Universal Communication, Universal Graphs, and Graph Labeling

Nathaniel Harms
University of Waterloo, Canada
https://cs.uwaterloo.ca/~nharms
nharms@uwaterloo.ca

Abstract

We introduce a communication model called *universal SMP*, in which Alice and Bob receive a function f belonging to a family $\mathcal{F}$, and inputs x and y. Alice and Bob use shared randomness to send a message to a third party who cannot see f, x, y, or the shared randomness, and must decide $f(x, y)$. Our main application of universal SMP is to relate communication complexity to graph labeling, where the goal is to give a short label to each vertex in a graph, so that adjacency or other functions of two vertices x and y can be determined from the labels $\ell(x), \ell(y)$. We give a universal SMP protocol using $O(k^2)$ bits of communication for deciding whether two vertices have distance at most k in distributive lattices (generalizing the k-Hamming Distance problem in communication complexity), and explain how this implies a $O(k^2 \log n)$ labeling scheme for deciding $\mathsf{dist}(x, y) \le k$ on distributive lattices with size n; in contrast, we show that a universal SMP protocol for determining $\mathsf{dist}(x, y) \le 2$ in modular lattices (a superset of distributive lattices) has super-constant $\Omega(n^{1/4})$ communication cost. On the other hand, we demonstrate that many graph families known to have efficient adjacency labeling schemes, such as trees, low-arboricity graphs, and planar graphs, admit constant-cost communication protocols for adjacency. Trees also have an $O(k)$ protocol for deciding $\mathsf{dist}(x, y) \le k$ and planar graphs have an $O(1)$ protocol for $\mathsf{dist}(x, y) \le 2$, which implies a new $O(\log n)$ labeling scheme for the same problem on planar graphs.

2012 ACM Subject Classification Mathematics of computing → Probabilistic algorithms; Mathematics of computing → Graph coloring; Mathematics of computing → Trees; Theory of computation → Models of computation; Theory of computation → Communication complexity; Theory of computation → Computational geometry; Theory of computation → Generating random combinatorial structures

Keywords and phrases Universal graphs, graph labeling, distance labeling, planar graphs, lattices, hamming distance

Digital Object Identifier 10.4230/LIPIcs.ITCS.2020.33

Related Version https://arxiv.org/abs/1911.03757

Funding *Nathaniel Harms*: This research partially supported by the David R. Cheriton and GO-Bell Graduate Scholarships.

Acknowledgements Thanks to Eric Blais for comments on the structure of this paper; Amit Levi for helpful discussions and comments on the presentation; Anna Lubiw for an introduction to planar graphs and graph labeling; Corwin Sinnamon for comments on distributive lattices; and Sajin Sasy for observing the possible applications to privacy.

1 Introduction

In the simultaneous message passing (SMP) model of communication, introduced by Yao [34], Alice and Bob separately receive inputs x and y to a function f. They send messages $a(x), b(y)$ to a third party, called the referee, who knows f and must output $f(x, y)$ (with high probability) using the messages $a(x), b(y)$. But what if the referee *doesn't* know f? Can they still compute $f(x, y)$? Yes: Alice can include in her message a description of f, and then the referee knows it; however, if f is restricted, they can sometimes do much better. Here is a simple example: the players receive vertices $x, y \in \{1, \ldots, n\}$ in a graph G of maximum degree 2, and want to decide if (x, y) is an edge in G. Sharing a source of randomness, Alice and Bob randomly label each vertex of G with a number up to 200; Alice sends the label of both neighbors of x and Bob sends the label of y. The referee says *yes* if one of Alice's labels matches the label of y, *no* otherwise. They will be correct with probability at least 99/100, and the referee never needs to learn G. This is also an example where the referee can decide many problems using only one strategy. In this work we will see that more interesting families of graphs, such as trees, planar graphs, and distributive lattices, also exhibit these phenomena, even when we wish to compute *distances* instead of just adjacency.

To study this, we introduce the *universal SMP* model, which operates as follows. Fix some family $\mathcal{F}$ of functions. Alice and Bob receive a function $f \in \mathcal{F}$ and inputs x, y, and they use shared randomness to each send one message to the referee. The referee knows the family $\mathcal{F}$ and the size of the inputs, but doesn't know f, x, y or the shared randomness, and must compute $f(x, y)$ with high probability. By choosing the family $\mathcal{F}$ to be the singleton family, one sees that this model includes standard SMP. As in the earlier example, we will be studying communication problems on graphs, but this is not a significant restriction: every Boolean-valued communication problem f is equivalent to determining adjacency in some graph (use f as the adjacency matrix), so we will treat $\mathcal{F}$ as a family of graphs.

A surprising but intuitive application of universal SMP is that it connects two apparently disjoint areas of study: communication complexity and graph labeling. For a graph family $\mathcal{F}$, the graph labeling problem (introduced by Kannan, Naor, and Rudich [23]) asks how to assign the shortest possible labels $\ell(v)$ to each vertex v of a graph $G \in \mathcal{F}$, so that the adjacency (or some other function [29]) of vertices x, y can be computed from $\ell(x), \ell(y)$ by a decoder that knows $\mathcal{F}$. We observe the following principle (Theorem 1.1):

If there is a (randomized) universal SMP protocol for the graph family $\mathcal{F}$ with communication cost c, then there is a labeling scheme for graphs $G \in \mathcal{F}$ with labels of size $O(c \log n)$, where n is the number of vertices.

Common variants of graph labeling are *distance labeling* [15], where the goal is to compute $\mathsf{dist}(x, y)$ from the labels, and *small-distance* labeling, where the goal is to compute $\mathsf{dist}(x, y)$ if it is at most k and output "$> k$" otherwise [24, 2]. This is similar to the well-studied k-Hamming Distance problem in communication complexity, where the players must decide if their vertices x, y have distance at most k in the Boolean hypercube graph. A natural generalization of the Boolean hypercube is the family of distributive lattices (which also include, for example, the hypergrids). We demonstrate that techniques from communication complexity can be used to obtain new graph labelings, by adapting the k-Hamming Distance protocol of Huang et al. [21] to the universal SMP model, achieving an $O(k^2)$ protocol for computing $\mathsf{dist}(x, y) \leq k$ and the corresponding k-distance labeling scheme with label size $O(k^2 \log n)$. It is interesting to note that, in contrast to the standard application of communication complexity as a method for obtaining lower bounds, we are using it to obtain upper bounds.

Generalizing in another direction, we ask: for which graphs other than the Boolean hypercube can we obtain efficient communication protocols for k-distance? For constant k, k-Hamming Distance can be computed with communication cost $O(1)$; which other graphs admit a constant-cost protocol? To approach this question, we observe that many (but not all) graph families known to have efficient $O(\log n)$ adjacency labeling schemes also admit an $O(1)$ universal SMP protocol for adjacency. Commonly studied families in the adjacency and distance labeling literature are trees [23, 24, 2, 5, 3] and planar graphs [23, 15, 14, 16, 6]. We study the k-distance problem on these families and find that trees admit an $O(k)$ protocol, while planar graphs admit an $O(1)$ protocol for 2-distance; this implies a new labeling scheme for planar graphs.

Further motivation for the universal SMP model comes from *universal graphs*. Introduced by Rado [30], an induced-universal graph U for a set $\mathcal{F}$ is one that contains each $G \in \mathcal{F}$ as an induced subgraph. An efficient adjacency labeling scheme for a set $\mathcal{F}$ implies a small induced-universal graph for that set [23]. Deterministic universal SMP protocols are equivalent to universal graphs (Theorem 1.7), and we introduce *probabilistic universal graphs* as the analogous objects for randomized univeral SMP protocols. We think probabilistic universal graphs are worthy of study alongside universal graphs, especially since many non-trivial families admit one of *constant-size*.

The universal SMP model is also related to a recent line of work studying communication between parties with imperfect knowledge of each other's "context". The most relevant incarnation of this idea is the recent work [18, 17], who study the 2-way communication model where Alice and Bob receive functions f and g respectively, with inputs x and y, and must compute $f(x, y)$ under the guarantee that f and g are close in some metric. In other words, one party does not have full knowledge of the function to be computed. The universal SMP model provides a framework for studying a similar problem in the SMP setting, where the players know the function but the referee does not; the similarity is especially clear when we define the family $\mathcal{F}$ to be all graphs of distance δ to a reference graph G in some metric (we discuss this situation in more detail at the end of the paper). This could model, for example, a situation where the clients of a service operate in a shared environment but the server does not; or, a situation in which the clients want to keep their shared environment secret from the server, and their inputs secret from each other. This suggests a possible application to privacy and security. A relevant example is private proximity testing (e.g. [27]), where two clients should be notified by the server when they are at distance at most k from each other, without revealing to each other or the server their exact locations.

The Discussion at the end of the paper highlights some interesting questions and open problems related to universal SMP.

1.1 Results

A universal SMP protocol *decides k-distance* for a family $\mathcal{F}$ if for all graphs $G \in \mathcal{F}$ and vertices x, y, the protocol will correctly decide if $\mathsf{dist}(x, y) \leq k$, with high probability. A labeling scheme decides k-distance if $\mathsf{dist}(x, y) \leq k$ can be decided from the labels of x, y. Below, the variable n always refers to the number of vertices in the input graph.

Implicit graph representations. The main principle connecting communication and graph labeling is:

▶ **Theorem 1.1.** *Any graph family $\mathcal{F}$ with universal SMP cost m has an adjacency labeling scheme with labels of size $O(m \log n)$. In particular, if the universal SMP cost for $\mathcal{F}$ is $O(1)$ then $\mathcal{F}$ has an $O(\log n)$ adjacency labeling scheme.*

Adjacency labeling schemes of size $O(\log n)$ are of special interest because $\log n$ is the minimum number of bits required to label each vertex uniquely, and they correspond to *implicit graph representations*, as defined by Kannan, Naor, and Rudich [23] (we omit their requirement that the encoding and decoding be computable in polynomial-time). Section 2.3 elaborates further. To obtain implicit representations, we can relax our requirements:

▶ **Corollary 1.2.** *For any constant c, any graph family $\mathcal{F}$ where each $G \in \mathcal{F}$ has a public-coin 2-way communication protocol computing adjacency with cost c has an implicit representation.*

Distributive & Modular Lattices. Distributive and modular lattices are generalizations of the Boolean hypercube and hypergrids (see Section 3 for definitions). We define a *weakly-universal* SMP protocol as one where the referee shares the randomness of Alice and Bob. For distributive lattices we get the following:

▶ **Theorem 1.3.** *The k-distance problem on the family of distributive lattices has: a weakly-universal SMP protocol with cost $O(k \log k)$; a universal SMP protocol with cost $O(k^2)$; and a size $O(k^2 \log n)$ labeling scheme.*

Modular lattices are a superset of distributive lattices, but they do not admit k-distance protocols with a cost independent of n; we show that any universal SMP protocol (and any labeling scheme) deciding 2-distance must have cost $\Omega(n^{1/4})$ (Theorem 3.14). To our knowledge, there are no known labeling schemes for distributive or modular lattices. Our adjacency labeling scheme (i.e. for $k = 1$) requires $O(n \log n)$ space to store the whole lattice; this can be compared to Munro and Sinnamon [26], who present a data structures of size $O(n \log n)$ for distributive lattices that supports *meet* and *join* operations (and therefore distance queries, due to our Lemma 3.5). However, these are not labelings, so the result is not directly comparable.

Planar graphs and other efficiently-labelable families. When they introduced graph labeling, Kannan, Naor, and Rudich [23] studied trees, low-arboricity graphs (whose edges can be partitioned into a small number of trees), and planar graphs, and interval graphs (whose vertices are intervals in $\mathbb{R}$, with an edge if the intervals intersect), among others. These families have $O(\log n)$ adjacency labeling schemes. Trees, low-arboricity graphs, and planar graphs have constant-cost universal SMP protocols for adjacency. Trees admit an efficient k-distance protocol:

▶ **Theorem 1.4.** *The family of trees has a universal SMP protocol deciding k-distance with cost $O(k)$ and a $O(k \log n)$ labeling scheme deciding k-distance.*

Planar graphs admit an efficient 2-distance protocol, which implies a new 2-distance labeling scheme:

▶ **Theorem 1.5.** *The 2-distance problem on the family of planar graphs has a universal SMP protocol with cost $O(1)$ and a labeling scheme of size $O(\log n)$.*

On the other hand, a universal SMP protocol deciding 2-distance on the family of graphs with arboricity 2 has cost at least $\Omega(\sqrt{n})$ (Proposition 4.4), and a universal SMP protocol deciding adjacency in interval graphs has cost $\Theta(\log n)$ (Proposition 4.5).

Gavoille et al. [15] showed that trees have an $O(\log^2 n)$ labeling allowing $\mathsf{dist}(x, y)$ to be computed exactly from labels of x, y, and gave a matching lower bound; Kaplan and Milo [24] and Alstrup *et al* [2] studied k-distance for trees, with the latter achieveing a $\log n + O(k^2(\log \log n + \log k))$ labeling scheme. For planar graphs, [15] gives a lower bound of $\Omega(n^{1/3})$ for computing distances exactly, and an upper bound of $O(\sqrt{n} \log n)$, which was later improved to $O(\sqrt{n})$ in [16].

Communication Complexity. Our lower bounds are achieved by reduction from the family of all graphs, which has complexity $\Theta(n)$, in contrast to the upper bound of $\lceil \log n \rceil$ for the standard SMP cost of computing adjacency in any graph (since Alice and Bob can send $\lceil \log n \rceil$ bits to identify their vertices).

▶ **Theorem 1.6.** *For the family $\mathcal{G}$ of all graphs, the universal SMP cost of computing adjacency in $\mathcal{G}$ is $\Theta(n)$.*

The basic relationships between universal SMP, standard SMP, and universal graphs are as follows. Below, we use $D^{\|}(\textsc{Adj}(G))$ and $R^{\|}(\textsc{Adj}(G))$ for the deterministic and randomized (standard) SMP cost of computing adjacency on G, and $D^{\mathsf{univ}}(\mathcal{F}), R^{\mathsf{univ}}(\mathcal{F})$ for the deterministic and randomized universal SMP cost for computing adjacency in the family $\mathcal{F}$. We use the term "$\sqsubset$-universal graph" as opposed to "induced-universal" to denote a slightly different object that allows non-injective embeddings (see Section 2 for definitions).

