduzione che ogni bigrafo è decomponibile in due strutture tra loro ortogonali (place graph e link graph), e che quindi l'isomorfismo può venire trattato separatamente per i due casi. Trattandosi di grafi, ogni istanza di P_{big} può venire ridotta a due istanze di P_{graph} . Abbiamo quindi trovato una riduzione da P_{big} a P_{graph} .

Si è quindi dimostrata l'equivalenza fra il problema dell'isomorfismo tra bigrafi e quella tra grafi, concludendo quindi che il problema P_{big} è equivalente al problema P_{graph} .

E' noto che P_{graph} appartiene alla classe NP, ma non è ancora stato dimostrato che sia completo. Per qui si è creata una nuova classe di complessità, nota con il nome di GI, che raccoglie tutti i problemi che possono essere ridotti in tempo polinomiale al problema P_{graph} . Quindi si ha che $P_{big} \in GI$.

Come già accennato, l'importanza di trovare la classe di complessità a cui appartiene un dato problema è enorme: se si trovasse un algoritmo che risolve in tempo

polinomiale un problema NP-completo (cioè se la famosa domanda *P is NP?* avesse risposta affermativa), allora tutti i problemi appartenenti alla classe NP, incluso P_{big} , potrebbero essere ridotti in tempo polinomiale al problema NP-completo di cui si ha l'algoritmo polinomiale. In questo modo, anche l'isomorfismo tra bigrafi sarebbe risolvibile in tempo polinomiale.

3

Model Checker per bigrafi

Nel capitolo precedente si è visto come il fatto di poter riconoscere quando due bigrafi sono uguali permetta di poter arrestare l'esecuzione del BRS, evitando sue evoluzioni infinite. In questo capitolo invece si vedrà l'altro principale problema: come poter verificare date proprietà sul BRS. Riprendendo l'esempio della rete, una proprietà che potremmo verificare è l'arrivo a destinazione di un pacchetto, oppure assicurarci che nessun pacchetto non autorizzato passi attraverso un firewall.

Come per l'isomorfismo, anche questo problema necessita di una soluzione generale, che prescinde dal dominio che i bigrafi rappresentano. Si è creata quindi una semplice logica a predicati, con cui è possibile esprimere le proprietà che si vuole verificare. Essa andrà a formare la *politica* per il Model Checker, che servirà a verificare le proprietà sul grafo degli stati visto nel capitolo precedente.

3.1 Model Checker

Un Model Checker (MC) è un metodo per verificare delle proprietà in un sistema formale. Nel nostro caso, si è costruito un MC basato sul grafo degli stati (come quello di figura 3.1): il problema sarà capire se un nodo rispetti le proprietà specificate.

Si è visto come nel *grafo degli stati* ogni nodo sia a sua volta un bigrafo. In figura 3.1 c'è il grafo degli stati dell'esempio 2.5.1 sullo scambio di pacchetti tra due router. Ci possiamo chiedere se in uno dei due nodi il pacchetto sia arrivato a destinazione, cioè se uno dei due stati S_i ($i \in \{0,1\}$) il pacchetto sia nello stesso dominio dell'host destinazione.

Nei MC queste proprietà sono di solito esprimibili attraverso una qualche logica, per cui possiamo esprimere formalmente cosa significa che un MC verifichi una certa proprietà.

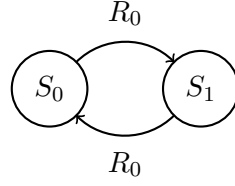


Figura 3.1: Grafo degli stati.

Proposizione 3. *Il problema della verifica di una proprietà da parte di un MC è esprimibile come:*

$$MC, S_0 \models p$$

dove MC è un model checker, S_0 è lo stato iniziale e p è una proprietà espressa in una qualche logica.

Ovviamente, dallo stato S_0 il MC evolverà secondo precise regole per formare tutti i possibili stati $S_0 \dots S_n$: nel nostro caso, ogni arco tra due nodi del *grafo degli stati* è una regola di reazione. Per cui il model checker controllerà l'intero grafo: appena trova uno stato S_i che soddisfa p ($MC, S_i \models p$) ritorna True, altrimenti, cioè nel caso in cui *tutti* gli stati del grafo non rispettino la proprietà, ritorna False.

Queste considerazioni ci portano a definire il comportamento del MC:

Proposizione 4. *Il comportamento di un model checker MC è definito dalla seguente relazione:*

$$\begin{cases} \text{return } True & \text{if } \exists S_i \in MC : MC, S_i \models p \\ \text{return } False & \text{otherwise } (\forall S_i \in MC (MC, S_i \not\models p)) \end{cases}$$

Nell'esempio 3.1, il problema è quindi banale: il model checker ritorna vero se e solo se è vera la formula $MC, S_0 \models p \vee MC, S_1 \models p$.

3.1.1 Generazione degli stati

Si è appena visto che in un model checker si possono esprimere delle proprietà: ogni MC ha però anche un altro grado di libertà, che riguarda la generazione degli stati. Come creare il grafo degli stati? E con che ordine?

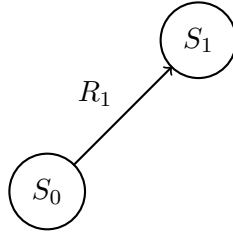
Nel MC costruito per questa tesi, che chiameremo MC_{big} , ci sono varie strategie ed ognuna è adatta per certi scopi. Vediamone alcune:

- *Strategia Breadth First*: per ogni stato S_i vengono generati tutti gli stati possibili adiacenti ad S_i . Per esempio, in figura 3.2, si mostrano i primi tre passi

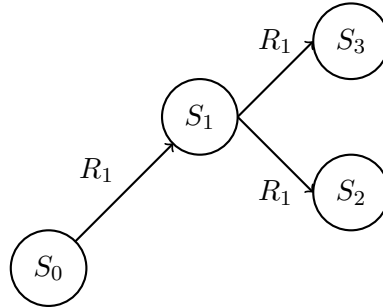
della strategia Breadth First. Il suo vantaggio è che non si tralascia nessuno stato, ottenendo un grafo degli stati *completo*. Inoltre, se un nodo porta ad un vicolo cieco (cioè se non genera nessun bigrafo tramite nessuna regola) allora questo viene semplicemente tolto dalla coda. Lo svantaggio è che può essere molto lenta: se da ogni stato si generano k stati (con k molto alto), allora prima di verificare la proprietà potrebbero volerci molte iterazioni.



(a) Primo passo



(b) Secondo passo



(c) Terzo passo

Figura 3.2: Esempio di generazione Breadth First.

- *Strategia Random*: se dallo stato S_i si possono applicare k regole allora viene scelto in maniera random un numero naturale $m \in \{1 \dots k\}$ e si genera solamente lo stato S_m . Questo consente di non memorizzare l'intero grafo degli stati (che in certi casi può essere molto grande) e verificare al momento della generazione di S_k se $MC, S_k \models p$. Lo svantaggio è quello che l'esecuzione potrebbe andare avanti all'infinito, infatti il grafo *non è completo*. Per cui potenzialmente potrebbero occorrere infinite evoluzioni prima di verificare una proprietà. Un esempio di generazione con la strategia random è quello in figura 3.3.

