The Complexity of Counting Homomorphisms to Cactus Graphs Modulo 2

ANDREAS GÖBEL, LESLIE ANN GOLDBERG, and DAVID RICHERBY, University of Oxford

A homomorphism from a graph G to a graph H is a function from $V(G)$ to $V(H)$ that preserves edges. Many combinatorial structures that arise in mathematics and in computer science can be represented naturally as graph homomorphisms and as weighted sums of graph homomorphisms. In this article, we study the complexity of counting homomorphisms modulo 2. The complexity of modular counting was introduced by Papadimitriou and Zachos and it has been pioneered by Valiant who famously introduced a problem for which counting modulo 7 is easy but counting modulo 2 is intractable. Modular counting provides a rich setting in which to study the structure of homomorphism problems. In this case, the structure of the graph H has a big influence on the complexity of the problem. Thus, our approach is graph-theoretic. We give a complete solution for the class of cactus graphs, which are connected graphs in which every edge belongs to at most one cycle. Cactus graphs arise in many applications such as the modelling of wireless sensor networks and the comparison of genomes. We show that, for some cactus graphs H, counting homomorphisms to H modulo 2 can be done in polynomial time. For every other fixed cactus graph H, the problem is complete in the complexity class $\oplus$P, which is a wide complexity class to which every problem in the polynomial hierarchy can be reduced (using randomised reductions). Determining which H lead to tractable problems can be done in polynomial time. Our result builds upon the work of Faben and Jerrum, who gave a dichotomy for the case in which H is a tree.

Categories and Subject Descriptors: F.2.2 [**Analysis of Algorithms and Problem Complexity**]: Nonnumerical Algorithms and Problems—*Computations on discrete structures*; G.2.1 [**Discrete Mathematics**]: Combinatorics—*Counting problems*; G.2.2 [**Discrete Mathematics**]: Graph Theory—*Graph algorithms*

General Terms: Algorithms, Theory

Additional Key Words and Phrases: Graph homomorphism, cactus graph, counting modulo 2, parity complexity dichotomy

ACM Reference Format:
Göbel, A., Goldberg, L. A., and Richerby, D. 2014. The complexity of counting homomorphisms to cactus graphs modulo 2. *ACM Trans. Comput. Theory* 6, 4, Article 17 (August 2014), 29 pages.
DOI:http://dx.doi.org/10.1145/2635825

1. INTRODUCTION

A homomorphism from a graph G to a graph H is a function from $V(G)$ to $V(H)$ that preserves edges. That is, the function maps every edge of G to an edge of H. Many combinatorial structures that arise in mathematics and in computer science can be

Authors' address: A. Göbel, L. A. Goldberg, and D. Richerby (corresponding author), Department of Computer Science, University of Oxford, Wolfson Building, Parks Road, Oxford OX1 3QD, UK; email: david.richerby@cs.ox.ac.uk.
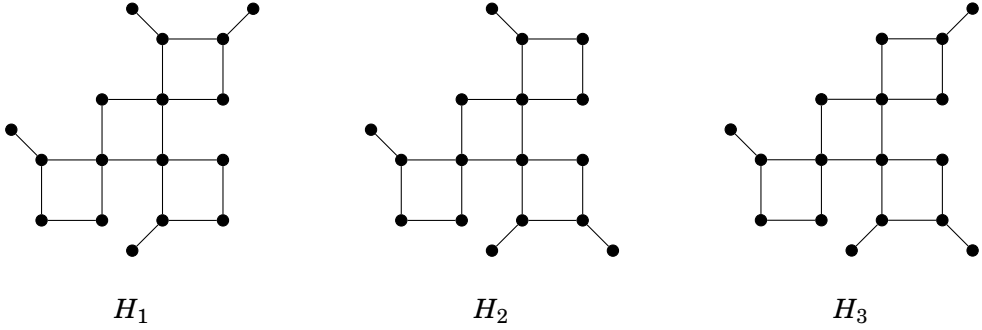
Fig. 1. $\oplus$HOMSTOH_1 and $\oplus$HOMSTOH_3 are $\oplus$P-complete, but $\oplus$HOMSTOH_2 is in FP.

represented naturally as graph homomorphisms. For example, the proper q-colourings of a graph G correspond to the homomorphisms from G to the q-clique. The independent sets of G correspond to the homomorphisms from G, the 2-vertex connected graph with one self-loop (vertices of G which are mapped to the self-loop are out of the corresponding independent set; vertices which are mapped to the other vertex are in it). Partition functions in statistical physics such as the Ising model, the Potts model, and the hard-core model arise naturally as weighted sums of homomorphisms. See, for example, Bulatov and Grohe [2005] and Goldberg et al. [2010].

In this paper, we study the complexity of counting homomorphisms modulo 2. For graphs G and H, let $\mathrm{Hom}(G, H)$ denote the set of homomorphisms from G to H. For each fixed H, we study the computational problem $\oplus$HOMSTOH, which is the problem of computing $\big|\mathrm{Hom}(G, H)\big|$ mod 2, given an input graph G.

The structure of the graph H has a big influence on the complexity of $\oplus$HOMSTOH. For example, consider the graphs H_1, H_2, and H_3 depicted in Figure 1. Our result implies that $\oplus$HOMSTOH_1 is complete for the class $\oplus$P (with respect to polynomial-time Turing reductions). The graph H_2 is constructed by moving the top right bristle from H_1 down to the bottom right. Under the standard assumption that $\oplus$P $\neq$ FP (which will be explained in the following), moving this bristle makes the problem easier—our result implies that $\oplus$HOMSTOH_2 is solvable in polynomial time. H_3 is constructed by moving the top bristle from left to right in H_2. This again makes the problem more difficult—$\oplus$HOMSTOH_3 is $\oplus$P-compete. The goal of this research is to study the complexity of $\oplus$HOMSTOH for every fixed graph H and to determine for which graphs H the problem is in FP, for which graphs it is $\oplus$P-complete, and whether there are any graphs H for which the problem has intermediate complexity. In this article, we give a complete solution to this problem for the class of *cactus graphs*.

A cactus graph is a connected graph in which every edge belongs to at most one cycle. Cactus graphs were first defined by Harary and Uhlenbeck [1953] who attributed them to the physicist Husimi and therefore called them *Husimi Trees*. Cactus graphs arise, for example, in the modelling of wireless sensor networks [Ben-Moshe et al. 2012] and in the comparison of genomes [Paten et al. 2011]. Some NP-hard graph problems can be solved in polynomial time on cactus graphs [Ben-Moshe et al. 2007].

1.1. The Complexity of Mmodular Counting

The complexity of modular counting is an interesting topic with some surprising results and we only mention a few highlights here. First, it is important to understand that $\oplus$P (which was first studied by Papadimitriou and Zachos [1982] and Goldschlager and Parberry [1986]) is a very large complexity class. We will think of this class from

the point of view of function computation, so $\oplus$P consists of all problems of the form "compute $f(x)$ mod 2," where computing $f(x)$ is a problem in #P. $\oplus$P is sufficiently powerful that there is randomised polynomial-time reduction [Toda 1991] from every problem in the polynomial hierarchy to some problem in $\oplus$P. Thus, subject to the natural hypothesis that problems in the higher levels of the polynomial hierarchy are not solvable in randomised polynomial time, we conclude that $\oplus$P-complete problems are much harder than problems in FP, which is the class of of function-computation problems that are solvable in polynomial time.

The complexity of counting modulo 2 is different from the complexity of decision problems or counting problems. First, consider an NP-complete decision problem. The mod-2 counting version of this problem can be intractable, as you might expect (for example, counting vertex covers or independent sets modulo 2 is $\oplus$P-complete [Valiant 2006]) but it can also be tractable. As an example, consider the problem of counting proper 3-colourings of a graph modulo 2. There are an even number of 3-colourings that use exactly 3 colours, since there are 6 permutations of these colours. There are also an even number of 3-colourings that use exactly 2 colours, since the colours can be swapped. But it is easy to count 1-colourings. Thus, it is easy to count all proper colourings modulo 2. Next, consider a #P-complete counting problem. The mod-2 counting version of this problem can be intractable or tractable, as the previous examples illustrate. As another example where the mod-2 counting version is tractable, consider the problem of computing the permanent of a matrix modulo 2. Since $-1 \equiv 1 \bmod 2$, the permanent is equal to the determinant modulo 2, so it can readily be computed in polynomial time.

Another interesting aspect of modular counting is the fact that the value of the modulus can affect the tractability of the problem. As an example, consider the well-known work of Valiant [2006], who identified a certain satisfiability problem where satisfying assignments are easy to compute modulo 7 and difficult to compute modulo 2.

1.2. Dichotomies for Graph Homomorphism Problems

Determining the border between tractability and intractability for large classes of modular counting problems is an important step towards understanding the structure of the problems themselves. In this article we work within the context of graph homomorphism problems because graph homomorphisms are general enough to capture a wide variety of combinatorial problems, yet they exhibit sufficient structure that dichotomies exist. Hell and Nešetřil [1990] pioneered this direction by completely classifying undirected graphs according to the difficulty of the graph homomorphism decision problem. They showed if a fixed graph H has a self-loop, or is bipartite, then the problem of determining whether an input graph has a homomorphism to H is in P. For every other fixed graph H, the decision problem is NP-complete.

Over recent years, dichotomy theorems have also been established for the problem of counting graph homomorphisms and computing weighted sums of homomorphisms. Dyer and Greenhill [2000] showed that the problem of counting homomorphisms to H is solvable in polynomial time if every component of H is an isolated vertex, a complete graph with all self-loops present, or a complete bipartite graph with no self-loops. For every other H, it is #P-complete. In particular, there are no graphs H for which the problem has intermediate complexity. This dichotomy was extended to the problem of computing weighted sums of homomorphisms to H. A dichotomy was given by Bulatov and Grohe [2005] for the case where the weights are positive, by Goldberg et al. [2010] for the case where the weights are real, and by Cai et al. [2010] for the case where the weights are complex.

1.3. The Complexity of Counting Graph Homomorphisms Modulo 2

The first results on the complexity of counting graph homomorphisms modulo 2 were obtained by Faben [2012] and Faben and Jerrum [2013] who made some important structural discoveries which we also use.

An *involution* of a graph is an automorphism of order 2. If σ is an automorphism of a graph H then H^σ denotes the subgraph of H induced by the fixed points of σ.

LEMMA 1.1. *([Faben and Jerrum 2013, Lemma 3.3]) If H is a graph and σ is an involution of H then, for any graph G, $\left|\mathrm{Hom}(G, H)\right| \equiv \left|\mathrm{Hom}(G, H^\sigma)\right|$ (mod 2).*

This lemma is useful because it enables us to reduce the problem of counting homomorphisms to H modulo 2 to the problem of counting homomorphisms to H^σ modulo 2. This leads naturally to the idea of reduction by involutions. Let $\to$ be the relation on graphs where $H \to H'$ if and only if there is an involution σ of H such that $H' = H^\sigma$. Let $\to^*$ be the transitive closure of $\to$. Faben and Jerrum showed that repeatedly applying $\to$ to a graph H reduces H to a unique involution-free graph, up to isomorphism.

LEMMA 1.2. *([Faben and Jerrum 2013, Theorem 3.7]) Let H be any graph. If $H \to^* H'$ and $H \to^* H''$ and H' and H'' are involution-free then H' is isomorphic to H''.*

Finally, they showed that, to classify the complexity of counting homomorphisms to H, one only needs to study the complexity of counting homomorphisms to its connected components.

LEMMA 1.3. *([Faben and Jerrum 2013, Theorem 6.1]) Let H be an involution-free graph. If H has a connected component H_1 such that $\oplus$HOMSTOH_1 is $\oplus$P-hard with respect to polynomial-time Turing reductions, then $\oplus$HOMSTOH is also $\oplus$P-hard.*

To complement Lemma 1.3, it is easy to see that if $\oplus$HOMSTOH_i is solvable in polynomial time for every connected component H_i of H, then $\oplus$HOMSTOH is also solvable in polynomial time. Faben and Jerrum used the structural results to give a dichotomy for the complexity of $\oplus$HOMSTOH when H is a tree. Define the *involution-free reduction H'* of a graph H to be the lexicographically-minimal involution-free graph such that $H \to^* H'$. We can then state their result as follows.

THEOREM 1.4. *([Faben and Jerrum 2013, Theorem 3.8]) If H is a tree then $\oplus$HOMSTOH is $\oplus$P-complete if the involution-free reduction of H has more than one vertex. Otherwise, it is in FP.*

Every involution-free tree is asymmetric, which means that it has no nontrivial automorphisms. Thus, the technical work of proving Theorem 1.4 is to consider every asymmetric tree H with more than one vertex and show that $\oplus$HOMSTOH is $\oplus$P-hard. Fortunately, this can be done without too much technical complexity.

Developing a dichotomy to cover all graphs seems to be much more difficult and even the dichotomy for cactus graphs requires a substantial technical effort, as we will see. Nevertheless, there is a general conjecture as to what the outcome would be.

CONJECTURE 1.5 (FABEN AND JERRUM). *Let H be a (not necessarily simple) graph. $\oplus$HOMSTOH is in FP if the involution-free reduction of H is the empty graph, a singleton vertex (with or without a self-loop), or a graph with two isolated vertices, exactly one of which has a self-loop. Otherwise, it is $\oplus$P-complete.*

1.4. Our Result

Recall that a cactus graph is a connected, simple graph in which every edge belongs to at most one cycle. Our main result gives a proof of Faben and Jerrum's conjecture for cactus graphs.
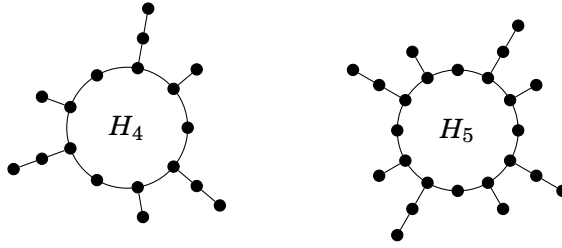
Fig. 2.   ⊕HOMSTOH_4 is ⊕P-complete but ⊕HOMSTOH_5 is in FP.

