Indice

1 Nozioni di Base

1.1 Relazioni Binarie

Riportiamo la definizione di *relazione binaria* su uno o due insiemi, che sarà utile per definire formalmente il concetto di *grafo*, fondamentale all'interno di questo elaborato.

Definizione 1.1. Chiameremo *relazione binaria* su A, B qualsiasi sottoinsieme del prodotto cartesiano $A \times B$.
Chiameremo *relazione binaria* su A qualsiasi sottoinsieme del prodotto cartesiano $A \times A$.
Diremo che u, v sono *in relazione* rispetto a R se $(u, v) \in R$. In questo caso potremo usare la notazione uRv.

Alcune relazioni binarie mostrano proprietà fondamentali, che presentiamo nella definizione seguente:

Definizione 1.2. Sia R una relazione binaria su A. Diremo che R è

- *riflessiva* se $\forall x \in A, xRx$;
- *simmetrica* se $xRy \implies yRx$ $(x, y \in A)$
- *transitiva* se $(xRy \wedge yRz) \implies xRz$ $(x, y, z \in A)$

Esempio 1.1. La relazione $\leq$ sui naturali è riflessiva e transitiva, ma non simmetrica.
La relazione $=$ $(a = b \iff$ "a, b sono lo stesso numero") sui naturali è simmetrica, riflessiva e transitiva.

Definizione 1.3. Una relazione binaria riflessiva, simmetrica e transitiva si dice *relazione di equivalenza*.
Una relazione di equivalenza divide un insieme in *classi di equivalenza* all'interno delle quali tutte le coppie di elementi sono in relazione.

A partire da una relazione binaria R possiamo costruire relazioni binarie che contengono R, e che mostrano una o più delle proprietà presentate sopra, le cosiddette *chiusure*. Ogni chiusura è costituita dall'unione della relazione iniziale e di un insieme di coppie costruito con un criterio differente a seconda del tipo di chiusura, che fornisce la proprietà desiderata.

Definizione 1.4. Sia R una relazione binaria su A. Definiamo le seguenti chiusure:

- *riflessiva*: $R_r = R \cup \{(x, x)\ \forall x \in A\}$
- *simmetrica*: $R_s = R \cup \{(y, x)\ \forall x, y : (x, y) \in R\}$
- *transitiva*: $R_t = R \cup \{(x, z)\ \forall x, z : \exists y : (x, y) \in R \wedge (y, z) \in R\}$

Esempio 1.2. La chiusura riflessiva della relazione $<$ (minore stretto) è la relazione $\leq$.

Nel seguito utilizzeremo la seguente notazione:

Definizione 1.5. Sia A un insieme. Denoteremo con $|A|$ la *cardinalità* di A, cioè il numero dei suoi elementi.
Analogamente, data una relazione binaria R, denoteremo con $|R|$ il numero delle coppie messe in relazione da R.

1.2 Grafi

Con queste premesse possiamo definire un *grafo* come segue:

Definizione 1.6. Sia V un insieme finito non vuoto. Sia $\rightarrow$ una relazione binaria su V.
Chiameremo *grafo diretto* o *grafo orientato* la coppia $G = (V, \rightarrow)$.
In questo caso

- V è l'insieme dei *nodi* o *vertici*;
- $\rightarrow$ è una relazione binaria che mette in relazione alcuni dei nodi di G

Esempio 1.3. Il grafo di Figura 1 è descritto dalla coppia

- $V = \{a, b, c, d, e\}$
- $\rightarrow = \{(a, b), (a, d), (b, c), (d, c), (c, e), (d, e)\}$

Nel seguito utilizzeremo ampiamente la seguente terminologia:

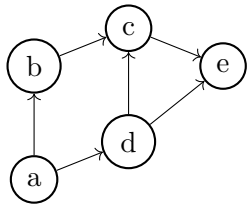


Figura 1: Rappresentazione grafica di un grafo

Definizione 1.7. Sia $G = (V, \to)$ un grafo. Diremo che un nodo $u \in V$ è una *foglia* se $\nexists v \in V : u \to v$. Diremo che u è *parente* di v e che v è *figlio* di u se $u \to v$. Chiaramente ogni nodo può avere più parenti e più figli.

