A New Architecture for Choreographic Programming Languages

A Dissertation Proposed

by

Mako Bates

to

The Faculty of the Graduate College

of

The University of Vermont

In Partial Fullfillment of the Requirements
for the Degree of Doctor of Philosophy
Specializing in Computer Science

August, 2025

Accepted by the Faculty of the Graduate College, The University of Vermont, in partial fulfillment of the requirements for the degree of Doctor of Philosophy, specializing in Computer Science.

Dissertation Examination Committee:

Joseph P. Near, Ph.D. — Advisor

Christian Skalka, Ph.D.

Yuanyuan Feng, Ph.D.

Andrew K. Hirsch, Ph.D.

Alice Patania, Ph.D. — Chairperson

Holger Hoock, Ph.D. — Dean, Graduate College

Date: June XX, 2025

Abstract

Choreographic programming (CP) is a paradigm for implementing distributed systems that uses a single global program to define the actions and interactions of all participants. Library-level CP implementations, which enable choreographic programming in mainstream programming languages, can facilitate real-world use of CP, but existing implementations like HasChor have limitations: Their conditionals require extra communication, and they lack support for programming patterns that are essential for implementing realistic distributed applications.

We make three contributions to library-level CP to specifically address these challenges. First, we propose and formalize *enclaves* and *multiply-located values*, which enable efficient conditionals in library-level CP without redundant communication. Second, we implement this "enclaves-&-MLVs" paradigm in Haskell as the MultiChor library. MultiChor is available to end-users now, and contains solutions to key engineering problems. Third, we propose *census polymorphism*, a technique for abstracting over the number of participants in a choreography.

CITATIONS

Material from this proposal has been submitted for publication in *PLDI* on 06/16/2025 in the following form:

Mako Bates and Shun Kashiwa and Syed Jafri and Gan Shen and Lindsey Kuper and Joseph P. Near. (2025). Efficient, Portable, Census-Polymorphic Choreographic Programming. *PLDI25*.

(*NB:* This will still be in a state of uncertainty when I defend the proposal. Specifically, we will have responded to the first round of reviews and be awaiting subsequent decision.)

Material from this proposal was presented to the choreographic programming research committee on 06/24/2024 in the following form:

Mako Bates and Joseph P. Near. (2024). We Know I Know You Know; Choreographic Programming With Multicast and Multiply Located Values. *CP24* `https://youtu.be/mnjhUZM4krU?si=Whx7l1F_UZUdDN2h`

Material from this proposal is additionally available as archived pre-prints in the following forms:

Bates, Mako, and Joseph P. Near. 'We Know I Know You Know; Choreographic Programming With Multicast and Multiply Located Values'. arXiv [Cs.PL], 2024. arXiv. `http://arxiv.org/abs/2403.05417`.

Bates, Mako, Syed Jafri, and Joseph P. Near. 'MultiChor: Census Polymorphic Choreographic Programming with Multiply Located Values'. arXiv [Cs.PL], 2024. arXiv. `http://arxiv.org/abs/2406.13716`.

Tools described in this proposal are availibe for use in the following from:

Mako Bates. 2024. MultiChor: Type-safe and efficient choreographies with location-set polymorphism. `https://hackage.haskell.org/package/MultiChor-1.0.1.1`

Table of Contents

List of Figures

Chapter 1

Introduction and Literature Review

1.1 Introduction

Choreographic programming (CP) is a language paradigm for implementing distributed systems in which the programmer writes one unified program, called a choreography, that describes how the participants of the system interact from a third-person-omniscient perspective. (Carbone and Montesi 2013, Montesi 2014, Montesi 2023) A choreography can be translated into to a collection of executable programs for use in the real world, one for each participant; this process is called endpoint projection (EPP). The CP approach has benefits both for understandability of distributed system implementations, and for strong static guarantees about the deadlock-freedom of the resulting executable code (Carbone and Montesi 2013).

The study of CP is comparatively young; while some of the ideas have existed informally as far back as the 1970s, choreographic programming as it's understood today was first formalized in (Carbone and Montesi 2013). In this chapter we describe the central concepts of choreographic programming, its advantages and disadvantages, and past and ongoing work to push the boundaries of the kinds of systems it can implement.

1.1.1 An illustrative example

Consider the three programs in Figure 1.1, which are intended to run concurrently and pass messages back and forth between each other. The overall effect is an elementary process in which the client makes a `Get` or `Put` request to a server (with a backup) that manages a key-value-store (KVS). Even this simplified example

takes a moment for a reader to make sense of; one must read the three programs, infer the correspondence between messages sent and received by the three parties, and judge for oneself if the communication protocol implemented is sensical. One might even judge that this simple protocol has a bug: if the request is a `Get`, the backup server will hang indefinitely!

```haskell
kvs_client :: Request -> IO Response
kvs_clien = request = do
    request `send` primary    -- send request to the primary node
    response <- recv primary  -- receive the response
    return response
```

(a) The function to be called by the client process. They pass in their `Request` object and send it to the server. Then they receive a response from the server and return it.

```haskell
-- handle a Get or Put request
handleRequest :: Request -> IORef State -> IO Response

kvs_primary :: IORef State -> IO ()
kvs_primary stateRef = do
    request <- recv client                      -- receive the request
    case request of                             -- branch on the request
      Get _ -> pure ()                          -- no-op
      Put _ _ -> do request `send` backup       -- send request to the backup node
                    ack <- recv backup          -- and get back an acknowlegement
                    pure ()
    response <- handleRequest request stateRef  -- process the request locally
    response `send` client                      -- send response to client
```

(b) The function to be called by the primary server. They pass in a reference to their mutable state, and receive a message of type `Request` from the client. In the case of a `Put` request, they forward it to the backup server and check for the backup's acknowledgement. In either case, they process the request against their own mutable state and send the response back to the client.

```haskell
kvs_backup :: IORef State -> IO ()
kvs_backup stateRef = do
    request@(Put _) <- recv primary  -- receive the request
    success <- handleRequest request stateRef  -- process the request locally
    success `send` client  -- acknowlege to the primary server that we're done
```

(c) The function to be called by the backup server. They pass in a reference to their mutable state, and receive a `Put` message from the primary server. They process it against their mutable state and send back an acknowledgement message to indicate their success.

Figure 1.1: A Simple Concurrent Protocol: a key-value store with a backup server

In Section 1.2.1 we will mention some intermediate frameworks that have historically been used to facilitate writing large and complicated concurrent protocols, but here we jump ahead to choreographic programming (CP). Figure 1.2 shows the same protocol as Figure 1.1, but implemented as a choreography. In this form there is no cognitive overhead for matching `send` and `recv` operations, because matching pairs of them

are combined into monolithic `comm` operations. The entire protocol can be read at once in a sensical order. (The order in which operations are presented in a choreography is not necessarily the order in which they will happen; the participants are not guaranteed to all start at the same physical time, or to operate at the same speeds.) Re-writing the example KVS system as a choreography does not immediately solve the issue of what the backup server should do in the event of a `Get` request, but it makes the problem detectable by static analysis. In fact, the choreography in Figure 1.2 cannot compile in any real CP system because `"backup"`'s behavior is ambiguous! Figure 1.3 shows two variations of how to realize the KVS behavior in Haskell using our MultiChor library.

```
kvs :: Located '["client"] Request ->
       Located '["primary"] (IORef State) ->
       Located '["backup"] (IORef State) ->
       Choreo Participants IO (Located '["client"] Response)
kvs request primaryStateRef backupStateRef = do
  request' <- (client, request) `comm` primary  -- send request to the primary node
  case request' of                              -- branch on the request
    Get _ -> pure ()
    Put _ _ -> do
      request'' <- (primary, request') `comm` backup  -- forward the request to the backup
      success <- backup `locally`                     -- the backup does local work:
                   (handleRequest <$> request'' <*> backupStateRef)
      ack <- (backup, success) `comm` primary
      pure ()
  response <- primary `locally`                 -- the primary server does local work:
                (handleRequest <$> request' <*> primaryStateRef)
  result <- (primary, response) `comm` client @@ nobody  -- send response to client
  return result
```

This pseudo-code choreography implements the protocol from Figure 1.1 as a single program. As written, it is not actually realizable because `backup` doesn't know whether to expect a message or not. Real CP systems have ways of detecting and fixing problems like this.

Figure 1.2: A Simple Choreography: a key-value store with a backup server

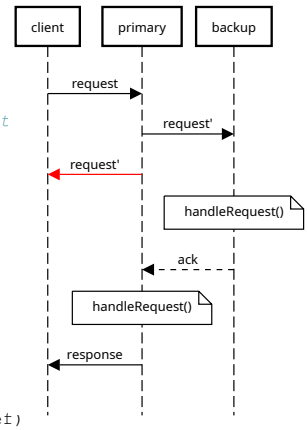
1.1.2 Layout and Contributions

The remainder of this chapter covers the history and theory of CP and discusses some modern work relevant to the ongoing development of CP systems. In particular, Section 1.2.3 discusses the "Knowledge of Choice" problem, a central difficulty in the design of CP systems, and a number of strategies that have been used to solve it.

Chapter 2 presents our first contribution: a formal model of a CP system with two novel features: *multiply-located values* (MLVs) and *enclaves*. These features combine to allow a compelling new strategy for KoC management. In particular, all well-typed λ_C choreographies are projectable and have cromulent KoC by

```haskell
-- sub-choreography: backup may or may not do anything...
handleBackup :: Located '["backup"] (IORef State)
             -> Request
             -> Choreo Participants IO ()
handleBackup state    (Get key)       = pure () -- no-op.
handleBackup state r@(Put key value) = do
    success <- backup `locally` \un -> -- the backup's local work
      handleRequest r (un backup state)
    ack <- (backup, success) `comm` primary  -- send acknowlegement
    pure ()

kvs :: Located '["client"] Request
    -> Located '["primary"] (IORef State),
    -> Located '["backup"] (IORef State)
    -> Choreo Participants IO (Located '["client"] Response)
kvs request primaryStateRef backupStateRef = do
  -- send request to the primary node:
  request' <- (client, request) ~> primary @@ nobody
  -- branch on the request:
  broadcast (primary, request') >>= (handleBackup backupStateRef)
  -- process request on the primary node:
  response <- primary `locally` \un ->
    handleRequest (un primary request') (un primary primaryStateRef)
  -- send response to client:
  (primary, response) ~> client @@ nobody
```

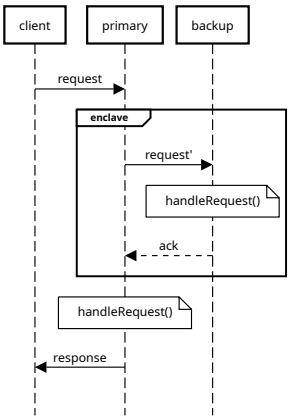


(a) A key-value store with a backup server, written in MultiChor. The backup server sends an acknowledgement message ack to the primary server if and only if `request` is a `Put`. The `broadcast` operator (line 19) ensures KoC so that the primary and backup servers are guaranteed to use the same case of `handleBackup`, but it results in redundant communication (shown in red in the sequence diagram).

```haskell
type Servers = ["primary", "backup"]
servers :: Subset Servers Participants
servers = primary @@ backup @@ nobody

-- Change to handleBackup: now a sub-choreography for *servers only*
handleBackup :: Located '["backup"] (IORef State)
             -> Request
             -> Choreo Servers IO ()

-- Change to line 20: sub-choreography is *enclaved*
enclave servers $
    broadcast (primary, request') >>= (handleBackup backupStateRef)
```



(b) In this variation, the `enclave` operator eliminates the redundant communication. The enclaved sub-choreography is indicated by a box in the sequence diagram. On line 3, `@@ nobody` is MultiChor idiom explained in Section 3.3.

Figure 1.3: A Real Choreography: a key-value store writing using MultiChor, two variations.

construction. In Section 2.3 we compare λ_C to representative systems that use other KoC management strategies.

Chapter 3 presents our second contribution: an implementation of the enclaves-&-MLVs paradigm in Haskell. The MultiChor library is already available on Hackage, Haskell's main package management system. MultiChor directly implements the main concepts of λ_C as a monadic eDSL in Haskell, and combines Haskell's Hindley–Milner-based type system with a proof-witness system to capture the requisite notion of a well-typed choreography.

Because MultiChor is fully embedded in and interoperable with Haskell, functional-programming patterns can be applied to the choreographic setting without further theoretical or infrastructural work. The most important example of this, which we call "census polymorphism" is the ability to write choreographies that are parametric over their set of participants. This capability is novel among CP systems, and the third contribution presented in this work. We discuss census polymorphism in greater detail in Section 3.4.

Chapter 4 explains a plan for modifications to the MultiChor system to simplify its core mechanisms and facilitate further theoretical work.

1.2 Background

Choreographic programming is a paradigm that expresses a distributed system as a single, global program describing the behavior and interactions of all parties. The global view of the distributed system enables easier reasoning about the system's behavior; for example choreographic languages can ensure *deadlock freedom* (Carbone and Montesi 2013) and choreographies can be composed modularly like normal single-threaded protocols.

1.2.1 History

Although in this present work we use the noun "choreography" to refer to actual programs written in CP systems, the word was already in use before the invention of choreographic programming *per se*. The broader sense of the word is any unified 3rd-person description of or plan for interaction between two or more participating systems. Pseudo-code diagrams featuring a unified communication operator "→" were being used to describe cryptographic protocols at least as early as 1978 (Needham and Schroeder

1978). (W3C 2005) presented the *"Web Services Choreography Description Language"* in which a user could specify the interaction, the sequence of communications, between parties. This was a specification language; implementations compatible with a given specification needed to be written separately. Later tools were to developed to statically check if a specification was actually implement*able*, whether a provided implementation was faithful to a specification, and whether the specification had other desired properties. In particular, *multiparty session types* are a system in which a communication plan is specified as a "global type"; the global type is *projected* to a single party, resulting in a "local type" against which an implementation of that party's role can type-check (Honda et al. 2008). Multiparty session types also provided communication safety (*e.g.* a party never misinterprets received data as being of the wrong type) and a form of deadlock freedom. One way to think about choreographic programming is as the extension of multiparty session types to include both the communication plan and the implementation of the computation each party is doing.

1.2.2 Endpoint Projection

CP systems necessarily include a means by which a given computer can execute the behavior of a role in the choreography. Typically, this takes the form of a function from choreographies to programs in a "local" language which the target computer can execute. Such a function is parameterized by the target role, and is called *Endpoint Projection* (EPP); the roles are "endpoints", *i.e.* surfaces from which and into which messages pass, and the choreography is "projected" in the sense that the given endpoint's view of it is extracted.

For example, EPP of the choreography in Figure 1.3*(b)* to each of the three participants would yield respective programs very similar to the ones in Figure 1.1, except that the primary server would always send the request to the backup server (and therefor the backup server would know how to proceed).

1.2.3 Knowledge of Choice

Choreographies with conditionals (`if`-expressions or anything that could be used for conditional control-flow) introduce a challenge for endpoint projection: *some parties might not know which branch to take!* This challenge is referred to as the *knowledge of choice* (KoC) (Castagna et al. 2011) problem. All choreographic programming languages include a strategy for KoC that ensures that relevant parties have enough information to play their part in the program.

The pseudo-code in Figure 1.2 shows a simple instance of this exact problem: `backup` doesn't know whether to expect a message or not, because that decision depends on a value (`request'`) that `backup` doesn't have. Figure 1.3*(a)* implements HasChor's KoC strategy: the branch guard is broadcast to everyone. HasChor's authors knew this to be an inefficient (but expedient) solution. As we show in Figure 1.3*(b)*, MultiChor can do better.

A more traditional approach, which we refer to as *select-&-merge*, is to include in one's language a special operator just for communicating KoC. This operator is called " **`select`** "; it sends a statically-declared flag to the recipient to select which of that party's possible behaviors should be activated. For example, Figure 1.4 shows how our KVS choreography might be expressed in a select-&-merge system. Under both the centralized semantics and type analysis, **`select`** is a no-op! During EPP, **`select`** results in "offer" and "choose" actions at the receiver and sender, respectively. Because **`select`** doesn't affect typing, in Figure 1.4 it would not be possible to encode the need for the lines 9 and 12 in Haskell's type system. Instead, such CP systems enforce KoC requirements in their "merge" operator, which is applied during EPP. Any party besides the owner of a branch guard will replace the entire conditional expression with the merge of their projections of the branches. The merge of two "offer" expressions is an offer of the union of the possible continuations; merges of any other combinations of expressions are only defined when the two expressions are the same. Thus, if lines 9 and 12 were omitted from Figure 1.4, the error would be detected during EPP to `backup` when the system tried to merge `{}` with

```
{ request'' <- recv primary;
  success <- handleRequest request'' backupStateRef;
  send success primary  }
```

A substantial body of research has explored the soundness select-&-merge and its fundamentals, implementation, and extensions (Carbone and Montesi 2013, Cruz-Filipe and Montesi 2020, Giallorenzo et al. 2024, Montesi and Peressotti 2017). That said, HasChor, MultiChor, ChoRus, and ChoreoTS all do EPP at runtime(Bates et al. 2024), so using EPP to detect KoC problems would not be a satisfactory solution for them.

Yet another KoC strategy was proposed by (Jongmans and van den Bos 2022). Their approach requires writing distinct guards for every participant in a conditional expression; they show how to use predicate

```
kvs :: Located '["client"] Request ->
       Located '["primary"] (IORef State) ->
       Located '["backup"] (IORef State) ->
       Choreo Participants IO (Located '["client"] Response)
kvs request primaryStateRef backupStateRef = do
  request' <- (client, request) `comm` primary  -- send request to the primary node
  case request' of                              -- branch on the request
    Get _ -> do
      select primary backup LEFT
      pure ()
    Put _ _ -> do
      select primary backup RIGHT
      request'' <- (primary, request') `comm` backup  -- forward the request to the backup
      success <- backup `locally`                     -- the backup does local work:
                   (handleRequest <$> request'' <*> backupStateRef)
      ack <- (backup, success) `comm` primary
      pure ()
  response <- primary `locally`                 -- the primary server does local work:
                (handleRequest <$> request' <*> primaryStateRef)
  result <- (primary, response) `comm` client @@ nobody  -- send response to client
  return result
```

This pseudo-code choreography implements the protocol from Figure 1.3*(b)* using "select-&-merge" syntax. Attempting to engineer a real select-&-merge CP eDSL in the style of MultiChor would result in a system that could not detect KoC errors until runtime.

Figure 1.4: A Select-&-Merge Choreography: a key-value store with a backup server

transformers to check that such distributed decisions are unanimous. This system is verbose, but at least as expressive as the one we describe in this work.

1.2.4 The "Census" typing context

Although it is a hallmark of CP that a user may write actions for various parties in any given place in the program without demarcations of who "control" is passing to, it is not necessarily the case that every party that exists is eligible to take action at every place in the choreography. Some earlier works, *e.g.* (Cruz-Filipe et al. 2022), have tracked these sets of participants in their type systems, and used that typing context to control participation inside of function bodies. Such a typing context plays a more active role in this present work, so we coin the term *"census"* for a typing context that controls which parties are "present" to participate in any given part of a choreography.

A party not listed in a census should will typically skip evaluating that section of the choreography. In terms of EPP, that's done by projecting the entire clause to $\perp$ or some similar marker.

1.2.5 Additional Literature

Research and development of CP systems seems to have accelerated since approximately 2022. Pirouette (Hirsch and Garg 2022), Chorλ (Cruz-Filipe et al. 2022), and PolyChorλ (Graversen et al. 2024) are (higher order) functional languages for writing select-&-merge choreographies; PolChorλ additionally introduces polymorphism over identities of parties. Choral (Giallorenzo et al. 2024) is a choreographic language implementing the select-&-merge paradigm and targeting industrial use; it runs on the JVM and can easily import local Java code.

Excitingly, CP libraries for a variety of general purpose languages have recently appeared on the scene. These include UniChorn (Chakraborty 2024), Chorex (Wiersdorf and Greenman 2024), and Klor (Lugović and Jongmans 2024). All three are under development; here we report on their state toward the end of 2024. UniChorn is a port of HasChor into the Unison programming language. To implement EPP, it uses the Unison feature of *abilities*, better known in the literature as algebraic effects (Plotkin and Power 2003, Plotkin and Pretnar 2013). This implementation approach, which was also recently proposed by (Shen and Kuper 2024), can be thought of as a generalization of the free(r)-monad approach. As a direct port of HasChor, UniChorn does not support enclaves, MLVs, or census polymorphism. Chorex is a CP system for Elixir, and Klor is a CP system for Clojure; both Chorex and Klor leverage the powerful macro systems of their respective host languages to carry out EPP. Chorex uses the select-&-merge KoC strategy, and unprojectable choreographies can be detected at macro expansion time. Klor, on the other hand, is effectively an enclaves-&-MLVs system, but their API differs from the implementations we present here, and the authors have not yet shown what safety guarantees it does or does not offer. Neither Chorex nor Klor support census polymorphism.

Wysteria (Rastogi et al. 2014) and Symphony (Sweet et al. 2023) are domain-specific languages for *secure multiparty computation*. Programs in these languages can exhibit census polymorphism, but they have homomorphic encryption baked into their semantics for communication, and they are not intended for general-purpose choreographic programming. Wysteria has a `par` language construct, used for evaluating an expression at a set of locations, that is somewhat similar in spirit to our enclaves. However, applying the enclave concept to choreographic programming, and to the choreographic knowledge-of-choice problem in particular, is to our knowledge a novel contribution of this paper. Symphony does not support conditionals, and therefore KoC propagation is a moot point for them.

Bibliography

Bates, M., S. Kashiwa, S. Jafri, G. Shen, L. Kuper, and J. P. Near (2024). Efficient, portable, census-polymorphic choreographic programming.

Carbone, M. and F. Montesi (2013). Deadlock-freedom-by-design: multiparty asynchronous global programming. In *Proceedings of the 40th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '13, New York, NY, USA, pp. 263–274. Association for Computing Machinery.

Castagna, G., M. Dezani-Ciancaglini, and L. Padovani (2011). On global types and multi-party sessions. In R. Bruni and J. Dingel (Eds.), *Formal Techniques for Distributed Systems*, Berlin, Heidelberg, pp. 1–28. Springer Berlin Heidelberg.

Chakraborty, K. (2024). Unichorn.

Cruz-Filipe, L., E. Graversen, L. Lugović, F. Montesi, and M. Peressotti (2022, September). *Theoretical Aspects of Computing*, Volume 13572 of *Lecture Notes in Computer Science*, Chapter Functional choreographic programming, pp. 212–237. Tbilisi, Georgia: Springer.

Cruz-Filipe, L. and F. Montesi (2020). A core model for choreographic programming. *Theor. Comput. Sci. 802*, 38–66.

