AN ALGEBRAIC FRAMEWORK FOR QUANTITATIVE INFORMATION FLOW

ARTHUR AMÉRICO PASSOS DE REZENDE

AN ALGEBRAIC FRAMEWORK FOR QUANTITATIVE INFORMATION FLOW

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais como requisito parcial para a obtenção do grau de Mestre em Ciência da Computação.

Orientador: Mário S. Alvim
Coorientador: Annabelle McIver

Belo Horizonte

Julho de 2018

ARTHUR AMÉRICO PASSOS DE REZENDE

AN ALGEBRAIC FRAMEWORK FOR QUANTITATIVE INFORMATION FLOW

Dissertation presented to the Graduate Program in Computer Science of the Federal University of Minas Gerais in partial fulfillment of the requirements for the degree of Master in Computer Science.

Advisor: Mário S. Alvim
Co-Advisor: Annabelle McIver

Belo Horizonte
July 2018

Ficha catalográfica elaborada pela Biblioteca do ICEx - UFMG

Rezende, Arthur Américo Passos de

R467a An algebraic framework for quantitative information flow / Arthur Américo Passos de Rezende — Belo Horizonte, 2018.
xxi, 104 f.: il.; 29 cm.

Dissertação (mestrado) - Universidade Federal de Minas Gerais – Departamento de Ciência da Computação.

Orientador: Mário Sérgio Ferreira Alvim Júnior.
Coorientadora: Annabelle McIver

1. Computação – Teses. 2. Teoria da informação. 3. Redes de informação - Controle de acesso. I. Orientador. II. Coorientadora. III. Título.

CDU 519.6*44(043)

UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

FOLHA DE APROVAÇÃO

An Algebraic Framework for Quantitative Information Flow

ARTHUR AMERICO PASSOS DE REZENDE

Dissertação defendida e aprovada pela banca examinadora constituída pelos Senhores:

Prof. Mario Sérgio Ferreira Alvim Júnior - Orientador
Departamento de Ciência da Computação - UFMG

A. McIver
Profa. Annabelle McIver - Coorientadora
Departamento de Computação - Macquarie University

Prof. Gabriel de Morais Coutinho
Departamento de Ciência da Computação - UFMG

Vinicius Fernandes dos Santos
Prof. Vinícius Fernandes dos Santos
Departamento de Ciência da Computação - UFMG

Prof. Carlos Alberto Olarte Vega
Escola de Ciência e Tecnologia - UFRN

Belo Horizonte, 4 de julho de 2018.

Acknowledgments

First of all, I would like to thank Professor Mário Sérgio Alvim. I had the honour to be the first graduate student he advised, and he did an exceptional job. Mário is the most hard-working academic I have ever met, always trying to do his best in all the different activities that his position consists of. His passion for research is contaminating, and his dedication to being the best teacher possible is truly inspiring. The career and personal advise I received from him are invaluable, and he is a professional I will always look up to as a model in my career.

I would also like to thank Professor Annabelle McIver, who, despite the distance, was present at every step during my degree. Annabelle is a brilliant and creative researcher, and a very kind person. Working with her during these last two years was an extremely rewarding experience. Having her as an advisor was a privilege, and a fundamental piece in my growth as a researcher. I cannot express how much I appreciate all the time and effort she put into my academic formation.

I would like to express my deep appreciation to Professors Gabriel Coutinho, Vinícius Fernandes dos Santos and Carlos Olarte for dedicating part of their time to read this thesis. Their observations were extremely helpful, greatly improving the quality of this work and prompting illuminating discussions about its content, which might lead to many interesting new research topics.

I am grateful for all the friends I have made in the Computer Science Department, especially for all the members of the INSCRYPT lab. I am particularly grateful for the help I received from my friends Artur Vaz, with whom I published a paper and had great conversations about my research topics; Thiago Vieira, who has been a great colleague to talk about the most diverse subjects in Quantitative Information Flow; and Guilherme Gomes, who was the first to suggest I should undertake a master's degree in Computer Science, and who helped me with my first steps in the field.

Many thanks to Dr. Catuscia Palamidessi and Dr. Kostas Chatzikokolakis for the amazing time I had during my internship at INRIA. Working with such brilliant and passionate researchers was an amazingly enriching experience, and I am very glad for having met some great people whose friendships I hope to cultivate. I would also like to thank INRIA for the financial support I received during my stay.

I am extremely fortunate to have a considerable number of really good friends. I dare not try to mention them all, for fearing to forget someone (and consequently ending up having fewer really good friends). I would like them to know how much I appreciate their friendship, and their always being there, supporting me through the hard parts of life and celebrating with me the good bits. Know that I will always be there to return the favour.

I would like to thank my girlfriend Cassi for all her love and support. Thank you for being a constant source of happiness and companionship. I can only hope to make as much a positive impact on your life as you do in mine.

I am very grateful for my family; they are the most precious thing I have, and from them I learned the most important values that guide my life. Special thanks are due to my aunts Tê and Du and to my cousins Ana Flávia, Fernanda, Isabela and Guilherme. There are no words that can describe how lucky I am to have you in my life.

I would particularly like to thank my parents for their unwavering love, support and dedication, and for all the sacrifices they have made to guarantee I would always have access to the best education possible. They are the most important people in my life, and anything I have achieved or will ever achieve is largely due to them.

Finally, I am grateful to all Brazilian citizens, who paid for my academic education since my undergraduate degree; including the financial support I received from CAPES during my master's course.

Abstract

The field of *quantitative information flow* (QIF) is concerned with measuring and controlling information leakage in computational systems. The traditional approach to QIF models systems as monolithic *information-theoretic channels*. Many real-world systems, however, consist of a collection of interacting parts and are better represented by an assemblage of channels.

In this thesis, we investigate the information leakage properties of channel compositions with regards to the recently developed *g-leakage framework*. We study five different types of compositions, each capturing a typical way in which parts interact in real-world systems. For each type, we derive equivalences and bounds that relate their information leakage to that of their components. We also establish whether *monotonicity* holds, i.e., whether a component can always be substituted with a more secure one without compromising the security of the system as a whole. Perhaps surprisingly, our results prove that monotonicity does not always hold.

Furthermore, we establish and compile a number of algebraic properties, and model two well-known security protocols in the literature, the *Dining Cryptographers* and the *Crowds* protocols. Our results yield simple algorithms to model their respective channels and, for the latter, one that is faster than the state-of-the-art algorithms in the literature.

Palavras-chave: Quantitative Information Flow, Channel Composition, Information Leakage, g-leakage.

Resumo

O campo de *fluxo de informação quantitativo* (QIF) se interessa em medir e controlar vazamentos de informação em sistemas computacionais. A abordagem tradicional em QIF modela sistemas como *canais de teoria de informação* indivisíveis. Contudo, muitos sistemas reais consistem em várias partes que interagem entre si, sendo melhor representados por uma coleção de canais.

Nessa dissertação, investigamos as propriedades de vazamento de informação de composições de canais com respeito ao recentemente proposto arcabouço de *g-leakage*. Nós estudamos cinco tipos de composições que capturam maneiras típicas com que partes interagem em sistemas reais. Para cada tipo, nós derivamos equivalências e limites que relacionam o seu vazamento de informação com a de seus componentes. Nós também estabelecemos se eles respeitam *monotonicidade*, isso é, se um componente sempre pode ser substituído por um mais seguro sem comprometer a segurança do sistema como um todo. Talvez surpreendentemente, nossos resultados provam que esse nem sempre é o caso

Além disso, nós estabelecemos e compilamos algumas propriedades algébricas, e modelamos dois famosos protocolos da literatura, o *Dining Cryptographers* e o *Crowds*. Nossos resultados possibilitam algoritmos simples para o cálculo de seus canais e, para o segundo protocolo, um algoritmo mais rápido do que aqueles do estado da arte na literatura.

Palavras-chave: Fluxo de Informação Quantitativo, Composição de Canais, Vazamento de Informação, g-leakage.

List of Figures

List of Tables

Contents

Chapter 1

Introduction

The last few decades have witnessed an astonishing rise in the use of technology in day-to-day life. Having constant access to the Internet through all sort of devices is now a constant motif in the routine of a great number of people, and the results of this constant flow of information have changed almost all aspects of our civilization.

Being it inconceivable that society will ever abandon all the conveniences and practicalities provided by this new technological arrangement, one of the most pressing concerns of our age is understanding the various hazards within the technology we use on a daily basis and devising ways to either prevent or remedy them.

One such hazard regards individual security and privacy, which can be put in peril by our partaking in diverse online activities, from the seemingly harmless data collection in social media for advertisement purposes to the more evident risks associated with Internet banking and e-commerce. Therefore, a solid framework for assessing the security liabilities of such systems is paramount for the safety and general well-being of our ever connected society.

In this thesis, we investigate aspects of foundational and practical interest to the field of *Quantitative Information Flow* (QIF). A central focus of recent research in QIF has been to establish a robust framework to quantify sensitive information leakage in computational systems, enabling us to properly assess security risks in real-life scenarios. The traditional approach to QIF, however, models systems as monolithic blocks represented as *information-theoretic channels*. This approach overlooks the fact that most realistic systems are the composition of many interacting parts. In this thesis we focus on extending the QIF framework to facilitate the analysis of large or complex systems that can be described as *compositions* of smaller components.

1.1 Quantitative Information Flow

Protecting sensitive information from unintended disclosure is a crucial research topic in computational security. Intuitively, it may seem that we should always aim at completely eradicating any leakage of sensitive information in our systems. This stance, however, can be so restrictive in practice as to render many desirable system functionalities impossible to be implemented, and we must face the fact that *some* information leakage is often inevitable. An execution of a password checker, for example, will always leak some information about the secret password kept by the system, as it will be always revealed whether or not the user's input was the correct password.

We rely on systems such as password checkers not because they are leakage-free, but because we intuitively understand that the amount of information they reveal is acceptably small. It follows from this intuition, therefore, the need to develop a mathematical framework within which we can not only identify the occurrence of information leakage but also *quantify* it. The field of *Quantitative Information Flow* (QIF) takes interest in studying *how much* information systems leak, and in developing techniques to prevent those leaks.

Being mainly interested in quantifying information, many of the foundational aspects of QIF are based on *Information Theory*, and a number of information-theoretic frameworks have been successfully used to model security systems. These models usually describe the secret or sensitive information in question as a *secret input* (or simply *secret*) which is fed to the system. This input can be a number of different things, including passwords, users' identities or locations. The value of this secret is object to the ambition of an *adversary*, an external observer who wishes to obtain information about the secret input value. We model the knowledge that the adversary has about the secret by a *probability distribution* over the possible values that the secret can take. In particular, before the first execution of the system, the adversary is assumed to have some *prior* knowledge about the secret, which we model by a *prior* distribution. For example, if the adversary knows the secret to be defined by a randomly generated string, his prior knowledge can be represented by a uniform probability distribution on the set of all randomly generated strings.

The secret value can interfere with the system's behaviour that is visible to the adversary (such as execution time, dissipated heat, or the value of a public variable), who might improve his knowledge of the secret value by factoring in the information obtained by observing the system. We model the system as an *information-theoretic channel*, which is a simple yet useful model that abstracts away any specificities of the systems not linked to information leakage. This channel reflects the probability that an execution of the system will yield a certain *public output* given a secret value. Whenever the system is run and produces a public output, we are able to use the channel to model the new state of knowledge of the adversary, which is another probability distribution obtained from the prior distribution via *Bayesian updating*. We call the updated distribution a *posterior distribution*.

In order to quantify *how much* information the adversary currently possesses we need to use an *information measure*, which is a function that maps probability distributions to real numbers. This function yields how much information each probability distribution contains, enabling us to assess how vulnerable the secret is at the current state of knowledge of the adversary. We then take the value yielded by the prior distribution under this measure as the *prior vulnerability* of the secret, and average the value of this function over all possible posterior distributions — one for each output — to obtain the *posterior vulnerability* of the secret after the run of a system. By comparing the posterior and prior vulnerabilities, we are able to assess by how much the system increases the vulnerability of the secret, and therefore acquire a better understanding of its security properties.

Far from being trivial, the choice of information measure is the subject of ongoing discussion in the literature, some of which we give a brief overview in Chapter 2. Recently, Alvim et al. [2012] proposed the *g-leakage* framework, which was shown by Alvim et al. [2016] to generalize any reasonable information measure (i.e., that satisfies some intuitive information-theoretic properties). Having this versatile characteristic of the g-leakage framework in mind, we concentrate our investigations in this thesis on this framework.

1.2 Thesis objective: g-leakage properties of channel compositions

Having been proposed only in 2012, it is not surprising that there is much foundational work to be done regarding the g-leakage framework and its properties. One aspect of this framework in which more in-depth studies have only recently begun is its behaviour regarding *channel compositions* [Kawamoto et al., 2017; Engelhardt, 2017; Alvim et al., 2018]. A channel composition is a combination of two or more channels that can be itself regarded as a channel. The study of the g-leakage properties of channel compositions is paramount for future applications of the framework as it enables, on a number of occasions, a simpler or faster approach to either modelling a system as a channel or studying the leakage properties of a given channel.

There are at least two clear problems in QIF that would benefit from research on channel compositions. The first one concerns the very task of modelling real-life systems as information-theoretic channels. Despite channels being relatively simple objects, obtaining a correct model can be a challenge in itself, and numerous tools have been used for that end, such as probabilistic model checking [Chatzikokolakis et al., 2008; Kawamoto et al., 2017; Américo et al., 2017] and reachability analysis of probabilistic automata [Andrés et al., 2010]. In many cases, the system of interest can be naturally described as a composition of simpler or smaller parts, and its modelling can benefit greatly by a well-established framework that contemplates channel compositions.

A second problem that can benefit from our investigations emerges when the channel itself is very large — i.e., with a large number of possible secret values and producible behaviours. In such situations, a direct calculation of the leakage properties of a channel might be computationally infeasible. A compositional approach, however, can sometimes circumvent this issue, allowing us to infer some of the larger channel g-leakage properties in terms of that of its components.

Concisely, we can define the main objective of this thesis as follows.

Main objective: Study the g-leakage properties of channel compositions, and establish results regarding how they are related to the g-leakage properties of their components.

1.2.1 Specific objectives

In this section, we present two specific objectives of this thesis. The first and more straightforward one is to find a way to determine how much information a composition of channels leaks solely by evaluating its components.

First specific objective: Vulnerabilities of channel compositions Given two channels and their composition,

1. Can we establish how much information the composition leaks by examining how much each channel leaks individually?
2. Failing that, can we at least establish upper and lower bounds to the leakage of the composition in terms of the leakage of their components?

Our second specific objective is based on a question of practical interest: given a composition of channels, are we able to substitute one channel for a *safer* one without compromising the security of the composition?

More formally, we can state this goal as follows.

Second specific objective: relative monotonicity of compositions Consider two channels C_1 and C_2 such that the information leakage of C_1 is never greater than the information leakage of C_2.

1. Given a third channel C, is the information leakage of the composition of C_1 and C less than or equal to that of the composition of C_2 and C? In other words, is it possible to ensure that the overall leakage of a system does not increase if we decrease the leakage of its individual components?

2. Conversely, for two channels C_1, C_2, if the composition of C_1 and C does not leak more information than the composition of C_2 and C for any channel C, can we deduce that C_1 does not leak more information than C_2?

1.3 A motivating example: the Dining Cryptographers protocol

The compositional approach we present in this thesis seems particularly natural for modelling security protocols, which often involve interactions among various entities. In this section, we give an idea of how our framework can be applied to model the well-known *Dining Cryptographers* anonymity protocol, proposed by Chaum [1988].

The protocol is usually explained in the following way. A group of n cryptographers has been invited for dinner by the NSA (American National Security Agency), who will either pay the bill, or secretly ask one of the cryptographers to be the payer. The cryptographers want to determine whether one among them is the payer, or whether the NSA is, but maintaining the payer identity unrevealed in the former case. For that, they execute the following protocol. Sitting on a round table, each cryptographer tosses a coin and privately shares the result only with the cryptographer to his right. Therefore, each cryptographer knows the result of two tosses, his own and that of the participant to his left.

After tossing his coin and sharing his result, each cryptographer makes a public announcement based on the coins he observed. If the cryptographer is not paying the bill, he announces 0 if the two coins he saw landed on the same face, or 1 if they disagreed. If he was asked to be the payer, however, he will invert the announcement, saying 1 if the coins agreed with each other and 0 if they did not.

Representing a coin toss that landed on heads by 1 and one that landed on tails by 0, a non-paying cryptographer is simply outputting the exclusive-or of the two results he had access to. Let us first analyse what happens whenever the NSA is paying the bill. In this case, if we take the exclusive-or of all cryptographers' outputs, it will be the same as taking the exclusive-or of all coins twice, as each coin is shared between two participants. Therefore, whenever the NSA is sponsoring the dinner, the exclusive-or of the outputs shall be 0 — or in other words, their sum is even.

If one of the cryptographers is paying, however, the sum of all announcements will be either increased or decreased by one. Thus, by undertaking this protocol, the cryptographers can infer that the NSA is paying for the dinner if, and only if, the sum off all their announcements is even. Chaum [1988] showed that, if all coins are fair, no information is leaked about who the paying cryptographer is — i.e., neither the non-paying cryptographers, nor any external observer obtains any information about the payer's identity, if it is not the NSA.

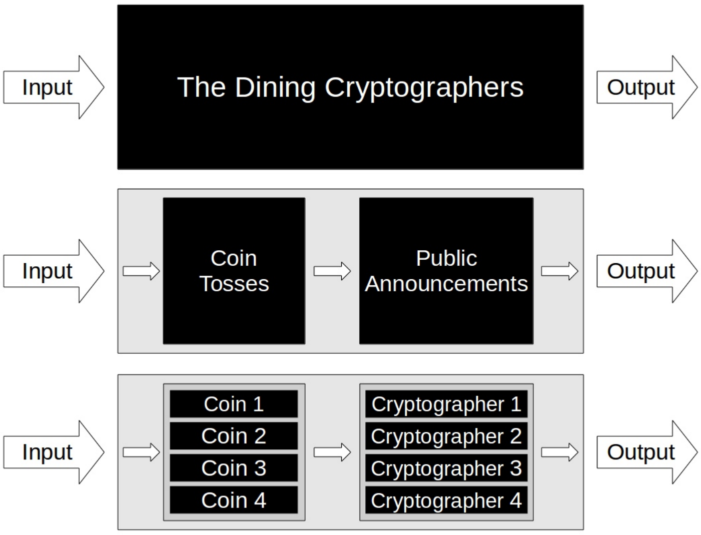

Figure 1.1. Schematic representation of the Dining Cryptographers protocol as: (i) a monolithic channel (top); (ii) a composition of two channels (middle); and (ii) a composition of eight channels (bottom).

Despite the Dining Cryptographers relative simplicity, deriving its channel can be a challenging task. Since each of the n cryptographers can announce either 0 or 1, the size of the output set and, consequently, of the channel, increases exponentially with the number of cryptographers. The problem is worsened by the fact that computing the probabilities constituting the entries of the channel is not trivial. The algebra we introduce in this thesis allows for an intuitive and compositional way of building a channel for a protocol from each of its components.

To illustrate the concept, Figure 1.3 depicts three alternative representations, using channels, for the Dining Cryptographers with 4 cryptographers and 4 coins. In all models, the input is the identity of the payer (one of the cryptographers or the NSA), and the output are the public announcements of all cryptographers. The top model uses a single (enormous) channel to represent the protocol; the middle one models the protocol as the interaction between two smaller components (the coins and the party of cryptographers); the bottom one uses interactions between even smaller channels (one for each coin and each cryptographer).

We will return to this example in Section 3.3, after introducing our operators, to give an explicit modelling of this protocol.

1.4 Contributions

The main contributions of this thesis are the following:

1. A compilation of algebraic and information-theoretic properties of operators that represent compositions of channels based on interactions common to real-life systems. Namely, we investigate the *parallel*, *visible choice*, *hidden choice*, *visible if-then-else* and *hidden if-then-else* operators;

2. An investigation of the algebraic properties of these operators, the results of which are compiled in Section 3.2 . These properties can prove to be helpful tools when studying models described by several channel compositions;

3. Results that address both specific objectives discussed in Section 1.2.1 for each type of channel composition;

4. The modelling of two anonymity protocols well-known in the literature, the Crowds [Reiter and Rubin, 1998] and the Dining Cryptographers [Chaum, 1988]. In particular, we derive an algorithm faster than those in the literature to derive a channel for the latter.

1.5 Related work

Compositionality is a fundamental notion in computer science, being a natural way of inductively building data structures and the basis of many "divide and conquer" algorithms. The development of compositional frameworks for security systems has been subject of growing interest in the QIF community during the past decade.

Espinoza and Smith [2013] derived a number of *min-capacity* bounds for different channel compositions, including cascading and parallel composition.

However, it was not until recently that compositionality results regarding the more general g-leakage information measure started to be explored. Kawamoto et al. [2017] defined a generalization of the parallel operator for channels with different input sets, and gave upper bounds for their corresponding information leakage. Our bound for compatible channels (Theorem 4.2) are tighter than theirs.

Recently, Engelhardt [2017] defined the *mix operator*, another generalization of parallel composition, and derived results similar to ours regarding the parallel operator. Specifically, he provided commutative and associative properties (Equations (3.1) and (3.6)), and from his results the lower bound of Theorem 4.1 can be inferred. He also proved properties similar to Equations (3.16) and (3.19), albeit using more restrictive definitions of null and transparent channels. Both Kawamoto et al. [2017] and Engelhardt [2017] provided results similar to Corollary 4.18.

Just recently, Alvim et al. [2018] investigated some algebraic properties of hidden and visible choice operators in the context of game-theoretic aspects of QIF, and derived Theorems 4.3 and 4.5.

1.6 Thesis roadmap

After this introduction, we present some preliminaries on QIF and the g-leakage framework in Chapter 2. Chapter 3 introduces the different types of compositions we investigate in this thesis, and a list of their algebraic properties.

The results regarding the two specific objectives defined in Section 1.2.1 are detailed in Chapter 4, and are followed by the case studies regarding the Crowds and the Dining Cryptographers protocols in Chapter 5. Finally, Chapter 6 concludes the thesis.

Chapter 2

Preliminaries and Literature Review

In this chapter, we introduce some important results in the literature regarding the g-leakage framework and QIF in general.

2.1 Secrets, knowledge and information

The most basic notion when reasoning about computer security is that of a *secret.* A secret is some sensitive information that should not be disclosed, such as a user's identity, social security number or current location. The *set of secret values* $\mathcal{X}$ is the set of all possible values the secret can take. We assume $\mathcal{X}$ is nonempty and finite.

In the QIF framework, it is assumed the existence of an *adversary* that is interested in obtaining some information regarding the value of the secret. We model the adversary's *knowledge* or *state of knowledge* about the secret as a probability distribution $\pi \in \mathbb{D}\mathcal{X}$, where $\mathbb{D}\mathcal{X}$ is defined as follows.

Definition 2.1. *Let $\mathcal{A}$ be a nonempty and finite set. We define $\mathbb{D}\mathcal{A}$ as the set of all probability distributions over $\mathcal{A}$.*

Given $\pi \in \mathbb{D}\mathcal{A}$, the support of π *is the set $\lceil \pi \rceil = \{a \in \mathcal{A} \mid \pi(a) > 0\}$.*

For example, suppose the secret is a four bit string produced at random. An appropriate choice of the set of secret values would be the set $\mathcal{X} = \{0, 1\}^4$, while the probability distribution which best represents the knowledge of the adversary is the uniform distribution $\pi_u \in \mathbb{D}\mathcal{X}$, given by $\pi_u(x) = {}^1/_{|\mathcal{X}|}$ for all $x \in \mathcal{X}$.

Given a state of knowledge $\pi \in \mathbb{D}\mathcal{X}$, we wish to assess how much *information* the adversary has about the aspects of the secret he is interested in. This is done by a suitable *information-theoretic measure.*

Definition 2.2. *An* information-theoretic measure*, or simply* information measure*, is a function $\phi : \mathbb{D}\mathcal{X} \to \mathbb{R}$.*

Needless to say, not all functions $\mathbb{D}\mathcal{X} \to \mathbb{R}$ constitute a reasonable choice for an information-theoretic measure. A necessary, though not sufficient, condition for an information-theoretic measure to be reasonable is to be either a *vulnerability measure* or an *uncertainty measure*.

Definition 2.3. *A* vulnerability measure *is an information-theoretic measure ϕ such that $\phi(\pi_1) > \phi(\pi_2)$ if, and only if, the adversary possesses more information about the secret with knowledge π_1 than with knowledge π_2.*

Definition 2.4. *An* uncertainty measure *is an information-theoretic measure ϕ such that $\phi(\pi_1) > \phi(\pi_2)$ if, and only if, the adversary possesses more information about the secret with knowledge π_2 than with knowledge π_1.*

We may use the terms *vulnerability* and *uncertainty* instead of *vulnerability measure* and *uncertainty measure*, respectively.

Far from being trivial, the choice of which information measure to use has been subject of much discussion on the literature. We present a brief description of the most common choices in QIF.

2.1.1 Shannon entropy

The first information measure used in QIF was *Shannon entropy* [Shannon, 1948], which is largely used in Information Theory.

The Shannon entropy of a distribution $\pi \in \mathbb{D}\mathcal{X}$ represents, loosely speaking, the minimum average amount of Boolean questions (i.e., questions of the form "is the secret an element of subset $\mathcal{X}' \subset \mathcal{X}$?") an adversary with knowledge π would need to identify the secret value. Hence, it is an uncertainty measure.

Definition 2.5. *Given a nonempty and finite set $\mathcal{X}$, the* Shannon entropy *is the function $H : \mathbb{D}\mathcal{X} \to \mathbb{R}$ defined as*

$$H(\pi) = -\sum_{x \in \mathcal{X}} \pi(x) \log_2(\pi(x)).$$

2.1.2 Guessing entropy

Guessing entropy, first proposed by Massey [1994], is also an uncertainty measure. It measures the expected number of tries an adversary, using an optimal strategy, would need to correctly guess the secret by only asking questions of the type "is the secret value x?".

Definition 2.6. *Given a nonempty and finite set $\mathcal{X}$, the* guessing entropy *is the function $G : \mathbb{D}\mathcal{X} \to \mathbb{R}$ defined as*

$$G(\pi) = \sum_{i=1}^{|\mathcal{X}|} i\pi(x_i),$$

where $\{x_i\}_{i\in\{1,\dots,|\mathcal{X}|\}}$ is an indexing of $\mathcal{X}$ such that $i < j \implies \pi(x_i) \geq \pi(x_j)$.

2.1.3 Bayes vulnerability

It was noted by Smith [2009] that both Shannon entropy and guessing entropy are not appropriate to model scenarios in which the adversary has only one shot at guessing the secret correctly.

For example, suppose $\mathcal{X} = \{x_1, x_2, x_3, ..., x_9\}$, and consider two probability distributions $\pi_1, \pi_2 \in \mathbb{D}\mathcal{X}$, given by

$$\pi_1(x_i) = \begin{cases} {}^1\!/_2, & \text{if } i = 1, \\ {}^1\!/_{16}, & \text{otherwise.} \end{cases} \qquad \pi_2(x_i) = \begin{cases} {}^1\!/_4, & \text{if } i \leq 4, \\ 0, & \text{otherwise.} \end{cases}$$

If the adversary is interested in guessing the secret value correctly in one try, π_1 should represent a state of knowledge containing more information than π_2, since the odds of getting the result correct on the first case are 50%, while being only 25% on the latter. However, Shannon entropy yields

$$H(\pi_1) = \frac{1}{2} + 8 \times 4 \times \frac{1}{16} = \frac{5}{2}, \quad H(\pi_2) = 4 \times 2 \times \frac{1}{4} = 2,$$

while guessing entropy gives us

$$G(\pi_1) = \frac{1}{2} + \frac{8(9+2)}{2} \times \frac{1}{16} = \frac{13}{4}, \quad G(\pi_2) = \frac{4(1+5)}{2} \times \frac{1}{4} = 3.$$

Being uncertainty measures, both Shannon and Guessing entropies therefore deem that the adversary is better served with knowledge π_2 than π_1.

To address this issue, Smith suggested the use of *Bayes vulnerability* as an information measure.

Definition 2.7. *Given a nonempty and finite set $\mathcal{X}$, the* Bayes vulnerability *is the function $V : \mathbb{D}\mathcal{X} \to \mathbb{R}$ defined as,*

$$V(\pi) = \max_{x \in \mathcal{X}} \pi(x).$$

As its name suggests, the Bayes vulnerability is a vulnerability measure. Its value reflects simply the probability the adversary has of guessing the secret correctly in one try, if he picks a best guess according to his knowledge.

2.1.4 g-vulnerability

We now define g-vulnerability, the information measure used on the g-leakage framework, and the one we will focus on the rest of this thesis.

Implicit in the definition of Bayes Vulnerability is the assumption that the only interest of the adversary is obtaining the secret value exactly, and in one try. However, there are several situations in which this assumption is inaccurate, as the adversary may be satisfied by learning the secret value only partially, or after several guesses. For example, an adversary can benefit from knowing the neighbourhood of a user, despite his complete address being out of reach; and any intruder would not be unhappy by managing to invade a system only after guessing the pass-code in his third try.

To model the above scenarios, and many others, Alvim et al. [2012] introduced the g-leakage framework. This framework proposed a vulnerability measure that is predicated in a *gain function g*.

Definition 2.8. *Let $\mathcal{W}$ and $\mathcal{X}$ be finite, nonempty sets. A gain function g is a function of type $g : \mathcal{W} \times \mathcal{X} \to [0, 1]$. Given a finite, nonempty set $\mathcal{X}$, we define $\mathbb{G}\mathcal{X}$ as the set of all gain functions over $\mathcal{X}$, i.e.*

$$\mathbb{G}\mathcal{X} = \{g \mid g : \mathcal{W} \times \mathcal{X} \to [0, 1], \textit{ where } \mathcal{W} \subset \mathbb{N} \textit{ is nonempty and finite}\}.$$

We restrict the choice of $\mathcal{W}$ to a finite subset of natural numbers because $\mathbb{G}\mathcal{X}$ would not be a well-defined set otherwise. As the names of the actions themselves are not relevant, this does not affect our framework. A similar approach is taken in Definition 2.15, for the same reason.

The set $\mathcal{W}$ is called the set of *actions* the adversary can take, and $g(w, x)$ represents the gain the adversary obtain by taking action $w \in \mathcal{W}$ when the secret value is $x \in \mathcal{X}$. Unless otherwise stated, we use $\mathcal{W}$ to refer to the action set of the gain function relevant to the context.

Given a probability distribution $\pi \in \mathbb{D}\mathcal{X}$ and a gain function $g \in \mathbb{G}\mathcal{X}$, we define the g-vulnerability of π as the adversary's largest expected gain among all actions.

Definition 2.9. *Given a nonempty and finite set $\mathcal{X}$ and a gain function $g \in \mathbb{G}\mathcal{X}$,* g-vulnerability *is a function $V_g : \mathbb{D}\mathcal{X} \to \mathbb{R}$ defined as, for all $\pi \in \mathbb{D}\mathcal{X}$,*

$$V_g(\pi) = \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \pi(x) g(w, x).$$

2.1.4.1 Some examples of gain-functions

As an illustration of the versatility of the g-leakage framework, we briefly present some interesting examples of gain functions studied by Alvim et al. [2012].

Definition 2.10. *The* identity gain function $g_{id} \in \mathbb{G}\mathcal{X}$ *is a function $g_{id} : \mathcal{X} \times \mathcal{X} \to [0, 1]$ defined as, for all $x, x' \in \mathcal{X}$,*

$$g_{id}(x, x') = \begin{cases} 1 & \textit{if } x = x', \\ 0 & \textit{otherwise.} \end{cases}$$

This gain function makes g-vulnerability coincide with Bayes vulnerability, since

$$V_{g_{id}}(\pi) = \max_{x' \in \mathcal{X}} \sum_{x \in \mathcal{X}} \pi(x) g_{id}(x', x) = \max_{x \in \mathcal{X}} \pi(x) = V(\pi).$$

Therefore, g-vulnerability can be seen as a generalization of Bayes vulnerability.

Definition 2.11. *A gain function $g \in \mathbb{G}\mathcal{X}$ is said to be a* pertinence gain function *if it is a function $g : \mathcal{W} \times \mathcal{X} \to [0, 1]$, where $\mathcal{W} \subset 2^{\mathcal{X}}$ and, for all $W \in \mathcal{W}$, $x \in \mathcal{X}$,*

$$g(W, x) = \begin{cases} 1 & \textit{if } x \in W, \\ 0 & \textit{otherwise.} \end{cases}$$

This family of gain functions is extremely useful whenever the adversary obtains a significant gain by inferring the secret value to be a member of one subset of $\mathcal{X}$.

Two more specific types of pertinence gain functions of practical use are *partition gain functions* and *k-tries gain functions.*

Definition 2.12. *A pertinence gain function $g : \mathcal{W} \times \mathcal{X} \to [0, 1]$ is a* partition gain function *if $\mathcal{W}$ is a partition of $\mathcal{X}$.*

A partition gain function models the scenario when the adversary obtains maximum gain by correctly identifying to which of the subsets of $\mathcal{W}$ the secret value belongs. It can be useful in a number of situations, for example when the sole objective of the adversary is knowing only the first few bits of a secret, or the last numbers of a user's credit card. Note that the identity gain function is a partition gain function whose action set is $\mathcal{W} = \{\{x\} \mid x \in \mathcal{X}\}$.

Definition 2.13. *A pertinence gain function $g : \mathcal{W} \times \mathcal{X} \rightarrow [0,1]$ is a k-*tries gain function *if $\mathcal{W} = \{W \in 2^{\mathcal{X}} \mid |W| \leq k\}$.*

As hinted by its name, k-tries gain function are useful for modelling scenarios in which the adversary can make up to k guesses, being rewarded whenever one of his guesses is correct; a common occurrence, for example, in ATM machines, online banking and email providers.

2.2 Systems and information leakage

2.2.1 Systems as information-theoretic channels

Beside secrets, another fundamental notion in QIF is that of *computational systems* (or simply *systems*), which can be a variety of things, such as security protocols or computer programs. In the QIF framework, a computational system processes a secret and produces a *behaviour* observable to the adversary. We define the *output set* of the system as the set $\mathcal{Y}$ of all the different producible behaviours of the system visible to the adversary. Those behaviours can be, for example, running time, a message printed on the screen, or the value assigned to a public variable.

In our framework, we model a system as an *information-theoretic channel*, or *channel* for short. This representation preserves the information-theoretic properties of the system, while abstracting away its irrelevant technicalities.

Definition 2.14. *Let $\mathcal{X}$, $\mathcal{Y}$ be finite and nonempty sets. An* information-theoretic channel *is a function $C : \mathcal{X} \times \mathcal{Y} \rightarrow [0,1]$, such that $\forall x \in \mathcal{X}, \sum_{y \in \mathcal{Y}} C(x,y) = 1$.*

The sets $\mathcal{X}$ and $\mathcal{Y}$ are referred to as, respectively, the input *and* output *sets of channel C.*

A system with input set $\mathcal{X}$ and output set $\mathcal{Y}$ can be modelled as a channel $C : \mathcal{X} \times \mathcal{Y} \rightarrow [0,1]$ in which $C(x,y)$ is the conditional probability that the system will produce behaviour $y \in \mathcal{Y}$ given that $x \in \mathcal{X}$ is the secret input value. The restriction

$\sum_{y\in\mathcal{Y}} C(x,y) = 1$ guarantees that, for each $x \in \mathcal{X}$, the values of $C(x,y)$ are indeed a probability distribution over $\mathcal{Y}$.

It is sometimes useful to represent channels as matrices, associating a line with each input value and a column with each output value. For example, Table 2.1. represents a channel $C : \mathcal{X} \times \mathcal{Y} \to [0,1]$, where $\mathcal{X} = \{x_1, x_2, x_3\}$ and $\mathcal{Y} = \{y_1, y_2, y_3, y_4\}$. By examining it we can infer that, for example, $C(x_2, y_3) = 1/4$ and $C(x_3, y_1) = 1$.

C	y_1	y_2	y_3	y_4
x_1	$1/2$	$1/4$	$1/8$	$1/8$
x_2	$1/4$	$1/2$	$1/4$	0
x_3	1	0	0	0

Table 2.1. A channel represented as a matrix.

Definition 2.15. *Let $\mathcal{X}$, $\mathcal{Y}$ be finite and nonempty sets. We define $\mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ as the set of all channels that have $\mathcal{X}$ as input set and $\mathcal{Y}$ as output set, and $\mathcal{C}_{\mathcal{X}}$ as the set of all channels that have $\mathcal{X}$ as input set. That is,*

$$\mathcal{C}_{\mathcal{X}}^{\mathcal{Y}} = \{C \,|\, C{:}\mathcal{X} \times \mathcal{Y} \to [0,1] \text{ and } C \text{ is a channel}\},$$
$$\mathcal{C}_{\mathcal{X}} = \{C \,|\, C{:}\mathcal{X} \times \mathcal{Y} \to [0,1] \text{ for some nonempty finite set } \mathcal{Y}{\subset}\mathbb{N}, \text{ and } C \text{ is a channel}\}.$$

For the sake of brevity, when no confusion arises, we may say "let $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$" as a shorthand for "let $\mathcal{X}$, $\mathcal{Y}$ be finite and nonempty sets, and $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$" or, when the input set is already defined, for "let $\mathcal{Y}$ be a finite and nonempty set and $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$".

2.2.2 Knowledge updating and hyper-distributions

We assume that the adversary *knows* the channel corresponding to the system, i.e. he knows the conditional probability of each output value given each secret value. This pessimistic assumption gives a strong guarantee on the amount of information leaked by the system, and is in line with Kerckhoffs's principle, stated by Kerckhoffs [1883] in the context of cryptography systems. According to this principle, a (cryptographic) system should be secure even if the adversary knows everything about the system, but the secret key. This approach is opposed to the idea of guaranteeing *security through obscurity*, in which one relies in the fact that the adversary does not know some aspects of the system.

By observing the behaviour of a system, the adversary may use the channel to update his knowledge — thus obtaining more information about the secret. Let the probability distribution $\pi \in \mathbb{D}\mathcal{X}$ represent the adversary's initial knowledge, also called a *prior distribution* or simply *prior*, and let $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ be the channel modelling the system in question. The prior π and channel C induce a *joint probability distribution* over the set $\mathcal{X} \times \mathcal{Y}$.

$p(x,y)$	y_1	y_2	y_3	y_4
x_1	$1/4$	$1/8$	$1/16$	$1/16$
x_2	$1/12$	$1/6$	$1/12$	0
x_3	$1/6$	0	0	0

Table 2.2. The joint probability distribution induced by $\pi = (1/2, 1/3, 1/6)$ and channel C of Table 2.1.

Definition 2.16. *Given* $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$, $\pi \in \mathbb{D}\mathcal{X}$ *we define their* joint probability distribution $p \in \mathbb{D}(\mathcal{X} \times \mathcal{Y})$ *as* $p(x,y) = \pi(x)C(x,y)$, *for all* $x \in \mathcal{X}$, $y \in \mathcal{Y}$.

We define the marginal distribution $p_{\mathcal{Y}} \in \mathbb{D}\mathcal{Y}$ *as* $p_{\mathcal{Y}}(y) = \sum_{x \in \mathcal{X}} p(x,y)$, *and, for each* $y \in \mathcal{Y}$ *such that* $p_{\mathcal{Y}}(y) > 0$, *the* conditional distribution $p_{\mathcal{X}|y} \in \mathbb{D}\mathcal{X}$ *as* $p_{\mathcal{X}|y}(x) = p(x,y)/p_{\mathcal{Y}}(y)$. *We define* $p_{\mathcal{X}} \in \mathbb{D}\mathcal{X}$ *and* $p_{\mathcal{Y}|x} \in \mathbb{D}\mathcal{Y}$ *analogously.*

Notice that $p_{\mathcal{X}}$ coincides with π and, for all $x \in \mathcal{X}$ such that $\pi(x) > 0$ and for all $y \in \mathcal{Y}$, $p_{\mathcal{Y}|x}(y) = C(x,y)$.

After observing the output $y \in \mathcal{Y}$, the state of knowledge of the adversary changes accordingly, being updated from π to the distribution $p_{\mathcal{X}|y}$ — i.e., the distribution reflecting the probability of each secret value, given behaviour y. We give the name of *posterior distribution* to the distribution modelling the knowledge of the adversary after the execution of the system. Each channel $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ and prior $\pi \in \mathbb{D}\mathcal{X}$ induce a set of posterior distributions, one for each possible output value. As can be seen in Table 2.3, some of these posterior distributions can be identical.

	$p_{\mathcal{X}\|y_1}$	$p_{\mathcal{X}\|y_2}$	$p_{\mathcal{X}\|y_3}$	$p_{\mathcal{X}\|y_4}$
x_1	$1/2$	$3/7$	$3/7$	1
x_2	$1/6$	$4/7$	$4/7$	0
x_3	$1/3$	0	0	0

Table 2.3. The posterior distributions calculated from the joint distribution p in table 2.2.