▶ **Theorem 1.7.** *For a set $\mathcal{F}$, the following relationships hold. Let U range over the set of all $\sqsubset$-universal graphs:*

$$\max_{G \in \mathcal{F}} D^{\|}(\textsc{Adj}(G)) \le D^{\mathsf{univ}}(\mathcal{F}_i) = \min_U D^{\|}(\textsc{Adj}(U)) = \min_U \lceil \log |U| \rceil \,,$$

with equality on the left iff $\exists H \in \mathcal{F}$ such that $\forall G \in \mathcal{F}$, G can be embedded *in H. For $\widetilde{U}$ ranging over the set of all* probabilistic universal graphs*:*

$$\max_{G \in \mathcal{F}} R^{\|}(\textsc{Adj}(G)) \le R^{\mathsf{univ}}(\mathcal{F}) \le \min_{\widetilde{U}} D^{\|}(\textsc{Adj}(\widetilde{U})) \le O\left(R^{\mathsf{univ}}(\mathcal{F})\right) \,.$$

Randomized and deterministic universal SMP satisfy

$$\Omega\left(\frac{D^{\mathsf{univ}}(\mathcal{F})}{\log n}\right) \le R^{\mathsf{univ}}(\mathcal{F}) \le D^{\mathsf{univ}}(\mathcal{F}) \,.$$

The above results on graph labeling are proved through the relationship between randomized and deterministic universal SMP. We obtain this relationship by adapting Newman's Theorem [28], a standard derandomization result in communication complexity. Finally, we note the interesting fact that universal SMP characterizes the gap between standard SMP models where the referee does or does not share the randomness with Alice and Bob:

▶ **Proposition 1.8** (Informal). *Let $\mathcal{F}$ be a family of graphs and let Π be a weakly-universal SMP protocol for $\mathcal{F}$, which defines a distribution over the referee's decision functions F, which we interpret as the adjacency matrices of graphs. Let $\mathcal{U}_\Pi$ be the family on which this distribution is supported. Then, taking the minimum over all such protocols Π,*

$$R^{\mathsf{univ}}_{\epsilon}(\mathcal{F}) = \min_{\Pi} D^{\mathsf{univ}}(\mathcal{U}_\Pi) \,.$$

1.2 Other Related Work

Graph labeling. Randomized labeling schemes for trees have been studied by Fraigniaud and Korman [12], who give a randomized adjacency labeling scheme of $O(1)$ bits per label that has one-sided error (i.e. it can erroneously report that x, y are adjacent when they are not), and they show that achieving one-sided error in the opposite direction requires a randomized labeling with $\Omega(\log n)$ bits. They also give randomized schemes for determining if x is an ancestor of y, but they do not address distance problems. Spinrad's book [33] has a chapter on implicit graphs and Alstrup et al. [6] for a recent survey on adjacency labeling schemes and induced-universal graphs. We know of no labeling schemes for lattices, but Fraigniaud and Korman [13] recently studied adjacency labeling schemes for posets of low "tree-dimension".

Distance-preserving labeling studies an opposite problem to k-distance labeling, where distances must be accurately reported when they are *above* some threshold D. Recent work includes Alstrup et al. [4].

To our knowledge, k-distance or even 2-distance has not been studied for planar graphs, but there are many results on other types of planar graph labelings with restrictions at distance 2. An example is the *frequency assignment problem* or *$L(p,q)$-labeling* problem, which asks how to construct a labeling ℓ assigning integers $[k]$ to vertices of a planar graph so that $\mathsf{dist}(x,y) \le 1 \implies |\ell(x) - \ell(y)| \ge p$ and $\mathsf{dist}(x,y) \le 2 \implies |\ell(x) - \ell(y)| \ge q$, with various optimization goals. See [7] for a survey.

Uncertain communication. There are several works studying communication problems where the parties do not agree on the function to be computed, starting with Goldreich, Juba, and Sudan [19] who studied communication where parties have different "goals". Canonne et al. [8] study communication in the shared randomness setting where the randomness is shared imperfectly. Haramarty and Sudan [20] study compression (á la Shannon) in situations where the parties do not agree on a common distribution. As mentioned earlier, Ghazi et al. [17] and Ghazi and Sudan [18] study 2-way communication where the parties do not agree on the function to be computed.

1.3 Notation

$[k]$ means $\{1, \dots, k\}$. The letter n always denotes the number of vertices in a graph. We use the notation $\mathbb{1}[E] = 1$ iff the statement E holds, and $\mathbb{1}[E] = 0$ otherwise. For a graph G, $V(G)$ is the set of vertices and $E(G)$ is the set of edges. For vertices x, y, we write $G(x,y) = \mathbb{1}[x, y \text{ are adjacent in } G]$ for the entry in the adjacency matrix of G. For an undirected, unweighted graph G and vertices u, v, $\mathsf{dist}(u,v)$ is the length of the shortest path from u to v.

For any graph G and integer k, we denote by G^k the *k-closure* of G, where two vertices u, v are adjacent iff $\mathsf{dist}(u,v) \le k$ in G; it is convenient to require that each vertex is adjacent to itself in G^k. For a set of graphs $\mathcal{F}$, $\mathcal{F}^k = \{G^k : G \in \mathcal{F}\}$.

$D^{\parallel}(f)$ is the deterministic SMP cost of the function f and $R^{\parallel}(f)$ is the randomized SMP cost of the function f, in the model where Alice and Bob share randomness but the deterministic referee does not.

2 Universal Communication and Universal Graphs

In this paper we focus on deciding adjacency. Every Boolean communication problem $f : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ on finite domains $\mathcal{X}, \mathcal{Y}$ is equivalent to the adjacency problem on the graph G with vertex set $\mathcal{X} \cup \mathcal{Y}$ and $G(u,v) = f(u,v)$. We may either allow self-loops in G if $\mathcal{X} = \mathcal{Y}$ or take G to be bipartite. We will generally permit graphs to have self-loops.

▶ **Definition 2.1.** *A family of graphs $\mathcal{F} = (\mathcal{F}_i)$ is a sequence of sets $\mathcal{F}_i$ indexed by integers i, along with a strictly increasing size function $n(i)$, so that $\mathcal{F}_i$ is a set of graphs with vertex set $[n(i)]$. If $\mathcal{F}_i$ has size $n(i) = i$ then we write $\mathcal{F}_n$.*

▶ **Definition 2.2** (Universal SMP and Variations). *Let $\mathcal{F}$ be a family of graphs with size function n and let Φ be an operation taking size $n(i)$ graphs to size $n(i)$ graphs. Let $c : \mathbb{N} \to \mathbb{N}$ and let $\epsilon > 0$ be a constant. An ϵ-error, cost c sequence of* universal SMP *communication protocols for $\mathcal{F}$ is as follows. For any $i \in \mathbb{N}$, a protocol Π_i for $\mathcal{F}_i$ is a triple (a_i, b_i, F_i) where:*

- *Alice and Bob receive $(G, x), (G, y)$ respectively, where $G \in \mathcal{F}_i$ and $x, y \in V(G) = [n(i)]$;*
- *Alice and Bob share a random string r and compute messages $a_i(r, G, x), b_i(r, G, y) \in \{0,1\}^{c(i)}$, respectively;*
- *For each i, the (deterministic) referee has a function $F_i : \{0,1\}^{c(i)} \times \{0,1\}^{c(i)} \to \{0,1\}$, called the* decision function. *$F_i(a_i(r, G, x), b_i(r, G, y))$ must satisfy:*
  1. *If x, y are adjacent in $\Phi(G)$ then $\mathbb{P}_r[F_i(a_i(r, G, x), b_i(r, G, y)) = 1] > 1 - \epsilon$; and*
  2. *If x, y are not adjacent in $\Phi(G)$ then $\mathbb{P}_r[F_i(a_i(r, G, x), b_i(r, G, y))] < \epsilon$.*

A universal SMP protocol is symmetric *when the functions a_i, b_i computed by Alice and Bob are identical and the function F_i satisfies $F_i(a, b) = F_i(b, a)$ for all messages $a, b \in \{0,1\}^c$. We write $R^{\mathsf{univ}}_\epsilon(\Phi(\mathcal{F}))$ for the communication complexity in the universal SMP model of computing adjacency in graphs $\Phi(\mathcal{F}) = \{\Phi(G) : G \in \mathcal{F}\}$, where ϵ is the allowed probability of error. We write $R^{\mathsf{univ}}(\Phi(\mathcal{F}))$ for $R^{\mathsf{univ}}_{1/3}(\Phi(\mathcal{F}))$. If no operation Φ is specified, it is assumed to be the identity.*

It is also convenient to define a weakly-universal SMP *protocol as a universal SMP protocol where the referee can see the shared randomness, so the choice function is of the form $F_i(r, a(r, G, x), b(r, G, y))$ for random seed r, graph $G \in \mathcal{F}$, and $x, y \in V(G)$. We denote the ϵ-error complexity in this model with $R^{\mathsf{weak}}_\epsilon(\Phi(\mathcal{F}))$.*

Finally, we write $D^{\mathsf{univ}}(\Phi(\mathcal{F}))$ for the deterministic *universal SMP complexity.*

▶ Remark 2.3. We include the operator Φ in the definition to emphasize that the players are given the original graph G, not the graph $\Phi(G)$; for example, the players are not given G^k (from which it may be difficult to compute G), but are instead given G.

2.1 Deterministic Universal Communication and Universal Graphs

We will show that a deterministic universal SMP protocol is equivalent to an *embedding* into a $\sqsubset$-universal graph, which we we define using the following notion of embedding (following the terminology of Rado [30]):

▶ **Definition 2.4.** *For graphs G, H, a mapping $\phi : V(G) \to V(H)$ is an* embedding *iff $\forall u, v \in V(G)$, $G(u, v) = H(\phi(u), \phi(v))$. If such a mapping exists we write $G \sqsubset H$.*

For a set of graphs $\mathcal{F}_i$, a graph U is $\sqsubset$-universal *if $\forall G \in \mathcal{F}_i, G \sqsubset U$; i.e. $\forall G \in \mathcal{F}_i$ there exists an embedding $\phi_G : V(G) \to V(U)$. For a family of graphs $\mathcal{F} = (\mathcal{F}_i)$, a sequence $U = (U_i)$ is a* $\sqsubset$-universal graph sequence *if for each i, U_i is $\sqsubset$-universal for $\mathcal{F}_i$.*

Define an equivalence relation on $V(G)$ by $u \equiv v$ iff $\forall w \in V(G), G(u, w) = G(v, w)$, i.e. u, v have identical rows in the adjacency matrix. For a graph G, define the $\equiv$-reduction $G^{\equiv}$ as a graph on the equivalence classes $\mathcal{C}$ of $V(G)$ with $U, W \in \mathcal{C}$ adjacent iff $\exists u \in U, w \in W$ such that u, w are adjacent.

An embedding is not the same as a homomorphism since we must map non-edges to non-edges, and $G \sqsubset H$ is not the same as G being an induced subgraph of H since the mapping is not necessarily injective. Therefore a universal graph by our definition is not the same as an induced-universal graph, where G must exist as an induced subgraph. We could for example map the path $a — b — c \mapsto a' — b' — a'$. This difference between definitions is captured by the $\equiv$ relation between vertices. It is necessary to allow self-loops, otherwise the $\sqsubset$ relation is not transitive. The important properties of $\sqsubset, \equiv$, and $\equiv$-reductions are stated in the next proposition; the proofs are routine and for completeness are included in the appendix. The relation $\simeq$ is the isomorphism relation on graphs.

▶ **Proposition 2.5.** *The following properties are satisfied by the $\sqsubset$ relation, the $\equiv$ relation, and $\equiv$-reductions:*

1. $\sqsubset$ *is transitive.*
2. *For any graph G and $u, v \in V(G)$, $u \equiv v$ iff there exists H and an embedding $\phi : G \to H$ such that $\phi(u) = \phi(v)$.*
3. *For any graph $G, (G^\equiv)^\equiv \simeq G^\equiv$.*
4. *For any graph $G, G \sqsubset G^\equiv$ and $G^\equiv \sqsubset G$.*
5. *For any graphs G, H, $G \sqsubset H$ iff $G^\equiv \sqsubset H^\equiv$.*
6. *For any graphs G, H, $G^\equiv \sqsubset H^\equiv$ iff $G^\equiv$ is an induced subgraph of $H^\equiv$.*

These properties allows us to prove relationships between the standard SMP model, deterministic universal SMP, and $\sqsubset$-universal graphs. First we show that deterministic universal SMP protocols can always be made symmetric[1].

▶ **Proposition 2.6.** *If Π is a deterministic universal SMP protocol for the set $\mathcal{F}$, then there exists a deterministic universal SMP protocol Π' that is symmetric and has the same cost as Π.*

Proof. Let $G \in \mathcal{F}$ and let $a, b : V(G) \to \{0,1\}^m$ be the encoding functions for G and F the decision function for graphs of size $|G|$. The restriction of b to the domain $V(G^\equiv) \to \{0,1\}^m$ is injective so it has an inverse $b^{-1} : \text{image}(b) \to V(G^\equiv)$ that satisfies $b^{-1}b(x) \equiv x$; the same holds for a, a^{-1}. Define the encoding function $b' : V(G) \to \{0,1\}^m$ as $b' = ab^{-1}b$ and define the decision function $F'(p, q) = F(p, ba^{-1}(q))$. Then for any $x, y \in V(G), F'(a(x), b'(y)) = F(a(x), ba^{-1}ab^{-1}b(y)) = F(a(x), b(y)) = G(x, y)$ so this is a valid protocol. Since $\text{image}(b') \subseteq \text{image}(a)$ we can write $b'(x) = aa^{-1}b'(x) = aa^{-1}ab^{-1}b(x) = a(x)$ for every x so $b' = a$, thus $F'(a(x), a(y)) = G(x, y) = G(y, x) = F'(a(y), a(x))$ so the protocol is symmetric. ◀

The standard deterministic SMP complexity measure can be expressed in terms of $\equiv$-reductions:

▶ **Proposition 2.7.** *For all graphs G, $D^{\parallel}(\text{ADJ}(G)) = \lceil \log |G^\equiv| \rceil$.*

Proof. It is well-known that for any function $f : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$, $D^{\parallel}(f) = \lceil \log \min(r, c) \rceil$ where r is the number of distinct columns in the communication matrix of f, and c is the number of distinct rows [34]. The communication matrix of the function $\text{ADJ}(G)$ is the adjacency matrix of G, which is symmetric, and two rows (or columns) indexed by u, v are distinct iff $u \not\equiv v$; so the number of distinct rows is the size of $G^\equiv$. ◀

The analogous fact for universal SMP is that the deterministic universal SMP cost is determined by the size of the smallest universal graph.