Giallorenzo, S., F. Montesi, and M. Peressotti (2024, jan). Choral: Object-oriented choreographic programming. *ACM Trans. Program. Lang. Syst. 46*(1).

Graversen, E., A. K. Hirsch, and F. Montesi (2024). Alice or bob?: Process polymorphism in choreographies. *Journal of Functional Programming 34*, e1.

Hirsch, A. K. and D. Garg (2022, January). Pirouette: higher-order typed functional choreographies. *Proc. ACM Program. Lang. 6*(POPL).

Honda, K., N. Yoshida, and M. Carbone (2008). Multiparty asynchronous session types. In *Proceedings of the 35th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '08, New York, NY, USA, pp. 273–284. Association for Computing Machinery.

Jongmans, S.-S. and P. van den Bos (2022). *A Predicate Transformer for Choreographies (Full Version)*. Number 01 in OUNL-CS (Technical Reports). Open Universiteit Nederland.

Lugović, L. and S.-S. Jongmans (2024). Klor: Choreographies in clojure.

Montesi, F. (2014). Ph. D. thesis, Denmark.

Montesi, F. (2023). *Introduction to Choreographies*. Cambridge University Press.

Montesi, F. and M. Peressotti (2017). Choreographies meet communication failures. *CoRR abs/1712.05465*.

Needham, R. M. and M. D. Schroeder (1978, December). Using encryption for authentication in large networks of computers. *Commun. ACM 21*(12), 993–999.

Plotkin, G. and J. Power (2003). Algebraic operations and generic effects. *Applied categorical structures 11*, 69–94.

Plotkin, G. D. and M. Pretnar (2013, December). Handling algebraic effects. *Logical Methods in Computer Science Volume 9, Issue 4*.

Rastogi, A., M. A. Hammer, and M. Hicks (2014). Wysteria: A programming language for generic, mixed-mode multiparty computations. In *2014 IEEE Symposium on Security and Privacy*, pp. 655–670.

Shen, G. and L. Kuper (2024). Toward verified library-level choreographic programming with algebraic effects.

BIBLIOGRAPHY

Sweet, I., D. Darais, D. Heath, W. Harris, R. Estes, and M. Hicks (2023, February). Symphony: Expressive secure multiparty computation with coordination. *The Art, Science, and Engineering of Programming 7*(3).

W3C (2005). WS Choreography Description Language. http://www.w3.org/TR/ws-cdl-10/.

Wiersdorf, A. and B. Greenman (2024). Chorex: Choreographic programming in elixir.

Chapter 2

A New Core Choreographic Calculus

2.1 Introduction

While the most urgent shortcoming of HasChor's KoC strategy is that it induces extraneous communication costs, it has another shortcoming which it shares in common with many select-&-merge systems like Pirouette: Sequential conditional clauses on the same branch-guard (*aka* "scrutinee") require KoC to be *re*communicated. We address this issue directly by extending the notion of located values into *multiply located values* (MLVs). MLVs allow multiple parties to branch together on a shared guard; in addition to recyclability, this alleviates the need for a designated `select` operator. In this section we present λ_C, a formal model of a higher-order functional CP language that uses MLVs and *census tracking* to guarantee proper KoC management entirely by type-checking and without compromising efficiency or expressivity.

2.1.1 Multiply-located values

Previous choreography languages have featured *located values*, values annotated with (or implicitly assigned to) their owning party such that EPP to the owner results in the value itself and EPP to any other party results in a special "missing" value (*e.g.* $\bot$). *Multiply located values* are exactly the same except they are annotated with a non-empty *set* of parties. EPP of a multiply-located value for any of the owning parties results in the same value, and projection to any other party yields $\bot$. Prior works have objects with multiple owners as

emergent structures in a language (*e.g.* choreographic processes (Giallorenzo et al. 2024), distributed choice types (Cruz-Filipe et al. 2023)), but these project to each owner's distinct view of the structure.

Creation of an MLV within an choreographic runtime follows from the fact that if Alice sends Bob a number, both Alice and Bob know what number was sent. Representing this in the language can be done a few different ways:

- A `share` operator that updates the type of an MLV-typed variable to include the recipient(s) in the ownership set. This is a poor fit for a functional programming language because it mutates the type of a variable, and additional machinery would be needed to make it work with nested enclaves (see Section 2.1.2).
- A `comm` operator that returns a value owned by the original owners and the recipient(s). This is not as straightforward as it sounds; if the communication happens inside a conditional, some of the original owners may not know that the communication happened. Intersecting with the current census is a sound solution, but may be difficult to embed in the type system of existing host languages.
- A `multicast` operator (by whatever name) that returns a value owned by exactly the specified recipients. In practice, users will often list the sender (and possibly any subset of the original owners) among the recipients; an ideal implementation would omit the actual communication to recipients who already have the data.
- A `broadcast` operator that always returns an MLV owned by the entire current census. This is actually equivalent to the above `multicast` operator; the choice is purely ergonomic.

Multiply-located values can also enable concise expression of programs in which multiple parties compute the same thing in parallel, a common occurrence when communication is more expensive than computation. For example, the λ_C expression $5@\{p, q, r\} + 3@\{p, q, r\}$ represents an addition performed in parallel by p, q, and r.

2.1.2 Managing KoC with MLVs

As discussed in Section 1.2.4, prior systems have tracked censuses as attributes of choreographic functions. The ChoRus system introduced the `enclave` operator to explicitly limit the census within its argument, and

showed how this could be used to avoid HasChor's overly broad `broadcasts`[1]. An `enclave` operator is a good design choice for an embedded DSL, but is not necessary in an abstract or bespoke language where the action of enclaving can be built into relevant constructs like functions and conditionals.

The combination of censuses with enclaving and MLVs constitutes a novel KoC strategy, on par with state-of-the-art select-&-merge systems like Chorλ in terms of communication efficiency and more amenable to implementation as an eDSL.

2.2 A Formal MLVs-&-Enclaves Language

We present the $\boldsymbol{\lambda_C}$ CP system. The syntax of $\boldsymbol{\lambda_C}$ and our overarching computational model and proof-approach are loosely based on Chorλ (Cruz-Filipe et al. 2022). $\boldsymbol{\lambda_C}$ is a higher-order choreographic lambda calculus; we omit recursion and polymorphism because they are orthogonal to our goals here. Specifically, we will show that multiply-located values and enclaving operations are sufficient for a sound CP language without further KoC management. In Sections 2.2.1 to 2.2.5 we describe the syntax, type system, and semantics of $\boldsymbol{\lambda_C}$. As in other choreographic languages, the primary semantics describes the intended *meaning* of choreographies and can be used to reason about their behavior, but is not the "ground truth" of concurrent execution. Sections 2.2.6 to 2.2.8 describe the languages of distributed processes, $\boldsymbol{\lambda_L}$ and $\boldsymbol{\lambda_N}$, and define endpoint projection for $\boldsymbol{\lambda_C}$. In Section 2.2.9, we prove that the behavior of a choreography's projection in $\boldsymbol{\lambda_N}$ matches that of the original $\boldsymbol{\lambda_C}$ choreography, and that $\boldsymbol{\lambda_C}$'s type system ensures deadlock-freedom. In Section 2.3 we provide some example choreographies in (a plain-text rendering of) $\boldsymbol{\lambda_C}$. For example, Figure 2.11 implements the KVS example from Section 1.1.

2.2.1 Syntax

The syntax of $\boldsymbol{\lambda_C}$ is in Figure 2.1. Location information sufficient for typing, semantics, and EPP is explicit in the expression forms. We distinguish between "pairs" ($\mathsf{Pair}\, V_1 V_2$, of type $(d_1 \times d_2)@p^+$) and "tuples" ((V_1, V_2), of type (T_1, T_2)) so that we can have a distinguishable concept of "data" as "stuff that can be sent"; we do not believe this to have any theoretic significance.

[1] As discussed in (Bates et al. 2024), ChoRus has since been upgraded to incorporate the innovations discussed in this work. (Kashiwa et al. 2023) is an unpublished pre-print describing their system as it existed without MLVs or census polymorphism.

The superscript-marked identifier p^+ is a semantic token representing a set of parties; an unmarked p is a completely distinct token representing a single party. Note the use of a superscript "+" to denote sets of parties instead of a hat or boldface; this denotes that these lists may never be empty.[2] The typing and semantic rules will enforce this invariant as needed. When referring to a census, or when a set of parties should be understood as a "context" rather than an "attribute", we write Θ rather than p^+; this is entirely to clarify intent and the distinction has no formal meaning.

M	$::=$	V	Values.
	$\mid$	MM	Function application.
	$\mid$	$\mathsf{case}_{p^+}\ M\ \mathsf{of}\ \mathsf{Inl}\ x \Rightarrow M; \mathsf{Inr}\ x \Rightarrow M$	Branching on a disjoint-sum value.
V	$::=$	x	Variables.
	$\mid$	$(\lambda x : T\,.\,M)@p^+$	Function literals annotated with participants.
	$\mid$	$()@p^+$	Multiply-located unit.
	$\mid$	$\mathsf{Inl}\,V$	Injection to a disjoint-sum.
	$\mid$	$\mathsf{Inr}\,V$	
	$\mid$	$\mathsf{Pair}\,VV$	Construction of data pairs (products).
	$\mid$	$(V, \ldots, V)$	Construction of heterogeneous tuples.
	$\mid$	fst_{p^+}	Projection of data pairs.
	$\mid$	snd_{p^+}	
	$\mid$	$\mathsf{lookup}^n_{p^+}$	Projection of tuples.
	$\mid$	$\mathsf{com}_{p:p^+}$	Send to one or more recipients.
d	$::=$	$()$	We provide a simple algebra of "data" types,
	$\mid$	$d + d$	which can encode booleans or other finite types
	$\mid$	$d \times d$	and could be extended with natural numbers if desired.
T	$::=$	$d@p^+$	A complete multiply-located data type.
	$\mid$	$(T \to T)@p^+$	Functions are located at their participants.
	$\mid$	$(T, \ldots, T)$	A fixed-length heterogeneous tuple.

Figure 2.1: The complete syntax of the $\boldsymbol{\lambda_C}$ language.

[2] Later, we'll use an "$*$" to denote a possibly-empty set or list, and a "?" to denote "zero or one".

2.2.2 The Mask Operator

Here we introduce the $\triangleright$ operator, the purpose of which is to allow Theorem 2 (semantic stepping preserves types) to hold without adding sub-typing or polymorphism to $\boldsymbol{\lambda_C}$. $\triangleright$ is a partial function defined in Figure 2.2; the left-hand argument is either a type (in which case it returns a type) or a value (in which case it returns a value). The effect of $\triangleright$ is very similar to EPP, except that it projects to a set of parties instead of just one, and instead of introducing a $\bot$ symbol it is simply undefined in some cases. Because it is used during type-checking, errors related to it are caught at that time.

Consider an expression using a "masking identity" function: $(\lambda x : ()@\{p\}\,.\,x)@\{p\}\;()@\{p,q\}$, where the lambda is an identity function *application of which* turns a multiply-located unit value into one located at just p. Clearly, the lambda should type as $(()@\{p\} \to ()@\{p\})@\{p\}$; and so the whole application expression should type as $()@\{p\}$. Masking in the typing rules lets this work as expected, and similar masking in the semantic rules ensures type preservation.

$$\textsc{MTData}\ \frac{p^+ \cap \Theta \neq \varnothing}{d@p^+ \triangleright \Theta \;\triangleq\; d@(p^+ \cap \Theta)} \qquad \textsc{MTFunction}\ \frac{p^+ \subseteq \Theta}{(T \to T')@p^+ \triangleright \Theta \;\triangleq\; (T \to T')@p^+}$$

$$\textsc{MTVector}\ \frac{T_1' = T_1 \triangleright \Theta, \quad \ldots \quad T_n' = T_n \triangleright \Theta}{(T_1, \ldots, T_n) \triangleright \Theta \;\triangleq\; (T_1', \ldots, T_n')}$$

$$\textsc{MVLambda}\ \frac{p^+ \subseteq \Theta}{(\lambda x : T\,.\,M)@p^+ \triangleright \Theta \;\triangleq\; (\lambda x : T\,.\,M)@p^+} \qquad \textsc{MVUnit}\ \frac{p^+ \cap \Theta \neq \varnothing}{()@p^+ \triangleright \Theta \;\triangleq\; ()@(p^+ \cap \Theta)}$$

$$\textsc{MVInL}\ \frac{V' = V \triangleright \Theta}{\mathsf{Inl}\, V \triangleright \Theta \;\triangleq\; \mathsf{Inl}\, V'} \qquad \textsc{MVInR}\ \frac{\cdots}{\cdots} \qquad \textsc{MVProj1}\ \frac{p^+ \subseteq \Theta}{\mathsf{fst}_{p^+} \triangleright \Theta \;\triangleq\; \mathsf{fst}_{p^+}} \qquad \textsc{MVProj2}\ \frac{\cdots}{\cdots}$$

$$\textsc{MVPair}\ \frac{V_1' = V_1 \triangleright \Theta \quad V_2' = V_2 \triangleright \Theta}{\mathsf{Pair}\, V_1\, V_2 \triangleright \Theta \;\triangleq\; \mathsf{Pair}\, V_1'\, V_2'} \qquad \textsc{MVVector}\ \frac{V_1' = V_1 \triangleright \Theta \quad \ldots \quad V_n' = V_n \triangleright \Theta}{(V_1, \ldots, V_n) \triangleright \Theta \;\triangleq\; (V_1', \ldots, V_n')}$$

$$\textsc{MVProjN}\ \frac{p^+ \subseteq \Theta}{\mathsf{lookup}^n_{p^+} \triangleright \Theta \;\triangleq\; \mathsf{lookup}^n_{p^+}} \qquad \textsc{MVCom}\ \frac{s \in \Theta \quad r^+ \subseteq \Theta}{\mathsf{com}_{s;r^+} \triangleright \Theta \;\triangleq\; \mathsf{com}_{s;r^+}} \qquad \textsc{MVVar}\ \frac{}{x \triangleright \Theta \;\triangleq\; x}$$

Figure 2.2: Definition of the $\triangleright$ operator.

2.2.3 Typing Rules

The typing rules for λ_C are in Figure 2.3. A judgment $\Theta; \Gamma \vdash M : T$ says that M has type T in the context of a non-empty census Θ and a (possibly empty) list of variable bindings $\Gamma = (x_1 : T_1), \ldots (x_n : T_n)$. In TLambda and TProjN we write preconditions $\texttt{noop}^{\triangleright p^+}(T)$ meaning $T = T \triangleright p^+$, *i.e.* masking to those parties is a "no-op".

$$\textsc{TLambda}\ \frac{p^+; \Gamma, (x : T) \vdash M : T' \quad p^+ \subseteq \Theta \quad \texttt{noop}^{\triangleright p^+}(T)}{\Theta; \Gamma \vdash (\lambda x : T\,.\,M)@p^+ : (T \to T')@p^+} \qquad \textsc{TVar}\ \frac{x : T \in \Gamma \quad T' = T \triangleright \Theta}{\Theta; \Gamma \vdash x : T'}$$

$$\textsc{TApp}\ \frac{\Theta; \Gamma \vdash M : (T_a \to T_r)@p^+ \quad \Theta; \Gamma \vdash N : T'_a \quad T'_a \triangleright p^+ = T_a}{\Theta; \Gamma \vdash MN : T_r}$$

$$\textsc{TCase}\ \frac{\begin{array}{c}\Theta; \Gamma \vdash N : T_N \quad (d_l + d_r)@p^+ = T_N \triangleright p^+ \\ p^+; \Gamma, (x_l : d_l@p^+) \vdash M_l : T \quad p^+; \Gamma, (x_r : d_r@p^+) \vdash M_r : T \quad p^+ \subseteq \Theta\end{array}}{\Theta; \Gamma \vdash \mathsf{case}_{p^+}\ N\ \mathsf{of}\ \mathsf{Inl}\ x_l \Rightarrow M_l; \mathsf{Inr}\ x_r \Rightarrow M_r : T}$$

$$\textsc{TUnit}\ \frac{p^+ \subseteq \Theta}{\Theta; \Gamma \vdash ()@p^+ : ()@p^+} \qquad \textsc{TPair}\ \frac{\Theta; \Gamma \vdash V_1 : d_1@p_1^+ \quad \Theta; \Gamma \vdash V_2 : d_2@p_2^+ \quad p_1^+ \cap p_2^+ \neq \varnothing}{\Theta; \Gamma \vdash \mathsf{Pair}\ V_1 V_2 : (d_1 \times d_2)@(p_1^+ \cap p_2^+)}$$

$$\textsc{TVec}\ \frac{\Theta; \Gamma \vdash V_1 : T_1 \quad \ldots \quad \Theta; \Gamma \vdash V_n : T_n}{\Theta; \Gamma \vdash (V_1, \ldots, V_n) : (T_1, \ldots T_n)} \qquad \textsc{TInl}\ \frac{\Theta; \Gamma \vdash V : d@p^+}{\Theta; \Gamma \vdash \mathsf{Inl}\ V : (d + d')@p^+} \qquad \textsc{TInr}\ \frac{\ldots}{\ldots}$$

$$\textsc{TProjN}\ \frac{p^+ \subseteq \Theta \quad \texttt{noop}^{\triangleright p^+}((T_1, \ldots, T_n))}{\Theta; \Gamma \vdash \mathsf{lookup}^i_{p^+} : ((T_1, \ldots, T_i, \ldots, T_n) \to T_i)@p^+} \qquad \textsc{TProj2}\ \frac{\ldots}{\ldots}$$

$$\textsc{TProj1}\ \frac{p^+ \subseteq \Theta}{\Theta; \Gamma \vdash \mathsf{fst}_{p^+} : ((d_1 \times d_2)@p^+ \to d_1@p^+)@p^+}$$

$$\textsc{TCom}\ \frac{s \in s^+ \quad s^+ \cup r^+ \subseteq \Theta}{\Theta; \Gamma \vdash \mathsf{com}_{s;r^+} : (d@s^+ \to d@r^+)@(\{s\} \cup r^+)}$$

Figure 2.3: λ_C typing rules.

Examine TCase as the most involved example. The actual judgment says that in the context of Θ and Γ, the case expression types as T. The first two preconditions say that the guard expression N must type in the parent context as some type T_N, which masks to the explicit party-set p^+ as a sum-type $(d_l + d_r)@p^+$. The only rule by which it can do that is MTData, so we can deduce that $T_N = (d_l + d_r)@q^+$, where q^+ is some unspecified superset of p^+. The third and forth preconditions say that M_l and M_r must both type as T with the reduced census p^+ and with the respective x_l and x_r bound to the right and left data types at p^+. The final

precondition says that p^+ is a subset of Θ, *i.e.* everyone who's supposed to be branching is actually present to do so.

The other rules are mostly normal, with similar masking of types and enclaving of censuses as needed. In TVar, the census masks the type bindings in Γ. In isolation, some expressions such as $\mathsf{Inr}()@\{p\}$ or the projection operators are flexible about their exact types; additional annotations could give them monomorphic typing, if that was desirable.

2.2.4 Masked Substitution

For $\triangleright$ to fulfil its purpose during semantic evaluation, it may need to be applied arbitrarily many times with different party-sets inside the new expressions, and it may not even be defined for all such party-sets. Conceptually, this just recapitulates the masking performed in TVar. To formalize these subtleties, in Figure 2.4 we specialize the normal variable-substitution notation $M[x := V]$ to perform location-aware substitution. In Appendix A.1 we prove Theorem 1, which shows that this specialized substitution operation satisfies the usual concept of substitution. (Our various definitons and proofs about them in this work all assume Barendregt's variable convention. Roughly, this says that bound variables are unique. (Urban et al. 2007) provide a more detailed discussion.)

Theorem 1 (Substitution)**.** *If* $\Theta; \Gamma, (x : T_x) \vdash M : T$ *and* $\Theta; \Gamma \vdash V : T_x$*, then* $\Theta; \Gamma \vdash M[x := V] : T$.

2.2.5 Centralized Semantics

The semantic stepping rules for evaluating $\boldsymbol{\lambda_C}$ expressions are in Figure 2.5. In Sections 2.2.6 to 2.2.8 we will develop the "ground truth" of the distributed process semantics and show that the $\boldsymbol{\lambda_C}$'s semantics correctly capture distributed behavior.