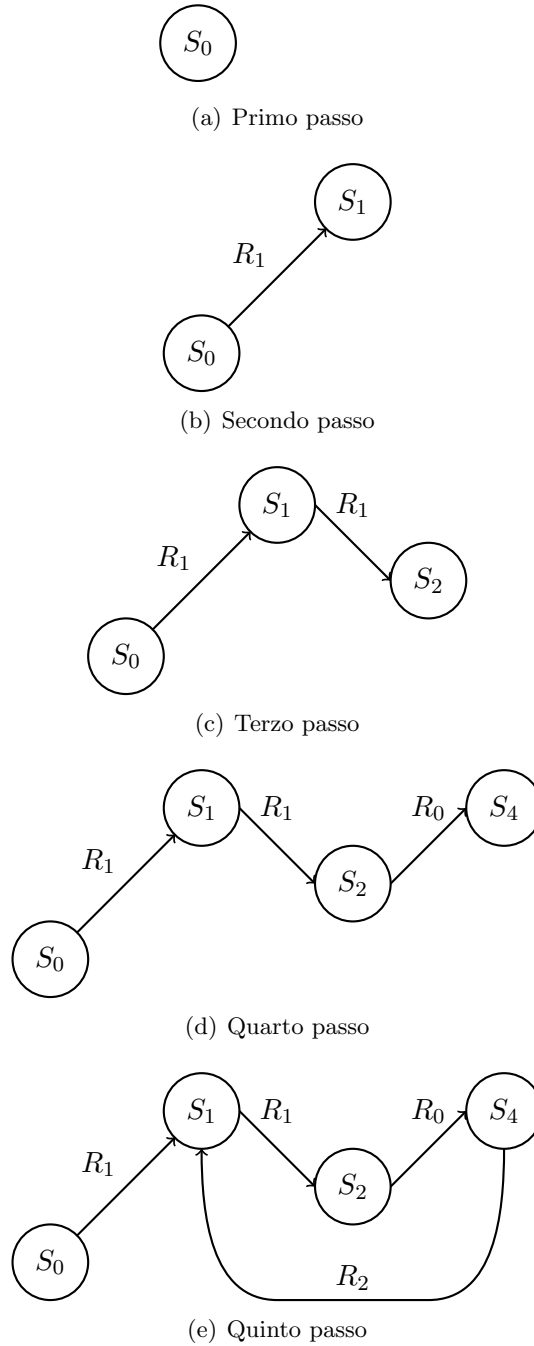


Figura 3.3: Esempio di generazione random.

E' possibile creare altre strategie a seconda degli scopi: in questa sede, se non specificato altrimenti, si assumerà che la strategia sia sempre quella Breadth First, che consente di computare l'intero grafo degli stati.

3.2 Logica per i bigrafi

Nella precedente sezione si è vista la struttura base del model checker per i bigrafi (MC_{big}): il grafo degli stati. L'altro aspetto importante di ogni MC sono le proprietà: necessitiamo quindi di un linguaggio per esprimerle. Il primo problema riscontrato è stato quello riguardante la flessibilità: come fare ad avere un unico linguaggio che astraesce dal dominio scelto e che potesse essere adatto per qualsiasi BRS? In altre parole, è necessario scegliere un linguaggio che sia flessibile e allo stesso tempo espressivo.

La linea guida seguita per la scelta del linguaggio è stata quindi la sua *universalità*. Per esempio: si prendano gli esempi 1.5.4 sulla moltiplicazione e 2.5.1 sulla rete. Sia la proprietà p_1 definita come “Il risultato è il numero 8”. Sia la proprietà p_2 definita come “Il pacchetto è arrivato a destinazione”. Si noti come i domini dei due esempi siano totalmente differenti: il nostro linguaggio deve permettere di esprimere le due proprietà p_1 e p_2 , senza dover ricorrere ad altri formalismi.

Si capisce bene come un tale linguaggio così generale sia molto comodo per esprimere le proprietà da fare verificare al model checker MC_{big} . Infatti, in questo modo si crea uno strumento generale **valido per qualsiasi BRS**.

Si è scelto di usare una logica a predicati, esprimibile attraverso il linguaggio generato da una grammatica *Context Free*.

3.2.1 Sintassi

Incominciamo con il descrivere la sintassi del linguaggio.

Proposizione 5. *Il linguaggio $L(G)$ per il model checker MC_{big} è generato dalla grammatica $G = (V, T, P, S)$, dove:*

- $V = \{\varphi, \sigma\}$ è l'insieme di variabili
- $U = \{T, \wedge, '(', ')', ', ', \neg, W, \pi, A \dots Z\}$ è l'insieme di simboli terminali
- P è l'insieme di produzioni, definito dalle seguenti relazioni:

$$\begin{aligned} \varphi &\rightarrow T \mid \varphi \wedge \varphi \mid \neg \varphi \mid W_{\sigma}(\varphi, \varphi, \varphi) \mid \pi_{\sigma} \\ \sigma &\rightarrow A\sigma \mid \dots \mid Z\sigma \mid \varepsilon \end{aligned}$$

- $S = \{\varphi\}$ è il simbolo iniziale

Il nostro linguaggio sarà quindi definito dall'insieme

$$L(M) = \{w \in U^* : S \Rightarrow_*^G w\}.$$

Seguendo l'usuale definizione di grammatica CF, diamo ora alcuni esempi di stringhe generabili dalla grammatica G , cioè di formule appartenenti al linguaggio $L(G)$:

- $\varphi = W_B(T, T, T) \wedge \pi_C$
- $\varphi = W_B(\pi_X, \pi_Y, \pi_Z)$
- $\varphi = \neg \pi_B \wedge \pi_C$

3.2.2 Semantica

Definiamo ora la semantica del linguaggio, cioè specifichiamo il significato di ogni predicato. Si vedrà che quella presentata è una logica spaziale e non temporale, motivo per cui le proprietà verranno chiamate **proprietà locali**. Spesso nei model checker si usano logiche temporali o spazio-temporali. Nell'implementazione, si è comunque dato spazio a tali logiche, rendendo le classi flessibili. In futuro, sarà quindi possibile aggiungere una nuova logica a MC_{big} .

La semantica è definita come segue (ricordiamo che ogni stato S_i è un bigrafo):

Proposizione 6. *Siano S uno stato e φ una proprietà espressa nel linguaggio $L(G)$. La relazione $S \models \varphi$ (lo stato S soddisfa la proprietà φ) è definita per ricorsione sulla complessità di φ :*

- $S \models T$ sempre
- $S \models \varphi_1 \wedge \varphi_2 \Leftrightarrow \begin{cases} S \models \varphi_1 \\ S \models \varphi_2 \end{cases}$
- $S \models \neg \varphi \Leftrightarrow S \not\models \varphi$
- $S \models W_\sigma(\varphi_1, \varphi_2, \varphi_3) \Leftrightarrow \begin{cases} \exists C, D : S = C \circ (\sigma \otimes id_I) \circ D \\ C \models \varphi_1 \quad \sigma \models \varphi_2 \quad D \models \varphi_3 \end{cases}$
- $S \models \pi_\sigma \Leftrightarrow S \simeq \sigma$

Si dirà che la formula φ costituisce la *politica* per il model checker.