The effect of channel C can thus be summarized as mapping a prior $\pi \in \mathbb{D}\mathcal{X}$ to a collection of posterior distributions $p_{\mathcal{X}|y}$, each associated with a probability $p_{\mathcal{Y}}(y)$ (in this case, $p_{\mathcal{Y}} = (1/2, 7/24, 7/48, 1/16)$). We can reason concisely about this effect with the aid of the concept of *hyper-distributions* over the set of secrets.

Definition 2.17. *Let $\mathcal{X}$ be a finite and nonempty set. $\mathbb{D}(\mathbb{D}\mathcal{X})$, also denoted by $\mathbb{D}^2\mathcal{X}$, is the set of probability distributions over $\mathbb{D}\mathcal{X}$ with finite support, where the support of $\Delta \in \mathbb{D}^2\mathcal{X}$ is the set $\lceil\Delta\rceil = \{\pi \in \mathbb{D}\mathcal{X} \mid \Delta(\pi) > 0\}$.*

An element $\Delta \in \mathbb{D}^2\mathcal{X}$ is called a hyper-distribution *over $\mathcal{X}$. We refer to the elements of $\lceil\Delta\rceil$ as the* inner distributions *of Δ, and to the probability distribution Δ over $\lceil\Delta\rceil$ (that is, the distribution over the inner distributions) as the* outer distribution.

Definition 2.18. *Let $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ and $\pi \in \mathbb{D}\mathcal{X}$. Let $p \in \mathbb{D}(\mathcal{X}\times\mathcal{Y})$ be their joint probability distribution. The hyper-distribution $[\pi \rangle C] \in \mathbb{D}^2\mathcal{X}$ is defined as, for all $\delta \in \mathbb{D}\mathcal{X}$,*

$$[\pi \rangle C](\delta) = \sum_{y \in \lceil p_{\mathcal{Y}} \rceil ; p_{\mathcal{X}|y} = \delta} p_{\mathcal{Y}}(y).$$

That is, $[\pi \rangle C]$ is the hyper-distribution whose inner distributions are the posterior distributions obtained from π and C. In Definition 2.18, it is necessary to limit the possible values of y to $\lceil p_{\mathcal{Y}} \rceil$, as $p_{\mathcal{X}|y}$ might be undefined otherwise. Note that identical distributions are merged, as depicted in Table 2.4.

$[\pi \rangle C]$	$1/2$	$7/16$	$1/16$
x_1	$1/2$	$3/7$	1
x_2	$1/6$	$4/7$	0
x_3	$1/3$	0	0

Table 2.4. The hyper-distribution $[\pi \rangle C]$, where $\pi = (1/2, 1/3, 1/6)$ and C is the channel given in Table 2.1. The outer distribution is depicted in the first line, and the inner distributions on the columns.

2.2.3 Posterior information measures and information leakage

To calculate how much information a system leaks, we need a measure that can be applied to hyper-distributions of the type defined on Definition 2.18. For that end, we define the concept of *posterior information measures.*

Definition 2.19. *Let $\phi : \mathbb{D}\mathcal{X} \to \mathbb{R}$ be an information measure. We associate with it a* posterior information measure *$\widehat{\phi} : \mathbb{D}^2\mathcal{X} \to \mathbb{R}$, defined by, for all $\Delta \in \mathbb{D}^2\mathcal{X}$,*

$$\widehat{\phi}\Delta = \sum_{\delta \in \lceil\Delta\rceil} \Delta(\delta)\phi(\delta).$$

The next result shows that a posterior information measure gives us the expected value of the associated information measure after the execution of the system.

Proposition 2.20. *Let $\mathcal{X}$ be a nonempty and finite set, $\phi : \mathbb{D}\mathcal{X} \to \mathbb{R}$ be an information measure, and $\widehat{\phi} : \mathbb{D}^2\mathcal{X} \to \mathbb{R}$ be its associated posterior information measure. Then, for all $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ and all $\pi \in \mathbb{D}\mathcal{X}$,*

$$\widehat{\phi}[\pi \rangle C] = \sum_{y \in \lceil p_{\mathcal{Y}} \rceil} p_{\mathcal{Y}}(y)\phi(p_{\mathcal{X}|y}).$$

Proof.

$$\begin{aligned}
&\widehat{\phi}[\pi \rangle C] \\
&= \sum_{\delta \in \lceil [\pi \rangle C] \rceil} [\pi \rangle C](\delta)\phi(\delta) && \text{(by Def. 2.19)} \\
&= \sum_{\delta \in \lceil [\pi \rangle C] \rceil} \left(\sum_{y \in \lceil p_{\mathcal{Y}} \rceil; p_{\mathcal{X}|y} = \delta} p_{\mathcal{Y}}(y) \right) \phi(\delta) && \text{(by Def. 2.18)} \\
&= \sum_{\delta \in \lceil [\pi \rangle C] \rceil} \sum_{y \in \lceil p_{\mathcal{Y}} \rceil; p_{\mathcal{X}|y} = \delta} p_{\mathcal{Y}}(y)\phi(p_{\mathcal{X}|y}) && (\delta = p_{\mathcal{X}|y}) \\
&= \sum_{y \in \lceil p_{\mathcal{Y}} \rceil} p_{\mathcal{Y}}(y)\phi(p_{\mathcal{X}|y}) && (\forall y \in \lceil p_{\mathcal{Y}} \rceil,\ \exists! \delta \in \lceil [\pi \rangle C] \rceil;\ \delta = p_{\mathcal{X}|y})
\end{aligned}$$

□

If $\phi(\pi)$ correctly models the amount of information the adversary has when his state of knowledge is $\pi \in \mathbb{D}\mathcal{X}$, $\widehat{\phi}[\pi \rangle C]$ is simply the expected value of the adversary's amount of information after he updates his knowledge by observing the behaviour of the system.

As this thesis is focused on the g-leakage framework, we instantiate Definition 2.19 to obtain the *posterior g-vulnerability* $\widehat{V_g} : \mathbb{D}^2\mathcal{X} \to \mathbb{R}$. Following the literature, we overload the notation and usually refer to it by the same symbol as the regular g-vulnerability, V_g. Given a channel $C \in \mathcal{C}_{\mathcal{X}}$ and a prior $\pi \in \mathbb{D}\mathcal{X}$, we refer to $V_g[\pi \rangle C]$ as the *posterior g-vulnerability of channel C w.r.t. prior π.*

Example 2.21. *Consider the posterior distributions depicted in Table 2.3. Using Proposition 2.20, we can calculate the posterior g-vulnerability of C with regard to $\pi = (1/2, 1/3, 1/6)$ and the identity gain function g_{id} as follows*

$$\begin{aligned}
V_{g_{id}}[\pi \rangle C] &= \sum_{y \in \mathcal{Y}} p_{\mathcal{Y}}(y) V_{g_{id}}(p_{\mathcal{X}|y}) \\
&= \sum_{y \in \mathcal{Y}} p_{\mathcal{Y}}(y) \max_{x \in \mathcal{X}} \left(p_{\mathcal{X}|y}(x) \right)
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{2} \times \frac{1}{2} + \frac{7}{24} \times \frac{4}{7} + \frac{7}{48} \times \frac{4}{7} + \frac{1}{16} \times 1 \\
&= \frac{9}{16} .
\end{aligned}
$$

Therefore, the execution of a system modelled by C increases the g-vulnerability of the secret from $V_{g_{id}}(\pi) = 1/2$ to $V_{g_{id}}[\pi \rangle C] = 9/16$.

The next proposition gives us an alternative way of defining the *g-vulnerability* of a channel w.r.t. a prior. This alternative is usually simpler in a number of situations, and we will use it when proving many of our results.

Proposition 2.22. *Let $g \in \mathbb{G}\mathcal{X}$, $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ and $\pi \in \mathbb{D}\mathcal{X}$. Then,*

$$V_g[\pi \rangle C] = \sum_{y \in \mathcal{Y}} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \pi(x) C(x,y) g(w,x).$$

Proof.

$$
\begin{aligned}
& V_g[\pi \rangle C] \\
&= \sum_{y \in \lceil p_{\mathcal{Y}} \rceil} p_{\mathcal{Y}}(y) V_g(p_{\mathcal{X}|y}) && \text{(by Prop. 2.20)} \\
&= \sum_{y \in \lceil p_{\mathcal{Y}} \rceil} p_{\mathcal{Y}}(y) \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} p_{\mathcal{X}|y}(x) g(w,x) && \text{(by Def. 2.9)} \\
&= \sum_{y \in \lceil p_{\mathcal{Y}} \rceil} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} p(x,y) g(w,x) && (p(x,y) = p_{\mathcal{X}|y}(x) p_{\mathcal{Y}}(y)) \\
&= \sum_{y \in \lceil p_{\mathcal{Y}} \rceil} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \pi(x) C(x,y) g(w,x) && \text{(by Def. 2.16)} \\
&= \sum_{y \in \mathcal{Y}} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \pi(x) C(x,y) g(w,x) && (\forall y \notin \lceil p_{\mathcal{Y}} \rceil,\ \pi(x) C(x,y) = 0)
\end{aligned}
$$

□

Having defined the posterior g-vulnerability, we are able to define the leakage of information occurring when an adversary with knowledge $\pi \in \mathbb{D}\mathcal{X}$ observes a system modelled by $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$.

Definition 2.23. *Let $g \in \mathbb{G}\mathcal{X}$, $\mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ and $\pi \in \mathbb{D}\mathcal{X}$. We define the* multiplicative g-leakage *of C with regard to π as*

$$\mathcal{L}_g[\pi \rangle C] = \frac{V_g[\pi \rangle C]}{V_g(\pi)},$$

and the additive g-leakage *of* C *with regard to* π *as*

$$\mathcal{L}_g^+[\pi\rangle C] = V_g[\pi\rangle C] - V_g(\pi).$$

The multiplicative and additive forms of g-leakage have both been studied in the literature [Alvim et al., 2012, 2014], the former being a useful quantity when the *ratio* of the posterior and prior information are of interest, and the latter when one wants to reason about information leakage as an absolute value of information increase. The choice between them should be made taking into consideration the specifics of the problem at hand, and neither are considered "canonical" in the literature.

Note that, as $V_g(\pi)$ does not depend on the channel, we have for any two channels $C_1, C_2 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$

$$\mathcal{L}_g[\pi\rangle C_1] \leq \mathcal{L}_g[\pi\rangle C_2] \Leftrightarrow \mathcal{L}_g^+[\pi\rangle C_1] \leq \mathcal{L}_g^+[\pi\rangle C_2] \Leftrightarrow V_g[\pi\rangle C_1] \leq V_g[\pi\rangle C_2].$$

Therefore, we can simply compare the appropriate posterior g-vulnerabilities whenever we want to establish whether a channel leaks more information than another.

We finish this section with an interesting result regarding g-vulnerabilities, established by Alvim et al. [2012]. This theorem proves that the g-leakage framework respects an important and intuitive property: the information an adversary has about a secret is never expected to decrease when he observes the output of a system.

Theorem 2.24. *Let* $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$*,* $\pi \in \mathbb{D}\mathcal{X}$ *and* $g \in \mathbb{G}\mathcal{X}$*. Then,*

$$V_g[\pi\rangle C] \geq V_g(\pi).$$

Proof.

$$\begin{aligned}
&V_g[\pi\rangle C] \\
=&\sum_{y\in\mathcal{Y}} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} \pi(x)C(x,y)g(w,x) && \text{(by Prop 2.22)} \\
\geq&\max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} \pi(x)g(w,x) \sum_{y\in\mathcal{Y}} C(x,y) && \text{(moving max outside a sum)} \\
=&\max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} \pi(x)g(w,x) && \text{(C is a channel)} \\
=&V_g(\pi) && \text{(by Def. 2.9)}
\end{aligned}$$

□

2.3 Channel ordering and equivalence

In this section, we investigate the properties that relate channels to their leakage, obtaining a preorder among channels and a notion of equivalence. Some of these ideas were proposed by Alvim et al. [2012], and were subsequently explored in depth by McIver et al. [2014].

2.3.1 Abstract channels and reduced matrices

In this section we introduce *abstract channels* and *reduced matrices*. Loosely speaking, these objects abstract aspects of channels that are irrelevant to their leakage properties (such as input and output labels, or redundant outputs), and focus on the essential information-theoretic ones. As we will see in Theorem 2.27, despite their different formulations, abstract channels and reduced matrices are equivalent concepts.

As discussed on Section 2.2.3, the information leaked by a channel C, according to a prior π, can be totally captured by the hyper-distribution $[\pi \rangle C]$. Aiming at abstracting away all other irrelevant properties of the channel, we define its abstract channel as follows.

Definition 2.25. *Let $C \in \mathcal{C}_{\mathcal{X}}$. The* abstract channel *of C is a mapping from $\mathbb{D}\mathcal{X}$ to $\mathbb{D}^2\mathcal{X}$, given by $\pi \mapsto [\pi \rangle C]$, for all $\pi \in \mathbb{D}\mathcal{X}$.*

Note that abstract channels provide a fully functional characterization of the behaviour of a channel. Sometimes, however, it is convenient to have a concrete, canonical matrix-like representation of the function corresponding to a channel. Reduced matrices do the job by ditching all input and output labels, and aggregating outputs that induce the same posterior distribution for all priors.

Definition 2.26. *Let $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$. The reduced matrix $[C^r]$ of channel C is a matrix obtained by the following procedure:*

1. *Index $\mathcal{X}$ and $\mathcal{Y}$, such that $\mathcal{X} = \{x_1, x_2, ..., x_{|\mathcal{X}|}\}$ and $\mathcal{Y} = \{y_1, y_2, ..., y_{|\mathcal{Y}|}\}$;*

2. *Define a matrix $[C]$ with $|\mathcal{X}|$ lines and $|\mathcal{Y}|$ columns, whose entry on line i and column j is equal to $C(x_i, y_j)$;*

3. *Eliminate all columns consisting entirely of zeros;*

4. *Add together all columns that are scalar multiples of each other;*

5. *Order the columns lexicographically.*

The lexicographically ordering of the columns at the end guarantees that to each channel C corresponds a unique reduced matrix $[C^r]$. As the following theorem by McIver et al. [2014] indicates, the two concepts above are equivalent.

Theorem 2.27. *Let C_1, $C_2 \in \mathcal{C}_\mathcal{X}$ be two channels. $[C_1^r] = [C_2^r]$ if, and only if, the abstract channel of C_1 is identical to the abstract channel of C_2.*

The intuition of the proof of this theorem is that a channel whose matrix is $[C^r]$ will always produce the same hyper-distribution as C for each prior, as it is not affected by any of the steps on Definition 2.26.

The following example illustrates the concepts defined above. It emphasizes the fact that channels with different matrices representations may, in fact, correspond to the same abstract channel and reduced matrix; being equivalent from an information-theoretic standpoint.

Example 2.28. *Consider the following channels C_1 and C_2.*

C_1	y_1	y_2	y_3
x_1	$^2/_5$	0	$^3/_5$
x_2	$^1/_8$	$^1/_2$	$^3/_8$
x_3	$^2/_{15}$	$^2/_3$	$^1/_5$

C_2	z_1	z_2	z_3
x_1	1	0	0
x_2	$^1/_2$	$^2/_7$	$^3/_{14}$
x_3	$^1/_3$	$^8/_{21}$	$^2/_7$

Despite perhaps appearing very different, by following the steps on Definition 2.26 we obtain

$$[C_1^r] = [C_2^r] = \begin{bmatrix} 1 & 0 \\ ^1/_2 & ^1/_2 \\ ^1/_3 & ^2/_3 \end{bmatrix}.$$

Which implies, by Theorem 2.27, that C_1 and C_2 have the same abstract channel. In fact, let $\pi = (p_1, p_2, p_3)$ be a distribution over the set $\mathcal{X} = \{x_1, x_2, x_3\}$. We have that, for all $\delta \in \mathbb{D}\mathcal{X}$,

$$[\pi\rangle C_1](\delta) = [\pi\rangle C_2](\delta) = \begin{cases} \frac{6p_1+3p_2+2p_3}{6}, & \textit{if } \delta = (\frac{6p_1}{6p_1+3p_2+2p_3}, \frac{3p_2}{6p_1+3p_2+2p_3}, \frac{2p_3}{6p_1+3p_2+2p_3}), \\ \frac{3p_2+4p_3}{6}, & \textit{if } \delta = (0, \frac{3p_2}{3p_2+4p_3}, \frac{4p_3}{3p_2+4p_3}), \\ 0, & \textit{otherwise.} \end{cases}$$

2.3.2 Cascading and leakage ordering

Cascading is a concept of fundamental importance on QIF. Intuitively, it models the scenario in which the output of a system is fed as input to another system — in which case we say that the output of the former is *post-processed* by the latter. It arises in a number of real-world systems; for example, when some noise is introduced to mask the physical location of a device, or simply when a computer program uses the output of another program as its input.

Despite its apparent simplicity, cascading plays a pivotal role in ordering channels according to their information leakage.

Definition 2.29. *Let $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$, $D \in \mathcal{C}_{\mathcal{Y}}^{\mathcal{Z}}$ be channels such that the output set of C is equal to the input set of D. We define their* cascade *$(CD) \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Z}}$ as, for all $x \in \mathcal{X}$, $z \in \mathcal{Z}$,*

$$(CD)(x,z) = \sum_{y\in\mathcal{Y}} C(x,y)D(y,z).$$

That a cascading of two channels is a channel can be readily seen, as

$$\begin{aligned}
&\sum_{x\in\mathcal{X}}(CD)(x,z) \\
=&\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} C(x,y)D(y,z) && \text{(by Definition 2.29)} \\
=&\sum_{y\in\mathcal{Y}} D(y,z)\sum_{x\in\mathcal{X}} C(x,y) && \text{(rearranging)} \\
=&\sum_{y\in\mathcal{Y}} D(y,z) && \text{(C is a channel)} \\
=&1 && \text{(D is a channel)}
\end{aligned}$$

Notice that, having the matrix representation of C and D in mind, CD can be understood as a matrix multiplication.

Definition 2.30. *Let $C_1, C_2 \in \mathcal{C}_{\mathcal{X}}$. We say that C_2 is* refined *by C_1, and write $C_2 \sqsubseteq_\circ C_1$, if there is a channel R such that $C_1 = C_2R$. We write $C_1{}_\circ\sqsupseteq C_2$ if $C_2 \sqsubseteq_\circ C_1$.*

We say that C_1 and C_2 are equivalent, *and write $C_1 \approx C_2$, if $C_1 \sqsubseteq_\circ C_2$ and $C_1{}_\circ\sqsupseteq C_2$.*

We refer to $\sqsubseteq_\circ$ as the refinement *relation, ${}_\circ\sqsupseteq$ as the* anti-refinement *relation and $\approx$ as the* equivalence *relation.*

There is a strict relation between the equivalence relation defined above and the notion of abstract channel, proved by McIver et al. [2014].

Theorem 2.31. *Let C_1, $C_2 \in \mathcal{C}_\mathcal{X}$. $C_1 \approx C_2$ if, and only if, $[C_1^r] = [C_2^r]$.*

Intuitively, if $C_1 = C_2R$, it must not be possible to obtain more information from C_1 than from C_2 since, once in possession of C_2, we can simply feed its output to R to obtain C_1. This intuition is formalized in the following important result, conjectured by Alvim et al. [2012] and finally proved by McIver et al. [2014].

Theorem 2.32 (The Coriaceous Theorem)**.** *Let C_1, $C_2 \in \mathcal{C}_\mathcal{X}$. $C_2 \sqsubseteq_\circ C_1$ if, and only if, $V_g[\pi \rangle C_1] \leq V_g[\pi \rangle C_2]$ for all $g \in \mathbb{G}\mathcal{X}$ and all $\pi \in \mathbb{D}\mathcal{X}$.*

Theorem 2.32 implies that the refinement relation ($\sqsubseteq_\circ$) coincides with our notion of security: if a channel C_2 is refined by a channel C_1, then C_1 never leaks more information about the secret than C_2. This relationship is of great practical value, since checking whether the refinement relation holds between two channels can be simplified to checking whether one can be described as a cascading in which the other is the first term.

We finish this section with a Corollary that summarizes the relation between abstract channels, reduced matrices, the equivalence relation ($\approx$) and posterior g-vulnerabilities.

Corollary 2.33. *Let $C_1, C_2 \in \mathcal{C}_\mathcal{X}$. The following statements are equivalent.*

1. *C_1 and C_2 have the same abstract channel;*
2. *$[C_1^r] = [C_2^r]$;*
3. *$C_1 \approx C_2$;*
4. *$\forall g \in \mathbb{G}\mathcal{X}$, $\forall \pi \in \mathbb{D}\mathcal{X}$, $V_g[\pi \rangle C_1] = V_g[\pi \rangle C_2]$.*

2.4 Expressiveness of the g-leakage framework

The versatile nature of the g-leakage framework, as demonstrated in Section 2.1.4.1, would be enough to justify the study of its properties. However, the framework can be extended to be even more expressive than what our examples suggest.

Alvim et al. [2016] proved that, if we allow for gain functions with countably infinite sets of guesses and negative values, the g-leakage framework can capture any vulnerability measure that satisfies a set of intuitively-reasonable information-theoretic axioms.

Before we enter into the details, we extend the g-leakage framework in the following manner. Given a set of secret values $\mathcal{X}$, we first allow the set of actions to be countably infinite, extending the set of gain functions from $\mathbb{G}\mathcal{X}$ to the set

$$\mathcal{G}\mathcal{X} = \{g \,|\, g : \mathcal{W} \times \mathcal{X} \to \mathbb{R}; \text{ where } \mathcal{W} \subset \mathbb{N} \text{ is nonempty and } \\ \forall \pi \in \mathbb{D}\mathcal{X}\, \exists w \in \mathcal{W}; \sum_{x \in \mathcal{X}} \pi(x) g(w,x) \geq 0\}.$$

Given $g \in \mathcal{G}\mathcal{X}$, we redefine g-vulnerability as $V_g[\pi] = \sup_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \pi(x) g(w,x)$.

The expressiveness of this extension of the g-leakage framework can be summarized by the following result, proved by Alvim et al. [2016].

Theorem 2.34. *Let $\mathcal{X}$ be a set of secret values. let $\phi : \mathbb{D}\mathcal{X} \to \mathbb{R}$ be a vulnerability measure, and let $\widehat{\phi} : \mathbb{D}^2\mathcal{X} \to \mathbb{R}$ be its associated* posterior measure *(as in Definition 2.19), such that the following properties hold*

1. *ϕ is continuous over $\mathbb{D}\mathcal{X}$;*

2. *Given $C_1, C_2 \in \mathcal{C}_\mathcal{X}$, if $C_2 \sqsubseteq_\circ C_1$, then $\widehat{\phi}[\pi \rangle C_1] \leq \widehat{\phi}[\pi \rangle C_2]$ for all $\pi \in \mathbb{D}\mathcal{X}$.*

Then $\exists g \in \mathcal{G}\mathcal{X}$ such that $\phi = V_g$. Conversely, for any $g \in \mathcal{G}\mathcal{X}$, V_g is a vulnerability measure that respects both properties above.

Alvim et al. argues that the two properties in Theorem 2.34 are intuitively-reasonable axioms any vulnerability measure should respect. The continuity property captures the idea that very small changes on the probability distribution over the set of secret values should not yield extreme differences on the vulnerability of the secret.

Meanwhile, property 2 guarantees that no information is gained by post-processing an output of a channel. As we discussed in Section 2.3.2, this is an intuitive requirement: if C_1 and C_2 are channels such that $C_1 = C_2 R$ for some channel R, the adversary should be able to simulate C_1 by feeding the output of C_2 to R.

For the remainder of this thesis, we will return to our regular definitions of g-leakage, i.e., we will call by gain functions the elements of the set $\mathbb{G}\mathcal{X}$, and define g-vulnerability as in Definition 2.9.

Chapter 3

Operators and their Algebraic Properties

In this chapter, we formally introduce the operators we studied. Each operator models a type of interaction between components commonly found in real-life systems. Hence, the study of their security properties is of immediate practical value.

After presenting the operators in Section 3.1, we explore some of their algebraic properties in Section 3.2, such as commutativity, associativity and distributivity, among others. These algebraic properties facilitate handling complex system representations, often simplifying their descriptions.

3.1 Introducing the operators

All operators we considered in this thesis are functions that take two channels with the same input set as arguments, and yield a channel also with the same input set. That is, given an input set $\mathcal{X}$, our operators are functions of the form $\mathcal{C}_{\mathcal{X}} \times \mathcal{C}_{\mathcal{X}} \to \mathcal{C}_{\mathcal{X}}$. We call two channels that have the same input set *compatible*. If, beyond that, they also share the same output set, we say that they are of the same *type*.

Before we present the operators, we make the following definition, which is useful to simplify the definitions and proofs that follow.

Definition 3.1. *Let $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$. We define, for all $y' \notin \mathcal{Y}$ and all $x \in \mathcal{X}$, $C(x, y') = 0$.*

This definition is a slight abuse of notation, as we still consider $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ to be a function over $\mathcal{X} \times \mathcal{Y}$ — we are merely "overloading" the notation to some elements in which C is undefined. Definition 2.26 and Corollary 2.33 assure us that this abuse has no undesirable consequences, since appending a channel with a set of outputs whose image is 0 does not change it in any meaningful way.

We now present the operators studied in this thesis. For the remaining of this section, let $\mathcal{X}$ be a (finite and nonempty) set of secret values.

3.1.1 Parallel composition operator ($\parallel$).

Consider the scenario in which on a given database there is some user's data that is of interest to an adversary. Let us suppose that, by using a request modelled by channel C_1, the adversary is able to obtain the age of said user. Using, instead, another request modelled by C_2, he is able to infer a rough approximation of this user's location. The *parallel composition operator* $\parallel$ applied to C_1 and C_2 models the situation in which the adversary observes the results of both requests.

More generally, given $C_1 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_1}$, $C_2 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_2}$, the channel $C_1 \parallel C_2$ models the scenario in which both channels C_1 and C_2 are fed the secret and each produces an output, both of which can be observed by the adversary. This operator assumes that C_1 and C_2 are independent given the secret — i.e., $p(y_1, y_2|x) = p(y_1|x)p(y_2|x)$ for all $x \in \mathcal{X}$, $y_1 \in \mathcal{Y}_1$ and $y_2 \in \mathcal{Y}_2$. Although there are certainly situations where independence does not hold, the amount of systems that can be modelled with this operator justifies its study.

Definition 3.2. *Let $C_1 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_1}$, $C_2 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_2}$ be compatible channels. Their* parallel composition $C_1 \parallel C_2 \in \mathcal{C}_{\mathcal{X}}^{(\mathcal{Y}_1 \times \mathcal{Y}_2)}$ *is defined as, for all $x \in \mathcal{X}$, $y_1 \in \mathcal{Y}_1$ and $y_2 \in \mathcal{Y}_2$,*

$$(C_1 \parallel C_2)(x, (y_1, y_2)) = C_1(x, y_1)C_2(x, y_2).$$

The parallel composition operator $\parallel$: $\mathcal{C}_{\mathcal{X}} \times \mathcal{C}_{\mathcal{X}} \to \mathcal{C}_{\mathcal{X}}$ *is the mapping $(C_1, C_2) \mapsto C_1 \parallel C_2$, for all $C_1, C_2 \in \mathcal{C}_{\mathcal{X}}$.*

Notice that this definition follows directly from independence, as $C_1(x, y_1)C_2(x, y_2) = p(y_1|x)p(y_2|x)$.

As an example of this operator, consider the following channels C_1, C_2 and their parallel composition.

$$\begin{array}{|c|cc|} \hline C_1 & y_1 & y_2 \\ \hline x_1 & 0.1 & 0.9 \\ x_2 & 0.8 & 0.2 \\ \hline \end{array} \parallel \begin{array}{|c|cc|} \hline C_2 & y_1 & y_2 \\ \hline x_1 & 1 & 0 \\ x_2 & 0.3 & 0.7 \\ \hline \end{array} = \begin{array}{|c|cccc|} \hline C_1 \parallel C_2 & (y_1, y_1) & (y_1, y_2) & (y_2, y_1) & (y_2, y_2) \\ \hline x_1 & 0.1 & 0 & 0.9 & 0 \\ x_2 & 0.24 & 0.56 & 0.06 & 0.14 \\ \hline \end{array}$$

3.1.2 Visible choice operator (${}_p\sqcup$).

Suppose there is a protocol that receives requests from users and randomly chooses with probability $p \in [0,1]$ one of two servers, one modelled by C_1 and another by C_2, to forward it to. Suppose further that the user will only know which server processed her request after the execution of the protocol. This scenario can be modelled by applying the *visible choice operator* ${}_p\sqcup$ to channels C_1, C_2.

Given $p \in [0,1]$, the channel $C_1 \;{}_p\sqcup\; C_2$ models a system which, receiving an input, chooses to feed it either to C_1, with probability p, or to C_2, with probability $1-p$, and reveals to the adversary (explicitly or implicitly) which channel was chosen.

Before giving a formal definition of this operator, we need to define the set operation of *disjoint union*, which is a modified set union operation that tags each element with a label indicating the set they came from.

Definition 3.3. *Let $\mathcal{A}$, $\mathcal{B}$ be sets. The* disjoint union *of $\mathcal{A}$ and $\mathcal{B}$ is defined as*

$$\mathcal{A} \sqcup \mathcal{B} = (\mathcal{A} \times \{1\}) \cup (\mathcal{B} \times \{2\}).$$

Definition 3.4. *Let $p \in [0,1]$ and let $C_1 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_1}$, $C_2 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_2}$ be compatible channels. Their* visible choice (w.r.t. *p) $C_1 \;{}_p\sqcup\; C_2 \in \mathcal{C}_{\mathcal{X}}^{(\mathcal{Y}_1 \sqcup \mathcal{Y}_2)}$ is defined as, for all $x \in \mathcal{X}$, $(y,i) \in \mathcal{Y}_1 \sqcup \mathcal{Y}_2$,*

$$(C_1 \;{}_p\sqcup\; C_2)(x,(y,i)) = \begin{cases} pC_1(x,y) & \text{if } y \in \mathcal{Y}_1 \text{ and } i = 1, \\ (1-p)C_2(x,y) & \text{if } y \in \mathcal{Y}_2 \text{ and } i = 2. \end{cases}$$

The visible choice operator (w.r.t *p) ${}_p\sqcup : \mathcal{C}_{\mathcal{X}} \times \mathcal{C}_{\mathcal{X}} \to \mathcal{C}_{\mathcal{X}}$ is the mapping $(C_1, C_2) \mapsto C_1 \;{}_p\sqcup\; C_2$, for all $C_1, C_2 \in \mathcal{C}_{\mathcal{X}}$.*

To illustrate this operator, consider the following application of ${}_{1/2}\sqcup$ to channels C_1, C_2.

C_1	y_1	y_2
x_1	0.4	0.6
x_2	0.8	0.2

${}_{1/2}\sqcup$

C_2	y_1	y_3
x_1	1	0
x_2	0.5	0.5

$=$

$C_1 \;{}_{1/2}\sqcup\; C_2$	$(y_1,1)$	$(y_2,1)$	$(y_1,2)$	$(y_3,2)$
x_1	0.2	0.3	0.5	0
x_2	0.4	0.1	0.25	0.25

3.1.3 Hidden choice operator (${}_p\oplus$).

Consider the following protocol to protect the identity of the participants of a yes/no poll in a sensitive subject (e.g. drug use, political opinion, etc). Firstly, each participant flips a fair coin. If it lands on heads, the participant answers the question sincerely.

If it lands on tails, the participant proceeds to toss it again, answering "yes" to the question if it lands on heads, and "no" otherwise. The interviewer, oblivious to the result of the coin tosses, is then able to infer the results of the sincere answers of the poll by subtracting the expected number of random "yes" and "no" answers from the total data. However, the interviewer cannot know for sure whether any answer given was sincere or not. Let C_1 be a channel which always outputs the real answer, and C_2 be a channel which outputs an answer randomly. This protocol can be modelled by applying the *hidden choice operator* ${}_{1/2}\oplus$ to C_1 and C_2.

Given $p \in [0,1]$, the channel $C_1 \;{}_p\oplus\; C_2$ is similar to $C_1 \;{}_p\oplus\; C_2$. Again, it models a system which, receiving an input, chooses to feed it either to C_1, with probability p, or to C_2, with probability $1-p$. This time however, as the name suggests, the channel that produced the output chosen is not explicitly revealed.

Definition 3.5. *Let $p \in [0,1]$ and let $C_1 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_1}$, $C_2 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_2}$ be compatible channels. Their* hidden choice (w.r.t. *p*) *$C_1 \;{}_p\sqcup\; C_2 \in \mathcal{C}_{\mathcal{X}}^{(\mathcal{Y}_1 \cup \mathcal{Y}_2)}$ is defined as, for all $x \in \mathcal{X}$, $y \in \mathcal{Y}_1 \cup \mathcal{Y}_2$,*

$$(C_1 \;{}_p\oplus\; C_2)(x,y) = \begin{cases} pC_1(x,y) + (1-p)C_2(x,y) & \textit{if } y \in \mathcal{Y}_1 \cap \mathcal{Y}_2, \\ pC_1(x,y) & \textit{if } y \in \mathcal{Y}_1 \setminus \mathcal{Y}_2, \\ (1-p)C_2(x,y) & \textit{if } y \in \mathcal{Y}_2 \setminus \mathcal{Y}_1. \end{cases}$$

The hidden choice operator (w.r.t *p*) *${}_p\oplus : \mathcal{C}_{\mathcal{X}} \times \mathcal{C}_{\mathcal{X}} \to \mathcal{C}_{\mathcal{X}}$ is the mapping $(C_1, C_2) \mapsto C_1 \;{}_p\oplus\; C_2$, for all $C_1, C_2 \in \mathcal{C}_{\mathcal{X}}$.*

As an example, consider the composition $C_1 \;{}_{1/2}\oplus\; C_2$ of the following channels C_1, C_2.

C_1	y_1	y_2
x_1	0.4	0.6
x_2	0.8	0.2

${}_{1/2}\oplus$

C_2	y_1	y_3
x_1	1	0
x_2	0.5	0.5

$=$

$C_1 \;{}_{1/2}\oplus\; C_2$	y_1	y_2	y_3
x_1	0.7	0.3	0
x_2	0.65	0.1	0.25

It might be helpful to compare this example to the one given for the visible choice operator. Notice how the entries with the same output valued are "merged" into a single one.

It might happen that the output sets of C_1 and C_2 are disjoint. In this case, the adversary can completely deduce which channel was used, and we have $C_1 \;{}_p\oplus\; C_2 \;\approx\; C_1 \;{}_p\sqcup\; C_2$.

3.1.4 Visible if-then-else operator (${}_{\mathcal{A}}\triangle$)

Suppose now there is a computer program that takes as input a string of bits and executes one of two processes. If the last bit of the string is 0, it executes a process modelled by a channel C_1, and, if the last bit is 1, it executes a process modelled by a channel C_2. Consider, further, that the system reveals to the adversary the last bit of the secret after its execution. Letting $\mathcal{A}$ be the set of secret values whose last bit is 0, this system can be modelled by applying the *visible if-then-else operator* ${}_{\mathcal{A}}\triangle$ to C_1 and C_2.

More generally, given a subset $\mathcal{A}$ of the secret set $\mathcal{X}$, the *visible if-then-else operator* models a scenario in which, similarly to visible and hidden choice, only one of two systems will be used and yield an output. Instead of the choice being made probabilistically, however, it is determined completely by the secret value. The channel $C_1 \;{}_{\mathcal{A}}\triangle\; C_2$ models a system which, upon receiving the secret, feeds it to C_1 if $x \in \mathcal{A}$ or to C_2 if $x \notin \mathcal{A}$. As the name suggests, the system also reveals (explicitly or implicitly) which channel yielded the output by the end of the execution.

Definition 3.6. *Let $\mathcal{A} \subset \mathcal{X}$ and let $C_1 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_1}$, $C_2 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_2}$ be compatible channels. Their* visible if-then-else (w.r.t. $\mathcal{A}$) $C_1 \;{}_{\mathcal{A}}\triangle\; C_2 \in \mathcal{C}_{\mathcal{X}}^{(\mathcal{Y}_1 \sqcup \mathcal{Y}_2)}$ *is defined as, for all $x \in \mathcal{X}$, $(y, i) \in \mathcal{Y}_1 \sqcup \mathcal{Y}_2$,*

$$(C_1 \;{}_{\mathcal{A}}\triangle\; C_2)(x, (y, i)) = \begin{cases} C_1(x, y) & \textit{if } x \in \mathcal{A},\ y \in \mathcal{Y}_1 \textit{ and } i = 1, \\ C_2(x, y) & \textit{if } x \notin \mathcal{A},\ y \in \mathcal{Y}_2 \textit{ and } i = 2, \\ 0, & \textit{otherwise.} \end{cases}$$

The visible if-then-else operator (w.r.t $\mathcal{A}$) ${}_{\mathcal{A}}\triangle\; : \mathcal{C}_{\mathcal{X}} \times \mathcal{C}_{\mathcal{X}} \to \mathcal{C}_{\mathcal{X}}$ *is the mapping $(C_1, C_2) \mapsto C_1 \;{}_{\mathcal{A}}\triangle\; C_2$, for all $C_1, C_2 \in \mathcal{C}_{\mathcal{X}}$.*

As an example, consider the following application of the visible if-then-else operator to channels C_1, C_2, with $\mathcal{A} = \{x_1, x_2\}$. For purely didactic purposes, we provide a larger example for this operator, as any composition with only two secret values and $|\mathcal{A}| = 1$ would completely reveal the secret.

$$\begin{array}{|c|cc|} \hline C_1 & y_1 & y_2 \\ \hline x_1 & 0.5 & 0.5 \\ x_2 & 0.3 & 0.7 \\ x_3 & 0 & 1 \\ x_4 & 0.6 & 0.4 \\ \hline \end{array} \;\; {}_{\mathcal{A}}\triangle \;\; \begin{array}{|c|cc|} \hline C_2 & y_1 & y_3 \\ \hline x_1 & 0.1 & 0.9 \\ x_2 & 0.7 & 0.3 \\ x_3 & 0.4 & 0.6 \\ x_4 & 0.8 & 0.2 \\ \hline \end{array} \;\; = \;\; \begin{array}{|c|cccc|} \hline C_1 \;{}_{\mathcal{A}}\triangle\; C_2 & (y_1, 1) & (y_2, 1) & (y_1, 2) & (y_3, 2) \\ \hline x_1 & 0.5 & 0.5 & 0 & 0 \\ x_2 & 0.3 & 0.7 & 0 & 0 \\ x_3 & 0 & 0 & 0.4 & 0.6 \\ x_4 & 0 & 0 & 0.8 & 0.2 \\ \hline \end{array}$$

3.1.5 Hidden if-then-else operator (${}_{\mathcal{A}}\text{⟁}$)

Consider now a computer program that performs one of two different tasks, the choice of which is never revealed explicitly to the attacker, depending on the parity of an integer secret value. Let C_1 describe the programs behaviour when the secret value is odd and C_2 when it is even. Letting $\mathcal{A}$ be the subset of the secret values that are odd, we can model this computer program by applying the *hidden if-then-else operator* ${}_{\mathcal{A}}\text{⟁}$ to C_1 and C_2.

The *hidden if-then-else operator* is similar to its visible counterpart. Letting $\mathcal{A} \subset \mathcal{X}$,the channel $C_1 \;{}_{\mathcal{A}}\text{⟁}\; C_2$ models a system that selects channel C_1 if $x \in \mathcal{A}$ or C_2 if $x \notin \mathcal{A}$. This time, however, the channel selection is not revealed to the adversary.

Definition 3.7. *Let $\mathcal{A} \subset \mathcal{X}$ and let $C_1 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_1}$, $C_2 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_2}$ be compatible channels. Their* hidden if-then-else (w.r.t. $\mathcal{A}$) $C_1 \;{}_{\mathcal{A}}\text{⟁}\; C_2 \in \mathcal{C}_{\mathcal{X}}^{(\mathcal{Y}_1 \cup \mathcal{Y}_2)}$ *is defined as, for all $x \in \mathcal{X}$, $y \in \mathcal{Y}_1 \cup \mathcal{Y}_2$,*

$$(C_1 \;{}_{\mathcal{A}}\text{⟁}\; C_2)(x,y) = \begin{cases} C_1(x,y) & \text{if } x \in \mathcal{A} \text{ and } y \in \mathcal{Y}_1, \\ C_2(x,y) & \text{if } x \notin \mathcal{A} \text{ and } y \in \mathcal{Y}_2, \\ 0 & \text{otherwise.} \end{cases}$$

The hidden if-then-else operator (w.r.t $\mathcal{A}$) ${}_{\mathcal{A}}\text{⟁}\; : \mathcal{C}_{\mathcal{X}} \times \mathcal{C}_{\mathcal{X}} \to \mathcal{C}_{\mathcal{X}}$ *is the mapping $(C_1, C_2) \mapsto C_1 \;{}_{\mathcal{A}}\text{⟁}\; C_2$, for all $C_1, C_2 \in \mathcal{C}_{\mathcal{X}}$.*

If $\mathcal{Y}_1 \cap \mathcal{Y}_2 = \emptyset$, the adversary can always tell which channel yielded the output, and we have $C_1 \;{}_{\mathcal{A}}\text{⟁}\; C_2 \approx C_1 \;{}_{\mathcal{A}}\triangle\; C_2$.