$\boldsymbol{\lambda_C}$ is equipped with a substitution-based semantics that, after accounting for the $\triangleright$ operator and the specialized implementation of substitution, is quite standard among lambda-calculi. In particular, we make no effort here to support the out-of-order execution supported by some choreography languages. Because the language and corresponding computational model are parsimonious, no step-annotations are needed for the centralized semantics.

$$
\begin{array}{rcl}
M[x := V] & \triangleq & \text{by pattern matching on } M\text{:} \\
y & \overset{\triangle}{\Longrightarrow} & \begin{cases} y \equiv x & \overset{\triangle}{\Longrightarrow} \quad V \\ y \not\equiv x & \overset{\triangle}{\Longrightarrow} \quad y \end{cases} \\
N_1 N_2 & \overset{\triangle}{\Longrightarrow} & N_1[x := V] N_2[x := V] \\
(\lambda y : T \,.\, N)@p^+ & \overset{\triangle}{\Longrightarrow} & \begin{cases} V \triangleright p^+ = V' & \overset{\triangle}{\Longrightarrow} \quad (\lambda y : T \,.\, N[x := V'])@p^+ \\ \text{otherwise} & \overset{\triangle}{\Longrightarrow} \quad M \end{cases} \\
\mathsf{case}_{p^+}\ N\ \mathsf{of}\ \mathsf{Inl}\ x_l \Rightarrow M_l;\ \mathsf{Inr}\ x_r \Rightarrow M_r & \overset{\triangle}{\Longrightarrow} & \begin{cases} V \triangleright p^+ = V' & \overset{\triangle}{\Longrightarrow} \quad \mathsf{case}_{p^+}\ N[x := V]\ \mathsf{of}\ \mathsf{Inl}\ x_l \Rightarrow M_l[x := V'];\ \mathsf{Inr}\ x_r \Rightarrow M_r[x := V'] \\ \text{otherwise} & \overset{\triangle}{\Longrightarrow} \quad \mathsf{case}_{p^+}\ N[x := V]\ \mathsf{of}\ \mathsf{Inl}\ x_l \Rightarrow M_l;\ \mathsf{Inr}\ x_r \Rightarrow M_r \end{cases} \\
\mathsf{Inl}\ V_1 & \overset{\triangle}{\Longrightarrow} & \mathsf{Inl}\ V_1[x := V] \\
\mathsf{Inr}\ V_2 & \overset{\triangle}{\Longrightarrow} & \mathsf{Inr}\ V_2[x := V] \\
\mathsf{Pair}\ V_1 V_2 & \overset{\triangle}{\Longrightarrow} & \mathsf{Pair}\ V_1[x := V] V_2[x := V] \\
(V_1, \ldots, V_n) & \overset{\triangle}{\Longrightarrow} & (V_1[x := V], \ldots, V_n[x := V]) \\
\left.\begin{array}{lll} ()@p^+ & \mathsf{fst}_{p^+} & \mathsf{snd}_{p^+} \\ \mathsf{lookup}_i^{p^+} & \mathsf{com}_{s;r^+} & \end{array}\right\} & \overset{\triangle}{\Longrightarrow} & M
\end{array}
$$

Figure 2.4: The customised substitution used in $\boldsymbol{\lambda_C}$'s semantics.

$$\textsc{AppAbs}\ \frac{V' = V \triangleright p^+}{((\lambda x : T\,.\,M)@p^+)V \longrightarrow M[x := V']} \qquad \textsc{App1}\ \frac{N \longrightarrow N'}{VN \longrightarrow VN'} \qquad \textsc{App2}\ \frac{M \longrightarrow M'}{MN \longrightarrow M'N}$$

$$\textsc{Case}\ \frac{N \longrightarrow N'}{\mathsf{case}_{p^+}\ N\ \mathsf{of}\ \mathsf{Inl}\,x_l \Rightarrow M_l; \mathsf{Inr}\,x_r \Rightarrow M_r \longrightarrow \mathsf{case}_{p^+}\ N'\ \mathsf{of}\ \mathsf{Inl}\,x_l \Rightarrow M_l; \mathsf{Inr}\,x_r \Rightarrow M_r}$$

$$\textsc{CaseL}\ \frac{V' = V \triangleright p^+}{\mathsf{case}_{p^+}\ \mathsf{Inl}\,V\ \mathsf{of}\ \mathsf{Inl}\,x_l \Rightarrow M_l; \mathsf{Inr}\,x_r \Rightarrow M_r \longrightarrow M_l[x_l := V']} \qquad \textsc{CaseR}\ \frac{\cdots}{\cdots}$$

$$\textsc{Proj1}\ \frac{V' = V_1 \triangleright p^+}{\mathsf{fst}_{p^+}(\mathsf{Pair}\,V_1 V_2) \longrightarrow V'} \qquad \textsc{Proj2}\ \frac{\cdots}{\cdots} \qquad \textsc{ProjN}\ \frac{V' = V_i \triangleright p^+}{\mathsf{lookup}^i_{p^+}(V_1, \ldots, V_i, \ldots, V_n) \longrightarrow V'}$$

$$\textsc{Com1}\ \frac{()@p^+ \triangleright \{s\} = ()@s}{\mathsf{com}_{s;r^+}()@p^+ \longrightarrow ()@r^+} \qquad \textsc{ComPair}\ \frac{\mathsf{com}_{s;r^+}\,V_1 \longrightarrow V_1' \quad \mathsf{com}_{s;r^+}\,V_2 \longrightarrow V_2'}{\mathsf{com}_{s;r^+}(\mathsf{Pair}\,V_1 V_2) \longrightarrow \mathsf{Pair}\,V_1' V_2'}$$

$$\textsc{ComInl}\ \frac{\mathsf{com}_{s;r^+}\,V \longrightarrow V'}{\mathsf{com}_{s;r^+}(\mathsf{Inl}\,V) \longrightarrow \mathsf{Inl}\,V'} \qquad \textsc{ComInr}\ \frac{\cdots}{\cdots}$$

Figure 2.5: $\boldsymbol{\lambda_C}$'s semantics.

The Com1 rule simply replaces one location-annotation with another. ComPair, ComInl, and ComInr are defined recursively amongst each other and Com1; the effect of this is that "data" values can be sent but other values (functions and variables) cannot.

As is typical for a typed lambda calculus, $\boldsymbol{\lambda_C}$ enjoys preservation and progress.

Theorem 2 (Preservation)**.** *If* $\Theta; \varnothing \vdash M : T$ *and* $M \longrightarrow M'$*, then* $\Theta; \varnothing \vdash M' : T$.

Theorem 3 (Progress)**.** *If* $\Theta; \varnothing \vdash M : T$*, then either M is of form V (which cannot step) or their exists* M' *s.t.* $M \longrightarrow M'$.

We prove these properties in Appendices A.2 and A.3 respectively.

2.2.6 The Local Process Language

In order to define EPP and a "ground truth" for $\boldsymbol{\lambda_C}$ computation, we need a locally-computable language, $\boldsymbol{\lambda_L}$, into which it can project. $\boldsymbol{\lambda_L}$ is very similar to $\boldsymbol{\lambda_C}$; to avoid ambiguity we denote $\boldsymbol{\lambda_L}$ expressions B

(for "behavior") instead of M (which denotes a $\boldsymbol{\lambda_C}$ expression) and $\boldsymbol{\lambda_L}$ values L instead of V. The syntax is presented in Figure 2.6.

B	$::=$	$L \mid BB$	Process expressions.
		$\mid \mathsf{case}\ B\ \mathsf{of}\ \mathsf{Inl}\ x \Rightarrow B; \mathsf{Inr}\ x \Rightarrow B$	
L	$::=$	$x \mid () \mid \lambda x\,.\,B$	Process values.
		$\mid \mathsf{Inl}\ L \mid \mathsf{Inr}\ L \mid \mathsf{Pair}\ L\,L$	
		$\mid \mathsf{fst} \mid \mathsf{snd}$	
		$\mid (L, \ldots, L) \mid \mathsf{lookup}^n$	
		$\mid \mathsf{recv}_p \mid \mathsf{send}_{p^*}$	Receive from one party. Send to many.
		$\mid \mathsf{send}^*_{p^*}$	Send to many *and* keep for oneself.
		$\mid \bot$	"Missing" (located someplace else).

Figure 2.6: Syntax for the $\boldsymbol{\lambda_L}$ language.

$\boldsymbol{\lambda_L}$ differs from $\boldsymbol{\lambda_C}$ in a few ways. It's untyped, and the party-set annotations are mostly missing. $\boldsymbol{\lambda_C}$'s $\mathsf{com}_{p;q^+}$ operator is replaced by send_{q^+} and recv_p, as well as a $\mathsf{send}^*_{q^+}$, which differs from send_{q^+} only in that the process which calls it keeps a copy of the sent value for itself. Syntactically, the recipient lists of send and send^* may be empty; this keeps semantics consistent in the edge case implied by a $\boldsymbol{\lambda_C}$ expression like $\mathsf{com}_{s;\{s\}}$ (which is useless but legal). Finally, the value-form $\bot$ ("bottom") is a stand-in for parts of the choreography that do not involve the target party. In the context of choreographic languages, $\bot$ does not denote an error but should instead be read as "unknown" or "somebody else's problem".

The behavior of $\bot$ during semantic evaluation can be handled a few different ways, the pros-and-cons of which are not important in this work. We use a $\bot$-normalizing "floor" function, defined in Figure 2.7, during EPP and semantic stepping to avoid ever handling $\bot$-equivalent expressions like $\mathsf{Pair}\ \bot\,\bot$ or $\bot()$.

$\boldsymbol{\lambda_L}$'s semantic stepping rules are given in Figure 2.8. Local steps are labeled with send ($\oplus$) and receive ($\ominus$) sets, like so: $B \xrightarrow{\oplus\{(p,L_1),(q,L_2)\};\ominus\{(r,L_3),(s,L_4)\}} B'$, or $B \xrightarrow{\oplus\mu;\ominus\eta} B'$ when we don't need to inspect the contents of the annotations. The floor function is used to keep expressions normalized during evaluation. Otherwise, most of the rules are analogous to the corresponding $\boldsymbol{\lambda_C}$ rules from Figure 2.5. The LSend- rules are defined recursively, similar to the Com- rules. LSendSelf shows that send^* is exactly like send except

$\lfloor B \rfloor \triangleq$ by pattern matching on B: (Observe that floor is idempotent.)

$$B_1 B_2 \overset{\triangle}{\Longrightarrow} \begin{cases} \lfloor B_1 \rfloor = \bot, \lfloor B_2 \rfloor = L \overset{\triangle}{\Longrightarrow} \bot \\ \text{else} \overset{\triangle}{\Longrightarrow} \lfloor B_1 \rfloor \lfloor B_2 \rfloor \end{cases}$$

$$\mathsf{case}\ B_G\ \mathsf{of}\ \mathsf{Inl}\ x_l \Rightarrow B_l ; \mathsf{Inr}\ x_r \Rightarrow B_r \overset{\triangle}{\Longrightarrow} \begin{cases} \lfloor B_G \rfloor = \bot \overset{\triangle}{\Longrightarrow} \bot \\ \text{else} \overset{\triangle}{\Longrightarrow} \mathsf{case}\ \lfloor B_G \rfloor\ \mathsf{of}\ \mathsf{Inl}\ x_l \Rightarrow \lfloor B_l \rfloor ; \mathsf{Inr}\ x_r \Rightarrow \lfloor B_r \rfloor \end{cases}$$

$$\lambda x\,.\,B' \overset{\triangle}{\Longrightarrow} \lambda x\,.\,\lfloor B' \rfloor$$

$$\mathsf{Inl}\ L \overset{\triangle}{\Longrightarrow} \begin{cases} \lfloor L \rfloor = \bot \overset{\triangle}{\Longrightarrow} \bot \\ \text{else} \overset{\triangle}{\Longrightarrow} \mathsf{Inl}\ \lfloor L \rfloor \end{cases}$$

$$\mathsf{Inr}\ L \overset{\triangle}{\Longrightarrow} \begin{cases} \lfloor L \rfloor = \bot \overset{\triangle}{\Longrightarrow} \bot \\ \text{else} \overset{\triangle}{\Longrightarrow} \mathsf{Inr}\ \lfloor L \rfloor \end{cases}$$

$$\mathsf{Pair}\ L_1 L_2 \overset{\triangle}{\Longrightarrow} \begin{cases} \lfloor L_1 \rfloor = \bot = \lfloor L_2 \rfloor \overset{\triangle}{\Longrightarrow} \bot \\ \text{else} \overset{\triangle}{\Longrightarrow} \mathsf{Pair}\ \lfloor L_1 \rfloor \lfloor L_2 \rfloor \end{cases}$$

$$(L_1, \ldots, L_n) \overset{\triangle}{\Longrightarrow} \begin{cases} \forall_{i \in [1,n]} \lfloor L_i \rfloor = \bot \overset{\triangle}{\Longrightarrow} \bot \\ \text{else} \overset{\triangle}{\Longrightarrow} (\lfloor L_1 \rfloor, \ldots, \lfloor L_n \rfloor) \end{cases}$$

$$\left.\begin{array}{l} x \\ () \\ \mathsf{fst} \\ \mathsf{snd} \\ \mathsf{lookup}^i \\ \mathsf{send}_{p^*} \\ \mathsf{send}^*_{p^*} \\ \mathsf{recv}_p \\ \bot \end{array}\right\} \overset{\triangle}{\Longrightarrow} B$$

Figure 2.7: The "floor" function, which reduces $\bot$-based expressions.

it locally acts like `id` instead of returning $\bot$. LRecv shows that the recv operator ignores its argument and can return *anything*, with the only restriction being that the return value must be reflected in the receive-set step-annotation.

$$\textsc{LAbsApp}\ \frac{}{(\lambda x\,.\,B)\,L \xrightarrow{\oplus\varnothing;\ominus\varnothing} \lfloor B[x := L] \rfloor} \qquad \textsc{LApp1}\ \frac{B \xrightarrow{\oplus\mu;\ominus\eta} B'}{LB \xrightarrow{\oplus\mu;\ominus\eta} \lfloor LB' \rfloor} \qquad \textsc{LApp2}\ \frac{B \xrightarrow{\oplus\mu;\ominus\eta} B'}{BB_2 \xrightarrow{\oplus\mu;\ominus\eta} \lfloor B'B_2 \rfloor}$$

$$\textsc{LCase}\ \frac{B \xrightarrow{\oplus\mu;\ominus\eta} B'}{\mathsf{case}\ B\ \mathsf{of}\ \mathsf{Inl}\ x_l \Rightarrow B_l; \mathsf{Inr}\ x_r \Rightarrow B_r \xrightarrow{\oplus\mu;\ominus\eta} \lfloor \mathsf{case}\ B'\ \mathsf{of}\ \mathsf{Inl}\ x_l \Rightarrow B_l; \mathsf{Inr}\ x_r \Rightarrow B_r \rfloor}$$

$$\textsc{LCaseL}\ \frac{}{\mathsf{case}\ \mathsf{Inl}\ L\ \mathsf{of}\ \mathsf{Inl}\ x_l \Rightarrow B_l; \mathsf{Inr}\ x_r \Rightarrow B_r \xrightarrow{\oplus\varnothing;\ominus\varnothing} \lfloor B_l[x_l := L] \rfloor} \qquad \textsc{LCaseR}\ \frac{\cdots}{\cdots}$$

$$\textsc{LProj1}\ \frac{}{\mathsf{fst}\,(\mathsf{Pair}\ L_1\,L_2) \xrightarrow{\oplus\varnothing;\ominus\varnothing} L_1} \qquad \textsc{LProj2}\ \frac{\cdots}{\cdots} \qquad \textsc{LProjN}\ \frac{}{\mathsf{lookup}^i\,(L_1, \ldots, L_i, \ldots, L_n) \xrightarrow{\oplus\varnothing;\ominus\varnothing} L_i}$$

$$\textsc{LSend1}\ \frac{}{\mathsf{send}_{p^*}\,() \xrightarrow{\oplus\{(p,())\mid p\in p^*\};\ominus\varnothing} \bot} \qquad \textsc{LSendPair}\ \frac{\mathsf{send}_{p^*}\ L_1 \xrightarrow{\oplus\mu_1;\ominus\varnothing} \bot \quad \mathsf{send}_{p^*}\ L_2 \xrightarrow{\oplus\mu_2;\ominus\varnothing} \bot}{\mathsf{send}_{p^*}\,(\mathsf{Pair}\ L_1\,L_2) \xrightarrow{\oplus\{(p,\mathsf{Pair}\ L_1\,L_2)\mid p\in p^*\};\ominus\varnothing} \bot}$$

$$\textsc{LSendInL}\ \frac{\mathsf{send}_{p^*}\ L \xrightarrow{\oplus\mu;\ominus\varnothing} \bot}{\mathsf{send}_{p^*}\,(\mathsf{Inl}\ L) \xrightarrow{\oplus\{(p,\mathsf{Inl}\ L)\mid p\in p^*\};\ominus\varnothing} \bot} \qquad \textsc{LSendInR}\ \frac{\cdots}{\cdots} \qquad \textsc{LSendSelf}\ \frac{\mathsf{send}_{p^*}\ L \xrightarrow{\oplus\mu;\ominus\varnothing} \bot}{\mathsf{send}^*_{p^*}\ L \xrightarrow{\oplus\mu;\ominus\varnothing} L}$$

$$\textsc{LRecv}\ \frac{}{\mathsf{recv}_p\ L_0 \xrightarrow{\oplus\varnothing;\ominus\{(p,L)\}} L}$$

Figure 2.8: The semantics of $\boldsymbol{\lambda_L}$.

2.2.7 Endpoint Projection

Endpoint projection (EPP) is the translation between the choreographic language $\boldsymbol{\lambda_C}$ and the local process language $\boldsymbol{\lambda_L}$; necessarily it's parameterized by the specific local process you're projecting *to*. $[\![M]\!]_p$ is the projection of M to p, as defined in Figure 2.9. It does a few things: Most location annotations are removed, some expressions become $\bot$, $\bot$-based expressions are normalized by the floor function, and $\mathsf{com}_{s;r^+}$ becomes send_{r^+}, $\mathsf{send}^*_{r^+}$, or recv_s, keeping only the identities of the peer parties and not the local party.

$[\![M]\!]_p \triangleq$ by pattern matching on M:

$$
\begin{array}{rcl}
N_1 N_2 & \overset{\triangle}{\Longrightarrow} & \lfloor [\![N_1]\!]_p [\![N_2]\!]_p \rfloor \\
\mathsf{case}_{p^+}\ N\ \mathsf{of}\ \mathsf{Inl}\ x_l \Rightarrow M_l;\ \mathsf{Inr}\ x_r \Rightarrow M_r & \overset{\triangle}{\Longrightarrow} & \begin{cases} p \in p^+ & \overset{\triangle}{\Longrightarrow} \quad \lfloor \mathsf{case}\, [\![N]\!]_p\ \mathsf{of}\ \mathsf{Inl}\ x_l \Rightarrow [\![M_l]\!]_p; \mathsf{Inr}\ x_r \Rightarrow [\![M_r]\!]_p \rfloor \\ \text{else} & \overset{\triangle}{\Longrightarrow} \quad \lfloor \mathsf{case}\, [\![N]\!]_p\ \mathsf{of}\ \mathsf{Inl}\ x_l \Rightarrow \bot; \mathsf{Inr}\ x_r \Rightarrow \bot \rfloor \end{cases} \\
x & \overset{\triangle}{\Longrightarrow} & x \\
(\lambda x : T\,.\,N)@p^+ & \overset{\triangle}{\Longrightarrow} & \begin{cases} p \in p^+ & \overset{\triangle}{\Longrightarrow} \quad \lambda x\,.[\![N]\!]_p \\ \text{else} & \overset{\triangle}{\Longrightarrow} \quad \bot \end{cases} \\
()@p^+ & \overset{\triangle}{\Longrightarrow} & \begin{cases} p \in p^+ & \overset{\triangle}{\Longrightarrow} \quad () \\ \text{else} & \overset{\triangle}{\Longrightarrow} \quad \bot \end{cases} \\
\mathsf{Inl}\ V & \overset{\triangle}{\Longrightarrow} & \lfloor \mathsf{Inl} [\![V]\!]_p \rfloor \\
\mathsf{Inr}\ V & \overset{\triangle}{\Longrightarrow} & \lfloor \mathsf{Inr} [\![V]\!]_p \rfloor \\
\mathsf{Pair}\ V_1 V_2 & \overset{\triangle}{\Longrightarrow} & \lfloor \mathsf{Pair} [\![V_1]\!]_p [\![V_2]\!]_p \rfloor \\
(V_1, \ldots, V_n) & \overset{\triangle}{\Longrightarrow} & \lfloor ([\![V_1]\!]_p, \ldots, [\![V_n]\!]_p) \rfloor \\
\mathsf{fst}_{p^+} & \overset{\triangle}{\Longrightarrow} & \begin{cases} p \in p^+ & \overset{\triangle}{\Longrightarrow} \quad \mathsf{fst} \\ \text{else} & \overset{\triangle}{\Longrightarrow} \quad \bot \end{cases} \\
\mathsf{snd}_{p^+} & \overset{\triangle}{\Longrightarrow} & \begin{cases} p \in p^+ & \overset{\triangle}{\Longrightarrow} \quad \mathsf{snd} \\ \text{else} & \overset{\triangle}{\Longrightarrow} \quad \bot \end{cases} \\
\mathsf{lookup}^i_{p^+} & \overset{\triangle}{\Longrightarrow} & \begin{cases} p \in p^+ & \overset{\triangle}{\Longrightarrow} \quad \mathsf{lookup}^i \\ \text{else} & \overset{\triangle}{\Longrightarrow} \quad \bot \end{cases} \\
\mathsf{com}_{s;r^+} & \overset{\triangle}{\Longrightarrow} & \begin{cases} p = s, p \in r^+ & \overset{\triangle}{\Longrightarrow} \quad \mathsf{send}^*_{r^+ \setminus \{p\}} \\ p = s, p \notin r^+ & \overset{\triangle}{\Longrightarrow} \quad \mathsf{send}_{r^+} \\ p \neq s, p \in r^+ & \overset{\triangle}{\Longrightarrow} \quad \mathsf{recv}_s \\ \text{else} & \overset{\triangle}{\Longrightarrow} \quad \bot \end{cases}
\end{array}
$$

Figure 2.9: EPP from $\boldsymbol{\lambda_C}$ to $\boldsymbol{\lambda_L}$.

2.2.8 Process Networks

A single party evaluating local code can hardly be considered the ground truth of choreographic computation; for a message to be sent it must be received *by* someone (and *visa-versa*). Our third "language", $\boldsymbol{\lambda_N}$, is just concurrent asynchronous threads of $\boldsymbol{\lambda_L}$. An $\boldsymbol{\lambda_N}$ "network" $\mathcal{N}$ is a dictionary mapping each party in its domain to a $\boldsymbol{\lambda_L}$ program representing that party's current place in the execution. We express party-lookup as $\mathcal{N}(p) = B$. A singleton network, written $\mathcal{N} = p[B]$, has the one party p in its domain and assigns the expression B to it. Parallel composition of networks is expressed as $\mathcal{N} \mid \mathcal{N}'$ (the order doesn't matter). Thus, the following statements are basically equivalent:

- $\mathcal{N}(p) = B$
- $\mathcal{N} = p[B] \mid \mathcal{N}'$
- $p[B] \in \mathcal{N}$

When many compositions need to be expressed at once, we can write $\mathcal{N} = \Pi_{p \in p^+} p[B_p]$. Parallel projection of all participants in M is expressed as $[\![M]\!] = \Pi_{p \in \mathtt{roles}(M)} p[[\![M]\!]_p]$. For example, if p and q are the only parties in M, then $[\![M]\!] = p[[\![M]\!]_p] \mid q[[\![M]\!]_q]$.

The rules for $\boldsymbol{\lambda_N}$ semantics are in Figure 2.10. $\boldsymbol{\lambda_N}$ semantic steps are annotated with *incomplete* send actions; $\mathcal{N} \xrightarrow{p:\{\ldots,(q_i,L_i),\ldots\}} \mathcal{N}'$ indicates a step in which p sent a respective L_i to each of the listed q_i and the q_is have *not* been noted as receiving. When there are no such incomplete sends and the p doesn't matter, it may be omitted (*e.g.* $\mathcal{N} \xrightarrow{\varnothing} \mathcal{N}'$ instead of $\mathcal{N} \xrightarrow{p:\varnothing} \mathcal{N}'$). **Only $\varnothing$-annotated steps are "real";** other steps are conceptual justifications used in the semantics's derivation trees. In other words, $\boldsymbol{\lambda_L}$ semantics only elevate to $\boldsymbol{\lambda_N}$ semantics when the message-annotations cancel out. Rule NCom allows annotations to cancel out. For example the network $[\![\mathsf{com}_{s;\{p,q\}}()@\{s\}]\!]$ gets to $[\![()@\{p,q\}]\!]$ by a *single* NCom step. The derivation tree for that step starts at the top with NPro: $s[\mathsf{send}_{\{p,q\}}()] \xrightarrow{s:\{(p,()),(q,())\}} s[\bot]$; this justifies two nestings of NCom in which the p step and q step (in either order) compose with the s step and remove the respective party from the step-annotation.

$$\textsc{NPro}\ \frac{B \xrightarrow{\oplus\mu;\ominus\varnothing} B'}{p[B] \xrightarrow{p:\mu} p[B']} \qquad \textsc{NCom}\ \frac{\mathcal{N} \xrightarrow{s:\mu\cup\{(r,L)\}} \mathcal{N}' \quad B \xrightarrow{\oplus\varnothing;\ominus\{(s,L)\}} B'}{\mathcal{N} \mid r[B] \xrightarrow{s:\mu} \mathcal{N}' \mid r[B']} \qquad \textsc{NPar}\ \frac{\mathcal{N} \xrightarrow{\varnothing} \mathcal{N}'}{\mathcal{N} \mid \mathcal{N}^{+} \xrightarrow{\varnothing} \mathcal{N}' \mid \mathcal{N}^{+}}$$

Figure 2.10: Semantic rules for $\boldsymbol{\lambda_N}$.

