

# Indice

	Pagina
<b>1 Nozioni di Base</b>	<b>2</b>
1.1 Relazioni Binarie . . . . .	2
1.2 Grafi . . . . .	3
1.3 Cenni di teoria degli insiemi . . . . .	5
1.4 Rappresentazione di insiemi tramite grafi . . . . .	5
1.5 Bisimulazione . . . . .	6
1.5.1 Bisimulazione massima . . . . .	9
1.5.2 Interpretazione insiemistica della bisimulazione . . . . .	10
<b>Bibliografia</b>	<b>13</b>

# 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 tutti gli 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  $A$ . Diamo le seguenti definizioni

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

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

La chiusura transitiva della relazione  $aRb \iff$  “ $a$  è più piccolo di  $b$ ” è la relazione  $<$ .

## 1.2 Grafi

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

**Definizione 1.5.** 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 la relazione di raggiungibilità:  $a \rightarrow b$  ( $a, b \in V$ ) significa “nel grafo  $G$  esiste un arco dal nodo  $a$  al nodo  $b$ ”.

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

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

Nel seguito utilizzeremo ampiamente la seguente terminologia:

**Definizione 1.6.** Sia  $G = (V, \rightarrow)$  un grafo. Diremo che un nodo  $u \in V$  è una *foglia* se  $\nexists v \in V : u \rightarrow v$ . Diremo che  $u$  è *parente* di  $v$  e che  $v$  è *figlio* di  $u$  se  $u \rightarrow v$ .

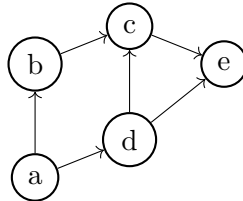


Figura 1: Rappresentazione grafica di un grafo

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 1.7.** Sia  $G = (V, \rightarrow)$  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  $u \rightarrow_t v$  (la  $t$  in pedice sta per “*transitivo*”), se  $\exists x_n \subset V$  (una sequenza finita di nodi) di lunghezza  $K : x_K = v, x_0 = u, x_n \rightarrow x_{n+1}$ .

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 1.8.** Diremo che un grafo  $(V, \rightarrow)$  è *fortemente connesso* se  $\forall v_1, v_2 \in V, v_1 \rightarrow_t v_2$ .

Le *componenti fortemente connesse* (CFC) di un grafo  $(V, \rightarrow)$  sono le classi di equivalenza della relazione  $\rightarrow_t$  [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 CFC sono state evidenziate con colori diversi:  $\{a, b, c, d\}, \{e\}$ .

Il partizionamento in CFC è definito come segue:

**Definizione 1.9.** Sia  $G = (V, \rightarrow)$  un grafo. Chiameremo *grafo delle componenti fortemente connesse* (CFC) di  $G$  il grafo  $G^{CFC} = (V^{CFC}, \rightarrow^{CFC})$  con

- $V^{CFC} = \{C : “C \text{ è una classe di equivalenza per } \rightarrow_t \text{ su } V”\}$

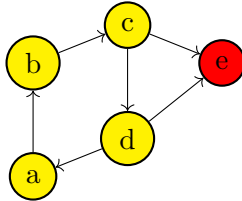


Figura 2: CFC di un grafo

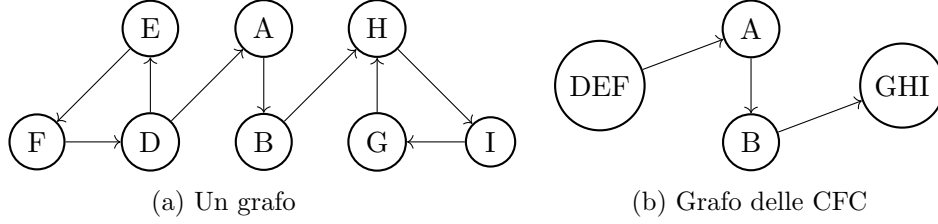


Figura 3: Un grafo ed il corrispondente grafo delle CFC

$$\bullet \rightarrow^{CFC} = \{(A, B) \in V^{CFC} \times V^{CFC} : A \neq B, \exists m \in A, n \in B : m \rightarrow n\}$$

Riportiamo la seguente proprietà immediata:

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

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

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

### 1.3 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:

**Definizione 1.10.** Diremo che un insieme  $A$  è *ben-fondato* se  $\forall B \in A : "B \text{ è un insieme}"$  si ha  $A \not\subset B$ . 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.

### 1.4 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 1.11.** 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 1.12.** 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 1.13.** Chiameremo *immagine* (o *picture* in [1]) di un insieme  $A$  la coppia di un APG  $(G, v)$  con 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.