To illustrate this operator, we consider the composition $C_1 \;{}_{\mathcal{A}}\text{⟁}\; C_2$ for the following channels C_1, C_2 and $\mathcal{A} = \{x_1, x_2\}$.

C_1	y_1	y_2
x_1	0.5	0.5
x_2	0.3	0.7
x_3	0	1
x_4	0.6	0.4

${}_{\mathcal{A}}\text{⟁}$

C_2	y_1	y_3
x_1	0.1	0.9
x_2	0.7	0.3
x_3	0.4	0.6
x_4	0.8	0.2

$=$

$C_1 \;{}_{\mathcal{A}}\text{⟁}\; C_2$	y_1	y_2	y_3
x_1	0.5	0.5	0
x_2	0.3	0.7	0
x_3	0.4	0	0.6
x_4	0.8	0	0.2

We suggest to the reader to compare this example to that given for the visible if-then-esle operator. Notice that the columns representing the same output value are combined into a single one.

Similarly to the hidden choice operator, if $\mathcal{Y}_1$ and $\mathcal{Y}_2$ are disjoint, the adversary is able to infer which one among C_1 and C_2 produced the output. In this case,

$C_1 \ {}_{\mathcal{A}}{\triangle\!\!\!\!\!\!+}\ C_2 \ \approx C_1 \ {}_{\mathcal{A}}\triangle \ C_2$.

3.2 Algebraic properties of operators

We now give a list of algebraic properties of the operators we introduced in the previous section. These algebraic properties, among other things, enable us to simplify complex channel descriptions and facilitate the derivation of security properties of the systems they are modelling.

First, we briefly recall the refinement relation introduced in Section 2.3.2. Given two channels $C_1, C_2 \in \mathcal{C}_{\mathcal{X}}$, we write $C_2 \sqsubseteq_\circ C_1$ if there is a channel R such that $C_1 = C_2R$. We say that C_1 and C_2 are *equivalent*, and write $C_1 \approx C_2$, if $C_1 \sqsubseteq_\circ C_2$ and $C_2 \sqsubseteq_\circ C_1$. Recall, also, that from Theorem 2.32 we know that a channel C_1 refines a channel C_2 if, and only if, C_1 never leaks more than C_2, no matter the prior π and gain function g. That is, for any channels $C_1, C_2 \in \mathcal{C}_{\mathcal{X}}$,

$$C_2 \sqsubseteq_\circ C_1 \Leftrightarrow \forall \pi \in \mathbb{D}\mathcal{X}, \forall g \in \mathbb{G}\mathcal{X}, V_g[\pi \rangle C_1] \leq V_g[\pi \rangle C_2].$$

The definitions of our operators are dependent not only on the leakage properties of the channels they act upon, but also on the names of the elements of the input and output sets. Therefore, before we present their algebraic properties, we define a stricter equivalence relation than the one given above, under which channels are considered equivalent whenever their matrix representation is the same but for the output values associated with each column.

Definition 3.8. *Let $C_1 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_1}$ and $C_2 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_2}$ be compatible channels. We say that C_1 and C_2 are* equal up to a permutation*, and write $C_1 \overset{\circ}{=} C_2$, if there is a bijection $\psi : \mathcal{Y}_1 \to \mathcal{Y}_2$ such that $C_1(x,y) = C_2(x, \psi(y))$ for all $x \in \mathcal{X}$, $y \in \mathcal{Y}_1$.*

Note that if $C_1 \overset{\circ}{=} C_2$, then $C_1 \approx C_2$: let $P \in \mathcal{C}_{\mathcal{Y}}^{\mathcal{Y}}$ be given by $P(y_1, y_2) = 1$ if $\phi(y_1) = y_2$ and 0 otherwise. Then, $C_2 = C_1P$ and $C_1 = C_2P^T$, where P^T is the channel whose matrix is the transpose of the matrix of P.

We will now present some algebraic properties we established for these operators. Most proofs on this section are somewhat lengthy, so instead of keeping them in the main body, we present them on Appendix 6.

In the remainder of this section, let $\mathcal{X}$ be a set of secret values, $C_1 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_1}$, $C_2 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_2}$ and $C_3 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_3}$ be compatible channels, $p, q \in [0,1]$ and $\mathcal{A}, \mathcal{B} \subset \mathcal{X}$ be subsets of the set of secret values $\mathcal{X}$. Let also $\bar{\mathcal{A}} = \mathcal{X} \setminus \mathcal{A}$ and $\bar{\mathcal{B}} = \mathcal{X} \setminus \mathcal{B}$.

3.2.1 Commutativity, associativity and idempotency

We first establish that our operators are associative and commutative. Strictly speaking, the visible choice and hidden choice operators w.r.t some $p \in [0,1]$, and the visible if-then-else and hidden if-then-else operators w.r.t some $\mathcal{A}$ are not, in general, commutative or associative. The "commutative" and "associative" properties we establish for them are relaxed versions, in which we allow the modification of the probability values for the visible and hidden choice, and of the subsets of secrets for the visible and hidden if-then-else.

Proposition 3.9 (Commutative Properties)**.**

$$C_1 \parallel C_2 \overset{\circ}{=} C_2 \parallel C_1, \tag{3.1}$$

$$C_1 \;{}_{p}{\dot\sqcup}\; C_2 \overset{\circ}{=} C_2 \;{}_{(\mathit{1}-p)}{\dot\sqcup}\; C_1, \tag{3.2}$$

$$C_1 \;{}_{p}{\oplus}\; C_2 = C_2 \;{}_{(\mathit{1}-p)}{\oplus}\; C_1, \tag{3.3}$$

$$C_1 \;{}_{\mathcal{A}}{\triangle}\; C_2 \overset{\circ}{=} C_2 \;{}_{\bar{\mathcal{A}}}{\triangle}\; C_1, \tag{3.4}$$

$$C_1 \;{}_{\mathcal{A}}{\triangle\mkern-14mu+}\; C_2 = C_2 \;{}_{\bar{\mathcal{A}}}{\triangle\mkern-14mu+}\; C_1. \tag{3.5}$$

Proposition 3.10 (Associative Properties)**.**

$$(C_1 \parallel C_2) \parallel C_3 \overset{\circ}{=} C_1 \parallel (C_2 \parallel C_3), \tag{3.6}$$

$$(C_1 \;{}_{p}{\dot\sqcup}\; C_2) \;{}_{q}{\dot\sqcup}\; C_3 \overset{\circ}{=} C_1 \;{}_{p'}{\dot\sqcup}\; (C_2 \;{}_{q'}{\dot\sqcup}\; C_3), \tag{3.7}$$

$$(C_1 \;{}_{p}{\oplus}\; C_2) \;{}_{q}{\oplus}\; C_3 = C_1 \;{}_{p'}{\oplus}\; (C_2 \;{}_{q'}{\oplus}\; C_3), \tag{3.8}$$

$$(C_1 \;{}_{\mathcal{A}}{\triangle}\; C_2) \;{}_{\mathcal{B}}{\triangle}\; C_3 \overset{\circ}{=} C_1 \;{}_{(\mathcal{A}\cap\mathcal{B})}{\triangle}\; (C_2 \;{}_{\mathcal{B}}{\triangle}\; C_3), \tag{3.9}$$

$$(C_1 \;{}_{\mathcal{A}}{\triangle\mkern-14mu+}\; C_2) \;{}_{\mathcal{B}}{\triangle\mkern-14mu+}\; C_3 = C_1 \;{}_{(\mathcal{A}\cap\mathcal{B})}{\triangle\mkern-14mu+}\; (C_2 \;{}_{\mathcal{B}}{\triangle\mkern-14mu+}\; C_3), \tag{3.10}$$

where $p'{=}pq$ *and* $q'{=}{}^{(q-pq)}/_{(1-pq)}$.

Aiming to establishing rules to simplify descriptions of channels, we consider the results of combining a channel with itself.

Proposition 3.11 (Idempotency).

$$
\begin{aligned}
C_1 \parallel C_1 &\sqsubseteq_\circ C_1, && (3.11)\\
C_1 \;{}_p\dot{\sqcup}\; C_1 &\approx C_1, && (3.12)\\
C_1 \;{}_p\oplus\; C_1 &= C_1, && (3.13)\\
C_1 \;{}_{\mathcal{A}}\triangle\; C_1 &\sqsubseteq_\circ C_1, && (3.14)\\
C_1 \;{}_{\mathcal{A}}\blacktriangle\; C_1 &= C_1. && (3.15)
\end{aligned}
$$

In the case of visible if-then-else, equivalence for idempotency does not hold in general, as $C_1 \;{}_{\mathcal{A}}\triangle\; C_1$ completely reveals whether $x \in \mathcal{A}$. Similarly, equivalence does not hold in general for the parallel composition, as repeating a run of a probabilistic system can reveal further information about the secret. However, equivalence holds for it when we are dealing with *deterministic channels* — that is, channels whose values are either 0 or 1, for any choice of input and output. This result is to be expected, as the output of a deterministic channel is completely determined by the input, and there can be no information gain for observing more than one execution of such a system.

Proposition 3.12. *Suppose $\exists C \in \mathcal{C}_{\mathcal{X}}$ such that C is deterministic and $C_1 \approx C$. Then*

$$C_1 \parallel C_1 \approx C_1.$$

3.2.2 Null and transparent channels

Null and transparent channels are important concepts on quantitative information flow. Loosely speaking, a null channel is a channel that never leaks any information, while a transparent channel is one that always completely reveals the secret value.

Formally, a *null channel* $\overline{0} \in \mathcal{C}_{\mathcal{X}}$ is a channel that, for every prior π and gain function g, $V_g[\pi \rangle \overline{0}] = V_g(\pi)$. From Theorem 2.24, we conclude that $C \sqsubseteq_\circ \overline{0}$ for all $C \in \mathcal{C}_{\mathcal{X}}$.

Proposition 3.13. *A channel $\overline{0} \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ is a null channel if, and only if, for all $y \in \mathcal{Y}$ and $x, x' \in \mathcal{X}$,*

$$\overline{0}(x, y) = \overline{0}(x', y).$$

On the other hand, a *transparent channel* $\overline{I} \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ is any channel such that, given any $C \in \mathcal{C}_{\mathcal{X}}$, $\overline{I} \sqsubseteq_\circ C$. That is, $\overline{I}$ leaks at least as much information as any other compatible channel, for every prior and gain function.

Proposition 3.14. *A channel $\overline{I} \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ is a transparent channel if, and only if, for all $y \in \mathcal{Y}$ and $x, x' \in \mathcal{X}$ such that $x \neq x'$,*

$$\overline{I}(x, y) > 0 \implies \overline{I}(x', y) = 0.$$

Being the null channel the channel that leaks the least, one might expect that its composition with any channel C_1 would be at least as secure as C_1 alone. Analogously, it could be assumed that the composition of C_1 with a transparent channel would yield a channel that leaks at least as much information as C_1. We formalize these notions in Propositions 3.15 and 3.16, which hold for any null channel $\overline{0}$ and transparent channel $\overline{I}$ compatible with C_1.

Proposition 3.15 (Null Channel Properties)**.**

$$C_1 \approx (C_1 \parallel \overline{0}), \tag{3.16}$$

$$C_1 \sqsubseteq_\circ (C_1 \; {}_p\!\sqcup \overline{0}), \tag{3.17}$$

$$C_1 \sqsubseteq_\circ (C_1 \; {}_p\!\oplus \overline{0}). \tag{3.18}$$

The properties $C_1 \sqsubseteq_\circ C_1 \; {}_{\mathcal{A}}\!\triangle \; \overline{0}$ and $C_1 \sqsubseteq_\circ C_1 \; {}_{\mathcal{A}}\!\blacktriangle \; \overline{0}$, however, do not hold in general. We can build a simple counterexample for both cases considering the following channels.

C_1	y_1	y_2
x_1	1	0
x_2	$1/2$	$1/2$

$\overline{0}_1$	y_2
x_1	1
x_2	1

Given $\pi_u = (1/2, 1/2)$, we have $V_g[\pi \rangle C_1] = 3/4$. Meanwhile, letting $\mathcal{A} = \{x_1\}$, we have

$C_1 \; {}_{\mathcal{A}}\!\triangle \; \overline{0}_1$	$(y_1, 1)$	$(y_2, 1)$	$(y_2, 2)$
x_1	1	0	0
x_2	0	0	1

$C_1 \; {}_{\mathcal{A}}\!\blacktriangle \; \overline{0}_1$	y_1	y_2
x_1	1	0
x_2	0	1

which yield $V_g[\pi \rangle C_1 \; {}_{\mathcal{A}}\!\triangle \; \overline{0}_1] = V_g[\pi \rangle C_1 \; {}_{\mathcal{A}}\!\blacktriangle \; \overline{0}_1] = 1$, so $C_1 \not\sqsubseteq_\circ C_1 \; {}_{\mathcal{A}}\!\triangle \; \overline{0}_1$ and $C_1 \not\sqsubseteq_\circ C_1 \; {}_{\mathcal{A}}\!\blacktriangle \; \overline{0}_1$.

Proposition 3.16 (Transparent Channel Properties)**.**

$$(C_1 \parallel \overline{I}) \approx \overline{I}, \tag{3.19}$$

$$(C_1 \; {}_p\!\sqcup \overline{I}) \sqsubseteq_\circ C_1, \tag{3.20}$$

$$(C_1 \; {}_{\mathcal{A}}\!\triangle \; \overline{I}) \sqsubseteq_\circ C_1. \tag{3.21}$$

In general, $(C_1 \;{}_{p}\!\oplus\; \overline{I}) \not\sqsubseteq_{\circ} C_1$ and $(C_1 \;{}_{\mathcal{A}}\mathbin{◬}\; \overline{I}) \not\sqsubseteq_{\circ} C_1$. Consider, for example, the following channel C_1, transparent channel $\overline{I}_1$, and their compositions, letting $\mathcal{A} = \{x_1\}$.

C_1	y_1	y_2
x_1	1	0
x_2	0	1

$\overline{I}_1$	y_1	y_2
x_1	0	1
x_2	1	0

$C_1 \;{}_{1/2}\!\oplus\; \overline{I}_1$	y_1	y_2
x_1	$1/2$	$1/2$
x_2	$1/2$	$1/2$

$C_1 \;{}_{\mathcal{A}}\mathbin{◬}\; \overline{I}_1$	y_1	y_2
x_1	1	0
x_2	1	0

Then, $C_1 \;{}_{1/2}\!\oplus\; \overline{I}_1$ and $C_1 \;{}_{\mathcal{A}}\mathbin{◬}\; \overline{I}_1$ are null channels, while C_1 is a transparent channel. Therefore, $C_1 \;{}_{1/2}\!\oplus\; \overline{I}_1 \not\sqsubseteq_{\circ} C_1$ and $C_1 \;{}_{\mathcal{A}}\mathbin{◬}\; \overline{I}_1 \not\sqsubseteq_{\circ} C_1$.

3.2.3 Distributive properties

We now consider distributive properties of the operators. These are not only helpful when simplifying descriptions of channels, but also give us some insight on how to organize our systems. If distributivity of an operator over another holds, we can choose between either applying the former to the result of the latter or applying the latter over the results of the former. In practice, this might allow us to manoeuvre parts of systems by changing the order in which these compositions take place.

We will abuse the nomenclature and also establish properties regarding the "distribution" of an operator is over itself.

Proposition 3.17 (Distributivity for the Parallel operator)**.**

$$C_1 \parallel (C_2 \parallel C_3) {}_{\circ}\!\sqsupseteq (C_1 \parallel C_2) \parallel (C_1 \parallel C_3), \tag{3.22}$$

$$C_1 \parallel (C_2 \;{}_{p}\!\dot\sqcup\; C_3) \overset{\circ}{=} (C_1 \parallel C_2) \;{}_{p}\!\dot\sqcup\; (C_1 \parallel C_3), \tag{3.23}$$

$$C_1 \parallel (C_2 \;{}_{p}\!\oplus\; C_3) = (C_1 \parallel C_2) \;{}_{p}\!\oplus\; (C_1 \parallel C_3), \tag{3.24}$$

$$C_1 \parallel (C_2 \;{}_{\mathcal{A}}\!\triangle\; C_3) \overset{\circ}{=} (C_1 \parallel C_2) \;{}_{\mathcal{A}}\!\triangle\; (C_1 \parallel C_3), \tag{3.25}$$

$$C_1 \parallel (C_2 \;{}_{\mathcal{A}}\mathbin{◬}\; C_3) = (C_1 \parallel C_2) \;{}_{\mathcal{A}}\mathbin{◬}\; (C_1 \parallel C_3). \tag{3.26}$$

Proposition 3.18 (Distributivity for Visible Choice)**.**

$$C_1 \;{}_{p}\!\dot\sqcup\; (C_2 \;{}_{q}\!\dot\sqcup\; C_3) \approx (C_1 \;{}_{p}\!\dot\sqcup\; C_2) \;{}_{q}\!\dot\sqcup\; (C_1 \;{}_{p}\!\dot\sqcup\; C_3), \tag{3.27}$$

$$C_1 \;{}_{p}\!\dot\sqcup\; (C_2 \;{}_{q}\!\oplus\; C_3) = (C_1 \;{}_{p}\!\dot\sqcup\; C_2) \;{}_{q}\!\oplus\; (C_1 \;{}_{p}\!\dot\sqcup\; C_3), \tag{3.28}$$

$$C_1 \;{}_{p}\!\dot\sqcup\; (C_2 \;{}_{\mathcal{A}}\!\triangle\; C_3) {}_{\circ}\!\sqsupseteq (C_1 \;{}_{p}\!\dot\sqcup\; C_2) \;{}_{\mathcal{A}}\!\triangle\; (C_1 \;{}_{p}\!\dot\sqcup\; C_3), \tag{3.29}$$

$$C_1 \;{}_{p}\!\dot\sqcup\; (C_2 \;{}_{\mathcal{A}}\mathbin{◬}\; C_3) = (C_1 \;{}_{p}\!\dot\sqcup\; C_2) \;{}_{\mathcal{A}}\mathbin{◬}\; (C_1 \;{}_{p}\!\dot\sqcup\; C_3). \tag{3.30}$$

Proposition 3.19 (Distributivity for Hidden Choice)**.**

$$C_1 \;{}_{p}\!\oplus\; (C_2 \;{}_{q}\!\oplus\; C_3) = (C_1 \;{}_{p}\!\oplus\; C_2) \;{}_{q}\!\oplus\; (C_1 \;{}_{p}\!\oplus\; C_3), \tag{3.31}$$

$$C_1 \;{}_{p}\!\oplus\; (C_2 \;{}_{\mathcal{A}}\!\blacktriangle\; C_3) = (C_1 \;{}_{p}\!\oplus\; C_2) \;{}_{\mathcal{A}}\!\blacktriangle\; (C_1 \;{}_{p}\!\oplus\; C_3). \tag{3.32}$$

Proposition 3.20 (Distributivity for Visible If-then-else)**.**

$$C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \parallel C_3)_{\circ}\!\sqsupseteq (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \parallel (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3), \tag{3.33}$$

$$C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \;{}_{p}\!\sqcup\; C_3) \approx (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \;{}_{p}\!\sqcup\; (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3), \tag{3.34}$$

$$C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \;{}_{p}\!\oplus\; C_3) = (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \;{}_{p}\!\oplus\; (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3), \tag{3.35}$$

$$C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \;{}_{\mathcal{B}}\!\triangle\; C_3)_{\circ}\!\sqsupseteq (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \;{}_{\mathcal{B}}\!\triangle\; (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3), \tag{3.36}$$

$$C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \;{}_{\mathcal{B}}\!\blacktriangle\; C_3) = (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \;{}_{\mathcal{B}}\!\blacktriangle\; (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3). \tag{3.37}$$

Proposition 3.21 (Distributivity for Hidden If-then-else)**.**

$$C_1 \;{}_{\mathcal{A}}\!\blacktriangle\; (C_2 \;{}_{p}\!\oplus\; C_3) = (C_1 \;{}_{\mathcal{A}}\!\blacktriangle\; C_2) \;{}_{p}\!\oplus\; (C_1 \;{}_{\mathcal{A}}\!\blacktriangle\; C_3), \tag{3.38}$$

$$C_1 \;{}_{\mathcal{A}}\!\blacktriangle\; (C_2 \;{}_{\mathcal{B}}\!\blacktriangle\; C_3) = (C_1 \;{}_{\mathcal{A}}\!\blacktriangle\; C_2) \;{}_{\mathcal{B}}\!\blacktriangle\; (C_1 \;{}_{\mathcal{A}}\!\blacktriangle\; C_3). \tag{3.39}$$

The other possible distributive properties do not hold in general.

Proposition 3.22 (Non-distributivity)**.** *The following expressions do not, in general, respect the refinement relation between them, in any direction*

$$(C_1 \;{}_{p}\!\sqcup\; (C_2 \parallel C_3)) \textit{ and } ((C_1 \;{}_{p}\!\sqcup\; C_2) \parallel (C_1 \;{}_{p}\!\sqcup\; C_3)), \tag{3.40}$$

$$(C_1 \;{}_{p}\!\oplus\; (C_2 \parallel C_3)) \textit{ and } ((C_1 \;{}_{p}\!\oplus\; C_2) \parallel (C_1 \;{}_{p}\!\oplus\; C_3)), \tag{3.41}$$

$$(C_1 \;{}_{p}\!\oplus\; (C_2 \;{}_{q}\!\sqcup\; C_3)) \textit{ and } ((C_1 \;{}_{p}\!\oplus\; C_2) \;{}_{q}\!\sqcup\; (C_1 \;{}_{p}\!\oplus\; C_3)), \tag{3.42}$$

$$(C_1 \;{}_{p}\!\oplus\; (C_2 \;{}_{\mathcal{A}}\!\triangle\; C_3)) \textit{ and } ((C_1 \;{}_{p}\!\oplus\; C_2) \;{}_{\mathcal{A}}\!\triangle\; (C_1 \;{}_{p}\!\oplus\; C_3)), \tag{3.43}$$

$$(C_1 \;{}_{\mathcal{A}}\!\blacktriangle\; (C_2 \parallel C_3)) \textit{ and } ((C_1 \;{}_{\mathcal{A}}\!\blacktriangle\; C_2) \parallel (C_1 \;{}_{\mathcal{A}}\!\blacktriangle\; C_3)), \tag{3.44}$$

$$(C_1 \;{}_{\mathcal{A}}\!\blacktriangle\; (C_2 \;{}_{p}\!\sqcup\; C_3)) \textit{ and } ((C_1 \;{}_{\mathcal{A}}\!\blacktriangle\; C_2) \;{}_{p}\!\sqcup\; (C_1 \;{}_{\mathcal{A}}\!\blacktriangle\; C_3)), \tag{3.45}$$

$$(C_1 \;{}_{\mathcal{A}}\!\blacktriangle\; (C_2 \;{}_{\mathcal{B}}\!\triangle\; C_3)) \textit{ and } ((C_1 \;{}_{\mathcal{A}}\!\blacktriangle\; C_2) \;{}_{\mathcal{B}}\!\triangle\; (C_1 \;{}_{\mathcal{A}}\!\blacktriangle\; C_3)). \tag{3.46}$$

Perhaps, the only really surprising result of Proposition 3.22 is (3.40). When ${}_{p}\!\oplus$ or ${}_{\mathcal{A}}\!\blacktriangle$ are the operator being distributed, the distribution may fail solely because of the divergences on the output sets. Take (3.41) for example. If $\mathcal{Y}_1 = \mathcal{Y}_2 = \mathcal{Y}_3$, there is a possibility that $C_1 \;{}_{p}\!\oplus\; C_2$ and $C_1 \;{}_{p}\!\oplus\; C_3$ (and therefore $(C_1 \;{}_{p}\!\oplus\; C_2) \parallel (C_1 \;{}_{p}\!\oplus\; C_3)$) are null channels and $C_1 \;{}_{p}\!\oplus\; (C_2 \parallel C_3)$ is not. Analogously, if $\mathcal{Y}_1 = \mathcal{Y}_2 \times \mathcal{Y}_3$, it is possible to have the opposite situation, in which $C_1 \;{}_p\!\oplus\; (C_2 \parallel C_3)$ is a null channel, while $(C_1 \;{}_p\!\oplus\; C_2) \;{}_p\!\oplus\; (C_1 \;{}_p\!\oplus\; C_3)$ is not.

We summarize all our distributivity results in Table 3.2.3.

	$\parallel$	${}_p\sqcup\!\!\!\!\cdot\;$	${}_p\oplus$	${}_{\mathcal{A}}\triangle$	${}_{\mathcal{A}}\triangle\!\!\!\!\!+\;$
$\parallel$	${}_{\circ}\!\sqsupseteq$	$\overset{\circ}{=}$	$=$	$\overset{\circ}{=}$	$=$
${}_p\sqcup\!\!\!\!\cdot\;$		$\approx$	$=$	${}_{\circ}\!\sqsupseteq$	$=$
${}_p\oplus$			$=$		$=$
${}_{\mathcal{A}}\triangle$	${}_{\circ}\!\sqsupseteq$	$\approx$	$=$	${}_{\circ}\!\sqsupseteq$	$=$
${}_{\mathcal{A}}\triangle\!\!\!\!\!+\;$			$=$		$=$

Table 3.1. Summary of the distributivity rules. The lines represent the operator being distributed, and the columns the operators upon which the distributivity is acted. For instance, $\parallel$ distributes over ${}_p\oplus$ with equality, and ${}_{\mathcal{A}}\triangle$ distributes over $\parallel$ with anti-refinement.

3.2.4 Properties regarding cascading

We conclude this section by exploring how our operators behave w.r.t. cascading (defined in Section 2.3.2). Cascading of channels is fundamental in QIF, as it captures the concept of a system *post-processing* the outputs of another system, and it is also the key to the refinement relation $\sqsubseteq_{\circ}$, fundamental to comparing leakage between channels.

The next propositions explore whether it is possible to express a composition of two post-processed channels by post-processing their composition. By virtue of cascading being a notion so closely related to leakage, these properties can facilitate the security analysis of complex systems.

Proposition 3.23. *Let $D_1 \in \mathcal{C}_{\mathcal{Y}_1}^{\mathcal{Z}_1}$, $D_2 \in \mathcal{C}_{\mathcal{Y}_2}^{\mathcal{Z}_2}$ be channels. Then,*

$$(C_1D_1) \parallel (C_2D_2) = (C_1 \parallel C_2)D^{\parallel},$$

where $D^{\parallel} : (\mathcal{Y}_1{\times}\mathcal{Y}_2){\times}(\mathcal{Z}_1{\times}\mathcal{Z}_2) \to [0,1]$ is defined as

$$D^{\parallel}((y_1,y_2),(z_1,z_2)) = D_1(y_1,z_1)D_2(y_2,z_2)$$

for all $y_1{\in}\mathcal{Y}_1$, $y_2{\in}\mathcal{Y}_2$, $z_1{\in}\mathcal{Z}_1$, and $z_2{\in}\mathcal{Z}_2$.

Proposition 3.24. *Let $D_1 \in \mathcal{C}_{\mathcal{Y}_1}^{\mathcal{Z}_1}$, $D_2 \in \mathcal{C}_{\mathcal{Y}_2}^{\mathcal{Z}_2}$ be channels. Then,*

$$(C_1 D_1) \;{}_{p}{\sqcup}\; (C_2 D_2) = (C_1 \;{}_{p}{\sqcup}\; C_2) D^{\sqcup},$$

where $D^{\sqcup}$:$(\mathcal{Y}_1 \sqcup \mathcal{Y}_2) \times (\mathcal{Z}_1 \sqcup \mathcal{Z}_2) \to [0,1]$ is defined as

$$D^{\sqcup}((y,i),(z,j)) = \begin{cases} D_1(y,z), & \textit{if } i=j=1, \\ D_2(y,z), & \textit{if } i=j=2, \\ 0, & \textit{otherwise.} \end{cases}$$

for all $y_1 \in \mathcal{Y}_1$, $y_2 \in \mathcal{Y}_2$, $z_1 \in \mathcal{Z}_1$, $z_2 \in \mathcal{Z}_2$.

Proposition 3.25. *Let $D_1 \in \mathcal{C}_{\mathcal{Y}_1}^{\mathcal{Z}_1}$, $D_2 \in \mathcal{C}_{\mathcal{Y}_2}^{\mathcal{Z}_2}$ be channels. Then,*

$$(C_1 D_1) \;{}_{\mathcal{A}}{\triangle}\; (C_2 D_2) = (C_1 \;{}_{\mathcal{A}}{\triangle}\; C_2) D^{\sqcup},$$

where $D^{\sqcup}$ is as defined in Proposition 3.24.

A similar rule, however, does not hold for hidden choice or hidden if-then-else. As a counterexample, consider the following channels C_1, C_2, D_1 and D_2.

C_1	y_1	y_2
x_1	1	0
x_2	0	1

C_2	y_1	y_2
x_1	0	1
x_2	1	0

D_1	z_1	z_2
y_1	1	0
y_2	0	1

D_2	z_1	z_2
y_1	0	1
y_2	1	0

Consider also the cascadings $C_1 D_1$ and $C_2 D_2$, and the compositions $C_1 \;{}_{1/2}{\oplus}\; C_2$ and $C_1 \;{}_{\{x_1\}}{\bigtriangleup}\; C_2$.

$C_1 D_1$	z_1	z_2
x_1	1	0
x_2	0	1

$C_2 D_2$	z_1	z_2
x_1	1	0
x_2	0	1

$C_1 \;{}_{1/2}{\oplus}\; C_2$	y_1	y_2
x_1	$1/2$	$1/2$
x_2	$1/2$	$1/2$

$C_1 \;{}_{\{x_1\}}{\bigtriangleup}\; C_2$	y_1	y_2
x_1	1	0
x_2	1	0

We see that $C_1 D_1 = C_2 D_2$. Then, $(C_1 D_1) \;{}_{1/2}{\oplus}\; (C_2 D_2) = C_1 D_1$ is a transparent channel, but $C_1 \;{}_{1/2}{\oplus}\; C_2$ is a null channel. Thus, it is impossible to describe $(C_1 D_1) \;{}_{1/2}{\oplus}\; (C_2 D_2)$ as $C_1 \;{}_{1/2}{\oplus}\; C_2$ post-processed by some channel.

Similarly, $(C_1 D_1) \;{}_{\{x_1\}}{\bigtriangleup}\; (C_2 D_2) = C_1 D_1$ is also transparent channel, but $C_1 \;{}_{\{x_1\}}{\bigtriangleup}\; C_2$ is a null channel, and the same argument applies. However, we can establish less general properties for these operators by considering only the case when both components are of the same type and are post-processed by a same channel C. In this scenario, the result is the same as if we post-processed their entire composition by C.

Proposition 3.26. *Let $C_1, C_2 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ be channels of the same type, let $D \in \mathcal{C}_{\mathcal{Y}}^{\mathcal{Z}}$ and let $p \in [0,1]$. Then, $(C_1 D) \;{}_p\!\oplus\; (C_2 D) = (C_1 \;{}_p\!\oplus\; C_2)D$.*

Proposition 3.27. *Let $C_1, C_2 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ be channels of the same type, let $D \in \mathcal{C}_{\mathcal{Y}}^{\mathcal{Z}}$ and let $\mathcal{A} \subset \mathcal{X}$. Then, $(C_1 D) \;{}_{\mathcal{A}}\!\triangle\; (C_2 D) = (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2)D$.*

3.3 The Dining Cryptographers protocol (cont.)

We now continue the example we introduced in Section 1.3, by developing a model of the Dining Cryptographers protocol using the operators we defined in this chapter. We consider the situation in which there are 4 cryptographers and 4 coins, and denote the channel of the protocol by *Dining*. The input set of the channel is $\mathcal{X} = \{c_1, c_2, c_3, c_4, n\}$, in which c_i represents that cryptographer i is the payer, and n represents that the NSA is the payer. The output set of the channel is $\mathcal{Y} = \{0,1\}^4$, i.e., all 4-tuples representing possible announcements by all cryptographers, in order.

Following the scheme in Figure 1.3 (middle), we begin by modelling the protocol as the interaction between two channels, *Coins* and *Announcements*. The first channel models the coin tosses, whereas the second one models the public announcements of the cryptographers. Since in the protocol first the coins are tossed, and only then the corresponding results are passed on to the party of cryptographers, a natural starting point is to describe *Dining* as the cascading of these two channels:

$$\mathit{Dining} = (\mathit{Coins})(\mathit{Announcements}).$$

The intuition behind this decision is to provide channel *Announcements* with the result of the coin tosses, which are necessary to calculate the output of each cryptographer.

To specify channel *Coins*, we use the parallel composition of channels Coin_1, Coin_2, Coin_3 and Coin_4, each representing one coin toss. Letting p_i denote the probability of coin i landing on tails, these channels are defined as in Table 3.2. Besides the result of the tosses, *Coins* also needs to pass on to *Announcements* the identity of the payer. We then introduce a fifth channel, $I \in \mathcal{C}_{\mathcal{X}}^{\mathcal{X}}$, that simply outputs the secret, i.e., $I(x, x') = 1$ if $x = x'$, and 0 otherwise. Hence, a complete definition of channel *Coins* is

$$\mathit{Coins} = \mathit{Coin}_1 \parallel \mathit{Coin}_2 \parallel \mathit{Coin}_3 \parallel \mathit{Coin}_4 \parallel I.$$

$Coin_i$	Tails	Heads
c_1	p_i	$1{-}p_i$
c_2	p_i	$1{-}p_i$
c_3	p_i	$1{-}p_i$
c_4	p_i	$1{-}p_i$
n	p_i	$1{-}p_i$

Table 3.2. Channel representing toss of coin $Coin_i$.

As we proved in Proposition 3.10, parallel composition is associative, allowing us to omit parentheses in the equation above.

We now specify the channel *Announcements*, which should take as input a 5-tuple with five terms. The first four elements are the results of the coin tosses, and the fifth is the identity of the payer. Therefore, the input set of this channel is $\mathcal{X}' = \{Tails, Heads\}^4 \times \mathcal{X}$. The input has all the information necessary to determine the output of each cryptographer, and we describe each participant as a channel with input set $\mathcal{X}'$ and output set $\{0, 1\}$, the possible announcements. For example, the channel $Crypto_1$ below describes the first cryptographer.

$$Crypto_1(t_1, t_2, t_3, t_4, x) = \begin{cases} 1, & \text{if } t_4 = t_1 \text{ and } x = c_1, \text{ or } t_4 \neq t_1 \text{ and } x \neq c_1, \\ 0, & \text{otherwise.} \end{cases}$$

Channels $Crypto_2$, $Crypto_3$ and $Crypto_4$ describing the remaining cryptographers are defined analogously. Channel *Announcements* is, hence, defined as

$$Announcements = Crypto_1 \parallel Crypto_2 \parallel Crypto_3 \parallel Crypto_4.$$

Note that our operators allow for an intuitive and succinct representation of the channel *Dining* modelling the Dining Cryptographers protocol, even when the number of cryptographers and coins is large.

The model we developed in this section gives us a straightforward way of calculating the channel of the protocol. In Table 3.3 we present the corresponding channels for three cryptographers in three different scenarios. The top channel $Dining_1$ depicts a situation when all coins are fair. The middle one, $Dining_2$, a situation when they are all equal but unfair. Finally, channel $Dining_3$ at the bottom represents a scenario in which the coins are all different.

Since half of the outputs occur if and only if the secret is one of the cryptographers, we can see that the protocol completely reveals whether the NSA is paying for dinner in all three channels. Moreover, the fact that the first three lines in $Dining_1$ are equal shows that no information is leaked regarding which cryptographer is the payer if the coins are fair.

$Dining_1$	001	010	100	111	000	011	101	110
c_1	0.25	0.25	0.25	0.25	0	0	0	0
c_2	0.25	0.25	0.25	0.25	0	0	0	0
c_3	0.25	0.25	0.25	0.25	0	0	0	0
n	0	0	0	0	0.25	0.25	0.25	0.25

$Dining_2$	001	010	100	111	000	011	101	110
c_1	0.21	0.21	0.37	0.21	0	0	0	0
c_2	0.21	0.37	0.21	0.21	0	0	0	0
c_3	0.37	0.21	0.21	0.21	0	0	0	0
n	0	0	0	0	0.37	0.21	0.21	0.21

$Dining_3$	001	010	100	111	000	011	101	110
c_1	0.18	0.26	0.36	0.2	0	0	0	0
c_2	0.2	0.36	0.26	0.18	0	0	0	0
c_3	0.36	0.2	0.18	0.26	0	0	0	0
n	0	0	0	0	0.36	0.2	0.18	0.26

Table 3.3. Channels $Dining_1$, in which $p_1 = p_2 = p_3 = 0.5$; $Dining_2$, in which $p_1 = p_2 = p_3 = 0.7$, and $Dining_3$, in which $p_1 = 0.6$, $p_2 = 0.7$ and $p_3 = 0.8$.

To analyse the leakage of these channels, we need to define a suitable gain function. We consider an adversary that is interested in obtaining the identity of a possible payer among the cryptographers, but not interested in the scenario in which the NSA is paying. A possible gain function with set of actions $\mathcal{W} = \{c_1, c_2, c_3\}$ (in which action c_i means the adversary guesses the payer is the cryptographer c_i) is given by

$$g_D(x, x') = \begin{cases} 1, & \text{if } x = x', \\ 0, & \text{otherwise.} \end{cases}$$

That is, the adversary gains whenever he guesses the correct identity of the payer, unless it is the NSA. Consider the uniform prior $\pi_u = (0.25, 0.25, 0.25, 0.25)$, which yields the g-vulnerability $V_{g_D}[\pi_u] = 0.25$. The corresponding posterior g-vulnerabilities are

$$V_{g_D}[\pi_u \rangle\, Dining_1] = 0.25,$$
$$V_{g_D}[\pi_u \rangle\, Dining_2] = 0.33,$$

$$V_{g_D}[\pi_u \rangle \mathit{Dining}_3] = 0.335.$$

As expected, the channel Dining_1 does not increase the vulnerability of the secret, which reflects the complete secrecy of the protocol when the coins are fair. The same cannot be said about channels Dining_2 and Dining_3, that additively increase the g-vulnerability of the secret by 0.08 and 0.085, respectively.

Chapter 4

Leakage Properties

In this chapter we discuss the main contribution of this thesis: a series of results showing how, using the proposed algebra, we can facilitate the security analysis of compound systems. More specifically, we tackle the two specific objectives presented in Section 1.2.1 for our operators.

For the remaining of the section, let $C_1 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_1}$ and $C_2 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_2}$ be compatible channels. We also recall Definition 3.1: for all $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$, we define $C(x, y) = 0$ for all $y \notin \mathcal{Y}$.

4.1 The problem of compositional vulnerability

The first problem consists in estimating the information leakage of a composition in terms of the leakage of its components. This can be formalized as follows.

The problem of compositional vulnerability: *Given a composition operator $*$ on channels, a prior π, and a gain function g, can we describe $V_g[\pi \rangle C_1 * C_2]$ in terms of $V_g[\pi \rangle C_1]$ and $V_g[\pi \rangle C_2]$?*

4.1.1 Compositional vulnerability for the parallel operator

There is no description of $V_g[\pi \rangle C_1 \parallel C_2]$ as a function of $V_g[\pi \rangle C_1]$ and $V_g[\pi \rangle C_2]$ that holds for all channels C_1, C_2 and prior π.

For example, consider the following channels and their parallel composition.

C_1	y_1	y_2
x_1	1	0
x_2	1	0
x_3	0	1

C_2	y_1	y_2
x_1	1	0
x_2	0	1
x_3	0	1

$C_1 \parallel C_2$	(y_1, y_1)	(y_1, y_2)	(y_2, y_1)	(y_2, y_2)
x_1	1	0	0	0
x_2	0	1	0	0
x_3	0	0	0	1

Consider also the composition $C_1 \parallel C_1$, that is equivalent to C_1 by Proposition 3.12. Let g_{id} be as in Definition 2.10, and $\pi_u = (1/3, 1/3, 1/3)$.

We have that $V_{g_{id}}[\pi_u \rangle C_1] = V_{g_{id}}[\pi_u \rangle C_2] = 2/3$. Therefore, if the g-vulnerability of a parallel composition could be described as a function of the g-vulnerability of its components, $V_{g_{id}}[\pi \rangle C_1 \parallel C_1]$ would be equal to $V_{g_{id}}[\pi \rangle C_1 \parallel C_2]$. However, we have $V_{g_{id}}[\pi_u \rangle C_1 \parallel C_1] = 2/3$ and $V_{g_{id}}[\pi_u \rangle C_1 \parallel C_2] = 1$.

For the parallel composition, therefore, we shall explore upper and lower bounds. We start with the following theorem, proving that the g-vulnerability of a parallel composition is at least as high as that of its components.