2.2.9 Deadlock Freedom

Above we introduced the necessary machinery of EPP and evaluation of a network of communicating processes. One of the advantages of choreogrphic programming is that a user can typically ignore this distributed computational setting, and just reason about their programs in a single-threaded way, *i.e.* under the centralized semantics of $\boldsymbol{\lambda_C}$. Such an andvantage only holds water if EPP to $\boldsymbol{\lambda_N}$ is sound and complete with respect to $\boldsymbol{\lambda_C}$; Theorems 4 and 5 show that it is.

Theorem 4 (Soundness)**.** *If* $\Theta; \varnothing \vdash M : T$ *and* $[\![M]\!] \xrightarrow{\varnothing}{}^{*} \mathcal{N}_n$*, then there exists* M' *such that* $M \longrightarrow^{*} M'$ *and* $\mathcal{N}_n \xrightarrow{\varnothing}{}^{*} [\![M']\!]$.

Theorem 5 (Completeness)**.** *If* $\Theta; \varnothing \vdash M : T$ *and* $M \longrightarrow M'$*, then* $[\![M]\!] \xrightarrow{\varnothing}{}^{*} [\![M']\!]$.

In Appendix A.4 we prove Theorem 4, which says that any behavior possible for the $\boldsymbol{\lambda_N}$ projection of a choreography is also possible in the original $\boldsymbol{\lambda_C}$. In Appendix A.5 we prove Theorem 5, which says that any behavior possible in $\boldsymbol{\lambda_C}$ is also possible in the $\boldsymbol{\lambda_N}$ projection.

A foundational promise of choreographic programming is that participants in well-formed choreographies will never get stuck waiting for messages they never receive. This important property, *"deadlock freedom by design"*, is trivial once our previous theorems are in place.

Corollary 1 (Deadlock Freedom)**.** *If* $\Theta; \varnothing \vdash M : T$ *and* $[\![M]\!] \xrightarrow{\varnothing}{}^{*} \mathcal{N}$*, then either* $\mathcal{N} \xrightarrow{\varnothing}{}^{*} \mathcal{N}'$ *or for every* $p \in \texttt{roles}(M)$*,* $\mathcal{N}(p)$ *is a value.*

This follows from Theorems 2 to 5.

2.3 Comparisons with other systems

In this section we compare recent choreography languages to λ_C, primarily in terms of how their KoC strategies impact communication efficiency. By "communication efficiency" we refer to the amount of information sent from each party to each other party in a choreography acomplishing some desired global behavior or end state.

For readability, we render λ_C examples in this section as plain-text. We use `fn` for λ, `=>` for ⇒, `->` for →, and `*` for ×. The annotations on lambdas, unit, and keyword functions are given as comma-separated lists in square brackets (*e.g.* `lookup[2][p_1,p_2,q]` and `com[s][r_1]`). Furthermore, we sugar our syntax with let-binding, *e.g.* $(\lambda var : T\,.\,M)@\Theta V$ is rendered as `let var : T = V; M`, and often we'll omit the type annotation `T`. We elide declarations of contextual functions and data types in our examples. We allow expressions in place of values, which can be de-sugared to temp variables. Some of the languages we compare against include polymorphic functions in their examples; we annotate such function names in our comparison code, similar to how our built-ins like `fst` get annotated.

2.3.1 HasChor

HasChor is a Haskell library for writing choreographies as values of a monad `Choreo` (Shen et al. 2023). The implementation is succinct and easy to use. HasChor does not have `select` statements; KoC is handled by broadcasting branch-guards to all participants in the choreography. This is not efficient. The choreography in Figure 1.3*(a)* is a translation into MultiChor of an example from (Shen et al. 2023), and shows explicitly the redundant communication that's implicit in HasChor choreographies. Figure 2.11 shows a λ_C version of the amended choreography from Figure 1.3*(b)*.

2.3.2 Pirouette

Pirouette (Hirsch and Garg 2022) is a functional choreographic language. It uses the select-&-merge KoC strategy formalized in (Carbone and Montesi 2013): a branching party sends flag symbols to peers who need to behave differently depending on the branch. These `select` statements are written explicitly by the user and can be quite parsimonious. Only if, and not until, the EPPs of the parallel program branches are different for a given user does that user need to be sent a `select`. EPP of an `if` statement uses a "merge" operation

```
1  (fn request : (PutRequest + GetRequest)@[client] .
2    let request_ = com[client][primary] request;
3    let req = com[primary][primary, backup] request_;
4    let _ = case[primary, backup] req of
5      Inl _put => let _ack = com[backup][primary] (handleRequest@[backup] req);
6                  ()@[primary, backup];
7      Inr _get => ()@[primary, backup];
8    let response : Response@[primary] = handleRequest@[primary] request_;
9    com[primary][client] response
10 )@[client, primary, backup]
```

This choreography is represented as a function from a Sum-Type located at `client` (`request` on line 1) to some unspecified "response" type also located at `client` (the return type of `com[_][client]`, line 9). The census annotation follows the function body (line 10). `request`, `request_`, and `req` all contain the same data, but have different owners (respectively, `[client]`, `[primary]`, and `[primary,backup]`). The `case` expression (line 4) explicitly enclaves to the sub-census `[primary,backup]`. Although the choreography looks (and in practice would execute) very much like the MultiChor version in Figure 1.3*(b)*, the actual semantics does not use a monad; this representation would de-sugar to a nesting of lambda abstractions and applications.

Figure 2.11: A λ_C choreography implementing the same KVS as in Figure 1.3.

to combine program branches that are not distinguishable to a given party. `select` statements project as the `offer` and `choose` operations from multiparty-session-types.

The "merge" function is partial; if needed `select`s are missing from a program then EPP can fail because the merge of the EPPs of two paths is undefined. Pirouette's type system doesn't detect this; to check if a Pirouette program is well-formed one must do all of the relevant endpoint projections. (All select-&-merge systems we've investigated work this way.) (Hirsch and Garg 2022) provide a standalone implementation of Pirouette and Coq proofs of their theorems.

`select` gives good communication efficiency because not every choice needs to be communicated, but it has a limitation in common with HasChor. The `select` flags can't be used as data, and the Knowledge of Choice they communicate can't be recycled in subsequent conditionals. Figure 2.12 shows a λ_C choreography with sequential branches: on lines 2 and 7 `alice` and `bob` branch on their shared MLV `choice`. To represent this behavior in Pirouette without redundant messages, the sequential conditionals must be combined and Carroll's actions that happen in between (lines 5 and 6) must be duplicated in each branch. This is shown in Figure 2.13; Notice that Carroll is never informed which branch she is in; her actions are the same in each case. We believe Pirouette's communication efficiency is as good as λ_C's, but scaling the above strategy for combining sequential conditionals across a large codebase could be challenging.

```
let choice : ()+()@[alice, bob] = com[alice][alice, bob] alices_choice;
let query : Query@[alice] = case[alice, bob] choice of
  Inl _ => com[bob][alice] bobs_query;
  Inr _ => alices_query;
let answerer : (Query@[carroll] -> Response@[carroll])@[carroll] = carrolls_func;
let response = com[carroll][bob, alice] (answerer (com[alice][carroll] query));
case[alice, bob] choice of
  Inl _ => bobs_terminal response;
  Inr _ => alices_terminal response;
```

Figure 2.12: A λ_C implementation of a two-client one-server choreography involving sequential branches. Client `bob` may delegate a query against server `carroll`, or client `alice` may provide the query herself.

```
if alice.choice
  then alice[L] ~> bob;
       bob.bobs_query ~> alice.query;
       alice.query ~> carroll.query;
       carroll.(answerer(query)) ~> bob.response;
       carroll.(answerer(query)) ~> alice.response;
       bob.(terminal response)
  else alice[R] ~> bob;
       alice.alices_query ~> carroll.query;
       carroll.(answerer(query)) ~> bob.response;
       carroll.(answerer(query)) ~> alice.response;
       alice.(terminal response)
```

Figure 2.13: A Pirouette implementation of the client-server-delegation choreography in Figure 2.12

2.3.3 Chorλ

Chorλ (Cruz-Filipe et al. 2022) is a functional choreographic language. The API and communication efficiency are similar to (Hirsch and Garg 2022) and (Giallorenzo et al. 2024), but (Cruz-Filipe et al. 2023) shows that Chorλ's semantics and typing can additionally support structures called *Distributed Choice Types*. A multiply-located `()@[p,q]` is isomorphic to a tuple of singly-located values `(()@p, ()@q)`. Distributed Choice Types extend this isomorphism to cover the entire algebra of Unit, Sum, and Product types in such a way that `p` and `q` never disagree about the value they each have. Specifically a multiply-located `(A + B)@[p,q]` becomes a singly-located `((A@p, A@q)+(B@p, B@q))`, a type which earlier systems do not support. [3]

Chorλ's "merge" operator supports branching on distributed choice types, so Chorλ can always match λ_C's communication efficiency with a similar program structure by declaring the needed `multicast` functions. The language still needs to support `select` (because Chorλ has no other way of implementing `multicast`), so well-formed-ness checking still depends on the partial function "merge".

Considering the other direction, λ_C can likewise match the communication efficiency of Chorλ and other `select`-based languages. Typically, this is as simple as multicasting the branch guard to all parties that would have received a `select` (and to oneself, the original branching party). In other situations a party might participate in branches without receiving a `select` because they don't need to know which one they are in; this is handled with the reverse of the transformation we showed between Figures 2.12 and 2.13

A fully-general algorithmic translation that never compromises on communication efficiency won't maintain the program's structure. The strategy is as follows:

- An expression M involving a party p who doesn't have KoC gets broken into three parts:
  - A computation N_1 of a cache data structure containing all variables bound up until the first part of M at which p actually does something.
  - A sub-expression N_2 involving p. p might be sending a message, receiving a message, receiving a `select`, or doing local computation.

[3] It should not be assumed that Chorλ is the last word in abstract models for the select-&-merge paradigm. Their `com` operator is defined for arbitrary arguments including functions; depending whether that's an aproperate defintion, `com` itself may not even be necessary.

  - A computation N_3 that unpacks the cache from N_1 and (possibly) the results from N_2 and proceeds with the *continuation*, the remainder of M. Note that N_3 will still need to undergo similar translation.

- Since there's KoC that p doesn't have, M must be a branch of a `case`. Since the original program was projectable, the other branch must have a similar breakdown *with the same* N_2 *middle part*. N_1, wrapped in a respective Inl or Inr, replaces M in the case statement. Depending if N_2 is to or from p, the branches of the new `case` may also have to provide the argument to N_2, but this should *not* be wrapped in a Sum Type.

- If N_2 is a `select` operation, then it gets translated into a multicast. Its argument, provided by the preceding `case`, will be $\mathsf{Inl}()@q^+$ or $\mathsf{Inr}()@q^+$ depending on the symbol `select`ed[4], where q^+ are the parties who already have KoC. Then $\{p\} \cup q^+$ branch together on the multicast flag. The N_3 continuations will be handled in duplicate in both of the flag-branches; this will often involve dead branches for which applicable caches or behavior do not exist. Since these branches will never be hit, it's safe to populate them with default values of the appropriate type.

- Otherwise, sequencing of N_2 after the N_1-generating `case` is straightforward.

- To handle the N_3 continuations, branch on the cache value (which was wrapped in a Sum Type). In each branch, unpack the cached variables (and bind the results of N_2 if needed) and proceed with recursive translation of the continuation.

Neither (Cruz-Filipe et al. 2022) nor (Cruz-Filipe et al. 2023) contain examples requiring such a complicated translation. Figure 2.14 shows a made-up Chorλ choreography; translating it into $\boldsymbol{\lambda_C}$ without compromising communication efficiency is more involved than earlier examples were. Figure 2.15 shows it's translation via the steps described above; the code is intermediate in verbosity between an actual machine-generated translation and a thoughtful human reimplementation.

We believe that, while select-&-merge languages like Chorλ are equivalent in expressivity and communication efficiency to enclaves-&-MLVs languages like $\boldsymbol{\lambda_C}$, $\boldsymbol{\lambda_C}$'s syntax and semantics are more user-friendly

[4] Chorλ supports arbitrary symbols for `select`, but since we're concerned with bit-level efficiency we assume the only symbols are `L` and `R`.

for most software engineering purposes. In the following chapter we present an eDSL implementation of enclave-&-MLVs choreographic programming, and demonstrate its use.

```
case ( first_secret[p] ()@p ) of
  Inl _ => case ( second_secret[p] ()@p ) of
             Inl _ => let w = com[q][p] n_q1;
                      select[p][q] L;
                      let _ = com[p][q] (w + 1@p);
                      w + 1@p;
             Inr _ => let w = com[q][p] n_q1;
                      let y = 2@p;
                      select[p][q] L;
                      let _ = com[p][q] (w + y);
                      w;
  Inr _ => let w = com[q][p] n_q1;
           case (second_secret[p] ()@p ) of
             Inl s => select[p][q] L;
                      let _ = com[p][q] 5@p;
                      s;
             Inr _ => select[p][q] R;
                      let z = com[q][p] n_q2;
                      w + z;
```

Figure 2.14: A contrived Chorλ choreography that is complicated to efficiently translate into $\boldsymbol{\lambda_C}$.

```
let m1 = com[q][p] n_q1;
let (cache1, flag1) = case ( first_secret[p] ()@[p] ) of
  Inl _ => let (c1_, f1_) = case ( second_secret[p] ()@[p] ) of
              Inl _ => let w = m1;
                       (Inl w, Inl ()@[p]);
              Inr _ => let w = m1;
                       let y = 2@p;
                       (Inr (Pair w y), Inl ()@[p]);
           (Inl c1_, f1_);
  Inr _ => let (c1_, f1_) = let w = m1;
                            case ( second_secret[p] ()@[p] ) of
                              Inl s => (Inl (Pair w s), Inl ()@[p]);
                              Inr _ => (Inr w, Inr ()@[p]);
           (Inr c1_, f1_);
let f1_ = com[p][p,q] flag1;
case f1_ of Inl _ => let (cache2, m2) = case cache1 of
                        Inl c1l => let (c2_, m2_) = case c1l of
                                     Inl c1ll => let w = c1ll;
                                                 (Inl w, w + 1@[p]);
                                     Inr c1lr => let (Pair w y) = c1lr;
                                                 (Inr (Pair w y), w + y);
                                   (Inl c2_, m2_);
                        Inr c1r => let (c2_, m2_) = case c1r of
                                     Inl c1rl => let (Pair w s) = c1rl;
                                                 (Pair w s, 5@[p]);
                                     Inr c1rr => (DEFAULT, DEFAULT); # DEAD BRANCH
                                   (Inr c2_, m2_);
                    let _ = com[p][q] m2;
                    case cache2 of
                      Inl c2l => case c2l of
                        Inl c2ll => let w = c2ll;
                                    w + 1@[p];
                        Inr c2lr => let (Pair w y) = c2lr;
                                    w;
                      Inr c2r => let (Pair w s) = c2r;
                                 s;
           Inr _ =>  let cache2 = case cache1 of
                       Inl c1l => DEFAULT; # DEAD BRANCH
                       Inr c1r => case c1r of
                         Inl c1rl => DEFAULT; # DEAD BRANCH
                         Inr c1rr => let w = c1rr;
                                     w;
                     let m2 = com[q][p] n_q2;
                     let w = cache2;
                     let z = m2;
                     w + z
```

Figure 2.15: An algorithmic λ_C translation of the choreography from Figure 2.14.

Bibliography

Bates, M., S. Kashiwa, S. Jafri, G. Shen, L. Kuper, and J. P. Near (2024). Efficient, portable, census-polymorphic choreographic programming.

Carbone, M. and F. Montesi (2013). Deadlock-freedom-by-design: multiparty asynchronous global programming. In *Proceedings of the 40th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '13, New York, NY, USA, pp. 263–274. Association for Computing Machinery.

Cruz-Filipe, L., E. Graversen, L. Lugović, F. Montesi, and M. Peressotti (2023). Modular Compilation for Higher-Order Functional Choreographies. In K. Ali and G. Salvaneschi (Eds.), *37th European Conference on Object-Oriented Programming (ECOOP 2023)*, Volume 263 of *Leibniz International Proceedings in Informatics (LIPIcs)*, Dagstuhl, Germany, pp. 7:1–7:37. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

Cruz-Filipe, L., E. Graversen, L. Lugović, F. Montesi, and M. Peressotti (2022, September). *Theoretical Aspects of Computing*, Volume 13572 of *Lecture Notes in Computer Science*, Chapter Functional choreographic programming, pp. 212–237. Tbilisi, Georgia: Springer.

Giallorenzo, S., F. Montesi, and M. Peressotti (2024, jan). Choral: Object-oriented choreographic programming. *ACM Trans. Program. Lang. Syst. 46*(1).

Hirsch, A. K. and D. Garg (2022, January). Pirouette: higher-order typed functional choreographies. *Proc. ACM Program. Lang. 6*(POPL).

Kashiwa, S., G. Shen, S. Zare, and L. Kuper (2023). Portable, efficient, and practical library-level choreographic programming.

Shen, G., S. Kashiwa, and L. Kuper (2023, aug). Haschor: Functional choreographic programming for all (functional pearl). *Proc. ACM Program. Lang. 7*(ICFP).

Urban, C., S. Berghofer, and M. Norrish (2007). Barendregt's variable convention in rule inductions. In F. Pfenning (Ed.), *Automated Deduction – CADE-21*, Berlin, Heidelberg, pp. 35–50. Springer Berlin Heidelberg.

Chapter 3

Real World Choreographic Programming

3.1 Introduction

In this chapter we demonstrate the practicality of enclaves-&-MLVs choreographic programming by presenting our implementation: the MultiChor Haskell library. MultiChor is a "just a library" CP system in the style of HasChor. We adopt HasChor's freer-monads and handlers design pattern, and embed the key aspects of λ_C's type system as type-level constraints with a bespoke proof-witness system.

A key innovation of λ_C is that KoC is enforced entirely by type-level management of the census. By representing the census as a type-level variable in Haskell, MultiChor enables polymorphism over both the size and membership of the census, a feature not considered in the construction of λ_C. All Haskell typing happens statically, and MultiChor's EPP happens at runtime (like HasChor's). This means that, like other cases of polymorphism in Haskell, location polymorphism in MultiChor must be resolved statically.

A few other desiderata motivate our implementation:

1. It should be possible to broadcast, *i.e.* to multicast a value to the entire census, and to use values known to the entire census as normal (un-located) values of their type.

2. It should be possible to know from an appropriately-written choreography's type that some certain party or parties are not involved, are not in its census. Users should be able to embed such "enclave" choreographies inside choreographies with larger, possibly polymorphic, censuses.

3. The type system should be able to reason about parties' membership in a census or ownership-set with normal subset reasoning.

The choreography in Figure 3.1 showcases the above points. The census of the whole program appears in the type and does not specify who the players are. The `enclaveTo` on line 18 embeds a choreography whose census is exactly the monomorphic `"dealer"` and a polymorphic `player` (#2). The helper-function `broadcast` on line 19 functions as described in #1. Many examples of #3 are automated or hidden in MultiChor, but on line 19 the function `inSuper` is applied to `players :: Subset players ("dealer" : players)` and `player :: Member player players` to attest that `player` is present in the census.

```
1  game :: forall players m. (KnownSymbols players) => Choreo ("dealer" ': players) (CLI m) ()
2  game = do
3    let players = consSuper (refl @players)
4        dealer = listedFirst @"dealer"    -- listedFirst is just First with the type-arguments rearranged.
5        everyone = refl @("dealer" ': players)
6    hand1 <- (fanIn everyone \(player :: Member player players) -> do
7        card1 <- locally dealer (\_ -> getInput ("Enter random card for " ++ toLocTm player))
8        (dealer, card1) ~> everyone
9      ) >>= naked everyone
10   wantsNextCard <- parallel players \_ _ -> do
11       putNote $ "All cards on the table: " ++ show hand1
12       getInput "I'll ask for another? [True/False]"
13   hand2 <- fanOut \(player :: Member player players) ->
14     enclave (inSuper players player @@ dealer @@ nobody) do
15         let dealer = listedSecond @"dealer"
16         choice <- broadcast (listedFirst @player, localize player wantsNextCard)
17         if choice then do
18             cd2 <- locally dealer (\_ -> getInput (toLocTm player ++ "'s second card:"))
19             card2 <- broadcast (dealer, cd2)
20             return [getLeaf hand1 player, card2]
21         else return [getLeaf hand1 player]
22   tblCrd <- locally dealer (\_ -> getInput "Enter a single card for everyone:")
23   tableCard <- (dealer, tblCrd) ~> players
24   void $ parallel players \player un -> do
25       let hand = un player tableCard : viewFacet un player hand2
26       putNote $ "My hand: " ++ show hand
27       putOutput "My win result:" $ sum hand > card 19
```

Figure 3.1: A card game expressed as a choreography written in MultiChor. This choreography is polymorphic over the number and identity of the players, but the party named `"dealer"` is an explicit member. The inner monad `CLI` that all parties have access to is a simple freer monad that can be handled to IO operations, or as `State` for testing purposes. The `newtype Card` encapsulates the modulo operation in its `Num` instance.

3.2 Censuses, Enclaves, and MLVs in Haskell

MultiChor uses the same free-monad approach as HasChor (Shen et al. 2023) to implement choreographic programming, EPP, and the final interpretation to a real communication mechanism. Also like HasChor, MultiChor's `Choreo` monad is parameterised by a *local monad* in which parties' local computations can be expressed. A MultiChor type `Located ps t` is a multiply-located `t` owned by the parties `ps`. It is possible to write MultiChor functions that look and work like each of HasChor's three primitive operators, but the derived API in which users write MultiChor choreographies contains a clear analog of only one of HasChor's primitives. Haskell's monadic-`do` notation and purity-oriented type system make MultiChor code concise and safe (in the sense that users are unlikely to accidentally invalidate important invariants).

