Empirical analysis and optimization of an *NP*-hard algorithm using CSP and FDR

Douglas A. Creager[1]

RedJack, LLC
1022 Stirling Road
Silver Spring, MD 20901
United States

Andrew C. Simpson[2]

Oxford University Computing Laboratory
Wolfson Building, Parks Road
Oxford, OX1 3QD
United Kingdom

Abstract

In many cases where an algorithm is provably *NP*-hard, this intractability is a worst-case bound that only applies to pathological inputs. In these cases, by exploiting knowledge of the specific structure of "real-world" inputs, the algorithm can be shown to be much more efficient in the "normal" case. However, when studying a new problem, this can be difficult to show if it is not obvious which structural constraints exist, and which ones would lead to increases in efficiency. In this paper, we show how one can describe the underlying problem declaratively as a CSP process and use the FDR refinement checker to explore the complexity space of the problem. By knowing which optimizations FDR uses to find solutions more efficiently, we can determine under which conditions the worst-case intractable algorithm executes efficiently, and incorporate analogous optimizations into the algorithm to exploit these conditions.

Keywords: Algorithm design and analysis, CSP, graph theory, model checking.

1 Introduction

The class *NP* is often used as a benchmark for deciding when an algorithm or problem is "difficult"; whereas the space requirements and running time of an algorithm with a polynomial solution will increase reasonably with the size of the input, *NP* space requirements and running times tend to scale exponentially. Algorithms in *NP* are often therefore only realistically useful on the most trivial of inputs.

Of course, the fact that a particular algorithm is in *NP* does not necessarily imply that the underlying problem is itself difficult — it might be that a polynomial-time

[1] Email: douglas.creager@redjack.com
[2] Email: andrew.simpson@comlab.ox.ac.uk

This paper is electronically published in
Electronic Notes in Theoretical Computer Science
URL: www.elsevier.nl/locate/entcs

algorithm exists but has not yet been discovered. *NP*-hard algorithms are those where this is highly unlikely; any polynomial-time solution to an *NP*-hard problem could be used to create polynomial-time solutions to *every* other algorithm in *NP*. Though it has not been proved, our current intuition is that $P \neq NP$, and therefore that *NP*-hard problems cannot have any polynomial-time solutions.

Sometimes, however, this is only a worst-case bound on the complexity of an algorithm. There might be classes of inputs for which the problem is simpler, and therefore tractable. For example, this is exactly the case with Petri nets [20,21]: in the general case, the reachability problem is *EXPSPACE*-complete. However, as summarized in [12], by introducing constraints on the structure of the Petri net, different classes are formed with tractable reachability algorithms. If we can guarantee that each place in the Petri net will only ever contain at most one token, then reachability becomes *PSPACE*-complete. If, in addition, the net contains no cycles, reachability becomes *NP*-hard. If we further stipulate that each place in the Petri net can have at most one output transition, reachability becomes polynomial.

When studying a new problem domain, an important task is to discover which of the associated algorithms are *NP*-hard, and, if possible, which simplifications of the problem domain make these algorithms tractable in the "normal" case. Finding these subproblems is not always trivial; often, a lot of analysis and intuition is needed before an appropriate breakthrough is made.

In this paper we present an alternative, empirical, approach, applying it to a new data transformation discovery algorithm that is provably *NP*-hard in the worst case. We first create a description of the problem using the Communicating Sequential Processes process algebra (CSP) [16,23]. This mathematically rigorous and machine-readable problem description can then be solved by the FDR refinement checker [22,25]. By using many varying inputs and slight modifications to the process description, FDR can be used to analyze the space and time complexity of different algorithmic solutions to the problem. With an understanding of the particular normalizations and optimizations that FDR uses "under the hood", we can then use the same strategies when developing our own algorithmic solution.

There are many other examples in the literature of empirical approaches to analyzing the complexity of an algorithm or program (including, but not limited to, [19,6,17]). However, these approaches focus on existing low-level implementations of an algorithm. Our approach differs from these examples in that we examine a high-level description of the *problem*, written in a declarative style. This allows us to identify useful optimizations and an overall implementation strategy *before* developing a low-level algorithm to solve the problem.

The rest of this paper is organized as follows. Section 2 presents an overview of our particular problem of interest. Section 3 shows how the problem can be formulated as a refinement between two CSP processes. Section 4 shows how FDR can be used to analyze the space and time complexity of the problem, and how different changes to the CSP script affect the complexity of the solution. In Section 5, we interpret these measurements in terms of real-world transformation graphs, and use these insights to develop a useful algorithmic solution. Finally, Section 6 discusses our results and suggests areas for future research.

2 Problem description

The problem that we consider involves the automated discovery of data transformations. In a heterogeneous environment like the Internet, communicating applications will likely encode and structure their data differently, even if the data represents logically similar real-world concepts and objects. Since rewriting the applications to use an identical data model will often be an infeasible solution, some form of *data transformation* is needed to reconcile these differences. Ideally, the discovery of these transformations would be automated, reducing the amount of effort needed to link two disparate applications.

The approach taken in [8] is to exploit the fact that transformations are composable. We assume that some *atomic transformations* will necessarily be written manually; however, given a sufficient number of them, a directed graph can be constructed with datatypes as nodes and atomic transformations as edges. An example transformation graph, containing datatypes and transformations for a variety of microscope image formats and their associated metadata, is shown in Figure 1. Since atomic transformations are composable, paths in the graph represent executable *compound transformations*, and an efficient pathfinding algorithm, such as Dijkstra's [10] or Bellman-Ford [3,13], can be used to discover them. Further, the same graph can be used to support use cases with different non-functional requirements through the appropriate use of edge weights.