Theorem 4.1 (Lower bound for V_g w.r.t. $\parallel$). *For all $g \in \mathbb{G}\mathcal{X}$ and all $\pi \in \mathbb{D}\mathcal{X}$,*

$$V_g[\pi \rangle C_1 \| C_2] \geq \max(V_g[\pi \rangle C_1], V_g[\pi \rangle C_2]).$$

Proof. For all $\pi \in \mathbb{D}\mathcal{X}$ and $g \in \mathbb{G}\mathcal{X}$,

$$\begin{aligned}
& V_g[\pi \rangle C_1 \parallel C_2] \\
= & \sum_{y_1 \in \mathcal{Y}_1} \sum_{y_2 \in \mathcal{Y}_2} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} (C_1 \parallel C_2)(x, (y_1, y_2)) g(w, x) \pi(x) && \text{(by Prop 2.22)} \\
= & \sum_{y_1 \in \mathcal{Y}_1} \sum_{y_2 \in \mathcal{Y}_2} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} C_1(x, y_1) C_2(x, y_2) g(w, x) \pi(x) && \text{(by def. of } \parallel) \\
\geq & \sum_{y_1 \in \mathcal{Y}_1} \max_{w \in \mathcal{W}} \sum_{y_2 \in \mathcal{Y}_2} \sum_{x \in \mathcal{X}} C_1(x, y_1) C_2(x, y_2) g(w, x) \pi(x) && \text{(moving max outside a sum)} \\
= & \sum_{y_1 \in \mathcal{Y}_1} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} C_1(x, y_1) g(w, x) \pi(x) \sum_{y_2 \in \mathcal{Y}_2} C_2(x, y_2) && \text{(rearranging)} \\
= & \sum_{y_1 \in \mathcal{Y}_1} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} C_1(x, y_1) g(w, x) \pi(x) && (C_2 \text{ is a channel}) \\
= & V_g[\pi \rangle C_1] && \text{(by Prop. 2.22)}
\end{aligned}$$

The proof that $V_g[\pi \rangle C_1 \parallel C_2] \geq V_g[\pi \rangle C_2]$ is analogous.

□

We present now the upper bound for V_g with regard to the parallel composition. It is obtained by multiplying the g-vulnerability of a component by the sum of the biggest values of the other channel for each output. This upper bound is easy to calculate from the description of C_1 and C_2, and can be specially useful when the channel $C_1 \parallel C_2$ is very large — that is, when the size of the input and output sets makes the calculation of V_g computationally infeasible.

Theorem 4.2 (Upper bound for V_g w.r.t. $\parallel$)**.** *For all $g \in \mathbb{G}\mathcal{X}$ and all $\pi \in \mathbb{D}\mathcal{X}$, let $\mathcal{X}' = \{x{\in}\mathcal{X} \mid \exists w{\in}\mathcal{W};\ \pi(x)g(w,x) > 0\}$. Then*

$$V_g[\pi\,\rangle\, C_1 \| C_2] \leq \min\left(V_g[\pi\,\rangle\, C_1] \sum_{y_2\in\mathcal{Y}_2} \max_{x\in\mathcal{X}'} C_2(x,y_2),\ V_g[\pi\,\rangle\, C_2] \sum_{y_1\in\mathcal{Y}_1} \max_{x\in\mathcal{X}'} C_1(x,y_1) \right).$$

Proof. For all $\pi \in \mathbb{D}\mathcal{X}$ and $g \in \mathbb{G}\mathcal{X}$,

$$\begin{aligned}
& V_g[\pi\,\rangle\, C_1 \parallel C_2] \\
&= \sum_{y_2\in\mathcal{Y}_2} \sum_{y_1\in\mathcal{Y}_1} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} (C_1 \parallel C_2)(x,(y_1,y_2))g(w,x)\pi(x) && \text{(by Prop. 2.22)} \\
&= \sum_{y_2\in\mathcal{Y}_2} \sum_{y_1\in\mathcal{Y}_1} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} C_1(x,y_1)C_2(x,y_2)g(w,x)\pi(x) && \text{(by def. of } \|) \\
&= \sum_{y_2\in\mathcal{Y}_2} \sum_{y_1\in\mathcal{Y}_1} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}'} C_1(x,y_1)C_2(x,y_2)g(w,x)\pi(x) \\
& \text{(if } x \notin \mathcal{X}',\ g(w,x)\pi(x) = 0\text{)} \\
&\leq \sum_{y_2\in\mathcal{Y}_2} \sum_{y_1\in\mathcal{Y}_1} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}'} C_1(x,y_1) \left(\max_{x'\in\mathcal{X}'} C_2(x',y_2) \right) g(w,x)\pi(x) \\
& \text{(for all } x \in \mathcal{X}',\ C_2(x,y_2) \leq \max_{x'\in\mathcal{X}'} C_2(x',y_2)) \\
&= \sum_{y_2\in\mathcal{Y}_2} \max_{x'\in\mathcal{X}'} C_2(x',y_2) \sum_{y_1\in\mathcal{Y}_1} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}'} C_1(x,y_1)g(w,x)\pi(x) && \text{(rearranging)} \\
&= \sum_{y_2\in\mathcal{Y}_2} \max_{x\in\mathcal{X}'} C_2(x,y_2) V_g[\pi\,\rangle\, C_1] && \text{(by Prop. 2.22)} \\
&= V_g[\pi\,\rangle\, C_1] \sum_{y_2\in\mathcal{Y}_2} \max_{x\in\mathcal{X}'} C_2(x,y_2)
\end{aligned}$$

The proof that $V_g[\pi\,\rangle\, C_1 \parallel C_2] \leq V_g[\pi\,\rangle\, C_2] \sum_{y_1\in\mathcal{Y}_1} \max_{x\in\mathcal{X}'} C_1(x,y_1)$ is analogous.

□

4.1.2 Compositional vulnerability for visible choice

Contrary to the parallel composition, the g-vulnerability of the visible choice composition can be easily calculated from the g-vulnerability of its components.

Theorem 4.3 (Linearity of V_g w.r.t. ${}_p\sqcup$). *For all $g \in \mathbb{G}\mathcal{X}$, $\pi \in \mathbb{D}\mathcal{X}$ and $p \in [0,1]$,*

$$V_g[\pi \rangle C_1 \ {}_p\sqcup \ C_2] = pV_g[\pi \rangle C_1] + (1-p)V_g[\pi \rangle C_2].$$

Proof. For all $\pi \in \mathbb{D}\mathcal{X}$, $g \in \mathbb{G}\mathcal{X}$ and $p \in [0,1]$,

$$\begin{aligned}
&V_g[\pi \rangle C_1 \ {}_p\sqcup \ C_2] \\
=&\sum_{(y,i)\in\mathcal{Y}_1\sqcup\mathcal{Y}_2} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} (C_1 \ {}_p\sqcup \ C_2)(x,(y,i))g(w,x)\pi(x) && \text{(by Prop. 2.22)} \\
=&\sum_{y\in\mathcal{Y}_1} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} (C_1 \ {}_p\sqcup \ C_2)(x,(y,1))g(w,x)\pi(x) \\
&+\sum_{y\in\mathcal{Y}_2} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} (C_1 \ {}_p\sqcup \ C_2)(x,(y,2))g(w,x)\pi(x) && \text{(separating } \mathcal{Y}_1 \text{ and } \mathcal{Y}_2\text{)} \\
=&\sum_{y\in\mathcal{Y}_1} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} pC_1(x,y)g(w,x)\pi(x) \\
&+\sum_{y\in\mathcal{Y}_2} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} (1-p)C_2(x,y)g(w,x)\pi(x) && \text{(by def. of } {}_p\sqcup\text{)} \\
=&pV_g[\pi \rangle C_1] + (1-p)V_g[\pi \rangle C_2] && \text{(by Prop. 2.22)}
\end{aligned}$$

□

4.1.3 Compositional vulnerability for hidden choice

The g-vulnerability of a hidden choice composition, however, cannot be assessed simply from the g-vulnerability of its components. Consider, for example, the following channels and compositions.

C_1	y_1	y_2
x_1	1	0
x_2	0	1

C_2	y_1	y_2
x_1	0	1
x_2	1	0

$C_1 \ {}_{1/2}\oplus \ C_1$	y_1	y_2
x_1	1	0
x_2	0	1

$C_1 \ {}_{1/2}\oplus \ C_2$	y_1	y_2
x_1	$1/2$	$1/2$
x_2	$1/2$	$1/2$

Despite the fact that $C_1 \approx C_2$, and therefore $V_g[\pi \rangle C_1] = V_g[\pi \rangle C_2]$ for any prior π and gain function g, we have that $C_1 \ {}_{1/2}\oplus \ C_1$ is a transparent channel, while $C_1 \ {}_{1/2}\oplus \ C_2$ is a null channel.

However, it is possible to establish upper and lower bounds for $V_g[\pi \rangle C_1 \ {}_p\oplus \ C_2]$ from the g-vulnerabilities of C_1 and C_2. In Chapter 5, we use these bounds to obtain an algorithm to estimate the channel of the *Crowds* protocol [Reiter and Rubin, 1998].

We start by presenting a lower bound. Loosely speaking, the channel $C_1 \ {}_p\oplus \ C_2$ can be seen as multiplying the values of C_1 by p, of C_2 by $1-p$, and summing them together. This bound is a consequence of the equation for V_g in Proposition 2.22 being monotonically non-decreasing on each channel entry.

Theorem 4.4 (Lower bound for V_g w.r.t. ${}_p\oplus$). *For all $g \in \mathbb{G}\mathcal{X}$, $\pi \in \mathbb{D}\mathcal{X}$ and $p \in [0,1]$,*

$$V_g[\pi\rangle C_1 \;{}_p\!\oplus C_2] \geq \max(pV_g[\pi\rangle C_1], (1-p)V_g[\pi\rangle C_2]).$$

Proof. For all $\pi \in \mathcal{X}$, $g \in \mathbb{G}\mathcal{X}$ and $p \in [0,1]$,

$$\begin{aligned}
&V_g[\pi\rangle C_1 \;{}_p\!\oplus C_2] \\
&= \sum_{y \in \mathcal{Y}_1 \cup \mathcal{Y}_2} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} (C_1 \;{}_p\!\oplus C_2)(x,y)g(w,x)\pi(x) && \text{(by Prop. 2.22)} \\
&= \sum_{y \in \mathcal{Y}_1 \cup \mathcal{Y}_2} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} (pC_1(x,y) + (1-p)C_2(x,y))g(w,x)\pi(x) && \text{(by def. of } {}_p\!\oplus) \\
&\geq \sum_{y \in \mathcal{Y}_1} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} (pC_1(x,y) + (1-p)C_2(x,y))g(w,x)\pi(x) && \text{(sub. nonegative terms)} \\
&\geq \sum_{y \in \mathcal{Y}_1} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} pC_1(x,y)g(w,x)\pi(x) && (C_2(x,y) \geq 0) \\
&= pV_g[\pi\rangle C_1] && \text{(by Prop. 2.22)}
\end{aligned}$$

The proof that $V_g[\pi\rangle C_1 \;{}_p\!\oplus C_2] \geq (1-p)V_g[\pi\rangle C_2]$ is similar.

□

Our next result shows that the g-vulnerability of a hidden choice of two channels is never greater than that of a visible choice of the same channels, with regard to the same probability p. This is intuitive, since the adversary has access to extra information in the visible choice scenario — namely, which component was executed.

Theorem 4.5 (Upper bound for V_g w.r.t. ${}_p\oplus$). *For all $g \in \mathbb{G}\mathcal{X}$, $\pi \in \mathbb{D}\mathcal{X}$ and $p \in [0,1]$,*

$$V_g[\pi\rangle C_1 \;{}_p\!\oplus C_2] \leq pV_g[\pi\rangle C_1] + (1-p)V_g[\pi\rangle C_2].$$

Proof. For all $\pi \in \mathbb{D}\mathcal{X}$, $g \in \mathbb{G}\mathcal{X}$ and $p \in [0,1]$,

$$\begin{aligned}
&V_g[\pi\rangle C_1 \;{}_p\!\oplus C_2] \\
&= \sum_{y \in \mathcal{Y}_1 \cup \mathcal{Y}_2} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} (C_1 \;{}_p\!\oplus C_2)(x,y)g(w,x)\pi(x) && \text{(by Prop. 2.22)} \\
&= \sum_{y \in \mathcal{Y}_1 \cup \mathcal{Y}_2} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} (pC_1(x,y) + (1-p)C_2(x,y))g(w,x)\pi(x) && \text{(by def. of } {}_p\!\oplus)
\end{aligned}$$

$$\begin{aligned}
&= \sum_{y\in\mathcal{Y}_1\cap\mathcal{Y}_2} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} (pC_1(x,y) + (1-p)C_2(x,y))g(w,x)\pi(x) \\
&\quad + \sum_{y\in\mathcal{Y}_1\setminus\mathcal{Y}_2} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} pC_1(x,y)g(w,x)\pi(x) \\
&\quad + \sum_{y\in\mathcal{Y}_2\setminus\mathcal{Y}_1} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} (1-p)C_2(x,y)g(w,x)\pi(x) && (C_i(x,y) = 0 \text{ if } y \notin \mathcal{Y}_i) \\
&\leq \sum_{y\in\mathcal{Y}_1\cap\mathcal{Y}_2} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} pC_1(x,y)g(w,x)\pi(x) \\
&\quad + \sum_{y\in\mathcal{Y}_1\cap\mathcal{Y}_2} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} (1-p)C_2(x,y)g(w,x)\pi(x) \\
&\quad + \sum_{y\in\mathcal{Y}_1\setminus\mathcal{Y}_2} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} pC_1(x,y)g(w,x)\pi(x) \\
&\quad + \sum_{y\in\mathcal{Y}_2\setminus\mathcal{Y}_1} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} (1-p)C_2(x,y)g(w,x)\pi(x) && \text{(distributing the max)} \\
&= \sum_{y\in\mathcal{Y}_1} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} pC_1(x,y)g(w,x)\pi(x) \\
&\quad + \sum_{y\in\mathcal{Y}_2} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} (1-p)C_2(x,y)g(w,x)\pi(x) && \text{(rearranging)} \\
&= pV_g[\pi \rangle C_1] + (1-p)V_g[\pi \rangle C_2] && \text{(by Prop. 2.22)}
\end{aligned}$$

□

Theorems 4.1, 4.3 and 4.5 above yield an interesting ordering between these three operators.

Corollary 4.6 (Ordering between $\|$, ${}_p\sqcup$ and ${}_p\oplus$)**.** *For all* $p \in [0,1]$,

$$C_1 \parallel C_2 \sqsubseteq_\circ C_1 \;{}_p\sqcup\; C_2 \sqsubseteq_\circ C_1 \;{}_p\oplus\; C_2.$$

Proof. We have that $pV_g[\pi \rangle C_1] + (1-p)V_g[\pi \rangle C_2] \leq \max(V_g[\pi \rangle C_1], V_g[\pi \rangle C_2])$, so Theorems 4.1 and 4.3 yield $C_1 \parallel C_2 \sqsubseteq_\circ C_1 \;{}_p\sqcup\; C_2$. That $C_1 \;{}_p\sqcup\; C_2 \sqsubseteq_\circ C_1 \;{}_p\oplus\; C_2$ is clear from Theorems 4.3 and 4.5. □

We emphasize that the relation $C_1 \;{}_p\sqcup\; C_2 \sqsubseteq_\circ C_1 \;{}_p\oplus\; C_2$ is only valid for a given p. In general, $C_1 \;{}_p\sqcup\; C_2 \sqsubseteq_\circ C_1 \;{}_q\oplus\; C_2$ is *not* true when $p \neq q$.

4.1.4 Channel and vulnerability restrictions

In contrast to the other operators, both the visible and hidden if-then-else operators have the peculiarity of partially disregarding the channels they act on. For example, the values of $C_1(x,y)$ for $x \in \bar{\mathcal{A}}$ have no influence on channels $C_1 \, {}_{\mathcal{A}}\!\triangle\, C_2$ or $C_1 \, {}_{\mathcal{A}}\!\triangle\kern-0.75em{\scriptstyle +}\kern0.3em C_2$.

Therefore, any result linking leakage properties of these compositions to $V_g[\pi\rangle C_1]$ and $V_g[\pi\rangle C_2]$, which take the whole channels C_1 and C_2 into account, is bound to be somewhat coarse. We are able to do much better, instead, by expressing their leakage properties in terms of *restrictions* on those channels and gain functions. We define those restrictions, and some of their properties, as follows.

Definition 4.7. *Let $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ be a channel and $\mathcal{A} \subset \mathcal{X}$. We define the* restriction of channel *C to $\mathcal{A}$, $C|_{\mathcal{A}} : \mathcal{A} \times \mathcal{Y} \to [0,1]$, as $C|_{\mathcal{A}}(x,y) = C(x,y)$ for all $x \in \mathcal{A}$, $y \in \mathcal{Y}$.*

It is worth noting that $C|_{\mathcal{A}}$ is a channel in its own right.

Definition 4.8. *Let $\mathcal{X}$ be an input set, $\mathcal{A} \subset \mathcal{X}$, and $g \in \mathbb{G}\mathcal{X}$. We define the* subset gain function *$g_{\mathcal{A}} : \mathcal{W} \times \mathcal{X} \to [0,1]$ of g w.r.t. $\mathcal{A}$ as, for all $w \in \mathcal{W}$ and $x \in \mathcal{X}$,*

$$g_{\mathcal{A}}(w,x) = \begin{cases} g(w,x), & \textit{if } x \in \mathcal{A}, \\ 0, & \textit{otherwise.} \end{cases}$$

The idea of the subset gain function $g_{\mathcal{A}}$ is that it considers only the values of the channel for which $x \in \mathcal{A}$. That is, for all $\pi \in \mathbb{D}\mathcal{X}$, $g \in \mathbb{G}\mathcal{X}$ and $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$,

$$V_{g_{\mathcal{A}}}[\pi\rangle C] = \sum_{y \in \mathcal{Y}} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} C(x,y) g_{\mathcal{A}}(w,y) \pi(x) = \sum_{y \in \mathcal{Y}} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{A}} C(x,y) g(w,y) \pi(x).$$

We now introduce two results relating channel restrictions to subset gain functions, which will be useful when investigating leakage properties of the visible and hidden if-then-else operators.

Proposition 4.9. *Let $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$, $\mathcal{A} \subset \mathcal{X}$, $g \in \mathbb{G}\mathcal{X}$ and $\pi \in \mathcal{X}$. Then,*

$$V_{g_{\mathcal{A}}}[\pi\rangle C] = V_{g'}[\pi'\rangle C|_{\mathcal{A}}] \sum_{x \in \mathcal{A}} \pi(x),$$

where $\pi' \in \mathbb{D}\mathcal{A}$ is defined as $\pi'(x) = \frac{\pi(x)}{\sum_{x' \in \mathcal{A}} \pi(x')}$ for all $x \in \mathcal{X}$, and $g' \in \mathbb{G}\mathcal{A}$ is a gain function with the same set of actions $\mathcal{W}$ as g, defined as $g'(w,x) = g(w,x)$ for all $w \in \mathcal{W}$ and $x \in \mathcal{A}$.

Proof.

$$\begin{aligned} & V_{g_{\mathcal{A}}}[\pi\rangle C] \\ = & \sum_{y \in \mathcal{Y}} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{A}} C(x,y) \pi(x) g_{\mathcal{A}}(w,x) && \text{(by Prop. 2.22)} \end{aligned}$$

$$
\begin{aligned}
&= \left(\sum_{x\in\mathcal{A}} \pi(x)\right) \sum_{y\in\mathcal{Y}} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{A}} C(x,y) g_{\mathcal{A}}(w,x) \frac{\pi(x)}{\sum_{x'\in\mathcal{A}} \pi(x')} && \text{(mul. and div. by } \textstyle\sum_{x\in\mathcal{A}} \pi(x))\\
&= \left(\sum_{x\in\mathcal{A}} \pi(x)\right) \sum_{y\in\mathcal{Y}} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{A}} C(x,y) g'(w,x) \pi'(x) && \text{(by def. of } \pi',\ g')\\
&= V_{g'}[\pi' \rangle C|_{\mathcal{A}}] \sum_{x\in\mathcal{A}} \pi(x) && \text{(by Prop. 2.22)}
\end{aligned}
$$

□

Corollary 4.10. $C_2|_{\mathcal{A}} \sqsubseteq_\circ C_1|_{\mathcal{A}} \iff \forall \pi \in \mathbb{D}\mathcal{X}, \forall g \in \mathbb{G}\mathcal{X}.\ V_{g_{\mathcal{A}}}[\pi \rangle C_1] \le V_{g_{\mathcal{A}}}[\pi \rangle C_2]$.

Proof. Let $\pi \in \mathbb{D}\mathcal{X}$, $g \in \mathbb{G}\mathcal{X}$, and define $\pi' \in \mathbb{D}\mathcal{X}$, $g' \in \mathbb{G}\mathcal{A}$ as in Proposition 4.9. Then, by the same proposition,

$$C_2|_{\mathcal{A}} \sqsubseteq_\circ C_1|_{\mathcal{A}} \implies V_{g'}[\pi' \rangle C_1|_{\mathcal{A}}] \le V_{g'}[\pi' \rangle C_2|_{\mathcal{A}}] \implies V_{g_{\mathcal{A}}}[\pi \rangle C_1] \le V_{g_{\mathcal{A}}}[\pi \rangle C_2].$$

Conversely, let $\pi \in \mathcal{A}$ and $g \in \mathbb{G}\mathcal{A}$. Define $\pi \in \mathbb{D}\mathcal{X}$ as $\pi'(x) = \pi(x)$ if $x \in \mathcal{A}$ and 0 otherwise, and define $g' \in \mathbb{G}\mathcal{X}$ similarly. Then, the left side of the equivalence implies $V_g[\pi \rangle C_1|_{\mathcal{A}}] \le V_g[\pi \rangle C_2|_{\mathcal{A}}]$. □

After this little detour, we are ready to present the compositional vulnerability results of the visible and hidden if-then-else operators.

4.1.5 Compositional vulnerability for visible if-then-else

Despite not being able to calculate $V_g[\pi \rangle C_1 \ {}_{\mathcal{A}}\triangle\ C_2]$ from $V_g[\pi \rangle C_1]$ and $V_g[\pi \rangle C_2]$, as the visible if-then-else composition only takes into account part of the channels of the components, we can fully describe it in terms of $V_{g_{\mathcal{A}}}[\pi \rangle C_1]$ and $V_{g_{\bar{\mathcal{A}}}}[\pi \rangle C_2]$, where $g_{\mathcal{A}}$, $g_{\bar{\mathcal{A}}}$ are defined as in Definition 4.8.

Theorem 4.11 (Linearity of V_g w.r.t ${}_{\mathcal{A}}\triangle$). *For all $\pi \in \mathbb{D}\mathcal{X}$, all sets $\mathcal{A} \subset \mathcal{X}$, and all $g \in \mathbb{G}\mathcal{X}$,*

$$V_g[\pi \rangle C_1 \ {}_{\mathcal{A}}\triangle\ C_2] = V_{g_{\mathcal{A}}}[\pi \rangle C_1] + V_{g_{\bar{\mathcal{A}}}}[\pi \rangle C_2].$$

Proof.

$$
\begin{aligned}
&V_g[\pi \rangle C_1 \ {}_{\mathcal{A}}\triangle\ C_2]\\
&= \sum_{(y,i)\in\mathcal{Y}_1\sqcup\mathcal{Y}_2} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} (C_1 \ {}_{\mathcal{A}}\triangle\ C_2)(x,(y,i)) \pi(x) g(w,x) && \text{(by Prop. 2.22)}\\
&= \sum_{(y,i)\in\mathcal{Y}_1\times\{1\}} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} (C_1 \ {}_{\mathcal{A}}\triangle\ C_2)(x,(y,i)) \pi(x) g(w,x)
\end{aligned}
$$

$$
\begin{aligned}
&+ \sum_{(y,i)\in\mathcal{Y}_2\times\{2\}} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} (C_1 \,{}_{\mathcal{A}}\!\triangle\, C_2)(x,(y,i))\pi(x)g(w,x) && \text{(distributing)}\\
&= \sum_{y\in\mathcal{Y}_1} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{A}} C_1(x,y)\pi(x)g(w,x)\\
&+ \sum_{y\in\mathcal{Y}_2} \max_{w\in\mathcal{W}} \sum_{x\in\bar{\mathcal{A}}} C_2(x,y)\pi(x)g(w,x) && \text{(by def. of } {}_{\mathcal{A}}\!\triangle\text{)}\\
&= V_{g_{\mathcal{A}}}[\pi\rangle C_1] + V_{g_{\bar{\mathcal{A}}}}[\pi\rangle C_2] && \text{(by Prop. 2.22)}
\end{aligned}
$$

□

4.1.6 Compositional vulnerability for hidden if-then-else

In an interesting parallel to visible and hidden choice, the g-vulnerability of a hidden if-then-else composition cannot, in general, be calculated simply from $V_{g_{\mathcal{A}}}[\pi\rangle C_1]$ and $V_{g_{\bar{\mathcal{A}}}}[\pi\rangle C_2]$, contrary to its visible counterpart.

As an example, consider the following channels and compositions, with $\mathcal{A}=\{x_1\}$.

C_1	y_1	y_2
x_1	1	0
x_2	0	1

C_2	y_1	y_2
x_1	0	1
x_2	1	0

$C_1 \,{}_{\mathcal{A}}\text{⟁}\, C_1$	y_1	y_2
x_1	1	0
x_2	0	1

$C_1 \,{}_{\mathcal{A}}\text{⟁}\, C_2$	y_1	y_2
x_1	1	0
x_2	1	0

We have that $C_1 \approx C_2$, and therefore, for any prior π and any gain function g (including $g_{\mathcal{A}}$ and $g_{\bar{\mathcal{A}}}$), $V_g[\pi\rangle C_1] = V_g[\pi\rangle C_2]$. However, $C_1 \,{}_{\mathcal{A}}\text{⟁}\, C_1$ is a transparent channel, and $C_1 \,{}_{\bar{\mathcal{A}}}\text{⟁}\, C_2$ is a null channel, which implies there is no general way of calculating $V_g[\pi\rangle C_1 \,{}_{\mathcal{A}}\text{⟁}\, C_2]$ simply from $V_{g_{\mathcal{A}}}[\pi\rangle C_1]$ and $V_{g_{\bar{\mathcal{A}}}}[\pi\rangle C_2]$.

The next result establishes a lower bound for the hidden if-then-else, which states that the g-leakage of the hidden if-then-else of two channels is never less than that of its components, w.r.t. the appropriate subset gain functions.

Theorem 4.12 (Lower bound for V_g w.r.t ${}_{\mathcal{A}}\text{⟁}$). *For all $\pi\in\mathbb{D}\mathcal{X}$, all sets $\mathcal{A}\subset\mathcal{X}$ and all $g\in\mathbb{G}\mathcal{X}$,*

$$
V_g[\pi\rangle C_1 \,{}_{\mathcal{A}}\text{⟁}\, C_2] \geq \max(V_{g_{\mathcal{A}}}[\pi\rangle C_1], V_{g_{\bar{\mathcal{A}}}}[\pi\rangle C_2]).
$$

Proof.

$$
\begin{aligned}
&V_g[\pi\rangle C_1 \,{}_{\mathcal{A}}\text{⟁}\, C_2]\\
&= \sum_{y\in\mathcal{Y}_1\cup\mathcal{Y}_2} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} (C_1 \,{}_{\mathcal{A}}\text{⟁}\, C_2)(x,y)\pi(x)g(w,x) && \text{(by Prop. 2.22)}
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{y\in\mathcal{Y}_1\cup\mathcal{Y}_2} \max_{w\in\mathcal{W}} \left(\sum_{x\in\mathcal{A}} C_1(x,y)\pi(x)g(w,x) \right.\\
&\qquad \left. + \sum_{x\in\bar{\mathcal{A}}} C_2(x,y)\pi(x)g(w,x) \right) && \text{(by def. of } {}_{\mathcal{A}}\triangle\text{)}\\
&\geq \sum_{y\in\mathcal{Y}_1\cup\mathcal{Y}_2} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{A}} C_1(x,y)\pi(x)g(w,x) && \text{(subtracting nonegative terms)}\\
&= \sum_{y\in\mathcal{Y}_1} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{A}} C_1(x,y)\pi(x)g(w,x) && (C_1(x,y)=0 \text{ if } y\notin\mathcal{Y}_1)\\
&= V_{g_{\mathcal{A}}}[\pi\rangle C_1] && \text{(by Prop. 2.22)}
\end{aligned}
$$

The proof that $V_g[\pi\rangle C_1 \mathbin{{}_{\mathcal{A}}\triangle} C_2] \geq V_{g_{\bar{\mathcal{A}}}}[\pi\rangle C_2]$ is similar. □

The visible if-then-else of two channels always reveals at least as much information as its hidden counterpart. This is intuitive, since the former chooses to execute each component in the same manner as the latter, but informs the adversary of the choice. The next theorem proves this intuition, providing an upper bound for the g-vulnerability of the hidden if-then-else composition.

Theorem 4.13 (Upper bound for V_g w.r.t ${}_{\mathcal{A}}\triangle$)**.** *For all $\pi \in \mathbb{D}\mathcal{X}$, all sets $\mathcal{A} \subset \mathcal{X}$, and all $g \in \mathbb{G}\mathcal{X}$,*

$$V_g[\pi\rangle C_1 \mathbin{{}_{\mathcal{A}}\triangle} C_2] \leq V_{g_{\mathcal{A}}}[\pi\rangle C_1] + V_{g_{\bar{\mathcal{A}}}}[\pi\rangle C_2].$$

Proof.

$$
\begin{aligned}
&V_g[\pi\rangle C_1 \mathbin{{}_{\mathcal{A}}\triangle} C_2]\\
&= \sum_{y\in\mathcal{Y}_1\cup\mathcal{Y}_2} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} (C_1 \mathbin{{}_{\mathcal{A}}\triangle} C_2)(x,y)\pi(x)g(w,x) && \text{(by Prop. 2.22)}\\
&= \sum_{y\in\mathcal{Y}_1\cup\mathcal{Y}_2} \max_{w\in\mathcal{W}} \left(\sum_{x\in\mathcal{A}} C_1(x,y)\pi(x)g(w,x) \right.\\
&\qquad \left. + \sum_{x\in\bar{\mathcal{A}}} C_2(x,y)\pi(x)g(w,x) \right) && \text{(by def. of } {}_{\mathcal{A}}\triangle\text{)}\\
&\leq \sum_{y\in\mathcal{Y}_1\cup\mathcal{Y}_2} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{A}} C_1(x,y)\pi(x)g(w,x)\\
&\qquad + \sum_{y\in\mathcal{Y}_1\cup\mathcal{Y}_2} \max_{w\in\mathcal{W}} \sum_{x\in\bar{\mathcal{A}}} C_2(x,y)\pi(x)g(w,x) && \text{(distributing the max)}\\
&= \sum_{y\in\mathcal{Y}_1} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{A}} C_1(x,y)\pi(x)g(w,x)
\end{aligned}
$$

$$
\begin{aligned}
&+\sum_{y\in\mathcal{Y}_2}\max_{w\in\mathcal{W}}\sum_{x\in\bar{\mathcal{A}}}C_2(x,y)\pi(x)g(w,x) && (C_i(x,y)=0 \text{ if } y\notin\mathcal{Y}_i)\\
=&V_{g_{\mathcal{A}}}[\pi\rangle C_1]+V_{g_{\bar{\mathcal{A}}}}[\pi\rangle C_2] && \text{(by Prop. 2.22)}
\end{aligned}
$$

□

For completeness, we present a corollary similar to Corollary 4.6, concisely stating the ordering relation between the if-then-else operators. This corollary follows immediately from Theorems 4.11 and 4.13.

Corollary 4.14 (Ordering between if-then-else operators). *For all $\mathcal{A}\subset\mathcal{X}$,*

$$C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2 \sqsubseteq_{\circ} C_1 \;{}_{\mathcal{A}}\!\text{⟁}\; C_2.$$

4.2 The problem of relative monotonicity

The second problem concerns establishing whether a component channel of a larger system can be safely substituted with another component, i.e., whether substituting a component with a safer one can cause an increase in the information leakage of the system as a whole. This can be formalized as follows.

The problem of relative monotonicity: *Given a composition operator $*$ on channels, is it the case that*

$$C_2\sqsubseteq_{\circ}C_1 \iff \forall C\in\mathcal{C}_{\mathcal{X}},\ (C_2*C)\sqsubseteq_{\circ}(C_1*C)\,?$$

We recall Theorem 2.32, which states that $C_2\sqsubseteq_{\circ}C_1$ is equivalent to

$$\forall\pi\in\mathbb{D}\mathcal{X},\forall g\in\mathbb{G}\mathcal{X},\ V_g[\pi\rangle C_1]\leq V_g[\pi\rangle C_2].$$

Given an operator $*$, we refer to

$$C_2\sqsubseteq_{\circ}C_1 \implies \forall C\in\mathcal{C}_{\mathcal{X}},\ (C_2*C)\sqsubseteq_{\circ}(C_1*C)$$

as the *direct implication* of relative monotonicity, and to

$$\forall C\in\mathcal{C}_{\mathcal{X}},\ (C_2*C)\sqsubseteq_{\circ}(C_1*C) \implies C_2\sqsubseteq_{\circ}C_1$$

as the *converse implication* of relative monotonicity.

While relative monotonicity does not hold at all for some operators, even stronger results can be found for the others. In this section, for all the operators that relative monotonicity holds, we will try first proving the following stronger equivalence. Given $\pi \in \mathbb{D}\mathcal{X}$ and $g \in \mathbb{G}\mathcal{X}$,

$$V_g[\pi \rangle C_1] \leq V_g[\pi \rangle C_2] \Leftrightarrow \forall C \in \mathcal{C}_{\mathcal{X}},\ V_g[\pi \rangle C_1 * C] \leq V_g[\pi \rangle C_2 * C]. \tag{4.1}$$

These stricter results may be of practical interest in a number of situations in which when we know π and g — i.e., the knowledge and interests of the adversary. It can be handy, in these cases, to establish some form of relative monotonicity even for channels that do not respect the refinement relation in any direction.

4.2.1 Relative monotonicity for the parallel operator

As we will see in this section, relative monotonicity does hold for the parallel operator. However, the direct implication on equivalence (4.1)— i.e., the implication

$$V_g[\pi \rangle C_1] \leq V_g[\pi \rangle C_2] \implies \forall C \in \mathcal{C}_{\mathcal{X}},\ V_g[\pi \rangle C_1 \parallel C] \leq V_g[\pi \rangle C_2 \parallel C] \tag{4.2}$$

does *not* hold for all $\pi \in \mathbb{D}\mathcal{X}$ and all $g \in \mathbb{G}\mathcal{X}$.

As a counter-example, consider the following channels.

C_1	y_1	y_2
x_1	1	0
x_2	1	0
x_3	0	1

C_2	y_1	y_2
x_1	1	0
x_2	0	1
x_3	0	1

Let $\pi_u = (1/3, 1/3, 1/3)$ and let g_{id} be as in Definition 2.10. Then, $V_{g_{id}}[\pi_u \rangle C_1] \leq V_{g_{id}}[\pi_u \rangle C_2]$. However, if we consider the composition of both with C_2, we obtain.

$C_1 \parallel C_2$	(y_1, y_1)	(y_1, y_2)	(y_2, y_1)	(y_2, y_2)
x_1	1	0	0	0
x_2	0	1	0	0
x_3	0	0	0	1

$C_2 \parallel C_2$	(y_1, y_1)	(y_1, y_2)	(y_2, y_1)	(y_2, y_2)
x_1	1	0	0	0
x_2	0	0	0	1
x_3	0	0	0	1

Which yields $V_{g_{id}}[\pi_u \rangle C_1 \parallel C_2] = 1$ and $V_{g_{id}}[\pi_u \rangle C_2 \parallel C_2] = {}^2\!/\!_3$, therefore $V_{g_{id}}[\pi_u \rangle C_1 \parallel C_2] > V_{g_{id}}[\pi_u \rangle C_2 \parallel C_2]$.

There is still, however, a result stricter than relative monotonicity that we can prove for the parallel operator. We present two weaker monotonicity results, obtained by restricting the antecedent in implication 4.2 to a stronger condition: either $\forall \pi \in \mathbb{D}\mathcal{X}$, $V_g[\pi \rangle C_1] \leq V_g[\pi \rangle C_2]$ for a fixed g, or $\forall g \in \mathbb{G}\mathcal{X}$, $V_g[\pi \rangle C_1] \leq V_g[\pi \rangle C_2]$ for a fixed π.

These conditions, despite being more restrictive, are still useful. When we can establish that a channel C_1 is always at least as secure as a channel C_2 for either a given knowledge of the adversary (represented by the prior π) or a given preference of the adversary (represented by the gain function g), we can use them to guarantee that substituting C_1 for C_2 on a parallel composition would not turn the system less secure.

We first enunciate the result for fixed g.

Theorem 4.15. *For all $g \in \mathbb{G}\mathcal{X}$,*

$$\forall \pi \in \mathbb{D}\mathcal{X}, V_g[\pi \rangle C_1] \leq V_g[\pi \rangle C_2] \Rightarrow \forall \pi \in \mathbb{D}\mathcal{X}, \forall C \in \mathcal{C}_{\mathcal{X}}, V_g[\pi \rangle C_1 \parallel C] \leq V_g[\pi \rangle C_2 \parallel C].$$

Proof. We will prove the contrapositive.

Let $g \in \mathbb{G}\mathcal{X}$. Assume that there is a probability distribution $\pi \in \mathbb{D}\mathcal{X}$ and a channel $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Z}}$ such that

$$V_g[\pi \rangle C_1 \parallel C] > V_g[\pi \rangle C_2 \parallel C].$$

From Proposition 2.22, we derive

$$\sum_{z \in \mathcal{Z}} \sum_{y_1 \in \mathcal{Y}_1} \max_{w \in \mathcal{W}} \left(\sum_{x \in \mathcal{X}} C_1(x, y_1) C(x, z) g(w, x) \pi(x) \right) >$$
$$\sum_{z \in \mathcal{Z}} \sum_{y_2 \in \mathcal{Y}_2} \max_{w \in \mathcal{W}} \left(\sum_{x \in \mathcal{X}} C_2(x, y_2) C(x, z) g(w, x) \pi(x) \right).$$

For this inequality to hold, it must be true that, for some $z' \in \mathcal{Z}$,

$$\sum_{y_1 \in \mathcal{Y}_1} \max_{w \in \mathcal{W}} \left(\sum_{x \in \mathcal{X}} C_1(x, y_1) C(x, z') g(w, x) \pi(x) \right) >$$
$$\sum_{y_2 \in \mathcal{Y}_2} \max_{w \in \mathcal{W}} \left(\sum_{x \in \mathcal{X}} C_2(x, y_2) C(x, z') g(w, x) \pi(x) \right).$$

The above inequality also implies that $\sum_{x' \in \mathcal{X}} C(x', z')\pi(x') > 0$, otherwise the left hand-side could not possibly be strictly greater than the right hand-side. We can therefore divide both sides by this quantity. Being a positive constant, we can put it "inside" the max in both sides, yielding

$$\sum_{y_1 \in \mathcal{Y}_1} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \left(C_1(x, y_1) g(w, x) \frac{C(x, z')\pi(x)}{\sum_{x' \in \mathcal{X}} (C(x', z')\pi(x'))} \right) >$$

$$\sum_{y_1 \in \mathcal{Y}_2} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \left(C_2(x, y_2) g(w, x) \frac{C(x, z')\pi(x)}{\sum_{x' \in \mathcal{X}} (C(x', z')\pi(x'))} \right).$$

We now define $\pi' : \mathcal{X} \to \mathbb{R}$ as

$$\pi'(x) = \frac{C(x, z')\pi(x)}{\sum_{x' \in \mathcal{X}} (C(x', z')\pi(x'))}.$$

It is clear that $\pi' \in \mathbb{D}\mathcal{X}$, for it is a non-negative function whose values sum to 1. Therefore, the above inequality reduces to

$$\sum_{y_1 \in \mathcal{Y}_1} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} C_1(x, y_1) g(w, x) \pi'(x) > \sum_{y_2 \in \mathcal{Y}_2} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} C_2(x, y_2) g(w, x) \pi'(x).$$

That is, $V_g[\pi' \rangle C_1] > V_g[\pi' \rangle C_2]$, which completes the proof. □

We now state the direct implication result for when we fix the prior distribution.

Theorem 4.16. *For all $\pi \in \mathbb{D}\mathcal{X}$,*

$$\forall g \in \mathbb{G}\mathcal{X}, V_g[\pi \rangle C_1] \leq V_g[\pi \rangle C_2] \Rightarrow \forall g \in \mathbb{G}\mathcal{X}, \forall C \in \mathcal{C}_{\mathcal{X}}, V_g[\pi \rangle C_1 \parallel C] \leq V_g[\pi \rangle C_2 \parallel C].$$

Proof. The proof is very similar to that of Theorem 4.15. We will, again, prove the contrapositive.