▶ **Proposition 2.8.** *For any graph family $\mathcal{F} = (\mathcal{F}_i)$,*

$$D^{\mathsf{univ}}(\mathcal{F}_i) = \min_U \{ \lceil \log |U^\equiv| \rceil : \forall G \in \mathcal{F}_i, G \sqsubset U^\equiv \}.$$

Proof. Let U be any graph such that $G \sqsubset U^\equiv$ for all $G \in \mathcal{F}_i$ and for each $G \in \mathcal{F}_i$ let g be the embedding $G \to U^\equiv$. Consider the protocol where on inputs $(G, x), (G, y)$, Alice and Bob send $g(x), g(y)$ using $\lceil \log |U^\equiv| \rceil$ bits and the referee outputs $U^\equiv(g(x), g(y))$. This is correct by definition so $D^{\mathsf{univ}}(\mathcal{F}_i) \le \lceil \log |U^\equiv| \rceil$.

[1] Note that this does not imply that every deterministic SMP protocol is symmetric, since in this paper we are only concerned with adjacency on an undirected graph, for which the communication matrix is symmetric. This proposition shows that for symmetric communication matrices, the deterministic SMP protocol is symmetric.

Now suppose there is a protocol Π for $\mathcal{F}_i$ with cost c and decision function F_i, and let $G \in \mathcal{F}_i$. By Proposition 2.6 we may assume that on inputs $(G, x), (G, y)$ Alice and Bob share the encoding function $g : V(G) \to \{0,1\}^c$. Let U be the graph with vertices $\{0,1\}^c$ and $U(u, v) = F(u, v)$. Then $U(g(x), g(y)) = F(g(x), g(y)) = G(x, y)$ so $G \sqsubset U \sqsubset U^{\equiv}$ (by transitivity). Now $|U^{\equiv}| \leq 2^c$ so $c \geq \log |U^{\equiv}|$. ◀

It is easy to see that $D^{\|}$ can be used as a lower bound on D^{univ} but such lower bounds are tight only when the family $\mathcal{F}$ is essentially a "trivial" family of equivalent graphs.

▶ **Lemma 2.9.** *For any family $\mathcal{F} = (\mathcal{F}_i)$, let $U = (U_i)$ be the smallest $\sqsubset$-universal graph sequence for $\mathcal{F}$. Then*

$$\max_{G \in \mathcal{F}_i} D^{\|}(\textsc{Adj}(G)) \leq D^{\mathsf{univ}}(\mathcal{F}_i) = D^{\|}(\textsc{Adj}(U_i)),$$

with equality holding on the left iff $\exists H \in \mathcal{F}_i$ such that $\forall G \in \mathcal{F}_i, G^{\equiv} \sqsubset H^{\equiv}$.

Proof. The equality on the right holds by the two prior propositions. The lower bound follows from the fact that any protocol Π_i for $\mathcal{F}_i$ in the universal model can be used as a protocol in the SMP model. Now we must show the equality condition. Let $U \in \mathcal{F}_i$ be a graph maximizing $|U^{\equiv}|$ over all graphs in $\mathcal{F}_i$, and suppose $D^{\mathsf{univ}}(\mathcal{F}_i) = \max_{G \in \mathcal{F}_i} D^{\|}(\textsc{Adj}(G)) = \max_{G \in \mathcal{F}_i} \lceil \log |G^{\equiv}| \rceil = \lceil \log |U^{\equiv}| \rceil$, so $\lceil \log |U^{\equiv}| \rceil = \min\{\lceil \log |H^{\equiv}| \rceil : \forall G \in \mathcal{F}_i, G \sqsubset H^{\equiv}\}$. Then there exists H such that $U^{\equiv} \sqsubset H^{\equiv}$ and $|U^{\equiv}| = |H^{\equiv}|$. Since $U^{\equiv}$ is an induced subgraph of $H^{\equiv}$ and $|U^{\equiv}| = |H^{\equiv}|$ we must have $U^{\equiv} \simeq H^{\equiv}$ so $\forall G \in \mathcal{F}_i, G^{\equiv} \sqsubset U^{\equiv}$. ◀

2.2 Randomized Universal Communication

Just as deterministic universal communication is equivalent to embedding a family into a universal graph, we will define probabilistic universal graphs and show that they are tightly related to universal communication with shared randomness.

▶ **Definition 2.10.** *For graphs G, H, a random mapping $\phi : V(G) \to V(H)$ (i.e. a distribution over such mappings) is an ϵ-*error embedding *iff $\forall u, v \in V(G)$,*

$$\mathbb{P}_{\phi}\left[G(u, v) = H(\phi(u), \phi(v))\right] > 1 - \epsilon .$$

*We will write $G \sqsubset_\epsilon H$ if there exists an ϵ-error embedding $G \to H$. A graph U is ϵ-*error universal *for a set of graphs S if $\forall G \in S, G \sqsubset_\epsilon U$. $U = (U_i)$ is an ϵ-error universal graph sequence for the family $\mathcal{F} = (\mathcal{F}_i)$ if for each i, U_i is ϵ-error universal for $\mathcal{F}_i$.*

In the randomized setting we obtain equivalence (up to a constant factor) between universal SMP protocols and probabilistic universal graphs.

▶ **Lemma 2.11.** *For any graph family $\mathcal{F} = (\mathcal{F}_i)$ and any $\epsilon > 0$, if there exists a ϵ-error universal SMP protocols for $\mathcal{F}$ with cost $c(i)$, then there exists a 2ϵ-error symmetric universal SMP protocols for $\mathcal{F}$ with cost at most $2c(i)$.*

Proof. On input $G \in \mathcal{F}_i, x, y \in V(G)$, and random string r, Alice and Bob send the concatentations $g_r(x) := a_i(r, G, x)b_i(r, G, x)$ and $g_r(y) := a_i(r, G, y)b_i(r, G, y)$. Then the referee computes

$$F'_i(g_r(x), g_r(y)) = \max\left\{F_i(a_i(r, G, x), b_i(r, G, y)), F_i(a_i(r, G, y), b_i(r, G, x))\right\} .$$

It is clear that F_i' is symmetric. If x, y are adjacent then

$$\mathop{\mathbb{P}}_r[F_i'(g_r(x), g_r(y)) = 0] \le \mathop{\mathbb{P}}_r[F_i(a_i(r,G,x), b_i(r,G,y)) = 0] < \epsilon\,,$$

and if x, y are not adjacent then, by the union bound,

$$\begin{aligned}&\mathop{\mathbb{P}}_r[F_i'(g_r(x), g_r(y)) = 1] \\ &\quad \le \mathop{\mathbb{P}}_r[F_i(a_i(r,G,x), b_i(r,G,y)) = 1] + \mathop{\mathbb{P}}_r[F_i(a_i(r,G,y), b_i(r,G,x)) = 1] < 2\epsilon\,.\end{aligned}$$ ◀

Applying this symmetrization, we get a relationship between universal SMP protocols and probabilistic universal graphs.

▶ **Lemma 2.12.** *Let $\mathcal{F} = (\mathcal{F}_i)$ be a graph family and $\epsilon > 0$. Then*

1. *There is an ϵ-error universal graph sequence of size at most $2^{2R^{\mathsf{univ}}_{\epsilon/2}(\mathcal{F})}$; and*
2. *If there is an ϵ-error universal graph sequence of size $c(i)$ then $R^{\mathsf{univ}}_{\epsilon}(\mathcal{F}) \le \lceil \log c \rceil$.*

Proof. If Π_i is an ϵ-error symmetric universal protocol for $\mathcal{F}_i$ then there exists a function F_i such that for every $G \in \mathcal{F}_i$ there is a random g such that $\mathop{\mathbb{P}}_g[F_i(g(x), g(y)) \ne G(x,y)] < \epsilon$. Using F_i as an adjacency matrix, we get a graph U_i of size at most 2^c, where c is the cost of Π_i, such that for all $G \in \mathcal{F}_i, G \sqsubset_\epsilon U_i$. Then $U = (U_i)$ is an ϵ-error probabilistic universal graph sequence. By Lemma 2.11 we obtain an ϵ-error symmetric protocol with cost $2R^{\mathsf{univ}}_{\epsilon/2}(\mathcal{F})$, so we have proved the first conclusion. The second conclusion follows by definition. ◀

The basic relationships to standard SMP models follow essentially by definition and from the above lemma.

▶ **Lemma 2.13.** *Let $\mathcal{F}$ be any graph family and let $\epsilon > 0$. Let $U = (U_i)$ be an $\sqsubset$-universal graph sequence for $\mathcal{F}$, and $\widetilde{U} = (\widetilde{U}_i)$ an ϵ-error universal graph sequence. Then*

$$\begin{aligned}\max_{G \in \mathcal{F}_i} R^{\|}_{\epsilon}(\textsc{Adj}(G)) \le R^{\mathsf{univ}}_{\epsilon}(\mathcal{F}_i) &\le D^{\|}(\textsc{Adj}(\widetilde{U}_i)) \\ &\le 2R^{\mathsf{univ}}_{\epsilon/2}(\mathcal{F}_i) \quad \textit{and} \quad R^{\mathsf{univ}}_{\epsilon}(\mathcal{F}_i) \le R^{\|}_{\epsilon}(\textsc{Adj}(U_i))\,.\end{aligned}$$

Proof. The inequalities on the left follow the definitions and from the above lemma. On the right, we can obtain a universal SMP protocol by choosing for each $G \in \mathcal{F}_i$ a (deterministic) embedding $g : G \to U_i$ and then using the randomized SMP protocol for $\textsc{Adj}(U_i)$. ◀

Universal graphs describe an interesting relationship between weakly-universal and universal SMP protocols (and therefore between standard SMP protocols where the referee does and does not share the randomness); namely, the optimal universal protocol is obtained by finding the smallest universal graph for the family of protocol graphs (decision functions) defined by a weakly-universal protocol.

▶ **Proposition 1.8** (Restated). *Let $\mathcal{F}$ be a family of graphs, let $\epsilon > 0$, and let W_ϵ be the set of all ϵ-error weakly-universal SMP protocols for $\mathcal{F}$. For each $\Pi \in W_\epsilon$ let $\mathcal{U}_\Pi = (\mathcal{U}_{\Pi,i})$ be the family of graphs $\mathcal{U}_{\Pi,i} = \{F_i(r,\cdot,\cdot) : r \text{ is a random seed for } \Pi\}$ where F_i is the decision function of Π. Then*

$$R^{\mathsf{univ}}_{\epsilon}(\mathcal{F}) = \min_{\Pi \in W_\epsilon} D^{\mathsf{univ}}(\mathcal{U}_\Pi)\,.$$

Proof. Let $\Pi \in W_\epsilon$; we will construct a universal SMP protocol as follows. On input $(G,x),(G,y)$, Alice and Bob use shared randomness r to simulate Π and obtain vertices $a(r,G,x), b(r,G,y)$ in some graph $U_r \in \mathcal{U}_\Pi$ with $\mathbb{P}_r[U_r(a(r,G,x),b(r,G,y)) \neq G(x,y)] < \epsilon$. They now simulate the deterministic universal SMP protocol, i.e. an embedding $\phi : V(U_r) \to U'$ for some graph U' that is $\sqsubset$-universal for $\{U_r\}$, and send $\phi(a(r,G,x)), \phi(b(r,G,y))$ to the referee who computes $U'(\phi(a(r,G,x)), \phi(b(r,G,x))) = U_r(a(r,G,x), b(r,G,y))$.

Now let Π be an ϵ-error universal SMP protocol. Then $\Pi \in W_\epsilon$ and for each i, $\mathcal{U}_{\Pi,i} = \{U_i\}$, where U_i is the graph of the decision function. $D^{\mathsf{univ}}(\mathcal{U}_\Pi) \leq \lceil \log |U_i| \rceil$, which is the cost of Π, so $\min_{\Pi \in W_\epsilon} D^{\mathsf{univ}}(\mathcal{U}_\Pi) \leq R^{\mathsf{univ}}_\epsilon(\mathcal{F})$. ◀

Newman's Theorem for public-coin randomized (2-way) protocols is a classic result that gives a bound on the number of uniform random bits required to compute a function $f : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ in terms of the size of the input domain [28]. In the universal model, the input size can be very large since the graph (function) itself is part of the input. However, the shared part of the input does not contribute to the number of random bits required in the universal SMP model.

▶ **Lemma 2.14** (Newman's Theorem for universal SMP). *Let $\epsilon, \delta > 0$ and suppose there is an ϵ-error universal SMP protocol Π for the family $\mathcal{F} = (\mathcal{F}_i)$. Then there is an $(\epsilon+\delta)$-error universal SMP protocol for the family $\mathcal{F}$ that uses at most $\log\log\left(n(i)^{O(\epsilon/\delta^2)}\right)$ bits of randomness and has the same communication cost.*

Proof. Fix i, let F be the deterministic decision function for $\mathcal{F}_i$, and let $a(r,\cdot,\cdot), b(r,\cdot,\cdot)$ be Alice and Bob's encoding functions for the random seed r. For $G \in \mathcal{F}_i$ and $x,y \in V(G)$ we will say a seed r is *bad* for G,x,y if $F(a(r,G,x),b(r,G,y)) \neq G(x,y)$, and we will call this event $\mathsf{bad}(G,x,y,r)$.