Proposizione 7. *Ogni formula del linguaggio $L(G)$ viene chiamata **proprietà locale** perchè deriva da una logica spaziale e quindi può fare riferimento solamente ad aspetti spaziali/locali di un bigrafo.*

Analizziamo ora i vari predicati. I primi tre consentono le usuali operazioni della logica proposizionale, mentre il terzo è un predicato ad-hoc per questa logica: W_σ è detto “Wario Predicate”, e usa l’operazione di Match per controllare le tre proprietà che ha come argomento. Facciamo un esempio: sia $W_B(T, T, T)$ un Wario Predicate. Lo stato S soddisfa questo predicato ($S \models W_B(T, T, T)$) se e solo se esiste un match M di B nel bigrafo S tale che rispetti queste condizioni: il contesto del match M deve soddisfare φ_1 , il redex di M deve soddisfare φ_2 mentre i parametri di M devono soddisfare φ_3 . Poichè $\varphi_1 = \varphi_2 = \varphi_3 = T$, si ha che $S \models W_B(T, T, T)$ se e solo se esiste un match di B in S . Il Wario Predicate consente quindi di isolare contesto, redex e parametri e verificare le proprietà in modo indipendente per ognuno di questi tre bigrafi.

L’ultimo predicato, π_σ , controlla se esiste un isomorfismo tra due bigrafi. Per esempio, lo stato S_i soddisfa il predicato π_A (in formule $S_i \models \pi_A$) se e solo se S_i è isomorfo al bigrafo A , cioè $S_i \simeq A$. Questo predicato è di particolare importanza: esso funge da simbolo di uguaglianza tra bigrafi, rendendo quindi la nostra logica una *logica con uguaglianza*.

Si osservino tutti e cinque i predicati: dai i primi tre è possibile derivare ogni formula della logica proposizionale. Per esempio: se si vuole esprimere la formula $\varphi_1 \vee \varphi_2$, allora si possono usare le leggi di De Morgan e scrivere $\neg(\neg\varphi_1 \wedge \neg\varphi_2)$. Oppure, se si vuole esprimere il falso, basterà la formula $\neg T$. Gli ultimi due predicati sono invece propri dei bigrafi. Si osservi la loro definizione: si può notare che il Wario Predicate fa riferimento alla struttura interna del bigrafo consentendo infinite scomposizioni. Tramite questo predicato posso quindi *isolare* qualsiasi parte del bigrafo ed esprimere proprietà su di essa. Si può pensare alla sua funzionalità in questo modo: W_σ permette di spostarci all’interno del bigrafo, scegliere una sua parte (σ) e verificare se essa soddisfa una certa proprietà. Il predicato π_σ , come abbiamo già notato, ci consente di avere una logica con uguaglianza, permettendo quindi di aumentare la sua espressibilità.

3.3 Dettagli Implementativi

Nel codice sorgente di questa tesi, i bigrafi e i BRS, nonché la loro evoluzione, è stata modellata tramite *JLibbig* [...], una libreria Java che tra le altre cose consente di specificare le varie regole di reazione ed eseguirle sul bigrafo.

3.3.1 Property Matcher

JLibbig mette a disposizione la possibilità di assegnare ad ogni nodo delle proprietà. Per esempio, ai due router dell'esempio 2.5.1 si possono assegnare delle stringhe (in realtà qualsiasi tipo di oggetto) che descrivano il loro nome, per esempio R_S (Router Sender) e R_R (Router Receiver). Inoltre, è possibile estendere la classe *Matcher* e creare il proprio *Matcher* personale: in questa sede, si era interessati a definire un matcher in cui due nodi potessero *costituire* un match se e solo se avessero le stesse proprietà.

Il *Property Matcher* è molto comodo per esprimere le proprietà per il model checker: per esempio, potremmo essere interessati a sapere quando il pacchetto con destinazione 158.110.144.31 arrivi all'host con tale indirizzo IP. Quindi si potrebbe creare un Wario Predicate che consenta di capire quando il pacchetto e il destinatario sono dentro lo stesso dominio. Però, senza il *Property Matcher*, la presenza di più pacchetti creerebbe confusione. Infatti non sapremmo più a quale pacchetto fare riferimento. Essendo interessati *solamente* al pacchetto destinato a 158.110.144.31, ci occorre il *Property Matcher*.

3.3.2 Regole di Reazione con Proprietà

In *JLibbig* le regole di reazione non fanno alcun riferimento alle proprietà, il che significa che dopo l'applicazione di una regola ogni nodo coinvolto (cioè attivo) perde le sue proprietà. Si è creata quindi una classe che ne consenta il *mantenimento* anche dopo lo scatto della regola. Chiaramente, il modo in cui le proprietà si devono conservare è lasciato da definire all'utente, perchè è impossibile definirlo a priori. Per esempio: prendiamo la regola di figura 3.4, che inoltra e duplica un pacchetto.

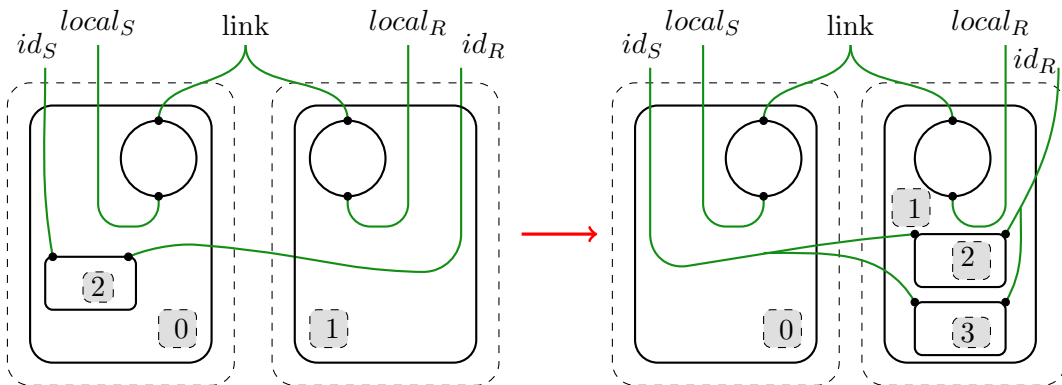


Figura 3.4: Regola di inoltra tra router.

Secondo la definizione di regola di reazione, il redex viene sostituito dal reactum: esso però è un *nuovo* bigrafo e quindi ha nuovi nomi per tutti gli outer e inner names, e tutti i suoi nodi sono privi di proprietà. Supponiamo che prima dell'esecuzione della regola il pacchetto del redex abbia come proprietà la stringa P_1 . Dopo l'esecuzione si vuole che il primo pacchetto del reactum abbia tutte le proprietà di P_1 , mentre il secondo abbia la nuova proprietà *Newpacket*. E' ovvio che tale scelta è arbitraria, ed è questo il motivo per cui la definizione del modo in cui le proprietà si conservano è stata lasciata all'utente.

Infine, creando delle regole di reazione che consentano il mantenimento delle proprietà, è possibile usare il *Property Matcher* anche dopo l'esecuzione di varie regole: di conseguenza lo possiamo usare anche nel model checker MC_{big} .

3.4 Esempi

Si vedranno ora degli esempi di formule e di come poterle usare con il model checker MC_{big} .

3.4.1 Moltiplicazione

Il primo esempio che si propone riprende la moltiplicazione tra numeri naturali della sottosezione 1.5.4. Se rappresentiamo la moltiplicazione $x * y$, ci possiamo chiedere se il BRS funzioni correttamente con le regole che abbiamo definito e verificare che il risultato sia corretto. La proprietà da verificare è quindi questa: “Dati due numeri x e y , il risultato della loro moltiplicazione deve essere il numero $x * y$ ”. Vediamo ora la formula corrispondente: sappiamo che con la segnatura iniziale (vedi 1.5.4) un numero naturale n è rappresentato da un nodo di tipo *num* che contiene n nodi di tipo 1. Per esempio, il numero 8 è il bigrafo di figura 3.5.