Let π be a prior distribution. Assume that there is a gain function $g \in \mathbb{G}\mathcal{X}$ and a channel $C \in \mathcal{C}_{\mathcal{X}}$ such that

$$V_g[\pi \rangle C_1 \parallel C] > V_g[\pi \rangle C_2 \parallel C].$$

Similarly to the proof of Theorem 4.15, this implies that $\exists z' \in \mathcal{Z}$ such that

$$\sum_{y_1 \in \mathcal{Y}_1} \max_{w \in \mathcal{W}} \left(\sum_{x \in \mathcal{X}} C_1(x, y_1) C(x, z') g(w, x) \pi(x) \right) >$$

$$\sum_{y_2 \in \mathcal{Y}_2} \max_{w \in \mathcal{W}} \left(\sum_{x \in \mathcal{X}} C_2(x, y_2) C(x, z') g(w, x) \pi(x) \right).$$

We now define another gain function $g'(w, x) = C(x, z')g(w, x)$. Substituting this value in the inequality above, we obtain

$$\sum_{y_1 \in \mathcal{Y}_1} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} C_1(x, y_1) g'(w, x) \pi(x) > \sum_{y_2 \in \mathcal{Y}_2} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} C_2(x, y_2) g'(w, x) \pi(x).$$

That is, $V_{g'}[\pi \rangle C_1] > V_{g'}[\pi \rangle C_2]$, which completes the proof. □

As we show in our next result the converse implication of (4.1) holds for the parallel operator.

Theorem 4.17. *For all $\pi \in \mathbb{D}\mathcal{X}$ and all $g \in \mathbb{G}\mathcal{X}$*

$$\forall C \in \mathcal{C}_{\mathcal{X}},\ V_g[\pi \rangle C_1 \parallel C] \leq V_g[\pi \rangle C_2 \parallel C] \implies V_g[\pi \rangle C_1] \leq V_g[\pi \rangle C_2].$$

Proof. Let $\overline{0} \in \mathcal{C}_{\mathcal{X}}$ be a null channel. From Equation 3.16 in Proposition 3.15, we obtain

$$\begin{aligned} & V_g[\pi \rangle C_1] && \\ =& V_g[\pi \rangle C_1 \parallel \overline{0}] && \text{(from Proposition 3.15)} \\ \leq& V_g[\pi \rangle C_2 \parallel \overline{0}] && \text{(from assumption)} \\ =& V_g[\pi \rangle C_2] && \text{(from Proposition 3.15)} \end{aligned}$$

□

Having established the stricter results, we enunciate the original formulation of the relative monotonicity as a corollary.

Corollary 4.18 (Relative monotonicity for $\parallel$)**.**

$$C_2 \sqsubseteq_\circ C_1 \iff \forall C \in \mathcal{C}_{\mathcal{X}},\ (C_2 \parallel C) \sqsubseteq_\circ (C_1 \parallel C).$$

4.2.2 Relative monotonicity for visible choice

For the visible choice operator, the equivalence in (4.1) holds. Note, however, that because $V_g[\pi \rangle C_1 \ {}_p\!\sqcup\ C] \leq V_g[\pi \rangle C_2 \ {}_p\!\sqcup\ C]$ is vacuously true if $p = 0$, we consider only $p \in (0, 1]$.

Theorem 4.19. *For all $g \in \mathbb{G}\mathcal{X}$, $\pi \in \mathbb{D}\mathcal{X}$ and $p \in (0,1]$,*

$$V_g[\pi \rangle C_1] \leq V_g[\pi \rangle C_2] \iff \forall C \in \mathcal{C}_{\mathcal{X}},\ V_g[\pi \rangle C_1 \,{}_p\!\sqcup\, C] \leq V_g[\pi \rangle C_2 \,{}_p\!\sqcup\, C].$$

Proof. For all $p \in (0,1]$, $\pi \in \mathbb{D}\mathcal{X}$ and $g \in \mathbb{G}\mathcal{X}$

$$\begin{aligned}
& V_g[\pi \rangle C_1] \leq V_g[\pi \rangle C_2] \\
\Leftrightarrow & pV_g[\pi \rangle C_1] \leq pV_g[\pi \rangle C_2] && (p > 0) \\
\Leftrightarrow & \forall C \in \mathcal{C}_{\mathcal{X}}.\ pV_g[\pi \rangle C_1] + (1-p)V_g[\pi \rangle C] \\
& \quad \leq pV_g[\pi \rangle C_2] + (1-p)V_g[\pi \rangle C] && \text{(adding in both sides)} \\
\Leftrightarrow & \forall C \in \mathcal{C}_{\mathcal{X}}.\ V_g[\pi \rangle C_1 \,{}_p\!\sqcup\, C] \leq V_g[\pi \rangle C_2 \,{}_p\!\sqcup\, C] && \text{(from Theorem 4.3)}
\end{aligned}$$

□

Corollary 4.20 (Relative monotonicity for ${}_p\!\sqcup$)**.**

$$C_2 \sqsubseteq_\circ C_1 \iff \forall C \in \mathcal{C}_{\mathcal{X}},\ (C_2 \parallel C) \sqsubseteq_\circ (C_1 \parallel C).$$

4.2.3 Relative monotonicity for hidden choice

Perhaps surprisingly, the direct implication of relative monotonicity does not hold for the hidden choice operator.

Theorem 4.21 (Relative monotonicity for ${}_p\oplus$, direct implication)**.** *Let $\mathcal{X}$ be an input set such that $|\mathcal{X}| \geq 2$. For all p$\in$(0,1), there are $C_1, C_2 \in \mathcal{C}_{\mathcal{X}}$ such that*

$$C_2 \sqsubseteq_\circ C_1 \text{ and } \exists \pi \in \mathbb{D}\mathcal{X}, \exists g \in \mathbb{G}\mathcal{X}, \exists C \in \mathcal{C}_{\mathcal{X}},\ V_g[\pi \rangle C_1 \,{}_p\!\oplus\, C] > V_g[\pi \rangle C_2 \,{}_p\!\oplus\, C].$$

Proof. Let $\mathcal{X} = \{x_1, x_2, ..., x_n\}$ be an input set, where $n = |\mathcal{X}|$. Let $\pi_u \in \mathcal{X}$ be such that $\pi_u(x) = {}^1\!/n$ for all $x \in \mathcal{X}$, and let $g_{id} \in \mathbb{G}\mathcal{X}$ be as in Definition 2.10. Furthermore, let $\mathcal{Y} = \{y_1, y_2, ..., y_n\}$ and channels $C_2, C_3 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ defined as

$$C_2(x_i, y_j) = \begin{cases} 1, \text{ if } j = i+1 \text{ or } i = n \text{ and } j = 1, \\ 0, \text{ otherwise,} \end{cases} \qquad C_3(x_i, y_j) = \begin{cases} 1, \text{ if } i = j, \\ 0, \text{ otherwise,} \end{cases}$$

for all $i, j \in \{1, ..., n\}$. We divide the proof in two cases:

Case 1: ($p \leq 0.5$) Let $C_1 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ be defined as follows.

$$C_1(x_i, y_j) = \begin{cases} 1/2, & \text{if } j = 1, \text{ or } j = 2, \\ 0, & \text{otherwise,} \end{cases}$$

for all $i, j \in \{1, ..., n\}$. Notice that C_2 is a transparent channel, and therefore $C_2 \sqsubseteq_{\circ} C_1$.

We have, for all $i, j \in \{1, ..., n\}$,

$$(C_1 \; {}_{p}\!\oplus C_3)(x_i, y_j) = \begin{cases} 1 - p/2, & \text{if } i = j = 1 \text{ or } i = j = 2, \\ 1 - p, & \text{if } i = j \text{ and } i > 2, \\ p/2, & \text{if } j \in \{1, 2\} \text{ and } i \neq j, \\ 0, & \text{otherwise.} \end{cases}$$

$$(C_2 \; {}_{p}\!\oplus C_3)(x_i, y_j) = \begin{cases} 1 - p, & \text{if } i = j, \\ p, & \text{if } j = i + 1 \text{ or } i = n \text{ and } j = 1, \\ 0, & \text{otherwise.} \end{cases}$$

We notice from Proposition 2.22 that for any channel $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$, $V_{g_{id}}[\pi_u \rangle C] = 1/|\mathcal{X}| \sum_{y \in \mathcal{Y}} \max_{x \in \mathcal{X}} C(x, y)$. Therefore, $V_{g_{id}}[\pi_u \rangle C_1 \; {}_{p}\!\oplus C_3] = 1/n(1 + (n-1)(1-p))$ and $V_{g_{id}}[\pi_u \rangle C_2 \; {}_{p}\!\oplus C_3] = 1 - p$. Thus, we have $V_{g_{id}}[\pi_u \rangle C_1 \; {}_{p}\!\oplus C_3] > V_{g_{id}}[\pi_u \rangle C_2 \; {}_{p}\!\oplus C_3]$.

Case 2: ($p > 0.5$) Let $C_1 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ be defined as follows.

$$C_1(x_i, y_j) = \begin{cases} 3/2 - 1/2p, & \text{if } i = j, \\ 1/2p - 1/2, & \text{if } j = i + 1 \text{ or } i = n \text{ and } j = 1, \\ 0, & \text{otherwise.} \end{cases}$$

for all $i, j \in \{1, ..., n\}$. Since C_2 is a transparent channel, $C_2 \sqsubseteq_{\circ} C_1$.

We have, for all $i, j \in \{1, ..., n\}$,

$$(C_1 \; {}_{p}\!\oplus C_3)(x_i, y_j) = \begin{cases} p/2 + 1/2 & \text{if } i = j, \\ 1/2 - p/2 & \text{if } j = i + 1 \text{ or } i = n \text{ and } j = 1, \\ 0 & \text{otherwise.} \end{cases}$$

$$(C_2 \ {}_p\!\oplus C_3)(x_i, y_j) = \begin{cases} 1-p & \text{if } i = j, \\ p & \text{if } j = i+1 \text{ or } i = n \text{ and } j = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Thus, $V_{g_{id}}[\pi_u \rangle C_1 \ {}_p\!\oplus \ C_3] = \frac{1}{2}(p+1)$ and $V_{g_{id}}[\pi_u \rangle C_2 \ {}_p\!\oplus \ C_3] = p$. Hence, $V_{g_{id}}[\pi_u \rangle C_1 \ {}_p\!\oplus C_3] > V_{g_{id}}[\pi_u \rangle C_2 \ {}_p\!\oplus C_3]$. □

The converse implication of relative monotonicity, however, holds even in the stricter form of Equation (4.1).

Theorem 4.22 (Relative monotonicity for ${}_p\!\oplus$, converse implication)**.** *For all $g \in \mathbb{G}\mathcal{X}$, $\pi \in \mathbb{D}\mathcal{X}$ and $p \in (0,1]$,*

$$\forall C \in \mathcal{C}_{\mathcal{X}},\ V_g[\pi \rangle C_1 \ {}_p\!\oplus C] \leq V_g[\pi \rangle C_2 \ {}_p\!\oplus C] \Rightarrow V_g[\pi \rangle C_1] \leq V_g[\pi \rangle C_2].$$

Proof. For all $\pi \in \mathbb{D}\mathcal{X}$ and $g \in \mathbb{G}\mathcal{X}$,

$$\begin{aligned} & V_g[\pi \rangle C_1] \\ =& V_g[\pi \rangle C_1 \ {}_p\!\oplus C_1] && \text{(from Proposition 3.11)} \\ \leq& V_g[\pi \rangle C_2 \ {}_p\!\oplus C_1] && \text{(from assumption)} \\ \leq& pV_g[\pi \rangle C_2] + (1-p)V_g[\pi \rangle C_1] && \text{(from Theorem 4.5)} \end{aligned}$$

Thus, $V_g[\pi \rangle C_1] \leq pV_g[\pi \rangle C_2] + (1-p)V_g[\pi \rangle C_1]$, which yields $V_g[\pi \rangle C_1] \leq V_g[\pi \rangle C_2]$. □

4.2.4 Relative monotonicity for visible if-then-else

For both the visible and hidden if-then-else operators, we consider restrictions of channels as in Definition 4.7 and subset gain functions as in Definition 4.8. This is because, as discussed in the beginning of Section 4.1.4, these operators disregard partially the values of each channel, and we can obtain much more useful results by disregarding these parts as well.

By considering the g-leakage of the components with the appropriate subset gain function, the strict version of relative monotonicity in equation 4.1 holds for the visible if-then-else operator. However, as $V_g[\pi \rangle C_1 \ {}_{\mathcal{A}}\!\triangle \ C] \leq V_g[\pi \rangle C_2 \ {}_{\mathcal{A}}\!\triangle \ C]$ is vacuously true if $\mathcal{A} = \emptyset$, we force $\mathcal{A}$ to be nonempty in our results.

Theorem 4.23. *Let $\mathcal{A} \subset \mathcal{X}$ such that $\mathcal{A} \neq \emptyset$, $g \in \mathbb{G}\mathcal{X}$ and $\pi \in \mathbb{D}\mathcal{X}$. Then*

$$V_{g_{\mathcal{A}}}[\pi \rangle C_1] \leq V_{g_{\mathcal{A}}}[\pi \rangle C_2] \iff \forall C \in \mathcal{C}_{\mathcal{X}},\ V_g[\pi \rangle C_1 \ {}_{\mathcal{A}}\!\triangle \ C] \leq V_g[\pi \rangle C_2 \ {}_{\mathcal{A}}\!\triangle \ C].$$

Proof.

$$
\begin{aligned}
& V_{g_{\mathcal{A}}}[\pi \rangle C_1] \leq V_{g_{\mathcal{A}}}[\pi \rangle C_2] \\
\Leftrightarrow & \forall C \in \mathcal{C}_{\mathcal{X}}.\ V_{g_{\mathcal{A}}}[\pi \rangle C_1] + V_{g_{\bar{\mathcal{A}}}}[\pi \rangle C] \leq V_{g_{\mathcal{A}}}[\pi \rangle C_2] + V_{g_{\bar{\mathcal{A}}}}[\pi \rangle C] && \text{(add. both sides)} \\
\Leftrightarrow & \forall C \in \mathcal{C}_{\mathcal{X}}.\ V_g[\pi \rangle C_1 \ {}_{\mathcal{A}}\triangle\ C] \leq V_g[\pi \rangle C_2 \ {}_{\mathcal{A}}\triangle\ C] && \text{(by Theorem 4.11)}
\end{aligned}
$$

□

Corollary 4.24 (Relative monotonicity for ${}_{\mathcal{A}}\triangle$).

$$C_2|_{\mathcal{A}} \sqsubseteq_{\circ} C_1|_{\mathcal{A}} \iff \forall C \in \mathcal{C}_{\mathcal{X}},\ (C_2 \ {}_{\mathcal{A}}\triangle\ C) \sqsubseteq_{\circ} (C_1 \ {}_{\mathcal{A}}\triangle\ C).$$

Proof. Follows from Theorem 4.23 and Corollary 4.10. □

4.2.5 Relative monotonicity for hidden if-then-else

In an interesting parallel to the visible and hidden choice operators, the direct implication of relative monotonicity does not hold for the hidden if-then-else, in contrast to its visible counterpart.

Theorem 4.25 (Relative monotonicity for ${}_{\mathcal{A}}⟁$, direct implication). *Let $\mathcal{X}$ be a finite set such that $|\mathcal{X}| > 1$, and let $\mathcal{A} \subsetneq \mathcal{X}$ and $\mathcal{A} \neq \emptyset$. Then, there are compatible channels $C_1, C_2 \in \mathcal{C}_{\mathcal{X}}$ such that*

$$C_2|_{\mathcal{A}} \sqsubseteq_{\circ} C_1|_{\mathcal{A}} \text{ and } \exists g \in \mathbb{G}\mathcal{X}, \exists \pi \in \mathbb{D}\mathcal{X}, \exists C \in \mathcal{C}_{\mathcal{X}},\ V_g[\pi \rangle C_1 \ {}_{\mathcal{A}}⟁\ C] > V_g[\pi \rangle C_2 \ {}_{\mathcal{A}}⟁\ C].$$

Proof. Let $|\mathcal{X}| = n$, and let $\mathcal{X} = \{x_1, ..., x_n\}$ be an idexing of $\mathcal{X}$. Without losing generality, let $\mathcal{A} = \{x_1, ..., x_k\}$, for some $k = |\mathcal{A}| < n$. Let $\mathcal{Y} = \{y_1, ..., y_n\}$. We define $C_1, C_2 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ as

$$C_1(x_i, y_j) = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{otherwise.} \end{cases} \qquad C_2(x_i, y_j) = \begin{cases} 1, & \text{if } i = n - j + 1, \\ 0, & \text{otherwise.} \end{cases}$$

for all $i, j \in \{1, ..., n\}$. Note that $C_1|_{\mathcal{A}}$ and $C_2|_{\mathcal{A}}$ are both transparent channels, and thus, $C_2|_{\mathcal{A}} \sqsubseteq_{\circ} C_1|_{\mathcal{A}}$.

We have, for all $i, j \in \{1, ..., n\}$,

$$(C_1 \,{}_{\mathcal{A}}⟁\, C_1)(x_i, y_j) = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{otherwise.} \end{cases}$$

$$(C_2 \,{}_{\mathcal{A}}⟁\, C_1)(x_i, y_j) = \begin{cases} 1, & \text{if } i = j \text{ and } i \leq k, \\ 1, & \text{if } i = n - j + 1 \text{ and } i > k, \\ 0, & \text{otherwise.} \end{cases}$$

Let $\pi_u \in \mathbb{D}\mathcal{X}$ be the uniform distribution over $\mathcal{X}$ and g_{id} be as in Definition 2.10. From Proposition 2.22 we derive that, for any channel $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$, $V_{g_{id}}[\pi_u \rangle C] = {}^1\!/\!_{|\mathcal{X}|} \sum_{y \in \mathcal{Y}} \max_{x \in \mathcal{X}} C(x, y)$. We thus obtain $V_{g_{id}}[\pi_u \rangle C_1 \,{}_{\mathcal{A}}⟁\, C_1] = 1$.

Notice that, for $j \geq \max(k, n - k)$, $(C_2 \,{}_{\mathcal{A}}⟁\, C_1)(x_i, y_j) = 0$ for all $i \in \{1, ..., n\}$. Therefore, $V_{g_{id}}[\pi_u \rangle C_2 \,{}_{\mathcal{A}}⟁\, C_1] \leq {}^1\!/\!_n(\max(k, n - k))$. Since $0 < k < n$, we obtain

$$V_{g_{id}}[\pi_u \rangle C_1 \,{}_{\mathcal{A}}⟁\, C_1] > V_{g_{id}}[\pi_u \rangle C_2 \,{}_{\mathcal{A}}⟁\, C_1].$$

□

The converse implication of the stronger version relative monotonicity (Equation (4.1)), however, does hold for the hidden if-then-else operator.

Theorem 4.26 (Relative monotonicity for ${}_{\mathcal{A}}⟁$, converse implication)**.** *For all $g \in \mathbb{G}\mathcal{X}$, $\pi \in \mathbb{D}\mathcal{X}$ and $\mathcal{A} \subset \mathcal{X}$ such that $\mathcal{A} \neq \emptyset$,*

$$\forall C \in \mathcal{C}_{\mathcal{X}},\ V_g[\pi \rangle C_{1\mathcal{A}} ⟁\, C] \leq V_g[\pi \rangle C_{2\mathcal{A}} ⟁\, C] \Rightarrow V_g[\pi \rangle C_1] \leq V_g[\pi \rangle C_2].$$

Proof. Let y_3 be an element such that $y_3 \notin \mathcal{Y}_1 \cup \mathcal{Y}_2$, and $C_3 \in \mathcal{C}_{\mathcal{X}}^{\{y_3\}}$. Since $\mathcal{Y}_1$ and $\{y_3\}$ are disjoint, for all $\pi \in \mathbb{D}\mathcal{X}$ and $g \in \mathbb{G}\mathcal{X}$, we have $V_g[\pi \rangle C_1 \,{}_{\mathcal{A}}⟁\, C_3] = V_g[\pi \rangle C_1 \,{}_{\mathcal{A}}\triangle\, C_3] = V_{g_{\mathcal{A}}}[\pi \rangle C_1] + V_{g_{\bar{\mathcal{A}}}}[\pi \rangle C_3]$. Similarly, $V_g[\pi \rangle C_2 \,{}_{\mathcal{A}}⟁\, C_3] = V_{g_{\mathcal{A}}}[\pi \rangle C_2] + V_{g_{\bar{\mathcal{A}}}}[\pi \rangle C_3]$.

Therefore, $V_g[\pi \rangle C_1 \,{}_{\mathcal{A}}⟁\, C_3] \leq V_g[\pi \rangle C_2 \,{}_{\mathcal{A}}⟁\, C_3] \implies V_{g_{\mathcal{A}}}[\pi \rangle C_1] \leq V_{g_{\mathcal{A}}}[\pi \rangle C_2]$. □

Chapter 5

Case Study: the Crowds protocol

The interest in a better understanding regarding the leakage properties of channel compositions is not limited to the foundational aspects of QIF. The investigations presented in this thesis also aim to have immediate practical value: reasoning about systems in an algebraic manner does often provide us with easier or more efficient ways to model them and and study their leakage properties.

In this chapter, we use the operators studied in this thesis to model the well-known *Crowds* [Reiter and Rubin, 1998] protocol. We were able to use some of our results from Chapters 3 and 4 to devise an algorithm for obtaining an appropriate channel representation.

5.1 Description of the protocol

The *Crowds* protocol, developed by Reiter and Rubin [1998], is one of the best known anonymity protocols in the literature, and its ideas were essential for the widely used *Onion Routing* protocol [Goldschlag et al., 1996]. Crowds was designed to be used by a group of *users* who wish to anonymously send requests to a *server*. When a user wants to send a request to the server, he first randomly picks a user in the group (maybe himself) and forwards the request to that user. From that point on, each user, upon receiving a request, sends it to the server with probability $p \in (0, 1]$, or forwards it to another user with probability $1-p$. This second phase is repeated until the request finally reaches the server. Assuming every user acts in good faith, the server (which doubles as the adversary in this case) is usually not able to derive much information about the identity of the initiator of the request.

In order to obtain more information from the protocol, the server might employ *corrupt* users, who infiltrate among the regular, *honest*, ones. When a corrupt user receives a forwarded request, he shares the identity of the forwarder with the server, and we say that the forwarder was *detected.* As no information can be gained after a corrupt user intercepts a request, we need only to consider the execution of the protocol until a detection occurs, or the message reaches the server.

In the original description of Crowds, all users have equal probability of being forwarded a message, regardless of the forwarder. The channel modelling such a case is easily computed, and well-known in the literature. Here we consider the more general case in which each user may employ a different probability distribution when choosing which user to forward a request to. Thus, we can capture scenarios in which not all users can easily reach each other (a common problem in, for instance, *ad-hoc* networks). We make the simplifying assumption that corrupt users are evenly distributed, i.e., that all honest users have the same probability $q \in (0,1]$ of choosing a corrupt user as a recipient when forwarding a request.

5.2 Modelling the protocol

We model Crowds as a channel $Crowds{:}\mathcal{X}{\times}\mathcal{Y}{\rightarrow}[0,1]$. The input of the channel, taken from set $\mathcal{X}{=}\{u_1, u_2, \ldots, u_{n_h}\}$, represents the identity u_i of the honest user (among a total of n_h honest users) who initiated the request.

The output of the channel can be of two different types. Either one honest user forwards a request to a corrupt one, in which case the output is the identity of the detected user, or the request eventually reaches the server, in which case the output is the identity of the user who finally forwarded it to the server. Outputs of the first type are represented by the set $\mathcal{D}{=}\{d_1, d_2, \ldots, d_{n_h}\}$, in which d_i indicates that user u_i was detected, while outputs of the second type are represented by the set $\mathcal{S}{=}\{s_1, s_2, \ldots, s_{n_h}\}$ (disjoint from $\mathcal{D}$), in which s_i indicates that user u_i forwarded a message to the server. The output set of *Crowds* is, therefore, $\mathcal{Y} = \mathcal{D} \cup \mathcal{S}$.

To compute the entries of the channel, we model the protocol as a time-stationary Markov chain $M = (\mathcal{U}, \boldsymbol{P})$, whose set of states is the set of honest users $\mathcal{U}$, and its transition function $\boldsymbol{P}$ is such that $\boldsymbol{P}(u_i, u_j)$ is the probability of u_j being the recipient of a request forwarded by u_i, given that u_i will not be detected.

To help us model the protocol, we first define four auxiliary channels, whose purpose will be clear soon. Two transparent channels $I_d \in \mathcal{C}_{\mathcal{U}}^{\mathcal{D}}$ and $I_s \in \mathcal{C}_{\mathcal{U}}^{\mathcal{S}}$, defined as, for all $i, j \in \{1, ..., n_h\}$,

$$I_d(u_i, d_j) {=} I_s(u_i, s_j) = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{otherwise,} \end{cases}$$

and two other channels $P_d \in \mathcal{C}_{\mathcal{D}}^{\mathcal{D}}$ and $P_s \in \mathcal{C}_{\mathcal{S}}^{\mathcal{S}}$, based on the transition function of our Markov chain M, defined as, for all $i, j \in \{1, ..., n_h\}$

$$P_d(d_i, d_j) {=} P_s(s_i, s_j) {=} \boldsymbol{P}(u_i, u_j).$$

We begin by reasoning about what happens if each request can be forwarded only once. There are two possible situations: either the initiator of the request is detected, or he succeeds in forwarding his request to an honest user, who will in turn send it to the server. The channel corresponding to the initiator being detected is I_d, since in this case the output has to be d_i whenever u_i is the initiator. The channel corresponding to the latter situation is I_sP_s—i.e., the channel I_s postproccessed by P_s. This is because, being P_s based on the transition function of M, the entry $(I_sP_s)(u_i, s_j)$ gives us exactly the probability that user u_j received the request originated by user u_i after it being forwarded once. Therefore, when Crowds is limited to one forwarding, it can be modelled by the channel $I_d \;{}_q{\oplus}\; I_sP_s$ [1], representing the fact that: (1) with probability q the initiator is detected, and the output is generated by I_d; and (2) with probability $1 - q$ the output is generated by I_sP_s.

Let us now restrict our protocol to at most two forwards. If the initiator is not immediately detected, the first recipient will have a probability p of sending the message to the server. If the recipient forwards the message instead, he may be detected. Because the request was already forwarded once, the channel that will produce the output in this case is I_dP_d (notice that, despite this channel being equivalent to I_sP_s, it is of a different type). On the other hand, if the first recipient forwards the message to an honest user, this second recipient will now send the message to the server, making the protocol produce an output according to $I_sP_sP_s$ (or simply $I_sP_s^2$), since $(I_sP_s^2)(u_i, s_j)$ is the probability that user u_j received the request originated by user u_i after it being forwarded twice. Therefore, when Crowds is limited to two forwards, it can be modelled by the channel $I_d \;{}_q{\oplus}\; (I_sP_s \;{}_p{\oplus}\; (I_dP_d \;{}_q{\oplus}\; I_sP_s^2))$. Note the disposition of the parentheses, as it reflects the order in which the events occur. First, there is a probability q of the initiator being detected, and $1 - q$ of the protocol continuing. Then, there is a

[1] To simplify notation, we assume cascading has precedence over hidden choice, i.e., $AB \;{}_p{\oplus}\; CD = (AB) \;{}_p{\oplus}\; (CD)$.

probability p of the first recipient sending it to the server, and so on.

Similarly, limiting the protocol to three forwards, we obtain the channel $I_d \;{}_q\!\oplus\; (I_sP_s \;{}_p\!\oplus\; (I_dP_d \;{}_q\!\oplus\; (I_sP_s^2 \;{}_p\!\oplus\; (I_dP_d^2 \;{}_q\!\oplus\; I_sP_s^3))))$. Proceeding this way, we can inductively construct a sequence $\{C_i\}_{i\in\mathbb{N}^*}$,

$$C_i = I_d \;{}_q\!\oplus\; (I_sP_s \;{}_p\!\oplus\; (I_dP_d \;{}_q\!\oplus\; (\dots \;{}_p\!\oplus\; (I_dP_d^{i-1} \;{}_q\!\oplus\; I_sP_s^i)\dots))),$$

in which each C_i represents our protocol capped at i forwards per request. We will use this sequence to obtain an approximation of *Crowds* in Theorem 5.4. A straightforward proof would be too lengthy, however, so we break it into a discussion and a series of lemmas.

For starters, the limited versions of the protocol, modelled by $\{C_i\}_{i\in\mathbb{N}}$, should behave more and more similarly to the unlimited Crowds as i becomes large. Indeed, the probability of the original protocol to exceed n forwards is $(1-p)^n(1-q)^{n+1}$, which means that the probability of *Crowds* behaving differently than C_n can be made arbitrarily low for a large enough choice of n. We can, therefore, obtain a description of *Crowds* by taking $\lim_{i\to\infty} C_i$, if such limit exists.

We now proceed to prove the lemmas that will culminate with Theorem 5.4. The outline is the following. First, we use the associativity of the hidden choice operator to rearrange the parenthesis of the channels C_i. Then, we prove the existence of the limit $\lim_{i\to\infty} C_i$. Finally, we prove a small lemma that simplifies the upper-bound on Theorem 5.4.

Lemma 5.1. *Let n be a positive integer and $\{A_i\}_{i\in\{0,1,\dots,n\}}$ a collection of compatible channels. If q, $p \in [0,1]$ and are not both 0, then*

$$A_0 \;{}_q\!\oplus\; (A_1 \;{}_p\!\oplus\; (\dots \;{}_p\!\oplus\; A_n)\dots) = \left(\left(\dots\left(A_0 \;{}_{\frac{t_0}{t_1}}\!\oplus\; A_1\right) \;{}_{\frac{t_1}{t_2}}\!\oplus\; \dots\right) \;{}_{t_{(n-1)}}\!\oplus\; A_n\right), \textit{ for even } n,$$

$$A_0 \;{}_q\!\oplus\; (A_1 \;{}_p\!\oplus\; (\dots \;{}_q\!\oplus\; A_n)\dots) = \left(\left(\dots\left(A_0 \;{}_{\frac{t_0}{t_1}}\!\oplus\; A_1\right) \;{}_{\frac{t_1}{t_2}}\!\oplus\; \dots\right) \;{}_{t_{(n-1)}}\!\oplus\; A_n\right), \textit{ for odd } n,$$

where

$$t_{2i} = 1-(1-q)^{i+1}(1-p)^i, \textit{ and} \tag{5.1}$$

$$t_{(2i+1)} = 1-(1-q)^{i+1}(1-p)^{i+1}. \tag{5.2}$$

Proof. Firstly, from Equation (3.8) on Proposition 3.10, we deduce the following equivalence. For any probabilities $u, v \in [0,1]$ (with u and v not both 0) and compatible channels C_1, C_2 and C_3:

$$C_1 \ {}_{u}\!\oplus\ (C_2 \ {}_{v}\!\oplus\ C_3) = (C_1 \ {}_{\frac{u}{u+v-uv}}\!\oplus\ C_2) \ {}_{(u+v-uv)}\!\oplus\ C_3. \tag{5.3}$$

Now, we proceed to the proof. We prove by induction on n on the set of positive integers.

The case when $n = 1$ is immediate. Let us suppose it is proven for $n \geq 1$. Then, if n is odd,

$$\begin{aligned}
&A_0 \ {}_{q}\!\oplus\ (\dots \ {}_{p}\!\oplus\ (A_{n-1} \ {}_{q}\!\oplus\ (A_{np}\!\oplus\! A_{n+1}))) && \\
=&A_0 \ {}_{q}\!\oplus\ (\dots \ {}_{p}\!\oplus\ (A_{n-1} \ {}_{q}\!\oplus\ A'_n)\dots)) && (\text{let } A'_n{=}A_n \ {}_{p}\!\oplus\ A_{n+1}) \\
=&\left(\dots \left(A_0 \ {}_{\frac{t_0}{t_1}}\!\oplus \dots\right) \ {}_{\frac{t_{(n-2)}}{t_{(n-1)}}}\!\oplus\ A_{n-1}\right) \ {}_{t_{(n-1)}}\!\oplus\ A'_n && (\text{by ind. hyp.}) \\
=&\left(\dots \left(A_0 \ {}_{\frac{t_0}{t_1}}\!\oplus \dots\right) \ {}_{\frac{t_{(n-2)}}{t_{(n-1)}}}\!\oplus\ A_{n-1}\right) \ {}_{t_{(n-1)}}\!\oplus\ (A_n \ {}_{p}\!\oplus\ A_{n+1}) && (A'_n = A_n \ {}_{p}\!\oplus\ A_{n+1}) \\
=&\left(\dots \left(A_0 \ {}_{\frac{t_0}{t_1}}\!\oplus \dots\right) \ {}_{\frac{t_{(n-1)}}{t_{(n-1)}+p-pt_{(n-1)}}}\!\oplus A_n\right) \ {}_{t_{(n-1)}+p-pt_{(n-1)}}\!\oplus\ A_{n+1} && (\text{by Eq.}(5.3)) \\
=&\left(\dots \left(A_0 \ {}_{\frac{t_0}{t_1}}\!\oplus \dots\right) \ {}_{\frac{t_{(n-1)}}{t_n}}\!\oplus\ A_n\right) \ {}_{t_n}\!\oplus\ A_{n+1} && (\text{by Eq.}(5.1),\ (5.2))
\end{aligned}$$

The proof for when n is even is almost identical. □

Lemma 5.2. *If q and p are not both 0, $\lim_{i\to\infty} C_i$ exists.*

Proof. Each C_i is a channel of type $\mathcal{U} \times (\mathcal{D} \cup \mathcal{S})$, and can thus be understood as an element of the set $\mathbb{R}^{|\mathcal{U}\times(\mathcal{D}\cup\mathcal{S})|}$. Therefore, if each entry of C_i converges to a real value as $i \to \infty$, then $\lim_{i\to\infty} C_i$ exists.

Having that in mind, we prove that, for all $j, k \in \{1, 2, ..., n\}$, $\{C_i(u_j, d_k)\}_{i\in\mathbb{N}^*}$ and $\{C_i(u_j, s_k)\}_{i\in\mathbb{N}^*}$ are Cauchy sequences in the reals. We start by proving that $\{C_i(u_j, d_k)\}_{i\in\mathbb{N}^*}$ is a Cauchy sequence.

Let $\epsilon > 0$. From equations (5.1) and (5.2), $\lim_{i\to\infty} t_i = 1$. Therefore, $\exists M \in \mathbb{N} \setminus \{0\}$ such that $i > M \implies 1 - t_i < \epsilon/2$.

Suppose $m_1, m_2 > M + 1$. By lemma 5.1, we have

$$\begin{aligned}
C_{m_1} &= \left(\left(\left(\dots \left(I_d \ {}_{\frac{t_0}{t_1}}\!\oplus\ I_sP_s\right) \ {}_{\frac{t_1}{t_2}}\!\oplus\ I_dP_d\right) \ {}_{\frac{t_2}{t_3}}\!\oplus \dots\right) \ {}_{\frac{t_{(2M-1)}}{t_{2M}}}\!\oplus\ I_dP_d^M\right) \ {}_{t_{2M}}\!\oplus\ D_1, \\
C_{m_2} &= \left(\left(\left(\dots \left(I_d \ {}_{\frac{t_0}{t_1}}\!\oplus\ I_sP_s\right) \ {}_{\frac{t_1}{t_2}}\!\oplus\ I_dP_d\right) \ {}_{\frac{t_2}{t_3}}\!\oplus \dots\right) \ {}_{\frac{t_{(2M-1)}}{t_{2M}}}\!\oplus\ I_dP_d^M\right) \ {}_{t_{2M}}\!\oplus\ D_2,
\end{aligned}$$

where $D_i = I_sP_s^{M+1} \ {}_p\!\oplus (I_dP_d^{M+1} \ {}_q\!\oplus (\dots \ {}_q\!\oplus I_sP_s^{m_i})\dots)$, for $i \in \{1,2\}$. The definition of hidden choice then gives us

$$\begin{aligned}
C_{m_1}(u_j,d_k) =& t_{2M}\left(\dots\left(I_d \ {}_{\frac{t_0}{t_1}}\!\oplus \dots\right) \ {}_{\frac{t_{(2M-1)}}{t_{2M}}}\!\oplus I_dP_d^M\right)(u_j,d_k) + (1-t_{2M})D_1(u_j,d_k),\\
C_{m_2}(u_j,d_k) =& t_{2M}\left(\dots\left(I_d \ {}_{\frac{t_0}{t_1}}\!\oplus \dots\right) \ {}_{\frac{t_{(2M-1)}}{t_{2M}}}\!\oplus I_dP_d^M\right)(u_j,d_k) + (1-t_{2M})D_2(u_j,d_k).
\end{aligned}$$

Thus,

$$\begin{aligned}
&|C_{m_1}(u_j,d_k) - C_{m_2}(u_j,d_k)|\\
=&|(1-t_{2M})D_1(u_j,d_k) - (1-t_{2M})D_2(u_j,d_k)|\\
\leq&|(1-t_{2M})D_1(u_j,d_k)| + |(1-t_{2M})D_2(u_j,d_k)| && (|a-b| \leq |a|+|b|)\\
\leq&|(1-t_{2M})| + |(1-t_{2M})| && (D_i(u_j,d_k) \leq 1)\\
<&{}^{\epsilon}\!/2 + {}^{\epsilon}\!/2 = \epsilon && (2M > M)
\end{aligned}$$

The proof that for $\{C_i(u_j,s_k)\}_{i\in\mathbb{N}}$ is a Cauchy sequence is almost identical. □

Lemma 5.3. *Let $\pi \in \mathbb{D}\mathcal{X}$ for some finite set $\mathcal{X}$ and g be any gain function. Let $n \in \mathbb{N} \setminus \{0,1\}$ and $\{A_i\}_{i\in\{1,2,\dots,n\}}$ be a collection of channels with input $\mathcal{X}$ such that*

$$i < j \implies V_g[\pi\rangle A_i] \geq V_g[\pi\rangle A_j].$$

Let $\{p_i\}_{i\in\{1,\dots,n-1\}}$ be a collection of real numbers in the interval $[0,1]$. Then, for any $n \in \mathbb{N}$,

$$V_g[\pi\rangle A_1 \ {}_{p_1}\!\oplus (A_2 \ {}_{p_2}\!\oplus (\dots \ {}_{p_{n-1}}\!\oplus (A_n)))] \leq V_g[\pi\rangle A_1].$$

Proof. We proceed by induction on the size of the collection. The theorem is true for $n = 2$ since, from Theorem 4.5,

$$V_g[\pi\rangle A_1 \ {}_p\!\oplus A_2] \leq pV_g[\pi\rangle A_1] + (1-p)V_g[\pi\rangle A_2] \leq V_g[\pi\rangle A_1].$$

Suppose it is true for $n \geq 2$ and let $\{A_i\}_{i\in\{1,\dots,n+1\}}$ be a collection of $n+1$ channels with the property described in the Lemma. Then,

$$\begin{aligned}
&V_g[\pi\rangle A_1 \ {}_{p_1}\!\oplus (A_2 \ {}_{p_2}\!\oplus (\dots \ {}_{p_n}\!\oplus (A_{n+1})))]\\
\leq&p_1V_g[\pi\rangle A_1] + (1-p_1)V_g[\pi\rangle A_2 \ {}_{p_2}\!\oplus (\dots \ {}_{p_n}\!\oplus A_{n+1})] && \text{(by Theorem 4.5)}
\end{aligned}$$

$$\begin{aligned}
&\leq p_1 V_g[\pi\,\rangle\, A_1] + (1-p_1)V_g[\pi\,\rangle\, A_2] && \text{(by the ind. hypothesis)}\\
&\leq p_1 V_g[\pi\,\rangle\, A_1] + (1-p_1)V_g[\pi\,\rangle\, A_1] = V_g[\pi\,\rangle\, A_1] && (V_g[\pi\,\rangle\, A_1] \geq V_g[\pi\,\rangle\, A_2])
\end{aligned}$$

□

We are finally in the position to prove our main result.

Theorem 5.4. *Let* $\{t_i\}_{i\in\mathbb{N}}$ *be the sequence defined by equations* (5.1) *and* (5.2) .