Let $r_1,\dots,r_m$ be independent random seeds, and let $i \sim [m]$ be uniformly random, where $m > \frac{3\epsilon}{\delta^2}\ln(n^2)$. Then for every G, the expected number of vertex pairs x,y for which the strings $r_1,\dots,r_m$ fail is

$$\begin{aligned}
&\mathop{\mathbb{E}}_{r_1,\dots,r_m}\left[\sum_{x,y} \mathbb{1}\left[\mathop{\mathbb{P}}_{i\sim[m]}[\mathsf{bad}(G,x,y,r_i)] > \epsilon+\delta\right]\right] \\
&\quad\leq n^2 \max_{x,y} \mathop{\mathbb{E}}_{r_1,\dots,r_m}\left[\mathbb{1}\left[\mathop{\mathbb{P}}_{i}[\mathsf{bad}(G,x,y,r_i)] > \epsilon+\delta\right]\right] \\
&\quad= n^2 \max_{x,y} \mathop{\mathbb{P}}_{r_1,\dots,r_m}\left[\mathop{\mathbb{P}}_{i}[\mathsf{bad}(G,x,y,r_i)] > \epsilon+\delta\right] \\
&\quad= n^2 \max_{x,y} \mathop{\mathbb{P}}_{r_1,\dots,r_m}\left[\sum_{i=1}^m \mathbb{1}[\mathsf{bad}(G,x,y,r_i)] > m(\epsilon+\delta)\right].
\end{aligned}$$

The sum has mean $\mu = \sum_{i=1}^m \mathop{\mathbb{E}}_{r_i}[\mathbb{1}[\mathsf{bad}(G,x,y,r_i)]] < m\epsilon$, so by the Chernoff bound, the probability is at most

$$\begin{aligned}
&n^2 \mathop{\mathbb{P}}_{r_1,\dots,r_m}\left[\sum_{i=1}^m \mathbb{1}[\mathsf{bad}(G,x,y,r_i)] > (1+m\delta/\mu)\mu\right] \\
&\quad\leq n^2 \exp\left(-\frac{m^2\delta^2}{3\mu}\right) \leq n^2 \exp\left(-\frac{m\delta^2}{3\epsilon}\right) < 1.
\end{aligned}$$

Since the expected number of pairs x,y where choosing $i \sim [m]$ fails with probability more than $\epsilon+\delta$ is less than 1, there must be some values of $r_1,\dots,r_m$ with no bad pairs for G. So for every $G \in \mathcal{F}_i$ we may choose $r_1, \ldots, r_m$ so that choosing i uniformly at random is the only random step; since $m = \frac{6\epsilon}{\delta^2} \ln n = \log n^{O(\epsilon/\delta^2)}$ this requires at most $\log m = \log\log\left(n^{O(\epsilon/\delta^2)}\right)$ random bits. ◀

With this result, we can conclude the proof of Theorem 1.7 in the next lemma.

▶ **Lemma 2.15.** *For any family $\mathcal{F} = (\mathcal{F}_i)$ with size function $n(i)$,*

$$\Omega\left(\frac{D^{\mathsf{univ}}(\mathcal{F}_i)}{\log n(i)}\right) \leq R^{\mathsf{univ}}(\mathcal{F}_i) \leq D^{\mathsf{univ}}(\mathcal{F}_i)\,.$$

Proof. The upper bound is clear, so we prove lower bound. Let $\Pi = (\Pi_i)$ be a sequence of randomized universal SMP protocols for $\mathcal{F}$. By Newman's theorem, we may assume that Π_i uses at most $\log\log n(i)^c$ random bits for some constant c and has error probability $3/8$. Let F_i be the decision function of Π_i, let $m(i)$ be the cost of Π_i, and let $k = \lceil c \log n(i) \rceil$. To obtain a deterministic protocol, we can define the decision function F_i' on messages of $k \cdot m(i)$ bits as $F_i'(a_1, b_1, a_2, b_2, \ldots, a_k, b_k) = \text{majority}(F_i(a_j, b_j))_j$. Alice and Bob iterate over all $k = 2^{\log\log n(i)^c}$ random strings r and send $a(r, G, x), b(r, G, y)$ for each. Since the probability of error is at most $3/8$ when r is uniform, at least $5k/8 > k/2$ of the functions $F_i(a_j, b_j)$ will give the correct answer. This proves that $D^{\mathsf{univ}}(\mathcal{F}_i) = O(R^{\mathsf{univ}}(\mathcal{F}_i) \log n(i))$. ◀

In this paper we show lower bounds for a family $\mathcal{F}$ by giving embeddings of an arbitrary graph G into $\mathcal{F}$, so we need to know the complexity of the family $\mathcal{G} = (\mathcal{G}_n)$ of all graphs with n vertices. For our purposes, it is convenient to require that each graph $G \in \mathcal{G}_n$ has $G(u, u) = 1$ for all u (i.e. all self-loops are present). However, since equality can be checked with cost $O(1)$, the presence or absence of self-loops does not affect the complexity.

▶ **Theorem 1.6** (Restated). *$R^{\mathsf{univ}}(\mathcal{G}) = \Theta(n)$.*

Proof. For the upper bound, consider the (deterministic) protocol where on input G, x, y, Alice and Bob send x and y and the respective rows of the adjacency matrix of G. This has cost $n + \lceil \log n \rceil = O(n)$ and the referee can determine $G(x, y)$ by finding y in the row sent by Alice.

Let Π be any protocol for $\mathcal{G}_n$ with cost c. By Lemma 2.11, we may assume that Π is symmetric. Let F be the decision function for graphs on n vertices and let $G \in \mathcal{G}_n$ with vertex set $[n]$. Π defines a distribution over functions $g : [n] \to \{0,1\}^c$ so that for all $x, y, \mathbb{P}_g[F(g(x), g(y)) \neq G(x, y)] < \epsilon$. Therefore, for x, y drawn uniformly from $[n]$, $\mathbb{E}_{f,x,y}[\mathbb{1}[F(f(x), f(y)) \neq G(x, y)]] < \epsilon$. Therefore, for every graph $G \in \mathcal{G}_n$ there is a function f_G such that for $x, y \sim [n]$ uniformly at random, $\mathbb{P}_{x,y}[F(f_G(x), f_G(y)) \neq G(x, y)] < \epsilon$. Write $N = \binom{n}{2}$. There are at most 2^{cn} functions $[n] \to \{0,1\}^c$ and there are 2^N simple graphs on $[n]$ so there is some function $f : [n] \to \{0,1\}^c$ where the number of graphs G such that $f_G = f$ is at least $\frac{2^N}{2^{cn}} = 2^{N-cn}$. Let G, G' be any two such graphs. Then

$$\begin{aligned}
&\mathbb{P}_{x,y\sim[n]}[G(x, y) \neq G'(x, y)] \\
&\qquad \leq \mathbb{P}_{x,y\sim[n]}[G(x, y) \neq F(f(x), f(y)) \text{ or } G'(x, y) \neq F(f(x), f(y))] < 2\epsilon\,.
\end{aligned}$$

So G, G' differ on at most $2\epsilon N$ pairs. However, the largest number of graphs that differ from any graph G on at most $2\epsilon N$ pairs of vertices is at most

$$\sum_{k=0}^{2\epsilon N} \binom{N}{k} \leq 2\epsilon N \binom{N}{2\epsilon N} \leq \epsilon N \left(\frac{eN}{2\epsilon N}\right)^{2\epsilon N} = 2^{2\epsilon N \log(e/2\epsilon) + \log(2\epsilon N)}\,.$$

Therefore we must have

$$N - cn \le 2\epsilon N \log(e/2\epsilon) + \log(2\epsilon N)$$

so $c = \Omega(n)$. ◀

Recall the example in the first paragraph of the introduction, for which we observed that a single decision function would work for many problems. We now make a note about this phenomenon. A communication protocol for a graph family $\mathcal{F} = (\mathcal{F}_i)$ is really a sequence of protocols, one for each set $\mathcal{F}_i$ of graphs with $n(i)$ vertices. Our next proposition addresses the uniformity of the sequence of protocols, that is, the question of how the protocols are related to one another as the size of the input grows. In general, we ask the question: If the family $\mathcal{F}$ has some relationship between $\mathcal{F}_i$ and $\mathcal{F}_{i+1}$, what does this imply about the relationship between the protocols for i and $i+1$? The families of graphs we study in this paper have constant-cost protocols and they are also *upwards families*, which we define next. These families have enough structure so that there exists a single, one-size-fits-all probabilistic universal graph, into which all graphs can be embedded regardless of their size; in other words, the referee can be ignorant not only of the graph G and vertices x, y, but also of the *size* of the graph, without increasing the cost of the protocol.[2]

▶ **Definition 2.16.** *We call a graph family $\mathcal{F} = (\mathcal{F}_i)$ an* upwards family *if for every i and every $G \in \mathcal{F}_i$ there exists $G' \in \mathcal{F}_{i+1}$ such that G is an induced subgraph of G'.*

Many graph families are upwards families, for example: bounded-degree graphs, bounded-arboricity graphs, planar graphs, and transitive reductions of distributive lattices.

▶ **Proposition 2.17.** *If $\mathcal{F}$ is an upwards graph family with an ϵ-error randomized universal graph sequence $U = (U_i)$ satisfying $|V(U_i)| \le c$ for some constant c (which may depend on ϵ), then there exists a graph U^* of size c such that $\forall G \in \mathcal{F}, G \sqsubset_\epsilon U^*$. Furthermore, for any $i < j$ and any $G \in \mathcal{F}_i$, there exists $G' \in \mathcal{F}_j$ with ϵ-error embedding $g' : V(G') \to V(U^*)$ such that G is an induced subgraph of G' and the restriction of g' to the domain $V(G)$ is an ϵ-error embedding $V(G) \to V(U^*)$.*

Proof. Let $G \in \mathcal{F}_i$ and let $G' \in \mathcal{F}_{i+1}$ be such that G is an induced subgraph of G'. Let $g' : V(G') \to V(U_{i+1})$ the random function determined by the randomized universal graph sequence. Then g' restricted to the domain $V(G) \subset V(G')$ satisfies

$$\mathbb{P}_{g'}\left[U_{i+1}(g'(x), g'(y)) = G(x,y)\right] = \mathbb{P}_{g'}\left[U_{i+1}(g'(x), g'(y)) = G'(x,y)\right] > 1 - \epsilon\,.$$

Therefore we may replace U_i with U_{i+1} in the sequence, for any i.

Since each U_i has size at most c, there are at most 2^{c^2} graphs U_i appearing in the sequence U. Thus there is some graph U^* that occurs an infinite number of times in the sequence. For every i there exists $j > i$ such that $U_j = U^*$. By applying the above argument, we may replace U_i with $U_j = U^*$ in the sequence. We arrive at the sequence $U' = (U'_i)$ with $U'_i = U^*$ for every i. ◀

---

[2] Any family $\mathcal{F}$ with a constant-cost protocol can be turned into a protocol ignorant of the size by requiring that Alice and Bob tell the referee which of the 2^{c^2} possible decision functions to use, where $c = 2^{R^{\text{univ}}(\mathcal{F})}$.

2.3 Implicit Graph Representations and Induced-Universal Graphs

Kannan, Naor, and Rudich [23] call a family of graphs an *implicit* graph family if each of the n vertices can be given a label of $O(\log n)$ bits so that adjacency can be determined from the labels of two vertices. They observe that an implicit encoding gives an upper bound on the size of an *induced-universal graph*. We define these terms below in slightly more generality (and omit the requirement that encoding and decoding be done in polynomial time):

▶ **Definition 2.18.** *Let $\mathcal{F} = (\mathcal{F}_i)$ be a graph family and $m(i)$ a function of the graph size. The family $\mathcal{F}$ has an m-*implicit *encoding if $\forall i, \exists F_i : \{0,1\}^{m(i)} \times \{0,1\}^{m(i)} \to \{0,1\}$ such that F_i is symmetric and $\forall G \in \mathcal{F}_i, \exists g : V(G) \to \{0,1\}^{m(i)}$ satisfying $\forall x, y \in V(G), F_i(g_i(x), g_i(y)) = G(x,y)$.*

For a graph family $\mathcal{F} = (\mathcal{F}_i)$, an induced-universal graph sequence *is a sequence $U = (U_i)$ such that for each i and all $G \in \mathcal{F}_i$, G is an induced sugraph of U_i.*

Our notion of $\sqsubset$-universal graphs differs from induced-universal graphs, since the embedding relation $G \sqsubset U_i$ allows non-injective mappings (two vertices of G may be mapped to the same vertex in U_i). This difference accounts for the extra factor $n(i)$ in the next theorem.

▶ **Theorem 2.19** ([33]). *Let $\mathcal{F} = (\mathcal{F}_i)$ be a graph family with size $n(i)$. If there exists an m-implicit encoding of $\mathcal{F}$ there is an induced-universal graph sequence $U = (U_i)$ such that $|U_i| \le n(i) 2^{m(i)} = 2^{m(i) + \log n(i)}$.*

Due to the fact that a deterministic universal SMP protocol may always be assumed to be symmetric (Proposition 2.6), it follows by definition and from Lemma 2.15 that:

▶ **Theorem 1.1** (Restated). *A graph family $\mathcal{F} = (\mathcal{F}_i)$ is m-implicit iff $D^{\mathsf{univ}}(\mathcal{F}_i) \le m(i)$ for every i. Therefore, $\mathcal{F}$ is $O(R^{\mathsf{univ}}(\mathcal{F}) \cdot \log n)$-implicit.*

If one's goal is merely to obtain an $O(1)$-cost universal SMP protocol for a family $\mathcal{F}$, the next observation shows that it suffices to find an $O(1)$-cost, public-coin, 2-way protocol for each member of $\mathcal{F}$. Therefore the family of all graphs with an $O(1)$-cost 2-way protocol is an implicit graph family with a polynomial-size induced-universal graph.

▶ **Corollary 1.2** (Restated). *Let $\mathcal{F} = (\mathcal{F}_i)$ be a family of graphs with size $n(i)$ and suppose that for every graph $G \in \mathcal{F}_i$ there is an ϵ-error 2-way randomized communication protocol with cost at most $c(i)$. Then $R^{\mathsf{univ}}_\epsilon(\mathcal{F}) \le 2^{c(i)}$. Furthermore, for any fixed constant c, the family $\mathcal{F}$ of graphs with $R^{\leftrightarrow}(\textsc{Adj}(G)) \le c$ is $O(\log n)$-implicit.*

Proof. Every 2-way, deterministic cost c protocol can be represented as a binary tree with at most 2^c nodes, where each node is owned by either Alice or Bob and the message sent at each step is a 0 or 1 informing the other player of which branch to take in the tree. A randomized 2-way protocol is a distribution over such trees. To obtain a universal SMP protocol for the family $\mathcal{F}$, Alice and Bob do the following. On input $G \in \mathcal{F}$ and $x, y \in V(G)$, Alice and Bob use shared randomness to draw the deterministic cost c protocol for G from the distribution defined by the randomized 2-way protocol. Alice sends the size 2^c protocol tree and for each node she owns she identifies the branch to be taken. Bob does the same. The referee may then simulate the protocol. The conclusion follows from Theorem 1.1. ◀

3 Distance Labeling of Distributive Lattices

Distributive lattices and distances on these lattices will be defined in the next subsection, where we also give a necessary lemma characterizing the distances in terms of the *meet* and *join*. We will then present an $O(k \log k)$ weakly-universal protocol and an $O(k^2)$ universal communication protocol for the family $\mathcal{D}^k$, where $\mathcal{D}$ are the distributive lattices. This implies a $O(k^2 \log n)$-implicit encoding $\mathcal{D}^k$ of the family $\mathcal{D}$ of distributive lattices. The $O(k \log k)$ weakly-universal protocol is optimal for sufficiently small values of k, since it applies to the k-Hamming Distance problem as a special case, for which Sağlam [31] recently gave a matching lower bound (even for 2-way communication). We obtain this result by adapting the optimal $O(k \log k)$ communication protocol for k-Hamming Distance originally presented by Huang et al. [21].