THEOREM 1.6. *Let H be a simple graph in which every edge belongs to at most one cycle. If the involution-free reduction of H has at most one vertex, then ⊕HOMSTOH is solvable in polynomial time. Otherwise, ⊕HOMSTOH is complete for ⊕P with respect to polynomial-time Turing reductions.*

To prove Theorem 1.6 we have to investigate all involution-free cactus graphs, and not just those that happen to be asymmetric. The reason for this is that, unlike the situation for trees, there are involution-free cactus graphs that have nontrivial automorphisms. An example is the graph H_4 in Figure 2. This graph has an automorphism of order 3 which rotates the cycle. It has no automorphism of order 2. Incidentally, it is easy to see that the graph H_5 in the figure has an involution that moves all vertices. Thus, ⊕HOMSTOH_5 is in FP. Our result implies that ⊕HOMSTOH_4 is ⊕P-complete.

In order to prove the hardness result in Theorem 1.6, we introduce three graph-theoretic notions: hardness gadgets, partial hardness gadgets, and mosaics. Hardness gadgets and partial hardness gadgets are, as the name suggests, structures for proving ⊕P-hardness. Mosaics are graphs built on unions of 4-cycles. They are what is left in inductive cases where hardness gadgets don't exist and we use them inductively to prove overall hardness. Our approach is therefore recursive: we show how to decompose involution-free cactus graphs at cut vertices in such a way that every component contains at least one of these three induced structures. We then show how to combine these structures to obtain hardness gadgets in the original graph. If an asymmetric graph H contains a hardness gadget, then it is relatively easy to show that ⊕HOMSTOH is ⊕P-compete—the proof is by reduction from the problem of counting weighted independent sets modulo 2, generalising the argument for trees. We will discuss the situation in which H is not asymmetric, presently.

Even when H is asymmetric, the most difficult part of the argument is showing that every nontrivial involution-free cactus graph does actually contain a hardness gadget. The presence of cycles in the graph greatly complicates the structure of the argument, hence the need to define hardness gadgets, partial hardness gadgets, and mosaics and to decompose cactus graphs into components with these three different structures, which can then be combined to form hardness gadgets.

When the graph has nontrivial automorphisms, there is a further complication. Suppose that G and H are graphs and that p is a function from $V(G)$ to $2^{V(H)}$. A homomorphism f from G to H is said to satisfy the *pinning function p* if, for every $v \in V(G)$, we have $f(v) \in p(v)$. Now suppose that H is an involution-free graph containing a hardness gadget. The high-level strategy for proving that ⊕HOMSTOH is ⊕P-hard is to first reduce the problem of counting weighted independent sets modulo 2 to the problem of counting pinned homomorphisms from G to H (modulo 2) and then to reduce the latter problem to ⊕HOMSTOH. This pinning approach has been used successfully in dichotomy theorems in related domains [Bulatov and Grohe 2005; Creignou and Hermann 1996; Dyer et al. 2009]. When H is asymmetric, the application of pinning

works smoothly. Building on work of Lovász [1967], Faben and Jerrum reduced the pinned problem to the unpinned one for the case in which the pinning function pins some vertex to an orbit in the automorphism group of H. When H is asymmetric (as it is when H is a tree), the orbit is just a single vertex, and this is just what is required. If H is not asymmetric, then we do not know how to pin a vertex of G to a particular vertex in H. To get around this, we augment G with a copy of H and we pin every vertex in the copy to its own orbit in the automorphism group of H. We show that every homomorphism from an involution-free cactus graph to itself that respects the orbits of all of its vertices is in fact an automorphism of H, and this enables us to solve the problem.

Theorem 1.6 gives a dichotomy for cactus graphs. If the involution-free reduction of H has at most one vertex then ⊕HOMSTOH is in FP. Otherwise, it is ⊕P-complete. Furthermore, the meta-problem of determining which is the case, given input H, is computationally easy. Finding an involution of H reduces in polynomial time to computing the size of H's automorphism group modulo 2. The latter problem is in FP for cactus graphs because, for example, cactus graphs are planar and have tree-width at most 2.

All of the graph-theoretic work in this article depends heavily on the structure of cactus graphs. For example, the construction of hardness gadgets relies on the fact that removing the edges of a cycle splits the vertices of that cycle into different components. New ideas would be needed to generalise our result to a wider class of graphs.

1.5. Related Work

Modular counting has also been considered in the context of Boolean constraint satisfaction problems (CSPs). Graph homomorphism problems are CSPs but they are not known to be representable as Boolean CSPs. The known results are as follows. Faben [2008, 2012] provided a modular counting dichotomy for unweighted Boolean CSPs. This was extended by Guo et al. [2011] to the weighted case. Guo et al. [2013] also provided a dichotomy for the solution of Boolean Holant problems modulo 2.

2. PRELIMINARIES

Our analysis is based primarily on decomposing graphs, particularly by splitting them at cut vertices, as follows.

Definition 2.1. Given a graph H with a cut vertex v, let $H'_1, \ldots, H'_\kappa$ be the connected components of $H - \{v\}$. The *split* of H at v is the set of graphs $\{H_1, \ldots, H_\kappa\}$, where $H_j = H[V(H'_j) \cup \{v\}]$.

Our proofs of ⊕P-completeness are based on a weighted generalisation of the independent set problem.

Definition 2.2. Let $\mathcal{I}(G)$ denote the set of independent sets of a graph G. The *Parity Generalised Independent Set* problem ⊕IS(λ, μ) is defined as follows, where the parameters λ and μ are natural numbers.

Name: ⊕IS(λ, μ).
Input: A graph G.
Output: $Z_{\lambda,\mu}(G) = \displaystyle\sum_{J \in \mathcal{I}(G)} \lambda^{|J|} \mu^{|V(G) \setminus J|} \pmod 2$.

The following observation follows from the fact that counting independent sets modulo 2 is ⊕P-complete [Valiant 2006].

Observation 2.3. If λ or μ is even, then $\oplus\mathrm{IS}(\lambda, \mu)$ is in FP. Otherwise, for every graph, $Z_{\lambda,\mu}(G) \equiv |\mathcal{I}(G)| \pmod 2$, so $\oplus\mathrm{IS}(\lambda, \mu)$ is $\oplus$P-complete.

We use the following notation. $[n]$ denotes the set $\{1, \ldots, n\}$. Given two graphs G and H (not necessarily vertex-disjoint), let $G \cup H$ denote the graph $(V(G) \cup V(H), E(G) \cup E(H))$. If E is a set of edges, let $V(E)$ denote the set of endpoints of edges in E and let $G \cup E$ denote the graph $G \cup (V(E), E)$. Given sets $V' \subseteq V(G)$ and $E' \subseteq E(G)$, let $G - V' = G[V(G) \setminus V']$ and let $G - E' = (V(G), E(G) \setminus E')$. We use the phrase "$j$-walk" in a graph to refer to a walk of length j.

In drawings of graphs, a wavy line between two vertices indicates an omitted portion of the graph whose structure is unimportant, except that it contains a unique shortest path between the endpoints of the wavy line.

Graphs are simple: they do not have multiple edges or self-loops. We use $d_H(u, v)$ to denote the length of a shortest path from u to v in H. If $S \subseteq V(H)$, then $d_H(u, S)$ denotes $\min\{d_H(u, v) \mid v \in S\}$. We use $\Gamma_H(v)$ to denote the set of neighbours of vertex v in H and $\deg_H(v)$ to denote the degree of v in H. We normally view a path P as a graph with vertex set $V(P)$ and edge set $E(P)$. However, where convenient, we specify P by simply listing the vertices of the path, in order. As such, if $P = x_1 \ldots x_\ell$ and $P' = y_1 \ldots y_{\ell'}$, we write Pz for the path $P \cup \{(x_\ell, z)\}$, PP' for the path $P \cup \{(x_\ell, y_1)\} \cup P'$ and so on. We also use $\ell(P)$ to denote $|E(P)|$, the length of the path P. Similarly, we view a cycle C as a graph, but we sometimes specify C by listing its vertices in order. The length of a cycle is $\ell(C) = |E(C)|$.

For $v_1, \ldots, v_r \in V(H)$, we use the tuple $(H, v_1, \ldots, v_r)$ to denote the graph H together with the ordered list of distinguished vertices. A graph with a single distinguished vertex is often called a *rooted graph*, where the distinguished vertex is the *root*. $(H, v_1, \ldots, v_r)$ is said to be *involution-free* if H has no involution that fixes each of the distinguished vertices. We use $\mathrm{Aut}(H)$ to denote the automorphism group of H and, for $v \in V(H)$, we use $\mathrm{Orb}_H(v)$ to denote the set of vertices of H in the orbit of v under the action of $\mathrm{Aut}(H)$.

3. PINNING

As we discussed in the introduction, pinning is a useful technique for obtaining hardness results related to graph homomorphisms and constraint satisfaction problems. Where it can be achieved, pinning allows a reduction from the list version of the problem, which considers homomorphisms from G to H in which the images of the vertices of G are constrained by lists, to the ordinary version of the problem. The list version is referred to as the "conservative case" in the constraint satisfaction community.

As in the introduction, let p be a function from $V(G)$ to $2^{V(H)}$. A homomorphism $f \in \mathrm{Hom}(G, H)$ satisfies the pinning function p if, for every $v \in V(G)$, $f(v) \in p(v)$. Let $\mathrm{HomPin}(G, H, p)$ be the set of homomorphisms from G to H that satisfy the pinning function p. It will be useful to consider the following computational problem, which is parameterised by a graph H.

Name: $\oplus$PINNEDHOMSTOH.
Input: A graph G and a pinning function $p \colon V(G) \to 2^{V(H)}$.
Output: $\left|\mathrm{HomPin}(G, H, p)\right| \pmod 2$.

Faben and Jerrum give a polynomial-time Turing reduction from $\oplus$PINNEDHOMSTOH to $\oplus$HOMSTOH [Faben and Jerrum 2013, Cor 4.18] for the following special case: for vertices $v_1, v_2 \in V(G)$ and $h_1, h_2 \in V(H)$, $p(v_1) = \mathrm{Orb}_H(h_1)$ and $p(v_2) = \mathrm{Orb}_H(h_2)$; for every other vertex w of G, $p(w) = V(H)$, so vertex w is unconstrained by the pinning. We require a generalisation in which more vertices of G

are constrained by the pinning. We start by introducing the relevant concepts and notation.

Given rooted graphs (G, x) and (G', x'), the graph $(G, x) \cdot (G', x')$ is formed by taking the union of disjoint copies of G and G' and identifying x and x'. For each $y \in H$, we would like to produce a rooted graph $(\Theta_{H,y}, z)$ such that, for any rooted graph (G, x), the number of homomorphisms from G to H in which x is pinned to y is congruent modulo 2 to the number of homomorphisms from $(G, x) \cdot (\Theta_{H,y}, z)$ to H. However, it is not clear that such graphs always exist so Faben and Jerrum adopt a more subtle approach.

Suppose that (G, x) is a rooted graph and that H is an involution-free graph with $V(H) = \{h_1, \ldots, h_m\}$. For $i \in [m]$, let p_i be the pinning function

$$p_i(y) = \begin{cases} \{h_i\} & \text{if } y = x \\ V(H) & \text{otherwise.} \end{cases}$$

Let $v_i = |\mathrm{HomPin}(G, H, p_i)| \pmod 2$. Finally, let $\mathbf{v}_H(G, x)$ be the vector $(v_1, \ldots, v_m)$. We say that a vector $(u_1, \ldots, u_m)$ in $\mathrm{GF}(2)^m$ is *consistent for* H if, for every pair of vertices h_i and h_j in the same orbit of $\mathrm{Aut}(H)$, $u_i = u_j$. Faben and Jerrum observe that $\mathbf{v}_H(G, x)$ is consistent for H.

Let $+$ and $*$ be component-wise addition and multiplication of vectors in $\mathrm{GF}(2)^m$. Then we have Faben and Jerrum [2013, Lemma 4.11]

$$\mathbf{v}_H((G, x) \cdot (G', x'), x) = \mathbf{v}_H(G, x) * \mathbf{v}_H(G', x').$$

Now, given a graph H with $V(H) = \{h_1, \ldots, h_m\}$ and a vector $\mathbf{v} \in \mathrm{GF}(2)^m$, we say that $\mathbf{v}$ is *implementable for* H if there is a set $\{(\Theta_1, z_1), \ldots, (\Theta_k, z_k)\}$ of graphs such that $\mathbf{v} = \sum_{j=1}^{k} \mathbf{v}_H(\Theta_j, z_j)$. The key result allowing pinning is the following [Faben and Jerrum 2013, Lemmas 4.14–4.16]

LEMMA 3.1. *Let H be an involution-free graph with $V(H) = \{h_1, \ldots, h_m\}$. Every vector in $\mathrm{GF}(2)^m$ that is consistent for H is implementable for H.*

Suppose that G and H are graphs. We say that a pinning function $p \colon V(G) \to 2^{V(H)}$ is *r-restrictive* if there is a set $\{x_1, \ldots, x_r\} \subseteq V(G)$ such that

— for every $i \in [r]$ there is subset $W_i \subseteq V(H)$ such that $p(x_i) = \bigcup_{h \in W_i} \mathrm{Orb}_H(h)$; and
— for every $w \in V(G) \setminus \{x_1, \ldots, x_r\}$, $p(w) = V(H)$.

Consider the following computational problem, which is parameterised by a graph H and a natural number r.

Name: $\oplus r$-PINNEDHOMSTOH.
Input: A graph G and a r-restrictive pinning function $p \colon V(G) \to 2^{V(H)}$.
Output: $|\mathrm{HomPin}(G, H, p)| \pmod 2$.

The following theorem suffices for our purposes. The same proof would establish a slightly more general result. Instead of fixing the parameter r, we could allow r to depend on $|V(G)|$, as long as $r = \mathrm{O}(\log |V(G)|)$. However, we do not need this generalisation.

THEOREM 3.2. *Let H be an involution-free graph and let r be a positive integer. There is a polynomial-time Turing reduction from $\oplus r$-PINNEDHOMSTOH to $\oplus$HOMSTOH.*

PROOF. Consider an instance (G, p) of $\oplus r$-PINNEDHOMSTOH with $|V(H)| = m$ and let $\{x_1, \ldots, x_r\}$ be the set of vertices restricted by the r-restrictive pinning function p. For $i \in [r]$, let $\mathbf{v}_i \in \{0, 1\}^m$ be the characteristic vector of $p(x_i)$ (the vector that has

1s in positions corresponding to elements of $p(x_i)$ and 0s in every other position). By Lemma 3.1, for each i, there are gadgets $(\Theta_{i,1}, z_{i,1}), \ldots, (\Theta_{i,k_i}, z_{i,k_i})$ that implement $\mathbf{v}_i$ for H. We assume that G, H, and all the graphs $\Theta_{i,j}$ are pairwise disjoint.