Let $K_m{=}((\ldots(I_d \;{}_{t_0/t_1}{\oplus}\; I_sP_s) \;{}_{t_1/t_2}{\oplus}\; \ldots) \;{}_{t_{2m-1}/t_{2m}}{\oplus}\; I_dP_d^m$*. Then, for all* $\pi \in \mathbb{D}\mathcal{X}$*,* $g \in \mathbb{G}\mathcal{X}$ *and all* $m \in \mathbb{N}^*$*,*

$$V_g[\pi\,\rangle \lim_{i\to\infty} C_i] \;\geq\; t_{2m}V_g[\pi\,\rangle\, K_m], \tag{5.4}$$

$$V_g[\pi\,\rangle \lim_{i\to\infty} C_i] \;\leq\; t_{2m}V_g[\pi\,\rangle\, K_m] + (1-t_{2m})V_g[\pi\,\rangle\, I_sP_s^{m+1}], \quad \textit{and} \tag{5.5}$$

$$(1-t_{2m})V_g[\pi\,\rangle\, I_sP_s^{m+1}] \;\leq\; (1-q)^{m+1}(1-p)^m. \tag{5.6}$$

Proof. From Lemma 5.1, we note that, for any $m' > m$, $C_{m'}$ can be written as

$$\begin{aligned}
C_{m'} =&\left(\left(\left(\ldots\left(I_d \;{}_{\frac{t_0}{t_1}}{\oplus}\; I_sP_s\right) \;{}_{\frac{t_1}{t_2}}{\oplus}\; I_dP_d\right) \;{}_{\frac{t_2}{t_3}}{\oplus}\; \ldots\right) \;{}_{\frac{t_{2m-1}}{t_{2m}}}{\oplus}\; I_dP_d^m\right) \;{}_{t_{2m}}{\oplus}\; D,\\
C_{m'} =&K_m \;{}_{t_{2m}}{\oplus}\; D.
\end{aligned} \tag{5.7}$$

Where $D = I_sP_s^{m+1} \;{}_{p}{\oplus}\; (I_dP_d^{m+1} \;{}_{q}{\oplus}\; (\ldots \;{}_{q}{\oplus}\; I_sP_s^{m'})\ldots)$. From Equation (5.7) and Theorem 4.4, we derive that, for any $m' > m$,

$$V_g[\pi\,\rangle\, C_{m'}] \geq t_{2m}V_g[\pi\,\rangle\, K_m].$$

For each π and g, $V_g[\pi\,\rangle\, C]$, being a sum of maxima of continuous functions over C, is itself continuous over C. Therefore, the equation above implies (5.4)

For the proof of the upper bound, Theorem 4.5 gives us

$$V_g[\pi\,\rangle\, C_{m'}] \leq t_{2m}V_g[\pi\,\rangle\, K_m] + (1-t_{2m})V_g[\pi\,\rangle\, D].$$

Notice that, $\forall k, j \in \mathbb{N}^*$, $I_sP_s^k \;\overset{\circ}{=}\; I_dP_d^k$, and $I_sP_s^k \sqsubseteq_\circ I_sP_s^{k+j} = (I_sP_s^k)P_s^j$. Thus, Lemma 5.3 yields $V_g[\pi\,\rangle\, D] \leq V_g[\pi\,\rangle\, I_sP_s^{m+1}]$. Thus

$$V_g[\pi\,\rangle\, C_{m'}] \leq t_{2m}V_g[\pi\,\rangle\, K_m] + (1-t_{2m})V_g[\pi\,\rangle\, I_sP_s^{m+1}],$$

which, by continuity of V_g, implies the upper bound (5.5).

Finally, to prove Equation (5.6), it suffices to notice that

$$\begin{aligned}
&(1-t_{2m})V_g[\pi\,\rangle\, I_sP_s^{m+1}] \\
\leq &1-t_{2m} && (V_g[\pi\,\rangle\, I_sP_s^{m+1}] \leq 1) \\
= &(1-q)^{m+1}(1-p)^m && \text{(by Equation (5.1))}
\end{aligned}$$

□

Notice that, from the proof of Theorem 5.4, we can actually derive two stronger conditions than Equations (5.4) and (5.5). Namely, that for all $m' > m$,

$$\begin{aligned}
&V_g[\pi\,\rangle\, C_{m'}] \geq t_{2m}V_g[\pi\,\rangle\, K_m], \\
&V_g[\pi\,\rangle\, C_{m'}] \leq t_{2m}V_g[\pi\,\rangle\, K_m] + (1-t_{2m})V_g[\pi\,\rangle\, I_sP_s^{m+1}].
\end{aligned}$$

Equations (5.4) and (5.5) provide an effective way to approximate the g-leakage of information of the channel *Crowds* with arbitrary precision, whereas Equation (5.6) lets us easily estimate how many interactions are needed to achieve any degree of precision.

To obtain K_m, we need to calculate m matrix multiplications due to the cascadings, and m matrix additions due to the hidden choices. Thus, Theorem 5.4 implies that we can obtain a channel whose posterior vulnerability differs from that of *Crowds* by at most $(1{-}q)^{m+1}(1{-}p^m)$ in $\approx O(mn_h^\omega)$ time, where ω is the exponent corresponding to the complexity of matrix multiplication. Even for low values of p and q, $(1{-}q)^{m+1}(1{-}p)^m$ decreases very fast. For instance, to obtain a precision of 0.001 on the leakage bound, we need $m{=}10$ when $(1{-}q)(1{-}p)$ is 0.5, $m{=}20$ when it is 0.7, and $m{=}66$ when it is 0.9, regardless of the number n_h of honest users.

Therefore, our method has time complexity $O(n_h^\omega)$ when the number of users is large (which is the usual case for Crowds), and reasonable values of p, q, and precision desired. To the best of our knowledge this method is the fastest in the literature, beating the previous $O(n_h^{\omega+1})$ that can be achieved by modifying the method developed by Andrés et al. [2010]—although their method does not require our assumption of corrupt users being evenly distributed.

Chapter 6

Conclusion

In this thesis, we studied in depth five compositional operators in Quantitative Information Flow. While the parallel, visible choice and hidden choice operators have been treated elsewhere, this thesis is, to the best of our knowledge, the first study regarding the visible and hidden if-then-else operators in the field.

The first objective of this thesis was to address the specific questions on Chapter 1. Once this was done, we set ourselves to the task of giving the most general account of these operators we possibly could, which led to the algebraic properties described in Chapter 4.

After that, it seemed natural to give a glimpse on the kind of modelling these operators could be useful for. For that end, we presented in Chapter 5 two well-known security protocols in the literature, the *Dining Cryptographers* [Chaum, 1988] and the *Crowds* [Reiter and Rubin, 1998] protocols. We believe that a great number of systems and security protocols can be modelled in similar manners, which in some cases might lead to a more efficient way to calculate their leakage properties. Case in point, the model of the Crowds protocol we provided in Chapter 5 naturally suggested a fast and very simple algorithm to compute its channel, as we discussed after Theorem 5.4.

The study of compositionality in Quantitative Information Flow is only beginning, and its results promise to significantly enhance not only our capacity to model and study real-life scenarios, but also our understanding of information leakage as a whole. One natural future direction of inquiry concerns studying analogues of the operators studied in this thesis to abstract channels, as in Definition 2.25. Another topic for future research regards the *utility* of a system — that is, how useful the system is from the point of view of the user. We believe the operators studied in this thesis can also be applied in a similar manner in this scenario, and the utility of a composition might be studied from that of its components.

Bibliography

Alvim, M. S., Chatzikokolakis, K., Kawamoto, Y., and Palamidessi, C. (2018). Leakage and protocol composition in a game-theoretic perspective. In *Proc. of POST*, pages 134--159.

Alvim, M. S., Chatzikokolakis, K., McIver, A., Morgan, C., Palamidessi, C., and Smith, G. (2014). Additive and multiplicative notions of leakage, and their capacities. In *Proc. of CSF*, pages 308--322. IEEE.

Alvim, M. S., Chatzikokolakis, K., McIver, A., Morgan, C., Palamidessi, C., and Smith, G. (2016). Axioms for information leakage. In *Proc. of CSF*, pages 77--92.

Alvim, M. S., Chatzikokolakis, K., Palamidessi, C., and Smith, G. (2012). Measuring information leakage using generalized gain functions. In *Proc. of CSF*, pages 265–279.

Américo, A., Vaz, A., Alvim, M., Campos, S., and McIver, A. (2017). *Formal analysis of the information leakage of the DC-nets and crowds anonymity protocols*, pages 142--158. Lecture Notes in Computer Science. Springer International Publishing.

Andrés, M. E., Palamidessi, C., van Rossum, P., and Smith, G. (2010). Computing the leakage of information-hiding systems. In *Proc. of TACAS*, volume 6015 of *LNCS*, pages 373–389. Springer.

Chatzikokolakis, K., Palamidessi, C., and Panangaden, P. (2008). Anonymity protocols as noisy channels. *Inf. and Comp.*, 206(2–4):378--401.

Chaum, D. (1988). The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1:65--75.

Engelhardt, K. (2017). A better composition operator for quantitative information flow analyses. In *European Symposium on Research in Computer Security, Proceedings, Part I*, pages 446--463.

Espinoza, B. and Smith, G. (2013). Min-entropy as a resource. *Inf. and Comp.*, 226:57--75.

Goldschlag, D. M., Reed, M. G., and Syverson, P. F. (1996). Hiding routing information. In Anderson, R., editor, *Information Hiding*, pages 137--150, Berlin, Heidelberg. Springer Berlin Heidelberg.

Kawamoto, Y., Chatzikokolakis, K., and Palamidessi, C. (2017). On the Compositionality of Quantitative Information Flow. *Logical Methods in Computer Science*, Volume 13, Issue 3.

Kerckhoffs, A. (1883). La cryptographie militaire. *Journal des sciences militaires*, IX:5–38.

Massey (1994). Guessing and entropy. In *Proceedings of the IEEE Int. Symposium on Information Theory*, page 204. IEEE.

McIver, A., Morgan, C., Smith, G., Espinoza, B., and Meinicke, L. (2014). Abstract channels and their robust information-leakage ordering. In *Proc. of POST*, volume 8414 of *LNCS*, pages 83--102. Springer.

Reiter, M. K. and Rubin, A. D. (1998). Crowds: anonymity for Web transactions. *ACM Trans. on Information and System Security*, 1(1):66--92.

Shannon, C. E. (1948). A mathematical theory of communication. *Bell System Technical Journal*, 27:379--423, 625–56.

Smith, G. (2009). On the foundations of quantitative information flow. In *Proc. of FOSSACS*, volume 5504 of *LNCS*, pages 288--302. Springer.

Appendix A

Proofs of Chapter 3

Here we present the proofs of Chapter 3. Throughout this appendix, let $C_1 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_1}$, $C_2 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_2}$ and $C_2 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_2}$. We recall Definition 3.1: given any $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$, we define $C(x, y') = 0$ for any $y' \notin \mathcal{Y}$.

The sections of this appendix are named as in Section 3.2.

A.1 Commutativity, associativity and idempotency

Proposition 3.9 (Commutative Properties)**.**

$$C_1 \parallel C_2 \overset{\circ}{=} C_2 \parallel C_1, \tag{3.1}$$

$$C_1 \;{}_{p}\dot\sqcup\; C_2 \overset{\circ}{=} C_2 \;{}_{(1-p)}\dot\sqcup\; C_1, \tag{3.2}$$

$$C_1 \;{}_{p}\oplus\; C_2 = C_2 \;{}_{(1-p)}\oplus\; C_1, \tag{3.3}$$

$$C_1 \;{}_{\mathcal{A}}\triangle\; C_2 \overset{\circ}{=} C_2 \;{}_{\bar{\mathcal{A}}}\triangle\; C_1, \tag{3.4}$$

$$C_1 \;{}_{\mathcal{A}}\boxplus\; C_2 = C_2 \;{}_{\bar{\mathcal{A}}}\boxplus\; C_1. \tag{3.5}$$

Proof. (3.1) The bijection is given by $\psi((y_1, y_2)) = (y_2, y_1)$. For all $x \in \mathcal{X}$, $y_1 \in \mathcal{Y}_1$ and $y_2 \in \mathcal{Y}_2$,

$$\begin{aligned}
&(C_1 \parallel C_2)(x, (y_1, y_2)) && \\
=&C_1(x, y_1)C_2(x, y_2) && \text{(by def. of } \parallel) \\
=&(C_2 \parallel C_1)(x, (y_2, y_1)) && \text{(by def. of } \parallel)
\end{aligned}$$

(3.2) The bijection is given by $\psi((y, 1)) = (y, 2)$ and $\psi((y, 2)) = (y, 1)$. For all

$x \in \mathcal{X}$ and $(y,1) \in (\mathcal{Y}_1 \sqcup \mathcal{Y}_2)$,

$$\begin{aligned}
&(C_1 \ {}_{p}\dot{\sqcup}\ C_2)(x,(y,1)) && \\
=&pC_1(x,y) && \text{(by def. of } {}_{p}\dot{\sqcup}\text{)} \\
=&(C_2 \ {}_{(1-p)}\dot{\sqcup}\ C_1)(x,(y,2)) && \text{(by def. of } {}_{(1-p)}\dot{\sqcup}\text{)}
\end{aligned}$$

Similarly, for all $x \in \mathcal{X}$ and $(y,2) \in (\mathcal{Y}_1 \sqcup \mathcal{Y}_2)$

$$\begin{aligned}
&(C_1 \ {}_{p}\dot{\sqcup}\ C_2)(x,(y,2)) && \\
=&(1-p)C_2(x,y) && \text{(by def. of } {}_{p}\dot{\sqcup}\text{)} \\
=&(C_2 \ {}_{(1-p)}\dot{\sqcup}\ C_1)(x,(y,1)) && \text{(by def. of } {}_{(1-p)}\dot{\sqcup}\text{)}
\end{aligned}$$

(3.3) For all $x \in \mathcal{X}$ and $y \in \mathcal{Y}_1 \cup \mathcal{Y}_2$,

$$\begin{aligned}
&(C_1 \ {}_{p}\oplus\ C_2)(x,y) && \\
=&pC_1(x,y) + (1-p)C_2(x,y) && \text{(by def. of } {}_{p}\oplus\text{)} \\
=&(C_2 \ {}_{(1-p)}\oplus\ C_1)(x,y) && \text{(by def. of } {}_{(1-p)}\oplus\text{)}
\end{aligned}$$

(3.4) The bijection is given by $\psi((y,1)) = (y,2)$ and $\psi((y,2)) = (y,1)$. For all $x \in \mathcal{A}$ and $(y,1) \in \mathcal{Y}_1 \sqcup \mathcal{Y}_2$,

$$\begin{aligned}
&(C_1 \ {}_{\mathcal{A}}\triangle\ C_2)(x,(y,1)) && \\
=&C_1(x,y) && \text{(by def. of } {}_{\mathcal{A}}\triangle\text{)} \\
=&(C_2 \ {}_{\bar{\mathcal{A}}}\triangle\ C_1)(x,(y,2)) && \text{(by def. of } {}_{\bar{\mathcal{A}}}\triangle\text{)}
\end{aligned}$$

Similarly, for all $x \in \bar{\mathcal{A}}$ and $(y,2) \in \mathcal{Y}_1 \sqcup \mathcal{Y}_2$

$$\begin{aligned}
&(C_1 \ {}_{\mathcal{A}}\triangle\ C_2)(x,(y,2)) && \\
=&C_2(x,y) && \text{(by def. of } {}_{\mathcal{A}}\triangle\text{)} \\
=&(C_2 \ {}_{\bar{\mathcal{A}}}\triangle\ C_1)(x,(y,1)) && \text{(by def. of } {}_{\bar{\mathcal{A}}}\triangle\text{)}
\end{aligned}$$

For all other pairs $(x,(y,i)) \in \mathcal{X} \times (\mathcal{Y}_1 \sqcup \mathcal{Y}_2)$ not contemplated above,

$$(C_1 \ {}_{\mathcal{A}}\triangle\ C_2)(x,(y,i)) = (C_2 \ {}_{\bar{\mathcal{A}}}\triangle\ C_1)(x,\psi(y,i)) = 0,$$

(3.5) For all $x \in \mathcal{A}$ and $y \in \mathcal{Y}_1 \cup \mathcal{Y}_2$,

$$
\begin{aligned}
&(C_1 \;{}_{\mathcal{A}}\mathbin{\triangle\!\!\!\!\!+}\; C_2)(x,y) && \\
=&C_1(x,y) && \text{(by def. of } {}_{\mathcal{A}}\mathbin{\triangle\!\!\!\!\!+}) \\
=&(C_2 \;{}_{\bar{\mathcal{A}}}\mathbin{\triangle\!\!\!\!\!+}\; C_1)(x,y) && \text{(by def. of } {}_{\bar{\mathcal{A}}}\mathbin{\triangle\!\!\!\!\!+})
\end{aligned}
$$

Similarly, for all $x \in \bar{\mathcal{A}}$ and $y \in \mathcal{Y}_1 \cup \mathcal{Y}_2$

$$
\begin{aligned}
&(C_1 \;{}_{\mathcal{A}}\mathbin{\triangle\!\!\!\!\!+}\; C_2)(x,y) && \\
=&C_2(x,y) && \text{(by def. of } {}_{\mathcal{A}}\mathbin{\triangle\!\!\!\!\!+}) \\
=&(C_2 \;{}_{\bar{\mathcal{A}}}\mathbin{\triangle\!\!\!\!\!+}\; C_1)(x,y) && \text{(by def. of } {}_{\bar{\mathcal{A}}}\mathbin{\triangle\!\!\!\!\!+})
\end{aligned}
$$

□

Proposition 3.10 (Associative Properties)**.**

$$
\begin{aligned}
(C_1 \parallel C_2) \parallel C_3 &\overset{\circ}{=} C_1 \parallel (C_2 \parallel C_3), && (3.6)\\
(C_1 \;{}_{p}\mathbin{\dot\sqcup}\; C_2) \;{}_{q}\mathbin{\dot\sqcup}\; C_3 &\overset{\circ}{=} C_1 \;{}_{p'}\mathbin{\dot\sqcup}\; (C_2 \;{}_{q'}\mathbin{\dot\sqcup}\; C_3), && (3.7)\\
(C_1 \;{}_{p}\!\oplus C_2) \;{}_{q}\!\oplus C_3 &= C_1 \;{}_{p'}\!\oplus (C_2 \;{}_{q'}\!\oplus C_3), && (3.8)\\
(C_1 \;{}_{\mathcal{A}}\triangle\; C_2) \;{}_{\mathcal{B}}\triangle\; C_3 &\overset{\circ}{=} C_1 \;{}_{(\mathcal{A}\cap\mathcal{B})}\triangle\; (C_2 \;{}_{\mathcal{B}}\triangle\; C_3), && (3.9)\\
(C_1 \;{}_{\mathcal{A}}\mathbin{\triangle\!\!\!\!\!+}\; C_2) \;{}_{\mathcal{B}}\mathbin{\triangle\!\!\!\!\!+}\; C_3 &= C_1 \;{}_{(\mathcal{A}\cap\mathcal{B})}\mathbin{\triangle\!\!\!\!\!+}\; (C_2 \;{}_{\mathcal{B}}\mathbin{\triangle\!\!\!\!\!+}\; C_3), && (3.10)
\end{aligned}
$$

where $p'{=}pq$ *and* $q'{=}{}^{(q-pq)}/_{(1-pq)}$.

Proof. (3.6) The bijection is given by $\psi(((y_1, y_2), y_3)) = (y_1,(y_2, y_3))$. For all $x \in \mathcal{X}$, $y_1 \in \mathcal{Y}_1$, $y_2 \in \mathcal{Y}_2$ and $y_3 \in \mathcal{Y}_3$,

$$
\begin{aligned}
&((C_1 \parallel C_2) \parallel C_3)(x,((y_1,y_2),y_3)) && \\
=&(C_1 \parallel C_2)(x,(y_1,y_2))C_3(x,y_3) && \text{(by def. of } \parallel) \\
=&C_1(x,y_1)C_2(x,y_2)C_3(x,y_3) && \text{(by def. of } \parallel) \\
=&C_1(x,y_1)(C_2 \parallel C_3)(x,(y_2,y_3)) && \text{(by def. of } \parallel) \\
=&(C_1 \parallel (C_2 \parallel C_3))(x,(y_1,(y_2,y_3))) && \text{(by def. of } \parallel)
\end{aligned}
$$

(3.7) The bijection is given by $\psi(((y_1, 1), 1)) = (y_1, 1)$, $\psi(((y_2, 2), 1)) = ((y_2, 1), 2)$ and $\psi((y_3, 2)) = ((y_3, 2), 1)$. For all $x \in \mathcal{X}$ and $((y, 1), 1) \in (\mathcal{Y}_1 \sqcup \mathcal{Y}_2) \sqcup \mathcal{Y}_3$,

$$
((C_1 \;{}_{p}\mathbin{\dot\sqcup}\; C_2) \;{}_{q}\mathbin{\dot\sqcup}\; C_3)(x,((y,1),1))
$$

$$
\begin{aligned}
&=pqC_1(x,y) && \text{(by def. of } {}_{p}\dot{\sqcup},\ {}_{q}\dot{\sqcup}\text{)}\\
&=p'C_1(x,y) && \text{(by def. of } p'\text{)}\\
&=(C_1\ {}_{p'}\dot{\sqcup}\ (C_2\ {}_{q'}\dot{\sqcup}\ C_3))(x,(y,1)) && \text{(by def. of } {}_{p'}\dot{\sqcup},\ {}_{q'}\dot{\sqcup}\text{)}
\end{aligned}
$$

For all $x \in \mathcal{X}$ and $((y,2),1) \in (\mathcal{Y}_1 \sqcup \mathcal{Y}_2) \sqcup \mathcal{Y}_3$,

$$
\begin{aligned}
&((C_1\ {}_{p}\dot{\sqcup}\ C_2)\ {}_{q}\dot{\sqcup}\ C_3)(x,((y,2),1))\\
&=(1-p)qC_2(x,y) && \text{(by def. of } {}_{p}\dot{\sqcup},\ {}_{q}\dot{\sqcup}\text{)}\\
&=(1-p')q'C_2(x,y) && \text{(by def. of } p',\ q'\text{)}\\
&=(C_1\ {}_{p'}\dot{\sqcup}\ (C_2\ {}_{q'}\dot{\sqcup}\ C_3))(x,((y,1),2)) && \text{(by def. of } {}_{p'}\dot{\sqcup},\ {}_{q'}\dot{\sqcup}\text{)}
\end{aligned}
$$

For all $x \in \mathcal{X}$ and $(y,2) \in (\mathcal{Y}_1 \sqcup \mathcal{Y}_2) \sqcup \mathcal{Y}_3$,

$$
\begin{aligned}
&((C_1\ {}_{p}\dot{\sqcup}\ C_2)\ {}_{q}\dot{\sqcup}\ C_3)(x,(y,2))\\
&=(1-q)C_3(x,y) && \text{(by def. of } {}_{p}\dot{\sqcup},\ {}_{q}\dot{\sqcup}\text{)}\\
&=(1-p')(1-q')C_3(x,y) && \text{(by def. of } p',\ q'\text{)}\\
&=(C_1\ {}_{p'}\dot{\sqcup}\ (C_2\ {}_{q'}\dot{\sqcup}\ C_3))(x,((y,2),2)) && \text{(by def. of } {}_{p'}\dot{\sqcup},\ {}_{q'}\dot{\sqcup}\text{)}
\end{aligned}
$$

(3.8) (${}_{p}\oplus$) For all $x \in \mathcal{X}$ and $y \in \mathcal{Y}_1 \cup \mathcal{Y}_2 \cup \mathcal{Y}_3$,

$$
\begin{aligned}
&((C_1\ {}_{p}\oplus\ C_2)\ {}_{q}\oplus\ C_3)(x,y)\\
&=pqC_1(x,y)+(1{-}p)qC_2(x,y){+}(1{-}q)C_3(x,y) && \text{(by def. of } {}_{p}\oplus,\ {}_{q}\oplus\text{)}\\
&=p'C_1(x,y){+}(1{-}p')q'C_2(x,y){+}(1{-}p')(1{-}q')C_3(x,y) && \text{(by def. of } p',\ q'\text{)}\\
&=(C_1\ {}_{p'}\oplus\ (C_2\ {}_{q'}\oplus\ C_3))(x,y) && \text{(by def. of } {}_{p'}\oplus,\ {}_{q'}\oplus\text{)}
\end{aligned}
$$

(3.9) The bijection is given by $\psi(((y_1,1),1)) = (y_1,1)$, $\psi(((y_2,2),1)) = ((y_2,1),2)$ and $\psi((y_3,2)) = ((y_3,2),1)$. For all $x \in \mathcal{A} \cap \mathcal{B}$ and $((y,1),1) \in (\mathcal{Y}_1 \sqcup \mathcal{Y}_2) \sqcup \mathcal{Y}_3$,

$$
\begin{aligned}
&((C_1\ {}_{\mathcal{A}}\triangle\ C_2)\ {}_{\mathcal{B}}\triangle\ C_3)(x,((y,1),1))\\
&=(C_1\ {}_{\mathcal{A}}\triangle\ C_2)(x,(y,1)) && \text{(by def. of } {}_{\mathcal{B}}\triangle\text{)}\\
&=C_1(x,y) && \text{(by def. of } {}_{\mathcal{A}}\triangle\text{)}\\
&=(C_1\ {}_{(\mathcal{A}\cap\mathcal{B})}⨹\ (C_2\ {}_{\mathcal{B}}⨹\ C_3))(x,(y,1)) && \text{(by def. of } {}_{\mathcal{A}\cap\mathcal{B}}\triangle,\ {}_{\mathcal{B}}\triangle\text{)}
\end{aligned}
$$

For all $x \in \bar{\mathcal{A}} \cap \mathcal{B}$ and $((y,2),1) \in (\mathcal{Y}_1 \sqcup \mathcal{Y}_2) \sqcup \mathcal{Y}_3$,

$$
((C_1\ {}_{\mathcal{A}}\triangle\ C_2)\ {}_{\mathcal{B}}\triangle\ C_3)(x,((y,2),1))
$$

$$\begin{aligned}
&=(C_1 \,{}_{\mathcal{A}}\!\triangle\, C_2)(x,(y,2)) && \text{(by def. of } {}_{\mathcal{B}}\triangle\text{)}\\
&=C_2(x,y) && \text{(by def. of } {}_{\mathcal{A}}\triangle\text{)}\\
&=(C_1 \,{}_{(\mathcal{A}\cap\mathcal{B})}\text{⟁}\, (C_2 \,{}_{\mathcal{B}}\text{⟁}\, C_3))(x,((y,1),2)) && \text{(by def. of } {}_{\mathcal{A}\cap\mathcal{B}}\triangle,\ {}_{\mathcal{B}}\triangle\text{)}
\end{aligned}$$

For all $x \in \bar{\mathcal{B}}$ and $(y,2) \in (\mathcal{Y}_1 \sqcup \mathcal{Y}_2) \sqcup \mathcal{Y}_3$,

$$\begin{aligned}
&((C_1 \,{}_{\mathcal{A}}\!\triangle\, C_2) \,{}_{\mathcal{B}}\!\triangle\, C_3)(x,(y,2))\\
=&C_3(x,y) && \text{(by def. of } {}_{\mathcal{B}}\triangle\text{)}\\
=&(C_1 \,{}_{(\mathcal{A}\cap\mathcal{B})}\text{⟁}\, (C_2 \,{}_{\mathcal{B}}\text{⟁}\, C_3))(x,((y,2),2)) && \text{(by def. of } {}_{\mathcal{A}\cap\mathcal{B}}\triangle,\ {}_{\mathcal{B}}\triangle\text{)}
\end{aligned}$$

For all the remaining pairs $(x,y') \in \mathcal{X} \times ((\mathcal{Y}_1 \sqcup \mathcal{Y}_2) \sqcup \mathcal{Y}_3)$ not contemplated above, we have

$$((C_1 \,{}_{\mathcal{A}}\!\triangle\, C_2) \,{}_{\mathcal{B}}\!\triangle\, C_3)(x,y') = (C_1 \,{}_{(\mathcal{A}\cap\mathcal{B})}\!\triangle\, (C_2 \,{}_{\mathcal{B}}\!\triangle\, C_3))(x,\phi(y')) = 0$$

(3.9) For all $x \in \mathcal{A} \cap \mathcal{B}$ and $y_1 \in \mathcal{Y}_1 \cup \mathcal{Y}_2 \cup \mathcal{Y}_3$,

$$\begin{aligned}
&((C_1 \,{}_{\mathcal{A}}\text{⟁}\, C_2) \,{}_{\mathcal{B}}\text{⟁}\, C_3)(x,y_1)\\
=&(C_1 \,{}_{\mathcal{A}}\text{⟁}\, C_2)(x,y_1) && \text{(by def. of } {}_{\mathcal{B}}\text{⟁)}\\
=&C_1(x,y_1) && \text{(by def. of } {}_{\mathcal{A}}\text{⟁)}\\
=&(C_1 \,{}_{(\mathcal{A}\cap\mathcal{B})}\text{⟁}\, (C_2 \,{}_{\mathcal{B}}\text{⟁}\, C_3))(x,y_1) && \text{(by def. of } {}_{\mathcal{A}\cap\mathcal{B}}\text{⟁},\ {}_{\mathcal{B}}\text{⟁)}
\end{aligned}$$

For all $x \in \bar{\mathcal{A}} \cap \mathcal{B}$ and $y_2 \in \mathcal{Y}_1 \cup \mathcal{Y}_2 \cup \mathcal{Y}_3$,

$$\begin{aligned}
&((C_1 \,{}_{\mathcal{A}}\text{⟁}\, C_2) \,{}_{\mathcal{B}}\text{⟁}\, C_3)(x,y_2)\\
=&(C_1 \,{}_{\mathcal{A}}\text{⟁}\, C_2)(x,y_2) && \text{(by def. of } {}_{\mathcal{B}}\text{⟁)}\\
=&C_2(x,y) && \text{(by def. of } {}_{\mathcal{A}}\text{⟁)}\\
=&(C_1 \,{}_{(\mathcal{A}\cap\mathcal{B})}\text{⟁}\, (C_2 \,{}_{\mathcal{B}}\text{⟁}\, C_3))(x,y_2) && \text{(by def. of } {}_{\mathcal{A}\cap\mathcal{B}}\text{⟁},\ {}_{\mathcal{B}}\text{⟁)}
\end{aligned}$$

For all $x \in \bar{\mathcal{B}}$ and $y_3 \in \mathcal{Y}_1 \cup \mathcal{Y}_2 \cup \mathcal{Y}_3$,

$$\begin{aligned}
&((C_1 \,{}_{\mathcal{A}}\text{⟁}\, C_2) \,{}_{\mathcal{B}}\text{⟁}\, C_3)(x,y_3)\\
=&C_3(x,y_3) && \text{(by def. of } {}_{\mathcal{B}}\text{⟁)}\\
=&(C_1 \,{}_{(\mathcal{A}\cap\mathcal{B})}\text{⟁}\, (C_2 \,{}_{\mathcal{B}}\text{⟁}\, C_3))(x,y_3) && \text{(by def. of } {}_{\mathcal{A}\cap\mathcal{B}}\text{⟁},\ {}_{\mathcal{B}}\text{⟁)}
\end{aligned}$$

□

Proposition 3.11 (Idempotency)**.**

$$C_1 \parallel C_1 \sqsubseteq_\circ C_1, \tag{3.11}$$

$$C_1 \;{}_{p}{\sqcup\!\!\!\cdot\;}\; C_1 \approx C_1, \tag{3.12}$$

$$C_1 \;{}_{p}\!\oplus C_1 = C_1, \tag{3.13}$$

$$C_1 \;{}_{\mathcal{A}}\!\triangle\; C_1 \sqsubseteq_\circ C_1, \tag{3.14}$$

$$C_1 \;{}_{\mathcal{A}}\text{⟁}\; C_1 = C_1. \tag{3.15}$$

Proof. (3.11) Let $D \in \mathcal{C}^{\mathcal{Y}_1}_{\mathcal{Y}_1\times\mathcal{Y}_1}$ be defined as, for all $y_1, y_2, y_3 \in \mathcal{Y}_1$,

$$D((y_1, y_2), y_3) = \begin{cases} 1, & \text{if } y_1 = y_3, \\ 0, & \text{otherwise.} \end{cases}$$

Then, $C_1 = (C_1 \parallel C_1)D$.

(3.12) For all $g \in \mathbb{G}\mathcal{X}$ and all $\pi \in \mathbb{D}\mathcal{X}$,

$$\begin{aligned} & V_g[\pi \rangle\, C_1 \;{}_{p}{\sqcup\!\!\!\cdot\;}\; C_1] \\ =& pV_g[\pi \rangle\, C_1] + (1-p)V_g[\pi \rangle\, C_1] && \text{(from Theorem 4.3)} \\ =& V_g[\pi \rangle\, C_1] \end{aligned}$$

(3.13) We have, for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}_1$:

$$(C_1 \;{}_{p}\!\oplus C_1)(x, y) = p \cdot C_1(x, y) + (1-p) \cdot C_1(x, y) = C_1(x, y)$$

(3.14) Let $D \in \mathcal{C}^{\mathcal{Y}}_{\mathcal{Y}_1\sqcup\mathcal{Y}_1}$ be defined as, for all $y_1, y_2 \in \mathcal{Y}_1$ and $i \in \{1, 2\}$,

$$D((y_1, i), y_2) = \begin{cases} 1, & \text{if } y_1 = y_2, \\ 0, & \text{otherwise.} \end{cases}$$

Then, $C_1 = (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_1)D$.

(3.15) By definition of ${}_{\mathcal{A}}\text{⟁}$, for all $x \in \mathcal{A} \cup \bar{\mathcal{A}} = \mathcal{X}$ and all $y \in \mathcal{Y}_1$,

$$(C_1 \;{}_{\mathcal{A}}\text{⟁}\; C_1)(x, y) = C_1(x, y)$$

□

Proposition 3.12. *Suppose* $\exists C \in \mathcal{C}_{\mathcal{X}}$ *such that* C *is deterministic and* $C_1 \approx C$*. Then*

$$C_1 \parallel C_1 \approx C_1.$$

Proof. Let $C_1 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}_1}$ be a channel and let $C \in \mathcal{C}_{\mathcal{A}}^{\mathcal{Y}}$ be a deterministic channel such that $\exists D_1 \in \mathcal{C}_{\mathcal{Y}_1}^{\mathcal{Y}}$ and $\exists D_2 \in \mathcal{C}_{\mathcal{Y}}^{\mathcal{Y}_1}$ such that $C = C_1 D_1$ and $C_1 = CD_2$.

We first claim that $C \sqsubseteq_\circ C \parallel C$. We have that,

$$(C \parallel C)(x, (y_1, y_2)) = \begin{cases} 1, \text{ if } y_1 = y_2 \text{ and } C(x, y_1) = 1 \\ 0, \text{ otherwise} \end{cases}$$

Therefore, $C \parallel C = CD_3$ where $D_3 \in \mathcal{C}_{\mathcal{Y}}^{\mathcal{Y}\times\mathcal{Y}}$ is given by $D(y_1, (y_2, y_3)) = 1$ if $y_1 = y_2 = y_3$, and 0 otherwise.

Let $D^{\parallel} \in \mathcal{C}_{\mathcal{Y}\times\mathcal{Y}}^{\mathcal{Y}_1\times\mathcal{Y}}$ such that $D^{\parallel}((y_1, y_2), (y_3, y_4)) = D_2(y_1, y_3) D_2(y_2, y_4)$. We obtain

$$\begin{aligned}
& C_1 \parallel C_1 \\
=& (CD_2) \parallel (CD_2) && (C_1 = CD_2) \\
=& (C \parallel C) D^{\parallel} && (\text{by Proposition 3.23}) \\
=& CD_3 D^{\parallel} && (C \parallel C = CD_3) \\
=& C_1 D_1 D_3 D^{\parallel} && (C = C_1 D_1)
\end{aligned}$$

Therefore, $C_1 \sqsubseteq_\circ C_1 \parallel C_1$. Proposition 3.11 then implies $C_1 \approx C_1 \parallel C_1$ □

A.2 Null and transparent channels

Proposition 3.13. *A channel $\overline{0} \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ is a null channel if, and only if, for all $y \in \mathcal{Y}$ and $x, x' \in \mathcal{X}$,*

$$\overline{0}(x, y) = \overline{0}(x', y).$$

Proof. First, let $\overline{0} \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ be a channel such that, for all $y \in \mathcal{Y}$ and $x, x' \in \mathcal{X}$, $\overline{0}(x, y) = \overline{0}(x', y)$. We choose any $x \in \mathcal{X}$ and define, for each $y \in \mathcal{Y}$, $\overline{0}(y) = \overline{0}(x, y)$. Therefore, for all $x \in \mathcal{X}$, $y \in \mathcal{Y}$, $\overline{0}(x, y) = \overline{0}(y)$

To see that $\overline{0}$ is a null channel, observe that, for all $\pi \in \mathbb{D}\mathcal{X}$ and all $g \in \mathbb{G}\mathcal{X}$,

$$\begin{aligned}
& V_g[\pi \rangle \overline{0}] \\
=& \sum_{y \in \mathcal{Y}} \max_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \pi(x) \overline{0}(x, y) g(w, x) && (\text{by def. of } V_g)s
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{y\in\mathcal{Y}} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} \pi(x)\overline{0}(y)g(w,x) && (\overline{0}(x,y)=\overline{0}(y))\\
&= \sum_{y\in\mathcal{Y}} \overline{0}(y) \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} \pi(x)g(w,x) && (\overline{0}(y) \text{ does not depend on } x)\\
&= \sum_{y\in\mathcal{Y}} \overline{0}(y)V_g[\pi] && (\text{by def. of } V_g)\\
&= V_g[\pi] && (\overline{0} \text{ is a channel})
\end{aligned}
$$

Conversely, let $C \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ such that $C(x_1,y') > C(x_2,y')$ for some $x_1,x_2 \in \mathcal{X}$, $y' \in \mathcal{Y}$. let $g_{id} \in \mathbb{G}\mathcal{X}$ be as in Definition 2.10, and let $\pi_u \in \mathbb{D}\mathcal{X}$ be the uniform distribution on $\mathcal{X}$. We have

$$
\begin{aligned}
&V_{g_{id}}[\pi_u \rangle C]\\
&= \sum_{y\in\mathcal{Y}} \max_{w\in\mathcal{X}} \sum_{x\in\mathcal{X}} \pi_u(x)C(x,y)g_{id}(w,x) && (\text{by def. of } V_{g_{id}})\\
&= \max_{w\in\mathcal{X}} \sum_{x\in\mathcal{X}} \pi_u(x)C(x,y')g_{id}(w,x)\\
&\quad + \sum_{y\in\mathcal{Y}\setminus\{y'\}} \max_{w\in\mathcal{X}} \sum_{x\in\mathcal{X}} \pi_u(x)C(x,y)g_{id}(w,x) && (\text{reorganizing})\\
&\geq \max_{w\in\mathcal{X}} \pi_u(x_1)C(x_1,y')g_{id}(w,x_1)\\
&\quad + \sum_{y\in\mathcal{Y}\setminus\{y'\}} \max_{w\in\mathcal{X}} \pi_u(x_2)C(x_2,y)g_{id}(w,x_2) && (\text{Subtracting nonegative terms})\\
&= \pi_u(x_1)C(x_1,y') + \sum_{y\in\mathcal{Y}\setminus\{y'\}} \pi_u(x_2)C(x_2,y) && (\text{by def. of } g_{id})\\
&> \sum_{y\in\mathcal{Y}} \pi_u(x_2)C(x_2,y) && (C(x_1,y') > C(x_2,y'))\\
&= \pi_u(x_2) && (C \text{ is a channel})\\
&= V_{g_{id}}(\pi_u) && (\text{by def. of } V_{g_{id}},\ \pi_u)
\end{aligned}
$$

Therefore, $V_{g_{id}}[\pi_u \rangle C] > V_{g_{id}}(\pi_u)$, and C is not null. □

Proposition 3.14. *A channel $\overline{I} \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ is a transparent channel if, and only if, for all $y \in \mathcal{Y}$ and $x, x' \in \mathcal{X}$ such that $x \neq x'$,*

$$\overline{I}(x,y) > 0 \implies \overline{I}(x',y) = 0.$$

Proof. Let $\overline{I} \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ be a channel such that, for all $y \in \mathcal{Y}$ and for all $x, x' \in \mathcal{X}$ such that

$x \neq x'$, $\overline{I}(x, y) > 0 \implies \overline{I}(x', y) = 0$.

Let $I_1 \in \mathcal{C}^{\mathcal{X}}_{\mathcal{Y}}$ be given by

$$I_1(y, x) = \begin{cases} 1, & \text{if } \overline{I}(x, y) > 0 \\ 1/|\mathcal{X}|, & \text{if } \forall x' \in \mathcal{X}, \overline{I}(x', y) = 0 \\ 0, & \text{otherwise} \end{cases}$$

Since, for each $y \in \mathcal{Y}$, there is at most one $x \in \mathcal{X}$ such that $\overline{I}(x, y) > 0$, I_1 is a channel. Now, for all $x_1, x_2 \in \mathcal{X}$, we have,

$$(\overline{I}I_1)(x_1, x_2) = \sum_{y \in \mathcal{Y}} \overline{I}(x_1, y) I_1(y, x_2) = \begin{cases} 1, \text{ if } x_1 = x_2 \\ 0, \text{ otherwise} \end{cases}$$

Let $C \in \mathcal{C}_{\mathcal{X}}$. Then, $C = (\overline{I}I_1)C = \overline{I}(I_1 C)$. Therefore, $\overline{I} \sqsubseteq_\circ C$.