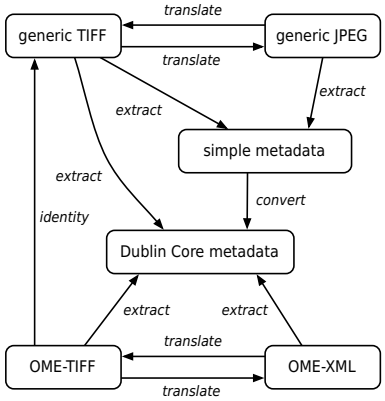

Fig. 1. A transformation graph for images and associated metadata

Unfortunately, since graph edges have exactly one source node and exactly one sink node, this graph-based model limits transformations to a single input and output. If we want to support transformations of higher arity, a more complex model is needed. An obvious extension is to use *hypergraphs* [4,5,1], whose *hyperedges* can connect multiple nodes. Figure 2 shows how a polyadic transformation graph could be represented as a hypergraph. The analogous *shortest hyperpath* algorithm would then be used to discover compound transformations. Hyperpaths are more complex than standard paths, in that there are a number of ways to calculate a hyperpath's weight given the weights of its constituent edges [18,2]. For instance, if an edge appears in a hyperpath multiple times, its weight can either be counted exactly once, or once for each of its appearances in the hyperpath. These different metrics yield different complexities for the shortest hyperpath problem, some of which are

polynomial; however, the metric that we would use for transformation discovery, *cost*, is *NP*-hard.

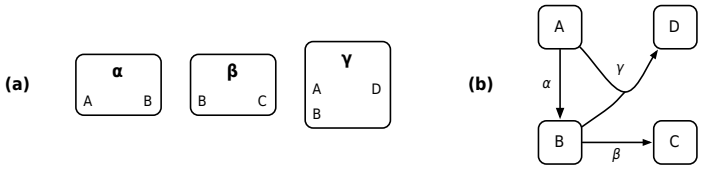

Fig. 2. A polyadic transformation graph represented by a hypergraph

The hope, however, is that this is a worst-case bound for pathological transformation graphs, and that for more common "real-world" graphs, the discovery algorithm would be tractable. In the remainder of this paper, we use CSP and FDR to investigate this hypothesis.

3 CSP implementation

In this section, we describe a prototype implementation of the transformation discovery problem described in the previous section, written in CSP. The usual strategy for working with CSP specifications is to define two processes: one providing a specification of what the system should do, and the other describing a particular implementation of the system. One then uses a refinement checker such as FDR to verify that the implementation refines, and therefore satisfies, the specification.

We will follow a similar approach, though our CSP processes will not describe a "specification" and "implementation", *per se*. Instead, we will use the first process to describe the structure of the graph, and the basic rules about when transformations can be executed. We will use the second process to describe the specific property that we are looking for in a solution: that, given instances of a particular set of *initial datatypes*, there is some sequence of transformations that can be executed that will yield instances of a different set of *desired datatypes*. Note that we do not describe *how* to find solutions; we only provide a declarative description of the problem structure and of valid solutions.

3.1 Graph structure

We start by declaring the CSP types needed for the specification. The *Datatype* type represents a single datatype from the transformation graph. (The overloading of the term "datatype" is unfortunate but unavoidable; we will use "type" to refer to the syntactic concept in the CSP language, and "datatype" to refer to a node in a transformation graph.) A *Transformation* has a unique identifier, and is defined by two sets of datatypes: one for its inputs and one for its outputs. A particular transformation graph can be encoded by providing concrete values for the *Datatype* type and the *Transformations*, *GivenTypes*, and *DesiredTypes* variables. The *Transformations* variable contains all of the transformations in the graph. The *GivenTypes* variable specifies which datatypes we are given instances of, while *DesiredTypes* specifies which datatypes need to be generated by the discovered compound transformation.

datatype $Datatype, XformID$
nametype $Transformation = XformID \times (\mathbb{P}\, Datatype) \times (\mathbb{P}\, Datatype)$
variable $Transformations, GivenTypes, DesiredTypes$

Next we define the event channels that will be used in the specification. The *have* channel signals when a datatype has become available, regardless of how it was obtained. The *given* channel is used to notify other processes which datatypes are given. The *execute* channel signals that a particular atomic transformation has executed. The *produce* channel indicates that a datatype has been produced as the output of some transformation. Finally, the *finish* channel signifies that a datatype has been used as the final result of the compound transformation.

channel $given, have, produce, finish : Datatype$
channel $execute : XformID$

Now we can construct the CSP process that represents the structure and rules of a transformation graph. We follow the standard approach of declaring subprocesses for each of the individual properties or constraints of the system, which we then compose together into a final specification using parallel composition.

We first define a *MakeAvailable* process that is responsible for generating *have* messages whenever a datatype instance becomes available. This can happen in one of two ways: we can be given the instance (in which case we match a *given* message), or it can be generated by the execution of a transformation (in which case we match a *produce* message).

$$\alpha(MakeAvailable) = \{|given, produce, have|\}$$
$$\begin{aligned} &MakeAvailable = \\ &\quad given?t \rightarrow have!t \rightarrow MakeAvailable \\ &\quad \Box \\ &\quad produce?t \rightarrow have!t \rightarrow MakeAvailable \end{aligned}$$

Next we define a *Given* process that generates the initial *given* messages for the datatypes that we start with. The alphabet of this process contains *all* *given* messages, even though only certain *given* messages are created; this ensures that CSP events only appear for those datatypes that actually are given to us.

$$\alpha(Given) = \{|given|\}$$
$$Given = \|\| t : GivenTypes \bullet given!t \rightarrow Stop$$

Next we define a process to handle the *finish* messages. We keep track of which datatypes we have; when one of the *DesiredTypes* becomes available, we allow a *finish* event for it. We do not want to generate multiple *finish* events for any datatype, so we must also keep track of the datatypes that have already been *finish*ed. This means that we only allow a *finish* event if the datatype is one of the desired outputs, it is available, and we have not already generated a *finish* event for it.

$$\alpha(Finish) = \{\!|finish, have|\!\}$$
$$Finish =$$
$$\quad \text{let}$$
$$\quad\quad Have(avail, finished) =$$
$$\quad\quad\quad have?t \rightarrow Have(avail \cup \{t\}, finished)$$
$$\quad\quad\quad \Box$$
$$\quad\quad\quad finish?t : (avail \setminus finished) \cap DesiredTypes \rightarrow$$
$$\quad\quad\quad\quad Have(avail, finished \cup \{t\})$$
$$\quad \text{within}$$
$$\quad\quad Have(\varnothing, \varnothing)$$