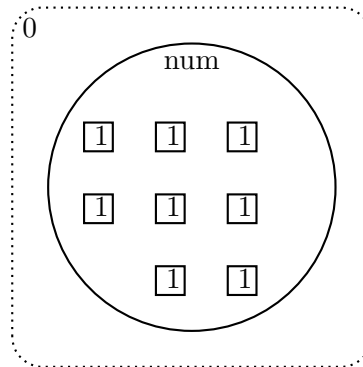


Figura 3.5: Bigrafo per il numero 8

Chiamiamo B il bigrafo di figura 3.5. La proprietà di cui sopra si può esprimere con la seguente formula logica: $\varphi = \pi_B$.

Diamo ora al model checker la formula φ . MC_{big} incomincerà a generare il grafo degli stati con la strategia Breadth First (se non specificato altrimenti), e per ogni nuovo stato S_i controllerà se $MC, S_i \models \varphi$. In questo esempio, il grafo generato sarà quello di figura 3.6. Per gli stati S_0 e S_1 il model checker troverà che la proprietà non è soddisfatta, perchè nessuno di questi stati è isomorfo a B . Arrivando però a S_2 , la proprietà φ sarà soddisfatta, ovvero $MC, S_2 \models \varphi$, e MC_{big} ritornerà True.

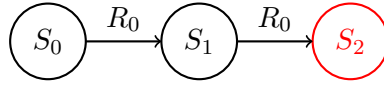


Figura 3.6: Model Checker.

3.4.2 Router

Il secondo esempio riprende quello della sottosezione 2.5.1. Vogliamo modellare una rete con quattro domini, come quella di figura 3.7. L'host h_1 vuole comunicare con h_4 , inviando un pacchetto IP. Tra questi due host ci sono due domini, con due router ciascuno. Prendiamo in considerazione il dominio D_2 : l'arco tra $R_{2.1}$ e $R_{2.2}$ significa che i due router sono collegati e quindi, essendo nello stesso dominio, ogni pacchetto che arriverà a $R_{2.1}$ arriverà anche a $R_{2.1}$.

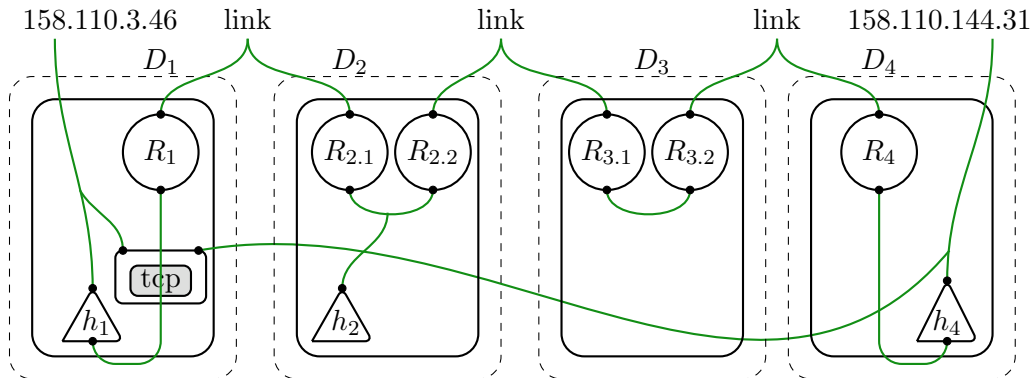


Figura 3.7: Bigrafo di partenza

Si ricordi che un router inoltra non deterministicamente ogni pacchetto verso tutte le uscite (interfacce). Questo permette di creare un compromesso tra numero di regole ed efficienza del BRS. Perciò, l'unica regola di cui abbiamo bisogno è quella di figura 3.8 (si rimanda alla sottosezione 2.5.1 per la sua descrizione).

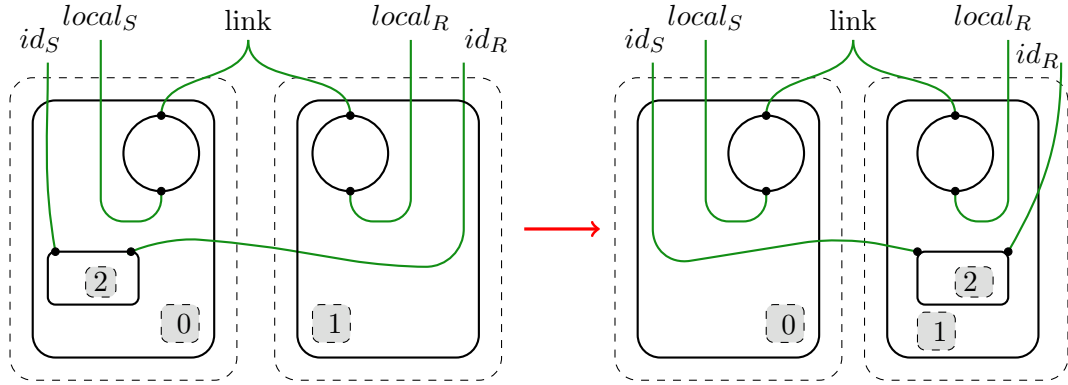


Figura 3.8: Regola di inoltro tra router.

Ora il problema di capire quando un pacchetto è arrivato a destinazione diventa più interessante. Ci sono tre host, e bisogna prestare attenzione a quale sia il corretto destinatario.

Per esempio, non si deve fare il seguente errore: vogliamo esprimere la proprietà “Il pacchetto è arrivato a destinazione”. Nella logica descritta precedentemente, si potrebbe sbagliare e creare una formula del genere: $\varphi = W_B(T, T, T)$, dove B è il bigrafo di figura 3.9.a.

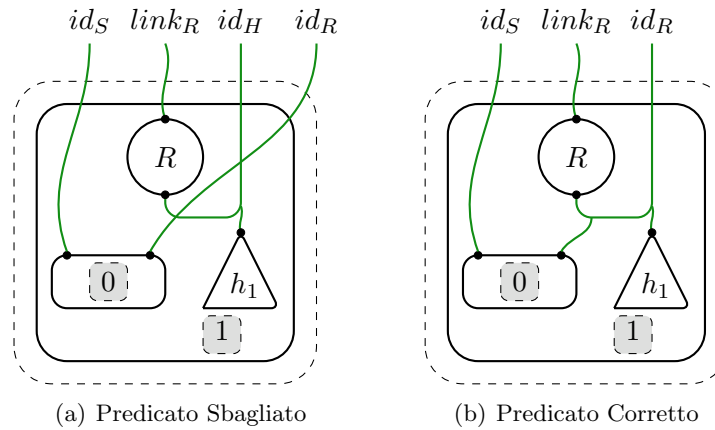


Figura 3.9: Esempi di predicati

Questa proprietà **non** verifica l'arrivo a destinazione di un pacchetto, infatti è soddisfatta anche esso si trova per esempio nel dominio D_2 . Quello che non abbiamo

considerato sono gli outernames: quello del pacchetto e quello dell'host devono essere lo stesso outername; solo così il *Wario Predicate* sarà soddisfatto. Il predicato corretto è quindi quello di figura 3.9.a.

Testiamo ora la formula $\varphi = W_B(T, T, T)$ sul bigrafo di partenza, cioè quello di figura 3.7, che sarà chiamato S_0 . Per prima cosa, il model checker controlla se in questo stato iniziale la formula sia soddisfatta, ovvero se $MC, S_0 \models \varphi$. Non essendo soddisfatta continua. Inizialmente la regola R_0 (in figura 3.8) trova un solo match, per cui il pacchetto viene inoltrato dal dominio D_1 a D_2 , dando origine allo stato S_1 . E' utile guardare il grafo degli stati di figura 3.10 per tenere traccia di tutte le esecuzioni.