Conversely, let $C \in \mathcal{C}^{\mathcal{Y}}_{\mathcal{X}}$ such that $C(x_1, y') > 0$ and $C(x_2, y') > 0$ for some $x_1, x_2 \in \mathcal{X}$, $y' \in \mathcal{Y}$. Let $g_{id} \in \mathbb{G}\mathcal{X}$ be as in Definition 2.10, and let $\pi \in \mathbb{D}\mathcal{X}$ be given by $pi(x) = 1/2$ if $x \in \{x_1, x_2\}$, or 0 otherwise. We have

$$\begin{aligned}
& V_{g_{id}}[\pi_u \rangle C] \\
=& \sum_{y \in \mathcal{Y}} \max_{w \in \mathcal{X}} \sum_{x \in \mathcal{X}} \pi(x) C(x, y) g_{id}(w, x) && \text{(by def. of } V_{g_{id}}\text{)} \\
=& \sum_{y \in \mathcal{Y}} \max_{w \in \mathcal{X}} \Big(\pi(x_1) C(x_1, y) g_{id}(w, x_1) \\
& + \pi(x_2) C(x_2, y) g_{id}(w, x_2) \Big) && \text{(by def. of } \pi\text{)} \\
=& \sum_{y \in \mathcal{Y}} \max(\pi(x_1) C(x_1, y), \pi(x_2) C(x_2, y)) && \text{(by def. of } g_{id}\text{)} \\
<& \sum_{y \in \mathcal{Y}} \pi(x_1) C(x_1, y) + \pi(x_2) C(x_2, y) && (C(x_1, y') > 0 \text{ and } C(x_2, y') > 0) \\
=& 1 && (C_1,\ C_2 \text{ are channels})
\end{aligned}$$

Let $I \in \mathcal{C}^{\mathcal{X}}_{\mathcal{X}}$ be given by $I(x, x') = 1$ if $x = x'$ and 0 otherwise. Then, $V_{g_{id}}[\pi \rangle I] = 1$, and therefore $C \not\sqsubseteq_\circ I$ □

Proposition 3.15 (Null Channel Properties)**.**

$$C_1 \approx (C_1 \parallel \overline{0}), \tag{3.16}$$

$$C_1 \sqsubseteq_\circ (C_1 \,{}_p{\sqcup}\, \overline{0}), \tag{3.17}$$

$$C_1 \sqsubseteq_\circ (C_1 \,{}_p{\oplus}\, \overline{0}). \tag{3.18}$$

Proof. (3.16) Firstly, from Proposition 3.13, we notice that $\overline{0}(x,z) = \overline{0}(x',z)$ for any $x, x' \in \mathcal{X}$ and $z \in \mathcal{Z}$. Thus, given $z \in \mathcal{Z}$ we can uniquely define chose $\overline{0}(z) = \overline{0}(x,z)$ for an arbitrarily chosen $x \in \mathcal{X}$.

We then have that, for any $\pi \in \mathbb{D}\mathcal{X}$ and $g \in \mathbb{G}\mathcal{X}$:

$$\begin{aligned}
& V_g[\pi \rangle C_1 \parallel \overline{0}] \\
=& \sum_{z\in\mathcal{Z}} \sum_{y\in\mathcal{Y}} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} C_1(x,y)\cdot\overline{0}(x,z)\cdot g(w,x)\cdot\pi(x) && \text{(by def. of } \parallel\text{)} \\
=& \sum_{z\in\mathcal{Z}} \sum_{y\in\mathcal{Y}} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} C_1(x,y)\cdot\overline{0}(z)\cdot g(w,x)\cdot\pi(x) && \text{(by def. of } \overline{0}(z)\text{)} \\
=& \sum_{z\in\mathcal{Z}} \overline{0}(z) \sum_{y\in\mathcal{Y}} \max_{w\in\mathcal{W}} \sum_{x\in\mathcal{X}} C_1(x,y)\cdot g(w,x)\cdot\pi(x) && \text{(reorganizing)} \\
=& \sum_{z\in\mathcal{Z}} \overline{0}(z)\cdot V_g[\pi \rangle C_1] && \text{(by def. of vulnerability)} \\
=& V_g[\pi \rangle C_1] && (\overline{0} \text{ is a channel})
\end{aligned}$$

(3.17) We have, for all $\pi \in \mathbb{D}\mathcal{X}$, and all $g \in \mathbb{G}\mathcal{X}$,

$$\begin{aligned}
& V_g[\pi \rangle C_1 \,{}_p{\sqcup}\, \overline{0}] \\
=& pV_g[\pi \rangle C_1] + (1-p)V_g[\pi \rangle \overline{0}] && \text{(from Theorem 4.3)} \\
\leq& pV_g[\pi \rangle C_1] + (1-p)V_g[\pi \rangle C_1] && (V_g[\pi \rangle \overline{0}] \leq V_g[\pi \rangle C_1]) \\
=& V_g[\pi \rangle C_1]
\end{aligned}$$

(3.18) We have, for all $\pi \in \mathbb{D}\mathcal{X}$ and all $g \in \mathbb{G}\mathcal{X}$,

$$\begin{aligned}
& V_g[\pi \rangle C_1 \,{}_p{\oplus}\, \overline{0}] \\
\leq& pV_g[\pi \rangle C_1] + (1-p)V_g[\pi \rangle \overline{0}] && \text{(from Theorem 4.5)} \\
\leq& pV_g[\pi \rangle C_1] + (1-p)V_g[\pi \rangle C_1] && (V_g[\pi \rangle \overline{0}] \leq V_g[\pi \rangle C_1]) \\
=& V_g[\pi \rangle C_1]
\end{aligned}$$

□

Proposition 3.16 (Transparent Channel Properties).

$$(C_1 \parallel \overline{I}) \approx \overline{I}, \tag{3.19}$$

$$(C_1 \;{}_{p}\dot{\sqcup}\; \overline{I}) \sqsubseteq_\circ C_1, \tag{3.20}$$

$$(C_1 \;{}_{\mathcal{A}}\triangle\; \overline{I}) \sqsubseteq_\circ C_1. \tag{3.21}$$

Proof. (3.19) From Theorem 4.1, we have, for all $\pi \in \mathbb{D}\mathcal{X}$ and $g \in \mathbb{G}\mathcal{X}$, $V_g[\pi \rangle C_1 \parallel \overline{I}] \geq V_g[\pi \rangle \overline{I}]$. From Proposition 3.14, $\overline{I} \sqsubseteq_\circ C_1 \parallel \overline{I}$. Thus, $C_1 \parallel \overline{I} \approx \overline{I}$

(3.20) We have, for all $\pi \in \mathbb{D}\mathcal{X}$ and $g \in \mathbb{G}\mathcal{X}$,

$$\begin{aligned}
& V_g[\pi \rangle C_1 \;{}_{p}\dot{\sqcup}\; \overline{I}] \\
=& pV_g[\pi \rangle C_1] + (1-p)V_g[\pi \rangle \overline{I}] && \text{(from Theorem 4.3)} \\
\geq& pV_g[\pi \rangle C_1] + (1-p)V_g[\pi \rangle C_1] && (V_g[\pi \rangle \overline{I}] \geq V_g[\pi \rangle C_1]) \\
=& V_g[\pi \rangle C_1]
\end{aligned}$$

(3.21) We have, for all $\pi \in \mathbb{D}\mathcal{X}$ and $g \in \mathbb{G}\mathcal{X}$,

$$\begin{aligned}
& V_g[\pi \rangle C_1] \\
\leq& V_g[\pi \rangle C_1 \;{}_{\mathcal{A}}\triangle\; C_1] && \text{(by Eq. (3.14))} \\
=& V_{g_{\mathcal{A}}}[\pi \rangle C_1] + V_{g_{\overline{\mathcal{A}}}}[\pi \rangle C_1] && \text{(by Theorem 4.11)} \\
\leq& V_{g_{\mathcal{A}}}[\pi \rangle C_1] + V_{g_{\overline{\mathcal{A}}}}[\pi \rangle \overline{I}] && \text{(by corollary 4.10 and } \overline{I}|_{\overline{\mathcal{A}}} \sqsubseteq_\circ C_1|_{\overline{\mathcal{A}}}) \\
=& V_g[\pi \rangle C_1 \;{}_{\mathcal{A}}\triangle\; \overline{I}] && \text{(by Theorem 4.11)}
\end{aligned}$$

□

A.3 Distributive properties

Proposition 3.17 (Distributivity for the Parallel operator).

$$C_1 \parallel (C_2 \parallel C_3){}_\circ\!\sqsupseteq (C_1 \parallel C_2) \parallel (C_1 \parallel C_3), \tag{3.22}$$

$$C_1 \parallel (C_2 \;{}_{p}\dot{\sqcup}\; C_3) \overset{\circ}{=} (C_1 \parallel C_2) \;{}_{p}\dot{\sqcup}\; (C_1 \parallel C_3), \tag{3.23}$$

$$C_1 \parallel (C_2 \;{}_{p}\oplus\; C_3) = (C_1 \parallel C_2) \;{}_{p}\oplus\; (C_1 \parallel C_3), \tag{3.24}$$

$$C_1 \parallel (C_2 \;{}_{\mathcal{A}}\triangle\; C_3) \overset{\circ}{=} (C_1 \parallel C_2) \;{}_{\mathcal{A}}\triangle\; (C_1 \parallel C_3), \tag{3.25}$$

$$C_1 \parallel (C_2 \ {}_{\mathcal{A}}\triangleplus\ C_3) = (C_1 \parallel C_2)\ {}_{\mathcal{A}}\triangleplus\ (C_1 \parallel C_3). \tag{3.26}$$

Proof. (3.22) Using the commutative and associative properties of the parallel operator, it is easy to show that

$$(C_1 \parallel C_2) \parallel (C_1 \parallel C_3) \approx (C_1 \parallel C_1) \parallel (C_2 \parallel C_3)$$

Now, from Proposition 3.11, $(C_1 \parallel C_1) \sqsubseteq_\circ C_1$. Thus, Theorem 4.16 implies

$$(C_1 \parallel C_1) \parallel (C_2 \parallel C_3) \sqsubseteq_\circ C_1 \parallel (C_2 \parallel C_3)$$

(3.23) The bijection is given by $\phi((y_1,(y_2,i))) = ((y_1,y_2),i)$, for all $((y_1,(y_2,i))) \in \mathcal{Y}_1 \times (\mathcal{Y}_2 \sqcup \mathcal{Y}_3)$. For all $x \in \mathcal{X}$, $y_1 \in \mathcal{Y}_1$ and $y_2 \in \mathcal{Y}_2$,

$$\begin{aligned}
&(C_1 \parallel (C_2\ {}_p\sqcupdot\ C_3))(x,(y_1,(y_2,1))) \\
=&C_1(x,y_1)(C_2\ {}_p\sqcupdot\ C_3)(x,(y_2,1)) && \text{(by definition of $\parallel$)} \\
=&pC_1(x,y_1)C_2(x,y_2) && \text{(by definition of ${}_p\sqcupdot$)} \\
=&p(C_1 \parallel C_2)(x,(y_1,y_2)) && \text{(by definition of $\parallel$)} \\
=&((C_1 \parallel C_2)\ {}_p\sqcupdot\ (C_1 \parallel C_3))(x,((y_1,y_2),1)) && \text{(by definition of ${}_p\sqcupdot$)}
\end{aligned}$$

For all $x \in \mathcal{X}$, $y_1 \in \mathcal{Y}_1$ and $y_3 \in \mathcal{Y}_3$,

$$\begin{aligned}
&(C_1 \parallel (C_2\ {}_p\sqcupdot\ C_3))(x,(y_1,(y_3,2))) \\
=&C_1(x,y_1)(C_2\ {}_p\sqcupdot\ C_3)(x,(y_3,2)) && \text{(by definition of $\parallel$)} \\
=&(1-p)C_1(x,y_1)C_3(x,y_3) && \text{(by definition of ${}_p\sqcupdot$)} \\
=&(1-p)(C_1 \parallel C_2)(x,(y_1,y_3)) && \text{(by definition of $\parallel$)} \\
=&((C_1 \parallel C_2)\ {}_p\sqcupdot\ (C_1 \parallel C_3))(x,((y_1,y_3),2)) && \text{(by definition of ${}_p\sqcupdot$)}
\end{aligned}$$

(3.24) For all $x \in \mathcal{X}$, $y_1 \in \mathcal{Y}_1$ and $y' \in \mathcal{Y}_2 \cup \mathcal{Y}_3$,

$$\begin{aligned}
&(C_1 \parallel (C_2\ {}_p\oplus\ C_3))(x,(y_1,y')) \\
=&C_1(x,y_1)(C_2\ {}_p\oplus\ C_3)(x,y') && \text{(by definition of $\parallel$)} \\
=&C_1(x,y_1)(pC_2(x,y') + (1-p)C_3(x,y')) && \text{(by definition of ${}_p\oplus$)} \\
=&p(C_1 \parallel C_2)(x,(y_1,y')) + (1-p)(C_1 \parallel C_2)(x,(y_1,y')) && \text{(by definition of $\parallel$)} \\
=&((C_1 \parallel C_2)\ {}_p\oplus\ (C_1 \parallel C_3))(x,(y_1,y')) && \text{(by definition of ${}_p\oplus$)}
\end{aligned}$$

(3.25) The bijection is given by $\phi((y_1,(y_2,i))) = ((y_1,y_2),i)$, for all $((y_1,(y_2,i))) \in \mathcal{Y}_1 \times (\mathcal{Y}_2 \sqcup \mathcal{Y}_3)$. For all $x \in \mathcal{A}$ and $(y_1,(y_2,1)) \in \mathcal{Y}_1 \times (\mathcal{Y}_2 \sqcup \mathcal{Y}_3)$,

$$\begin{aligned}
&C_1 \parallel (C_2 \,{}_{\mathcal{A}}\triangle\, C_3)(x,(y_1,(y_2,1))) \\
=&C_1(x,y_1)(C_2 \,{}_{\mathcal{A}}\triangle\, C_3)(x,(y_2,1)) && \text{(by def of } \parallel) \\
=&C_1(x,y_1)C_2(x,y_2) && \text{(by def of } {}_{\mathcal{A}}\triangle) \\
=&(C_1 \parallel C_2)(x,(y_1,y_2)) && \text{(by def of } \parallel) \\
=&((C_1 \parallel C_2) \,{}_{\mathcal{A}}\triangle\, (C_1 \parallel C_3))(x,((y_1,y_2),1)) && \text{(by def of } {}_{\mathcal{A}}\triangle)
\end{aligned}$$

Similarly, for all $x \in \bar{\mathcal{A}}$ and $(y_1,(y_2,2)) \in \mathcal{Y}_1 \times (\mathcal{Y}_2 \sqcup \mathcal{Y}_3)$,

$$\begin{aligned}
&C_1 \parallel (C_2 \,{}_{\mathcal{A}}\triangle\, C_3)(x,(y_1,(y_2,2))) \\
=&C_1(x,y_1)(C_2 \,{}_{\mathcal{A}}\triangle\, C_3)(x,(y_2,2)) && \text{(by def of } \parallel) \\
=&C_1(x,y_1)C_3(x,y_2) && \text{(by def of } {}_{\mathcal{A}}\triangle) \\
=&(C_1 \parallel C_3)(x,(y_1,y_2)) && \text{(by def of } \parallel) \\
=&((C_1 \parallel C_2) \,{}_{\mathcal{A}}\triangle\, (C_1 \parallel C_3))(x,((y_1,y_2),2)) && \text{(by def of } {}_{\mathcal{A}}\triangle)
\end{aligned}$$

For all other pairs $(x,y') \in \mathcal{X} \times (\mathcal{Y}_1 \times (\mathcal{Y}_2 \sqcup \mathcal{Y}_3))$, we have

$$C_1 \parallel (C_2 \,{}_{\mathcal{A}}\triangle\, C_3)(x,y') = ((C_1 \parallel C_2) \,{}_{\mathcal{A}}\triangle\, (C_1 \parallel C_3))(x,\phi(y')) = 0$$

(3.26) For all $x \in \mathcal{A}$ and $(y_1,y_2) \in \mathcal{Y}_1 \times (\mathcal{Y}_2 \cup \mathcal{Y}_3)$,

$$\begin{aligned}
&C_1 \parallel (C_2 \,{}_{\mathcal{A}}⨹\, C_3)(x,(y_1,y_2)) \\
=&C_1(x,y_1)(C_2 \,{}_{\mathcal{A}}⨹\, C_3)(x,y_2) && \text{(by def of } \parallel) \\
=&C_1(x,y_1)C_2(x,y_2) && \text{(by def of } {}_{\mathcal{A}}⨹) \\
=&(C_1 \parallel C_2)(x,(y_1,y_2)) && \text{(by def of } \parallel) \\
=&((C_1 \parallel C_2) \,{}_{\mathcal{A}}⨹\, (C_1 \parallel C_3))(x,(y_1,y_2)) && \text{(by def of } {}_{\mathcal{A}}⨹)
\end{aligned}$$

Similarly, for all $x \in \bar{\mathcal{A}}$ and $(y_1,y_2) \in \mathcal{Y}_1 \times (\mathcal{Y}_2 \cup \mathcal{Y}_3)$,

$$\begin{aligned}
&C_1 \parallel (C_2 \,{}_{\mathcal{A}}⨹\, C_3)(x,(y_1,y_2)) \\
=&C_1(x,y_1)(C_2 \,{}_{\mathcal{A}}⨹\, C_3)(x,y_2) && \text{(by def of } \parallel) \\
=&C_1(x,y_1)C_3(x,y_2) && \text{(by def of } {}_{\mathcal{A}}⨹) \\
=&(C_1 \parallel C_3)(x,(y_1,y_2)) && \text{(by def of } \parallel)
\end{aligned}$$

$$=((C_1 \parallel C_2)\ {}_{\mathcal{A}}\mathbin{\triangle\!\!\!\!{\scriptstyle+}\,}\ (C_1 \parallel C_3))(x,(y_1,y_2)) \qquad \text{(by def of } {}_{\mathcal{A}}\mathbin{\triangle\!\!\!\!{\scriptstyle+}\,}\text{)}$$

□

Proposition 3.18 (Distributivity for Visible Choice).

$$C_1\ {}_{p}\dot{\sqcup}\ (C_2\ {}_{q}\dot{\sqcup}\ C_3) \approx (C_1\ {}_{p}\dot{\sqcup}\ C_2)\ {}_{q}\dot{\sqcup}\ (C_1\ {}_{p}\dot{\sqcup}\ C_3), \tag{3.27}$$

$$C_1\ {}_{p}\dot{\sqcup}\ (C_2\ {}_{q}\oplus\ C_3) = (C_1\ {}_{p}\dot{\sqcup}\ C_2)\ {}_{q}\oplus\ (C_1\ {}_{p}\dot{\sqcup}\ C_3), \tag{3.28}$$

$$C_1\ {}_{p}\dot{\sqcup}\ (C_2\ {}_{\mathcal{A}}\triangle\ C_3)_{\circ}\!\sqsupseteq (C_1\ {}_{p}\dot{\sqcup}\ C_2)\ {}_{\mathcal{A}}\triangle\ (C_1\ {}_{p}\dot{\sqcup}\ C_3), \tag{3.29}$$

$$C_1\ {}_{p}\dot{\sqcup}\ (C_2\ {}_{\mathcal{A}}\mathbin{\triangle\!\!\!\!{\scriptstyle+}\,}\ C_3) = (C_1\ {}_{p}\dot{\sqcup}\ C_2)\ {}_{\mathcal{A}}\mathbin{\triangle\!\!\!\!{\scriptstyle+}\,}\ (C_1\ {}_{p}\dot{\sqcup}\ C_3). \tag{3.30}$$

Proof. (3.27) For all $\pi \in \mathbb{D}\mathcal{X}$ and $g \in \mathbb{G}\mathcal{X}$, we have

$$\begin{aligned}
&V_g[\pi\,\rangle\, C_1\ {}_{p}\dot{\sqcup}\ (C_2\ {}_{q}\dot{\sqcup}\ C_3)] \\
=&pV_g[\pi\,\rangle\, C_1] + (1-p)V_g[\pi\,\rangle\, C_2\ {}_{q}\dot{\sqcup}\ C_3] && \text{(from Theorem 4.3)}\\
=&pV_g[\pi\,\rangle\, C_1] + (1-p)qV_g[\pi\,\rangle\, C_2] + (1-p)(1-q)V_g[\pi\,\rangle\, C_3] && \text{(from Theorem 4.3)}\\
=&pqV_g[\pi\,\rangle\, C_1] + (1-p)qV_g[\pi\,\rangle\, C_2]\\
&+ p(1-q)V_g[\pi\,\rangle\, C_1] + (1-p)(1-q)V_g[\pi\,\rangle\, C_3] && \text{(rearranging)}\\
=&qV_g[\pi\,\rangle\, C_1\ {}_{p}\dot{\sqcup}\ C_2] + (1-q)V_g[\pi\,\rangle\, C_1\ {}_{p}\dot{\sqcup}\ C_3] && \text{(from Theorem 4.3)}\\
=&V_g[\pi\,\rangle\, (C_1\ {}_{p}\dot{\sqcup}\ C_2)\ {}_{q}\dot{\sqcup}\ (C_1\ {}_{p}\dot{\sqcup}\ C_3)] && \text{(from Theorem 4.3)}
\end{aligned}$$

(3.28) For all $x \in \mathcal{X}$ and $(y,1) \in \mathcal{Y}_1 \sqcup (\mathcal{Y}_2 \cup \mathcal{Y}_3)$,

$$\begin{aligned}
&(C_1\ {}_{p}\dot{\sqcup}\ (C_2\ {}_{q}\oplus\ C_3))(x,(y,1)) \\
=&pC_1(x,y_1) && \text{(by def. of } {}_{p}\dot{\sqcup}\text{)}\\
=&q(pC_1(x,y_1)) + (1-q)(pC_1(x,y)) && \text{(rearranging)}\\
=&q(C_1\ {}_{p}\dot{\sqcup}\ C_2)(x,(y,1)) + (1-q)(C_1\ {}_{p}\dot{\sqcup}\ C_3)(x,(y,1)) && \text{(by def. of } {}_{p}\dot{\sqcup}\text{)}\\
=&((C_1\ {}_{p}\dot{\sqcup}\ C_2)\ {}_{q}\oplus\ (C_1\ {}_{p}\dot{\sqcup}\ C_3))(x,(y,1)) && \text{(by def. of } {}_{q}\oplus\text{)}
\end{aligned}$$

For all $x \in \mathcal{X}$ and $(y,2) \in \mathcal{Y}_1 \sqcup (\mathcal{Y}_2 \cup \mathcal{Y}_3)$,

$$\begin{aligned}
&(C_1\ {}_{p}\dot{\sqcup}\ (C_2\ {}_{q}\oplus\ C_3))(x,(y,2)) \\
=&(1-p)(C_2\ {}_{q}\oplus\ C_3)(x,y) && \text{(by def. of } {}_{p}\dot{\sqcup}\text{)}\\
=&(1-p)(qC_2(x,y) + (1-q)C_3(x,y)) && \text{(by def. of } {}_{q}\oplus\text{)}\\
=&q(1-p)C_2(x,y) + (1-q)(1-p)C_3(x,y) && \text{(rearranging)}\\
=&q(C_1\ {}_{p}\dot{\sqcup}\ C_2)(x,(y,2)) + (1-q)(C_1\ {}_{p}\dot{\sqcup}\ C_3)(x,(y,2)) && \text{(by def. of } {}_{p}\dot{\sqcup}\text{)}
\end{aligned}$$

$$=((C_1 \,{}_{p}\dot\sqcup\, C_2) \,{}_{q}\oplus\, (C_1 \,{}_{p}\dot\sqcup\, C_3))(x,(y,2)) \qquad \text{(by def. of } {}_{q}\oplus\text{)}$$

(3.29) For all $\pi \in \mathbb{D}\mathcal{X}$ and $g \in \mathbb{G}\mathcal{X}$,

$$\begin{aligned}
&V_g[\pi\,\rangle\, C_1 \,{}_{p}\dot\sqcup\, (C_2 \,{}_{\mathcal{A}}\triangle\, C_3)] \\
=&pV_g[\pi\,\rangle\, C_1] + (1-p)V_g[\pi\,\rangle\, C_2 \,{}_{\mathcal{A}}\triangle\, C_3] && \text{(by thm 4.3)} \\
\leq&pV_g[\pi\,\rangle\, C_1 \,{}_{\mathcal{A}}\triangle\, C_1] + (1-p)V_g[\pi\,\rangle\, C_2 \,{}_{\mathcal{A}}\triangle\, C_3] && \text{(by eq. 3.14)} \\
=&pV_{g_{\mathcal{A}}}[\pi\,\rangle\, C_1] + pV_{g_{\bar{\mathcal{A}}}}[\pi\,\rangle\, C_1] \\
&\quad + (1-p)V_{g_{\mathcal{A}}}[\pi\,\rangle\, C_2] + (1-p)V_{g_{\bar{\mathcal{A}}}}[\pi\,\rangle\, C_3] && \text{(by thm 4.11)} \\
=&V_{g_{\mathcal{A}}}[\pi\,\rangle\, C_1 \,{}_{p}\dot\sqcup\, C_2] + V_{g_{\bar{\mathcal{A}}}}[\pi\,\rangle\, C_1 \,{}_{p}\dot\sqcup\, C_3] && \text{(by thm 4.3)} \\
=&V_{g_{\mathcal{A}}}[\pi\,\rangle\, (C_1 \,{}_{p}\dot\sqcup\, C_2) \,{}_{\mathcal{A}}\triangle\, (C_1 \,{}_{p}\dot\sqcup\, C_3)] && \text{(by thm 4.11)}
\end{aligned}$$

(3.30) For all $x \in \mathcal{A}$, $(y,1) \in \mathcal{Y}_1 \sqcup (\mathcal{Y}_2 \cup \mathcal{Y}_3)$

$$\begin{aligned}
&(C_1 \,{}_{p}\dot\sqcup\, (C_2 \,{}_{\mathcal{A}}\triangle\mkern-13mu+\, C_3))(x,(y,1)) \\
=&pC_1(x,y) && \text{(by def. of } {}_{p}\dot\sqcup\text{)} \\
=&(C_1 \,{}_{p}\dot\sqcup\, C_2)(x,(y,1)) && \text{(by def. of } {}_{p}\dot\sqcup\text{)} \\
=&(C_1 \,{}_{p}\dot\sqcup\, C_2) \,{}_{\mathcal{A}}\triangle\mkern-13mu+\, (C_1 \,{}_{p}\dot\sqcup\, C_3)(x,(y,1)) && \text{(by def. of } {}_{\mathcal{A}}\triangle\mkern-13mu+\text{)}
\end{aligned}$$

For all $x \in \bar{\mathcal{A}}$, $(y,1) \in \mathcal{Y}_1 \sqcup (\mathcal{Y}_2 \cup \mathcal{Y}_3)$

$$\begin{aligned}
&(C_1 \,{}_{p}\dot\sqcup\, (C_2 \,{}_{\mathcal{A}}\triangle\mkern-13mu+\, C_3))(x,(y,1)) \\
=&pC_1(x,y) && \text{(by def. of } {}_{p}\dot\sqcup\text{)} \\
=&(C_1 \,{}_{p}\dot\sqcup\, C_3)(x,(y,1)) && \text{(by def. of } {}_{p}\dot\sqcup\text{)} \\
=&(C_1 \,{}_{p}\dot\sqcup\, C_2) \,{}_{\mathcal{A}}\triangle\mkern-13mu+\, (C_1 \,{}_{p}\dot\sqcup\, C_3)(x,(y,1)) && \text{(by def. of } {}_{\mathcal{A}}\triangle\mkern-13mu+\text{)}
\end{aligned}$$

For all $x \in \mathcal{A}$, $(y,2) \in \mathcal{Y}_1 \sqcup (\mathcal{Y}_2 \cup \mathcal{Y}_3)$

$$\begin{aligned}
&(C_1 \,{}_{p}\dot\sqcup\, (C_2 \,{}_{\mathcal{A}}\triangle\mkern-13mu+\, C_3))(x,(y,2)) \\
=&(1-p)(C_2 \,{}_{\mathcal{A}}\triangle\mkern-13mu+\, C_3)(x,y) && \text{(by def. of } {}_{p}\dot\sqcup\text{)} \\
=&(1-p)C_2(x,y) && \text{(by def. of } {}_{\mathcal{A}}\triangle\mkern-13mu+\text{)} \\
=&(C_1 \,{}_{p}\dot\sqcup\, C_2)(x,(y,2)) && \text{(by def. of } {}_{p}\dot\sqcup\text{)} \\
=&(C_1 \,{}_{p}\dot\sqcup\, C_2) \,{}_{\mathcal{A}}\triangle\mkern-13mu+\, (C_1 \,{}_{p}\dot\sqcup\, C_3)(x,(y,2)) && \text{(by def. of } {}_{\mathcal{A}}\triangle\mkern-13mu+\text{)}
\end{aligned}$$

For all $x \in \bar{\mathcal{A}}$, $(y, 2) \in \mathcal{Y}_1 \sqcup (\mathcal{Y}_2 \cup \mathcal{Y}_3)$

$$\begin{aligned}
&(C_1 \ {}_{p}\dot{\sqcup}\ (C_2 \ {}_{\mathcal{A}}\triangle\ C_3))(x, (y, 2)) && \\
=&(1 - p)(C_2 \ {}_{\mathcal{A}}\triangle\ C_3)(x, y) && \text{(by def. of } {}_{p}\dot{\sqcup}\text{)} \\
=&(1 - p)C_3(x, y) && \text{(by def. of } {}_{\mathcal{A}}\triangle\text{)} \\
=&(C_1 \ {}_{p}\dot{\sqcup}\ C_3)(x, (y, 2)) && \text{(by def. of } {}_{p}\dot{\sqcup}\text{)} \\
=&(C_1 \ {}_{p}\dot{\sqcup}\ C_2) \ {}_{\mathcal{A}}\triangle\ (C_1 \ {}_{p}\dot{\sqcup}\ C_3)(x, (y, 2)) && \text{(by def. of } {}_{\mathcal{A}}\triangle\text{)}
\end{aligned}$$

□

Proposition 3.19 (Distributivity for Hidden Choice)**.**

$$C_1 \ {}_{p}\oplus\ (C_2 \ {}_{q}\oplus\ C_3) = (C_1 \ {}_{p}\oplus\ C_2) \ {}_{q}\oplus\ (C_1 \ {}_{p}\oplus\ C_3), \tag{3.31}$$

$$C_1 \ {}_{p}\oplus\ (C_2 \ {}_{\mathcal{A}}\triangle\ C_3) = (C_1 \ {}_{p}\oplus\ C_2) \ {}_{\mathcal{A}}\triangle\ (C_1 \ {}_{p}\oplus\ C_3). \tag{3.32}$$

Proof. (3.31) For all $x \in \mathcal{X}$ and $y \in \mathcal{Y}_1 \cup \mathcal{Y}_2 \cup \mathcal{Y}_3$,

$$\begin{aligned}
&(C_1 \ {}_{p}\oplus\ (C_2 \ {}_{q}\oplus\ C_3))(x, y) && \\
=&pC_1(x, y) + (1 - p)qC_2(x, y) + (1 - p)(1 - q)C_3(x, y) && \text{(by def. of } {}_{p}\oplus,\ {}_{q}\oplus\text{)} \\
=&pqC_1(x, y) + (1 - p)qC_2(x, y) && \\
&+ p(1 - q)C_1(x, y) + (1 - p)(1 - q)C_3(x, y) && \text{(rearranging)} \\
=&q(C_1 \ {}_{p}\oplus\ C_2)(x, y) + (1 - q)(C_1 \ {}_{p}\oplus\ C_3)(x, y) && \text{(by def. of } {}_{p}\oplus\text{)} \\
=&((C_1 \ {}_{p}\oplus\ C_2) \ {}_{q}\oplus\ (C_1 \ {}_{p}\oplus\ C_3))(x, y) && \text{(by def. of } {}_{q}\oplus\text{)}
\end{aligned}$$

(3.32) For all $x \in \mathcal{A}$, $y \in \mathcal{Y}_1 \cup \mathcal{Y}_2 \cup \mathcal{Y}_3$

$$\begin{aligned}
&(C_1 \ {}_{p}\oplus\ (C_2 \ {}_{\mathcal{A}}\triangle\ C_3))(x, y) && \\
=&pC_1(x, y) + (1 - p)(C_2 \ {}_{\mathcal{A}}\triangle\ C_3)(x, y) && \text{(by def. of } {}_{p}\oplus\text{)} \\
=&pC_1(x, y) + (1 - p)C_2(x, y) && \text{(by def. of } {}_{\mathcal{A}}\triangle\text{)} \\
=&(C_1 \ {}_{p}\oplus\ C_2)(x, y) && \text{(by def. of } {}_{p}\oplus\text{)} \\
=&((C_1 \ {}_{p}\oplus\ C_2) \ {}_{\mathcal{A}}\triangle\ (C_1 \ {}_{p}\oplus\ C_3))(x, y) && \text{(by def. of } {}_{\mathcal{A}}\triangle\text{)}
\end{aligned}$$

For all $x \in \bar{\mathcal{A}}$, $y \in \mathcal{Y}_1 \cup \mathcal{Y}_2 \cup \mathcal{Y}_3$

$$\begin{aligned}
&(C_1 \ {}_{p}\oplus\ (C_2 \ {}_{\mathcal{A}}\triangle\ C_3))(x, y) && \\
=&pC_1(x, y) + (1 - p)(C_2 \ {}_{\mathcal{A}}\triangle\ C_3)(x, y) && \text{(by def. of } {}_{p}\oplus\text{)}
\end{aligned}$$

$$
\begin{aligned}
&= pC_1(x,y) + (1-p)C_3(x,y) && \text{(by def. of } {}_{\mathcal{A}}⨹\text{)}\\
&= (C_1 \;{}_{p}\!\oplus\; C_3)(x,y) && \text{(by def. of } {}_{p}\!\oplus\text{)}\\
&= ((C_1 \;{}_{p}\!\oplus\; C_2) \;{}_{\mathcal{A}}⨹\; (C_1 \;{}_{p}\!\oplus\; C_3))(x,y) && \text{(by def. of } {}_{\mathcal{A}}⨹\text{)}
\end{aligned}
$$

□

Proposition 3.20 (Distributivity for Visible If-then-else).

$$
\begin{aligned}
C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \parallel C_3) &{}_{\circ}\!\sqsupseteq (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \parallel (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3), && (3.33)\\
C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \;{}_{p}\dot{\sqcup}\; C_3) &\approx (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \;{}_{p}\dot{\sqcup}\; (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3), && (3.34)\\
C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \;{}_{p}\!\oplus\; C_3) &= (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \;{}_{p}\!\oplus\; (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3), && (3.35)\\
C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \;{}_{\mathcal{B}}\!\triangle\; C_3) &{}_{\circ}\!\sqsupseteq (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \;{}_{\mathcal{B}}\!\triangle\; (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3), && (3.36)\\
C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \;{}_{\mathcal{B}}⨹\; C_3) &= (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \;{}_{\mathcal{B}}⨹\; (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3). && (3.37)
\end{aligned}
$$

Proof. (3.33) Let $D : ((\mathcal{Y}_1 \sqcup \mathcal{Y}_2) \times (\mathcal{Y}_1 \sqcup \mathcal{Y}_3)) \times (\mathcal{Y}_1 \sqcup (\mathcal{Y}_2 \times \mathcal{Y}_3)) \to [0,1]$ be a channel given by

$$
D(((y_1,i),(y_2,j)),(y',k)) = \begin{cases} 1, & \text{if } i=j=k=1 \text{ and } y'=y_1\\ 1, & \text{if } i=j=k=2 \text{ and } y'=(y_1,y_2)\\ {}^{1}\!/_{|\mathcal{Y}_1\sqcup(\mathcal{Y}_2\times\mathcal{Y}_3)|}, & \text{if } i\neq j\\ 0, & \text{otherwise} \end{cases}
$$

We claim that $C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \parallel C_3) = ((C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \parallel (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3))D$.