Let $J = [k_1] \times \cdots \times [k_r]$. For any $\mathbf{j} = (j_1, \ldots, j_r) \in J$, let $G(\mathbf{j})$ be the graph formed from $G \cup \Theta_{1,j_1} \cup \cdots \cup \Theta_{r,j_r}$ by identifying x_i with z_{i,j_i} for each $i \in [r]$.

We have

$$\sum_{\mathbf{j} \in J} |\operatorname{Hom}(G(\mathbf{j}), H)| = \sum_{\mathbf{j} \in J} \sum_{\phi \in \operatorname{Hom}(G,H)} \prod_{i \in [r]} \left| \{ \psi \in \operatorname{Hom}(\Theta_{i,j_i}, H) \mid \psi(z_{i,j_i}) = \phi(x_i) \} \right|$$

$$= \sum_{\phi \in \operatorname{Hom}(G,H)} \sum_{\mathbf{j} \in J} \prod_{i \in [r]} \left| \{ \psi \in \operatorname{Hom}(\Theta_{i,j_i}, H) \mid \psi(z_{i,j_i}) = \phi(x_i) \} \right|$$

$$= \sum_{\phi \in \operatorname{Hom}(G,H)} \prod_{i \in [r]} \sum_{j \in [k_i]} \left| \{ \psi \in \operatorname{Hom}(\Theta_{i,j}, H) \mid \psi(z_{i,j}) = \phi(x_i) \} \right|.$$

Let $\mathbb{1}_{a \in A} = 1$ if $a \in A$ and equal 0, otherwise. Since the gadgets $(\Theta_{i,j}, z_{i,j})$ implement the characteristic vector v_i of $p(x_i)$, we have

$$\sum_{\mathbf{j} \in J} |\operatorname{Hom}(G(\mathbf{j}), H)| \equiv \sum_{\phi \in \operatorname{Hom}(G,H)} \prod_{i \in [r]} \mathbb{1}_{\phi(x_i) \in p(x_i)} \pmod 2$$

$$\equiv \left| \{ \phi \in \operatorname{Hom}(G,H) \mid \phi(x_i) \in p(x_i) \text{ for all } i \in [r] \} \right| \pmod 2$$

$$\equiv \left| \operatorname{HomPin}(G,H,p) \right| \pmod 2.$$

So the output corresponding to (G, p) is $\sum_{\mathbf{j} \in J} |\operatorname{Hom}(G(\mathbf{j}), H)|$, and the reduction consists of computing J, and for each $\mathbf{j} \in J$, constructing $G(\mathbf{j})$ and summing the oracle's answers.

We now consider the complexity of the reduction. Let b be the greatest number of gadgets required to implement a pin to any union of orbits of vertices of H and let c be the greatest size of all the gadgets used to implement any such pinning. Since H is a fixed parameter, b and c are constants, independent of the input graph G. Also, $\max_{i \in [r]} k_i \leq b$ and $\max_{i \in [r], j \in [k_i]} |V(\Theta_{i,j})| \leq c$.

Computing $\sum_{\mathbf{j} \in J} |\operatorname{Hom}(G(\mathbf{j}), H)|$ requires $|J| \leq b^r$ oracle calls. Each of these oracle calls applies to a graph $G(\mathbf{j})$ with at most $n + rc$ vertices, each of which can be trivially constructed in polynomial time. Therefore, we have a polynomial-time Turing reduction, as claimed. □

4. GADGETS

In this section, we define the gadgets we use to prove ⊕P-hardness of ⊕HOMSTOH problems by reduction from ⊕IS. These gadgets should not be confused with the pinning gadgets of the previous section though, in the rest of the article, we only use the pinning gadgets implicitly, through Theorem 3.2.

Definition 4.1. A *hardness gadget* in a graph H is a tuple $(\beta, s, t, O, i, K, k, w)$, where β is a positive integer, s, t, and i are vertices of H, $(O, \{i\}, K)$ is a partition of $\Gamma_H(s)$, and $k \colon K \to \mathbb{N}_{>0}$ and $w \colon K \to V(H)$ are functions. The following conditions must be satisfied.

(1) $|O|$ is odd.
(2) For any $o \in O$ and $y \in O \cup \{i\}$, s is the unique vertex that is adjacent to o and y and has an odd number of β-walks to t.
(3) There are an even number of $(1 + \beta)$-walks from i to t.

(4) For all $u \in K$, $w(u)$ has an even number of $k(u)$-walks to u and an odd number of $k(u)$-walks to every vertex in $O \cup \{i\}$.

These conditions simplify if $\beta = 1$, since having an odd number of 1-walks to a vertex is the same as being adjacent to it. In cases where $\beta = 1$, we will use this simplified condition without comment.

The construction used in our reduction from $\oplus$IS is given formally in Definition 8.6. Given a graph G and a hardness gadget Γ, we will produce a graph G_Γ that includes a copy of $V(G)$. We call the vertices in this copy, "G-vertices." We will consider homomorphisms from G_Γ to H. Using the pinnings described in the previous section, we will restrict attention to homomorphisms that map all G-vertices to neighbours of s. Part 4 of the definition ensures that there will be an even number of such homomorphisms that map any G-vertices to members of K. These contribute nothing to the total modulo 2 so the effect is to restrict to homomorphisms that map every G-vertex to $O \cup \{i\}$. Part 3 of the definition will ensure that the number of homomorphisms that map adjacent vertices in G to i is even so these also do not contribute. Thus, the homomorphisms that remain are those in which an independent set of G-vertices mapped to i. Our key technical result is that every nontrivial, involution-free cactus graph contains a hardness gadget (Theorem 7.3).

Our analysis is based primarily on decompositions of graphs into their subgraphs, so we need conditions under which a hardness gadget in an induced subgraph of H is a hardness gadget in H. The idea here is that, if a hardness gadget satisfies the distance requirements for a vertex v, the structure of the graph beyond v cannot interfere with the gadget's paths.

Definition 4.2. Consider a hardness gadget $(\beta, s, t, O, i, K, k, w)$ in H and a vertex $v \in V(H)$. The *primary distance requirement* of the gadget with respect to v is

$$d_H(v, O \cup \{i\}) + d_H(v, t) > \beta - 1.$$

The *secondary distance requirement* of the gadget with respect to v is that, for each $u \in K$,

$$d_H(v, w(u)) + d_H(v, O \cup \{i, u\}) > k(u) - 2.$$

Suppose that $H_1, \ldots, H_\kappa$ is a split of the graph H at some cut vertex v. If there is a hardness gadget Γ in H_1 that satisfies the distance restrictions for v, it is easy to see that it also satisfies the distance restrictions for all $x \in V' = V(H_2) \cup \cdots \cup V(H_\kappa)$, since any path from H_1 to V' must go through v. This ensures that Γ is also a hardness gadget in H, since the number of walks of various lengths required by the definition of the hardness gadget cannot be affected by vertices beyond v.

In some cases, our decomposition might yield subgraphs that do not contain hardness gadgets. We are still able to make progress using structures that can be combined with other parts of the graph to produce a hardness gadget. A partial hardness gadget is, essentially, a simplified hardness gadget that has $K = \emptyset$ and that doesn't yet have a "t" vertex: at a later point, we will find a vertex t with the properties necessary to produce a full hardness gadget.

Definition 4.3. A *partial hardness gadget* in a rooted graph (H, x) is a tuple (s, i, O, P) where s is a vertex of H, $(\{i\}, O)$ is a partition of $\Gamma_H(s)$, and P is a path in H satisfying the following conditions.

— $|O|$ is odd.
— P is the unique shortest path from x to i in H.
— Ps is the unique shortest path from x to s in H.
— For each $o \in O$, Pso is the unique shortest path from x to o in H.
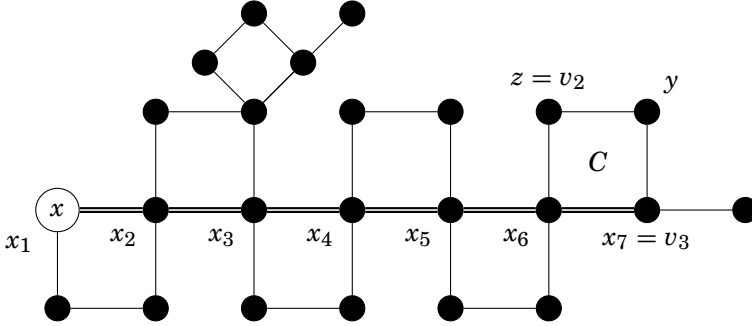
Fig. 3. A mosaic with the 2,3-path (P, v_2, v_3) that can be found using Lemma 5.3. P is drawn with a double line.

5. MOSAICS

The final structure that can arise from our decompositions is a subgraph made entirely from 4-cycles and from edges between vertices of those cycles and additional vertices of degree 1. Some mosaics (the "shortcut mosaics" defined in the following) already contain hardness gadgets. In the other cases, we identify structures called "2,3-paths" in mosaics and these will provide a "t" vertex for a partial hardness gadget elsewhere in the decomposed graph.

Definition 5.1. A *mosaic* is a rooted graph defined as follows.

— An unbristled mosaic is the one-vertex rooted graph or a rooted cactus graph that is a union of 4-cycles.
— A *mosaic* is a rooted graph (H, x) for which there is a partition (V', V'') of $V(H)$ such that x is in V', $(H[V'], x)$ is an unbristled mosaic, and $E(H) - E(H[V'])$ is a perfect matching between V'' and a subset of V'. The edges of the matching are called *bristles*.
— A *proper mosaic* is a mosaic that contains at least one cycle.

The graphs in Figure 1 would be mosaics if a root were placed at any vertex on a cycle. Note that every vertex of a mosaic is adjacent to at most one bristle. Note also that the one-vertex rooted graph and a rooted edge are both mosaics (but not proper mosaics).

Definition 5.2. A *2,3-path* in a rooted graph (H, x) is a tuple (P, v_2, v_3) such that v_2 and v_3 are in the same cycle of H and that, for $j \in \{2, 3\}$, $\deg_H(v_j) = j$ and Pv_j is the unique shortest x–v_j path in H.

LEMMA 5.3. *Every involution-free proper mosaic (H, x) contains a 2,3-path.*

PROOF. See Figure 3. Write $x_1 = x$ and let $P = x_1 \ldots x_\ell$ be a longest path from x_1 in H that uses only edges from cycles and uses at most one edge from each cycle. P contains at least one edge because x is on a cycle. Let $C = x_{\ell-1} x_\ell y z x_{\ell-1}$ be the cycle containing $x_{\ell-1}$ and x_ℓ.

x_ℓ is on a cycle, so $\deg(x_\ell) \geq 2$. Also, $\deg(x_\ell) \leq 3$ since, otherwise, x_ℓ would have a neighbour $x_{\ell+1}$ on a cycle other than C and the path $Px_{\ell+1}$ would contradict the choice of P. By the same argument, $2 \leq \deg(z) \leq 3$. Furthermore, $\deg(x_\ell) \neq \deg(z)$ or H would have an involution exchanging these two vertices. Note that $P' = x_1 \ldots x_{\ell-1} z$ is the unique shortest x–z path in H, since any other x–z path must include edges from
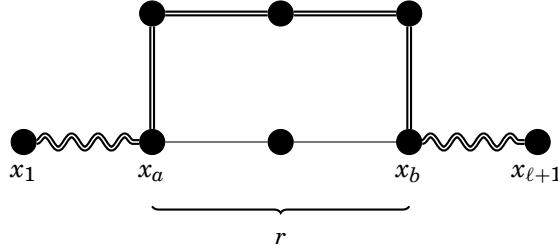
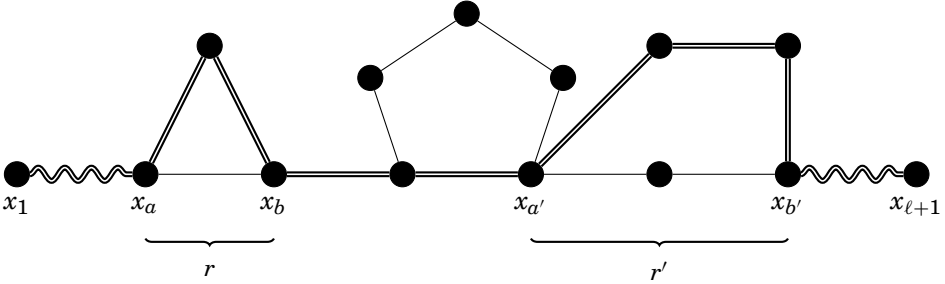Fig. 4.   An example of a walk in $T_1(P)$, shown with double lines.

Fig. 5.   An example of a walk in $T_2(P)$, shown with double lines.

exactly the same cycles as P' and must include at least two edges from one of them. Thus, either $(x_1 \ldots x_{\ell-1}, x_\ell, z)$ or $(x_1, \ldots, x_{\ell-1}, z, x_\ell)$ is a 2,3-path. □

In several cases, we have a unique shortest path of length ℓ between two vertices in a graph and we are interested in the number of $(\ell + 2)$ walks between those two vertices. The following definition helps us count such walks.

Definition 5.4. Let $P = x_1 \ldots x_{\ell+1}$ be a path in a graph H. We define the following three sets of $(\ell + 2)$-walks from x_1 to $x_{\ell+1}$.

(1) $T_1(P)$ is the set of walks that differ from P by going the long way around a $(2r+2)$-cycle from which P uses r consecutive edges, as shown in Figure 4. Formally, these are the walks $x_1 \ldots x_a P' x_b \ldots x_{\ell+1}$, where $1 \le a < b \le \ell+1$ and $x_a P' x_b$ is a $(b-a+2)$-path in $H - \{x_{a+1}, \ldots, x_{b-1}\}$.
(2) $T_2(P)$ is the set of walks that differ from P by going the long way around cycles of length $2r+1$ and $2r'+1$, from which P uses r and r' consecutive edges, respectively, as shown in Figure 5. Formally, these are the $x_1 \ldots x_a P' x_b \ldots x_{a'} P'' x_{b'} \ldots x_{\ell+1}$, where $1 \le a < b \le a' < b' \le \ell + 1$, $x_a P' x_b$ is a $(b - a + 1)$-path in $H - \{x_{a+1}, \ldots, x_{b-1}\}$ and $x_{a'} P'' x_{b'}$ is a $(b' - a' + 1)$-path in $H - \{x_{a'+1}, \ldots, x_{b'-1}\}$.
(3) $T_3(P)$ is the set of walks $x_1 \ldots x_a z x_a \ldots x_{\ell+1}$, where $1 \le a \le \{\ell + 1\}$ and $z \in \Gamma_H(x_a)$ (we allow the case $z = x_{a\pm1}$).