As explained in Section 2, our KoC strategy requires that the correctness (well-typed-ness) of choreographies be judged in the context of a census. MultiChor adds the census as a type parameter of the `Choreo` monad. Its kind is `[Symbol]`, which is to say that the census is a type-level list of parties and parties are type-level strings. `Choreo` is *not* an *indexed* monad (that is, executing a monadic operation doesn't change the census), but monadic operations can take choreographies with smaller censuses as arguments.

```
1  locally' :: (KnownSymbol l) => (Unwrap l -> m a) -> Choreo '[l] m a
2
3  congruently' :: (KnownSymbols ls) => (Unwraps ls -> a) -> Choreo ls m a
4
5  broadcast' :: (Show a, Read a, KnownSymbol l) =>
6                Member l ps -> (Member l ls, Located ls a) -> Choreo ps m a
7
8  enclave :: (KnownSymbols ls) => Subset ls ps -> Choreo ls m a -> Choreo ps m (Located ls a)
```

Figure 3.2: The fundamental operators for writing expressions in MultiChor's `Choreo` monad. Of these four operators, `enclave` is the only one users will usually call directly; the other three can combine with each other (and with `enclave`) to make more user-friendly alternatives.

The fundamental operations of MultiChor's `Choreo` monad are `enclave`, `broadcast'`, `locally'`, and `congruently'`. Their type signatures are given in Figure 3.2. Like in HasChor, these are free-monad constructors; their behavior is implemented in interpreters that carry out EPP or implement a centralized semantics. Three of them have their names "primed" because the un-primed versions of these names are reserved for more ergonomic derived functions. For example, `locally'` takes a single argument, a computation in the local monad, and requires that the census contains *a single party*, who will execute that

computation. The un-primed `locally` takes an additional argument that identifies a single party from a larger census; it uses `enclave` to correctly call `locally'`. `broadcast` shares a **`Located`** value with the entire census so the unwrapped value can be used; by combining this with `enclave` we can implement point-to-point or multicast communication. From the perspective of a centralized semantics, `enclave` doesn't do anything at all besides run the sub-choreography, but EPP to a party *not* in the sub-census skips the sub-choreography and just returns **`Empty`**.

`congruently` lets us leverage MLVs to concisely write actively-replicated computations. In contrast to `locally`, the computation is performed by multiple parties and the result is multiply-located across all of them.[1] For the execution of these actively-replicated computations to correctly return an MLV, all the parties must be guaranteed to be doing a pure computation on the same data. Haskell makes it easy to enforce such a guarantee to a practical (but not unbreakable) extent. This is why `congruently` does not grant access to the local monad `m`. It also requires that the computation not have access to the specific identity of the computing party, unlike `locally` and the similar-looking function `parallel` mentioned in Section 3.4. Weakening (or subverting) these restrictions would allow a user to violate MultiChor's invariant that MLVs (**`Located`** values) have the same value across all their owners.

It is critical to the safety of MultiChor that the projection of a choreography to any given party will not use any other party's **`Located`** values. We use the same basic strategy for this as HasChor: **`Located`**'s constructors, **`Wrap`** and **`Empty`**, are hidden inside the core module and afforded only by dependency injection to `locally` and `congruently`. The specific "unwrapper" functions afforded to `locally` and `congruently` are known to user code only by their type signatures, which have respective aliases **`Unwrap`** and **`Unwraps`**. **`Located`**'s constructors are also used by two less-critical functions, `flatten` and `othersForget`. These are needed for shrinking ownership sets or un-nesting **`Located`** values; they could be written using `congruently`, but by implementing them in the core module where they can pattern-match **`Located`** values we are able to make them not-monadic, and so more convenient.

[1] The entire census participates in the primed version, and its result is returned naked. The behavior of `enclave` and the more fundamental rules of monadic programming ensure the un-primed `congruently` behaves correctly.

3.3 Membership Constraints

It is not trivial for Haskell's type-checker (a component of GHC, the compiler) to judge if a particular participant owns a multiply-located value or is present in a particular census when the party or the set are polymorphic. Declaring membership and subset relations as class constraints can work in some situations, but this strategy has serious limitations which we find unacceptable. For example, a rule as obvious as $(p \in ps_1 \wedge ps1 \subseteq ps_2) \rightarrow p \in ps_2$, represented in Haskell as `instance ( IsMember p ps1, IsSubset ps1 ps2) => IsMember p ps2`, would be impossible to use because the compiler has no way of guessing which set `ps1` it should be checking `p`'s membership in (and even if it could *guess*, it wouldn't backtrack and try a different guess if its first try didn't work).

To work around such limitations, MultiChor uses a strategy of *proof witnesses* like those described by (Noonan 2018). These are vacuous runtime values with specially crafted types, such that the existence of a value of the given type guarantees the truth of some logical assertion. We do not actually use the `gdp`[2] package; we found that writing our own purpose-specific system had a few advantages. First, we were able to write everything we needed without hand-waving any foundations as `axiom`s. Second, pattern matching against the constructors of `Member l ls` suffices to convince GHC that `ls` is not empty, which is sometimes useful. Finally, the implicit paradigm of "memberships as indices & subsets as functions" was qualitatively easier to work with when we were building the census-polymorphism tools described in Section 3.4.

In MultiChor, locations are identified by type-level strings, uninhabited types with "kind" `Symbol`. A values of type `Member p ps` can be used both as proof that `p` is eligible to take some action (because of their membership in `ps`) and as a term-level identifier for the party `p`. It's actual form will be that of an index in the type-level list `ps` at which `p` appears. Subset relations are expressed and used similarly. A value of type `Subset ps qs` has the underlying form of a function from `Member p ps` to `Member p qs`, *universally quantified over* `p`. Because these logical structures can be built from scratch inside Haskell's type system, all of the machinery we use to do so can safely be exposed to end-users so that they can write their own proofs, as needed, inside choreographies. In practice however, they will usually use higher-level operators.

[2] "Ghosts of Departed Proofs" (Noonan 2019)

For example, the pattern `p @@ nobody`, read as *" `p` and nobody else"*, makes a `Subset '[p] ps` out of a `Member p ps`.

3.4 Census Polymorphism

So far, the example choreographies we have discussed have had fixed numbers of participants. In all prior CP systems this has been a syntactic constraint: even systems that allow polymorphism over the identities of participants require the participants' "roles" to be explicitly defined in-context. This is a serious limitation for writing choreographic software; modern concurrent systems often use dozens to thousands of participants and are defined parametrically over their number of participants (Beck et al. 2023, Corrigan-Gibbs and Boneh 2017, Wu et al. 2020, Bonawitz et al. 2017, Keeler et al. 2023). We assert that such parametric protocol declarations are a required feature for CP to find mainstream use; our systems provide it in the form of *census polymorphism*.

By "census polymorphism", we mean that a choreographic expression is polymorphic over its census type-variable, including not just the specific identities listed but also the quantity.[3] Naïvely, this is trivial; any MultiChor expression can easily be written with a type variable as its census and the relevant parties (whose exact identities can also be polymorphic) can be guaranteed to be present by taking membership proofs as arguments. However, this approach has a limitation: Since the number of type variables of a choreography must be fixed and there is no way to *explicitly list* a variable number of parties, it follows that there may be parties in the census who are not identified by the proof arguments. Such un-enumerated parties will receive any broadcasts and participate in any active replication that applies to the whole census, but there's no way to specify them as the senders of messages, nor is there any way to specify that they should receive a message except by broadcasting it. For this reason, when we speak of "census polymorphism", we mean *useful* polymorphism that lets an unspecified quantity of parties actively participate in the choreography. For example one might wish to write a `gather` operation in which a polymorphic list of participants each send a computed value to a common recipient who aggregates them. Figure 3.3 shows an example MultiChor choreography for a key-value store with a polymorphic list of backup servers. In Section 3.5 we implement the GMW protocol (Goldreich et al. 2019), a foundational protocol in multi-party cryptography.

[3] In principle, one can split hairs between census polymorphism and similar polymorphism over other sets of parties, *e.g.* ownership sets. We have not found such distinctions to be useful for describing system capabilities, but they can be relevant when talking about the type of a given expression.

In earlier CP systems it would have been necessary to hard-code the number of participants when writing such choreographies; Census polymorphism is precisely the absence of such a restriction. Census polymorphism is achieved in MultiChor library by type-level programming in modern Haskell.

```
1  handleRequest :: forall backups. (KnownSymbols backups)
2                => Located '["primary"] Request
3                -> (Located '["primary"] (IORef State), Faceted backups '[] (IORef State))
4                -> Choreo ("primary" ': backups) IO (Located '["primary"] Response)
5  handleRequest request (primaryStateRef, backupsStateRefs) = broadcast (primary, request) >>= \case
6      Put key value -> do oks <- parallel backups \backup un ->
7                                    handlePut (viewFacet un backup backupsStateRefs) key value
8                          gathered <- gather backups (primary @@ nobody) oks
9                          locally primary \un -> if all isOk (un primary gathered)
10                                               then handlePut (un primary primaryStateRef) key value
11                                               else return errorResponse
12     Get key -> locally primary \un -> handleGet (un primary primaryStateRef) key
13   where primary = listedFirst ; backups = consSuper refl
14
15 kvs :: forall backups. (KnownSymbols backups)
16     => Located '["client"] Request
17     -> (Located '["primary"] (IORef State), Faceted backups '[] (IORef State))
18     -> Choreo ("client" ': "primary" ': backups) IO (Located '["client"] Response)
19 kvs request stateRefs = do
20     request' <- (client, request) ~> primary @@ nobody
21     response <- enclave (primary @@ backups) (handleRequest request' stateRefs)
22     (primary, flatten (First @@ nobody) (First @@ nobody) response) ~> client @@ nobody
23   where client = listedFirst ; primary = listedSecond ; backups = consSuper $ consSuper refl
```

Figure 3.3: A key-value store choreography with an unspecified number of backup servers. The main action happens in `handleRequest`, a choreography involving only the servers which is called via `enclave` on line 21. `handleRequest`'s census explicitly includes the primary server, but is polymorphic over the list of backup servers. The primary server broadcasts the request (line 5–12); the backups will update their state and report their health only for a `Put` request. On line 7 the backups call the local IO function `handlePut` in `parallel` using their individual state references; `oks` is therefore a `Faceted backups '[] Response`. (The extra `'[]` denotes that no party yet knows all of the `oks`.) `gather` (line 8) communicates all the `oks` to the primary server where they're stored as a `Quire backups Response`. If all the backups are ok, then the primary server also handles the request (line 10).

3.4.1 Loops, Facets, and Quires

The first thing that is necessary is a way to loop over a polymorphic list of parties. Census polymorphism as discussed in this work is *static*, *i.e.*, while one can write choreographies and choreographic functions that are census-polymorphic, it is always possible in principal to unroll the top-level choreography (that actually gets compiled) into a monomorphic form before you actually run anything. In Section 3.4.2 we discuss MultiChor's `sequenceP`, a runtime loop over statically-defined type level lists.

Less flexible options would still be viable. The most recent versions of ChoRus and ChoreoTS lack constructs analogous to `sequenceP`, and instead offer the pair of functions `fanOut` and `fanIn` (Bates et al. 2024). These are both "for loops" over parties; `fanOut`'s return type is a heterogeneous structure of the returned values for each looped-over party (see next paragraph) and `fanIn` works similarly except the owners of the aggregated data do not vary over the loop. It's an open question whether the additional flexibility of MultiChor's approach has any real-world use! We also conjecture that even more restricted implementations would suffice for a majority of use-cases, specifically by offering the three operations `scatter`, `gather`, and `parallel`. `scatter` is multi-cast operation in which a distinct value is sent to each recipient, and `gather` is its dual. `parallel` is exactly like `locally`, except a list of parties execute the local computation in parallel. In MultiChor, these are derived operations, and we use them frequently in our case studies.

The second thing required for useful census polymorphism is the ability to express and use divergent data known by un-enumerated parties. We call such data structures *faceted values*[4]. (They're basically the same as the faceted values introduced in (Austin and Flanagan 2012), except their public facet is always "⊥" and multiple parties have distinct private facets.) Conceptually, a faceted value is similar to an MLV, in that it projects to an owner as a simple value and to a non-owner as a placeholder, but different owners of a faceted value will have different values for it. To see the need for faceted values, consider how one would express a census-polymorphic `gather` operation using only a type-level `for`-loop: The argument couldn't simply be a list, because `Located` values with different owners have different types. Each sender would need to generate its value to send *inside* the loop body, and the only way for the sent values to be distinct would be by using private local state accessed by `locally`. This would hardly be satisfying, and the dual case of `scatter` would be even worse: Any use to which the received values were to be put would also have to fit inside the body of the `for`-loop. Again, one couldn't simply append the `scatter`ed values to a list and return it because (in Haskell) all the values in a list must have the same type.

The dual of a faceted value is a "quire"[5], a vector of values indexed by type-level parties. Quires are not inherently located, but they can be located the same way as any other data structure. For example, the return type of `gather` is `Located recipients (Quire senders a)`.

[4]The word "faceted" is most commonly used in reference to a cut gemstone, but analogy to the facets of polyhedral playing dice might be more on-the-nose.

[5]"Quire" is pronounced "choir"; it rhymes with "buyer" and means "a stack of sheets of paper, all cut to the same size". Each individual piece of paper is a "leaf".

3.4.2 Census Polymorphism in MultiChor

We leverage the type system of modern Haskell to achieve useful census polymorphism in MultiChor. This behavior is implemented as a layer *on top of* MultiChor's central monad and data-types; from a theory perspective MultiChor gets census polymorphism "for free" because it's a Haskell library. (Therefore, we do not bother with a separate proof of the soundness of census polymorphism.) The MultiChor repository contains over a dozen example choreographies, several of which use census polymorphism. In Figure 3.3 we showcase a key-value store choreography that's polymorphic over the number of backup servers. Section 3.5 presents a more involved census-polymorphic example.

Key to MultiChor's strategy is Haskell's ability to express quantified type variables. For example, a `Faceted` value is (underneath a little boiler-plate) a function. Its argument is a `Member` proof that some party is in the list of owners, and it returns a `Located` value known to the party in question. Notably, nothing about the type, `Faceted ps cmn x`, indicates who the (type-level!) party indicated by the argument might be. (The second type parameter, `cmn`, represents parties who know *all* the contained values; it's frequently `'[]`.)

`Faceted ps cmn x` is actually a special case of a more general type, `PIndexed ps f`, where `f` can be any *type-level function* from a party to a concrete type. A `PIndexed` is like a type-indexed vector, except that the type of the value retrieved depends on the index. (The case where it does not depend on the index, *i.e.* when `f` is `Const`, is precisely `Quire`.) Because of its unusual `kind`, type classes that one would expect to apply to vectors generally do not apply to `PIndexed`. What's actually needed for census polymorphism is the ability to `sequence` a `PIndexed` of choreographies. Since `PIndexed` is not an instance of `Traversable`, we implement the needed function `sequenceP`, which is effectively just a `for`-loop (in any monad) over type-level lists of parties. These loops are not unrolled at compile time; the type class `KnownSymbols` affords to the runtime environment sufficient knowledge of the type-level list.

The type-level programming necessary to use `sequenceP` and `PIndexed` directly can involve some boilerplate. We provide the derived functions `fanOut` and `fanIn` which suffice for every situation studied so far. `fanOut`'s argument is a choreography that results in a `Located` value at the party identified by the loop variable; it aggregates these results as a `Faceted`. `fanIn` is almost the same, except that the locations of the resulting values do not vary, and they are aggregated in a `Quire` located at some list of recipients.

```
sequenceP :: forall b (ls :: [Symbol]) m. (KnownSymbols ls, Monad m)
          => PIndexed ls (Compose m b) -> m (PIndexed ls b)

fanOut :: (KnownSymbols qs)
       => (forall q. (KnownSymbol q) => Member q qs
                                     -> Choreo ps m (Located (q ': common) a))
       -> Choreo ps m (Faceted qs common a)

scatter :: forall census sender recipients a m.
           (KnownSymbol sender, KnownSymbols recipients, Show a, Read a)
         => Member sender census
         -> Subset recipients census
         -> Located '[sender] (Quire recipients a)
         -> Choreo census m (Faceted recipients '[sender] a)
```

Figure 3.4: Type signatures for `sequenceP`, `fanOut`, and `scatter`.

Figure 3.4 shows the type signatures for `sequenceP`, `fanOut`, and `scatter`. Keen readers may notice that the "`cmn`" parties' views of a **`Faceted`** are effectively just a **`Quire`**, and so wonder at the need for `fanIn`. In fact, `fanIn` *is* less often used than `fanOut`, but it's necessary for expressing choreographic loops that yield values which aren't known to the parties over whom the loop is defined. For example, the GMW protocol, which we implement using MultiChor in Section 3.5, cannot be written using only `fanOut`.

Modern Haskell language features, especially type-variable quantification, enable MultiChor's implementation of census polymorphism to be entirely type-safe and transparent to users. This is a flexible system within which users can easily write their own novel and bespoke functions and data structures.

3.5 The GMW Protocol in MultiChor

Secure multiparty computation (Evans et al. 2018) (MPC) is a family of techniques that allow a group of parties to jointly compute an agreed-upon function of their distributed data without revealing the data or any intermediate results to the other parties. We consider an MPC protocol named Goldreich-Micali-Widgerson (GMW) (Goldreich et al. 2019) after its authors. The GMW protocol requires the function to be computed to be specified as a binary circuit, and each of the parties who participates in the protocol may provide zero or more inputs to the circuit. At the conclusion of the protocol, all participating parties learn the circuit's output.

The GMW protocol is based on two important building blocks: *additive secret sharing*, a method for encrypting distributed data that still allows computing on it, and *oblivious transfer* (OT) (Naor and Pinkas 2001), a building-block protocol in applied cryptography. The GMW protocol starts by asking each party

to secret share its input values for the circuit. Then, the parties iteratively evaluate the gates of the circuit while keeping the intermediate values secret shared. Oblivious transfer is used to evaluate AND gates. When evaluation finishes, the parties reveal their secret shares of the output to decrypt the final result.

```
gmw :: forall parties m. (KnownSymbols parties, MonadIO m, CRT.MonadRandom m)
    => Circuit parties -> Choreo parties (CLI m) (Faceted parties '[] Bool)
gmw circuit = case circuit of
  InputWire p -> do         -- process a secret input value from party p
    value :: Located '[p] Bool <- _locally p $ getInput "Enter a secret input value:"
    secretShare p value
  LitWire b -> do           -- process a publicly-known literal value
    let chooseShare :: forall p. (KnownSymbol p) =>
                       Member p parties -> Choreo parties (CLI m) (Located '[p] Bool)
        chooseShare p = congruently (p @@ nobody) $ \_ -> case p of First  -> b
                                                                    Later _ -> False
    fanOut chooseShare
  AndGate l r -> do         -- process an AND gate
    lResult <- gmw l; rResult <- gmw r;
    fAnd lResult rResult
  XorGate l r -> do         -- process an XOR gate
    lResult <- gmw l; rResult <- gmw r
    parallel (allOf @parties) \p un -> pure $ xor [viewFacet un p lResult, viewFacet un p rResult]

data Circuit :: [LocTy] -> Type where
  InputWire :: (KnownSymbol p) => Member p ps -> Circuit ps
  LitWire :: Bool -> Circuit ps
  AndGate :: Circuit ps -> Circuit ps -> Circuit ps
  XorGate :: Circuit ps -> Circuit ps -> Circuit ps

mpc :: forall parties m. (KnownSymbols parties, MonadIO m, CRT.MonadRandom m)
    => Circuit parties -> Choreo parties (CLI m) ()
mpc circuit = do
  outputWire <- gmw circuit
  result <- reveal outputWire
  void $ _parallel (allOf @parties ) $ putOutput "The resulting bit:" result
```

Figure 3.5: A choreography for the GMW protocol. The choreography works for an arbitrary number of parties. Figure 3.6 contains the `xor` function to compute the OR gate, the `secretShare` choreography to handle an INPUT, and the `fAnd` choreography to compute the result of an AND gate. `mpc` uses `gmw` protocol as well as `reveal` (also in Figure 3.6, and prints the resulting bit at each party.

Additive secret sharing We begin by describing additive secret sharing, a common building block in MPC protocols. A secret bit x can be *secret shared* by generating n random *shares* $s_1, \ldots, s_n$ such that $x = \sum_{i=1}^{n} s_i$. If $n - 1$ of the shares are generated uniformly and independently randomly, and the final share is chosen to satisfy the property above, then the shares can be safely distributed to the n parties without revealing x—recovering x requires access to all n shares. Importantly, secret shares are *additively homomorphic*—adding together shares of secrets x and y produces a share of $x + y$.