Un grafo è quindi un insieme di elementi (i *nodi*) accoppiato con un insieme di relazioni tra questi elementi (gli *archi* o *rami*).
È naturale associare questo concetto all'idea di percorso: ogni grafo è definito da un insieme di nodi ed un insieme di *cammini* che consentono di spostarsi da un nodo ad un altro.
La seguente definizione sorge in modo spontaneo da questo punto di vista:

Definizione 1.8. Sia $G = (V, \to)$ un grafo. Siano $u, v \in V$. Diremo che v *è raggiungibile da* u, o in alternativa *esiste un cammino da* u *a* v, o ancora $u \to_t v$ (la t in pedice sta per "*transitivo*"), se $\exists x_n \subset V$ (una sequenza finita di nodi) di lunghezza $K : x_K = v, x_0 = u, x_n \to x_{n+1}$.

L'esistenza di un cammino tra nodi fornisce un criterio immediato per partizionare un grafo in gruppi di nodi. Diamo innanzitutto la seguente definizione:

Definizione 1.9. Diremo che un grafo $(V, \to)$ è *fortemente connesso* se $\forall v_1, v_2 \in V, v_1 \to_t v_2$.

In generale un grafo non è fortemente connesso. Tuttavia possiamo individuare facilmente i sottografi massimali fortemente connessi.

Definizione 1.10. Le *componenti fortemente connesse* (*strongly connected components*, *SCC*) di un grafo $(V, \to)$ sono le classi di equivalenza della relazione $\to_t$ [2, Appendice B].

In altre parole, i nodi contenuti in una stessa componente fortemente connessa sono mutuamente raggiungibili.

Esempio 1.4. Nel grafo di Figura 2 le SCC sono evidenziate con colori diversi: $\{a, b, c, d\}, \{e\}$.

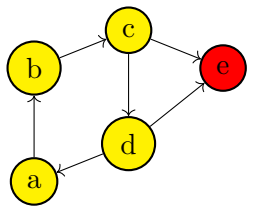


Figura 2: SCC di un grafo

Dato un grafo, possiamo definire il partizionamento dei nodi in SCC come segue:

Definizione 1.11. Sia $G = (V, \to)$ un grafo. Definiamo il grafo $G^{SCC} = (V^{SCC}, \to^{SCC})$ delle componenti fortemente connesse:

- $V^{SCC} = \{C : \text{“}C \text{ è una classe di equivalenza per } \to_t \text{ su } V\text{”}\}$
- $\to^{SCC} = \{(A, B) \in V^{SCC} \times V^{SCC} : A \neq B, \exists m \in A, n \in B : m \to n\}$

Riportiamo la seguente proprietà immediata:

Proposizione 1.1. *Sia G^{SCC} il grafo delle SCC di un grafo G generico. Allora G^{SCC} è aciclico.*

Dimostrazione. Suppongo per assurdo che in G^{SCC} esista un ciclo. Allora tutti i nodi di V^{SCC} facenti parte del ciclo sono mutuamente raggiungibili (percorrendo il ciclo). Quindi tutti i nodi fanno parte della stessa SCC, ma questo è assurdo. □

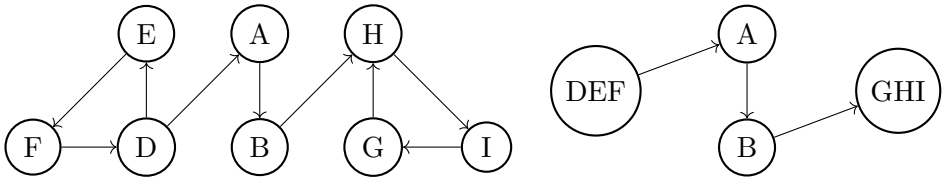
Esempio 1.5. La Figura 3.a rappresenta un grafo generico, la Figura 3.b rappresenta il suo grafo delle componenti fortemente connesse associato.

Dato un grafo generico possiamo determinare la partizione in SCC sfruttando un algoritmo avente complessità lineare $\Theta(|V|+| \to |)$ [5]. L'algoritmo non verrà trattato in questo elaborato.

1.3 Insiemi

1.3.1 Cenni di teoria degli insiemi

In generale ammettiamo che un insieme possa contenere altri insiemi. Questa concessione diventa problematica nel caso in cui tra i membri di un insieme A risulti lo stesso insieme A, o un insieme contenente l'insieme A. Diamo quindi la seguente definizione:



(a) Un grafo (b) Corrispondente grafo delle SCC

Figura 3: Un grafo ed il corrispondente grafo delle SCC

Definizione 1.12. Diremo che un insieme A è *ben-fondato* se $\forall B \in A$: "B è un insieme" si ha $A \notin B$. Altrimenti diremo che A è *non-ben-fondato*.