Our next process is responsible for preventing a particular transformation from executing before all of its inputs are satisfied. We define it similarly to the *Finish* process: we keep track of which input datatypes we have; once all of them are available, we allow any number of *execute* events to occur for this transformation. The process alphabet contains a *have* event for each input datatype, and the *execute* event for the transformation.

$$\alpha(XformPrereq(\,(id, inputTypes, outputTypes)\,)) =$$
$$\quad \{execute.id\} \cup \{\, t : inputTypes \bullet have.t \,\}$$
$$XformPrereq(\,(id, inputTypes, outputTypes)\,) =$$
$$\quad \text{let}$$
$$\quad\quad Have(avail) =$$
$$\quad\quad\quad (avail = inputTypes)\ \&\ execute!id \rightarrow Have(avail)$$
$$\quad\quad\quad \Box$$
$$\quad\quad\quad have?t : inputTypes \rightarrow Have(avail \cup \{t\})$$
$$\quad \text{within}$$
$$\quad\quad Have(\varnothing)$$

For the transformation graphs described in this paper, we assume that every datatype is *reusable*: that any instance of the datatype can be used multiple times without penalty. For this reason, we do not remove any elements from the set of available datatypes in the *Finish* and *XformPrereq* processes. If desired, we could use a more complicated definition for these processes to limit the number of times that a particular datatype could be consumed.

The above process verifies that the prerequisites are satisfied for a single transformation. We must use parallel composition to combine them: since multiple transformations might be waiting for the same datatype to satisfy an input, they must be notified of its availability simultaneously. This means that they must synchronize on the corresponding *have* event. This parallel composition yields the *Prereqs* process, which verifies the prerequisites of each atomic transformation simultaneously.

$$\alpha(Prereqs) = \bigcup\{\, xf : Transformations \bullet \alpha(XformPrereq(xf)) \,\}$$
$$Prereqs = \Big\|\, xf : Transformations \bullet XformPrereq(xf)$$

Next we define a process that describes what happens when a particular transformation is executed. The process is fairly straightforward: it waits for the appro-

priate *execute* event, after which it outputs *produce* events for each of the transformation's output datatypes. We use replicated interleaving to allow the *produce* events to occur in any order. The overall process then ends in *Skip*. The process alphabet does not contain any extra events — only the *execute* and *produce* messages appropriate to the transformation.

$$\alpha(ExecuteOneOnce(\,(id, inputTypes, outputTypes)\,)) = \\ \quad \{execute.id\} \cup \{\, t : outputTypes \bullet produce.t \,\}$$
$$ExecuteOneOnce(\,(id, inputTypes, outputTypes)\,) = \\ \quad execute!id \rightarrow (|||\, t : outputTypes \bullet produce!t \rightarrow Skip)$$

The *ExecuteOneOnce* process is parameterized on the definition of a transformation; now we instantiate this process for each of the actual transformations in the graph. The *ExecuteAnyOnce* process allows the environment to execute any one transformation. Its alphabet consists of *all* of the *produce* messages, since we want to prevent datatypes that do not play a part in some transformation from being produced.

$$\alpha(ExecuteAnyOnce) = \{|\, execute, produce \,|\}$$
$$ExecuteAnyOnce = \Box\, xf : Transformations \bullet ExecuteOneOnce(xf)$$

With the *ExecuteAnyOnce* process, we have allowed the environment to execute a single transformation. Now we allow it to execute a sequence of them. Since the *ExecuteAnyOnce* process ends with a *Skip* (due to it being defined in terms of *ExecuteOneOnce*), we can accomplish this with a recursive sequential composition. The *Execute* process allows *any* sequence of transformations to be executed; it does not need to take into account whether a transformation has its inputs satisfied. This constraint is handled by the *Prereqs* process, and so it will be introduced automatically when we compose together all of the graph processes.

$$\alpha(Execute) = \alpha(ExecuteAnyOnce)$$
$$Execute = ExecuteAnyOnce \fatsemi Execute$$

Finally, we can merge together all of the previous processes using parallel composition. This yields an overall *Graph* process that satisfies the constraints introduced by each of its constituent parts. We also provide a view of the graph (*GraphOutputs*) that hides everything except for the *finish* channel; this allows us to only concern ourselves with which final datatypes can actually be produced, without worrying about the details of which transformations were executed.

$$\alpha(Graph) = \{|\, given, have, execute, produce, finish \,|\}$$
$$Graph = MakeAvailable \parallel Given \parallel Finish \parallel Prereqs \parallel Execute$$

$$\alpha(GraphOutputs) = \{|\, finish \,|\}$$
$$GraphOutputs = Graph \setminus (\alpha(Graph) \setminus \{|\, finish \,|\})$$

3.2 Transformation discovery process

Next we construct the CSP process that tests whether all of the desired datatypes are eventually produced by some compound transformation. When we only have a single desired type, this is exceedingly simple. Since we have hidden everything except for the *finish* message for our desired type, we just want to ensure that this message occurs. This property is given by the $Want'_T$ process, which has exactly two traces:

$$Want'_T(\{t\}) = finish!t \rightarrow Stop$$
$$traces\,[\![\ Want'_T(\{t\})\ ]\!] = \{\langle\rangle, \langle finish.t\rangle\}$$

The empty sequence is a trace of every process. We are hoping that $\langle finish.t\rangle$ will be a trace of $GraphOutputs$, since this would imply that there is some sequence of transformations that produces the desired datatype. If this is true, the traces of $Want'_T$ will be a subset of the traces of $GraphOutputs$. Therefore, a traces refinement check will provide us with a solution:

$$\text{assert } GraphOutputs \sqsubseteq_T Want'_T(DesiredTypes)$$

We can use a similar traces check when we have many desired output datatypes. We can construct a $Want_T$ process that allows the appropriate *finish* events in any order:

$$Want_T(\varnothing) = Stop$$
$$Want_T(types) = |||\ t : types \bullet finish!t \rightarrow Stop$$
$$traces\,[\![\ Want_T(\{t_1, t_2\})\ ]\!] =$$
$$\{\langle\rangle, \langle finish.t_1\rangle, \langle finish.t_2\rangle, \langle finish.t_1, finish.t_2\rangle, \langle finish.t_2, finish.t_1\rangle\}$$

If the transformation graph can generate all of these datatypes, the *GraphOutputs* process will output exactly one *finish* message for each. Further, since the *finish* messages are not coupled to the order in which the atomic transformations are executed, $GraphOutputs$ will be able to output these *finish* messages in any order. Thus, the traces of $Want_T$ will be a subset of the traces of $GraphOutputs$. (In fact, because neither process has any other visible events, they will be traces-equivalent.)