We also consider *modular* lattices, a generalization of distributive lattices, and show that deciding $\mathsf{dist}(x, y) \leq 2$ requires a protocol with cost $\Omega(n^{1/4})$.

3.1 Preliminaries on Distributive Lattices

A lattice is a type of partial order. We briefly review distributive lattices (see e.g. [9] for a good introduction) and then give a characterization of distances in modular and distributive lattices. The undirected graphs we study are the *cover graphs* of partial orders. For x, y in a partial order P, we say that y *covers* x and write $x \prec y$ if $\forall z \in P$: if $x \leq z < y$ then $x = z$. The *cover graph* (which is the undirected version of the *transitive reduction*) is the graph $\text{cov}(P)$ on vertex set P with an edge $\{x, y\}$ iff $x \prec y$ or $y \prec x$.

We will define a few types of lattices.

▶ **Definition 3.1.** *Let $(P, <)$ be a partial order. For a pair $x, y \in P$:*
- *If the set $\{z \in P : x, y \geq z\}$ has a unique maximum, we call that maximum the* join *of x, y and write it as $x \wedge y$;*
- *If the set $\{z \in P : x, y \leq z\}$ has a unique minimum, we call that minimum the* meet *of x, y and write it as $x \vee y$.*

If $\forall x, y \in P$ the elements $x \wedge y, x \vee y$ exist, then P is a lattice*. A lattice L is* ranked *if there exists a rank function such that $x \prec y \implies \text{rank}(x) + 1 = \text{rank}(y)$ and the minimum element 0_L satisfies $\text{rank}(0_L) = 0$. A finite lattice L is* upper-semimodular *if for every $x, y \in L$, $x \wedge y \prec x, y \implies x, y \prec x \vee y$. L is* lower-semimodular *if for every $x, y \in L$, $x, y \prec x \vee y \implies x \wedge y \prec x, y$. L is* modular *if it is both upper- and lower-semimodular. A lattice L is* distributive *if for all $x, y, z \in L$, $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$. Every distributive lattice is modular and every modular lattice is ranked [9].*

A point x in a lattice L is join-irreducible *if there is no set $S \subseteq L$ such that $x = \bigvee S$ and* meet-irreducible *if there is no set $S \subseteq L$ such that $x = \bigwedge S$. Write $J(L)$ for the set of join-irreducible elements.*

A subset D of a partial order P is a downset *or* ideal *if: for all $x, y \in L$, if $x \in D$ and $y \leq x$ then $y \in D$. We will write $D(P)$ for the set of ideals of P.*

▶ **Theorem 3.2** (Birkhoff (see e.g. [9])). *Every distributive lattice L is isomorphic to the lattice of downsets of the partial order on its join-irreducible elements, ordered by inclusion; i.e. $L \simeq D(J(L))$, with the meet and join operations given by set union and intersection respectively.*

We need to prove some facts about distances in modular lattices.

▶ **Proposition 3.3.** *Let L be a graded lattice and let $x, y \in L$. Then $\mathsf{dist}(x, y) \geq |\text{rank}(x) - \text{rank}(y)|$, with equality if $x < y$ or $y < x$.*

Proof. This follows from the fact that for every edge $u \prec v$ in the path from x to y has $\text{rank}(u) + 1 = \text{rank}(v)$. ◀

To prove our characterization of distance, we define *inversions* in the path.

▶ **Definition 3.4.** *Let L be a lattice and let $c_1, \dots, c_m$ be a path in $\mathrm{cov}(L)$, so that $c_i \prec c_{i+1}$ or $c_{i+1} \prec c_i$ for each i. If $c_{i-1}, c_{i+1} \prec c_i$ or $c_i \prec c_{i-1}, c_{i+1}$ we call c_i an* inversion *on the path.*

▶ **Lemma 3.5.** *The following holds for any x, y in a lattice $\mathcal{M}$:*
1. *If $\mathcal{M}$ is lower-semimodular then $\mathsf{dist}(x, y) = \mathsf{dist}(x, x \wedge y) + \mathsf{dist}(y, x \wedge y)$;*
2. *If $\mathcal{M}$ is upper-semimodular then $\mathsf{dist}(x, y) = \mathsf{dist}(x, x \vee y) + \mathsf{dist}(y, x \vee y)$;*
3. *If $\mathcal{M}$ is distributive then $\mathsf{dist}(x, y) = |X \Delta Y|$ where $X, Y \in D(J(\mathcal{M}))$ are isomorphic images of x, y in Birkhoff's representation.*

Proof. It suffices to prove the first statement: the second follows by the analogous argument and the third follows from the modulartiy of distributive lattices and Birkhoff's representation.

Let $\mathcal{M}$ be lower-semimodular, let $x, y \in \mathcal{M}$, and let $x = c_0, c_1, \dots, c_m = y$ be a shortest path between x and y, so that $\mathsf{dist}(x, y) = \mathsf{dist}(x, c_i) + \mathsf{dist}(y, c_i)$ for any i. The statement holds trivially when $x < y$ or $y < x$ (since $x \wedge y = x$ or $x \wedge y = y$), so we assume x, y are incomparable. We prove the statement by induction on the largest rank of an inversion of the form $c_{i-1}, c_{i+1} \prec c_i$ in the path.

First suppose that c_i is any element of the path and assume for contradiciton that $\mathrm{rank}(c_i) < \mathrm{rank}(x \wedge y)$. Then

$$\mathsf{dist}(x, x \wedge y) = \mathrm{rank}(x) - \mathrm{rank}(x \wedge y) < \mathrm{rank}(x) - \mathrm{rank}(c_i) \leq \mathsf{dist}(x, c_i),$$

a contradiction. Thus $\mathrm{rank}(c_i) \geq \mathrm{rank}(x \wedge y)$ for each element of the path.

Suppose there are no inversions of the form $c_{i-1}, c_{i+1} \prec c_i$. Then $c_i < x, y$ and therefore $c_i \leq x \wedge y$ so $\mathrm{rank}(c_i) \leq \mathrm{rank}(x \wedge y)$, and by the above inequality we have $\mathrm{rank}(c_i) \geq \mathrm{rank}(x \wedge y)$, so $\mathrm{rank}(c_i) = \mathrm{rank}(x \wedge y)$. Therefore, as desired,

$$\begin{aligned}\mathsf{dist}(x, y) &= \mathsf{dist}(x, c_i) + \mathsf{dist}(y, c_i) = \mathrm{rank}(x) - \mathrm{rank}(c_i) + \mathrm{rank}(y) - \mathrm{rank}(c_i) \\ &= \mathrm{rank}(x) - \mathrm{rank}(x \wedge y) + \mathrm{rank}(y) - \mathrm{rank}(x \wedge y) \\ &= \mathsf{dist}(x, x \wedge y) + \mathsf{dist}(y, x \wedge y) .\end{aligned}$$

Now let c_i be an inversion of the form $c_{i-1}, c_{i+1} \prec c_i$ with $\mathrm{rank}(c_i) > \mathrm{rank}(x \wedge y)$. Then by lower-semimodulariity there is an element $c_i' = c_{i-1} \wedge c_{i+1} \prec c_{i-1}, c_{i+1}$. Then replacing c_i with c_i' maintains the length of the path. Performing the same operation on all such inversions of maximum rank reduces the maximum rank by 1 and the result holds by induction. ◀

3.2 A Universal Protocol for Distributive Lattices

Write $\mathcal{D} = (\mathcal{D}_n)$ for the family of cover graphs of distributive lattices on n vertices. We first give an optimal protocol for distances in distributive lattices in the *weak* universal model (recall that in this model, the referee sees the shared randomness). This protocol is adapted from a simplified presentation of Huang et al.'s k-Hamming Distance protocol ([21]) communicated to us by E. Blais.

▶ **Theorem 3.6.** *For any $\epsilon > 0$ and integer k, $R_\epsilon^{\mathsf{weak}}(\mathcal{D}^k) = O\left(k \log(k/\epsilon)\right)$.*

Proof. For any distributive lattice $L \simeq D(J(L))$, identify each vertex $x \in L$ with its ideal $X \subseteq J(L)$ of join-irreducibles. Write $e_1, \dots, e_m$ for the basis vectors of $\mathbb{F}_2^m$. Consider the following protocol. On the distributive lattice L and vertices x, y, Alice and Bob perform the following:

1. Define $m = \lceil \frac{(k+2)^2}{\epsilon} \rceil, q = \lceil \log \frac{1}{\epsilon} + \log \sum_{i=0} \binom{m}{i} \rceil$.
2. Let $S = (s_1, \dots, s_m)$ be a multiset of uniformly random elements of $\mathbb{F}_2^q$.
3. For each join-irreducible element $j \in J(L)$ assign a uniformly random index $i_j \sim [m]$.
4. For each vertex $v \subseteq J(L)$ there is an indicator vector $a(v) \in \mathbb{F}_2^m$ defined by $a(v) = \sum_{j \in v} e_{i_j}$. Label v with $\ell(v) = \sum_{i=1}^m a(v)_i s_i$.
5. Alice sends $\ell(x)$ and Bob sends $\ell(y)$ to the referee.
6. The referee accepts iff $\ell(x) + \ell(y)$ is a sum of at most k elements of S.

By Lemma 3.5 and Birkhoff's theorem, $\mathsf{dist}(x, y) = \mathsf{dist}(x, x \wedge y) + \mathsf{dist}(x \wedge y, y) = |X \setminus Y| + |Y \setminus X| = |X \Delta Y|$, where Δ denotes the symmetric difference. Suppose $\mathsf{dist}(x, y) = |X \Delta Y| \le k$. Then $\ell(x) + \ell(y) = \sum_{j \in X \Delta Y} c(j)$ is a sum of at most k elements of S, so the protocol accepts with probability 1 (so this protocol has 1-sided error).

Now suppose $\mathsf{dist}(x, y) = |X \Delta Y| \ge k + 1$. The correctness of the protocol follows from the next two claims along with the observations that $a(x) + a(y) = a(x \wedge y)$ and $\ell(x) + \ell(y) = \ell(x \wedge y)$ (with arithmetic in $\mathbb{F}_2$) and that $\mathsf{dist}(x, y) \ge k + 1$ implies $\operatorname{rank}(x \wedge y) \ge k + 1$. We will write $|a(v)|$ for the number of 1's in the vector $a(v)$.

▷ Claim 3.7. Any vertex $v \subseteq J(L)$ with $\operatorname{rank}(v) \ge k + 1$ has $|a(v)| \ge k + 1$ with probability at least $1 - \epsilon/2$.

Proof of claim. If $\operatorname{rank}(v) = k + 1$, so v is a set of $k + 1$ join-irreducibles, then the probability that any two indices $i_j, i_{j'}$ collide, for $j, j' \in v$, is by the union bound at most

$$\binom{k+1}{2} \mathbb{P}\left[i_j = i_{j'}\right] = \frac{k(k+1)}{2} \frac{1}{m} \le \frac{(k+1)^2}{2} \frac{\epsilon}{(k+2)^2} = \epsilon/2 \,.$$

For $\operatorname{rank}(v) > k + 1$ choose $v' \prec v$ so $k + 1 \le \operatorname{rank}(v') < \operatorname{rank}(v)$, so using induction and the assumption $\epsilon < 1/2$,

$$\begin{aligned} \mathbb{P}\left[|a(v)| \le k\right] &= \frac{k+1}{m} \mathbb{P}\left[|a(v')| = k+1\right] + \frac{k}{m} \mathbb{P}\left[|a(v')| \le k\right] < \frac{\epsilon}{k+2} + \frac{\epsilon}{k+2} \cdot \frac{\epsilon}{2} \\ &= \epsilon \left(\frac{1}{k+2} + \frac{\epsilon}{2(k+2)} \right) \le \epsilon \left(\frac{1}{3} + \frac{1}{12} \right) < \epsilon/2 \,. \end{aligned}$$ ◁

▷ Claim 3.8. For any vertex $v \subseteq J(L)$, if the indicator vector $a(v)$ has weight $\ge k + 1$ then, with probability at least $1 - \epsilon/2$, $\ell(v)$ is not a sum of at most k vectors in S.

Proof of claim. Write kS for the set of all sums of at most k vectors of S. Fix any $a(v)$ with weight $\ge k + 1$ and let $A = \{i : a(v)_i = 1\}$ so $|A| \ge k + 1$. Let $b \in kS$ be any sum of k vectors in S, and let $B \subset [m]$ be a set of indices of size $|B| \le k$ such that $b = \sum_{i \in B} s_i$.

Since $|B| \le k < |A|$ we must always have $A \setminus B \neq \emptyset$ and $\ell(v) + b = \sum_{i \in A \setminus B} s_i$, so $\mathbb{P}\left[\ell(v) + b = 0\right] = 2^{-q}$. Therefore, by the union bound over all such vectors b,

$$\mathbb{P}\left[\ell(v) \in kS\right] \le \sum_{i=0}^{k} \binom{m}{i} 2^{-q} < \epsilon/2 \,.$$ ◁

We can put a bound on q by using

$$\sum_{i=0}^{k} \binom{m}{i} \le k \binom{m}{k} \le k \left(\frac{em}{k} \right)^k$$

so

$$q \le 1 + \log \frac{1}{\epsilon} + \log k + k \log \frac{em}{k} \le \log \frac{2k}{\epsilon} + k \log \lceil \frac{ek}{\epsilon} \rceil = O\left(k \log \frac{k}{\epsilon} \right) \,.$$ ◀

Observe that the referee must see the set S for the above protocol to work. We can easily modify the above protocol to get $O(k^2)$.

▶ **Theorem 3.9.** *For any $\epsilon > 0$ and any integer k, $R_\epsilon^{\mathsf{univ}}(\mathcal{D}^k) = O\left(k^2 \log(1/\epsilon)\right)$.*

Proof. The protocol is the same as above, with the following modification: Alice and Bob each send the indicator vectors $a(x), a(y) \in \mathbb{F}_2^m$.