Esempio 1.6. L'insieme $\Omega = \{\Omega\}$ è non-ben-fondato. L'insieme $A = \{1, 2, 3\}$ è ben-fondato.

1.3.2 Rappresentazione di insiemi tramite grafi

In alcuni casi risulta conveniente fornire un'interpretazione insiemistica della nozione di grafo vista sopra. Introduciamo innanzitutto una nozione fondamentale:

Definizione 1.13. Sia $G = (V, \rightarrow)$ un grafo orientato. Sia $u \in V : \forall v \in V, u \rightarrow_t v$, cioè ogni nodo di G è raggiungibile da u. Allora la terna $(V, \rightarrow, u)$ si dice *accessible pointed graph*, o *APG*.

Per pervenire allo scopo di rappresentare un insieme tramite un grafo è necessario definire un processo denominato *decorazione*:

Definizione 1.14. Chiameremo *decorazione* di un APG l'assegnazione di un insieme ad ogni suo nodo.

Associando la relazione di raggiungibilità $\rightarrow$ alla relazione di appartenenza $\in$ abbiamo tutto il necessario per la rappresentazione di insiemi:

Definizione 1.15. Chiameremo *immagine* (o *picture* in [1]) di un insieme A la coppia composta da un APG (G, v) e da una decorazione, in cui a v è associato A.

Ad un APG aciclico è possibile associare un'unica decorazione. Questo risultato tuttavia non può essere dimostrato nel caso di un APG contenente almeno un ciclo. Per questo motivo in [1] viene dato il seguente assioma:

Assioma 1.1 (AFA, Anti-Foundation-Axiom)**.** Ogni APG possiede un'unica decorazione.

L'assioma AFA ha un'ovvia conseguenza:

Corollario 1.1. *Ogni APG è immagine di un unico insieme.*

Esempio 1.7. In Figura 4 sono rappresentati alcuni insiemi sotto forma di APG.

In [1] viene fornita una formulazione alternativa dell'assioma AFA, data dalla congiunzione dei seguenti assiomi:

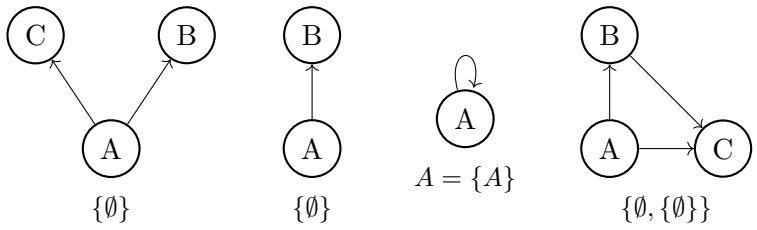


Figura 4: Rappresentazione di insiemi tramite grafi

Assioma 1.2. (AFA1) Ogni grafo ha almeno una decorazione.

Assioma 1.3. (AFA2) Ogni grafo ha al più una decorazione.

Chiaramente le due formulazioni sono equivalenti. Consideriamo adesso la seguente relazione binaria su insiemi:

$$a \equiv b \iff \text{“esiste un APG che è immagine di entrambi”}$$

Proposizione 1.2. *AFA2 e* $(a \equiv b \implies a = b)$ *sono equivalenti.*

Dimostrazione. Supponendo valido AFA2, la decorazione di un APG (immagine di a, b) è unica. Quindi a, b devono necessariamente essere lo stesso insieme.
Supponendo $(a \equiv b \implies a = b)$, se per assurdo esistesse un APG avente più di una decorazione, i due insiemi X, Y rappresentati rispettivamente dalle coppie (APG, “Decorazione #1”), (APG, “Decorazione #2”) dovrebbero essere in realtà lo stesso insieme. Ma dall'ipotesi assurda si osserva che, nell'assegnare ad ogni nodo dell'APG un insieme, ad almeno un nodo è stato assegnato un insieme diverso nella prima e nella seconda decorazione. Questo significa che $X \neq Y$, che è assurdo. □

La formulazione alternativa di AFA sarà utile nel seguito, in quanto consente di collegare il concetto di *bisimulazione* con la teoria degli insiemi.