We refer to the cycles appearing in the definition of T_1 and T_2 as *detour cycles*.

It is easy to see that, when P is the unique shortest x_1–$x_{\ell+1}$ path in a cactus graph, $T_1(P)$, $T_2(P)$ and $T_3(P)$ is a partition of the set of all $(\ell(P) + 2)$-walks from x_1 to $x_{\ell+1}$.

LEMMA 5.5. *Let H be a cactus graph containing distinct odd-degree vertices v_1 and v_2, with a unique shortest path P between them. Suppose that every edge of P is on a*
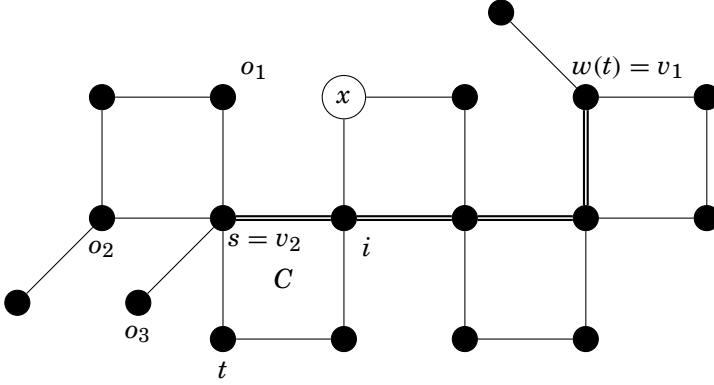
Fig. 6. A mosaic containing containing a hardness gadget as in Lemma 5.5. The path P is shown with a double line and $O = \{o_1, o_2, o_3\}$.

4-*cycle of H and no* 4-*cycle of H contains two edges of P. Then H contains a hardness gadget that satisfies the distance requirements for every* $v \in (V(H) \setminus V(P)) \cup \{v_2\}$.

Note that the premise of the lemma is symmetric about v_1 and v_2, while the conclusion is not. By symmetry, we could, of course, find a different hardness gadget satisfying the distance requirements for v_1 instead of v_2.

PROOF. See Figure 6. Choose v_1, v_2, and P satisfying the given conditions so that $\ell(P)$ is as small as possible. Note that v_1 and v_2 have degree at least 3, since they have odd degree and are on cycles.

Let $\beta = 1$. Let $s = v_2$, let i be the neighbour of s in P and let t be the neighbour of s that is in the same 4-cycle as i; call this cycle C. Let $K = \{t\}$ and $O = \Gamma_H(s) \setminus (\{i\} \cup K)$. Let $w(t) = v_1$ and $k(t) = \ell(P) + 1$.

To see that $\Gamma = (\beta, s, t, O, i, K, k, w)$ is a hardness gadget, note first that $|O|$ is odd, since $\deg_H(s)$ is odd. Consider any $o \in O$ and $y \in O \cup \{i\}$. Since H is a cactus graph, s is the unique vertex adjacent to o, y and t. However, there are two vertices that are adjacent to i and t: s and the fourth vertex on cycle C. Therefore, there are two $(\beta + 1)$-walks from i to t. Finally, consider vertex $w(t) = v_1$. Vertex v_1 has two $(\ell(P) + 1)$-walks to t (going around the cycle C in either direction). For every vertex $o \in O$, Po is the unique $(\ell(P) + 1)$-walk from v_1 to o.

We will finish the proof that Γ is a hardness gadget by showing that $w(t) = v_1$ has an odd number of $(\ell(P) + 1)$-walks to i. Let P_i be the length-$(\ell(P) - 1)$ prefix of P. P_i is the unique shortest path from v_1 to i. Consider Definition 5.4, with $x_1 = v_1$, $\ell = \ell(P_i)$ and $x_{\ell+1} = i$. Since P_i only uses one edge from each cycle it meets and each such cycle is a 4-cycle, $T_2(P_i) = \emptyset$. There are $\ell(P_i)$ walks in $T_1(P_i)$, since every edge of P (hence, every edge of P_i) is on a distinct 4-cycle of H. The number of walks in $T_3(P_i)$ is $\sum_{v \in P_i} \deg_H(v) - \ell(P_i)$, since every edge adjacent to P_i may be repeated, but edges in P_i should not be counted twice. The total number of walks is therefore $\sum_{v \in P_i} \deg_H(v)$. This is odd since $\deg_H(v_1)$ is odd, and every vertex in P_i other than v_1 has even degree (otherwise the minimality of $\ell(P)$ would be contradicted).

The hardness gadget Γ satisfies the primary distance requirement $d_H(v, O \cup \{i\}) + d_H(v, t) > 0$ for any $v \in V(H)$ since $t \notin O \cup \{i\}$, so at least one of the terms $d_H(v, O \cup \{i\})$ and $d_H(v, t)$ is positive. Now consider any $v \in V(H) \setminus V(P_i)$. We wish to show that the

secondary distance requirement $d_H(v, v_1) + d_H(v, O \cup \{i, t\}) > \ell(P) - 1$ is satisfied. We do this by establishing the following inequalities.

$$d_H(v, v_1) + d_H(v, i) > \ell(P) - 1 \tag{1}$$
$$d_H(v, v_1) + d_H(v, O \cup \{t\}) > \ell(P) - 1. \tag{2}$$

Establishing (1) is easy. Since $v \notin P_i$ and P_i is the unique shortest path from v_1 to i, $d_H(v, v_1) + d_H(v, i) > \ell(P_i) = \ell(P) - 1$. Establishing (2) is similar. For each $y \in O \cup \{t\}$, $d_H(v_1, y) = \ell(P) + 1$. Therefore, for any $v \in V(H) \setminus V(P_i)$, $d_H(v, v_1) + d_H(v, y) \geq \ell(P) + 1$.   □

Definition 5.6. A *shortcut* in a mosaic (H, x) is a pair of odd-degree vertices v_1, v_2, with degree at least 3, that have a unique shortest path P between them, and this path does not contain x. A *shortcut mosaic* is a mosaic that contains a shortcut.

If v_1, v_2 is a shortcut in a mosaic (H, x), then v_1 and v_2 are on cycles (since their degrees are at least 3), so every edge of the unique shortest path P between them is on a 4-cycle. Since P is unique, these edges are on distinct 4-cycles. Thus, Lemma 5.5 has the following corollary.

COROLLARY 5.7. *If (H, x) is a shortcut mosaic then H contains a hardness gadget that satisfies the distance requirements for x.*

6. COMBINATION LEMMAS

We mostly proceed by splitting graphs at cut vertices and investigating the resulting components. In this section, we present a number of technical lemmas that show how to combine structures in the various parts of a graph split to obtain hardness gadgets.

Observation 6.1. If $\{H_1, \ldots, H_\kappa\}$ is the split of an involution-free graph H at a cut vertex v then, for each $j \in [\kappa]$, the rooted graph (H_j, v) is involution-free even though H_j itself might not be involution-free. To see that (H_j, v) is involution-free, note that an involution of H_j that fixes v induces an involution of H.

LEMMA 6.2. *Let x be a cut vertex of an involution-free cactus graph H. If there exists a split of H at x into $\{H_1, \ldots, H_\kappa\}$ such that (H_1, x) and (H_2, x) are both proper mosaics then H has a hardness gadget which satisfies the distance requirements for every vertex $v \in V(H) \setminus (V(H_1) \cup V(H_2))$.*

PROOF. If, for $j = 1$ or $j = 2$, (H_j, x) is a shortcut mosaic then, by Corollary 5.7, H_j contains a hardness gadget Γ that satisfies the distance requirements for x. Since x is a cut vertex, Γ is a hardness gadget in H and satisfies the distance restrictions for every vertex outside H_1 and H_2.
Suppose that neither of (H_1, x) and (H_2, x) is a shortcut mosaic. For $j \in \{1, 2\}$, apply Lemma 5.3 to (H_j, x) to obtain a 2,3-path (P_j, y_j, z_j). Since $z_j \neq x$ and x is a cut vertex, $\deg_H(z_j) = \deg_{H_j}(z_j) = 3$. $z_1 P_1 P_2 z_2$ is the unique shortest z_1–z_2 path in H and each edge of this path is in a different 4-cycle. By Lemma 5.5, H contains a hardness gadget which satisfies the distance requirements for every $v \in (V(H) \setminus V(P)) \cup \{z_2\}$.   □

LEMMA 6.3. *Let H be a cactus graph with a cut vertex x of odd degree. If there exists a split of H at x into $\{H_1, \ldots, H_\kappa\}$ such that (H_1, x) is an involution-free proper mosaic, then H has a hardness gadget that satisfies the distance requirements for every $v \in V(H) \setminus V(H_1)$.*

PROOF. If (H_1, x) is a shortcut mosaic, then Corollary 5.7 gives a hardness gadget in H_1. As in the previous lemma, this is a hardness gadget in H and satisfies the distance requirements. If (H_1, x) is not a shortcut mosaic, apply Lemma 5.3 to (H_1, x) to obtain
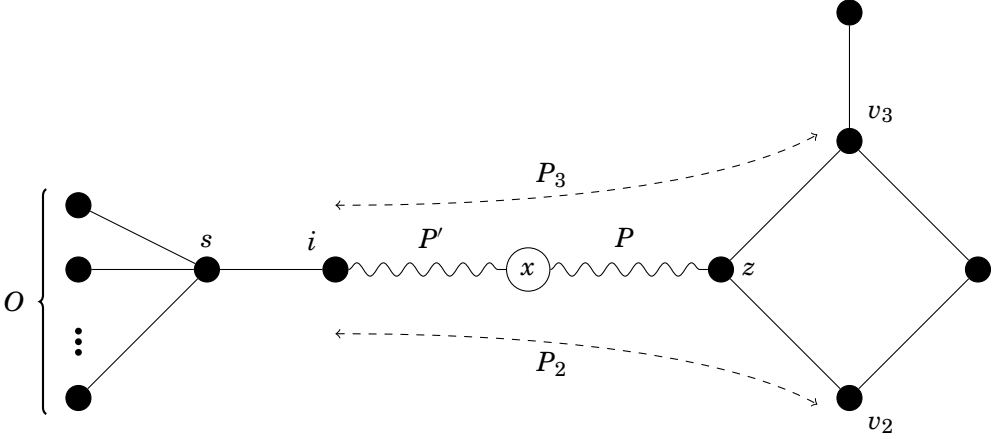
Fig. 7.   The paths appearing in the proof of Lemma 6.4.

a 2,3-path (P, v_2, v_3). Since $v_3 \neq x$ and x is a cut vertex, $\deg_H(v_3) = \deg_{H_1}(v_3) = 3$ and P is the unique shortest path in H between v_3 and x. Since (H_1, x) is a proper mosaic, every edge of P is on a distinct 4-cycle of H. By Lemma 5.5, H contains a hardness gadget that satisfies the distance requirements for every $v \in (V(H) \setminus V(P)) \cup \{x\}$, which proves the lemma.   □

LEMMA 6.4.   *Let H be a cactus graph. Suppose that $\{H_1, \ldots, H_\kappa\}$ is the split of H at x, that (H_1, x) contains a 2,3-path (P, v_2, v_3), and that (H_2, x) contains a partial hardness gadget (s, i, O, P'). Then H has a hardness gadget that satisfies the distance requirements for very vertex $v \in V(H) \setminus (V(PP') \cup \{v_2, v_3\})$.*

PROOF.   See Figure 7. Let z be the endpoint of the path P that is not x, or let $z = x$ if $\ell(P) = 0$. Since H is a cactus graph and v_2 and v_3 are on a cycle together, the cycle must contain the edges (z, v_2) and (z, v_3). Since $v_2 \neq x$ and $v_3 \neq x$ and x is a cut vertex, $\deg_H(v_2) = 2$ and $\deg_H(v_3) = 3$. It is easy to see that $(P'P, v_2, v_3)$ is a 2,3-path in H. For $j \in \{2, 3\}$, let $P_j = P'Pv_j$.

We next show that the number of $(\ell(P_2) + 2)$-walks from i to v_2 differs in parity from the number of $(\ell(P_2) + 2)$-walks from i to v_3. There are two kinds of walks to consider—those that detour around cycles, and those that repeat an edge. Using the notation from Definition 5.4, walks that detour around cycles are in T_1 or T_2 and those that repeat an edge are in T_3. Since (z, v_2) and (z, v_3) are not on any cycles other than the one that contains them both, all of these walks pass through z, progressing on to v_2 or to v_3. Furthermore, the number of $(\ell(P_2) + 2)$-walks that detour around cycles is the same for both endpoints, v_2 and v_3. Now note that the number of $(\ell(P_2) + 2)$-walks in $T_3(P_3)$ is exactly one more than the number in $T_3(P_2)$, because $\deg_H(v_3) = \deg_H(v_2) + 1$.

We can now define the hardness gadget. Let $\beta = \ell(P_2) + 1$. s, O, and i are already defined by the partial hardness gadget; let $K = \emptyset$. Choose $t \in \{v_2, v_3\}$ so that the number of $(1 + \beta)$-walks from i to t is even.