On the other hand, if the graph *cannot* generate each desired datatype, then the *GraphOutput* process will not have any trace containing every *finish* event. Since $Want_T$ does contain such a trace, the traces of $Want_T$ will *not* be a subset of the traces of $GraphOutputs$. This means that a valid compound transformation exists iff the following refinement holds:

$$\text{assert } GraphOutputs \sqsubseteq_T Want_T(DesiredTypes)$$

Unfortunately, while this correctly tells us if a compound transformation *exists*, it does not tell us what the transformation *is*. Luckily, we can find this information with only slight modifications. We create a new $Want_F$ process as follows:

$$Want_F(\varnothing) = Stop$$
$$Want_F(\{t\}) = Stop$$
$$Want_F(types) = \sqcap\, t : types \bullet finish!t \rightarrow Want_F(types \setminus \{t\})$$

This differs from $Want_T$ in two respects. First, we use internal choice instead of interleaving to establish each permutation of the *finish* events. Second, for each of these permutations, we only accept *all but one* of the *finish* events, refusing the final one.

With these changes, we can use the *stable failures* model of CSP instead of the previous traces model. If there is a valid compound transformation, the *GraphOutputs* process must allow every *finish* message to occur, in any permutation. The $Want_F$ process, however, only accepts all but one of these events; there is no situation where it will accept every *finish* event. Thus, the stable failures of *GraphOutputs* are *not* a subset of the stable failures of $Want_F$.

If, on the other hand, no compound transformation is possible, then there must be at least one *finish* event that *GraphOutputs* refuses. Further, it will refuse this *finish* event at every point during its execution. $Want_F$ can also refuse this event at any point: either because there are other *finish* events for the internal choice to fall back on, or because it is the final remaining *finish* event, which it always refuses. Thus, the stable failures of *GraphOutputs* *are* a subset of the stable failures of $Want_F$. We can now check the following negated refinement:

$$\text{assert } Want_F\,(DesiredTypes) \not\sqsubseteq_F GraphOutputs$$

(Note that our choice of model is important. The *Graph* process can execute the same transformation repeatedly forever, which causes the *GraphOutputs* process to diverge. By using the stable failures model instead of the failures-divergences model, we ignore these situations.)

When we check this refinement, there are two possible outcomes. If the refinement check succeeds, then we know that there is no valid compound transformation. If it fails, then the compound transformation exists, and FDR will provide a counterexample to the refinement. By examining this counterexample, we will find the sequence of *execute* events that defines the execution order of the compound transformation solution. Furthermore, since FDR uses a breadth-first search to perform the refinement check, the counterexample returned will be the one with the fewest events in its trace. Since this corresponds to the compound transformation with the fewest atomic transformations, the result of the refinement check will be the optimal transformation solution.

4 Analysis using FDR

In the previous section we presented a declarative description of the polyadic discovery problem using the CSP process algebra. By casting the problem as a suitable refinement test between two processes, we can use the FDR refinement checker as a prototype implementation. In this section, we run this refinement check over many different transformation graphs, of varying shapes and sizes, recording how

efficiently FDR can find solutions. Doing so gives us an empirical view of the complexity space of the problem, with the hope of finding regions of inputs for which the discovery algorithm is more efficient than the *NP*-hard worst-case bound. Ideally, these regions will correspond to the kinds of transformation graphs that are more likely to appear in practice, suggesting that there is an algorithmic solution that will be useful in the normal case.

The obvious way to measure the space and time complexity of our prototype would be to record the maximal amount of memory used by FDR, and the amount of wallclock or actual processor time that it takes to perform the refinement check. However, we use a different metric: all measurements are made with respect to the underlying labeled transition system (LTS) that FDR creates for a compiled CSP process. Because of *supercompilation* [14], FDR will usually not have to store the process's entire abstract LTS in memory. We measure the space complexity as the size of this smaller supercompiled LTS. The refinement check, however, must be performed on the full abstract LTS, which requires *explicating* the supercompiled LTS into its full form. (The explicated LTS nodes are allocated and deallocated as they are needed, so as to avoid storing the full LTS in memory at once.) We therefore use the number of explicated LTS states visited during the refinement check as a measure of the time complexity.

We measure the space and time complexity in this way because these measurements depend only on the definition of the CSP process. The space complexity metric is fully deterministic, since FDR will always compile a CSP process into the same LTS. The time metric is fully deterministic, as well, since FDR will perform the same search for any particular refinement check. Our measurements, therefore, do not depend on the speed or load of the machine used to perform the refinement check, and are more reproducible.

4.1 Space complexity

Our first experiment is to measure the space complexity of the constructed graph representation. The "before" curves in Figure 3 show the size of the labeled transition system that FDR constructs for the transformation graph processes. Initially, we only consider how the graph size is affected by the number of datatypes in the graph, so we consider graphs containing a varying number of datatypes and no transformations. As the figure shows, the graph size grows very quickly; graphs with more than twenty datatypes took over an hour to compile on a reasonably fast workstation.