## 1.5 Bisimulazione

**Definizione 1.14.** Siano  $G_1 = (V_1, \rightarrow_1), G_2 = (V_2, \rightarrow_2)$  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:

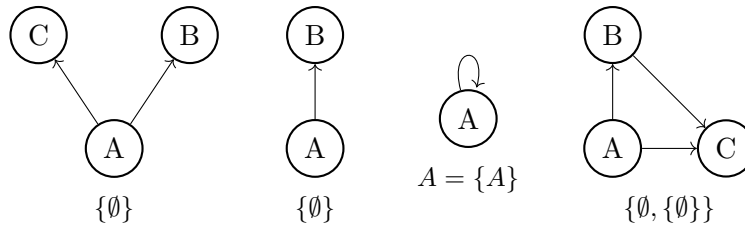


Figura 4: Rappresentazione di insiemi tramite grafi

- $aRb, a \rightarrow_1 a' \implies \exists b' \in V_2 : (a'Rb' \wedge b \rightarrow_2 b')$
- $aRb, b \rightarrow_2 b' \implies \exists a' \in V_1 : (a'Rb' \wedge a \rightarrow_1 a')$

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 1.15.** Siano  $G_1 = (V_1, \rightarrow_1), G_2 = (V_2, \rightarrow_2)$  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  $aRb \iff "a, b \text{ sono lo stesso nodo}"$  su un grafo qualsiasi è una bisimulazione riflessiva, simmetrica e transitiva.

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

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

*Dimostrazione.* Consideriamo separatamente le tre relazioni  $b_r, b_s, b_t$ , rispettivamente la chiusura riflessiva, simmetrica e transitiva:

$b_r$  Per definizione  $b \subset b_r$ , quindi è sufficiente dimostrare che  $b_r$  è una bisimulazione quando gli argomenti  $u, v \in N$  non sono distinti.

Sia  $u \in N$ . Chiaramente per definizione di  $b_r$  si ha  $ub_r u$ . Se  $\exists u' \in N : u \rightarrow u'$  allora (sempre per definizione di  $b_r$ ) si ha  $u'b_r u'$ .

$b_s$  Per definizione  $b \subset b_s$ , quindi è sufficiente dimostrare che  $b_s$  è una bisimulazione quando per gli argomenti  $u, v \in N$  si ha  $ubv$  ma non  $vbu$ .

Sia  $(u, v) \in N \times N$ . Allora

$$ub_s v \implies ubv \vee vbu$$

Suppongo ad esempio che  $vb_u$ .

$$\begin{aligned} &\implies \forall v' \in N : (v \rightarrow v') \exists u' \in N : (u \rightarrow u' \wedge v'bu') \\ &\implies u'b_s v' \end{aligned}$$

e

$$\begin{aligned} &\implies \forall u' \in N : (u \rightarrow u') \exists v' \in N : (v \rightarrow v' \wedge v'bu') \\ &\implies u'b_s v' \end{aligned}$$

cioè sono dimostrate le due condizioni caratteristiche della bisimulazione.

La dimostrazione è analoga se  $ub_v$ .

$b_t$  Per definizione  $b \subset b_t$ , quindi è sufficiente dimostrare che  $b_t$  è una bisimulazione quando per gli argomenti  $u, v, z \in N$  si ha  $ub_v, vb_z$  ma non  $ub_z$ .

Sia  $(u, v, z) \in N \times N \times N$  con questa proprietà. Allora  $\forall u' \in N : u \rightarrow u' \implies \exists v' \in N : v \rightarrow v' \wedge u'bv'$ . Inoltre  $\exists z' : z \rightarrow z' \wedge v'bz'$ .

Riordinando si ha  $u'bv', v'bz'$ . Allora per definizione di  $b_t$ ,  $u'b_t z'$ .

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  $b$  è possibile associare una bisimulazione  $\tilde{b} : b \subset \tilde{b} \wedge \tilde{b}$  è una relazione di equivalenza.*

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

**Proposizione 1.2.** *Siano  $b_1, b_2$  due bisimulazioni su  $G_1, G_2$ . Allora  $b = b_1 \cup b_2$  è ancora una bisimulazione.*

*Dimostrazione.* Siano  $u, v : ub_v$ . Sia  $u' : u \rightarrow u'$ . Allora deve essere  $ub_1 v \vee ub_2 v$ . Ma quindi  $\exists v' : (v \rightarrow v' \wedge u'b_{1|2}v')$ . □



### 1.5.1 Bisimulazione massima

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

**Definizione 1.16.** Diremo che una bisimulazione  $b_M$  su  $G_1, G_2$  è *massima* se  $\forall b : "b \text{ è una bisimulazione su } G_1, G_2"$  si ha  $ubv \implies ub_Mv \quad \forall a \in N_1, b \in N_2$ .