To see that this is a hardness gadget, consider $o \in O$ and $y \in O \cup \{i\}$. s is the only vertex that is both adjacent to o and y and has an odd number of $(\ell(P_2) + 1)$-walks to t (otherwise, there would be more than one shortest path from o to t). By construction, there are an even number of $(1 + \beta)$-walks from i to t. $K = \emptyset$ so the requirements on K are vacuous.
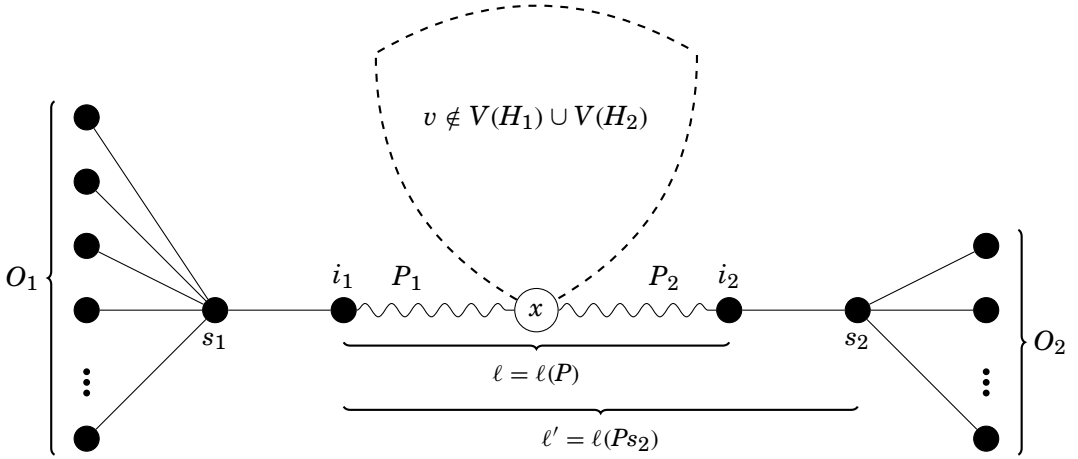
Fig. 8.   The two partial hardness gadgets of Lemma 6.6.

Now consider the primary distance requirement $d_H(v, O \cup \{i\}) + d_H(v, t) > \beta - 1 = \ell(P_2)$. The unique shortest path in H from t to $O \cup \{i\}$ is either P_2 or P_3 and this path has length $\ell(P_2)$ so the requirement is satisfied for any vertex v that is not on P_2 or P_3, which is to say, any vertex of $V(H) \setminus (V(P) \cup V(P') \cup \{v_2, v_3\})$, as required. There are no secondary distance requirements, since $K = \emptyset$, so the lemma is proved.   □

COROLLARY 6.5.   *Let H be an involution-free cactus graph and let x be a cut vertex of H. If there exists a split of H at x into $\{H_1, \ldots, H_\kappa\}$ such that (H_1, x) is a proper mosaic and (H_2, x) contains a partial hardness gadget (s, i, O, P), then H has a hardness gadget that satisfies the distance requirements for very vertex $v \in V(H) \setminus V(H_1 \cup P)$.*

PROOF.   By Lemma 5.3, (H_1, x) contains a 2,3-path; Lemma 6.4 gives the hardness gadget.   □

LEMMA 6.6.   *Let x be a cut vertex of an involution-free cactus graph H. If there is a split of H at x into $\{H_1, \ldots, H_\kappa\}$, such that (H_1, x) contains a partial hardness gadget (s_1, i_1, O_1, P_1) and (H_2, x) contains a partial hardness gadget (s_2, i_2, O_2, P_2), then H contains a hardness gadget that satisfies the distance requirements for every vertex $v \in V(H) \setminus V(P_1 P_2 s_2)$.*

PROOF.   See Figure 8. The two partial hardness gadgets ensure that $P = P_1 P_2$ is the unique shortest path in H from i_1 to i_2 and $P_1 P_2 s_2$ is the unique shortest path from i_1 to s_2. Let $\ell = \ell(P)$ and $\ell' = \ell(P s_2) = \ell + 1$.

We first show that the number of $(\ell + 2)$-walks from i_1 to i_2 (walks which use two more edges than P) differs in parity from the number of $(\ell' + 2)$-walks from i_1 to s_2. To do this, we use the sets of walks T_1, T_2, and T_3 from Definition 5.4.

First, we show that $T_1(P) = T_1(P s_2)$, by arguing that every detour cycle C that is available from $P s_2$ is also available from P. Consider a walk $x_1 \ldots x_a P' x_b \ldots x_{\ell'} s_2$ as in the definition of $T_1(P s_2)$, where $x_1 = i_1$ and $x_{\ell'} = i_2$. The claim is obvious if $x_b \in P$ so suppose for contradiction that $x_b = s_2$ and the detour cycle is $x_a \ldots x_{\ell'} s_2 P' x_a$. Then, by the definition of partial hardness gadgets, the neighbour y of s_2 in P' is in O_2 (see Figure 9). However, the definition also requires that every vertex in O_2 has a unique shortest path to x but the detour cycle gives two paths of length $\ell(P_2) + 2$ from y to x.
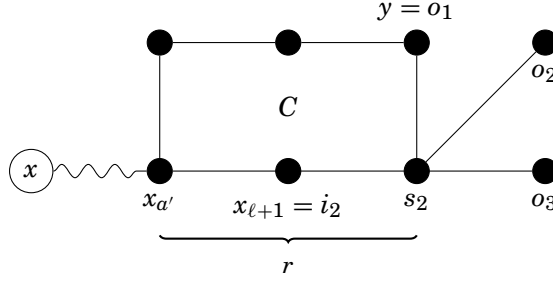
Fig. 9.   An example of an impossible detour cycle C in $T_1(Ps_2)$, using neighbours of s_2. Here $O_2 = \{o_1, o_2, o_3\}$.

A similar argument shows that $T_2(P) = T_2(Ps_2)$. This is obvious when $x_{b'} \in P$. If $x_{b'} = s_2$, the same construction gives a contradiction: the path from y to x via P'' is shorter than the one via s_2, which the definition requires to be the unique shortest y–x path.

Finally, we show that $T_3(P) \not\equiv T_3(Ps_2) \pmod 2$. This is because s_2 offers an additional set of edges that may be repeated, $\{(s_2, o) \mid o \in O_2\}$, and there are an odd number of edges in this set, since $|O_2|$ is odd.

We now construct the hardness gadget. If the number of $(\ell + 2)$-walks from i_1 to i_2 is even, then let $t = i_2$ and $\beta = \ell + 1$. Otherwise, let $t = s_2$ and $\beta = \ell' + 1$. In either case, the number of $(1 + \beta)$-walks from i_1 to t is even. Then let $s = s_1$, $O = O_1$, $i = i_1$ and $K = \emptyset$.

To see that this is a hardness gadget, consider $o \in O$ and $y \in O \cup \{i\}$. s is the unique vertex adjacent to o and to y which has an odd number of β-walks to t. (The odd number is one.) The construction guarantees an even number of $(1 + \beta)$-walks from i_1 to t.

Now consider the primary distance requirement $d_H(v, O \cup \{i\}) + d_H(v, t) > \beta - 1$. The unique shortest path in H from t to $O \cup \{i\}$ has length $\beta - 1$ so the requirement is satisfied for any vertex v that is not on this path. This is guaranteed by the restriction on v in the statement of the lemma. There are no secondary distance requirements, since $K = \emptyset$.   □

LEMMA 6.7.   *Let (H, x) be a rooted cactus graph containing a cycle $C = x_1 x_2 \ldots x_\ell x_1$, where $\ell \neq 4$. For $j \in [\ell]$, let H_j be the component containing x_j in the graph $H - E(C)$. Suppose that the rooted graph $(H[(V(H) \setminus V(H_1)) \cup \{x_1\}] , x_1)$ is involution-free. If ℓ is even, let $\mathcal{J} = [\ell] \setminus \{1, \ell/2 + 1\}$. Otherwise, let $\mathcal{J} = [\ell] \setminus \{1\}$. If, for each $j \in \mathcal{J}$, (H_j, x_j) is a mosaic, then H contains a hardness gadget that satisfies the distance requirements for each $v \in V(H_1)$.*

PROOF.   Note that for each $j \in \mathcal{J}$, (H_j, x_j) is involution-free. We start by dispensing with some easy cases. First, if there is a $j \in \mathcal{J}$ such that (H_j, x_j) is a shortcut mosaic then, by Corollary 5.7, H_j contains a hardness gadget which satisfies the distance requirements for x_j and this is also a hardness gadget in H that satisfies the distance requirements for all $v \in V(H) \setminus V(H_j)$, in particular for all $v \in V(H_1)$. Second, suppose that there is a $j \in \mathcal{J}$ such that (H_j, x_j) is a proper mosaic and $\deg_H(x_j)$ is odd. x_j is a cut vertex of H since H is a cactus graph. Therefore, Lemma 6.3 guarantees that H has a hardness gadget which satisfies the distance requirements for every $v \in V(H) \setminus V(H_j)$.

Thus, we can assume without loss of generality that, for every $j \in \mathcal{J}$, (H_j, x_j) is a shortcut-free mosaic. The two possibilities are:

— (H_j, x_j) is a (possibly trivial) shortcut-free mosaic and $\deg_H(x_j)$ is even, or
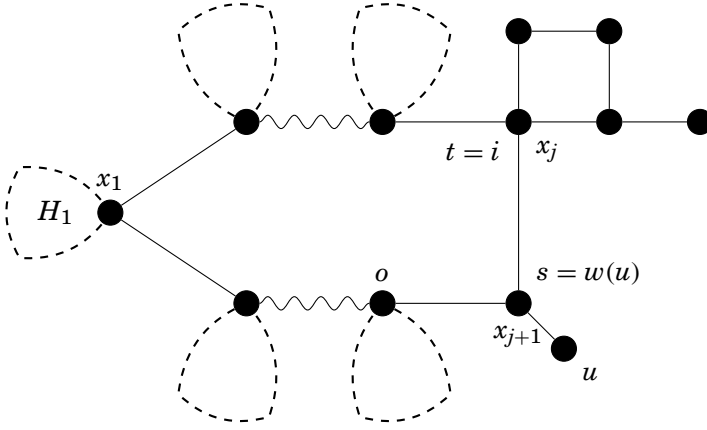— (H_j, x_j) consists of a single bristle.

Fig. 10.   The hardness gadget of Case 1.1 of Lemma 6.7. In this case, $K = \{u\}$.

Since $(H[(V(H) \setminus V(H_1)) \cup \{x_1\}], x_1)$ is involution-free, there is some $j \in \mathcal{J}$ such that $\deg_H(x_j)$ is even. Otherwise, for each $j \in \mathcal{J}$, (H_j, x_j) is a bristle. Hence H has an involution which fixes H_1 but exchanges H_{1+d} with $H_{\ell+1-d}$ for each $d \in \{1, \ldots, \lfloor \ell/2 \rfloor\}$. We will consider two cases, depending on ℓ.

Case 1. ℓ is odd. We split the analysis into two cases.

Case 1.1. There is a $j \in \{\lceil \ell/2 \rceil, \lceil \ell/2 \rceil + 1\}$ such that $\deg_H(x_j)$ is even. See Figure 10. Without loss of generality, suppose that $j = \lceil \ell/2 \rceil$ (otherwise this could be achieved by relabelling the vertices of C, going the other way around the cycle). We will construct a hardness gadget. Let $\beta = 1$, $s = x_{j+1}$, $t = x_j$, and $i = t$. Let o be the neighbour of s in C that is not t. (That is, $o = x_1$ if $\ell = 3$ and $o = x_{j+1}$, otherwise.) Let $O = \{o\}$ and let $K = \Gamma_H(s) \setminus \{o, i\}$. For every $u \in K$ let $w(u) = s$ and $k(u) = \ell - 1$.

To see that this is a hardness gadget, consider o and $y \in \{o, i\}$. s is the only vertex that is adjacent to o, y and t. However, there are an even number of vertices that are adjacent to t since $\deg_H(t)$ is even.

Consider the $(\ell - 1)$-walks from $w(u) = s$ to each $u \in K$, noting that every vertex in K is a neighbour of s. Since $s = x_{\lceil \ell/2 \rceil + 1}$, no $(\ell - 1)$-walk from s to one of its neighbours can use any edge that is not in $H' = C \cup H_3 \cup \ldots H_\ell$. Since each of $(H_3, x_3), \ldots, (H_\ell, x_\ell)$ is a mosaic, C is the only odd cycle in H'. Since $\ell - 1$ is even and the distance from s to u is one, which is odd, there is exactly one $(\ell - 1)$-walk from s to each of its two neighbours i and o in C (going the long way around the cycle) and there are no $(\ell - 1)$-walks from s to K, the set of its neighbours outside C.

Now consider the primary distance requirement $d_H(v, \{o, i\}) + d_H(v, t) > 0$. This is satisfied for any $v \in V(H) \setminus \{t\}$, including each $v \in V(H_1)$. Finally, consider the secondary distance requirement $d_H(v, s) + d_H(v, \{o, i, u\}) > \ell - 3$. This is true for any $v \in V(H_1)$ since $d_H(x_1, s) + d_H(x_1, \{o, i, u\}) = d_H(x_1, s) + d_H(x_1, o) = \lfloor \ell/2 \rfloor + \lfloor \ell/2 \rfloor - 1 = \ell - 2$.

Case 1.2. We are not in Case 1.1 but there is still a $j \in \mathcal{J}$ such that $\deg_H(x_j)$ is even. Without loss of generality, we may assume that $j < \lceil \ell/2 \rceil$, numbering the vertices of the cycle the other way around, if necessary.

Again we will construct a hardness gadget. See Figure 11. This time, let $s = x_{\lceil \ell/2 \rceil}$ and $i = x_{\lceil \ell/2 \rceil - 1}$. Since we are not in Case 1.1, $\deg_H(s) = 3$. Choose $t \in \{x_2, \ldots, x_{\lceil \ell/2 \rceil - 1}\}$ such that $\deg_H(t)$ is even and $d_H(t, i)$ is as small as possible. Let $\beta = d_H(t, s)$. Let
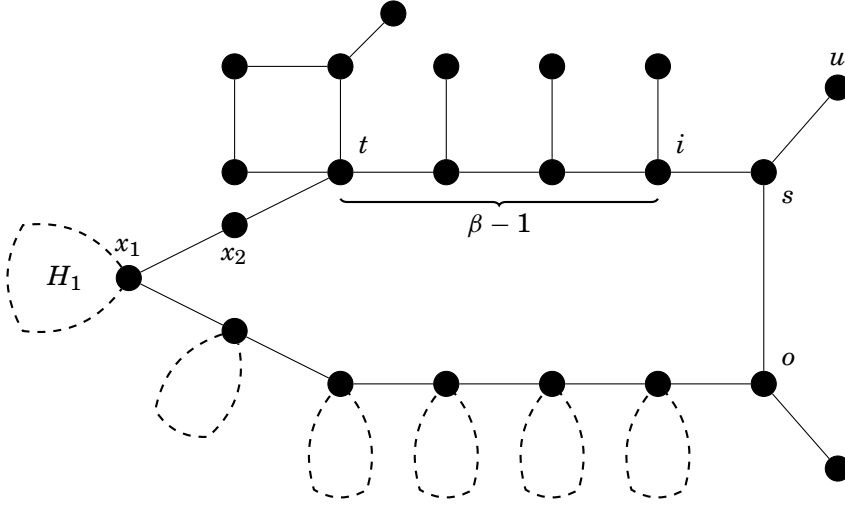
Fig. 11.   The hardness gadget of Case 1.2 of Lemma 6.7. Here, $\ell = 13$, $\beta = 4$, and $K = \{u\}$.