The problem is with the *Finish* and *XformPrereq* processes, specifically with their internal *Have* subprocesses. These subprocesses track the set of available datatypes as a state parameter. Unfortunately, sets require exponential space; since FDR is compiling this subprocess into a low-level operator tree, the *Have* process's LTS also requires exponential space. Luckily, we can modify the *Finish* process as follows:

```
Finish =
  let
```

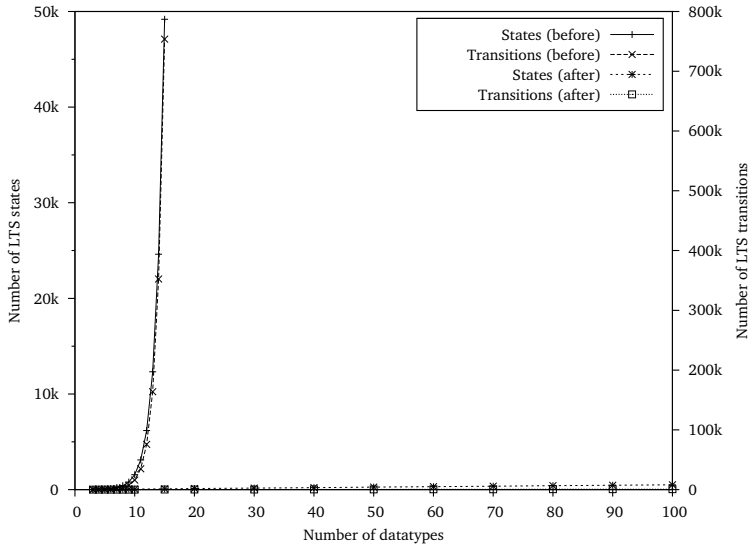

Fig. 3. Space required for the transformation graph process

$$
\begin{array}{l}
\quad DontHave(t) = have!t \rightarrow Have(t) \\
\quad Have(t) = \\
\qquad (t \in DesiredTypes)\ \&\ finish!t \rightarrow Finished(t) \\
\qquad \Box \\
\qquad have!t \rightarrow Have(t) \\
\quad Finished(t) = have!t \rightarrow Finished(t) \\
\text{within} \\
\quad ||| \ t : Datatype \bullet DontHave(t)
\end{array}
$$

We can make a similar modification to *XformPrereq*:

$$
\begin{array}{l}
XformPrereq(\ (id, inputTypes, outputTypes)\ ) = \\
\quad \text{let} \\
\qquad \alpha(DontHave(t)) = \{execute.id, have.t\} \\
\qquad DontHave(t) = have!t \rightarrow Have(t) \\
\qquad Have(t) = (execute!id \rightarrow Have(t)) \ \Box \ (have!t \rightarrow Have(t)) \\
\quad \text{within} \\
\qquad || \ t : inputTypes \bullet DontHave(t)
\end{array}
$$

Here we have redefined the internal subprocesses to only keep track of a single datatype. We then create copies of these internal subprocesses for each of the datatypes, and use a composition operator to combine them. For the *Finish* process, we can use interleaving, since the subprocess alphabets are disjoint. In the *XformPrereq* process, on the other hand, the subprocesses for each input datatype must synchronize on the *execute* event, since all of the inputs must be available before the transformation can proceed. We must therefore use alphabetized parallel for the composition. FDR will compile these subprocesses into low-level operator trees; however, since they no longer maintain exponential state, these trees will be small. The composition of these smaller processes is far more efficient than the original

exponential LTS; the "after" curves in Figure 3 show the same space measurements for a graph constructed with the modified subprocesses. With this modification, we are easily able to represent graphs with hundreds of datatypes.

Next we show how the size of the graph process is affected by the number and arrangement of transformations in the graph. For this experiment, we fix the number of datatypes in the graph, and examine four situations. First, as a control, we examine the graph with no transformations. Second, we introduce a single directed cycle of transformations that encompasses all of the datatypes in the graph. Third, we consider a graph with two directed cycles, pointing in opposite directions. Finally, we consider the fully-connected graph, where a transformation directly connects every possible pair of datatypes.

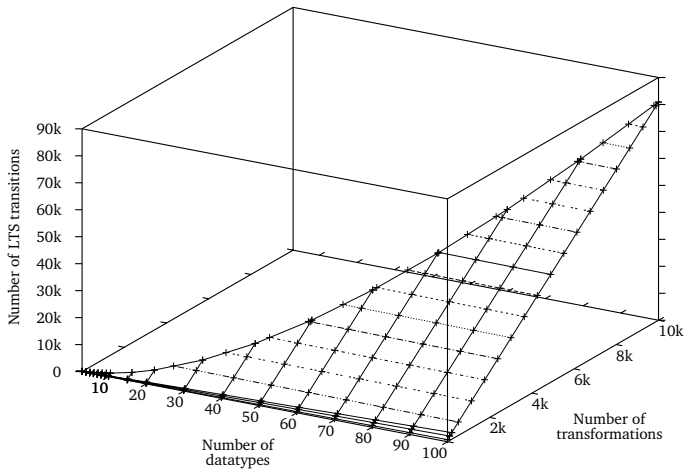

Fig. 4. Relationship between datatypes, transformations, and LTS size

Figure 4 shows how the size of the LTS depends on the number of datatypes and transformations for each style of graph. Part of the overall growth comes from the datatypes, and part comes from the transformations. The contour lines show that the resulting surface is planar, yielding an $O(D + T)$ overall size for a graph's LTS. The XY plane represents how the number of transformations depends on the number of datatypes for a particular style of graph; projecting a particular graph's curve up onto the growth plane then yields a single growth curve for that style of transformation graph.

4.2 Time complexity

Next we examine the time complexity of the algorithm. We again look at four different "shapes" of transformation graph, shown in Figure 5. In all cases, we are seeking a transformation between the source datatype S and the destination datatype D. The shapes differ in the number of additional datatypes in the graph, and in how the datatypes are connected. In part (a), we have a single sequence of datatypes A_1 through A_n, with a single path through the graph from S to D. In part (b), we have the same sequence of datatypes A_1 through A_n, but in this case,

they are not needed to transform from S to D. In part (c), we have two sequences of datatypes, A_1 through A_n and B_1 through B_n, between S and D. Either one can be used as a valid transformation path. Finally, in part (d), we again have two sequences of datatypes between S and D, but we introduce crosslinks as well, allowing the algorithm to jump from the A datatypes to the B datatypes at any point in the sequence. In this graph, there are $n + 2$ valid transformations between S and D.