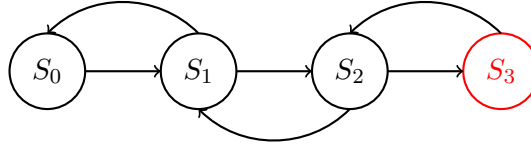


Figura 3.10: Grafo degli stati

In S_1 la formula non è soddisfatta ($MC, S_1 \not\models \varphi$), quindi MC_{big} continua. Dallo stato S_1 , la regola R_0 trova ora due match: il primo coinvolge il router $R_{2,2}$ e manderà il pacchetto nel dominio D_3 , mentre il secondo riguarda il router $R_{2,1}$ e manderà il pacchetto indietro verso D_1 . Quindi il grafo degli stati avrà rispettivamente gli archi: $S_1 \rightarrow S_2$ e $S_1 \rightarrow S_0$. Il model checker ora dovrà duplicare le computazioni, cioè seguire sia il primo che il secondo arco.

Seguendo l'arco $S_1 \rightarrow S_0$, il MC trova il nodo S_0 grazie all'algoritmo per l'isomorfismo e riconosce che appartiene già al grafo degli stati. La computazione di questo ramo **viene interrotta** perchè il model checker capisce che continuando si causerebbe un'esecuzione infinita.

Seguendo l'arco $S_1 \rightarrow S_2$, si genera invece un nuovo stato S_2 . Il model checker cerca in tutto il grafo degli stati un nodo isomorfo a S_2 e, se non lo trova, capisce che esso è un *nuovo* stato. Dato che $MC, S_2 \not\models \varphi$, la computazione di questo ramo quindi continua.

Applicando R_0 a S_2 il discorso è lo stesso: la computazione che segue l'arco $S_2 \rightarrow S_1$ si interrompe, mentre quella che segue $S_2 \rightarrow S_3$ continua. Si noti come la strategia *Breadth First* consenta di interrompere da subito le computazioni che causano cicli infiniti: è uno dei vantaggi di questa strategia.

Infine, lo stato S_3 è il bigrafo in cui il pacchetto è dentro il dominio D_4 . La regola R_0 trova solamente un match, ed eseguendola rimanda il pacchetto indietro verso il dominio D_3 , creando nel grafo degli stati l'arco $S_3 \rightarrow S_2$. Questa volta però lo stato S_3 soddisfa la proprietà desiderata: il model checker trova che

$$MC, S_3 \models W_B(T, T, T) \quad \text{dove } B \text{ è il bigrafo di figura 3.9.b}$$

e quindi ritorna True.

Un'ultima osservazione: nel caso di più pacchetti si deve prestare attenzione ad un altro dettaglio. Se siamo interessati a verificare che il pacchetto spedito da 158.110.3.46 a 158.110.144.31 sia arrivato a destinazione, dobbiamo usare il Property Matcher. Definiremo quindi la formula sempre come $\varphi = W_B(T, T, T)$, ma ora il bigrafo B avrà nomi specifici nei suoi outernames, come in figura 3.11.

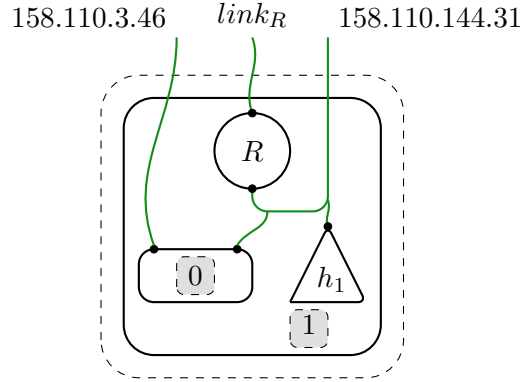


Figura 3.11: Predicato con proprietà

4

Esempi

In questo capitolo vedremo degli esempi che riguarderanno principalmente il model checker MC_{big} e la sua logica. Si cambierà spesso dominio, mostrando come i bigrafi siano flessibili per rappresentare vari tipi di sistema.

4.1 NFA

In questa sezione si propone una codifica in bigrafi degli NFA (*non-deterministic finite automata*). Come noto, ogni automa A denota un linguaggio $L(A)$. Vedremo come l'implementazione di un automa con i bigrafi consenta di avere una sorta di analizzatore lessicale il cui motore interno funziona tramite BRS. In questa sede, si è costruito un modulo che accetta dall'utente una stringa x e restituisce `True` se $x \in L(A)$, altrimenti `False`.

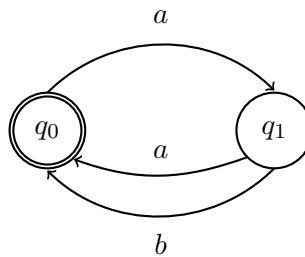


Figura 4.1: Automa per il linguaggio $(a(a + b))^*$

Prendiamo l'automa di figura 4.1, che chiameremo A . Definiamolo formalmente:

Proposizione 8. *L'automa A è una quintupla $(Q, \Sigma, \delta, q_0, F)$, dove:*

- $Q = \{q_0, q_1\}$ è l'insieme finito di stati
- $\Sigma = \{a, b\}$ è l'alfabeto di input
- $\delta : Q \times \Sigma \rightarrow Q$ è la funzione di transizione definita come:

$$\delta(q_0, a) = q_1$$

$$\delta(q_1, a) = q_0$$

$$\delta(q_1, b) = q_0$$

- q_0 è lo stato iniziale
- $F = \{q_0\}$ è l'insieme di stati finali

A riconosce il linguaggio $L(A) = (a(a+b))^*$.

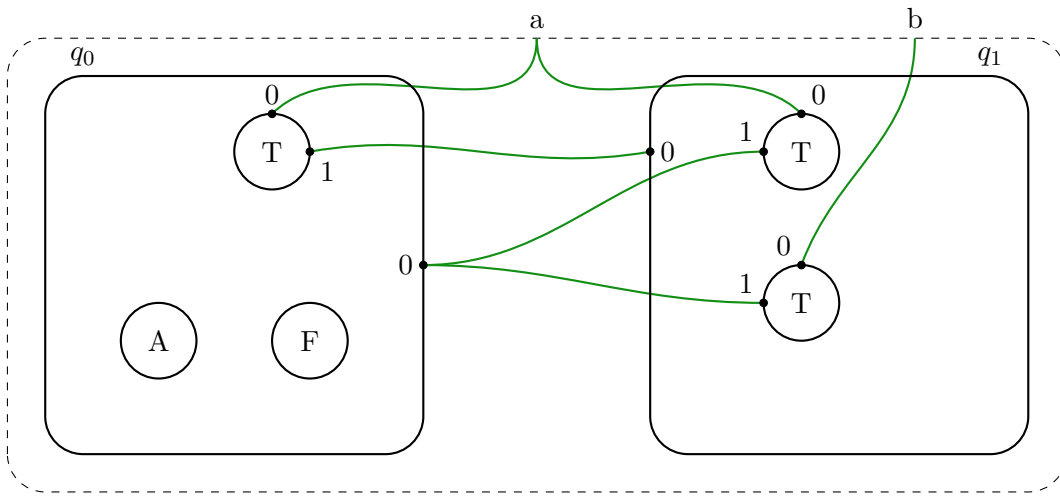


Figura 4.2: Bigrafo per l'automa A

Trattiamo ora il problema di come rappresentare gli automi tramite i bigrafi. Per prima cosa, guardiamo la figura 4.2. I due stati q_0 e q_1 sono stati modellati con dei rettangoli aventi una sola porta. Le transizioni sono i nodi di tipo T. Ogni stato q_i contiene al suo interno tutte le transizioni che partono da esso: per esempio q_0 contiene solo un nodo T perchè la sola transizione che parte da q_0 è $q_0 \xrightarrow{a} q_1$, mentre q_1 contiene due nodi T, che modellano le transizioni $q_1 \xrightarrow{a} q_0$ e $q_1 \xrightarrow{b} q_0$.