The correctness of this protocol for error 1/3 follows from Claim 3.7. Observe that Alice and Bob use the same strategy to send their messages and that the decision function is symmetric. The communication cost is now at most $m = \lceil 3(k+2)^2/2 \rceil$.

This protocol is one-sided, so to achieve error ϵ we can run the protocol $r = \lceil \log_3(1/\epsilon) \rceil$ times and take the AND of the results. The probability of failure is $(1/3)^r = 3^{-r} < \epsilon$. ◀

Now we apply Theorem 1.1 to obtain Theorem 1.3.

Since the family of distributive lattices is an upwards family (simply append a new least element to obtain a larger distributive lattice), we see from Proposition 2.17 that lattices in $\mathcal{D}^k$ can be randomly embedded into a constant-size graph, for any constant k. In fact, by inspection of the protocol, we see that the family $\mathcal{D}$ can be randomly embedded into a small-dimensional hypercube, while $\mathcal{D}^k$ can be embedded into the k-closure of the $O(k^2)$-dimensional hypercube.

▶ **Corollary 3.10.** *For any $\epsilon > 0$ and any k, there exists a graph U of size $2^{O(k^2 \log(1/\epsilon))}$ such that for all $L \in \mathcal{D}^k$, $L \sqsubset_\epsilon U$.*

3.3 Lower Bound for Modular Lattices

Since Lemma 3.5 works for any modular lattices, it is natural to ask whether we can achieve a similar constant-cost protocol for computing distance thresholds in modular lattices. However, we show that this is impossible.

▶ **Lemma 3.11.** *There is a function $m(n) = O(n^4)$ such that if G is any graph with n vertices (where $G(u,u) = 1$ for all u), there exists a modular lattice M with size $m(n)$ such that G is an induced subgraph of* $\mathrm{cov}(M)^2$.

Proof. Construct the lattice M as follows:

1. Start with vertices V, which are all incomparable.
2. For each edge $e = \{u, v\} \in E$, add vertices a_e, b_e such that $a_e < u, v < b_e$.
3. $\forall e = \{u, v\}, e' = \{u', v'\} \in E$ such that $e \cap e' = \emptyset$ add a vertex $c_{e,e'}$ with $a_e, a_{e'} < c_{e,e'} < b_e, b_{e'}$.
4. Add vertices 0_M and 1_M such that $0_M < a_e$ and $b_e < 1_M$ for all $e \in E$.

First we prove that M is a modular lattice and then we prove the bound on the size.

▷ Claim 3.12. M is a modular lattice.

Proof of claim. Observe that all orderings $<$ directly imposed by this process are covering orders $\prec$. Let $A = \{a_e\}_{e \in E}, B = \{b_e\}_{e \in E}, C = \{c_e\}_{e \in E}$ and V the original set of vertices. By construction, M is graded with $\mathrm{rank}(0_M) = 0, \mathrm{rank}(A) = 1, \mathrm{rank}(V) = \mathrm{rank}(C) = 2, \mathrm{rank}(B) = 3, \mathrm{rank}(1_M) = 4$. Note that for every pair of vertices $x, y \in M, 0_M \leq x, y \leq 1_M$ so upper- and lower-bounds exist.

Assume for contradiction that M is not a modular lattice, so there exist incomparable $x, y \in M$ such that either $x \wedge y$ or $x \vee y$ does not exist, or such that $x \wedge y \prec x, y \not\prec x \vee y$ or $x \wedge y \not\prec x, y \prec x \vee y$.

Case 1: Suppose $\mathrm{rank}(x) \neq \mathrm{rank}(y)$. Then $x \wedge y = 0_M$ and $x \vee y = 1_M$ so $x \wedge y \not\prec x, y \not\prec x \vee y$.

Case 2: Suppose $x, y \in A$ so $x = a_e, y = a_{e'}$. Then $0_M = a_e \wedge a_{e'} \prec a_e, a_{e'}$. If $a_e, a_{e'} < u, v$ for $u, v \in V$ then $u, v \in e \cap e'$ so $u = v$. If $a_e, a_{e'} < v, c_{d,d'}$ for $v \in V$ and $c_{d,d} \in C$ then $v \in e \cap e'$ and $c_{d,d'} = c_{e,e'}$ so $e \cap e' = \emptyset$, a contradiction. Finally, if $a_e, a_{e'} < c_{d,d'}, c_{d',d''}$ then $c_{d,d'} = c_{d',d''} = c_{e,e'}$. So $a_e \vee a_{e'}$ exists and $a_e \wedge a_{e'} \prec a_e, a_{e'} \prec a_e \vee a_{e'}$. The same argument holds for $x, y \in B$.

Case 3: Suppose $x, y \in V$ and assume $a_e, a_{e'} < x, y$. Then $x, y \in e \cap e'$ so $a_e = a_{e'}$. A similar argument holds for $x, y < b_e, b_{e'}$. So $x \wedge y \prec x, y \prec x \vee y$.

Case 4: Suppose $x, y \in C$ so $x = c_{e,e'}, y = c_{d,d'}$. Suppose $a_s, a_t < c_{e,e'}, c_{d,d'}$. Then $s, t \in \{e, e'\} \cap \{d, d'\}$ so either $\{e, e'\} = \{d, d'\}$ or $s = t$. The same argument holds for $c_{e,e'}, c_{d,d'} < b_s, b_t$ so $x \wedge y \prec x, y \prec x \vee y$.

Case 5: Suppose $x \in V, y \in C$ so $y = c_{e,e'}$ which implies $e \cap e' = \emptyset$. If $x \notin e \cup e'$ then $x \wedge c_{e,e'} = 0_M$ and $x \vee c_{e,e'} = 1_M$ so $x \wedge c_{e,e'} \not\prec x, c_{e,e'} \not\prec x \vee c_{e,e'}$; so suppose $x \in e \cup e'$. If $a_e, a_{e'} < x, c_{e,e'}$ then $x \in e \cap e'$ which is a contradiction. Then $x \in e$ or $x \in e'$; say $x \in e$. Then $a_e = x \wedge c_{e,e'}$. The same argument holds for B so $a_e = x \wedge c_{e,e'} \prec x, c_{e,e'} \prec x \vee c_{e,e'} = b_e$. ◁

▷ Claim 3.13. G is an induced subgraph of $\mathrm{cov}(M)^2$.

Proof of claim. Suppose $\{u, v\} \in E$. Then there is $a_e \prec u, v$ so $\mathsf{dist}(u, v) \leq 2$ in $\mathrm{cov}(M)$. Now let $u, v \in V(G)$ and suppose $\mathsf{dist}(u, v) \leq 2$ in $\mathrm{cov}(M)$ so that, by Lemma 3.5, $u \wedge v \prec u, v \prec u \vee w$. By construction, either $u = v$ so $G(u, v) = G(u, u) = 1$, or $u \wedge v = a_e$ for some $e \in E(G)$ so $u, v \in e$ and therefore $G(u, v) = 1$. ◁

The size of M is at most $2 + |E(G)| + |E(G)|^2 = O(n^4)$. Let $m(n)$ be the maximum size of a modular lattice obtained in this way from a graph of size n. We want all constructions to be of the same size, so repeatedly append new least elements until the size reaches $m(n)$; this maintains the modular lattice property. ◀

▶ **Theorem 3.14.** *Let $\mathcal{M} = (\mathcal{M}_n)$ be the family of cover graphs of modular lattices.* $R^{\mathsf{univ}}(\mathcal{M}^2) \geq \Omega(n^{1/4})$.

Proof. Suppose there is a protocol for $\mathcal{M}^2$ with cost $o(n^{1/4})$. Given a graph G of size n, Alice and Bob construct the modular lattice of size $m(n) = O(n^4)$ with G an induced subgraph of $\mathrm{cov}(M)^2$ and run the protocol for $\mathcal{M}^2$ with size $m(n)$ (observe that all possible constructions must be of the same size, since the referee does not know which lattice Alice and Bob construct). This has cost $o(m(n)^{1/4}) = o(n)$, which contradicts Theorem 1.6. ◀

4 Communication on Efficiently Labelable Graphs

In this section we take inspiration from the field of implicit graphs and graph labeling and show that one may often, but not always, obtain constant-cost adjacency and k-distance protocols for families that are commonly studied in the graph labeling literature.

4.1 Trees, Forests, and Interval Graphs

In this section we pick the low-hanging fruit from trees and forests (and interval graphs). Applying Theorem 1.1 with the next lemma, we get Theorem 1.4.

▶ **Lemma 4.1.** *Let $\mathcal{T} = (\mathcal{T}_n)$ be the family of trees of size n.* $R^{\mathsf{univ}}_{\epsilon}(\mathcal{T}^k) = O\left(k \log \frac{1}{\epsilon}\right)$, *and this protocol will correctly compute the distance in the case* $\mathsf{dist}(x, y) \leq k$.

Proof. Consider the following protocol. On input $(T, x), (T, y)$ for a tree T, Alice and Bob perform the following.

1. Partition the vertices of T into sets $T_1, \ldots, T_m$ such that $T_i = \{v \in V(T) : (i-1)k \leq \text{depth}(v) < ik\}$. For each $v \in V(T)$ let $t(v)$ be the index of the unique set satisfying $v \in T_{t(v)}$.
2. For each vertex $v \in V(T)$ assign a uniformly random color $\ell(v)$ in $[m]$ for $m = \lceil 6/\epsilon \rceil$. Let x' be root of the subtree of $T_{t(x)}$ that contains x, and let x'' be the root of the subtree of $T_{t(x)-1}$ that contains x. Let $x_0, x_1, \ldots, x_k, \ldots, x_{k_1} = x$ be the path from x'' to x (with $x_k = x'$) and let $y_0, \ldots, y_k, \ldots, y_{k_2}$ be the path from y'' to y. Alice and Bob send $\ell(x_0), \ldots, \ell(x_{k_1})$ and $\ell(y_0), \ldots, \ell(y_{k_2})$ respectively.
3. If $\ell(x') = \ell(y')$, let p be the maximum index such that $\ell(x_i) = \ell(y_i)$ for each $k < i \leq p$. Let $d = (k_1 - p) + (k_2 - p)$. If $\ell(x'') = \ell(y'')$, let p be the maximum index such that $\ell(x_i) = \ell(y_i)$ for each $i \leq p$ and let $d = (k_1 - p) + (k_2 - p)$. If $\ell(x'') = \ell(y')$ let p be the maximum index such that $\ell(x_i) = \ell(y_{k+i})$ for each $i \leq p$ and let $d = (k_1 - p) + (k_2 - k - p)$. If $\ell(x') = \ell(y'')$ do the same with x, y reversed. In each case, if $d \leq k$, the referee outputs d, otherwise they output "$> k$". If none of the above cases hold, output "$> k$".

The cost of this protocol is $2k\lceil \log m \rceil = O(k \log(1/\epsilon))$. With probability at least $1 - 4/m > 1 - \epsilon/2$, each of the possible equalities $x'' = y'', x' = y', x'' = y', x' = y''$ will be correctly observed by the referee. If $\{x', x''\} \cap \{y', y''\} = \emptyset$ then x, y are not in the same subtree rooted at depth $\text{depth}(x'')$, so the distance from x to any common ancestor of x, y is at least $\mathsf{dist}(x, x'') > k$. Therefore if $\mathsf{dist}(x, y) \leq k$, one of these equalities will hold. If $x'' = y''$ and q is the maximum integer such that $x_i = y_i$ for all $i \leq q$ then $\mathsf{dist}(x, y) = (k_1 - q) + (k_2 - q)$, because the deepest common ancestor of x, y is at depth $\text{depth}(x_0) + q$. Conditional on the 4 equalities being correctly observed, we will have $d = (k_1 - p) + (k_2 - p) \leq k$ since $p \geq q$. If $p > q$ then $\ell(x_{q+1}) = \ell(y_{q+1})$ even though $x_{q+1} \neq y_{q+1}$, which occurs with probability $1/m < \epsilon/2$. Therefore the probability that $d \neq \mathsf{dist}(x, y)$ is at most $2(\epsilon/2) = \epsilon$ when $\mathsf{dist}(x, y) \leq k$. A similar argument holds in the other 3 cases.

If $\mathsf{dist}(x, y) > k$ then still with probability at least $1 - \epsilon/2$ all 4 possible equalities are correctly observed. Following the same argument as in the equality case, we see that if any of the equalities hold we will have $d = \mathsf{dist}(x, y)$ with probability greater than $1 - \epsilon/2$, for total error probability less that ϵ. If none of the 4 equalities hold then the probability of error is at most $\epsilon/2$. ◀

Since trees have efficient protocols, one might wonder about generalizations of trees. The *arboricity* of a graph is one such generalization, which measures the minimum number of forests required to partition all the edges.

▶ **Definition 4.2.** *A graph $G = (V, E)$ has* arboricity α *iff there exists an edge partition of G into forests $T_1, \ldots, T_\alpha$. Equivalently, for S ranging over the set of subgraphs of G, G has*

$$\max_S \left\lceil \frac{E(S)}{V(S) - 1} \right\rceil \leq \alpha \,.$$

Low-arboricity graphs easily admit an efficient universal SMP protocol for adjacency.

▶ **Proposition 4.3.** *Let $\mathcal{F}$ be any family of graphs with arboricity at most α. For all $\epsilon > 0, R_\epsilon^{\mathsf{univ}}(\mathcal{F}) = O\left(\alpha \log \frac{\alpha}{\epsilon}\right)$.*

Proof. On the graph G and vertices x, y, Alice and Bob perform the following:

1. Compute a partition of G into α forests $T_1, \ldots, T_\alpha$.
2. Assign to each vertex v a uniformly random number $\ell(v) \sim [m]$ for $m = \lceil 2\alpha/\epsilon \rceil$.

3. Let x_i be the parent of x in tree i and let y_i be the parent of y. Alice sends $\ell(x)$ and $\ell(x_i)$ for each i, and Bob does this same with y.
4. The referee accepts iff $\ell(x) = \ell(y_i)$ or $\ell(y) = \ell(x_i)$ for any i.