MultiChor choreographies for performing secret sharing in the arithmetic field of booleans appear in Figure 3.6. The function `secretShare` takes a single secret bit located at party `p`, generates `shares`,

```
secretShare :: forall parties p m. (KnownSymbols parties, KnownSymbol p, MonadIO m)
            => Member p parties -> Located '[p] Bool -> Choreo parties m (Faceted parties '[] Bool)
secretShare p value = do
  shares <- locally p \un -> genShares p (un singleton value)
  PIndexed fs <- scatter p (allOf @parties) shares
  return $ PIndexed $ Facet . othersForget (First @@ nobody) . getFacet . fs

genShares :: forall ps p m. (MonadIO m, KnownSymbols ps) => Member p ps -> Bool -> m (Quire ps Bool)
genShares p x = quorum1 p gs'
  where gs' :: forall q qs. (KnownSymbol q, KnownSymbols qs) => m (Quire (q ': qs) Bool)
        gs' = do freeShares <- sequence $ pure $ liftIO randomIO -- generate n-1 random shares
                 return $ qCons (xor (qCons @q x freeShares)) freeShares

xor :: (Foldable f) => f Bool -> Bool
xor = foldr1 (/=)

fAnd :: forall parties m.
        (KnownSymbols parties, MonadIO m, CRT.MonadRandom m)
     => Faceted parties '[] Bool
     -> Faceted parties '[] Bool
     -> Choreo parties (CLI m) (Faceted parties '[] Bool)
fAnd uShares vShares = do
  let genBools = sequence $ pure randomIO
  a_j_s :: Faceted parties '[] (Quire parties Bool) <- _parallel (allOf @parties) genBools
  bs :: Faceted parties '[] Bool <- fanOut \p_j -> do
      let p_j_name = toLocTm p_j
      b_i_s <- fanIn (p_j @@ nobody) \p_i ->
        if toLocTm p_i == p_j_name
          then _locally p_j $ pure False
          else do
              bb <- locally p_i \un -> let a_ij = getLeaf (viewFacet un p_i a_j_s) p_j
                                           u_i = viewFacet un p_i uShares
                                       in pure (xor [u_i, a_ij], a_ij)
              enclaveTo (p_i @@ p_j @@ nobody) (listedSecond @@ nobody) (ot2 bb $ localize p_j vShares)
      locally p_j \un -> pure $ xor $ un singleton b_i_s
  parallel (allOf @parties) \p_i un ->
    let computeShare u v a_js b = xor $ [u && v, b] ++ toList (qModify p_i (const False) a_js)
    in pure $ computeShare (viewFacet un p_i uShares) (viewFacet un p_i vShares)
                           (viewFacet un p_i a_j_s)   (viewFacet un p_i bs)

ot2 :: (KnownSymbol sender, KnownSymbol receiver, MonadIO m, CRT.MonadRandom m) =>
  Located '[sender] (Bool, Bool) -> Located '[receiver] Bool
  -> Choreo '[sender, receiver] (CLI m) (Located '[receiver] Bool)
ot2 bb s = do
  let sender = listedFirst :: Member sender '[sender, receiver]
  let receiver = listedSecond :: Member receiver '[sender, receiver]

  keys <- locally receiver  \un -> liftIO $ genKeys $ un singleton s
  pks <- (receiver, \un -> let (pk1, pk2, _) = un singleton keys
                           in return (pk1, pk2)) ~~> sender @@ nobody
  encrypted <- (sender, \un -> let (b1, b2) = un singleton bb
                               in liftIO $ encryptS (un singleton pks) b1 b2) ~~> receiver @@ nobody
  locally receiver  \un -> liftIO $ decryptS (un singleton keys)
                                             (un singleton s)
                                             (un singleton encrypted)

reveal :: forall ps m. (KnownSymbols ps) => Faceted ps '[] Bool -> Choreo ps m Bool
reveal shares = xor <$> (gather ps ps shares >>= naked ps)
  where ps = allOf @ps
```

Figure 3.6: Various helpers for the GMW protocol. `fANd` computes the result of an AND gate on secret-shared inputs using pairwise oblivious transfer. The choreography works for an arbitrary number of parties, and leverages the 1 out of 2 OT defined earlier. `xor` computes the result of an OR gate as a standard non-choreographic function. `secretShare` handles Input gate secret sharing `p`'s secret value among `parties` and for revealing a secret-shared value. `ot` performs 1 out of 2 oblivious transfer (OT) using RSA public-key encryption. The choreography involves exactly two parties, `sender` and `receiver`. `genShares` uses **`Quire`** to map each member `p` in `ps` to a generated secret share **`Bool`**. `encryptS` `decryptS` which are omitted for brevity use the cryptonite library for encryption and decryption.

a `Quire` which maps each member in `parties` to a share, and then uses `scatter` to send the assigned share to each member. However `scatter` would return a `Faceted parties '[p] Bool` since by default it includes the sender. The choreographic function `gmw` expects shares of wires to be secret, so we must return a `Faceted parties '[] Bool`. We accomplish this by deconstructing and reconstructing via `PIndexed`, and using `othersForget (First @@ nobody)`. The resulting `Faceted` "bit" actually represents the differing values located at all parties; the bits held by the parties sum up to the original secret. `reveal` takes exactly such a shared value and broadcasts all the shares so everyone can reconstruct the plain-text.

Oblivious transfer The other important building block of the GMW protocol is oblivious transfer (OT) (Naor and Pinkas 2001). OT is a 2-party protocol between a *sender* and a *receiver*. In the simplest variant (*1 out of 2* OT, used in GMW), the sender inputs two secret bits b_1 and b_2, and the receiver inputs a single secret *select bit* s. If $s = 0$, then the receiver receives b_1; if $s = 1$, then the receiver receives b_2. Importantly, the sender does *not* learn which of b_1 or b_2 has been selected, and the receiver does *not* learn the non-selected value.

Oblivious transfer is a *two-party protocol*; it would be erroneous for any third-parties to be involved in the implementation. MultiChor's `Faceted` values and utilities for type-safe embedding of enclaved sub-protocols within larger censuses make it possible to embed the use of pairwise oblivious transfer between parties in a general version of multi-party GMW.

Computing secret-shared AND via OT To compute the result of an AND gate, the parties compute *pairwise* ANDs using their respective shares of the input values, then use the results to derive shares of the gate's output. The `fAnd` choreography (Figure 3.6 lines 17–39) takes `Faceted` values holding the parties' shares of the input values, and returns a `Faceted` value representing each party's share of the output. On line 25, the parties perform a `fanOut` to begin the pairwise computation; the `fanIn` on line 27 completes the pairing, and uses `enclaveTo` (line 34) to embed pairwise OTs (via `ot2`) in the larger set of parties.

The GMW protocol The complete GMW protocol operates as summarized earlier, by secret sharing input values and then evaluating the circuit gate-by-gate. Our implementation as a MultiChor choreography appears in Figure 3.5, defined as a recursive function over the structure of the circuit. The choreography returns a `Faceted` value, representing the secret-shared output of the circuit. For "input" gates (lines 4–6), the

choreography runs the secret sharing protocol in Figure 3.6 to distribute shares of the secret value. For XOR gates (lines 16–18) Figure 3.5, the parties recursively run the GMW protocol to compute the two inputs to the gate and then each party computes one share of the gate's output by XORing their shares of the inputs. This approach leverages the additive homomorphism of additive secret shares. For AND gates (lines 13–15) Figure 3.5, the parties compute shares of the gate's inputs, then use the `fAnd` protocol to perform multiplication of the two inputs. This implements the protocol as described in Section 3.2.1 of (Evans et al. 2018), namely the *Generalization to more than two parties* case. Since additive secret shares are not multiplicatively homomorphic, this operation leverages the oblivious transfer protocol to perform the multiplication.

Our implementation of GMW leverages MultiChor's **`Faceted`** values and utilities for type-safe parallel, enclaved, and pairwise choreographies to build a fully-general implementation of the protocol that works for an arbitrary number of parties.

Bibliography

Austin, T. H. and C. Flanagan (2012). Multiple facets for dynamic information flow. In *Proceedings of the 39th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '12, New York, NY, USA, pp. 165–178. Association for Computing Machinery.

Bates, M., S. Kashiwa, S. Jafri, G. Shen, L. Kuper, and J. P. Near (2024). Efficient, portable, census-polymorphic choreographic programming.

Beck, G., A. Goel, A. Hegde, A. Jain, Z. Jin, and G. Kaptchuk (2023). Scalable multiparty garbling. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, CCS '23, New York, NY, USA, pp. 2158–2172. Association for Computing Machinery.

Bonawitz, K., V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth (2017). Practical secure aggregation for privacy-preserving machine learning. In *proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1175–1191.

Corrigan-Gibbs, H. and D. Boneh (2017). Prio: Private, robust, and scalable computation of aggregate statistics. In *14th USENIX symposium on networked systems design and implementation (NSDI 17)*, pp. 259–282.

Evans, D., V. Kolesnikov, M. Rosulek, et al. (2018). A pragmatic introduction to secure multi-party computation. *Foundations and Trends® in Privacy and Security 2*(2-3), 70–246.

Goldreich, O., S. Micali, and A. Wigderson (2019). How to play any mental game, or a completeness theorem for protocols with honest majority. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pp. 307–328.

Keeler, D., C. Komlo, E. Lepert, S. Veitch, and X. He (2023, 07). Dprio: Efficient differential privacy with high utility for prio. *Proceedings on Privacy Enhancing Technologies 2023*, 375–390.

Naor, M. and B. Pinkas (2001). Efficient oblivious transfer protocols. In *SODA*, Volume 1, pp. 448–457.

Noonan, M. (2018). Ghosts of departed proofs (functional pearl). In *Proceedings of the 11th ACM SIGPLAN International Symposium on Haskell*, Haskell 2018, New York, NY, USA, pp. 119–131. Association for Computing Machinery.

Noonan, M. (2019). gdp: Reason about invariants and preconditions with ghosts of departed proofs.

Shen, G., S. Kashiwa, and L. Kuper (2023, aug). Haschor: Functional choreographic programming for all (functional pearl). *Proc. ACM Program. Lang. 7*(ICFP).

Wu, W., L. He, W. Lin, R. Mao, C. Maple, and S. Jarvis (2020). Safa: A semi-asynchronous protocol for fast federated learning with low overhead. *IEEE Transactions on Computers 70*(5), 655–668.

Chapter 4

Ongoing Work

We believe MultiChor to be the best off-the-shelf system presently available for any real-world applications of CP. We are also confident that λ_C and the associated theorems demonstrate the theoretical soundness of the enclaves-&-MLVs CP paradigm. That said, it is unsatisfying that the syntactic structures of these two systems are so different from each other. Furthermore, it is not clear that these systems as they stand are good foundations for the development of more advanced CP techniques. We propose to make changes to one or both systems in the coming months, to make them align with each other better and to facilitate subsequent work in this area.

4.1 ”Mini”-Chor

It is natural to ask why MultiChor has a ”core” API distinct from the ergonomic API afforded to end-users. This design pattern makes reasoning about MultiChor's implementation easier; whether there are any performance implications has not been explored[1]. In the coming months, we would like to push the simplicity of the core API even further:

1. The use of a freer monad system is not actually necessary. It facilitates implementation, but it's also an additional ”moving part” that can be removed without affecting the system's behavior.

[1] The need for methods for comparing the performance of CP systems was acknowleged by the community of CP researchers attending PLDI24.

2. As mentioned in Chapter 3, the functions `flatten` and `othersForget` could be removed from the core API and replaced with derived monadic functions. This would be a step backwards for the ergonomics of MultiChor, so we do not advocate making such a change to the version published on Hackage.

3. Replacing the core operation `congruently'` with `naked` (a monadic operator that unwraps an MLV known to the entire census) may degrade ergonomics. On the other hand, it would also allow simplification of `locally'` by obviating the `Unwrap` argument; *i.e.* `locally'`'s argument would no longer be a function at all!

4. Having made the above changes, the only remaining place where `Located` values would get unwrapped would be `naked`. We would be able to remove the underlying `Choreo` constructor for `naked` and change the implementation of `Located` to be a `newtype` wrapper for a census-polymorphic choreography yielding the target value. In other words, `naked` would be the field accessor function for `Located`.

By making these changes, which we expect to preserve in a clearly labeled fork of MultiChor, we will facilitate subsequent theoretical work on CP. In particular, the reduced API would make a good target for a more fully-featured formal model.

Bibliography

Austin, T. H. and C. Flanagan (2012). Multiple facets for dynamic information flow. In *Proceedings of the 39th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '12, New York, NY, USA, pp. 165–178. Association for Computing Machinery.

Bates, M., S. Kashiwa, S. Jafri, G. Shen, L. Kuper, and J. P. Near (2024). Efficient, portable, census-polymorphic choreographic programming.

Beck, G., A. Goel, A. Hegde, A. Jain, Z. Jin, and G. Kaptchuk (2023). Scalable multiparty garbling. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, CCS '23, New York, NY, USA, pp. 2158–2172. Association for Computing Machinery.

Bonawitz, K., V. Ivanov, B. Kreuter, A. Marcedone, H. B. McMahan, S. Patel, D. Ramage, A. Segal, and K. Seth (2017). Practical secure aggregation for privacy-preserving machine learning. In *proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1175–1191.

Carbone, M. and F. Montesi (2013). Deadlock-freedom-by-design: multiparty asynchronous global programming. In *Proceedings of the 40th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '13, New York, NY, USA, pp. 263–274. Association for Computing Machinery.

Castagna, G., M. Dezani-Ciancaglini, and L. Padovani (2011). On global types and multi-party sessions. In R. Bruni and J. Dingel (Eds.), *Formal Techniques for Distributed Systems*, Berlin, Heidelberg, pp. 1–28. Springer Berlin Heidelberg.

Chakraborty, K. (2024). Unichorn.

Corrigan-Gibbs, H. and D. Boneh (2017). Prio: Private, robust, and scalable computation of aggregate statistics. In *14th USENIX symposium on networked systems design and implementation (NSDI 17)*, pp. 259–282.

Cruz-Filipe, L., E. Graversen, L. Lugović, F. Montesi, and M. Peressotti (2023). Modular Compilation for Higher-Order Functional Choreographies. In K. Ali and G. Salvaneschi (Eds.), *37th European Conference on Object-Oriented Programming (ECOOP 2023)*, Volume 263 of *Leibniz International Proceedings in Informatics (LIPIcs)*, Dagstuhl, Germany, pp. 7:1–7:37. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

Cruz-Filipe, L., E. Graversen, L. Lugović, F. Montesi, and M. Peressotti (2022, September). *Theoretical Aspects of Computing*, Volume 13572 of *Lecture Notes in Computer Science*, Chapter Functional choreographic programming, pp. 212–237. Tbilisi, Georgia: Springer.

Cruz-Filipe, L. and F. Montesi (2020). A core model for choreographic programming. *Theor. Comput. Sci. 802*, 38–66.

Evans, D., V. Kolesnikov, M. Rosulek, et al. (2018). A pragmatic introduction to secure multi-party computation. *Foundations and Trends® in Privacy and Security 2*(2-3), 70–246.

Giallorenzo, S., F. Montesi, and M. Peressotti (2024, jan). Choral: Object-oriented choreographic programming. *ACM Trans. Program. Lang. Syst. 46*(1).

Goldreich, O., S. Micali, and A. Wigderson (2019). How to play any mental game, or a completeness theorem for protocols with honest majority. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pp. 307–328.

Graversen, E., A. K. Hirsch, and F. Montesi (2024). Alice or bob?: Process polymorphism in choreographies. *Journal of Functional Programming 34*, e1.

Hirsch, A. K. and D. Garg (2022, January). Pirouette: higher-order typed functional choreographies. *Proc. ACM Program. Lang. 6*(POPL).

Honda, K., N. Yoshida, and M. Carbone (2008). Multiparty asynchronous session types. In *Proceedings of the 35th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '08, New York, NY, USA, pp. 273–284. Association for Computing Machinery.

Jongmans, S.-S. and P. van den Bos (2022). *A Predicate Transformer for Choreographies (Full Version)*. Number 01 in OUNL-CS (Technical Reports). Open Universiteit Nederland.

Kashiwa, S., G. Shen, S. Zare, and L. Kuper (2023). Portable, efficient, and practical library-level choreographic programming.

Keeler, D., C. Komlo, E. Lepert, S. Veitch, and X. He (2023, 07). Dprio: Efficient differential privacy with high utility for prio. *Proceedings on Privacy Enhancing Technologies 2023*, 375–390.

Lugović, L. and S.-S. Jongmans (2024). Klor: Choreographies in clojure.

Montesi, F. (2014). Ph. D. thesis, Denmark.

Montesi, F. (2023). *Introduction to Choreographies*. Cambridge University Press.

Montesi, F. and M. Peressotti (2017). Choreographies meet communication failures. *CoRR abs/1712.05465*.

Naor, M. and B. Pinkas (2001). Efficient oblivious transfer protocols. In *SODA*, Volume 1, pp. 448–457.

Needham, R. M. and M. D. Schroeder (1978, December). Using encryption for authentication in large networks of computers. *Commun. ACM 21*(12), 993–999.

Noonan, M. (2018). Ghosts of departed proofs (functional pearl). In *Proceedings of the 11th ACM SIGPLAN International Symposium on Haskell*, Haskell 2018, New York, NY, USA, pp. 119–131. Association for Computing Machinery.

Noonan, M. (2019). gdp: Reason about invariants and preconditions with ghosts of departed proofs.

Plotkin, G. and J. Power (2003). Algebraic operations and generic effects. *Applied categorical structures 11*, 69–94.

Plotkin, G. D. and M. Pretnar (2013, December). Handling algebraic effects. *Logical Methods in Computer Science Volume 9, Issue 4*.

Rastogi, A., M. A. Hammer, and M. Hicks (2014). Wysteria: A programming language for generic, mixed-mode multiparty computations. In *2014 IEEE Symposium on Security and Privacy*, pp. 655–670.

Shen, G., S. Kashiwa, and L. Kuper (2023, aug). Haschor: Functional choreographic programming for all (functional pearl). *Proc. ACM Program. Lang. 7*(ICFP).

Shen, G. and L. Kuper (2024). Toward verified library-level choreographic programming with algebraic effects.

Sweet, I., D. Darais, D. Heath, W. Harris, R. Estes, and M. Hicks (2023, February). Symphony: Expressive secure multiparty computation with coordination. *The Art, Science, and Engineering of Programming 7*(3).

Urban, C., S. Berghofer, and M. Norrish (2007). Barendregt's variable convention in rule inductions. In F. Pfenning (Ed.), *Automated Deduction – CADE-21*, Berlin, Heidelberg, pp. 35–50. Springer Berlin Heidelberg.

W3C (2005). WS Choreography Description Language. http://www.w3.org/TR/ws-cdl-10/.

Wiersdorf, A. and B. Greenman (2024). Chorex: Choreographic programming in elixir.

Wu, W., L. He, W. Lin, R. Mao, C. Maple, and S. Jarvis (2020). Safa: A semi-asynchronous protocol for fast federated learning with low overhead. *IEEE Transactions on Computers 70*(5), 655–668.

Appendix A: Proofs of Theorems

A.1 Proof of The Substitution Theorem

Theorem 1 says that if $\Theta; \Gamma, (x : T_x) \vdash M : T$ and $\Theta; \Gamma \vdash V : T_x$, then $\Theta; \Gamma \vdash M[x := V] : T$. We first prove a few lemmas.

Lemma 1 (Enclave)**.** *If* $\Theta; \Gamma \vdash V : T$ *and* $\Theta' \subseteq \Theta$ *and* $T' = T \triangleright \Theta'$ *is defined then* $V' = V \triangleright \Theta'$ *is defined, and* $\Theta'; \Gamma \vdash V' : T'$.

A.1.1 Proof of Lemma 1

This is vacuous if T' doesn't exist, so assume it does. Do induction on the definition of masking for T:

- MTDATA: $\Theta; \Gamma \vdash V : d@p^+$ and $p^+ \cap \Theta' \neq \varnothing$ so $T' = d@(p^+ \cap \Theta')$. Consider cases for typing of V:
  - TVAR: $V' = V$ by MVVAR and it types by TVAR b.c. T' exists.
  - TUNIT: We've already assumed the preconditions for MVUNIT, and it types.
  - TPAIR: $V = \mathsf{Pair}\, V_1 V_2$, and $\Theta; \Gamma \vdash V_1 : d_1@(p_1^+ \supseteq p^+)$ and $\Theta; \Gamma \vdash V_2 : d_2@(p_2^+ \supseteq p^+)$. By MTDATA, these larger-owernership types will still mask with Θ', so this case come by induction.
  - TINL, TINR: Follows by simple induction.
- MTFUNCTION: $T' = T$ and $p^+ \subseteq \Theta'$, so lambdas and function-keywords all project unchanged, and the respective typings hold.
- MTVECTOR: Simple induction.

Lemma 2 (Quorum)**.** ***A)*** *If* $\Theta; \Gamma, (x : T_x) \vdash M : T$ *and* $T'_x = T_x \triangleright \Theta$*, then* $\Theta; \Gamma, (x : T'_x) \vdash M : T$*.*

B) *If* $\Theta; \Gamma, (x : T_x) \vdash M : T$ *and* $T_x \triangleright \Theta$ *is not defined, then* $\Theta; \Gamma \vdash M : T$*.*

A.1.2 Proof of Lemma 2

By induction on the typing of M. The only case that's not recursive or trivial is TVar, for which we just need to observe that masking on a given party-set is idempotent.

Lemma 3 (Unused)**.** *If* $\Theta; \Gamma \vdash M : T$ *and* $x \notin \Gamma$*, then* $M[x := V] = M$*.*

A.1.3 Proof of Lemma 3

By induction on the typing of M. There are no non-trivial cases.

A.1.4 Theorem 1

Theorem 1 says that if $\Theta; \Gamma, (x : T_x) \vdash M : T$ and $\Theta; \Gamma \vdash V : T_x$, then $\Theta; \Gamma \vdash M[x := V] : T$.

The proof is in 13 cases. TProjN, TProj1, TProj2, TCom, and TUnit are trivial base cases. TInL, TInR, TVec, and TPair are trivial recursive cases.

- TLambda where $T'_x = T_x \triangleright p^+$: $M = (\lambda y : T_y \,.\, N)@p^+$ and $T = (T_y \to T')@p^+$.

  1. $\Theta; \Gamma, (x : T_x) \vdash (\lambda y : T_y \,.\, N)@p^+ : (T_y \to T')@p^+$ by assumption.
  2. $\Theta; \Gamma \vdash V : T_x$ by assumption.
  3. $p^+; \Gamma, (x : T_x), (y : T_y) \vdash N : T'$ per preconditions of TLambda.
  4. $\Theta; \Gamma, (y : T_y) \vdash V : T_x$ by weakening (or strengthening?) #2.
  5. $V' = V \triangleright p^+$ and $p^+; \Gamma, (y : T_y) \vdash V' : T'_x$ by Lemma 1.
  6. $p^+; \Gamma, (x : T'_x), (y : T_y) \vdash N : T'$ by applying Lemma 2 to #3.
  7. $p^+; \Gamma, (y : T_y) \vdash N[x := V'] : T'$ by induction on #6 and #5.
  8. $M[x := V] = (\lambda y : T_y \,.\, N[x := V'])@p^+$ by definition, which typechecks by #7 and TLambda.

  QED.

- TLambda where $T_x \triangleright p^+$ is undefined: $M = (\lambda y : T_y \,.\, N)@p^+$.

1. $p^+; \Gamma, (x : T_x), (y : T_y) \vdash N : T'$ per preconditions of TLambda.
2. $p^+; \Gamma, (y : T_y) \vdash N : T'$ by Lemma 2 B.
3. $N[x := V] = N$ by Lemma 3, so regardless of the existence of $V \triangleright p^+$ the substitution is a noop, and it typechecks by #2 and TLambda.

- TVar: Follows from the relevant definitions, whether $x \equiv y$ or not.
- TApp: This is also a simple recursive case; the masking of T_a doesn't affect anything.
- TCase: Follows the same logic as TLambda, just duplicated for M_l and M_r.

A.2 Proof of The Preservation Theorem

Theorem 2 says that if $\Theta; \varnothing \vdash M : T$ and $M \longrightarrow M'$, then $\Theta; \varnothing \vdash M' : T$. We'll need a few lemmas first.

Lemma 4 (Sub-Mask)**.** *If $\Theta; \Gamma \vdash V : d@p^+$ and $\varnothing \neq q^+ \subseteq p^+$, then **A:** $d@p^+ \triangleright q^+ = d@q^+$ is defined and **B:** $V \triangleright q^+$ is also defined and types as $d@q^+$.*

A.2.1 Proof of Lemma 4

Part A is obvious by MTData. Part B follows by induction on the definition of masking for values.