1.4 Bisimulazione

Definizione 1.16. Siano $G_1 = (V_1, \to_1), G_2 = (V_2, \to_2)$ due grafi. Diremo che una relazione binaria $R : V_1 \times V_2$ è una *bisimulazione* su G_1, G_2 se $\forall a \in V_1, b \in V_2$ valgono congiuntamente le seguenti proprietà:

- $aRb, a \to_1 a' \implies \exists b' \in V_2 : (a'Rb' \wedge b \to_2 b')$
- $aRb, b \to_2 b' \implies \exists a' \in V_1 : (a'Rb' \wedge a \to_1 a')$

Possiamo definire in modo analogo una bisimulazione su un unico grafo G, ponendo $G_1 = G_2 = G$.

Definiamo un'importante caratteristica di una coppia qualsiasi di grafi, che verrà sfruttata ampiamente nel seguito

Definizione 1.17. Siano $G_1 = (V_1, \to_1), G_2 = (V_2, \to_2)$ due grafi. Diremo che sono *bisimili* se $\exists R : V_1 \times V_2 : R$ è una bisimulazione su G_1, G_2.
Diremo che due APG $(G_1, v_1), (G_2, v_2)$ sono *bisimili* se G_1, G_2 sono bisimili e vale $v_1 R v_2$ per almeno una bisimulazione su G_1, G_2.

Osservazione 1.1. Una bisimulazione può non essere riflessiva, simmetrica, nè transitiva.

Esempio 1.8. La relazione $aRb \iff$ "a, b sono lo stesso nodo" su un grafo qualsiasi è una bisimulazione riflessiva, simmetrica e transitiva.
La relazione $R = \emptyset$ è una bisimulazione su un grafo qualsiasi, ma non è riflessiva.
La relazione $R = \{(a,a), (b,b), (c,c), (d,d), (a,b), (b,c), (c,d)\}$ sul grafo $G = (\{a,b,c,d\}, \{(a,b), (b,c), (c,d), (d,d)\})$ è una bisimulazione, ed è solamente riflessiva.

Dalla definizione di bisimulazione possiamo dedurre una proprietà interessante di una qualsiasi sua chiusura:

Teorema 1.1. *Sia R una bisimulazione sul grafo G. La sua chiusura riflessiva, simmetrica o transitiva è ancora una bisimulazione su G.*

Dimostrazione. Consideriamo separatamente le tre relazioni R_r, R_s, R_t, rispettivamente la chiusura riflessiva, simmetrica e transitiva:

R_r Per definizione $R \subset R_r$, quindi è sufficiente dimostrare che R_r è una bisimulazione quando gli argomenti $u, v \in V$ non sono distinti.
Sia $u \in V$. Chiaramente per definizione di R_r si ha $u R_r u$. Se $\exists u' \in V : u \to u'$ allora (sempre per definizione di R_r) si ha $u' R_r u'$.

R_s Per definizione $R \subset R_s$, quindi è sufficiente dimostrare che R_s è una bisimulazione quando per gli argomenti $u, v \in V$ si ha uRv ma non vRu.
Sia $(u, v) \in V \times V$. Allora

$$u R_s v \implies uRv \vee vRu$$

Suppongo ad esempio che vRu.

$$\implies \forall v' \in V : (v \to v')\ \exists u' \in V : (u \to u' \wedge v'Ru')$$
$$\implies u'R_s v'$$

e

$$\implies \forall u' \in V : (u \to u')\ \exists v' \in V : (v \to v' \wedge v'Ru')$$
$$\implies u'R_s v'$$

cioè sono dimostrate le due condizioni caratteristiche della bisimulazione.
La dimostrazione è analoga se uRv.

R_t Per definizione $b \subset R_t$, quindi è sufficiente dimostrare che R_t è una bisimulazione quando per gli argomenti $u, v, z \in V$ si ha uRv, vRz ma non uRz.
Sia $(u, v, z) \in V \times V \times V$ con questa proprietà. Allora $\forall u' \in V : u \to u' \implies \exists v' \in V : v \to v' \wedge u'Rv'$. Inoltre $\exists z' : z \to z' \wedge v'Rz'$.
Riordinando si ha $u'Rv', v'Rz'$. Allora per definizione di b_t, $u'R_t z'$.
In modo speculare si ottiene la seconda condizione caratteristica della bisimulazione.