$o = x_{\lceil \ell/2 \rceil + 1}$, which also has degree 3, since we are not in Case 1.1; let $O = \{o\}$. Let u be the neighbour of s that is not in C and let $K = \{u\}$. Let $w(u) = s$ and $k(u) = \ell - 1$.

To see that this is a hardness gadget, consider o and $y \in \{o, i\}$. $d_H(o, t) = \beta + 1$ and s is the only neighbour of o that has any β-walks to t, and it has one such walk. Also, s is adjacent to y. On the other hand, there are an even number of $(\beta + 1)$-walks from i to t. All of these walks repeat an edge, and there are an even number of edges that can be repeated because, by the choice of t, every vertex between i and t has odd degree. The proof that $w(u) = s$ has an even number of $k(u)$-walks to u and odd number of $k(u)$-walks to each of o and i is exactly the same as in the proof of Case 1.1.

Now consider the primary distance requirement $d_H(v, \{o, i\}) + d_H(v, t) > \beta - 1$. This follows for any v which is not on the unique shortest path in H from t to i, which includes every $v \in V(H_1)$. Finally, consider the secondary distance requirement $d_H(v, s) + d_H(v, \{o, i, u\}) > \ell - 3$. As in Case 1.1, this is true for any $v \in V(H_1)$ since $d_H(x_1, s) + d_H(x_1, \{o, i, u\}) = \ell - 2$.

Case 2. ℓ is even. Recall that $\ell \neq 4$ by the hypothesis of the lemma. Choose $j \in \mathcal{J}$ such that $\deg_H(x_j)$ is even; again, we may assume that $j \leq \ell - 2$, and $1 \notin \mathcal{J}$ by definition. Let $s = x_{j+1}$. We will construct a hardness gadget for H in each of two cases.

Case 2.1. $\deg_H(s)$ is even. See Figure 12. Let $\beta = 1$, $i = t = x_j$ and $O = \Gamma_H(s) \setminus \{i\}$. Note that $|O|$ is odd. Let $K = \emptyset$.

To see that this is a hardness gadget, consider any $o \in O$ and $y \in O \cup \{i\}$. s is the unique vertex adjacent to o, y, and t. Since $\deg_H(x_j)$ is even, there are an even number of 2-walks from i to $t = i$. Consider the primary distance requirement $d_H(v, O \cup \{i\}) + d_H(v, t) > 0$. This is satisfied for every $v \neq t$, including every $v \in V(H_1)$. There are no secondary distance requirements since $K = \emptyset$.

Case 2.2. $\deg_H(s)$ is odd so, in fact, $\deg_H(s) = 3$. See Figure 13.

Let $\beta = \ell/2 - 1$. Let $i = x_{j+2}$, $K = \{x_j\}$ and $O = \Gamma_H(s) \setminus \{x_j, x_{j+2}\}$, which is a single vertex: call this o. Let t be the unique vertex in C at distance $\ell/2$ from i. Let $w(x_j) = x_j$ and $k(x_j) = 2$.

To see that this is a hardness gadget, consider o and any $y \in \{o, i\}$. There is a unique $(\beta + 1)$-walk from o to t, and this goes via s. Thus, s is the unique vertex adjacent
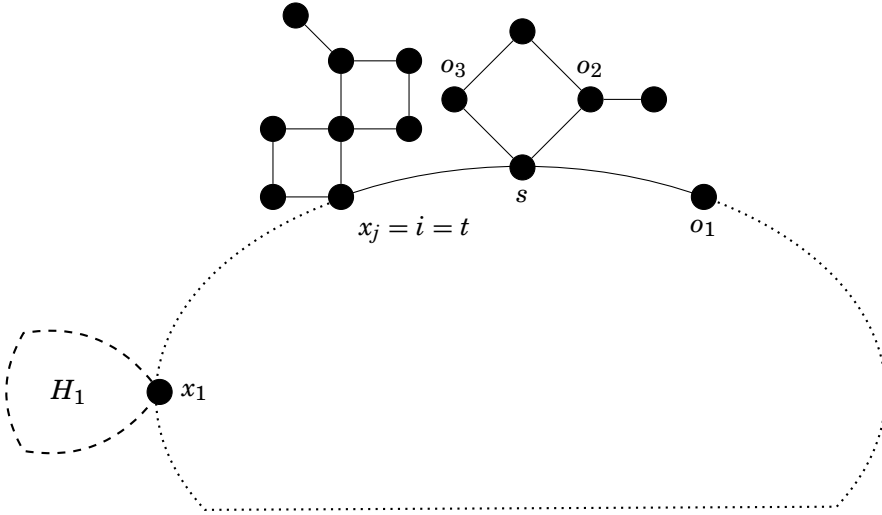
Fig. 12.   An example of a hardness gadget for Case 2.1 of Lemma 6.7. Here $O = \{o_1, o_2, o_3\}$; the dotted line indicates omitted portions of the cycle C.
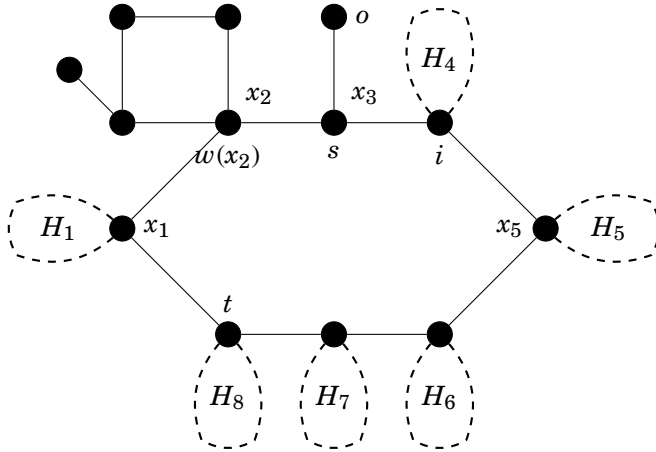

Fig. 13.   An example of a hardness gadget for Case 2.2 of Lemma 6.7. In this case, $\ell = 8$, $\beta = 3$, and $j = 2$.

to o and y that has an odd number (one) of β-walks to t. By construction, there are exactly two $(\beta + 1)$-walks from i to t, one going each way around the cycle C. Since $\deg_H(x_j)$ is even, there are an even number of 2-walks from x_j to itself, but there is exactly one 2-walk from x_j to each of o and i. The primary distance requirement is $d_H(v, \{o, i\}) + d_H(v, t) > \beta - 1$. Since $d_H(t, \{o, i\}) = \beta + 1$, this holds for any v. Finally, the secondary distance requirement is $d_H(v, x_j) + d_H(v, \{o, i\} \cup K) > 0$. This holds for any $v \neq x_j$, including all $v \in V(H_1)$.   □

7. HARDNESS GADGETS IN CACTUS GRAPHS

In this section, we show that every nontrivial involution-free cactus graph contains a hardness gadget. We first show that every involution-free rooted cactus graph that is not a mosaic contains a hardness gadget or a partial hardness gadget.

For rooted graphs, Observation 6.1 allows an inductive proof. Given an involution-free rooted graph (H, x) in which x is a cut vertex, we can take the split $\{H_1, \ldots, H_\kappa\}$ and recurse on the rooted graphs $\{(H_1, x), \ldots, (H_\kappa, x)\}$, since these are also involution-free. If x is not a cut vertex or splitting at x does not give helpful rooted subgraphs, we instead cut H up by deleting the edges of an appropriate cycle C to give components which can be rooted at the vertices in C. One of these contains x, so needs special attention; the others are dealt with inductively.

Finally, we need to show that every nontrivial, involution-free unrooted cactus graph contains a hardness gadget. To do this, we temporarily introduce a root at a suitable vertex.

LEMMA 7.1. *An involution-free rooted tree* (H, x) *with at least three vertices contains a partial hardness gadget.*

PROOF. Let o be a leaf of H at maximal distance from x. Let s be the neighbour of o. Since (H, x) is involution-free and H contains at least three vertices $d_H(x, o) > 1$ so $s \neq x$. Let i be the neighbour of s on the path to x. Any neighbour of s that is not on the path to x must be a leaf as, otherwise, there would be a leaf farther from x than o is. But no vertex in an involution-free tree can be adjacent to more than one leaf, so $\deg_H(s) = 2$. Let P be the (unique) path in the tree H from i to x. The partial hardness gadget is $(s, i, \{o\}, P)$. □

We say that a cut vertex $x \in V(H)$ is *cycle-separating* if at least two of the components of the split of H at x contain cycles.

LEMMA 7.2. *Let* (H, x) *be a connected, involution-free rooted cactus graph. Then at least one of the following is true:*

— H *contains a hardness gadget satisfying the distance requirements for x, or*
— (H, x) *contains a partial hardness gadget, or*
— (H, x) *is a shortcut-free mosaic.*

PROOF. The proof is by induction on the number of cycles in H. If H is acyclic and is a single vertex or a single edge, (H, x) is a shortcut-free mosaic; if it is acyclic and has more than one edge, it contains a partial hardness gadget by Lemma 7.1.

Otherwise, H contains at least one cycle. If x is a cycle-separating cut vertex, let $\{H_1, \ldots, H_\kappa\}$ be the split of H at x. Every (H_j, x) is an involution-free cactus graph and has fewer cycles than H. If some H_j contains a hardness gadget that satisfies the distance requirements for x, this is also a hardness gadget in H and still satisfies the distance requirements. Likewise, a partial hardness gadget in some (H_j, x) is also a partial hardness gadget in (H, x). If there is no hardness or partial hardness gadget in any (H_j, x_j) then, by the inductive hypothesis, every (H_j, x) is a shortcut-free mosaic. It follows that (H, x) is, itself, a shortcut-free mosaic. It is a mosaic because involution-freedom of (H, x) guarantees that the (H_j, x) are pairwise non-isomorphic so, in particular, x has at most one bristle in H. It is shortcut-free because any shortcut in (H, x) must be inside some (H_j, x), but all of them are shortcut-free.

For the remainder of the proof, we assume that x is not a cycle-separating cut vertex (indeed, it is not necessarily even a cut vertex). Let $C = x_1 \ldots x_\ell x_1$ be a cycle such that there is a path from x to x_1 in which only x_1 is on a cycle. (If x is on a cycle, then C is this cycle, $x_1 = x$ and the path is trivial.) For $j \in [\ell]$, let H_j be the component of $H - E(C)$ that contains x_j. Thus, $x \in V(H_1)$. We will use the fact that $x = x_1$ if x is on a cycle. Otherwise, there is a unique path in H from x to x_1.

Each of the rooted graphs (H_j, x_j) is a cactus graph with fewer cycles than H so, by the inductive hypothesis, each contains a hardness gadget satisfying the distance restrictions for x_j, contains a partial hardness gadget, or is a shortcut-free mosaic. If
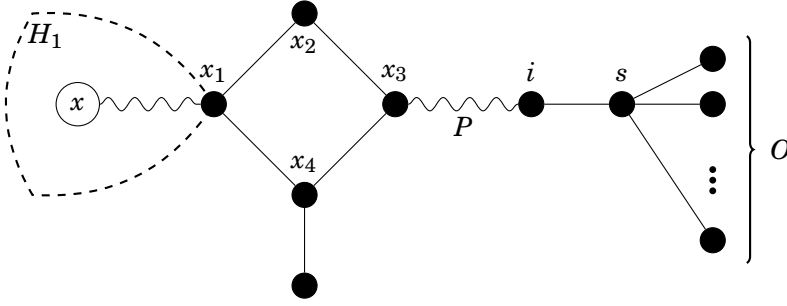
Fig. 14. An example for Case 1 of Lemma 7.2.

any of $H_2, \ldots, H_\ell$ contains a hardness gadget, this is a hardness gadget in H so we are done.

If ℓ is odd, let $\mathcal{J} = \{2, \ldots, \ell\}$; otherwise, let $\mathcal{J} = \{2, \ldots, \ell\} \setminus \{\ell/2 + 1\}$. Thus, $\mathcal{J}$ is the set of indices $j > 1$ such that H contains a unique shortest path from x to x_j.

Suppose that, for some $j \in \mathcal{J}$, (H_j, x_j) contains a partial hardness gadget (s, i, O, P). In H, x has a unique shortest path P' to x_j and $(s, i, O, P'P)$ is a partial hardness gadget in (H, x).

Otherwise, for every $j \in \mathcal{J}$, (H_j, x_j) is a shortcut-free mosaic. If $\ell \neq 4$ then, by Lemma 6.7, H contains a hardness gadget that satisfies the distance requirements for every vertex in H_1, which includes x.

We are left with the case $\ell = 4$. (H_2, x_2) and (H_4, x_4) are mosaics and (H_3, x_3) contains a partial hardness gadget or is a shortcut-free mosaic.

Case 1. (H_3, x_3) contains a partial hardness gadget.

If (H_2, x_2) is a proper mosaic, then by Lemma 5.3, it contains a 2,3-path. Then, by Lemma 6.4, H contains a hardness gadget that satisfies the distance requirements for every vertex $v \in V(H) \setminus (V(H_2) \cup V(H_3))$ and this includes $v = x$. Similarly, there is a hardness gadget if (H_4, x_4) is a proper mosaic.

So suppose that neither of (H_2, x_2) and (H_4, x_4) is a proper mosaic. Since (H, x_1) is involution-free, one of (H_2, x_2) and (H_4, x_4) is a single edge and the other is a single vertex. Suppose without loss of generality that x_2 is a single vertex. See Figure 14. Now let $H_1' = C \cup H_1 \cup H_2 \cup H_4$ and let P' be the empty path. Then (P', x_2, x_4) is a 2-3 path in (H_1', x_3). By Lemma 6.4, H has a hardness gadget that satisfies the distance requirements for every $v \in V(H) \setminus (V(H_3) \cup \{x_2, x_4\})$ including $v = x$.

Case 2. (H_3, x_3) is a shortcut-free mosaic, which means that $H' = C \cup H_2 \cup H_3 \cup H_4$ is an involution-free proper mosaic when rooted at either x_1 or x_3.