- MVLambda: Base case; can't happen because it wouldn't allow a data type.
- MVUnit: Base case; passes definition and typing.
- MVInL, MVInR: Recursive cases.
- MVPair: Recursive case.
- MVVector: Can't happen because it wouldn't allow a data type.
- MVProj1, MVProj2, MVProjN, and MVCom: Base cases, can't happen because they wouldn't allow a data type.
- MVVar: Base case, trivial.

Lemma 5 (Maskable)**.** *If $\Theta; \Gamma \vdash V : T$ and $T \triangleright p^+ = T'$, then **A:** $V \triangleright p^+ = V'$ is defined and **B:** $\Theta; \Gamma \vdash V' : T'$.*

A.2.2 Proof of Lemma 5

By induction on the definition of masking for values.

- MVLambda: Base case. From the type-masking assumption, MTFunction, p^+ is a superset of the owners, so $T' = T$, so $V' = V$.
- MVUnit: Base case; passes definition and typing.
- MVInL, MVInR: Recursive cases.
- MVPair: Recursive case.
- MVVector: Recursive case.
- MVProj1, MVProj2, MVProjN, and MVCom: From the typing assumption, p^+ is a superset of the owners, so $T' = T$ and $V' = V$.
- MVVar: Base case, trivial.

Lemma 6 (Exclave)**.** *If* $\Theta; \varnothing \vdash M : T$ *and* $\Theta \subseteq \Theta'$ *then* $\Theta'; \varnothing \vdash M : T$.

A.2.3 Proof of Lemma 6

By induction on the typing of M.

- TLambda: The recursive typing is unaffected, and the other tests are fine with a larger set.
- TVar: Can't apply with an empty type context.
- All other cases are unaffected by the larger party-set.

A.2.4 Theorem 2

To repeat: Theorem 2 says that if $\Theta; \varnothing \vdash M : T$ and $M \longrightarrow M'$, then $\Theta; \varnothing \vdash M' : T$.

We prove this by induction on typing rules for M. The eleven base cases (values) fail the assumption that M can step, so we consider the recursive cases:

- TCase: M is of form $\mathsf{case}_{p^+}\, N\, \mathsf{of}\, \mathsf{Inl}\, x_l \Rightarrow M_l; \mathsf{Inr}\, x_r \Rightarrow M_r$. There are three ways it might step:

- CaseL: N is of form $\mathsf{Inl}\, V$, V' exists, and $M' = M_l[x_l := V']$.
  1. $p^+; (x_l : d_l @ p^+) \vdash M_l : T$ by the preconditions of TCase.
  2. $\Theta; \varnothing \vdash V : d_l @ p^+$ because N must type by TInL.
  3. $p^+; \varnothing \vdash V' : d_l @ p^+$ by Lemma 1 and MTData.
  4. $p^+; \varnothing \vdash M_l[x_l := V'] : T$ by Lemma 1.
  5. $\Theta; \varnothing \vdash M_l[x_l := V'] : T$ by Lemma 6. **QED.**
- CaseR: Same as CaseL.
- Case: $N \longrightarrow N'$, and by induction and TCase, $\Theta; \Gamma \vdash N' : T_N$, so the original typing judgment will still apply.

- TApp: M is of form FA, and F is of a function type and A also types (both in the empty typing context). If the step is by App2or App1, then recursion is easy. There are eight other ways the step could happen:
  - AppAbs: F must type by TLambda. $M = ((\lambda x : T_x \,.\, B) @ p^+) A$. We need to show that $A' = A \triangleright p^+$ exists and $\Theta; \varnothing \vdash B[x := A'] : T$.
    1. $p^+; (x : T_x) \vdash B : T$ by the preconditions of TLambda.
    2. $\Theta; \varnothing \vdash A : T'_a$ such that $T_x = T'_a \triangleright p^+$, by the preconditions of TApp.
    3. A' exists and $p^+; \varnothing \vdash A' : T_x$ by Lemma 1 on #2.
    4. $p^+; \varnothing \vdash B[x := A'] : T$ by Lemma 1.
    5. **QED.** by Lemma 6.
  - Proj1: $F = \mathsf{fst}_{p^+}$ and $A = \mathsf{Pair}\, V_1 V_2$ and $M' = V_1 \triangleright p^+$. Necessarily, by TPair $\Theta; \varnothing \vdash V_1 : d_1 @ p_1^+$ where $p^+ \subseteq p_1^+$. By Lemma 4, $\Theta; \varnothing \vdash M' : T$.
  - Proj2: same as Proj1.
  - ProjN: $F = \mathsf{lookup}^i_{p^+}$ and $A = (\ldots, V_i, \ldots)$ and $M' = V_i \triangleright p^+$. Necessarily, by TVec $\Theta; \varnothing \vdash V_i : T_i$ and $\Theta; \varnothing \vdash A : (\ldots, T_i, \ldots)$. By TApp, $(\ldots, T_i, \ldots) \triangleright p^+ = T_a$, so by MTVector $T_i \triangleright p^+$ exists and (again by TApp and TProjN) it must equal T. **QED.** by Lemma 5.
  - Com1: By TCom and TUnit.
  - ComPair: Recusion among the Com* cases.

  - ComInl: Recusion among the Com* cases.
  - ComInr: Recusion among the Com* cases.

A.3 Proof of The Progress Theorem

Theorem 3 says that if $\Theta; \varnothing \vdash M : T$, then either M is of form V (which cannot step) or their exists M' s.t. $M \longrightarrow M'$.

The proof is by induction of typing rules. There are eleven base cases and two recursive cases. Base cases:

- TLambda
- TVar (can't happen, by assumption)
- TUnit
- TCom
- TPair
- TVec
- TProj1
- TProj2
- TProjN
- TInl
- TInr

Recursive cases:

- TCase: M is of form $\mathsf{case}_{p^+}\, N \,\mathsf{of}\, \mathsf{Inl}\, x_l \Rightarrow M_l; \mathsf{Inr}\, x_r \Rightarrow M_r$ and $\Theta; \varnothing \vdash N : (d_l + d_r)@p^+$. By induction, either N can step, in which case M can step by Case, or N is a value. The only typing rules that would give an N of form V the required type are TVar (which isn't compatible with the assumed

empty Γ), and TInl and TInr, which respectively force N to have the required forms for M to step by CaseL or CaseR. From the typing rules, MTData, and the first part of Lemma 1, the masking required by the step rules is possible.

- TApp: M is of form FA, and F is of a function type and A also types (both in the same empty Γ). By induction, either F can step (so M can step by App2), or A can step (so M can step by App1), or F and A are both values. Ignoring the impossible TVar cases, there are five ways an F of form V could type as a function; in each case we get to make some assumption about the type of A. Furthermore, by TApp and Lemma 1, we know that A can mask to the owners of F.
  - TProj1: A must be a value of type $(d_1 \times d_2)@q^+$, and must type by TPair, so it must have form $\mathsf{Pair}\, V_1 V_2$, so M must step by Proj1. We know V_1 can mask by MVPair.
  - TProj2: (same as TProj1)
  - TProjN: A must be a value of type $(T_1, \ldots, T_n)$ with $i \leq n$ and must type by TVec, so it must have from $(V_1, \ldots, V_n)$. M must step by ProjN. We known V_i can step by MVVector.
  - TCom: A must be a value of type $d@q^+$, such that $d@q^+ \triangleright s^+ = d@s^+$. For that to be true, MTData requires that $s^+ \subseteq q^+$. A can type that way under TUnit, TPair, TInl, or TInr, which respectively force forms $()@q^+$, $\mathsf{Pair}\, V_1 V_2$, $\mathsf{Inl}\, V$, and $\mathsf{Inr}\, V$, which respectively require that M reduce by Com1, ComPair, ComInl, and ComInr. In the case of (), this follows from Lemma 4, since $\{s\} \subseteq s^+ \subseteq q^+$; the other three are recursive among each other.
  - TLambda: M must reduce by AppAbs. By the assumption of TApp and Lemma 5, it can.

A.4 Proof of The Soundness Theorem

Theorem 4 says that if $\Theta; \varnothing \vdash M : T$ and $[\![M]\!] \xrightarrow{\varnothing}{}^{*} \mathcal{N}_n$, then there exists M' such that $M \longrightarrow^* M'$ and $\mathcal{N}_n \xrightarrow{\varnothing}{}^{*} [\![M']\!]$. We'll need a few lemmas first.

Lemma 7 (Values)**.** ***A):*** $[\![V]\!]_p = L$. ***B):*** *If* $[\![M]\!]_p = L \neq \bot$ *then* M *is a value* V.

Proof is by inspection of the definition of projection.

Corollary 2. *If* N *is well-typed and* $[\![N]\!]$ *can step at all, then* ***(A)*** N *can step to some* N' *and* ***(B)*** $[\![N]\!]$ *can multi-step to* $[\![N']\!]$ *with empty annotation.*

__A__ follows from Lemma 7 and Theorem 3. __B__ is just Theorem 5.

Lemma 8 (Determinism)**.** *If* $\mathcal{N}_a \mid \mathcal{N}_0 \xrightarrow{\varnothing} \mathcal{N}_a \mid \mathcal{N}_1$ *s.t. for every* $p[B_0] \in \mathcal{N}_0$, $\mathcal{N}_1(p) \neq B_0$, and $\mathcal{N}_b \mid \mathcal{N}_0 \xrightarrow{\varnothing} \mathcal{N}_c \mid \mathcal{N}_2$ *s.t. the domain of* $\mathcal{N}_2$ *equals the domain of* $\mathcal{N}_0$*, then* either

- $\mathcal{N}_2 = \mathcal{N}_0$, or
- $\mathcal{N}_2 = \mathcal{N}_1$ *and* $\mathcal{N}_b = \mathcal{N}_c$.

A.4.1 Proof of Lemma 8

First, observe that for every non-value expression in the process language, there is at most one rule in the process semantics by which it can step. (For values, there are zero.) Furthermore, the only way for the step annotation and resulting expression to *not* be fully determined by the initial expression is if the justification is based on a LRecv step, in which case the send-annotation will be empty and the resulting expression will match the (single) item in the receive-annotation.

$\mathcal{N}_a \mid \mathcal{N}_0 \xrightarrow{\varnothing} \mathcal{N}_a \mid \mathcal{N}_1$ must happen by NPar, so consider the $\mathcal{N}_0$ step that enables it; call that step $\mathfrak{S}$. $\mathfrak{S}$ can't be by NPar; that would imply parties in $\mathcal{N}_0$ who don't step.

- If $\mathfrak{S}$ is by NPro, then $\mathcal{N}_0 = p[B_0]$ is a singleton and $\mathfrak{S}$ is justified by a process step with empty annotation. As noted above, that process step is the only step B_0 can take, so the $\mathcal{N}_b \mid \mathcal{N}_0 \xrightarrow{\varnothing} \mathcal{N}_c \mid \mathcal{N}_2$ step must either be a NPar composing some other party(ies) step with $\mathcal{N}_0$ (satisfying the first choice), or a NPar composing $\mathfrak{S}$ with $\mathcal{N}_b$ (satisfying the second).
- If $\mathfrak{S}$ is by NCom, then there must be both a singleton NPro step justified by a process step (by some party s) with nonempty send-annotation and a nonempty sequence of other party steps (covering the rest of $\mathcal{N}_0$'s domain) that it gets matched with each with a corresponding receive-annotation. The send-annotated NPro step is deterministic in the same way as an empty-annotated NPro step. In order for the parties to cancel out, it can only compose by NCom with (a permutation of) the same sequence of peers. Considered in isolation, the peers are non-deterministic, but their process-steps can only be used in the network semantics by composing with s via NCom, and their resulting expressions are determined by the matched process annotation, which is determined by s's step.

  Thus, for any $p[B_2] \in \mathcal{N}_2$, $B_2 \neq \mathcal{N}_0(p)$ implies that for all $q[B_2'] \in \mathcal{N}_2$, $B_2' = \mathcal{N}_1(p)$. In the case where $\mathcal{N}_2 = \mathcal{N}_1$, the step from $\mathcal{N}_0$ could only have composed with $\mathcal{N}_b$ by NPar, so $\mathcal{N}_b = \mathcal{N}_c$, Q.E.D.

Lemma 9 (Parallelism)**.** ***A):*** *If* $\mathcal{N}_1 \xrightarrow{\varnothing}{}^{*} \mathcal{N}_1'$ *and* $\mathcal{N}_2 \xrightarrow{\varnothing}{}^{*} \mathcal{N}_2'$ *then* $\mathcal{N}_1 \mid \mathcal{N}_2 \xrightarrow{\varnothing}{}^{*} \mathcal{N}_1' \mid \mathcal{N}_2 \xrightarrow{\varnothing}{}^{*} \mathcal{N}_1' \mid \mathcal{N}_2'$.
B): *If* $\mathcal{N}_1 \mid \mathcal{N}_2 \xrightarrow{\varnothing}{}^{*} \mathcal{N}_1' \mid \mathcal{N}_2 \xrightarrow{\varnothing}{}^{*} \mathcal{N}_1' \mid \mathcal{N}_2'$*, then* $\mathcal{N}_1 \xrightarrow{\varnothing}{}^{*} \mathcal{N}_1'$ *and* $\mathcal{N}_2 \xrightarrow{\varnothing}{}^{*} \mathcal{N}_2'$.

A.4.2 Proof of Lemma 9

A is just repeated application of NPar.

For **B**, observer that in the derivation tree of ever step of the sequence, some (possibly different) minimal sub-network will step by NPro or NCom as a precondition to some number of layers of NPar. The domains of these minimal sub-networks will be subsets of the domains of $\mathcal{N}_1$ and $\mathcal{N}_2$ respectively, so they can just combine via NPar to get the needed step in the respective sequences for $\mathcal{N}_1$ and $\mathcal{N}_2$.

A.4.3 Theorem 4

Theorem 4 says that if $\Theta; \varnothing \vdash M : T$ and $[\![M]\!] \xrightarrow{\varnothing}{}^{*} \mathcal{N}_n$, then there exists M' such that $M \longrightarrow^{*} M'$ and $\mathcal{N}_n \xrightarrow{\varnothing}{}^{*} [\![M']\!]$.

Declare the predicate $\mathsf{sound}(\mathcal{N})$ to mean that there exists some $M_{\mathcal{N}}$ such that $M \longrightarrow^{*} M_{\mathcal{N}}$ and $\mathcal{N} \xrightarrow{\varnothing}{}^{*} [\![M_{\mathcal{N}}]\!]$.

Consider the sequence of network steps $[\![M]\!] = \mathcal{N}_0 \xrightarrow{\varnothing} \ldots \xrightarrow{\varnothing} \mathcal{N}_n$. By Corollary 2, $\mathsf{sound}(\mathcal{N}_0)$. Select the largest i s.t. $\mathsf{sound}(\mathcal{N}_i)$. We will derive a contradiction from an assumption that $\mathcal{N}_{i+1}$ is part of the sequence; this will prove that $i = n$, which completes the proof of the Theorem.

Choose a sequence of network steps (of the possibly many such options) $\mathcal{N}_i = \mathcal{N}_i^a \xrightarrow{\varnothing} \ldots \xrightarrow{\varnothing} \mathcal{N}_m^a = [\![M^a]\!]$ where $M \longrightarrow^{*} M^a$.

Assume $\mathcal{N}_{i+1}$ is part of the original sequence. Decompose the step to it as $\mathcal{N}_i = \mathcal{N}_i^0 \mid \mathcal{N}_i^1 \xrightarrow{\varnothing} \mathcal{N}_i^0 \mid \mathcal{N}_{i+1}^1 = \mathcal{N}_{i+1}$ where $\mathcal{N}_i^1$'s domain is as large as possible. We will examine two cases: either the parties in $\mathcal{N}_i^1$ make steps in the sequence to $\mathcal{N}_m^a$, or they do not. Specifically, consider the largest j s.t. $\mathcal{N}_j^a = \mathcal{N}_j^b \mid \mathcal{N}_i^1$.

- Suppose $j < m$.

  By Lemma 8 and our decision that j is as large as possible, $\mathcal{N}_{j+1}^a = \mathcal{N}_j^b \mid \mathcal{N}_{i+1}^1$. Thus we have $\mathcal{N}_i^0 \mid \mathcal{N}_i^1 \xrightarrow{\varnothing}{}^{*} \mathcal{N}_j^b \mid \mathcal{N}_i^1 \xrightarrow{\varnothing} \mathcal{N}_j^b \mid \mathcal{N}_{i+1}^1$. By Lemma 9, we can reorganize that into an alternative sequence where $\mathcal{N}_i^0 \mid \mathcal{N}_i^1 \xrightarrow{\varnothing} \mathcal{N}_i^0 \mid \mathcal{N}_{i+1}^1 \xrightarrow{\varnothing}{}^{*} \mathcal{N}_j^b \mid \mathcal{N}_{i+1}^1$. Since $\mathcal{N}_i^0 \mid \mathcal{N}_{i+1}^1 = \mathcal{N}_{i+1}$ and $\mathcal{N}_{j+1}^a \xrightarrow{\varnothing}{}^{*} [\![M^a]\!]$, this contradicts our choice that i be as large as possible.

- Suppose $j = m$, so $[\![M^a]\!] = \mathcal{N}_m^b \mid \mathcal{N}_i^1$.

  By Lemma 9, $[\![M^a]\!]$ can step (because $\mathcal{N}_i^1$ can step) so by Corollary 2, $M^a \longrightarrow M^{a+1}$. We can repeat our steps from our choice of $\mathcal{N}_i^a \xrightarrow{\varnothing}{}^{*} \mathcal{N}_m^a = [\![M^a]\!]$, but using M^{a+1} instead of M^a. Since $\boldsymbol{\lambda_C}$ doesn't have recursion, eventually we'll arrive at a M^{a++} that can't step, and then-or-sooner we'll be in the first case above. Q.E.D.

A.5 Proof of The Completeness Theorem

Theorem 5 says that if $\Theta; \varnothing \vdash M : T$ and $M \longrightarrow M'$, then $[\![M]\!] \xrightarrow{\varnothing}{}^{*} [\![M']\!]$. We'll need a few lemmas first.

Lemma 10 (Cruft)**.** *If* $\Theta; \varnothing \vdash M : T$ *and* $p \notin \Theta$*, then* $[\![M]\!]_p = \bot$.

A.5.1 Proof of Lemma 10

By induction on the typing of M:

- TLambda: $p^+ \subseteq \Theta$, therefore $p \notin p^+$, therefore $[\![M]\!]_p = \bot$.
- TVar: Can't happen because M types with empty Γ.
- TUnit, TCom, TProj1, TProj2, and TProjN: Same as TLambda.
- TPair, TVec, TInl, and TInr: In each of these cases we have some number of recursive typing judgments to which we can apply the inductive hypothesis. This enables the respective cases of the definition of floor (as used in the respective cases of the definition of projection) to map to $\bot$.
- TApp: $M = N_1 N_2$. By induction, $[\![N_1]\!]_p = \bot$ and $[\![N_2]\!]_p = \bot$, so $[\![M]\!]_p = \bot$
- TCase: Similar to TLambda, by induction the guard projects to $\bot$ and therefore the whole thing does too.

Lemma 11 (Existence)**.** *If* $\Theta; \Gamma \vdash V : d@p^+$ *and* $p, q \in p^+$*, then* $[\![V]\!]_p = [\![V]\!]_q \neq \bot$.

A.5.2 Proof of Lemma 11

By induction on possible typings of V:

- TVar: Projection is a no-op on variables.
- TUnit: $[\![V]\!]_p = [\![V]\!]_q = ()$.
- TPair: $p, q \in p_1^+ \cap p_2^+$, so both are in each of them, so we can recurse on V_1 and V_2.
- TInl and TInr: simple induction.

Lemma 12 (Bottom)**.** *If* $\Theta; \varnothing \vdash M : T$ *and* $[\![M]\!]_p = \bot$ *and* $M \longrightarrow M'$ *then* $[\![M']\!]_p = \bot$.

A.5.3 Proof of Lemma 12

By induction on the step $M \longrightarrow M'$.

- AppAbs: $M = (\lambda x : T_x \,.\, N)@p^+V$, and necessarily $[\![(\lambda x : T_x \,.\, N)@p^+]\!]_p = \bot$. Since the lambda doesn't project to a lambda, $p \notin p^+$. $M' = N[x := V \triangleright p^+]$. By TLambda, Lemma 1, and Lemma 10, $[\![N[x := V \triangleright p^+]]\!]_p = \bot$.
- App1: $M = VN$ and necessarily $[\![V]\!]_p = [\![N]\!]_p = \bot$. By induction on $N \longrightarrow N'$, $[\![N']\!]_p = \bot$.
- App2: Same as App1.
- Case: The guard must project to $\bot$, so this follows from induction.
- CaseL (and CaseR by mirror image): $M = \mathsf{case}_{p^+}\, \mathsf{Inl}\, V\, \mathsf{of}\, \mathsf{Inl}\, x_l \Rightarrow M_l; \mathsf{Inr}\, x_r \Rightarrow M_r$ and $M' = M_l[x_l := V \triangleright p^+]$. Necessarily, $[\![V]\!]_p = \bot$. By TCase and MTData, $\mathsf{Inl}\, V$ types as data, so by Lemma 11 $p \notin p^+$. By TCase, Lemma 1, and Lemma 10, $[\![M']\!]_p = [\![M_l[x_l := V \triangleright p^+]]\!]_p = \bot$.
- Proj1: $M = \mathsf{fst}_{p^+}(\mathsf{Pair}\, V_1 V_2)$, and $p \notin p^+$. $M' = V_1 \triangleright p^+$. Since $\Theta; \varnothing \vdash V_1 : T'$ (by TPair) and $T' \triangleright p^+ = T''$ is defined (by TApp and the indifference of MTData to the data's structure), by Lemma 1 $p^+; \varnothing \vdash V_1 \triangleright p^+ : T''$. By Lemma 10 this projects to $\bot$.
- Proj2, ProjN, and Com1 are each pretty similar to Proj1.
- Com1, ComPair, ComInl, and ComInr: For M to project to $\bot$, p must be neither a sender nor a recipient. By induction among these cases (with Com1 as the base case), M' will be some structure of $()@r^+$; since $p \notin r^+$ and projection uses floor, this will project to $\bot$.

Lemma 13 (Masked)**.** *If* $p \in p^+$ *and* $V' = V \triangleright p^+$ *then* $[\![V]\!]_p = [\![V']\!]_p$.