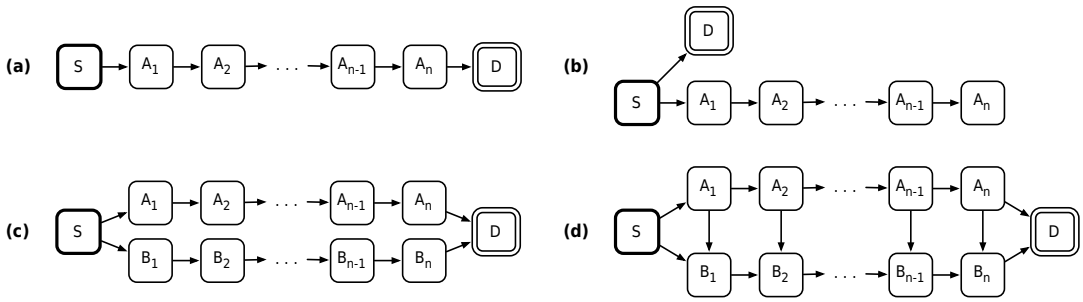

Fig. 5. Transformation graph shapes used for timing analysis

The results of this analysis are shown in Figure 6. Several important conclusions can be drawn from this data. In most cases, the number of LTS states and transitions that must be examined during the discovery algorithm is much greater than the number needed to represent the graph itself. This implies that with our more efficient subprocesses, FDR is not initially instantiating the entire structure of the graph; rather, the graph process is encoding a recipe for dynamically instantiating the graph as needed. This corresponds with our understanding of FDR's use of supercompilation to distinguish between low- and high-level operator trees: the exponential state is "hidden" by the high-level parallel compositions. We must still examine many of these exponential states during the refinement check, taking time, but it is not necessary to store them all in memory at once, saving space.

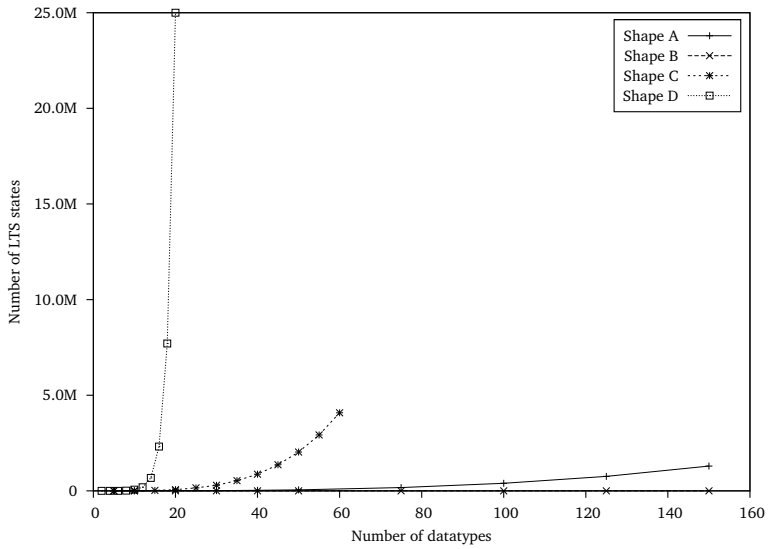

Fig. 6. Refinement running time for all shapes

Next, we can see that the execution time for the discovery algorithm is almost entirely dependent on the number of transformation paths that must be checked. This is most apparent in shape B, whose curve disappears into the X axis. Regardless of the number of datatypes in the shape B graph, there is a constant size transformation solution. Once the discovery algorithm finds this path, no more processing is required. In this case, the order of the operands in our stable failures refinement is beneficial, since FDR must *normalize* the left-hand side before performing the check. In this case, the left-hand side is $Want_F$ — whose LTS size depends only on the number of *desired* datatypes, and not on the size of the total transformation graph. For our earlier traces refinement, on the other hand, the left-hand side was *GraphOutputs*, whose size increases as new datatypes and transformations are added, even if they are not needed in the discovered solution. Thus, for the failures refinement, the normalization happens much faster, since it operates on a much smaller CSP process.

Figure 6 also shows the relationship between the complexity curves of shapes A, C, and D. Shape C seems to be a simple modification to the graph from shape A, only adding a single additional possible transformation path. However, since FDR is performing the equivalent of a breadth-first search, it will try to make progress down both paths simultaneously. Only after reaching the end of both intermediary sequences will FDR discover that only one was needed to reach the destination. Worse, it must consider every interleaving of the transformations in the two paths while advancing through the graph. Shape D exacerbates this problem by introducing crosslinking edges. Now, instead of having to consider all possible permutations of two transformation paths, FDR must consider the permutations of $n+2$ paths. The exponential growth is much more pronounced; whereas with shape A we were able to consider graphs with 150 datatypes in a reasonable amount of time, shape D quickly becomes intractable after only twenty datatypes.

Finally, it is important to point out we have not eliminated the exponential growth curve of the algorithm's running time; we have only made it less steep. This might seem to be a discouraging result at first, but it is in fact still useful in practice. As we will discuss in the next section, real-world transformation graphs tend not to contain a large number of datatypes and transformations, so any improvement in the efficiency of the discovery algorithm for smaller graphs will be helpful.

5 Interpreting the results

Having expressed the polyadic discovery problem as a CSP process, and analyzed the complexity space of this process, we can now interpret the measurements that we obtained. First, we examine the kinds of transformation graphs that were more efficient, identifying the features of those graphs that led to the efficiency gains, and showing why "real-life" transformation graphs will tend to have those features. Then, we show how this information can be used to construct an algorithmic solution.

5.1 Causes of the efficiency gains

According to our analysis, the space complexity for the discovery algorithm is fairly static, determined by the number of datatypes and transformations in the graph. This implies that reducing the number of datatypes in a graph can be an effective means of improving efficiency. In practice, this strategy should prove useful, since large transformation graphs tend to be easily separated into connected components. Intuitively, this is because the datatypes in the graph will tend to form "clumps", where a datatype can be transformed into anything in its clump, but not into anything outside of it. By treating these connected components as separate transformation graphs, we reduce the number of datatypes and the space required to represent the graph.