First, suppose that $x \neq x_1$. If $\deg_H(x_1)$ is odd then, by Lemma 6.3, H has a hardness gadget that satisfies the distance requirements for x_1 and this also satisfies the distance requirements for x. If $\deg_H(x_1)$ is even, let $s = x_1$, let i be s's neighbour on the shortest path to x and let P be the unique shortest path from x to i in H. $(s, i, \Gamma_H(s) \setminus \{i\}, P)$ is a partial hardness gadget in H.

Finally, suppose that $x = x_1$. Since x is not a cycle-separating cut vertex, every component of the split of H at x apart from (H', x) is a tree. If any of these contains more than one edge, it contains a partial hardness gadget by Lemma 7.1. Otherwise, either (H', x) is the unique component of the split, or there is exactly one other component, which is the one-edge tree rooted at x. In either case, (H, x) is a mosaic. If (H, x) is shortcut-free, we are done; if not, it contains a hardness gadget satisfying the distance requirements for x, by Corollary 5.7. □

We now show how to find hardness gadgets in unrooted cactus graphs by choosing an appropriate vertex to act temporarily as a root.

THEOREM 7.3. *Every involution-free cactus graph H with more than one vertex contains a hardness gadget.*

PROOF. Split H at a cut vertex x into rooted components $(H_1', x), \ldots, (H_k', x)$ with $|V(H_1')| \geq \cdots \geq |V(H_k')|$, choosing x to maximize $|V(H_2')|$. Each (H_j', x) is an involution-free, rooted cactus graph and, if any of them contains a hardness gadget satisfying the distance requirements for x, then this is also a hardness gadget in H and we are done. Otherwise, by Lemma 7.2 each (H_j', x) contains a partial hardness gadget or is a shortcut-free mosaic.

If $|V(H_2')| > 2$, then each of (H_1', x) and (H_2', x) is either a proper mosaic or contains a partial hardness gadget. Therefore, H contains a hardness gadget, by Lemma 6.6 (two partial hardness gadgets), Lemma 6.2 (two proper mosaics), or Corollary 6.5 (one of each).

$|V(H_2')|$ cannot be 1 since H is involution free. So suppose that $|V(H_2')| = 2$. H is not a tree because then there would be a vertex y with $\deg_H(y) \geq 3$, and choosing $x = y$ would give $|V(H_2')| > 2$. H does not have two cycles because every involution-free cactus graph with two cycles contains a vertex y with $\deg(y) \geq 3$ and choosing $x = y$ would give $|V(H_2')| > 2$. Further, x must be on H's single cycle as, otherwise, we could have chosen a vertex on the path from x to the cycle as our cut vertex and, again, obtained $|V(H_2')| > 2$.

Let the single cycle C of H be $x_1 x_2 \cdots x_\ell x_1$. For $j \in [\ell]$, let H_j be the component containing x_j in $H - E(C)$. Clearly, $|V(H_j)| \leq 2$ — otherwise we could have chosen $x = x_j$ to achieve $|V(H_2')| > 2$.

For H to be involution-free, we must have $\ell \geq 6$. Since H is involution-free, the rooted graph $(H[V(H) \setminus V(H_1) \cup \{x_1\}], x_1)$ is involution free, and for each $j \in [\ell(C)] \setminus \{1\}$, H_j is an isolated vertex or a bristle, so (H_j, x_j) is a mosaic. Lemma 6.7 guarantees the existence of a hardness gadget in H. □

8. HOMOMORPHISMS TO CACTUS GRAPHS

We now use hardness gadgets to show $\oplus$P-completeness of $\oplus$HOMSTOH for nontrivial involution-free cactus graphs H. This is more complicated than the case for trees because an involution-free cactus graph is not necessarily asymmetric—recall, for example, the graph H_4 in Figure 2. We first investigate the automorphisms of cactus graphs and then give our reduction from $\oplus$IS.

8.1. Automorphisms of cactus graphs

A *centre* of a graph H is a vertex x that minimises $\max_{y \in V(H)} d_H(x, y)$. It is well known that every tree has either one or two centres and that, if a tree has two centres, they are connected by an edge. This fact was apparently first proved by Jordan [1869].

LEMMA 8.1. *Every cactus graph $H = (V, E)$ has a set $S \subseteq V$ such that $H[S]$ is (a) a vertex, (b) an edge, or (c) a cycle and, for every $\pi \in \mathrm{Aut}(H)$, $\pi(S) = S$.*

PROOF. Let T be the tree formed from H by contracting all edges of H that are on cycles. Let $\rho : V(H) \to aV(T)$ be the function that maps every vertex of $V(H)$ to a corresponding vertex in the contraction T.

We will first consider the case that T has a single centre, c. In this case, every auto-morphism of T fixes c so every automorphism of H fixes $\rho^{-1}(c)$ setwise. If $|\rho^{-1}(c)| = 1$, then we are finished. Otherwise, let $C_1, \ldots, C_\kappa$ be the cycles of H containing vertices in $\rho^{-1}(c)$. Let $V(C_i)$ denote the set of vertices in C_i so $\rho^{-1}(c) = V(C_1) \cup \cdots \cup V(C_\kappa)$. Let T' be the graph with vertex set $\{C_1, \ldots, C_\kappa\}$ in which (C_i, C_j) is an edge if and only if cycles C_i and C_j intersect in H. Again, there are two cases. First, suppose that T' has a single centre, C_i. In this case, every automorphism of T' fixes C_i, so every auto-morphism of $H[\rho^{-1}(c)]$ fixes $V(C_i)$ setwise. Thus, every automorphism of H fixes $V(C_i)$ setwise so we are finished. Second, suppose that T' has two centres, C_i and C_j. In this case, every automorphism of T' fixes the edge (C_i, C_j) so every automorphism of $H[\rho^{-1}(c)]$ fixes $V(C_i) \cup V(C_j)$ setwise. Since $H[\rho^{-1}(c)]$ is a cactus graph, there is exactly one vertex, w, in $V(C_i) \cap V(C_j)$. Thus, every automorphism of $H[\rho^{-1}(c)]$ fixes w so every automorphism of H fixes w so we are finished.

Finally, suppose that T has two centres c and c'. Every automorphism of T fixes the edge (c, c'). Since H is a cactus graph, there is exactly one edge (u, u') of H with $\rho(u) = c$ and $\rho(u') = c'$. Thus, every automorphism of H fixes the edge (u, u') so it fixes $\{u, u'\}$ setwise so we are finished. □

LEMMA 8.2. *If (H, x) is a rooted cactus graph with a nontrivial automorphism, then it has an involution.*

PROOF. We prove this by induction on $n = |V(H)|$. The base case applies when $n \leq 2$. In this case, (H, x) has no nontrivial automorphisms.

For the inductive step, suppose $n > 2$. If $\deg_H(x) = 1$, then let y be the neighbour of x in H. If (H, x) has a nontrivial automorphism then this induces a nontrivial auto-morphism of $(H - x, y)$. By the inductive hypothesis, $(H - x, y)$ then has an involution, which can be extended to an involution of (H, x) by mapping x to itself.

So suppose that $\deg_H(x) > 1$ and that (H, x) has a nontrivial automorphism. Let $\{H_1, \ldots, H_\kappa\}$ be the split of H at x. If there exist an $i \in [\kappa]$ such that (H_i, x) has a nontrivial automorphism, then by the inductive hypothesis, (H_i, x) has an involution. This can be extended to an involution of (H, x) by fixing every vertex in $V(H) \setminus V(H_i)$. Otherwise, there are distinct $i, j \in [\kappa]$ such that (H_i, x) and (H_j, x) are isomorphic. The automorphism that exchanges these and fixes all other vertices of H is an involution of (H, x). □

LEMMA 8.3. *Let H be a cactus graph that has nontrivial automorphisms but no involution. Then it contains a cycle $x_1 \ldots x_\ell x_1$ such that every nontrivial automorphism of H induces a nontrivial rotation of C. Further, any two vertices at distance 2 in C are in different orbits under the action of $\mathrm{Aut}(H)$.*

PROOF. Note that H is not a tree, since involution-free trees are asymmetric. By Lemma 8.1, there is a set $S \subseteq V[H]$ such that $H[S]$ is a vertex, an edge, or a cycle and, for every $\pi \in \mathrm{Aut}(H)$, $\pi(S) = S$.

We start by showing that $H[S]$ is a cycle. If instead $H[S]$ is a vertex x then H has a non-trivial automorphism π which is also an automorphism of (H, x). By Lemma 8.2 there is an involution of (H, x), contradicting the involution-freedom of H. Similarly, if $H[S]$ is an edge (x, y), then H has no automorphism that swaps x and y since this would give an involution. This means that H has a nontrivial automorphism that fixes x. Once again, this is an automorphism of (H, x), which contradicts the fact that H is involution-free. So, let $H[S]$ be the cycle $C = x_1 \ldots x_\ell x_1$. Note that the automorphism group of H fixes $S = V(C)$ setwise so the restriction of $\mathrm{Aut}(H)$ to S is a subgroup of the

dihedral group acting on C. Since it does not contain an involution, it is a subgroup of the cyclic group generated by the permutation $g = (x_1 x_2 \ldots x_\ell)$.

So, for every nontrivial automorphism π of H, the restriction of π to $V(C)$ is g^{d_π} for some natural number d_π. To show that g^{d_π} is a nontrivial rotation of C, we will show that $d_\pi \neq 0$. For $i \in [\ell]$, let H_i be the connected component of $H - E(C)$ containing x_i. Suppose, for contradiction, that $d_\pi = 0$. Then there is an $i \in [\ell]$ such that the restriction of π to (H_i, x_i) is nontrivial. By Lemma 8.2, (H_i, x_i) has an involution π'. Therefore, H has an involution, which agrees with π' on H_i and fixes every vertex outside H_i. This gives a contradiction.

Finally, suppose for contradiction that x_i and x_j are in the same orbit, where $x_i, x_j \in C$ and $d_H(x_i, x_j) = 2$. Then there is an automorphism π of H with $\pi(x_i) = x_j$. So $d_\pi = 2$. But then $(H_{i'}, x_{i'})$ and $(H_{j'}, x_{j'})$ are isomorphic whenever i' and j' have the same parity, so H has an involution which flips the cycle C, contradicting the fact that H is involution-free. □

Definition 8.4. Say that a homomorphism π from H to H (an endomorphism of H) is *orbit-preserving* if $\pi(v) \in \mathrm{Orb}_H(v)$ for every $v \in V(H)$. Let $\mathrm{Hom}^\star(H, H)$ be the set of orbit preserving endomorphisms of H.

The following lemma shows that the orbit-preserving endomorphisms of an involution-free cactus graph are exactly its automorphisms. Note that this is not true for all cactus graphs. For example, any even cycle $x_1 \ldots x_{2\ell} x_1$ has an endomorphism mapping all odd-numbered vertices to x_1 and even-numbered vertices to x_2. This is orbit-preserving (any cycle has only one orbit) but not an automorphism.

LEMMA 8.5. *For any involution-free cactus graph H, $\mathrm{Aut}(H) = \mathrm{Hom}^\star(H, H)$.*

PROOF. It is immediate from Definition 8.4 that $\mathrm{Aut}(H) \subseteq \mathrm{Hom}^\star(H, H)$.

If H is asymmetric, then the lemma follows from the fact that $\mathrm{Aut}(H)$ and $\mathrm{Hom}^\star(H, H)$ are both trivial.

So suppose that H has a nontrivial automorphism. Note that this implies that H is not a tree, since every involution-free tree is asymmetric. Assume for contradiction that there is a $\phi \in \mathrm{Hom}^\star(H, H)$ that is not an automorphism of H. The homomorphism ϕ cannot be a permutation of $V(H)$, since a bijective homomorphism is an isomorphism. So there are vertices x, y, and z in $V(H)$ with $x \neq y$ and $\phi(x) = \phi(y) = z$.

Define $C = x_1 \ldots x_\ell x_1$ as in Lemma 8.3. For $i \in [\ell]$, let H_i denote the connected component of $H - E(C)$ containing x_i. Each (H_i, x_i) is asymmetric since every nontrivial automorphism of H induces a nontrivial rotation of C. (If (H_i, x_i) had a nontrivial automorphism then this could be extended to a nontrivial automorphism of H that induces the trivial rotation of C.) Suppose that $x \in V(H_i)$, $y \in V(H_{i'})$, and $z \in V(H_{i''})$. Then $i' \neq i$ since the definition of $\mathrm{Hom}^\star(H, H)$ ensures that both x and y are in the orbit of z in $\mathrm{Aut}(H)$ but the only vertex in $V(H_i)$ that is in the orbit of x is x itself.

There is an automorphism π of H with $\pi(x) = z$, because $z \in \mathrm{Orb}_H(x)$. π induces a rotation of C, $\pi(x_i) = x_{i''}$ so $d_H(x_i, x) = d_H(x_{i''}, z)$. Then, since $\phi(x) = z$ and ϕ is orbit-preserving and preserves edges of H, $\phi(x_i) = x_{i''}$. Similarly, $\phi(x_{i'}) = x_{i''}$. Let π' be an automorphism of H with $\pi'(x_{i''}) = x_{i'}$ and consider the homomorphism $\phi' \in \mathrm{Hom}^\star(H, H)$ formed by applying ϕ and then π'. The homomorphism ϕ' satisfies $\phi'(x_i) = x_{i'}$ and $\phi'(x_{i'}) = x_{i'}$.