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

**Proposizione 1.3.** *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 1.2.

1. Suppongo per assurdo che esistano due bisimulazioni massime  $b_{M_1}, b_{M_2}$ . 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  $\exists b_M$  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. □

### 1.5.2 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 1.4, il Teorema 1.3 dimostra che la bisimulazione può sostituire la relazione di uguaglianza tra insiemi quando questi sono rappresentati da degli APG [3].

Dopo questa considerazione, risulta naturale definire il seguente concetto:

**Definizione 1.17.** Sia  $b$  una bisimulazione su  $G$  che sia anche una relazione di equivalenza. Definiamo un nuovo grafo  $G_b = (N_b, \rightarrow_b)$  come in [4], che chiameremo *contrazione rispetto alla bisimulazione  $b$  di  $G$* :

- $N_b = \{A = \{m \in N : \forall n \in A, mbn\}\}$
- $[m]_b \rightarrow_b [n]_b \iff \exists c \in [n]_b : m \rightarrow c$

Risulta conveniente definire la *classe del nodo  $a$*  rispetto alla bisimulazione  $b$ , con la notazione  $[a]_b$  come il nodo di  $N_b$  a cui appartiene il nodo  $a$ .

La Definizione 1.17 è di fondamentale importanza per la seguente osservazione:

**Proposizione 1.4.** *Sia  $G$  un grafo, e sia  $G_b$  come nella Definizione 1.17, per una bisimulazione  $b$  qualsiasi. Allora  $G, G_b$  sono bisimili.*

*Dimostrazione.* Sia  $\equiv \subset N \times N_b$  la relazione binaria definita come segue:

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

Vogliamo dimostrare che tale relazione è una bisimulazione su i grafi  $G, G_b$ . Supponiamo che  $x \equiv X$ , e che  $x \rightarrow y$  per qualche  $y \in N$ . Chiamiamo  $Y := [y]_b$ . Allora, per la Definizione 1.17, si ha  $X \rightarrow Y$ . Inoltre vale banalmente  $y \equiv Y$ .

Per dimostrare la seconda condizione caratteristica della bisimulazione, supponiamo che  $x \equiv X$ , e che  $X \rightarrow Y$  per qualche  $Y \in N_b$ . Sempre per la Definizione 1.17 deve esistere un  $y \in Y : (y \equiv Y \wedge x \rightarrow y)$ . □

La Proposizione 1.4 ha una conseguenza ovvia, che risulta evidente per il Teorema 1.3:

**Corollario 1.3.** *Sia  $b$  una bisimulazione che sia anche una relazione di equivalenza. Allora l'APG  $(G, v)$  e l'APG  $(G_b, [v]_b)$  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 1.18.** Diremo che la rappresentazione  $(G_a, v_a)$  di un insieme è *minore* della rappresentazione equivalente  $(G_b, v_b)$  se  $\#N_a < \#N_b$ . Diremo che una rappresentazione è *minima* se non esiste un'altra rappresentazione minore.

**Osservazione 1.2.** La *contrazione per bisimulazione* di un grafo ha sempre un numero di nodi minore o uguale di quello del grafo 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  $b_M$  la bisimulazione massima su  $(G, v)$ . Allora la contrazione per bisimulazione indotta da  $b_M$  su  $(G, v)$  fornisce la rappresentazione minima dell'insieme.*

*Dimostrazione.* Suppongo per assurdo che esista una bisimulazione  $b_N$  su  $(G, v)$  che fornisce una contrazione avente un numero di nodi strettamente inferiore alla contrazione indotta da  $b_M$ . Ma questo implica che esistono almeno due nodi di  $G$  che sono in relazione secondo  $b_N$  e non secondo  $b_M$ . Chiaramente questa deduzione è in contrasto con il fatto che  $b_M$  è la bisimulazione massima.

Suppongo per assurdo che, dopo la contrazione indotta da  $b_M$ , sia possibile trovare una nuova bisimulazione  $b_O$  su  $(G_{b_M}, [v]_{b_M})$  che induca una contrazione avente un numero di nodi strettamente inferiore a quello di  $(G_{b_M}, [v]_{b_M})$ . Chiaramente  $b_O \subset N_{b_M} \times N_{b_M}$ .

Definisco una nuova bisimulazione  $b_{\widetilde{M}} \subset N \times N$  tale che

$$xb_{\widetilde{M}}y \iff (xb_My \vee [x]_{b_M}b_O[y]_{b_M})$$

Per definizione di bisimulazione massima bisogna avere  $b_{\widetilde{M}} \subset b_M$ , quindi non è possibile che la contrazione indotta da  $b_O$  sia una rappresentazione minore di quella indotta da  $b_M$ .  $\square$

## 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.