□

Da questa proposizione si deduce il seguente corollario, che risulta dall'applicazione iterativa delle tre chiusure viste in precedenza:

Corollario 1.2. *Ad ogni bisimulazione R è possibile associare una bisimulazione $\widetilde{R} : R \subset \widetilde{R}\ \wedge\ \widetilde{R}$ è una relazione di equivalenza.*

Concludiamo la sezione relativa ai risultati generali sulla bisimulazione con la seguente proposizione, che sarà utile nel seguito:

Proposizione 1.3. *Siano R_1, R_2 due bisimulazioni su G_1, G_2. Allora $R = R_1 \cup R_2$ è ancora una bisimulazione.*

Dimostrazione. Siano $u, v : uRv$. Sia $u' : u \to u'$. Allora deve essere $uR_1v \vee uR_2v$. Ma quindi $\exists v' : (v \to v' \wedge u'R_{1|2}v')$. □

1.4.1 Bisimulazione massima

Definiamo ora il concetto di *bisimulazione massima*, che gioca un ruolo chiave nella risoluzione dei problemi considerati in questo elaborato:

Definizione 1.18. Diremo che una bisimulazione R_M su G_1, G_2 è *massima* se $\forall R : "R$ è una bisimulazione su $G_1, G_2"$ si ha $uRv \implies uR_Mv$.

Naturalmente la bisimulazione massima dipende dai due grafi presi in esame. Possiamo dedurre alcune caratteristiche in modo molto semplice:

Proposizione 1.4. *Valgono le seguenti proprietà:*

1. *La bisimulazione massima su due grafi G_1, G_2 è unica*
2. *La bisimulazione massima è una relazione di equivalenza*

Dimostrazione. Le proprietà seguono banalmente dal Corollario 1.2 e dall'Osservazione 1.3.

1. Suppongo per assurdo che esistano due bisimulazioni massime R_{M_1}, R_{M_2}. La loro unione è ancora una bisimulazione, che è "più massima" delle supposte bisimulazioni massime.
2. Se per assurdo la bisimulazione massima non fosse una relazione di equivalenza, potremmo considerare la sua chiusura riflessiva, simmetrica e transitiva, che sarebbe "più massima" ed anche una relazione di equivalenza.

□

Naturalmente il concetto di *bisimulazione massima* può essere definito anche su unico grafo G. Questo caso si rivelerà di grande interesse nel seguito. Per ora dimostriamo il seguente risultato:

Teorema 1.2. *Sia G un grafo (finito). Allora $\exists R_M$ la bisimulazione massima su G.*

Dimostrazione. Può esistere solamente un numero finito di relazioni binarie su G, e questo numero fornisce un limite superiore al numero massimo di bisimulazioni su G. Allora possiamo considerare l'unione di questo numero finito di bisimulazioni, che sarà chiaramente la bisimulazione massima. □

1.4.2 Interpretazione insiemistica della bisimulazione

Il seguente teorema è la prova che la bisimulazione può essere utilizzata per verificare l'uguaglianza tra insiemi rappresentati da due APG differenti:

Teorema 1.3. *Due APG sono bisimili* $\iff$ *rappresentano lo stesso insieme.*

Dimostrazione. Da dimostrare... □

Tenendo conto di quanto affermato nella sezione 1.3.2, il Teorema 1.3 dimostra che la bisimulazione può sostituire la relazione di uguaglianza tra insiemi quando questi sono rappresentati con APG [3].
Dopo questa considerazone, risulta naturale definire il seguente concetto:

Definizione 1.19. Sia R una bisimulazione su G che sia anche una relazione di equivalenza. Definiamo un nuovo grafo $G_R = (VR, \to_R)$ come in [4], che chiameremo *contrazione rispetto alla bisimulazione* R *di* G:

- $VR = \{A = \{m \in V : \forall n \in A, mRn\}\}$
- $[m]_R \to_R [n]_R \iff \exists c \in [n]_R : m \to c$

Si definisce *classe del nodo* a rispetto alla bisimulazione R, con la notazione $[a]_R$, il nodo di VR in cui viene inserito il nodo a.