This protocol has one-sided error since if x, y are adjacent then either $x_i = y$ or $y_i = x$ for some i, so the referee will accept with probability 1. If x, y are not adjacent then the referee will accept with probability at most $2\alpha \cdot \frac{1}{m} < \epsilon$. ◀

However, even graphs of arboricity 2 do not admit efficient protocols or labeling schemes for distance 2, which we can show by embedding an arbitrary graph of size $\Omega(\sqrt{n})$ into the 2-closure of an arboricity 2 graph of size n:

▶ **Proposition 4.4.** *Let $\mathcal{F}$ be the family of arboricity-2 graphs. Then $R^{\mathsf{univ}}(\mathcal{F}^2) \geq \Omega(\sqrt{n})$.*

Proof. The lower bound is obtained via Theorem 1.6 in the same way as in Theorem 3.14, using the following construction. For all simple graphs $G = (V, E)$ with n vertices, there exists a graph A of size $n + \binom{n}{2}$ and arboricity 2 such that G is an induced subgraph of A^2. Let A be the graph defined as follows:

1. Add each vertex $v \in V$ to A;
2. For each pair of vertices $\{u, v\}$ add a vertex $e_{\{u,v\}}$ and add edges $\{u, e_{\{u,v\}}\}, \{v, e_{\{u,v\}}\}$ iff $\{u, v\} \in E$.

This graph has arboricity 2 since for each $e_{\{u,v\}}$ we may assign each of its 2 incident edges a color in $\{1, 2\}$ (if the edges exist). Then the edges with color $i \in \{1, 2\}$ form a forest with roots in V. ◀

Now we give an example of a family, the interval graphs, with size $O(\log n)$ adjacency labels but with no constant-cost universal SMP protocol; in fact, randomization does not give more than a constant-factor improvement for this family. An *interval graph* of size n is a graph G where for each vertex x there is an interval $X \subset [2n]$ such that any two vertices x, y are adjacent in G iff $X \cap Y \neq \emptyset$. These have an $O(\log n)$ adjacency labeling scheme [23] (one can simply label a vertex with its two endpoints in $[2n]$).

There is a simple reduction from the Greater-Than communication problem, in which Alice and Bob receive integers $x, y \in [n]$ and must decide if $x < y$. It is known that the one-way public-coin communication cost of Greater-Than is $\Omega(\log n)$ [25], so $R^{\|}(\text{Greater-Than}) = \Omega(\log n)$.

▶ **Proposition 4.5.** *For the family $\mathcal{F}$ of interval graphs, $R^{\mathsf{univ}}(\mathcal{F}) = \Omega(\log n)$.*

Proof. We can use a universal SMP protocol for $\mathcal{F}$ to get a protocol for Greater-Than as follows. Alice and Bob construct the interval graph with intervals $[1, i], [i, n]$ for each $i \in [n]$, so there are $2n$ vertices in G. On input $x, y \in [n]$, Alice and Bob compute adjacency on the intervals $[1, x], [1, y]$ and then again on $[1, x], [y, n]$. Assume both runs of the protcol succeed. Then when the output is 1 for both runs we must have $y \in [1, x]$ so $y \leq x$ and otherwise we have $y \notin [1, x]$ so $x < y$. ◀

4.2 Planar Graphs

Write $\mathcal{P}_n$ for the set of planar graphs of size n and write $\mathcal{P} = (\mathcal{P}_n)$ for the family of planar graphs. Gavoille et al. [15] gave an $O(\sqrt{n} \log n)$ labeling scheme where $\mathsf{dist}(x, y)$ can be computed from the labels of x, y, and Gawrychowski and Uznański [16] improved this to $O(\sqrt{n})$. These labeling schemes recursively identify size-$O(\sqrt{n})$ sets S and record the distance of each vertex v to each $u \in S$, so the $\sqrt{n}$ factor is unavoidable using this technique. We want to solve k-distance with a cost independent of n, so we need a new method. Our main tool is Schnyder's elegant decomposition of planar graphs into trees:

▶ **Theorem 4.6** (Schnyder [32], see [11]). *Define the dimension* $\dim(G)$ *of a graph* G *as is the minimum* d *such that there exist total orders* $<_1, \ldots, <_d$ *on* $V(G)$ *satisfying:*

(*) For every edge $\{u,v\} \in E$ *and* $w \notin \{u,v\}$ *there exists* $<_i$ *such that* $u, v <_i w$*.*

G *is planar iff* $\dim(G) \le 3$*. If* G *is planar then there exists a partition* T_1, T_2, T_3 *of the edges into directed trees satisfying the following. Let* T_i^{-1} *be edge-induced directed graph on* $V(G)$ *obtained by reversing the direction of each edge in* T_i*. The graphs with edges* $T_i \cup T_{i-1}^{-1} \cup T_{i+1}^{-1}$ *have linear extensions* $<_i$ *such that* $<_1, <_2, <_3$ *satisfy (*).*

Schnyder's Theorem implies that the arboricity of planar graphs is at most 3, so we may use the protocol for low-arboricity graphs (Proposition 4.3) to determine adjacency in $\mathcal{P}$, so we move on to $\mathcal{P}^2$, which may have large arboricity (arboricity is within a constant factor of *degeneracy*):

▶ **Theorem 4.7** ([1]). *There are planar graphs* P *for which the degeneracy of* P^2 *is* $\Theta(\deg P)$*, where* $\deg P$ *is the maximum degree of any vertex in* P*.*

We avoid this blowup in arboricity by treating edges of the form $a \leftarrow b \rightarrow c$ separately (with directions taken from the Schnyder wood). The proof uses the following split operation:

▶ **Definition 4.8.** *Let* $G \in \mathcal{P}$ *and fix a planar map and a Schnyder wood* T_1, T_2, T_3*. Define the graph* $\mathsf{split}(G)$ *by the following procedure (see Figure 1):*

1. *For each vertex* $s \in V(G)$ *add vertices* s, s_1, s_2, s_3 *to* $\mathsf{split}(G)$ *(excluding* s_i *if* s *has no incoming edge in* T_i*). Add edges* (s_i, s) *to* T_i'*;*
2. *For each (directed) edge* $(u,v) \in T_i$ *add the edges* $(u_{i-1}, v_i), (u_{i+1}, v_i)$ *(arithmetic mod 3) to* T_i'*;*
3. *For the unique (directed) edge* $(v,u) \in T_i$ *add the edges* $(v_{i-1}, u), (v_{i+1}, u)$ *to* T_i'*.*

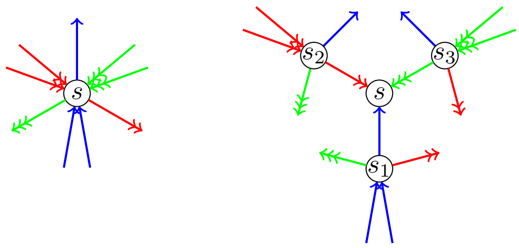

Figure 1 Splitting vertex s, with T_1, T_2, T_3 in blue, red, and green respectively (1,2, and 3 arrowheads).

▶ **Proposition 4.9.** $\mathsf{split}(G)$ *is planar.*

Proof. We prove that splitting any vertex s results in a planar graph. By induction we may then split each vertex in sequence and obtain a planar graph. Let $<_i$ be any total order on $V(G)$ extending $T_i \cup T_{i-1}^{-1} \cup T_{i+1}^{-1}$, which satisfies condition (*) by Schnyder's theorem. Let $<_1', <_2', <_3'$ be the same total orders, extending T_1', T_2', T_3', and augmented to include s_1, s_2, s_3 as follows:

1. For each $u \in V(G)$, $s_i <_j' u$ iff $s <_j u$ and $u <_j'$ iff $u <_j s$;
2. For each i, set $s_i <_i' s <_i' s_{i+1} <_i' s_{i-1}$. This is possible since $\{s_i\}$ do not have a defined ordering in $<_i$ and remain incomparable after the previous step.

Note that for any edge $(u,v) \in T_i'$ we have $u <_i' v$ and $v <_j' u$ for $j \neq i$. It suffices to prove that condition (*) is satisfied by the new orders. Let $\{u,v\} \in E(\mathsf{split}(G))$ and let $w \notin \{u,v\}$. We will show that there exists i such that $u, v <_i' w$.

If $u, v, w \in V(G)$ then we are done since the orders $<'_i$ are the same as $<_i$ on these vertices.

If $u = s_i$ then either $v \in V(G) \setminus s$, in which case $v <_i s$ so $v <'_i u$ and therefore $u <'_j v$ for $j \neq i$, or $v = s$ so $u <'_i v$ and therefore $v <'_j u$ for $j \neq i$. Let $v \neq s$. For any $w \in V(G) \setminus \{v\}$ we have, by (*), either $v, s <_i w$ so $v <'_i u <'_i s <'_i w$, or $v, s <_j w$ so $u <'_j v <'_j w$. If $v = s$ then by construction there exists $(u', u) \in T_i$. By (*), either $u', v <_i w$ so $u <'_i v <'_i w$, or $u', v <_j w$ so $v <'_j u <'_j u' <'_j w$.

The only case remaining is if $w = s_i$ and $u, v \in V(G)$. By construction there exists $(w', w) \in T_i$. Either $u, v <_i w' <'_i w <'_i s$ or by (*) there exists j such that $u, v <_j s$ and since (w, s) is an edge in T'_i, $s <'_j w$ for $j \neq i$. ◀

▶ **Definition 4.10.** *Let $G = (V, E)$ be a planar graph. Fix a planar map and a Schnyder wood T_1, T_2, T_3. For each i, define the graph $G_i = (V, E \setminus T_i)$ as the graph obtained by removing each edge in T_i. Define the* head-to-head closure *of G_i, written $G_i^{\leftarrow\rightarrow}$, as the graph with an edge $\{u, v\}$ iff there exists $w \in V$ such that $u \leftarrow w \rightarrow v$ in G_i. (Observe that the two outgoing edges of w must be in T_{i-1}, T_{i+1}.) Let $G^{\leftarrow\rightarrow}$ be the subgraph of G^2 containing all edges occuring in $G_i^{\leftarrow\rightarrow}$ for each i.*

▶ **Lemma 4.11.** *Let G be a planar graph. For any graph M, if M is a minor of $G_i^{\leftarrow\rightarrow}$ then M is a minor of* $\mathsf{split}(G)$.

Proof. We will prove the following claim.

▷ Claim 4.12. For any set $P = \{P_j\}$ of simple paths $P_j \subseteq V(G_i^{\leftarrow\rightarrow})$, with endpoints $\{(s_j, t_j)\}$ such that no two paths P_j, P_k have the same endpoints and $P_j \cap P_k \subseteq \{s_j, s_k, t_j, t_k\}$, there exists a set of paths $Q = \{Q_j\}$ of paths in $\mathsf{split}(G)$ with the same endpoints such that

$$Q_j \cap Q_k \subseteq \{s_j, s_k, t_j, t_k\} \cup \{(s_j)_{i-1}, (s_k)_{i-1}, (t_j)_{i-1}, (t_k)_{i-1}\} \cup \{(s_j)_{i+1}, (s_k)_{i+1}, (t_j)_{i+1}, (t_k)_{i+1}\},$$

where the vertices s_i, s_{i+1}, s_{i-1} are defined as in the split operation.

Proof of claim. For each path P_j, perform the following. For each edge $\{u, w\}$ in the path P_j, there is some (not necessarily unique) vertex v such that either $(v, u) \in T_{i-1}$ and $(v, w) \in T_{i+1}$, or the same holds with u, w reversed. Add the edges $\{u, u_{i-1}\}, \{u_{i-1}, v_i\}, \{v_i, w_{i+1}\}, \{w_{i+1}, w\}$ to Q_j. If P_j is a singleton $P_j = \{u\}$ so $s_j = t_j$ then add u to Q_j.

Consider two paths Q_j, Q_k constructed this way. $G_i^{\leftarrow\rightarrow}$ has vertex set V and $\mathsf{split}(G)$ has vertex set $V' \supset V$. By construction, $P_j \subseteq Q_j$ and $P_k \subseteq Q_k$ and $(Q_j \cap V) = P_j$. Suppose there exists $z \in Q_j \cap Q_k$ that is not an endpoint, so $z \notin \{s_j, s_k, t_j, t_k\}$. If $z \in V$ then $z \in P_j \cap P_k \subseteq \{s_j, s_k, t_j, t_k\}$, so we only need to worry about $z \in V' \setminus V$.

If $z = v_i$ for some vertex v then there are unique distinct vertices $u_{i-1}, w_{i+1} \in V'$ adjacent to v_i such that $u_{i-1}, w_{i+1} \in Q_j \cap Q_k$. Then $u, w \in Q_j \cap Q_k$ also, so $u, w \in P_j \cap P_k$; but then $u \neq w$ are the start and end points of P_j, P_k, so $P_j = P_k$, a contradiction.

If $z = v_{i-1}$ for some vertex $v \in V$ then $v \in Q_j \cap Q_k$, so by the case above, $v \in \{s_j, s_k, t_j, t_k\}$ and $z \in \{(s_j)_{i-1}, (s_k)_{i-1}, (t_j)_{i-1}, (t_k)_{i-1}\}$. Likewise for $z = v_{i+1}$. ◁

Let M be a minor of $G_i^{\leftarrow\rightarrow}$, so a subdivision of M occurs as a subgraph of $G_i^{\leftarrow\rightarrow}$. Therefore there is a set of paths P in $G_i^{\leftarrow\rightarrow}$ satisfying the conditions of the claim, so that by contracting each path into a single edge, and deleting the rest of the graph, we obtain M. Let $Q = \{Q_j\}$ be the set of paths given by the claim. For endpoints $s_j, t_j \in Q_j$, contract the edges $\{s_j, (s_j)_{i\pm1}\}$ and $\{t_j, (t_j)_{i\pm1}\}$. The result is a contraction of $\mathsf{split}(G)$ and a set of paths Q' that is a subdivision of M, so M is a minor of $\mathsf{split}(G)$, which proves the lemma. ◀

▶ **Corollary 4.13.** *$G_i^{\leftarrow\rightarrow}$ is planar and $G^{\leftarrow\rightarrow}$ has arboricity at most 9.*

Proof. A graph is planar iff it does not contain K_5 or $K_{3,3}$ as a minor (Kuratowski's Theorem). If $G_i^{\leftarrow\rightarrow}$ is not planar then it contains K_5 or $K_{3,3}$ as a minor, so by the above lemma, $\mathsf{split}(G)$ contains K_5 or $K_{3,3}$ as a minor, so $\mathsf{split}(G)$ is not planar, a contradiction. Since planar graphs have arboricity at most 3, the edge union $G^{\leftarrow\rightarrow}$ of 3 planar graphs has arboricity at most 9. ◀

By separating the $\leftarrow\rightarrow$ edges from the remaining edges of $\mathcal{P}^2$, we obtain a constant-cost universal SMP protocol for $\mathcal{P}^2$, and then by applying Theorem 1.1 we obtain Theorem 1.5.