Ogni transizione è quindi modellata da un nodo di controllo T con due porte: la prima è collegata al carattere che fa scattare la transizione, mentre la seconda è collegata allo stato destinazione. Nella precedente figura, si prenda in considerazione il nodo T dentro q_0 : esso simboleggia la transizione $q_0 \xrightarrow{a} q_1$ perchè:

- T è dentro q_0
- la prima porta di T è collegata all'outernome 'a'
- la seconda porta di T è collegata a q_1

Lo stesso discorso vale per le altre transizioni. Si noti come l'alfabeto Σ sia rappresentato tramite *l'insieme degli outernames*. Il nodo A (Active) indica che lo stato q_i che lo contiene è quello attivo, ovvero: l'automa si trova nello stato q_i se e solo se q_i contiene il nodo A . Infine, lo stato q_i è uno stato finale ($q_i \in F$) se e solo se contiene al suo interno il nodo di tipo F (Final). Queste considerazioni ci portano a definire la segnatura del bigrafo:

Proposizione 9 (Segnatura per gli NFA). *La segnatura del bigrafo rappresentante un generico NFA è definita come segue, dove la notazione $\text{Node} : n : (\text{active})$ significa che il nodo Node ha n porte ed è attivo, cioè può essere modificato dalle regole di reazione:*

- *State : 1 : passive*
- *Transition : 2 : passive*
- *ActiveState : 0 : active*
- *FinalState : 0 : passive*
- *String : 0 : passive*
- *Input : 3 : active*

Dalla segnatura di sopra si scopre che ci sono due nuovi controlli: *String* e *Input*. Il nodo di tipo *String* è quello che dovrà contenere la stringa che l'utente immetterà per farla riconoscere dall'automa, mentre ogni nodo di tipo *Input* è un carattere della stringa.

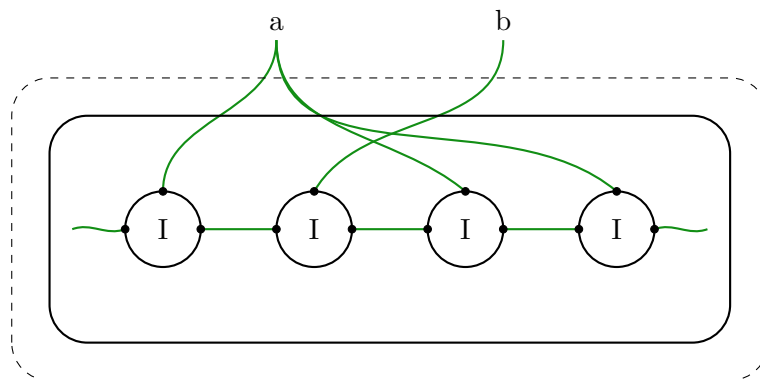


Figura 4.3: Bigrafo per la stringa “abaa”

Si prenda in considerazione la figura 4.3: ogni nodo di tipo *Input* ha tre porte, numerate da sinistra verso destra con 0, 1 e 2. La porta numero 0 è collegata al

carattere precedente: per esempio, il primo carattere a non è collegato a nessun altro nodo. La porta numero 2 è collegata al carattere successivo. Infine la porta numero 1 è collegata alla lettera (che è un outernome) che il carattere simboleggia. Così facendo si crea una *lista* di caratteri che forma la vera e propria stringa. Il nodo di tipo *String* raggruppa tutti questi caratteri al suo interno. Il bigrafo di figura 4.3 rappresenta dunque la stringa “abaa”. Nell’implementazione, si è costruito un modulo che accetta dall’utente una stringa e la trasforma nel bigrafo equivalente, secondo le regole appena citate.

Ora che si è definito come modellare un NFA e una sua stringa, rappresentiamo una istanza del problema. In particolare, costruiamo il bigrafo che ha come NFA l’automa di figura 4.2 e come stringa di input il bigrafo di figura 4.3. Il risultato è il bigrafo di figura 4.4.

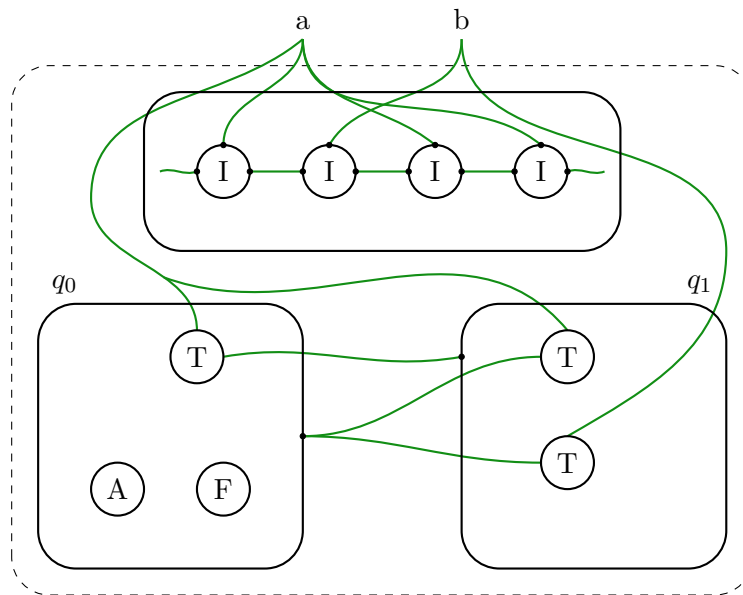
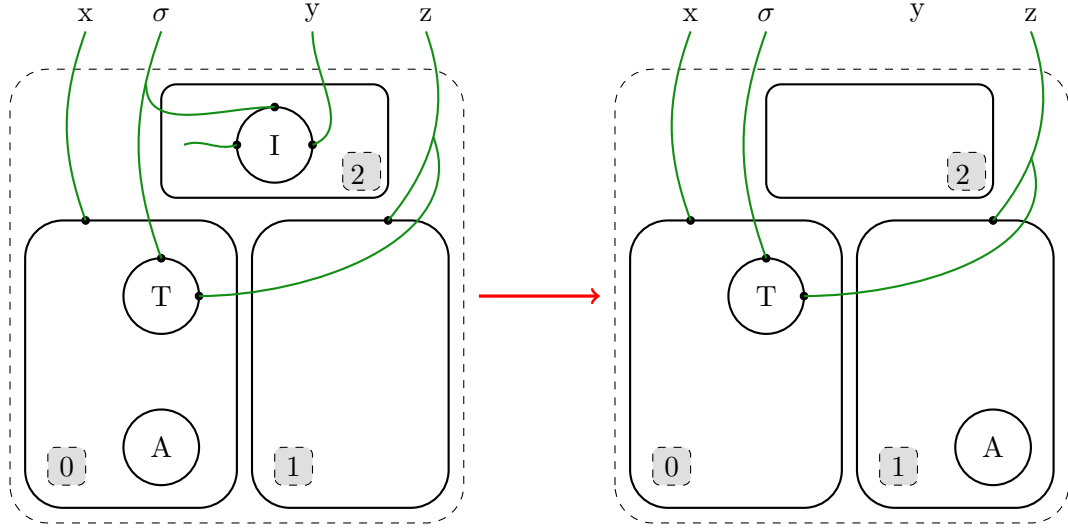


Figura 4.4: Istanza del problema: la stringa “abaa” viene accettata dall’automa A?