For all $x \in \mathcal{A}$, $(y_1, 1) \in (\mathcal{Y}_1 \sqcup (\mathcal{Y}_2 \times \mathcal{Y}_3))$,

$$
\begin{aligned}
&(((C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \parallel (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3))D)(x,(y,1))\\
&= \sum_{y_2\in\mathcal{Y}_1} ((C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \parallel (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3))(x,((y_1,1),(y_2,1))) && \text{(by mult. and def. of } D\text{)}\\
&= \sum_{y_2\in\mathcal{Y}_1} (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2)(x,(y_1,1))(C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3)(x,(y_2,1)) && \text{(by def. of } \parallel\text{)}\\
&= \sum_{y_2\in\mathcal{Y}_1} C_1(x,y_1)C_1(x,y_2) && \text{(by def. of } {}_{\mathcal{A}}\!\triangle\text{)}\\
&= C_1(x,y_1) && (C_1 \text{ is a channel})\\
&= (C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \parallel C_3))(x,(y_1,1)) && \text{(by def. of } {}_{\mathcal{A}}\!\triangle\text{)}
\end{aligned}
$$

For all $x \in \bar{\mathcal{A}}$, $((y_1, y_2), 2) \in (\mathcal{Y}_1 \sqcup (\mathcal{Y}_2 \times \mathcal{Y}_3))$,

$$\begin{aligned}
&(((C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \parallel (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3))D)(x, (y_1, y_2), 2)) \\
=&((C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \parallel (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3))(x, ((y_1, 2), (y_2, 2))) && \text{(by mult. and def. of } D\text{)} \\
=&(C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2)(x, (y_1, 2))(C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3)(x, (y_2, 2)) && \text{(by def. of } \parallel\text{)} \\
=&C_2(x, y_1)C_3(x, y_2) && \text{(by def. of } {}_{\mathcal{A}}\!\triangle\text{)} \\
=&(C_2 \parallel C_3)(x, (y_1, y_2)) && \text{(by def, of } \parallel\text{)} \\
=&(C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \parallel C_3))(x, (y_1, 1)) && \text{(by def. of } {}_{\mathcal{A}}\!\triangle\text{)}
\end{aligned}$$

For all other pairs $(x, y') \in \mathcal{X} \times (\mathcal{Y}_1 \sqcup (\mathcal{Y}_2 \times \mathcal{Y}_3))$, we have

$$(C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \parallel C_3))(x, y') = (((C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \parallel (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3))D)(x, y') = 0$$

(3.34) For all $\pi \in \mathbb{D}\mathcal{X}$ and all $g \in \mathbb{G}\mathcal{X}$,

$$\begin{aligned}
&V_g[\pi \rangle\, C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \;{}_{p}\dot{\sqcup}\; C_3)] \\
=&V_{g_{\mathcal{A}}}[\pi \rangle\, C_1] + V_{g_{\bar{\mathcal{A}}}}[\pi \rangle\, C_2 \;{}_{p}\dot{\sqcup}\; C_3] && \text{(by Theorem 4.11)} \\
=&V_{g_{\mathcal{A}}}[\pi \rangle\, C_1] + pV_{g_{\bar{\mathcal{A}}}}[\pi \rangle\, C_2] + (1-p)V_{g_{\bar{\mathcal{A}}}}[\pi \rangle\, C_3] && \text{(by Theorem 4.3)} \\
=&pV_{g_{\mathcal{A}}}[\pi \rangle\, C_1] + (1-p)V_{g_{\mathcal{A}}}[\pi \rangle\, C_1] \\
&+ pV_{g_{\bar{\mathcal{A}}}}[\pi \rangle\, C_2] + (1-p)V_{g_{\bar{\mathcal{A}}}}[\pi \rangle\, C_3] && \text{(reorganizing)} \\
=&pV_g[\pi \rangle\, C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2] + pV_g[\pi \rangle\, C_1 \;{}_{\bar{\mathcal{A}}}\!\triangle\; C_3] && \text{(by Theorem 4.11)} \\
=&pV_g[\pi \rangle\, (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \;{}_{p}\dot{\sqcup}\; (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3)] && \text{(by Theorem 4.3)}
\end{aligned}$$

(3.35) For all $x \in \mathcal{A}$, $(y, 1) \in \mathcal{Y}_1 \sqcup (\mathcal{Y}_2 \cup \mathcal{Y}_3)$,

$$\begin{aligned}
&(C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \;{}_{p}\!\oplus\; C_3))(x, (y, 1)) \\
=&C_1(x, y) && \text{(by def. of } {}_{\mathcal{A}}\!\triangle\text{)} \\
=&pC_1(x, y) + (1-p)C_1(x, y) && \text{(reorganizing)} \\
=&p(C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2)(x, (y, 1)) + (1-p)(C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3)(x, (y, 1)) && \text{(by def. of } {}_{\mathcal{A}}\!\triangle\text{)} \\
=&((C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \;{}_{p}\!\oplus\; (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3))(x, (y, 1)) && \text{(by def. of } {}_{p}\!\oplus\text{)}
\end{aligned}$$

For all $x \in \bar{\mathcal{A}}$, $(y, 2) \in \mathcal{Y}_1 \sqcup (\mathcal{Y}_2 \cup \mathcal{Y}_3)$,

$$(C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \;{}_{p}\!\oplus\; C_3))(x, (y, 2))$$

$$
\begin{aligned}
&=(C_2 \;{}_{p}\!\oplus\; C_3)(x,y) && \text{(by def. of } {}_{\mathcal{A}}\triangle\text{)}\\
&=pC_2(x,y)+(1-p)C_3(x,y) && \text{(by def. of } {}_{p}\oplus\text{)}\\
&=p(C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2)(x,(y,2))+(1-p)(C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3)(x,(y,2)) && \text{(by def. of } {}_{\mathcal{A}}\triangle\text{)}\\
&=((C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \;{}_{p}\!\oplus\; (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3))(x,(y,2)) && \text{(by def. of } {}_{p}\oplus\text{)}
\end{aligned}
$$

For all other pairs $(x,y') \in \mathcal{X} \times (\mathcal{Y}_1 \sqcup (\mathcal{Y}_2 \cup \mathcal{Y}_3))$, we have

$$(C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \;{}_{p}\!\oplus\; C_3))(x,y') = ((C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \;{}_{p}\!\oplus\; (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3))(x,y') = 0$$

(3.36) We have that, for all $\pi \in \mathbb{D}\mathcal{X}$ and $g \in \mathbb{G}\mathcal{X}$

$$
\begin{aligned}
&V_g[\pi\rangle\, C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \;{}_{\mathcal{B}}\!\triangle\; C_3)] &&\\
=&V_{g_{\mathcal{A}}}[\pi\rangle\, C_1] + V_{g_{\bar{\mathcal{A}}}}[\pi\rangle\, C_2 \;{}_{\mathcal{B}}\!\triangle\; C_3] && \text{(by Theorem 4.11)}\\
=&V_{g_{\mathcal{A}}}[\pi\rangle\, C_1] + V_{g_{\bar{\mathcal{A}}\cap\mathcal{B}}}[\pi\rangle\, C_2] + V_{g_{\bar{\mathcal{A}}\cap\bar{\mathcal{B}}}}[\pi\rangle\, C_2] && \text{(by Theorem 4.11)}\\
\leq&V_{g_{\mathcal{A}}}[\pi\rangle\, C_1 \;{}_{\mathcal{B}}\!\triangle\; C_1] + V_{g_{\bar{\mathcal{A}}\cap\mathcal{B}}}[\pi\rangle\, C_2] + V_{g_{\bar{\mathcal{A}}\cap\bar{\mathcal{B}}}}[\pi\rangle\, C_2] && \text{(by Eq. (3.14))}\\
=&V_{g_{\mathcal{A}\cap\mathcal{B}}}[\pi\rangle\, C_1] + V_{g_{\mathcal{A}\cap\bar{\mathcal{B}}}}[\pi\rangle\, C_1] &&\\
&+ V_{g_{\bar{\mathcal{A}}\cap\mathcal{B}}}[\pi\rangle\, C_2] + V_{g_{\bar{\mathcal{A}}\cap\bar{\mathcal{B}}}}[\pi\rangle\, C_2] && \text{(by Theorem 4.11)}\\
=&V_{g_{\mathcal{B}}}[\pi\rangle\, C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2] + V_{g_{\bar{\mathcal{B}}}}[\pi\rangle\, C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3] && \text{(by Theorem 4.11)}\\
=&V_g[\pi\rangle\, (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \;{}_{\mathcal{B}}\!\triangle\; (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3)] && \text{(by Theorem 4.11)}
\end{aligned}
$$

(3.37) For all $x \in \mathcal{A} \cap \mathcal{B}$, $(y,1) \in \mathcal{Y}_1 \sqcup (\mathcal{Y}_2 \cup \mathcal{Y}_3)$, we have

$$
\begin{aligned}
&(C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \;{}_{\mathcal{B}}\!\mathbin{\triangle\mkern-14mu+}\; C_3))(x,(y,1)) &&\\
=&C_1(x,y) && \text{(by def of } {}_{\mathcal{A}}\triangle\text{)}\\
=&(C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2)(x,(y,1)) && \text{(by def of } {}_{\mathcal{A}}\triangle\text{)}\\
=&((C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \;{}_{\mathcal{B}}\!\mathbin{\triangle\mkern-14mu+}\; (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3))(x,(y,1)) && \text{(by def of } {}_{\mathcal{B}}\triangle\text{)}
\end{aligned}
$$

For all $x \in \mathcal{A} \cap \bar{\mathcal{B}}$, $(y,1) \in \mathcal{Y}_1 \sqcup (\mathcal{Y}_2 \cup \mathcal{Y}_3)$, we have

$$
\begin{aligned}
&(C_1 \;{}_{\mathcal{A}}\!\triangle\; (C_2 \;{}_{\mathcal{B}}\!\mathbin{\triangle\mkern-14mu+}\; C_3))(x,(y,1)) &&\\
=&C_1(x,y) && \text{(by def of } {}_{\mathcal{A}}\triangle\text{)}\\
=&(C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3)(x,(y,1)) && \text{(by def of } {}_{\mathcal{A}}\triangle\text{)}\\
=&((C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2) \;{}_{\mathcal{B}}\!\mathbin{\triangle\mkern-14mu+}\; (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_3))(x,(y,1)) && \text{(by def of } {}_{\mathcal{B}}\triangle\text{)}
\end{aligned}
$$

For all $x \in \bar{\mathcal{A}} \cap \mathcal{B}$, $(y, 2) \in \mathcal{Y}_1 \sqcup (\mathcal{Y}_2 \cup \mathcal{Y}_3)$, we have

$$\begin{aligned}
&(C_1 \,{}_{\mathcal{A}}\!\triangle\, (C_2 \,{}_{\mathcal{B}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} C_3))(x, (y, 2)) \\
=&(C_2 \,{}_{\mathcal{B}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} C_3)(x, y) && \text{(by def. of } {}_{\mathcal{A}}\triangle\text{)} \\
=&C_2(x, y) && \text{(by def of } {}_{\mathcal{B}}\triangle \text{)} \\
=&(C_1 \,{}_{\mathcal{A}}\!\triangle\, C_2)(x, (y, 2)) && \text{(by def of } {}_{\mathcal{A}}\triangle \text{)} \\
=&((C_1 \,{}_{\mathcal{A}}\!\triangle\, C_2) \,{}_{\mathcal{B}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} (C_1 \,{}_{\mathcal{A}}\!\triangle\, C_3))(x, (y, 1)) && \text{(by def of } {}_{\mathcal{B}}\triangle \text{)}
\end{aligned}$$

For all $x \in \bar{\mathcal{A}} \cap \bar{\mathcal{B}}$, $(y, 2) \in \mathcal{Y}_1 \sqcup \mathcal{Y}_2 \cup \mathcal{Y}_3$, we have

$$\begin{aligned}
&(C_1 \,{}_{\mathcal{A}}\!\triangle\, (C_2 \,{}_{\mathcal{B}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} C_3))(x, (y, 2)) \\
=&(C_2 \,{}_{\mathcal{B}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} C_3)(x, y) && \text{(by def. of } {}_{\mathcal{A}}\triangle\text{)} \\
=&C_3(x, y) && \text{(by def of } {}_{\mathcal{B}}\triangle \text{)} \\
=&(C_1 \,{}_{\mathcal{A}}\!\triangle\, C_3)(x, (y, 2)) && \text{(by def of } {}_{\mathcal{A}}\triangle \text{)} \\
=&((C_1 \,{}_{\mathcal{A}}\!\triangle\, C_2) \,{}_{\mathcal{B}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} (C_1 \,{}_{\mathcal{A}}\!\triangle\, C_3))(x, (y, 1)) && \text{(by def of } {}_{\mathcal{B}}\triangle \text{)}
\end{aligned}$$

For all other pairs $(x, y') \in \mathcal{X} \times (\mathcal{Y}_1 \sqcup (\mathcal{Y}_2 \cup \mathcal{Y}_3))$, we have

$$(C_1 \,{}_{\mathcal{A}}\!\triangle\, (C_2 \,{}_{\mathcal{B}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} C_3))(x, y') = ((C_1 \,{}_{\mathcal{A}}\!\triangle\, C_2) \,{}_{\mathcal{B}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} (C_1 \,{}_{\mathcal{A}}\!\triangle\, C_3))(x, y') = 0$$

□

Proposition 3.21 (Distributivity for Hidden If-then-else)**.**

$$C_1 \,{}_{\mathcal{A}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} (C_2 \,{}_{p}\!\oplus C_3) = (C_1 \,{}_{\mathcal{A}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} C_2) \,{}_{p}\!\oplus (C_1 \,{}_{\mathcal{A}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} C_3), \tag{3.38}$$

$$C_1 \,{}_{\mathcal{A}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} (C_2 \,{}_{\mathcal{B}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} C_3) = (C_1 \,{}_{\mathcal{A}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} C_2) \,{}_{\mathcal{B}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} (C_1 \,{}_{\mathcal{A}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} C_3). \tag{3.39}$$

Proof. (3.39) For all $x \in \mathcal{A}$, $y \in \mathcal{Y}_1 \cup \mathcal{Y}_2 \cup \mathcal{Y}_3$,

$$\begin{aligned}
&(C_1 \,{}_{\mathcal{A}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} (C_2 \,{}_{p}\!\oplus C_3))(x, y) \\
=&C_1(x, y) && \text{(by def. of } {}_{\mathcal{A}}\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu}\text{)} \\
=&pC_1(x, y) + (1 - p)C_1(x, y) && \text{(reorganizing)} \\
=&p(C_1 \,{}_{\mathcal{A}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} C_2)(x, y) + (1 - p)(C_1 \,{}_{\mathcal{A}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} C_3)(x, y) && \text{(by def. of } {}_{\mathcal{A}}\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu}\text{)} \\
=&((C_1 \,{}_{\mathcal{A}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} C_2) \,{}_{p}\!\oplus (C_1 \,{}_{\mathcal{A}}\!\mathbin{\triangle\mkern-15mu{\scriptstyle+}\mkern3mu} C_3))(x, y) && \text{(by def. of } {}_{p}\oplus\text{)}
\end{aligned}$$

For all $x \in \bar{\mathcal{A}}$, $y \in \mathcal{Y}_1 \cup \mathcal{Y}_2 \cup \mathcal{Y}_3$,

$$\begin{aligned}
&(C_1 \ {}_{\mathcal{A}}\triangle \ (C_2 \ {}_{p}\oplus \ C_3))(x,y) && \\
=&(C_2 \ {}_{p}\oplus \ C_3))(x,y) && \text{(by def. of } {}_{\mathcal{A}}\triangle) \\
=&pC_2(x,y) + (1-p)C_3(x,y) && \text{(by def. of } {}_{p}\oplus) \\
=&p(C_1 \ {}_{\mathcal{A}}\triangle \ C_2)(x,y) + (1-p)(C_1 \ {}_{\mathcal{A}}\triangle \ C_3)(x,y) && \text{(by def. of } {}_{\mathcal{A}}\triangle) \\
=&((C_1 \ {}_{\mathcal{A}}\triangle \ C_2) \ {}_{p}\oplus \ (C_1 \ {}_{\mathcal{A}}\triangle \ C_3))(x,y) && \text{(by def. of } {}_{p}\oplus)
\end{aligned}$$

(3.39) For all $x \in \mathcal{A} \cap \mathcal{B}$, $y \in \mathcal{Y}_1 \cup \mathcal{Y}_2 \cup \mathcal{Y}_3$,

$$\begin{aligned}
&(C_1 \ {}_{\mathcal{A}}\triangle \ (C_2 \ {}_{\mathcal{B}}\triangle \ C_3))(x,y) && \\
=&C_1(x,y) && \text{(by def. of } {}_{\mathcal{A}}\triangle) \\
=&(C_1 \ {}_{\mathcal{A}}\triangle \ C_2)(x,y) && \text{(by def. of } {}_{\mathcal{A}}\triangle) \\
=&((C_1 \ {}_{\mathcal{A}}\triangle \ C_2) \ {}_{\mathcal{B}}\triangle \ (C_1 \ {}_{\mathcal{A}}\triangle \ C_3))(x,y) && \text{(by def. of } {}_{\mathcal{B}}\triangle)
\end{aligned}$$

For all $x \in \mathcal{A} \cap \bar{\mathcal{B}}$, $y \in \mathcal{Y}_1 \cup \mathcal{Y}_2 \cup \mathcal{Y}_3$,

$$\begin{aligned}
&(C_1 \ {}_{\mathcal{A}}\triangle \ (C_2 \ {}_{\mathcal{B}}\triangle \ C_3))(x,y) && \\
=&C_1(x,y) && \text{(by def. of } {}_{\mathcal{A}}\triangle) \\
=&(C_1 \ {}_{\mathcal{A}}\triangle \ C_3)(x,y) && \text{(by def. of } {}_{\mathcal{A}}\triangle) \\
=&((C_1 \ {}_{\mathcal{A}}\triangle \ C_2) \ {}_{\mathcal{B}}\triangle \ (C_1 \ {}_{\mathcal{A}}\triangle \ C_3))(x,y) && \text{(by def. of } {}_{\mathcal{B}}\triangle)
\end{aligned}$$

For all $x \in \bar{\mathcal{A}} \cap \mathcal{B}$, $y \in \mathcal{Y}_1 \cup \mathcal{Y}_2 \cup \mathcal{Y}_3$,

$$\begin{aligned}
&(C_1 \ {}_{\mathcal{A}}\triangle \ (C_2 \ {}_{\mathcal{B}}\triangle \ C_3))(x,y) && \\
=&(C_2 \ {}_{\mathcal{B}}\triangle \ C_3))(x,y) && \text{(by def. of } {}_{\mathcal{A}}\triangle) \\
=&C_2(x,y) && \text{(by def. of } {}_{\mathcal{B}}\triangle) \\
=&(C_1 \ {}_{\mathcal{A}}\triangle \ C_2)(x,y) && \text{(by def. of } {}_{\mathcal{A}}\triangle) \\
=&((C_1 \ {}_{\mathcal{A}}\triangle \ C_2) \ {}_{\mathcal{B}}\triangle \ (C_1 \ {}_{\mathcal{A}}\triangle \ C_3))(x,y) && \text{(by def. of } {}_{\mathcal{B}}\triangle)
\end{aligned}$$

For all $x \in \bar{\mathcal{A}} \cap \bar{\mathcal{B}}$, $y \in \mathcal{Y}_1 \cup \mathcal{Y}_2 \cup \mathcal{Y}_3$,

$$\begin{aligned}
&(C_1 \ {}_{\mathcal{A}}\triangle \ (C_2 \ {}_{\mathcal{B}}\triangle \ C_3))(x,y) && \\
=&(C_2 \ {}_{\mathcal{B}}\triangle \ C_3))(x,y) && \text{(by def. of } {}_{\mathcal{A}}\triangle) \\
=&C_3(x,y) && \text{(by def. of } {}_{\mathcal{B}}\triangle)
\end{aligned}$$

$$
\begin{aligned}
&=(C_1 \ {}_{\mathcal{A}}\text{⟁}\ C_3)(x,y) && \text{(by def. of } {}_{\mathcal{A}}\text{⟁)}\\
&=((C_1 \ {}_{\mathcal{A}}\text{⟁}\ C_2) \ {}_{\mathcal{B}}\text{⟁}\ (C_1 \ {}_{\mathcal{A}}\text{⟁}\ C_3))(x,y) && \text{(by def. of } {}_{\mathcal{B}}\text{⟁)}
\end{aligned}
$$

□

Proposition 3.22 (Non-distributivity)**.** *The following expressions do not, in general, respect the refinement relation between them, in any direction*

$$(C_1 \ {}_{p}\dot\sqcup\ (C_2 \parallel C_3)) \ \textit{and}\ ((C_1 \ {}_{p}\dot\sqcup\ C_2) \parallel (C_1 \ {}_{p}\dot\sqcup\ C_3)), \tag{3.40}$$

$$(C_1 \ {}_{p}\oplus\ (C_2 \parallel C_3)) \ \textit{and}\ ((C_1 \ {}_{p}\oplus\ C_2) \parallel (C_1 \ {}_{p}\oplus\ C_3)), \tag{3.41}$$

$$(C_1 \ {}_{p}\oplus\ (C_2 \ {}_{q}\dot\sqcup\ C_3)) \ \textit{and}\ ((C_1 \ {}_{p}\oplus\ C_2) \ {}_{q}\dot\sqcup\ (C_1 \ {}_{p}\oplus\ C_3)), \tag{3.42}$$

$$(C_1 \ {}_{p}\oplus\ (C_2 \ {}_{\mathcal{A}}\triangle\ C_3)) \ \textit{and}\ ((C_1 \ {}_{p}\oplus\ C_2) \ {}_{\mathcal{A}}\triangle\ (C_1 \ {}_{p}\oplus\ C_3)), \tag{3.43}$$

$$(C_1 \ {}_{\mathcal{A}}\text{⟁}\ (C_2 \parallel C_3)) \ \textit{and}\ ((C_1 \ {}_{\mathcal{A}}\text{⟁}\ C_2) \parallel (C_1 \ {}_{\mathcal{A}}\text{⟁}\ C_3)), \tag{3.44}$$

$$(C_1 \ {}_{\mathcal{A}}\text{⟁}\ (C_2 \ {}_{p}\dot\sqcup\ C_3)) \ \textit{and}\ ((C_1 \ {}_{\mathcal{A}}\text{⟁}\ C_2) \ {}_{p}\dot\sqcup\ (C_1 \ {}_{\mathcal{A}}\text{⟁}\ C_3)), \tag{3.45}$$

$$(C_1 \ {}_{\mathcal{A}}\text{⟁}\ (C_2 \ {}_{\mathcal{B}}\triangle\ C_3)) \ \textit{and}\ ((C_1 \ {}_{\mathcal{A}}\text{⟁}\ C_2) \ {}_{\mathcal{B}}\triangle\ (C_1 \ {}_{\mathcal{A}}\text{⟁}\ C_3)). \tag{3.46}$$

Proof. (3.40) Let the following be three compatible channels from the set $\mathcal{C}_{\mathcal{X}}$

C_1	y_1
x_1	1
x_2	1
x_3	1

C_2	y_1	y_2
x_1	1	0
x_2	1	0
x_3	0	1

C_3	y_1	y_2
x_1	1	0
x_2	0	1
x_3	0	1

Then, we have (the output labels were omitted for brevity)

$C_1 \ {}_{1/2}\dot\sqcup\ (C_2 \parallel C_3)$					
x_1	$1/2$	$1/2$	0	0	0
x_2	$1/2$	0	$1/2$	0	0
x_3	$1/2$	0	0	0	$1/2$

$(C_1 \ {}_{1/2}\dot\sqcup\ C_2) \parallel (C_1 \ {}_{1/2}\dot\sqcup\ C_3)$									
x_1	$1/4$	$1/4$	0	$1/4$	$1/4$	0	0	0	0
x_2	$1/4$	0	$1/4$	$1/4$	0	$1/4$	0	0	0
x_3	$1/4$	0	$1/4$	0	0	0	$1/4$	0	$1/4$

Let $g_{id} \in \mathbb{G}\mathcal{X}$ be as in Definition 2.10 and $\pi = (1/2, 0, 1/2)$. Then, $V_{g_{id}}[\pi \rangle C_1 \ {}_{1/2}\dot\sqcup\ (C_2 \parallel C_3)] = 3/4$, while $V_{g_{id}}[\pi \rangle (C_1 \ {}_{1/2}\dot\sqcup\ C_2) \parallel (C_1 \ {}_{1/2}\dot\sqcup\ C_3)] = 7/8$.

Therefore,

$$C_1 \;{}_{1/2}\dot{\sqcup}\; (C_2 \parallel C_3) \not\sqsubseteq_{\circ} (C_1 \;{}_{1/2}\dot{\sqcup}\; C_2) \parallel (C_1 \;{}_{1/2}\dot{\sqcup}\; C_3)$$

Conversely, we see that there is a column of the matrix representation of $C_1 \;{}_{1/2}\dot{\sqcup}\; (C_2 \parallel C_3)$ given by $(0, 1/2, 0)$. It can be easily checked that this column can not be described as a linear combination of the columns of $(C_1 \;{}_{1/2}\dot{\sqcup}\; C_2) \parallel (C_1 \;{}_{1/2}\dot{\sqcup}\; C_3)$ with coefficients in the range [0,1]. Therefore, there is no channel D such that

$$((C_1 \;{}_{1/2}\dot{\sqcup}\; C_2) \parallel (C_1 \;{}_{1/2}\dot{\sqcup}\; C_3))D = C_1 \;{}_{1/2}\dot{\sqcup}\; (C_2 \parallel C_3).$$

From here on, all the remaining proofs of this proposition will be based on the following idea. If there is a choice of C_1, C_2 and C_3 that make the first channel null and the second transparent and another choice of C_1, C_2 and C_3 that makes the second channel null and the first transparent, the inexistence of a refinement relation that holds in general is proved

(3.41) Let

C_1	y_1	y_2
x_1	1	0
x_2	0	1

C_2	y_1	y_2
x_1	0	1
x_2	1	0

C_3	y_1	y_2
x_1	0	1
x_2	1	0

C_4	(y_1, y_1)	(y_2, y_2)
x_1	1	0
x_2	0	1

We have that $(C_1 \;{}_{1/2}\oplus\; (C_2 \parallel C_3))$ is a transparent channel and $((C_1 \;{}_{1/2}\oplus\; C_2) \parallel (C_1 \;{}_{1/2}\oplus\; C_3))$ is a null channel, while $(C_4 \;{}_{1/2}\oplus\; (C_2 \parallel C_3))$ is a null channel and $((C_4 \;{}_{1/2}\oplus\; C_2) \parallel (C_4 \;{}_{1/2}\oplus\; C_3))$ is a transparent channel.

(3.42) Let

C_1	y_1	y_2
x_1	1	0
x_2	0	1

C_2	y_1	y_2
x_1	0	1
x_2	1	0

C_3	y_1	y_2
x_1	0	1
x_2	1	0

C_4	$(y_1, 1)$	$(y_2, 1)$	$(y_1, 2)$	$(y_2, 2)$
x_1	$1/2$	0	$1/2$	0
x_2	0	$1/2$	0	$1/2$

Then, $(C_1 \;{}_{1/2}\oplus\; (C_2 \;{}_{1/2}\dot{\sqcup}\; C_3))$ is a transparent channel and $((C_1 \;{}_{1/2}\oplus\; C_2) \;{}_{1/2}\dot{\sqcup}\; (C_1 \;{}_{1/2}\oplus\; C_3))$ is a null channel, while $(C_4 \;{}_{1/2}\oplus\; (C_2 \;{}_{1/2}\dot{\sqcup}\; C_3))$ is a null channel and $((C_4 \;{}_{1/2}\oplus\; C_2) \;{}_{1/2}\dot{\sqcup}\; (C_4 \;{}_{1/2}\oplus\; C_3))$ is a transparent channel.

(3.43) Let

C_1	y_1	y_2
x_1	1	0
x_2	0	1

C_2	y_1	y_2
x_1	0	1
x_2	1	0

C_3	y_1	y_2
x_1	0	1
x_2	1	0

C_4	$(y_2, 1)$	$(y_1, 2)$
x_1	0	1
x_2	1	0

Let $\mathcal{A} = \{x_1\}$. Then, $(C_1 \;{}_{1/2}{\oplus}\; (C_2 \;{}_{\mathcal{A}}{\triangle}\; C_3))$ is a transparent channel and $((C_1 \;{}_{1/2}{\oplus}\; C_2) \;{}_{\mathcal{A}}{\triangle}\; (C_1 \;{}_{1/2}{\oplus}\; C_3))$ is a null channel, while $(C_4 \;{}_{1/2}{\oplus}\; (C_2 \;{}_{\mathcal{A}}{\triangle}\; C_3))$ is a null channel and $((C_4 \;{}_{1/2}{\oplus}\; C_2) \;{}_{\mathcal{A}}{\triangle}\; (C_4 \;{}_{1/2}{\oplus}\; C_3))$ is a transparent channel.

(3.44) Let

C_1	y_1	y_2
x_1	1	0
x_2	0	1

C_2	y_1	y_2
x_1	0	1
x_2	1	0

C_3	y_1	y_2
x_1	0	1
x_2	1	0

C_4	(y_1, y_1)	(y_2, y_2)
x_1	1	0
x_2	0	1

Let $\mathcal{A} = \{x_1\}$. Then, $(C_1 \;{}_{\mathcal{A}}{⟁}\; (C_2 \parallel C_3))$ is a transparent channel and $((C_1 \;{}_{\mathcal{A}}{⟁}\; C_2) \parallel (C_1 \;{}_{\mathcal{A}}{⟁}\; C_3))$ is a null channel, while $(C_4 \;{}_{\mathcal{A}}{⟁}\; (C_2 \parallel C_3))$ is a null channel and $((C_4 \;{}_{\mathcal{A}}{⟁}\; C_2) \parallel (C_4 \;{}_{\mathcal{A}}{⟁}\; C_3))$ is a transparent channel

(3.45) Let

C_1	y_1	y_2
x_1	1	0
x_2	0	1

C_2	y_1	y_2
x_1	0	1
x_2	1	0

C_3	y_1	y_2
x_1	0	1
x_2	1	0

C_4	$(y_1, 1)$	$(y_1, 2)$
x_1	$1/2$	$1/2$
x_2	$1/2$	$1/2$

Let $\mathcal{A} = \{x_1\}$. Then, $(C_1 \;{}_{\mathcal{A}}{⟁}\; (C_2 \;{}_{1/2}{\dot\sqcup}\; C_3))$ is a transparent channel and $((C_1 \;{}_{\mathcal{A}}{⟁}\; C_2) \;{}_{1/2}{\dot\sqcup}\; (C_1 \;{}_{\mathcal{A}}{⟁}\; C_3))$ is a null channel, while $(C_4 \;{}_{\mathcal{A}}{⟁}\; (C_2 \;{}_{1/2}{\dot\sqcup}\; C_3))$ is a null channel and $((C_4 \;{}_{\mathcal{A}}{⟁}\; C_2) \;{}_{1/2}{\dot\sqcup}\; (C_4 \;{}_{\mathcal{A}}{⟁}\; C_3))$ is a transparent channel

(3.46) Let

C_1	y_1	y_2
x_1	1	0
x_2	0	1

C_2	y_1	y_2
x_1	0	1
x_2	1	0

C_3	y_1	y_2
x_1	0	1
x_2	1	0

C_4	$(y_2, 1)$	$(y_1, 2)$
x_1	0	1
x_2	1	0

Let $\mathcal{A} = \mathcal{B} = \{x_1\}$. Then, $(C_1 \;{}_{\mathcal{A}}{⟁}\; (C_2 \;{}_{\mathcal{B}}{\triangle}\; C_3))$ is a transparent channel and $((C_1 \;{}_{\mathcal{A}}{⟁}\; C_2) \;{}_{\mathcal{B}}{\triangle}\; (C_1 \;{}_{\mathcal{A}}{⟁}\; C_3))$ is a null channel, while $(C_4 \;{}_{\mathcal{A}}{⟁}\; (C_2 \;{}_{\mathcal{B}}{\triangle}\; C_3))$ is a null channel and $((C_4 \;{}_{\mathcal{A}}{⟁}\; C_2) \;{}_{\mathcal{B}}{\triangle}\; (C_4 \;{}_{\mathcal{A}}{⟁}\; C_3))$ is a transparent channel. □

A.4 Properties regarding cascading

Proposition 3.23. *Let* $D_1 \in \mathcal{C}_{\mathcal{Y}_1}^{\mathcal{Z}_1}$, $D_2 \in \mathcal{C}_{\mathcal{Y}_2}^{\mathcal{Z}_2}$ *be channels. Then,*

$$(C_1 D_1) \parallel (C_2 D_2) = (C_1 \parallel C_2) D^{\parallel},$$

where $D^{\|} : (\mathcal{Y}_1{\times}\mathcal{Y}_2){\times}(\mathcal{Z}_1{\times}\mathcal{Z}_2) \to [0,1]$ *is defined as*

$$D^{\|}((y_1,y_2),(z_1,z_2)) = D_1(y_1,z_1)D_2(y_2,z_2)$$

for all $y_1{\in}\mathcal{Y}_1$*,* $y_2{\in}\mathcal{Y}_2$*,* $z_1{\in}\mathcal{Z}_1$*, and* $z_2{\in}\mathcal{Z}_2$*.*

Proof. For all $x \in \mathcal{X}$, $z_1 \in \mathcal{Z}_1$ and $z_2 \in \mathcal{Z}_2$,

$$\begin{aligned}
&((C_1D_1) \parallel (C_2D_2))(x,(z_1,z_2)) \\
=&(C_1D_1)(x,z_1)(C_2D_2)(x,z_2) && \text{(by def. of } \|\text{)} \\
=&\left(\sum_{y_1\in\mathcal{Y}_1} C_1(x,y_1)D_1(y_1,z_1)\right)\left(\sum_{y_2\in\mathcal{Y}_2} C_2(x,y_2)D_2(y_2,z_2)\right) && \text{(by matrix mult.)} \\
=&\sum_{y_1\in\mathcal{Y}_1}\sum_{y_2\in\mathcal{Y}_2} C_1(x,y_1)C_2(x,y_2)D_1(y_1,z_1)D_2(y_2,z_2) && \text{(rearranging)} \\
=&\sum_{y_1\in\mathcal{Y}_1}\sum_{y_2\in\mathcal{Y}_2} (C_1 \parallel C_2)(x,(y_1,y_2))D^{\|}((y_1,y_2),(z_1,z_2)) && \text{(by def. of } \|,\ D^{\|}\text{)} \\
=&((C_1 \parallel C_2)D^{\|})(x,(z_1,z_2)) && \text{(by matrix mult.)}
\end{aligned}$$

□

Proposition 3.24. *Let* $D_1 \in \mathcal{C}_{\mathcal{Y}_1}^{\mathcal{Z}_1}$*,* $D_2 \in \mathcal{C}_{\mathcal{Y}_2}^{\mathcal{Z}_2}$ *be channels. Then,*

$$(C_1D_1)\ {}_p{\sqcup}\ (C_2D_2) = (C_1\ {}_p{\sqcup}\ C_2)D^{\sqcup},$$

where $D^{\sqcup}{:}(\mathcal{Y}_1{\sqcup}\mathcal{Y}_2){\times}(\mathcal{Z}_1{\sqcup}\mathcal{Z}_2){\to}[0,1]$ *is defined as*

$$D^{\sqcup}((y,i),(z,j)) = \begin{cases} D_1(y,z), & \textit{if } i=j=1, \\ D_2(y,z), & \textit{if } i=j=2, \\ 0, & \textit{otherwise.} \end{cases}$$

for all $y_1{\in}\mathcal{Y}_1$*,* $y_2{\in}\mathcal{Y}_2$*,* $z_1{\in}\mathcal{Z}_1$*,* $z_2{\in}\mathcal{Z}_2$*.*

Proof. For all $x \in \mathcal{X}$ and $(z,1) \in \mathcal{Z}_1 \sqcup \mathcal{Z}_2$,

$$\begin{aligned}
&((C_1D_1)\ {}_p{\sqcup}\ (C_2D_2))(x,(z,1)) \\
=&p(C_1D_1)(x,z) && \text{(by def. of } {}_p{\sqcup}\text{)} \\
=&p\sum_{y\in\mathcal{Y}_1} C_1(x,y)D_1(y,z) && \text{(by matrix mult.)}
\end{aligned}$$

$$\begin{aligned}
&= \sum_{y \in \mathcal{Y}_1} (pC_1(x,y))D_1(y,z) && \text{(by matrix mult.)} \\
&= \sum_{y \in \mathcal{Y}_1} (C_1 \ {}_p\sqcup \ C_2)(x,(y,1))D_1(y,z) && \text{(by def. of } {}_p\sqcup\text{)} \\
&= \sum_{y \in \mathcal{Y}_1} (C_1 \ {}_p\sqcup \ C_2)(x,(y,1))D^{\sqcup}((y,1),(z,1)) && \text{(by def. of } D^{\sqcup}\text{)} \\
&= \sum_{(y,i) \in \mathcal{Y}_1 \sqcup \mathcal{Y}_2} (C_1 \ {}_p\sqcup \ C_2)(x,(y,i))D^{\sqcup}((y_i,i),(z,1)) && (D^{\sqcup}((y,i),(z,1)) = 0 \text{ when } i \neq 1) \\
&= ((C_1 \ {}_p\sqcup \ C_2)D^{\sqcup})(x,(z,1)) && \text{(by matrix mult.)}
\end{aligned}$$

Similarly, for all $x \in \mathcal{X}$ and $(z,2) \in \mathcal{Z}_1 \sqcup \mathcal{Z}_2$,

$$\begin{aligned}
& ((C_1D_1) \ {}_p\sqcup \ (C_2D_2))(x,(z,2)) \\
&= (1-p)(C_2D_2)(x,z) && \text{(by def. of } {}_p\sqcup\text{)} \\
&= (1-p) \sum_{y \in \mathcal{Y}_2} C_2(x,y)D_2(y,z) && \text{(by matrix mult.)} \\
&= \sum_{y \in \mathcal{Y}_2} ((1-p)C_2(x,y))D_2(y,z) && \text{(by matrix mult.)} \\
&= \sum_{y \in \mathcal{Y}_2} (C_1 \ {}_p\sqcup \ C_2)(x,(y,2))D_2(y,z) && \text{(by def. of } {}_p\sqcup\text{)} \\
&= \sum_{y \in \mathcal{Y}_2} (C_1 \ {}_p\sqcup \ C_2)(x,(y,2))D^{\sqcup}((y,2),(z,2)) && \text{(by def. of } D^{\sqcup}\text{)} \\
&= \sum_{(y,i) \in \mathcal{Y}_1 \sqcup \mathcal{Y}_2} (C_1 \ {}_p\sqcup \ C_2)(x,(y,i))D^{\sqcup}((y_i,i),(z,2)) && (D^{\sqcup}((y,i),(z,2)) = 0 \text{ when } i \neq 2) \\
&= ((C_1 \ {}_p\sqcup \ C_2)D^{\sqcup})(x,(z,2)) && \text{(by matrix mult.)}
\end{aligned}$$

□

Proposition 3.25. *Let $D_1 \in \mathcal{C}_{\mathcal{Y}_1}^{\mathcal{Z}_1}$, $D_2 \in \mathcal{C}_{\mathcal{Y}_2}^{\mathcal{Z}_2}$ be channels. Then,*

$$(C_1D_1) \ {}_{\mathcal{A}}\triangle \ (C_2D_2) = (C_1 \ {}_{\mathcal{A}}\triangle \ C_2)D^{\sqcup},$$

where $D^{\sqcup}$ is as defined in Proposition 3.24.

Proof. For all $x \in \mathcal{A}$ and $(z,1) \in \mathcal{Z}_1 \sqcup \mathcal{Z}_2$,

$$\begin{aligned}
& ((C_1D_1) \ {}_{\mathcal{A}}\triangle \ (C_2D_2))(x,(z,1)) \\
&= (C_1D_1)(x,z) && \text{(by def. of } {}_{\mathcal{A}}\triangle\text{)} \\
&= \sum_{y \in \mathcal{Y}_1} C_1(x,y)D_1(y,z) && \text{(by matrix mult.)}
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{y \in \mathcal{Y}_1} (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2)(x,(y,1))D_1(y,z) && \text{(by def. of } {}_{\mathcal{A}}\!\triangle\text{)}\\
&= \sum_{y \in \mathcal{Y}_1} (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2)(x,(y,1))D^{\sqcup}((y,1),(z,1)) && \text{(by def. of } D^{\sqcup}\text{)}\\
&= \sum_{(y,i) \in \mathcal{Y}_1 \sqcup \mathcal{Y}_2} (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2)(x,(y,i))D^{\sqcup}((y,i),(z,1)) && (D^{\sqcup}((y,i),(z,1)) = 0 \text{ when } i \neq 1)\\
&=((C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2)D^{\sqcup})(x,(z,1)) && \text{(by matrix mult.)}
\end{aligned}
$$

Similarly, for all $x \in \bar{\mathcal{A}}$ and $(z,2) \in \mathcal{Z}_1 \sqcup \mathcal{Z}_2$,

$$
\begin{aligned}
&((C_1D_1) \;{}_{\mathcal{A}}\!\triangle\; (C_2D_2))(x,(z,2))\\
&=(C_2D_2)(x,z) && \text{(by def. of } {}_{\mathcal{A}}\!\triangle\text{)}\\
&= \sum_{y \in \mathcal{Y}_2} C_2(x,y)D_2(y,z) && \text{(by matrix mult.)}\\
&= \sum_{y \in \mathcal{Y}_2} (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2)(x,(y,2))D_2(y,z) && \text{(by def. of } {}_{\mathcal{A}}\!\triangle\text{)}\\
&= \sum_{y \in \mathcal{Y}_2} (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2)(x,(y,2))D^{\sqcup}((y,2),(z,2)) && \text{(by def. of } D^{\sqcup}\text{)}\\
&= \sum_{(y,i) \in \mathcal{Y}_1 \sqcup \mathcal{Y}_2} (C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2)(x,(y,i))D^{\sqcup}((y,i),(z,2)) && (D^{\sqcup}((y,i),(z,2)) = 0 \text{ when } i \neq 2)\\
&=((C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2)D^{\sqcup})(x,(z,2)) && \text{(by matrix mult.)}
\end{aligned}
$$

For all pairs $x \in \mathcal{X}$, $(z,i) \in \mathcal{Z}_1 \sqcup \mathcal{Z}_2$ not contemplated above, we have

$$((C_1D_1) \;{}_{\mathcal{A}}\!\triangle\; (C_2D_2))(x,(z,i)) = (((C_1 \;{}_{\mathcal{A}}\!\triangle\; C_2)D^{\sqcup})(x,(z,i)) = 0$$

□

Proposition 3.26. *Let $C_1, C_2 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ be channels of the same type, let $D \in \mathcal{C}_{\mathcal{Y}}^{\mathcal{Z}}$ and let $p \in [0,1]$. Then, $(C_1D) \;{}_p\!\oplus\; (C_2D) = (C_1 \;{}_p\!\oplus\; C_2)D$.*

Proof. For all $x \in \mathcal{X}$ and $z \in \mathcal{Z}$,

$$
\begin{aligned}
&((C_1D) \;{}_p\!\oplus\; (C_2D))(x,z)\\
&=p(C_1D)(x,z) + (1-p)(C_2D)(x,z) && \text{(by def. of } {}_p\!\oplus\text{)}\\
&=p\sum_{y \in \mathcal{Y}} C_1(x,y)D(y,z) + (1-p)\sum_{y \in \mathcal{Y}} C_2(x,y)D(y,z) && \text{(by matrix mult.)}\\
&= \sum_{y \in \mathcal{Y}} (pC_1(x,y) + (1-p)C_2(x,y))D(y,z) && \text{(rearranging)}
\end{aligned}
$$

$$
\begin{aligned}
=&\sum_{y\in\mathcal{Y}}(C_1 \,{}_p\!\oplus C_2)(x,y)D(y,z) && \text{(by def. of } {}_p\!\oplus\text{)}\\
=&((C_1 \,{}_p\!\oplus C_2)D)(x,z) && \text{(by matrix mult.)}
\end{aligned}
$$

□

Proposition 3.27. *Let $C_1, C_2 \in \mathcal{C}_{\mathcal{X}}^{\mathcal{Y}}$ be channels of the same type, let $D \in \mathcal{C}_{\mathcal{Y}}^{\mathcal{Z}}$ and let $\mathcal{A} \subset \mathcal{X}$. Then, $(C_1D) \,{}_{\mathcal{A}}\!\triangle\, (C_2D) = (C_1 \,{}_{\mathcal{A}}\!\triangle\, C_2)D$.*

Proof. For all $x \in \mathcal{A}$ and $z \in \mathcal{Z}$,

$$
\begin{aligned}
&((C_1D) \,{}_{\mathcal{A}}\!\triangle\, (C_2D))(x,z)\\
=&(C_1D)(x,z) && \text{(by def. of } {}_{\mathcal{A}}\!\triangle\text{)}\\
=&\sum_{y\in\mathcal{Y}}C_1(x,y)D(y,z) && \text{(by matrix mult.)}\\
=&\sum_{y\in\mathcal{Y}}(C_1 \,{}_{\mathcal{A}}\!\triangle\, C_2)(x,y)D(y,z) && \text{(by def. of } {}_{\mathcal{A}}\!\triangle\text{)}\\
=&((C_1 \,{}_{\mathcal{A}}\!\triangle\, C_2)D)(x,z) && \text{(by matrix mult.)}
\end{aligned}
$$

Similarly, for all $x \in \bar{\mathcal{A}}$ and $z \in \mathcal{Z}$,

$$
\begin{aligned}
&((C_1D) \,{}_{\mathcal{A}}\!\triangle\, (C_2D))(x,z)\\
=&(C_2D)(x,z) && \text{(by def. of } {}_{\mathcal{A}}\!\triangle\text{)}\\
=&\sum_{y\in\mathcal{Y}}C_2(x,y)D(y,z) && \text{(by matrix mult.)}\\
=&\sum_{y\in\mathcal{Y}}(C_1 \,{}_{\mathcal{A}}\!\triangle\, C_2)(x,y)D(y,z) && \text{(by def. of } {}_{\mathcal{A}}\!\triangle\text{)}\\
=&((C_1 \,{}_{\mathcal{A}}\!\triangle\, C_2)D)(x,z) && \text{(by matrix mult.)}
\end{aligned}
$$

□