▶ **Lemma 4.14.** *For all $\epsilon > 0, R_\epsilon^{\mathsf{univ}}(\mathcal{P}^2) = O\left(\log \frac{1}{\epsilon}\right)$.*

Proof. For a planar graph $G = (V, E)$ with a fixed planar map and a Schnyder wood T_1, T_2, T_3, define the graph $G_i = (V, E \setminus T_i)$ as the graph obtained by removing the edges in tree T_i.

On planar graph $G \in \mathcal{P}_n$ and vertices x, y, Alice and Bob perform the following:

1. For each i define x_i, y_i to be the parents of x, y in T_i. Run the protocol for adjacency with error $\epsilon/7$ on (x, y_i) and (x_i, y) for each i.
2. Run the protocol for low-arboricity graphs on $G^{\leftarrow\rightarrow}$ with error $\epsilon/7$.
3. Accept iff one of the above sub-protocols accepts.

By Corollary 4.13, $G^{\leftarrow\rightarrow}$ has arboricity at most 9, we may apply the protocol for low-arboricity graphs in step 2. If $\mathsf{dist}(x, y) > 2$ then the protocol will correctly reject with probability at least $1 - \epsilon$ since there are 7 applications of $\epsilon/7$-error protocols. It remains to show that if $\mathsf{dist}(x, y) = 2$ then the algorithm will accept.

Suppose x, y are of distance 2. Then the paths between them are of the following forms (with edge directions taken from the Schnyder wood).

1. $x \to v \to y$ or $x \to v \leftarrow y$. This is covered by step 1.
2. $x \leftarrow v \to y$. This is covered by step 2. ◀

Since planar graphs are an upwards family (just insert a new vertex), we obtain a constant-size probabilistic universal graph for $\mathcal{P}^2$.

▶ **Corollary 4.15.** *For any $\epsilon > 0$, there is a graph U of size $O(\log(1/\epsilon))$ such that for every $G \in \mathcal{P}^2$, $G \sqsubset_\epsilon U$.*

5 Discussion and Open Problems

Error-tolerance. In the introduction we mentioned that the universal SMP model allows us to study error-tolerance in the SMP model. This could be done as follows: suppose the referee knows a reference graph G and the players are guaranteed to see a graph that is "close" to G by some metric. How much does this change the complexity of the problem, compared to computing G? One common distance metric in, say, the property testing literature, is to count the number of edges that one must add or delete. That is, for two graphs G, H on vertex set $[n]$, write $\mathsf{dist}(G, H) = \frac{1}{n^2} \sum_{i,j \in [n]} \mathbb{1}\left[G(i, j) \neq H(i, j)\right]$. The distance is usually thought of as a constant. We can easily give a strong negative result for this situation:

▶ **Proposition 5.1.** *Let $\mathcal{F}$ be any family of graphs and $\mathcal{F}_\delta$ the family of graphs G such that $\min_{F \in \mathcal{F}} \mathsf{dist}(G, F) \leq \delta$. Then*

$$R^{\mathsf{univ}}(\mathcal{F}_\delta) = \Omega(\sqrt{\delta} n) .$$

Proof. Let G be any graph on $\sqrt{\delta}n$ vertices and let $F \in \mathcal{F}$. Choose any set $S \subseteq V(F)$ with $|S| = |G|$. Construct F' by replacing the subgraph induced by S with the graph G. Then $\mathsf{dist}(F, F') \leq \frac{|G|^2}{n^2} = \delta$ so $F' \in \mathcal{F}_\delta$. Then the conclusion follows from Theorem 1.6. ◀

This suggests that this is not the correct way to model contextual uncertainty in the SMP model, but universal SMP gives a framework for studying many other error tolerance settings. For example, we could suppose that the referee knows a reference planar graph G, and the players are guaranteed to see a graph G' that is close to G and also planar; this would not increase the cost of the protocol due to our results on planar graphs.

Implicit graph conjecture. A major open problem in graph labeling is the *implicit graph conjecture* of Kannan, Naor, and Rudich [23], which asks if every *hereditary* graph family $\mathcal{F}$ (where for each $G \in \mathcal{F}$, every induced subgraph of G is also in $\mathcal{F}$) containing at most $2^{O(n \log n)}$ graphs of size n has an $O(\log n)$ adjacency labeling scheme. Not much progress has been made on this conjecture (see e.g. [33, 10]). We ask a weakened version of this conjecture:

▶ **Question 5.2.** *For every hereditary family $\mathcal{F} = (\mathcal{F}_n)$ such that $|\mathcal{F}_n| \leq 2^{O(n \log n)}$, is $R^{\mathsf{univ}}(\mathcal{F}) = O(\log n)$?*

Good candidates for disproving the implicit graph conjecture are geometric intersection graphs, like disk graphs (intersections of disks in $\mathbb{R}^2$) or k-dot product graphs (graphs whose vertices are vectors in $\mathbb{R}^k$, with an edge if the inner product is at least 1) [33]. These are good candidates because encoding the coordinates of the vertices as integers will fail [22]. Randomized communication techniques may be able to make progress.

Modular lattices. We have shown that there is no constant-cost universal protocol for distance 2 in modular lattices but, like low-arboricity graphs, adjacency (and therefore $O(\log n)$-implicit encodings) may still be possible.

Planar graphs. Our protocol for computing distance 2 on planar graphs did not generalize in a straightforward fashion to distance 3. Nevertheless, we expect that there is a method for computing k-distance on planar graphs with complexity dependent only on k; given that a Schnyder wood partitions each edge into 3 groups, we expect that $\widetilde{O}(3^k)$ should be possible, and maybe only poly(k), considering that there is a $O(\sqrt{n})$ distance-labeling scheme.

Sharing randomness with the referee. Finally, it seems to be unknown what the relationship is between SMP protocols where the referee shares the randomness, and protocols where the referee is deterministic, even though both models are used extensively in the literature. Our Proposition 1.8 relates these two models via universal SMP but does not yet give a general upper bound on the universal cost in terms of the weakly-universal cost.

▶ **Question 5.3.** *What general upper bounds can we get on universal SMP in terms of weakly-universal SMP?*

References

1 Geir Agnarsson and Magnús M Halldórsson. Coloring powers of planar graphs. *SIAM Journal on Discrete Mathematics*, 16(4):651–662, 2003.

2 Stephen Alstrup, Philip Bille, and Theis Rauhe. Labeling schemes for small distances in trees. *SIAM Journal on Discrete Mathematics*, 19(2):448–462, 2005.

3 Stephen Alstrup, Søren Dahlgaard, and Mathias Bæk Tejs Knudsen. Optimal induced universal graphs and adjacency labeling for trees. *Journal of the ACM (JACM)*, 64(4):27, 2017.

4 Stephen Alstrup, Søren Dahlgaard, Mathias Bæk Tejs Knudsen, and Ely Porat. Sublinear distance labeling. In *24th Annual European Symposium on Algorithms (ESA 2016)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016.

5 Stephen Alstrup, Inge Li Gørtz, Esben Bistrup Halvorsen, and Ely Porat. Distance labeling schemes for trees. In *43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016)*, 2016.

6 Stephen Alstrup, Haim Kaplan, Mikkel Thorup, and Uri Zwick. Adjacency labeling schemes and induced-universal graphs. *SIAM Journal on Discrete Mathematics*, 33(1):116–137, 2019.

7 Tiziana Calamoneri. The $L(h, k)$-Labelling Problem: An Updated Survey and Annotated Bibliography. *The Computer Journal*, 54(8):1344–1371, 2011.

8 Clément L Canonne, Venkatesan Guruswami, Raghu Meka, and Madhu Sudan. Communication with imperfectly shared randomness. *IEEE Transactions on Information Theory*, 63(10):6799–6818, 2017.

9 Nathalie Caspard, Bruno Leclerc, and Bernard Monjardet. *Finite Ordered Sets: Concepts, Results and Uses*. Cambridge University Press, 2012.

10 Maurice Chandoo. On the implicit graph conjecture. In *41st International Symposium on Mathematical Foundations of Computer Science (MFCS 2016)*, volume 58, page 23. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2016.

11 Stefan Felsner. *Geometric graphs and arrangements: some chapters from combinatorial geometry*. Springer, 2012.

12 Pierre Fraigniaud and Amos Korman. On randomized representations of graphs using short labels. In *Proceedings of the 21st Annual Symposium on Parallelism in Algorithms and Architectures*, pages 131–137. ACM, 2009.

13 Pierre Fraigniaud and Amos Korman. An Optimal Ancestry Labeling Scheme with Applications to XML Trees and Universal Posets. *Journal of the ACM*, 63(1):6, 2016.

14 Cyril Gavoille and Arnaud Labourel. Shorter implicit representation for planar graphs and bounded treewidth graphs. In *European Symposium on Algorithms*, pages 582–593. Springer, 2007.

15 Cyril Gavoille, David Peleg, Stéphane Pérennes, and Ran Raz. Distance labeling in graphs. *Journal of algorithms*, 53(1):85–112, 2004.

16 Paweł Gawrychowski and Przemysław Uznański. A note on distance labeling in planar graphs, 2016. `arXiv:1611.06529`.

17 Badih Ghazi, Ilan Komargodski, Pravesh Kothari, and Madhu Sudan. Communication with Contextual Uncertainty. *Computational Complexity*, 27(3):463–509, 2018.

18 Badih Ghazi and Madhu Sudan. The power of shared randomness in uncertain communication. In *44th International Colloquium on Automata, Languages, and Programming (ICALP 2017)*, pages 49:1–49:14. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2017.

19 Oded Goldreich, Brendan Juba, and Madhu Sudan. A theory of goal-oriented communication. *Journal of the ACM*, 59(2):8, 2012.

20 Elad Haramaty and Madhu Sudan. Deterministic compression with uncertain priors. *Algorithmica*, 76(3):630–653, 2016.

21 Wei Huang, Yaoyun Shi, Shengyu Zhang, and Yufan Zhu. The communication complexity of the Hamming distance problem. *Information Processing Letters*, 99(4):149–153, 2006.

22 Ross J Kang and Tobias Müller. Sphere and dot product representations of graphs. *Discrete & Computational Geometry*, 47(3):548–568, 2012.

23 Sempath Kannan, Moni Naor, and Steven Rudich. Implicit Representations of Graphs. *SIAM Journal on Discrete Mathematics*, 5(4):596–603, 1992.

24 Haim Kaplan and Tova Milo. Short and Simple Labels for Small Distances and Other Functions. In *Workshop on Algorithms and Data Structures*, pages 246–257. Springer, 2001.

25 Peter Bro Miltersen, Noam Nisan, Schmuel Safra, and Avi Wigderson. On data structures and asymmetric communicaton complexity. *Journal of Computer and System Sciences*, 57(1):37–49, 1998.

26 J Ian Munro and Corwin Sinnamon. Time and space efficient representations of distributive lattices. In *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 550–567. Society for Industrial and Applied Mathematics, 2018.

27 Arvind Narayanan, Narendran Thiagarajan, Mugdha Lakhani, Michael Hamburg, and Dan Boneh. Location privacy via private proximity testing. In *NDSS*, volume 1, 2011.

28 Ilan Newman. Private vs. common random bits in communication complexity. *Information Processing Letters*, 39(2):67–71, 1991.

29 David Peleg. Informative Labeling Schemes for Graphs. *Theoretical Computer Science*, 340(3):577–593, 2005.

30 Richard Rado. Universal graphs and universal functions. *Acta Arithmetica*, 4(9):331–340, 1964.

31 Mert Sağlam. Near log-convexity of measured heat in (discrete) time and consequences. In *59th Annual Symposium on Foundations of Computer Science (FOCS 2018)*, pages 967–978. IEEE, 2018.

32 Walter Schnyder. Planar graphs and poset dimension. *Order*, 5(4):323–343, 1989.

33 Jeremy P Spinrad. *Efficient Graph Representations*. American Mathematical Society, 2003.

34 Andrew C.C. Yao. Some complexity questions related to distributive computing. In *Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing*, pages 209–213. ACM, 1979.

A Appendix

Proof of Proposition 2.5.

1. If $A \sqsubset B$ and $B \sqsubset C$ with ϕ, ψ being the respective embeddings then for all $u, v \in V(A)$ we have
$$C(\psi\phi(u), \psi\phi(v)) = B(\phi(u), \phi(v)) = A(u, v)\,.$$
2. In the "only if" direction, it suffices to choose $G^{\equiv}$. In the other direction, if $\phi : V(G) \to V(H)$ is an embedding and $\phi(u) = \phi(v)$ then for all $w \in V(G), G(u, w) = H(\phi(u), \phi(w)) = H(\phi(v), \phi(w)) = G(v, w)$ so $u \equiv v$.
3. Let g map a vertex of G to its equivalence class and let $u, v \in V(G)$. If $G(u, v) = 1$ then $G^{\equiv}(g(u), g(v)) = 1$ by definition. If $G^{\equiv}(g(u), g(v)) = 1$ then there exists $u' \in g(u), v' \in g(v)$ such that $G(u', v') = 1$, so $G(u, v) = G(u', v) = G(u', v') = 1$.
4. Let g map vertices in $V(G)$ to their equivalence class and let $g(u), g(v) \in V(G^{\equiv})$. If $g(u) \equiv g(v)$ then for any $w, G(u, w) = G^{\equiv}(g(u), g(w)) = G^{\equiv}(g(v), g(w)) = G(v, w)$ so $u \equiv v$ and therefore $g(u) = g(v)$. Therefore the map $g(u) \mapsto \{g(u)\}$ is an isomorphism $G^{\equiv} \to (G^{\equiv})^{\equiv}$.
5. If $G \sqsubset H$ then by transitivity, $G^{\equiv} \sqsubset G \sqsubset H \sqsubset H^{\equiv}$. Likewise, if $G^{\equiv} \sqsubset H^{\equiv}$ then $G \sqsubset G^{\equiv} \sqsubset H^{\equiv} \sqsubset H$.
6. If $G^{\equiv}$ is an induced subgraph of $H^{\equiv}$ then clearly there is an embedding. On the other hand, let $g(u), g(v) \in V(G^{\equiv})$ be the equivalence classes of $u, v \in V(G)$ and suppose there is an embedding $\phi : G^{\equiv} \to H^{\equiv}$. If $\phi(g(u)) = \phi(g(v))$ then $g(u) \equiv g(v)$ so $g(u) = g(v)$ since $(G^{\equiv})^{\equiv} \simeq G^{\equiv}$. Therefore $G^{\equiv}$ is an induced subgraph of $H^{\equiv}$. ◀