Vediamo ora come il bigrafo si può evolvere. L’idea principale è di far “consumare” al sistema un carattere alla volta. Si veda la regola della figura 4.5 che rappresenta la regola di reazione R_0 : se il primo carattere della stringa è la lettera σ e se lo stato attivo possiede una transizione tramite la lettera σ , allora si elimina tale carattere dal bigrafo e si sposta il nodo *Active* nello stato destinazione.

La regola R_0 è molto intuitiva: se per esempio prendiamo in considerazione il bigrafo di figura 4.4, allora applicando la regola si ha che il primo carattere (a) viene eliminato ed il nodo A passa dentro lo stato q_1 . Quindi il BRS per questo problema

Figura 4.5: Regola di reazione R_0

è definito da una sola regola (R_0), che itera finchè trova un match nel bigrafo, cioè si ferma solo quando il nodo di tipo *String* **non** contiene più nessun nodo *Input*.

Ora che abbiamo creato il BRS, è possibile usare il model checker MC_{big} definendo la formula che esso andrà a verificare. Nella teoria degli automi, vale la seguente preposizione:

Proposizione 10. *Una stringa x viene accettata se e solo se alla fine di essa l'automata si trova in uno stato finale.*

Nella nostra segnatura, tutti gli stati finali ($q_F \in F$) vengono distinti tramite un nodo F all'interno di essi: essendo passivi, nessuna regola di reazione può modificarli. Per cui la proprietà da verificare sarà la seguente: “Il nodo di tipo *String* non deve contenere nessun altro nodo e il nodo A e il nodo F si devono trovare dentro lo stesso stato S ”. Nella logica di MC_{big} , questo si traduce nella formula:

$$\varphi = W_B(T, T, T)$$

dove B è il bigrafo di figura 4.6.

Si noti la semplicità di quest'ultima formula: il nodo di tipo *String* deve essere vuoto, il che significa che tutti i caratteri sono stati “consumati” dall'automata. Inoltre, il nodo attivo e il nodo finale si devono trovare nello stesso stato, assicurando che l'automata dopo aver letto tutta la stringa è finito in uno stato finale. Quindi possiamo affermare che:

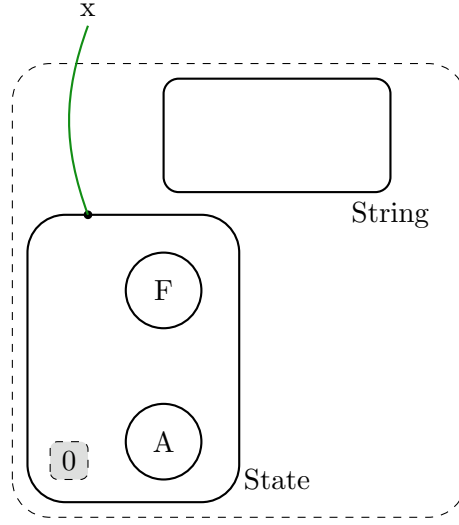


Figura 4.6: Bigrafo B

Proposizione 11. *Una stringa x viene accettata dall'automa A se e solo se $MC, S_i \models \varphi$ per qualche i , dove $\varphi = W_B(T, T, T)$.*

Prendiamo l'istanza del problema in figura 4.4. Seguiremo una traccia d'esecuzione, cioè faremo tutti i passi che fa MC_{big} per verificare la proprietà desiderata. Vedremo come il grafo degli stati sarà molto semplice: questo spesso è un indice di buona progettazione. Vuol dire che il sistema è stato modellato correttamente, scegliendo poche regole ed evitando di costruire regole ad-hoc per casi particolari. Il nostro BRS è formato da una sola regola, il che evita per esempio che in uno stato S_i venga applicata la regola sbagliata creando nodi inutili nel grafo degli stati.

In figura 4.8, c'è la traccia d'esecuzione di MC_{big} , mentre in 4.7 c'è il corrispondente grafo degli stati.

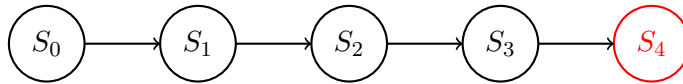


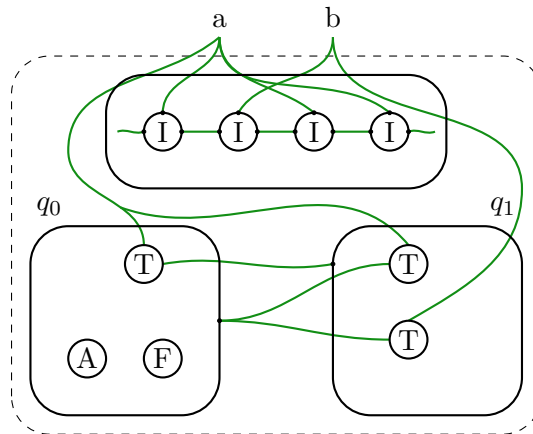
Figura 4.7: Grafo degli stati

Si noti come l'ultimo stato S_4 soddisfi la formula φ : il Wario Predicate $W_B(T, T, T)$ è soddisfatto dallo stato S_4 , in formule $MC, S_4 \models W_B(T, T, T)$, perchè il model checker trova in S_4 un match del bigrafo B. Poichè tutti gli argomenti del Wario Predicate sono True, basta che questo match esista perchè il predicato sia soddisfatto. Quindi, la proposizione 11 è rispettata.

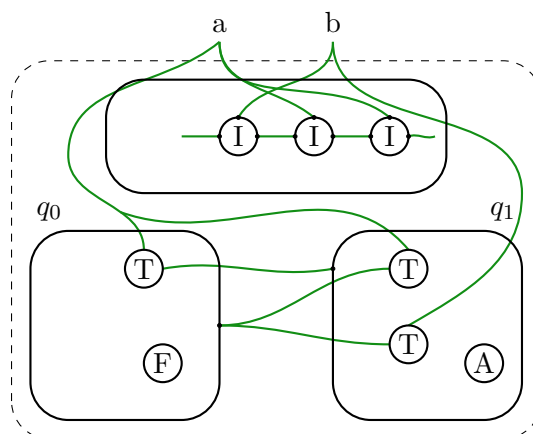
Questo esempio è molto importante perchè mostra due aspetti fondamentali:

- il primo è la flessibilità dei bigrafi: tramite una sola regola di reazione si è riusciti a modellare un NFA. Inoltre, si presti attenzione al grafo degli stati: è molto semplice e lineare. Come già scritto, questo è un indizio di buona progettazione, perchè significa che abbiamo creato una sola regola per tutti i casi possibili. Se avessimo creato una regola per casi particolari, allora ci sarebbero state diramazioni del grafo che avrebbero portato a vicoli ciechi, cioè rami in cui la foglia non rispetta la proprietà φ .
- il secondo è la generalità della logica per MC_{big} : si è espressa una proprietà di uno specifico dominio usando la logica generale creata per il model checker. In questo esempio si è usato il Wario Predicate, che permette di spostarsi all'interno del bigrafo e di verificare se una sua parte esiste e rispetta determinate proprietà. Nel NFA ci è bastato verificare che esistesse la parte denotata dal bigrafo B.