The time complexity, on the other hand, depends much more on the "shape" of the graph. As suspected, certain input graphs provide much more efficient executions of the discovery algorithm. The major determining factor is the number of possible transformation paths that must be checked. The time required by FDR grew dramatically as edges were added to the graph, especially when those edges added new transformation paths without making any new datatypes reachable. This yields a portion of the graph where several different possible sequences of transformations must be considered. Each of these sequences will eventually yield the same set of available datatypes, but will require different intermediary sets to get there.

In practice, transformation graphs will usually avoid this inefficiency, since the clumps of datatypes in a graph will not be highly interconnected. Indeed, the entire reason for using this graph-based approach is to limit the need to write direct transformations between datatypes. Instead, transformation graphs tend to follow an "intermediary format" pattern, as shown in Figure 7. In this pattern, one or more datatypes (the shaded types in the center of the graph) become de facto or official standards within different communities of users and developers. Individual application developers then write transformations between their datatypes (the unshaded types on the periphery of the graph) and one of these standards. These star-like graphs form trees, where there is exactly one path between any pair of nodes. While a real-world transformation graph is not likely to be a perfect tree (and might therefore allow multiple paths between a certain pair of datatypes), it can still provide full connectivity between all datatypes without providing an overabundance of transformation paths to check.

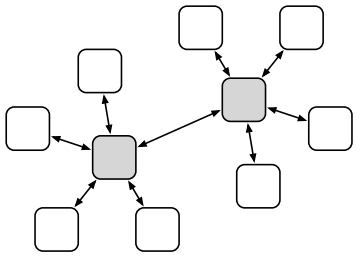

Fig. 7. Using intermediary datatypes to simplify a transformation graph

A similar factor affecting the algorithm's time complexity is whether the compound transformation that we are seeking actually exists. FDR is able to find a

correct transformation much faster than it is able to prove that no transformation exists. Intuitively, this makes sense; once FDR has found a solution, it does not need to consider any of the remaining possibilities and can stop processing. If there is no solution, FDR must check every possible transformation path to prove this. In practice, a program or user invokes the discovery algorithm because they know (or can reasonably assume) that the desired compound transformation exists. For real-world use cases, therefore, the time complexity will tend to be much more efficient than the worst case.

5.2 Developing an algorithm

With the insights gained by the CSP description of the problem and the efficiency analysis of using FDR to simulate a prototype implementation, we can now construct an algorithmic solution to the problem. In our initial formulation, our CSP processes kept track of which datatypes were available at any given time. We can do the same using a graph, where the nodes represent sets of datatypes. Each atomic transformation then yields several edges in the graph. For each node that contains all of a transformation's inputs, an edge is added from that node. The edge's destination is the union of the datatypes that were available previously (the source node) and the datatypes created by the transformation (the transformation's output set). This *set graph* representation is shown in Figure 8(a) for the example transformation graph from Figure 2.

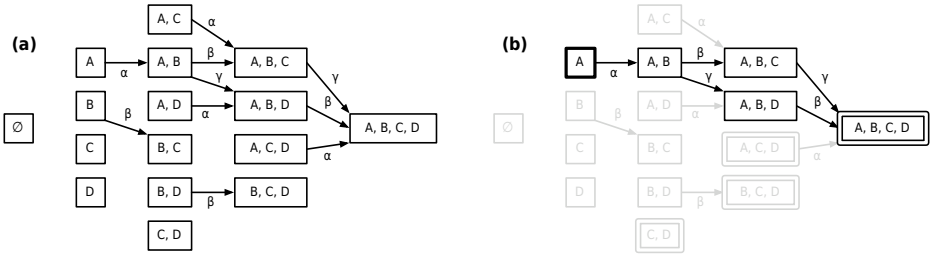

Fig. 8. A set-based graph representation

Using this model, compound transformations are once again represented by paths. Figure 8(b) shows the possible solutions that result if we are given an instance of datatype A and want to generate instances of datatypes C and D. There are two solutions, since β and γ can be executed in either order. Since solutions are represented by paths, we can use a shortest path algorithm to discover compound transformations.

However, we now have the same problem as with the initial CSP implementation: the space requirement for this representation is exponential in the number of datatypes. The next step in our analysis was to modify the CSP process to store a recipe for lazily deriving a transformation graph's LTS, rather than storing it in memory in its entirety.

This strategy of lazy evaluation can be easily added to the set-based graph algorithm, since a large fraction of nodes are not reachable from the $\{A\}$ source node. By only instantiating the nodes in the graph as they are encountered during the pathfinding algorithm, and by stopping the processing once a shortest path

has been discovered, we will only instantiate the subset of nodes that are actually reachable. Further, as we have shown, these reachable subsets will tend to be small for the transformation graphs that will appear more often in practice. Thus, while we cannot improve the problem's worst-case intractability, we have been able to empirically derive an algorithm that allows "real-world" transformations to be discovered efficiently and effectively.

6 Discussion

In this paper, we have described a transformation discovery problem that is provably intractable in the worst case. However, many problems are intractable in the worst case only because of pathological examples that do not arise in practice, and are more efficient in the "normal" case. We therefore formulated a declarative CSP description of the problem, and used FDR as a prototype implementation. This allowed us to identify classes of inputs for which solutions could be found more efficiently; using this information, we were then able to develop an algorithmic solution that is useful for real-world inputs.

One limitation of this technique is that it is highly dependent on our selection of inputs and on the tool that we use. We must choose an appropriate sampling of inputs if we want a true view of the problem's complexity space. More importantly, even if we choose an appropriate suite of test inputs, there is no guarantee that FDR will find all of the efficient solutions that are possible. When FDR finds a compound transformation inefficiently, for instance, this does not mean that this input graph has no efficient solution; instead, it might be that FDR's refinement checking strategies cannot reproduce the necessary optimizations. If we were to use a different modeling formalism and model checker, or even a different CSP refinement checker, we might get different results for our analysis. Because of this, we cannot establish a tight bound on the problem's complexity using this technique. However, we *can* establish an *upper* bound. Put another way, negative results are not indicative, in general. Positive results, on the other hand, represent real optimizations that can be exploited, though even these results might not be fully optimal.