A.5.4 Proof of Lemma 13

By (inductive) case analysis of endpoint projection:

- $[\![x]\!]_p = x$. By MVVar the mask does nothing.
- $[\![(\lambda x : T\,.\,M)@q^+]\!]_p$: Since $V \triangleright p^+$ is defined, by MVLambda it does nothing.
- $[\![()@q^+]\!]_p$: By MVUnit $V' = ()@(p^+ \cap q^+)$. p is in that intersection iff $p \in q^+$, so the projections will both be () or $\bot$ correctly.
- $\mathsf{Inl}\, V_l$, $\mathsf{Inr}\, V_r$, $\mathsf{Pair}\, V_1 V_2$, $(V_1, \ldots, V_n)$: simple recursion.
- fst_{q^+}, snd_{q^+}, $\mathsf{lookup}^i_{q^+}$, $\mathsf{com}_{q;q^+}$: Since the masking is defined, it does nothing.

Lemma 14 (Floor Zero)**.** $[\![M]\!]_p = \lfloor [\![M]\!]_p \rfloor$

A.5.5 Proof of Lemma 14

There are thirteen forms. Six of them (application, case, injection-r/l, pair and vector) apply floor directly in the definition of projection. Six of them (variable, unit, the three lookups, and com) can only project to values such that floor is a no-op. For a lambda $(\lambda x : T_x\,.\,N)@p^+$, the proof is by induction on the body N.

Lemma 15 (Distributive Substitution)**.** *If* $\Theta; (x : T_x) \vdash M : T$ *and* $p \in \Theta$*,*
then $[\![M[x := V]]\!]_p = \lfloor [\![M]\!]_p [x := [\![V]\!]_p] \rfloor$*. (Because* $[\![V]\!]_p$ *may be* $\bot$*, this isn't really distribution; an extra flooring operation is necessary.)*

A.5.6 Proof of Lemma 15

It'd be more elegant if substitution really did distribute over projection, but this weaker statement is what we really need anyway. The proof is by inductive case analysis on the form of M:

- $\mathsf{Pair}\, V_1 V_2$: $[\![M[x := V]]\!]_p = [\![\mathsf{Pair}\, V_1[x := V] V_2[x := V]]\!]_p$
  $= \lfloor \mathsf{Pair} [\![V_1[x := V]]\!]_p [\![V_2[x := V]]\!]_p \rfloor$
  and $[\![M]\!]_p [x := [\![V]\!]_p] = \lfloor \mathsf{Pair} [\![V_1]\!]_p [\![V_2]\!]_p \rfloor\, [x := [\![V]\!]_p]$.

– Suppose one of $[\![V_1]\!]_p, [\![V_2]\!]_p$ is not $\bot$. Then

$[\![M]\!]_p[x := [\![V]\!]_p] = (\mathsf{Pair}\, \lfloor [\![V_1]\!]_p \rfloor\, \lfloor [\![V_2]\!]_p \rfloor)[x := [\![V]\!]_p]$

which by Lemma 14 $= (\mathsf{Pair}[\![V_1]\!]_p[\![V_2]\!]_p)[x := [\![V]\!]_p]$

$= \mathsf{Pair}([\![V_1]\!]_p[x := [\![V]\!]_p])([\![V_2]\!]_p[x := [\![V]\!]_p])$.

Thus $\lfloor [\![M]\!]_p[x := [\![V]\!]_p] \rfloor = \lfloor \mathsf{Pair}([\![V_1]\!]_p[x := [\![V]\!]_p])([\![V_2]\!]_p[x := [\![V]\!]_p]) \rfloor$.

By induction, $[\![V_1[x := V]]\!]_p = \lfloor [\![V_1]\!]_p[x := [\![V]\!]_p] \rfloor$

and $[\![V_2[x := V]]\!]_p = \lfloor [\![V_2]\!]_p[x := [\![V]\!]_p] \rfloor$; with that in mind,

∗ Suppose one of $[\![V_1[x := V]]\!]_p, [\![V_1[x := V]]\!]_p$ is not $\bot$.

$\lfloor [\![M]\!]_p[x := [\![V]\!]_p] \rfloor = \mathsf{Pair}\, \lfloor [\![V_1]\!]_p[x := [\![V]\!]_p] \rfloor\, \lfloor [\![V_2]\!]_p[x := [\![V]\!]_p] \rfloor$,

and $[\![M[x := V]]\!]_p = \mathsf{Pair}\, \lfloor [\![V_1[x := V]\!]_p \rfloor\, \lfloor [\![V_2[x := V]]\!]_p \rfloor$

$= \mathsf{Pair}[\![V_1[x := V]\!]_p[\![V_2[x := V]]\!]_p$ Q.E.D.

∗ Otherwise, $\lfloor [\![M]\!]_p[x := [\![V]\!]_p] \rfloor = \bot = [\![M[x := V]]\!]_p$.

– Otherwise, $[\![M]\!]_p[x := [\![V]\!]_p] = \lfloor \mathsf{Pair}\, \bot\bot \rfloor\, [x := [\![V]\!]_p] = \bot$.

Note that, by induction *etc*, $[\![V_1]\!]_p = \bot = [\![V_1]\!]_p[x := [\![V]\!]_p] = \lfloor [\![V_1]\!]_p[x := [\![V]\!]_p] \rfloor = [\![V_1[x := V]]\!]_p$, and the same for V_2, so $[\![M[x := V]]\!]_p = \bot$, Q.E.D.

- $\mathsf{Inl}\, V_l$, $\mathsf{Inr}\, V_r$, $(V_1, \ldots, V_n)$: Follow the same inductive pattern as Pair.

- N_1N_2: $[\![M[x := V]]\!]_p = [\![N_1[x := V]N_2[x := V]]\!]_p = \lfloor [\![N_1[x := V]]\!]_p [\![N_2[x := V]]\!]_p \rfloor$

$$= \begin{cases} \lfloor [\![N_1[x := V]]\!]_p \rfloor = \bot, \lfloor [\![N_2[x := V]]\!]_p \rfloor = L : & \bot \\ \text{else} : & \lfloor [\![N_1[x := V]]\!]_p \rfloor\, \lfloor [\![N_2[x := V]]\!]_p \rfloor \end{cases}$$

$$= \begin{cases} [\![N_1[x := V]]\!]_p = \bot, [\![N_2[x := V]]\!]_p = L : & \bot \\ \text{else} : & [\![N_1[x := V]]\!]_p [\![N_2[x := V]]\!]_p \end{cases}$$

and $\lfloor [\![M]\!]_p[x := [\![V]\!]_p] \rfloor = \lfloor \lfloor [\![N_1]\!]_p [\![N_2]\!]_p \rfloor\, [x := [\![V]\!]_p] \rfloor$

$$= \begin{cases} \lfloor [\![N_1]\!]_p \rfloor = \bot, \lfloor [\![N_2]\!]_p \rfloor = L : & \lfloor \bot[x := [\![V]\!]_p] \rfloor = \bot \\ \text{else} : & \lfloor (\lfloor [\![N_1]\!]_p \rfloor\, \lfloor [\![N_2]\!]_p \rfloor)[x := [\![V]\!]_p] \rfloor \\ & \quad = \lfloor ([\![N_1]\!]_p[x := [\![V]\!]_p])([\![N_2]\!]_p[x := [\![V]\!]_p]) \rfloor \end{cases}$$

$$= \begin{cases} \lfloor [\![N_1]\!]_p[x := [\![V]\!]_p] \rfloor = \bot, \lfloor [\![N_2]\!]_p[x := [\![V]\!]_p] \rfloor = L : \bot \\ \text{else} : \lfloor [\![N_1]\!]_p[x := [\![V]\!]_p] \rfloor\, \lfloor [\![N_2]\!]_p[x := [\![V]\!]_p] \rfloor \end{cases}$$

(Note that we collapsed the $\lfloor [\![N_1]\!]_p \rfloor = \bot, \ldots$ case. We can do that because if $[\![N_1]\!]_p = \bot$ then so does $\lfloor [\![N_1]\!]_p[x := [\![V]\!]_p] \rfloor$ and if $[\![N_2]\!]_p = L$ then $\lfloor [\![N_2]\!]_p[x := [\![V]\!]_p] \rfloor$ is also a value.)
By induction, $[\![N_1[x := V]]\!]_p = \lfloor [\![N_1]\!]_p[x := [\![V]\!]_p] \rfloor$
and $[\![N_2[x := V]]\!]_p = \lfloor [\![N_2]\!]_p[x := [\![V]\!]_p] \rfloor$.

- y: trivial because EPP and floor are both no-ops.
- $(\lambda y : T_y \,.\, N)@p^+$:
  - If $p \notin p^+$, both sides of the equality are $\bot$.
  - If $V' = V \triangleright p^+$ is defined, then
    $[\![(\lambda y : T_y \,.\, N)@p^+[x := V]]\!]_p = [\![(\lambda y : T_y \,.\, N[x := V'])@p^+]\!]_p = \lambda y \,.[\![N[x := V']]\!]_p$
    and $\lfloor [\![(\lambda y : T_y \,.\, N)@p^+]\!]_p[x := [\![V]\!]_p] \rfloor$
    $= \lfloor (\lambda y \,.[\![N]\!]_p)[x := [\![V]\!]_p] \rfloor$
    $= \lfloor \lambda y \,.([\![N]\!]_p[x := [\![V]\!]_p]) \rfloor$
    $= \lfloor \lambda y \,.([\![N]\!]_p[x := [\![V']\!]_p]) \rfloor$ (by Lemma 13)
    $= \lambda y \,. \lfloor ([\![N]\!]_p[x := [\![V']\!]_p]) \rfloor$
    Then we do induction on N and V'.
  - Otherwise, substitution in the central program is a no-op.
    * $[\![(\lambda y : T_y \,.\, N)@p^+[x := V]]\!]_p = [\![(\lambda y : T_y \,.\, N)@p^+]\!]_p = \lambda y \,.[\![N]\!]_p$
      and
      $\lfloor [\![(\lambda y : T_y \,.\, N)@p^+]\!]_p[x := [\![V]\!]_p] \rfloor = \lfloor (\lambda y \,.[\![N]\!]_p)[x := [\![V]\!]_p] \rfloor$
      $= \lfloor \lambda y \,.([\![N]\!]_p[x := [\![V]\!]_p]) \rfloor$
      $= \lambda y \,. \lfloor [\![N]\!]_p[x := [\![V]\!]_p] \rfloor$.
    * Since we already known $(\lambda y : T_y \,.\, N)@p^+[x := V] = (\lambda y : T_y \,.\, N)@p^+$, we can apply Lemma 1 to M and unpack the typing of $M[x := V] = M$ to get $p^+; (y : T_y) \vdash N : T'$.
    * By Lemma 3, we get $N[x := V] = N$.
    * By induction on N and V, we get $\lfloor [\![N]\!]_p[x := [\![V]\!]_p] \rfloor = [\![N[x := V]]\!]_p = [\![N]\!]_p$, QED.
- $\mathsf{case}_{p^+} N \,\mathsf{of}\, \mathsf{Inl}\, x_l \Rightarrow N_l; \mathsf{Inr}\, x_r \Rightarrow N_r$:

  - If $[\![N]\!]_p = \bot$ then $\lfloor [\![N]\!]_p[x := [\![V]\!]_p] \rfloor = \bot = [\![N[x := V]]\!]_p$ (by induction), so both halfs of the equality are $\bot$.
  - Else if $p \notin p^+$, then we get

    $[\![\mathsf{case}_{p^+}\, N[x := V]\, \mathsf{of}\, \mathsf{Inl}\, x_l \Rightarrow N'_l; \mathsf{Inr}\, x_r \Rightarrow N'_r]\!]_p = \mathsf{case}_{p^+}[\![N[x := V]]\!]_p\, \mathsf{of}\, \mathsf{Inl}\, x_l \Rightarrow \bot; \mathsf{Inr}\, x_r \Rightarrow \bot$

    and

    $\lfloor [\![\mathsf{case}_{p^+}\, N\, \mathsf{of}\, \mathsf{Inl}\, x_l \Rightarrow N_l; \mathsf{Inr}\, x_r \Rightarrow N_r]\!]_p[x := [\![V]\!]_p] \rfloor$

    $= \lfloor (\mathsf{case}_{p^+}[\![N]\!]_p\, \mathsf{of}\, \mathsf{Inl}\, x_l \Rightarrow \bot; \mathsf{Inr}\, x_r \Rightarrow \bot)[x := [\![V]\!]_p] \rfloor$

    $= \lfloor \mathsf{case}_{p^+}[\![N]\!]_p[x := [\![V]\!]_p]\, \mathsf{of}\, \mathsf{Inl}\, x_l \Rightarrow \bot; \mathsf{Inr}\, x_r \Rightarrow \bot \rfloor$.

    Since we've assumed $\lfloor [\![N]\!]_p[x := [\![V]\!]_p] \rfloor \neq \bot$, these are equal by induction.
  - Else if $V' = V \triangleright p^+$ is defined then we can do induction similar similar to how we did for the respective lambda case, except the induction is three-way.
  - Otherwise, it's similar to the respective lambda case, just more verbose.

- $()@p^+$, fst_{p^+}, snd_{p^+}, $\mathsf{lookup}^i_{p^+}$, and $\mathsf{com}_{s;r^+}$: trivial because substitution and floor are no-ops.

Lemma 16 (Weak Completeness)**.** *If $\Theta; \varnothing \vdash M : T$ and $M \longrightarrow M'$ then $[\![M]\!]_p \xrightarrow{\oplus\mu;\ominus\eta}{}^{?} [\![M']\!]_p$. (i.e. it takes zero or one steps to get there.)*

A.5.7 Proof of Lemma 16

If $[\![M]\!]_p = \bot$ then this is follows trivially from Lemma 12, so assume it doesn't. We proceed with induction on the form of $M \longrightarrow M'$:

- AppAbs: $M = (\lambda x : T_x\,.\,N)@p^+V$, and $M' = N[x := V \triangleright p^+]$. By assumption, the lambda doesn't project to $\bot$, so $p \in p^+$ and $[\![M]\!]_p \xrightarrow{\oplus\varnothing;\ominus\varnothing} \lfloor [\![N]\!]_p[x := [\![V]\!]_p] \rfloor$ by LAbsApp.
  By Lemma 13 and Lemma 15 $\lfloor [\![N]\!]_p[x := [\![V]\!]_p] \rfloor = \lfloor [\![N]\!]_p[x := [\![V \triangleright p^+]\!]_p] \rfloor = [\![N[x := V \triangleright p^+]]\!]_p = [\![M']\!]_p$.
- App1: $M = VN \longrightarrow VN' = M'$. By induction, $[\![N]\!]_p \xrightarrow{\oplus\mu;\ominus\eta}{}^{?} [\![N']\!]_p$.

  - Assume $[\![V]\!]_p = \bot$. By our earlier assumption, $[\![N]\!]_p \neq \bot$. Since $[\![N]\!]_p$ can step; that step justifies a LApp1 step with the same annotations. If $[\![N']\!]_p$ is a value then that'll be handled by the floor built into LApp1.
  - Otherwise, the induction is even simpler, we just don't have to worry about possibly collapsing the whole thing to $\bot$.

- App2: $M = N_1 N_2 \longrightarrow N_1' N_2 = M'$. By induction, $[\![N_1]\!]_p \xrightarrow{\oplus\mu;\ominus\eta}{}^{?} [\![N_1']\!]_p$.
  - Assume $[\![N_2]\!]_p = L$. By our earlier assumption, $[\![N_1]\!]_p \neq \bot$. Since $[\![N_1]\!]_p$ steps, that step justifies a LApp2 step with the same annotations. If $[\![N_1']\!]_p$ is a value then that'll be handled by the floor built into LApp2.
  - Otherwise, the induction is even simpler.

- Case: By our assumptions, the guard can't project to $\bot$; we just do induction on the guard to satisfy LCase.

- CaseL (CaseR mirrors): $M = \mathsf{case}_{p^+} \mathsf{Inl}\, V \,\mathsf{of}\, \mathsf{Inl}\, x_l \Rightarrow M_l; \mathsf{Inr}\, x_r \Rightarrow M_r$, and $[\![M]\!]_p = \mathsf{case}\, \mathsf{Inl}[\![V]\!]_p \,\mathsf{of}\, \mathsf{Inl}\, x_l \Rightarrow B_l; \mathsf{Inr}\, x_r \Rightarrow B_r$. $[\![M]\!]_p \xrightarrow{\oplus\varnothing;\ominus\varnothing} \lfloor B_l[x_l := [\![V]\!]_p] \rfloor$ by LCaseL. $M' = M_l[x_l := V \triangleright p^+]$. If $p \in p^+$ then $B_l = [\![M_l]\!]_p$ and by Lemma 13 and Lemma 15 $\lfloor B_l[x_l := [\![V]\!]_p] \rfloor = \lfloor [\![M_l]\!]_p[x_l := [\![V]\!]_p] \rfloor = \lfloor [\![M_l]\!]_p[x_l := [\![V \triangleright p^+]\!]_p] \rfloor$
  $= [\![M_l[x_l := V \triangleright p^+]]\!]_p = [\![M']\!]_p$.
  Otherwise, $B_l[x_l := [\![V]\!]_p] = \bot$ and by TCase, Lemma 1, and Lemma 10, $[\![M']\!]_p = \bot$.

- Proj1: $M = \mathsf{fst}_{p^+}(\mathsf{Pair}\, V_1 V_2)$ and $M' = V_1 \triangleright p^+$. Since we assumed $[\![M]\!]_p \neq \bot$, $p \in p^+$.
  $[\![M]\!]_p = \mathsf{fst} \lfloor \mathsf{Pair}[\![V_1]\!]_p [\![V_2]\!]_p \rfloor = \mathsf{fst}(\mathsf{Pair}[\![V_1]\!]_p [\![V_2]\!]_p)$ by Lemma 11 and TPair. This steps by LProj1 to $[\![V_1]\!]_p$, which equals $[\![M']\!]_p$ by Lemma 13.

- Proj2, ProjN: Same as Proj1.

- Com1: $M = \mathsf{com}_{s;r^+}()@p^+$ and $M' = ()@r^+$.
  - $s = p$ and $p \in r^+$: By MVUnit, $p \in p^+$, so $[\![M]\!]_p = \mathsf{send}^*_{r^+ \setminus \{p\}}()$, which steps by LSendSelf (using LSend1) to $()$. $[\![M']\!]_p = ()$.

  - $s = p$ and $p \notin r^+$: By MVUnit, $p \in p^+$, so $[\![M]\!]_p = \mathsf{send}_{r^+}()$, which steps by LSend1 to $\bot$. $[\![M']\!]_p = \bot$.
  - $s \neq p$ and $p \in r^+$: $[\![M]\!]_p = \mathsf{recv}_s[\![()@p^+]\!]_p$, which can step (arbitrarily, but with respective annotation) by LRecv to $[\![M']\!]_p$.
  - Otherwise, we violate our earlier assumption.

- ComPair, ComInl, and ComInr: Each uses the same structure of proof as Com1, using induction between the cases to support the respective process-semantics step.

A.5.8 Theorem 5

Theorem 5 says that if $\Theta; \varnothing \vdash M : T$ and $M \longrightarrow M'$, then $[\![M]\!] \xrightarrow{\varnothing}{}^{*} [\![M']\!]$.

The proof is by case analysis on the semantic step $M \longrightarrow M'$:

- AppAbs, CaseL, CaseR, Proj1, Proj2, and ProjN: Necessarily, the set of parties p^+ for whom $[\![M]\!]_{p \in p^+} \neq \bot$ is not empty. For every $p \in p^+$, by Lemma 16 $[\![M]\!]_p \xrightarrow{\oplus\varnothing;\ominus\varnothing}{}^{?} [\![M']\!]_p$ (checking the cases to see that the annotations are really empty!). By NPro, each of those is also a network step, which by Lemma 9 can be composed in any order to get $[\![M]\!] \xrightarrow{\varnothing}{}^{*} \mathcal{N}$. For every $p \in p^+$, $\mathcal{N}(p) = [\![M']\!]_p$, and (by Lemma 12) for every $q \notin p^+$, $\mathcal{N}(q) = \bot = [\![M']\!]_q$, Q.E.D.

- Com1, ComPair, ComInl, and ComInr: $M = \mathsf{com}_{s;r^+} V$. By the recursive structure of Com1, ComPair, ComInl, and ComInr, M' is some structure of $\{\mathsf{Pair}, \mathsf{Inl}, \mathsf{Inr}, ()@r^+\}$, and $[\![M']\!]_{r \in r^+} = [\![V]\!]_s$. For every $q \notin r^+ \cup \{s\}$, $[\![M]\!]_q = \bot = [\![M']\!]_q$ by Lemma 12. Consider two cases:

  - $s \notin r^+$:

    By Lemma 16 $[\![M]\!]_s = \mathsf{send}_{r^+}[\![V]\!]_s \xrightarrow{\oplus\{(r,[\![V]\!]_s)\mid r \in r^+\};\ominus\varnothing} \bot$.

    By the previously mentioned structure of M', $[\![M']\!]_s = \bot$.

    For every $r \in r^+$, by Lemma 16 $[\![M]\!]_r = \mathsf{recv}_s[\![V]\!]_r \xrightarrow{\oplus\varnothing;\ominus\{(s,[\![V]\!]_s)\}} [\![V]\!]_s = [\![M']\!]_r$.

    By NPro, $s[[\![M]\!]_s] \xrightarrow{s:\{(r,[\![V]\!]_s)\mid r \in r^+\}} s[\bot = [\![M']\!]_s]$.

    This composes in parallel with each of the $r_{\in r^+}[[\![M]\!]_r]$ by NCom in any order until the unmactched send is empty. Everyone in and not-in $r^+ \cup \{s\}$ has stepped, if needed, to the respective projection of M'.

– $s \in r^+$: Let $r_0^+ = r^+ \setminus \{s\}$.
By Lemma 16 $[\![M]\!]_s = \mathsf{send}^*_{r_0^+}[\![V]\!]_s \xrightarrow{\oplus\{(r,[\![V]\!]_s)\mid r\in r_0^+\};\ominus\varnothing} [\![V]\!]_s = [\![M']\!]_{s\in r^+}$.
For every $r \in r_0^+$, by Lemma 16 $[\![M]\!]_r = \mathsf{recv}_s[\![V]\!]_r \xrightarrow{\oplus\varnothing;\ominus\{(s,[\![V]\!]_s)\}} [\![V]\!]_s = [\![M']\!]_r$.
We proceed as in the previous case.

- App1 (App2 and Case are similar): $M = VN$. By induction, $[\![N]\!] \xrightarrow{\varnothing}{}^* [\![N']\!]$. Every N step in that process in which a single party advances by NPro can justify a corresponding M step by LApp1. NCom steps are basically the same: each of the participating parties will justify a LApp1 M step with a N step; since this doesn't change the send & receive annotations, the cancellation will still work.