La Definizione 1.19 è di fondamentale importanza per la seguente osservazione:

Proposizione 1.5. *Sia* G *un grafo, e sia* G_R *come nella Definizione 1.19, per una bisimulazione* R *qualsiasi. Allora* G, G_R *sono bisimili.*

Dimostrazione. Sia $\equiv \subset V \times VR$ la relazione binaria definita come segue:

$$m \equiv M \iff M = [m]_R$$

Vogliamo dimostrare che tale relazione è una bisimulazione sui grafi G, G_R. Supponiamo che $x \equiv X$, e che $x \to y$ per qualche $y \in V$. Chiamiamo $Y := [y]_R$. Allora, per la Definizione 1.19, si ha $X \to Y$. Inoltre vale banalmente $y \equiv Y$.
Per dimostrare la seconda condizione caratteristica della bisimulazione, supponiamo che $x \equiv X$, e che $X \to Y$ per qualche $Y \in VR$. Sempre per la Definizione 1.19 deve esistere un $y \in Y : (y \equiv Y \wedge x \to y)$. □

La Proposizione 1.5 ha una conseguenza ovvia, che risulta evidente per il Teorema 1.3:

Corollario 1.3. *Sia R una bisimulazione che sia anche una relazione di equivalenza. Allora l'APG (G, v) e l'APG $(G_R, [v]_R)$ rappresentano lo stesso insieme.*

Quindi risulta naturale sfruttare le proprietà della bisimulazione per minimizzare la rappresentazione di insiemi, considerando che è sufficiente una bisimulazione sulla rappresentazione iniziale per ottenere una rappresentazione equivalente. Definiamo una relazione d'ordine sulle rappresentazioni:

Definizione 1.20. Diremo che la rappresentazione (G_a, v_a) di un insieme è *minore* della rappresentazione equivalente (G_b, v_b) se $|Va| < |Vb|$.
Diremo che una rappresentazione è *minima* se non esiste una rappresentazione equivalente minore.

Osservazione 1.2. La *contrazione per bisimulazione* è una rappresentazione minore (o eventualmente uguale) di quella iniziale.

Concludiamo la sezione con il seguente risultato, che stabilisce in modo univoco la bisimulazione prescelta per minimizzare la rappresentazione di un dato insieme:

Teorema 1.4. *Sia (G, v) un APG rappresentante un insieme. Sia R_M la bisimulazione massima su (G, v). Allora la contrazione per bisimulazione indotta da R_M su (G, v) fornisce la rappresentazione minima dell'insieme.*

Dimostrazione. Suppongo per assurdo che esista una bisimulazione R_V su (G, v) che fornisce una contrazione avente un numero di nodi strettamente inferiore alla contrazione indotta da R_M. Ma questo implica che esistono almeno due nodi di G che sono in relazione secondo R_V e non secondo R_M. Chiaramente questa deduzione è in contrasto con il fatto che R_M è la bisimulazione massima.
Suppongo per assurdo che, dopo la contrazione indotta da R_M, sia possibile trovare una nuova bisimulazione R_O su $(G_{R_M}, [v]_{R_M})$ che induca una contrazione avente un numero di nodi strettamente inferiore a quello di $(G_{R_M}, [v]_{R_M})$. Chiaramente $R_O \subset VR_M \times VR_M$.
Definisco una nuova bisimulazione $R_{\widetilde{M}} \subset V \times V$ tale che

$$xR_{\widetilde{M}}y \iff (xR_My \vee [x]_{R_M} R_O [y]_{R_M})$$

Per definizione di bisimulazione massima bisogna avere $R_{\widetilde{M}} \subset R_M$, quindi non è possibile che la contrazione indotta da R_O sia una rappresentazione minore di quella indotta da R_M. □

Bibliografia

[1] Peter Aczel. *Non-well-founded sets*, volume 14 of *CSLI lecture notes series*. CSLI, 1988.

[2] Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms, 3rd Edition*. MIT Press, 2009.

[3] Agostino Dovier, Carla Piazza, and Alberto Policriti. A fast bisimulation algorithm. In *International Conference on Computer Aided Verification*, pages 79–90. Springer, 2001.

[4] Raffaella Gentilini, Carla Piazza, and Alberto Policriti. From bisimulation to simulation: Coarsest partition problems. *Journal of Automated Reasoning*, 31(1):73–103, 2003.

[5] Robert Tarjan. Depth-first search and linear graph algorithms. *SIAM journal on computing*, 1(2):146–160, 1972.