Further work in this area can proceed along three lines of enquiry. First, if we want more confidence in our view of the problem's complexity space, we could create several prototypes, each using a different underlying declarative language, hoping that each efficient class of inputs would be found by at least one of them. SAT solvers, in particular, would be a good choice for an additional prototype; being the earliest and most visible *NP*-hard problem [7], Boolean satisfiability has inspired research into many sophisticated optimization techniques [15,26,9,11].

Second, there has been a lot of research into compression and optimization techniques for CSP processes. The supercompilation approach described in [14] is integral to the lazy evaluation strategy that we have already exploited. The hierarchical compression functions described in [24] seem promising, as well. It would be fruitful to see if any of these CSP compressions could be used to obtain further optimizations.

Finally, this technique could be similarly used for any algorithm or problem that

can expressed as a refinement of CSP processes — by finding the inputs that are solved more efficiently by FDR, and searching for common features of those inputs. This would then hopefully provide insights into how the algorithm could be made more efficient for those cases. One could verify this by applying this technique to several well-known *NP*-hard problems, seeing if it can reproduce existing results and lead to new insights.

Acknowledgments

Doug Creager's work is funded by the Software Engineering Programme of the Oxford University Computing Laboratory. The authors would like to thank Phil Armstrong for his advice on automating the FDR refinement checks in this paper; Jeremy Gibbons and Ed Smith for their suggestions on SAT solvers and other model-checking techniques; and our anonymous referees for providing valuable on the manuscript of this paper.

References

[1] Ausiello, G., A. D'Atri and D. Saccà, *Graph algorithms for functional dependency manipulation*, Journal of the ACM **30** (1983), pp. 752–766.

[2] Ausiello, G., G. F. Italiano and U. Nanni, *Optimal traversal of directed hypergraphs*, Technical Report TR-92-073, ICSI, Berkeley, CA (1992).

[3] Bellman, R., *On a routing problem*, Quarterly of Applied Mathematics **16** (1958), pp. 87–90.

[4] Berge, C., "Graphs and hypergraphs," North-Holland Mathematical Library **6**, Elsevier, Amsterdam, 1973.

[5] Berge, C., "Hypergraphs: Combinatorics of finite sets," North-Holland Mathematical Library **45**, Elsevier, Amsterdam, 1989.

[6] Breese, J. S., D. Heckerman and C. Kadie, *Empirical analysis of predictive algorithms for collaborative filtering*, Technical Report MSR-TR-98-12, Microsoft Research (1998).

[7] Cook, S. A., *The complexity of theorem-proving procedures*, in: *3rd ACM Symp. on the Theory of Computing* (1971), pp. 151–158.

[8] Creager, D. A. and A. C. Simpson, *A fully generic, graph-based approach to data transformation discovery*, in: *Graph Computation Models (GCM06)*, 2006.

[9] Davis, M., G. Logemann and D. Loveland, *A machine program for theorem-proving*, Communications of the ACM **5** (1962), pp. 394–397.

[10] Dijkstra, E. W., *A note on two problems in connexion with graphs*, Numerische Mathematik **1** (1959), pp. 269–271.

[11] Eén, N. and N. Sörensson, *An extensible SAT-solver*, in: *Theory and Applications of Satisfiability Testing*, LNCS **2919**, Springer-Verlag, Berlin, 2004 pp. 502–518.

[12] Esparza, J., *Decidability and complexity of Petri net problems — an introduction*, in: *Lectures on Petri Nets I: Basic Models*, LNCS 1491, Springer-Verlag, Berlin, 1998 pp. 374–428.

[13] Ford, L. R., Jr. and D. R. Fulkerson, "Flows in Networks," Princeton University Press, 1962.

[14] Goldsmith, M., *Operational semantics for fun and profit*, in: A. E. Abdallah, C. B. Jones and J. W. Sanders, editors, *Communicating Sequential Processes: The First 25 Years*, LNCS 3525 (2005), pp. 265–274.

[15] Gu, J., P. W. Purdom, J. Franco and B. W. Wah, "Algorithms for the satisfiability (SAT) problem: A survey," DIMACS Series in Discrete Mathematics and Theoretical Computer Science, American Mathematical Society, 1997.

[16] Hoare, C. A. R., "Communicating Sequential Processes," Prentice-Hall, 1985.

[17] Hunt, J. J., K.-P. Vo and W. F. Tichy, *Delta algorithms: an empirical analysis*, ACM Trans. on Software Engineering Methodologies **7** (1998), pp. 192–214.

[18] Italiano, G. F. and U. Nanni, *On-line maintenance of minimal directed hypergraphs*, in: *3rd Italian Conf. on Theoretical Computer Science* (1989), pp. 335–349.

[19] Jones, D. W., *An empirical comparison of priority-queue and event-set implementations*, Communications of the ACM **29** (1986), pp. 300–311.

[20] Petri, C. A., "Kommunikation mit Automaten," Ph.D. thesis, Institut für Instrumentelle Mathematik, Bonn (1962).

[21] Petri, C. A., *Fundamentals of a theory of asynchronous information flow*, in: *Int'l Fed. for Information Processing Congress (IFIP 62)*, 1963, pp. 386–390.

[22] Roscoe, A. W., *Model-checking CSP*, in: A. W. Roscoe, editor, *A classical mind: Essays in honour of C. A. R. Hoare*, Prentice-Hall, 1994 pp. 353–378.

[23] Roscoe, A. W., "The theory and practice of concurrency," Prentice-Hall, 1998.

[24] Roscoe, A. W., P. H. B. Gardiner, M. H. Goldsmith, J. R. Hulance, D. M. Jackson and J. B. Scattergood, *Hierarchical compression for model-checking CSP: How to check* 10^{20} *dining philosophers for deadlock*, in: *1st Int'l Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, LNCS 1019 (1995), pp. 133–152.

[25] Scattergood, J. B., "The semantics and implementation of Machine-Readable CSP," D.Phil. dissertation, Oxford University (1998).

[26] Zhang, L. and S. Malik, *The quest for efficient Boolean satisfiability solvers*, in: *14th Int'l Conference on Computer Aided Verification (CAV)*, LNCS **2404** (2002), pp. 641–653.