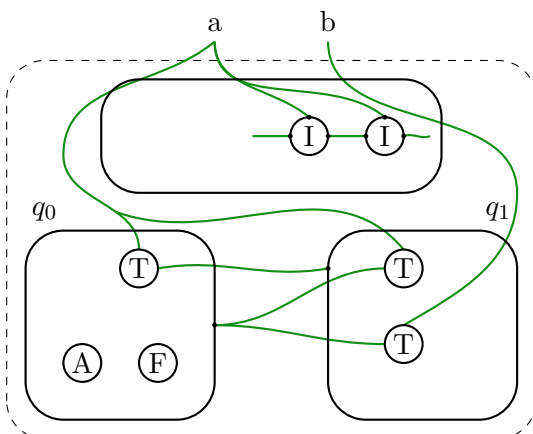
In questo esempio si è potuto apprezzare la comodità del model checker e della sua logica per verificare una generica proprietà, che rappresentano quindi uno strumento generale adatto per ogni BRS.



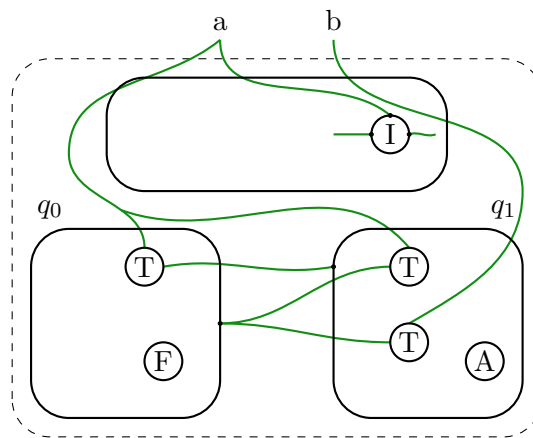
(a) Primo Passo



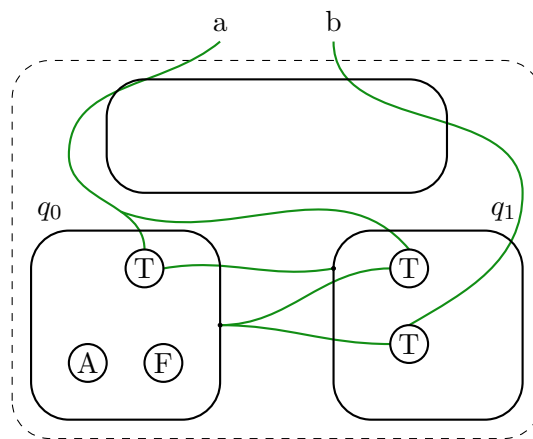
(b) Secondo Passo



(c) Terzo Passo



(d) Quarto Passo



(e) Quinto Passo

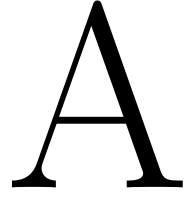
Figura 4.8: Traccia d'esecuzione di MC_{big}

Conclusioni

L'obiettivo principale di questa tesi era la creazione di uno strumento per la verifica di proprietà all'interno di un BRS, che è stato implementato risolvendo due problemi principali: l'isomorfismo tra bigrafi e la creazione di un model checker con una logica generale.

Il requisito principale su questo strumento di verifica è la sua *generalità*: esso deve permettere di esprimere le proprietà su qualsiasi dominio il BRS rappresenti. Questa tesi ha rispettato il requisito appena citato, grazie soprattutto alla semantica della logica creata, che risulta quindi sufficientemente generale. D'altra parte, potrebbe non risultare molto espressiva: essa è principalmente una logica spaziale, e quindi non tiene conto di fattori temporali che potrebbero aumentare la sua espressività. Si è però dato spazio a future logiche che potranno facilmente estendere MC_{big} .

L'isomorfismo tra bigrafi ha permesso invece la costruzione dello scheletro per il model checker: qualsiasi strumento di verifica deve permettere di evitare esecuzioni infinite quando è possibile. L'isomorfismo ha permesso quindi il raggiungimento di questo obiettivo. Il problema è stato risolto tramite la *programmazione a vincoli*, che ha ridotto notevolmente il tempo di sviluppo dell'algoritmo ma che potrebbe non essere la soluzione migliore in termini di complessità.



Notazione dei vari capitoli

Sono riportate le principali notazioni delle varie sezioni.

A.1 Notazione della sezione 1.2

Il più delle volte si tratterà un intero come l'insieme di tutti i suoi precedenti, così che se si scriverà m in realtà si intende $\{0, \dots, m-1\}$.

Scriviamo $S \# T$ per dire che i due insiemi S e T sono disgiunti. Scriviamo $S \uplus T$ per descrivere l'unione dei due insiemi S e T dopo che sappiamo o assumiamo che siano disgiunti.

Se f ha dominio S e $S' \subset S$, allora denotiamo con $f \upharpoonright S'$ la restrizione di f su S' . Per due funzioni f e g con dominio disgiunto S e T , scriviamo $f \uplus g$ per la funzione con dominio $S \uplus T$ tale che $(f \uplus g) \upharpoonright S = f$ e $(f \uplus g) \upharpoonright T = g$.

A.2 Notazione della sezione 1.4

I *posti* di $G : \langle m, X \rangle \rightarrow \langle n, Y \rangle$ sono i suoi siti m , i suoi nodi e le sue radici n .

I *punti* di G sono le sue porte e i suoi inner names X .

I *link* di G sono i suoi archi (edge) e i suoi outer names Y .

Gli edges sono *link chiusi* mentre gli outer names sono *link aperti*. Un punto è detto *aperto* se il suo punto è aperto, altrimenti è detto chiuso. G è detto *aperto* se tutti i suoi link sono aperti (ovvero se non ha edges).

Un place senza figli o un link senza punti viene detto *idle*. Due places con lo stesso genitore o due link con lo stesso punto vengono detti *fratelli*.

Se un' interfaccia $I = \langle m, X \rangle$ ha $X = \emptyset$, allora scriveremo I come m ; se $m = 0$ o $m = 1$, scriveremo I come X e $\langle X \rangle$ rispettivamente.

Si definisce l'unità ε come $\varepsilon = \langle 0, \emptyset \rangle$.

L'unico bigrafo con supporto vuoto in $\varepsilon \rightarrow I$ viene scritto come I . Un bigrafo

$g : \varepsilon \rightarrow I$, con dominio ε , viene detto *ground*. Useremo lettere minuscole per i bigrafi ground e li scriveremo come $g : I$.

A.3 Notazione della sezione ??

Spesso si omette ' $\dots \otimes id_I$ ' in una composizione del tipo $(F \otimes id_I) \circ G$, dove F non possiede un'interfaccia sufficiente per comporre con G . Si scriverà dunque, qualora non presenti ambiguità, $F \circ G$. Dato un linking $\lambda : Y \rightarrow Z$, potremmo volerlo applicare ad un bigrafo G con interfaccia esterna $\langle m, X \rangle$ avente meno nomi, i.e. $Y = X \uplus X'$. Scriveremo allora $\lambda \circ G$ per indicare $(id_m \otimes \lambda) \circ (G \otimes X')$, quando m e X' possono essere capiti dal contesto.

Bibliografia

- [1] Robin Milner. *The Space and Motion of Communicating Agents*. Cambridge University Press, 2009.