Since $\phi' \in \mathrm{Hom}^\star(H, H)$ it maps every vertex of H to an element of its own orbit. By Lemma 8.3 the orbit of every vertex in C is contained within C. Thus, $\phi'(C) = C$. To simplify the notation, assume without loss of generality (by relabelling the vertices
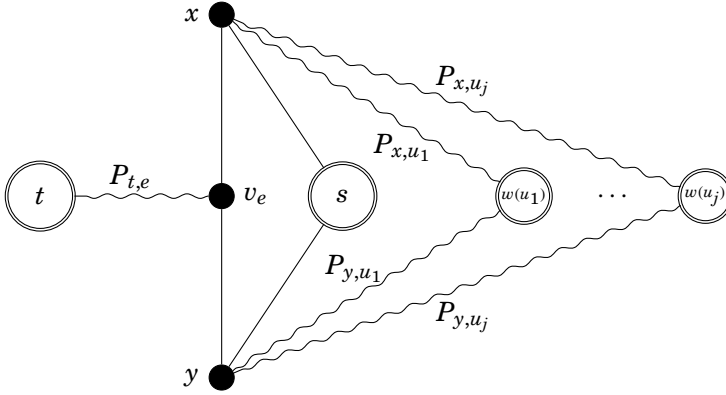
Fig. 15. The construction of G_Γ. Here $e = (x, y) \in E(G)$, so x and y are G-vertices in G_Γ. The figure illustrates the induced subgraph of G_Γ corresponding to the edge $(x, y) \in E(G)$, assuming $K = \{u_1, \ldots, u_j\}$. H-vertices are drawn with double circles; they will be pinned in the proof of Theorem 8.7.

around C if necessary) that $i' = 1$. Then $1 < i \leq \ell$ since $i \neq i'$. Also, $\phi'(x_1) = x_1$. Since (x_1, x_2) is an edge, $\phi'(x_2)$ must be a neighbour of $\phi'(x_1) = x_1$. But x_ℓ is not in the orbit of x_2 by Lemma 8.3 so $\phi'(x_2) = x_2$. Similarly, $\phi'(x_j) = x_j$ for every $j \in [\ell]$. Specifically, $\phi'(x_i) = x_i$. This contradicts $\phi'(x_i) = x_1$ since $i \neq 1$.   □

8.2. Reduction from ⊕IS

In the following definition, "adding a new path P from x to y" in a graph G means forming a graph $G \cup P$, where $V(G) \cap V(P) = \{x, y\}$.

Definition 8.6. Let $\Gamma = (\beta, s, t, O, i, K, k, w)$ be a hardness gadget in a graph H and let G be any graph. We construct the graph G_Γ as follows. Let $V'' = \{v_e \mid e \in E(G)\}$ and begin with the graph $G' = (V', E')$, where $V' = V(G) \cup V(H) \cup V''$ (these three sets are assumed to be disjoint) and $E' = E(H)$. To G', add the following:

— for every vertex $x \in V(G)$, the edge (x, s);
— for every edge $e = (x, y) \in E(G)$, the edges (x, v_e) and (y, v_e);
— for every edge $e \in E(G)$, a new β-path $P_{t,e}$ from t to v_e; and
— for every vertex $x \in V(G)$ and every $u \in K$, a new $k(u)$-path $P_{x,u}$ from x to $w(u)$.

In G_Γ, we refer to vertices that are in $V(G)$ as *G-vertices* and those in $V(H)$ as *H-vertices*. Figure 15 illustrates the construction.

Our construction of G_Γ is more complex than the one used for trees, because our hardness gadgets are more general than the corresponding structures in trees and because we must deal with graphs H that are involution-free but still have non-trivial automorphisms. To see the problem of nontrivial automorphisms, consider an involution-free cactus graph H that contains a hardness gadget Γ. Suppose that H has an automorphism π that moves Γ. For our reduction, we wish to pin one vertex to the s-vertex of Γ and another to the t-vertex. However, we cannot do this: we can only pin to the orbits of these vertices, which include $\pi(s)$ and $\pi(t)$, respectively. We must avoid counting "inconsistent" homomorphisms that, for example, map the first vertex to s and the second to $\pi(t)$, because we do not know how many such homomorphisms there are. Including the copy of H in G_Γ forbids such homomorphisms because, by pinning each vertex of the copy of H to its own orbit, we only allow homomorphisms whose restrictions to the copy of H are orbit-preserving endomorphisms. By Lemma 8.5, these

orbit-preserving endomorphisms are automorphisms of H. Hence, we will count only those homomorphisms that map to s and t and to $\pi(s)$ and $\pi(t)$, and not any that map inconsistently between the copies of Γ.

THEOREM 8.7. $\oplus$HOMSTOH *is* $\oplus$P-*complete for every involution-free cactus graph H that contains a hardness gadget.*

PROOF. Let $\Gamma = (\beta, s, t, O, i, K, k, w)$ be a hardness gadget in H. Let $r = |V(H)|$. We will give a polynomial-time Turing reduction from $\oplus$IS$(1, |O|)$ to $\oplus r$-PINNEDHOMSTOH. By the definition of hardness gadgets, $|O|$ is odd, so $\oplus$IS$(1, |O|)$ is $\oplus$P-complete by Observation 2.3. The result will then follow from Theorem 3.2, which reduces the problem $\oplus r$-PINNEDHOMSTOH to $\oplus$HOMSTOH.

Let G be an input to $\oplus$IS$(1, |O|)$ and let G_Γ be the graph defined in Definition 8.6. Let p be the r-restrictive pinning function $p \colon V(G_\Gamma) \to 2^{V(H)}$ with $p(v) = \mathrm{Orb}_H(v)$ for every $v \in V(H)$ and $p(w) = V(H)$ for every $w \in V(G_\Gamma) \setminus V(H)$. The vertices that are restricted by the pinning function p are drawn with double circles in Figure 15. We will establish the reduction from $\oplus$IS$(1, |O|)$ to $\oplus r$-PINNEDHOMSTOH by showing that

$$Z_{1,|O|}(G) \equiv \big|\mathrm{HomPin}(G_\Gamma, H, p)\big| \pmod 2. \tag{3}$$

The pinning function p pins every H-vertex in G_Γ to its own orbit. Therefore, Lemma 8.5 shows that the restriction of ϕ to $V(H)$ (which we denote $\phi|_{V(H)}$) is an automorphism of H. For $\pi \in \mathrm{Aut}(H)$, let $\Phi_\pi = \{\phi \in \mathrm{HomPin}(G_\Gamma, H, p) \mid \phi|_{V(H)} = \pi\}$. For any automorphisms π and π' of H, $|\Phi_\pi| = |\Phi_{\pi'}|$. Thus,

$$\big|\mathrm{HomPin}(G_\Gamma, H, p)\big| \equiv \big|\mathrm{Aut}(H)\big| \cdot |\Phi_{\mathrm{id}}| \pmod 2,$$

where id denotes the identity permutation. Since H is involution-free, Cauchy's Group Theorem guarantees that $\big|\mathrm{Aut}(H)\big|$ is odd [McKay 1959]. Thus,

$$\big|\mathrm{HomPin}(G_\Gamma, H, p)\big| \equiv |\Phi_{\mathrm{id}}| \pmod 2.$$

For every $\phi \in \Phi_{\mathrm{id}}$, $\phi(s) = s$ so, since $\Gamma_H(s) = O \cup \{i\} \cup K$, every G-vertex v satisfies $\phi(v) \in O \cup \{i\} \cup K$. Let $\Phi'_{\mathrm{id}} = \{\phi \in \Phi_{\mathrm{id}} \mid \forall v \in V(G), \phi(v) \in O \cup \{i\}\}$. Consider the decomposition

$$\Phi_{\mathrm{id}} = \bigcup_{\rho \colon V(G) \to V(H)} \{\phi \in \Phi_{\mathrm{id}} \mid \phi|_{V(G)} = \rho\}.$$

If $\rho(v) = u \in K$ for some $v \in V(G)$, then $\big|\{\phi \in \Phi_{\mathrm{id}} \mid \phi|_{V(G)} = \rho\}\big|$ is even. This is because the definition of the hardness gadget means there are an even number of $k(u)$-walks from $w(u)$ to u in H so there are an even number of homomorphisms $\rho' \colon P_{v, w(u)} \to H$ with $\rho'(v) = u$ and $\rho'(w(u)) = w(u)$. Thus, $|\Phi_{\mathrm{id}}| \equiv \big|\Phi'_{\mathrm{id}}\big| \pmod 2$ so

$$\big|\mathrm{HomPin}(G_\Gamma, H, p)\big| \equiv \big|\Phi'_{\mathrm{id}}\big| \pmod 2.$$

Finally, let $\Phi = \{\phi \in \Phi'_{\mathrm{id}} \mid \forall e = (x, y) \in E, \phi(x) \in O \text{ or } \phi(y) \in O\}$. Once again, the definition of the hardness gadget ensures that $|\Phi'_{\mathrm{id}}| \equiv |\Phi| \pmod 2$ because, the even number of $(1 + \beta)$-walks from i to t in H guarantees an even number of homomorphisms with $\phi(x) = \phi(y) = i$. So we have shown that $\big|\mathrm{HomPin}(G_\Gamma, H, p)\big| \equiv |\Phi| \pmod 2$. We will conclude the proof of (3) by showing that $|\Phi| \equiv Z_{1,|O|}(G) \pmod 2$.

Let Ψ be the set of functions $\pi \colon V(G) \to O \cup \{i\}$ such that $\pi^{-1}(i)$ is an independent set of G. Now $Z_{1,|O|}(G) \equiv |\Psi| \pmod 2$ so it will suffice to show $|\Psi| \equiv |\Phi| \pmod 2$. To do this, note that $\Phi = \bigcup_{\pi \in \Psi} \{\phi \in \Phi_{\mathrm{id}} \mid \phi|_{V(G)} = \pi\}$. So it suffices to show that, for every $\pi \in \Psi$, $|\{\phi \in \Phi_{\mathrm{id}} \mid \phi|_{V(G)} = \pi\}|$ is odd. This follows from the definition of the hardness gadget. Item 2 in the definition ensures that for each edge $e = (x, y)$, there are an odd

number of ways to extend π to v_e and $P_{t,e}$. Item 4 ensures that there are an odd number of ways to extend π to the internal vertices of the paths $P_{x,u}$ and $P_{y,u}$ for $u \in K$. □

We can now prove our main result.

THEOREM 1.6. *Let H be a simple graph in which every edge belongs to at most one cycle. If the involution-free reduction of H has at most one vertex, then $\oplus$HOMSTOH is solvable in polynomial time. Otherwise, $\oplus$HOMSTOH is complete for $\oplus$P with respect to polynomial-time Turing reductions.*

PROOF. Let H' be the involution-free reduction of H. If H' has at most one vertex, then $\oplus$HOMSTOH' is trivially solvable in polynomial time. By Lemma 1.1, every graph G satisfies

$$\big|\mathrm{Hom}(G,H)\big| \equiv \big|\mathrm{Hom}(G,H')\big| \pmod 2, \tag{4}$$

so $\oplus$HOMSTOH is also solvable in polynomial time.

If H' has more than one vertex, then some component H_1 of H' has more than one vertex (since H' is involution-free). Also, H_1 is involution-free. Since H_1 is an induced subgraph of H, it is a cactus graph. By Theorems 7.3 and 8.7, $\oplus$HOMSTOH_1 is $\oplus$P-hard. By Lemma 1.3, $\oplus$HOMSTOH' is $\oplus$P-hard. But (4) gives a reduction from $\oplus$HOMSTOH' to $\oplus$HOMSTOH, so $\oplus$HOMSTOH is also $\oplus$P-hard. □

REFERENCES

Ben-Moshe, B., Bhattacharya, B. K., Shi, Q., and Tamir, A. 2007. Efficient algorithms for center problems in cactus networks. *Theor. Comput. Sci. 378*, 3, 237–252.

Ben-Moshe, B., Dvir, A., Segal, M., and Tamir, A. 2012. Centdian computation in cactus graphs. *J. Graph Algor. Appl. 16*, 2, 199–224.

Bulatov, A. A. and Grohe, M. 2005. The complexity of partition functions. *Theor. Comput. Sci. 348*, 2–3, 148–186.

Cai, J.-Y., Chen, X., and Lu, P. 2010. Graph homomorphisms with complex values: a dichotomy theorem. In *Proceedings of ICALP (1)*. 275–286.

Creignou, N. and Hermann, M. 1996. Complexity of generalized satisfiability counting problems. *Inform. Comput. 125*, 1, 1–12.

Dyer, M. E., Goldberg, L. A., and Jerrum, M. 2009. The complexity of weighted Boolean #CSP. *SIAM J. Comput. 38*, 5, 1970–1986.

Dyer, M. E. and Greenhill, C. S. 2000. The complexity of counting graph homomorphisms. *Random Struct. Algor. 17*, 3–4, 260–289.

Faben, J. 2008. The complexity of counting solutions to generalised satisfiability problems modulo k. *CoRR abs/0809.1836*.

Faben, J. 2012. The complexity of modular counting in constraint satisfaction problems. Ph.D. Dissertation, Queen Mary, University of London.

Faben, J. and Jerrum, M. 2013. The complexity of parity graph homomorphism: an initial investigation. *CoRR abs/1309.4033*.

Goldberg, L. A., Grohe, M., Jerrum, M., and Thurley, M. 2010. A complexity dichotomy for partition functions with mixed signs. *SIAM J. Comput. 39*, 7, 3336–3402.

Goldschlager, L. M. and Parberry, I. 1986. On the construction of parallel computers from various bases of Boolean functions. *Theor. Comput. Sci. 43*, 43–58.

Guo, H., Huang, S., Lu, P., and Xia, M. 2011. The complexity of weighted Boolean #CSP modulo k. In *Proceedings of STACS*. 249–260.

Guo, H., Lu, P., and Valiant, L. G. 2013. The complexity of symmetric Boolean parity Holant problems. *SIAM J. Comput. 42*, 1, 324–356.

Harary, F. and Uhlenbeck, G. E. 1953. On the number of Husimi trees. I. *Proc. Nat. Acad. Sci. U. S. A. 39*, 315–322.

Hell, P. and Nešetřil, J. 1990. On the complexity of H-coloring. *J. Comb. Theory, Ser. B 48*, 1, 92–110.

Jordan, C. 1869. Sur les assemblages de lignes. *J. Reine Angew. Math. 70*, 185–190.

Lovász, L. 1967. Operations with structures. *Acta Math. Acad. Sci. Hungar. 18*, 321–328.

McKay, J. H. 1959. Another proof of Cauchy's group theorem. *Amer. Math. Monthly 66*, 119.

Papadimitriou, C. H. and Zachos, S. 1982. Two remarks on the power of counting. In *Proceedings of the 6th GI-Conference on Theoretical Computer Science*. Springer-Verlag, 269–276.

Paten, B., Diekhans, M., Earl, D., John, J. S., Ma, J., Suh, B. B., and Haussler, D. 2011. Cactus graphs for genome comparisons. *J. Comput. Biol. 18*, 3, 469–481.

Toda, S. 1991. PP is as hard as the polynomial-time hierarchy. *SIAM J. Comput. 20*, 5, 865–877.

Valiant, L. G. 2006. Accidental algorithms. In *Proceedings of FOCS*. 509–517.