

ON THE COMPLEXITY OF TORUS KNOT RECOGNITION

JOHN A. BALDWIN AND STEVEN SIVEK

ABSTRACT. We show that the problem of recognizing that a knot diagram represents a specific torus knot, or any torus knot at all, is in the complexity class $\text{NP} \cap \text{co-NP}$, assuming the generalized Riemann hypothesis. We also show that satellite knot detection is in NP under the same assumption and that cabled knot detection and composite knot detection are unconditionally in NP . Our algorithms are based on recent work of Kuperberg and of Lackenby on detecting knottedness.

1. INTRODUCTION

According to Thurston [Thu82], nontrivial knots in S^3 fall into one of three categories: torus knots, satellite knots, and hyperbolic knots. Our goal in this paper is to study the computational complexity of the recognition problem for each of these categories and for torus knots in particular.

Algorithms for unknot recognition have been studied for some time. This problem was first shown to be decidable by Haken [Hak61], using an algorithm based on the theory of normal surfaces. Hass, Lagarias, and Pippenger [HLP99] proved that the unknot recognition problem is in NP : this means that given a knot diagram, if the knot is unknotted, then there is a certificate which can be used to prove this in polynomial time. Other proofs come from work of Agol-Hass-Thurston [AHT06], who showed that determining if a knot in any 3-manifold has genus at most g is NP -complete, and from Ivanov [Iva08] as a corollary of his result that recognizing $S^1 \times D^2$ (among other 3-manifolds) is in NP .

More recently, unknot recognition has also been shown to be in co-NP , meaning that given a diagram which does *not* represent the unknot, there is a certificate which can be used to verify its knottedness in polynomial time with respect to the crossing number. A proof of this was first announced by Agol in 2002 but not published, and later Kuperberg [Kup14] proved it assuming the generalized Riemann hypothesis (GRH). Lackenby [Lac16] gave the first unconditional proof by showing that the knot genus problem in S^3 , and more generally the problem of determining the Thurston norm of a homology class in many 3-manifolds, is in NP . Thus

$$\text{UNKNOT} \in \text{NP} \cap \text{co-NP}.$$

It is still unknown whether unknot recognition is in P .

Received by the editors June 16, 2017, and, in revised form, September 6, 2017 and September 9, 2017.

2010 *Mathematics Subject Classification.* Primary 57M25; Secondary 68Q17.

The first author was supported by NSF Grant DMS-1406383 and NSF CAREER Grant DMS-1454865.

The second author was supported by the Max Planck Institute for Mathematics during some of the period in which this paper was completed.

Little else seems to be known about the complexity of other knot recognition problems. There are algorithms which can decide whether two knots are isotopic, due to work of Haken [Hak62], Hemion [Hem79], and Matveev [Mat03]; this also follows from an explicit (though enormous) upper bound of Coward and Lackenby [CL14] on the number of Reidemeister moves needed to convert one knot diagram to the other. For the unknot, this bound can be improved to a polynomial in the crossing number [Lac15], giving yet another proof that UNKNOT \in NP. We prove results about the complexity of recognizing any torus knot, as well as detecting whether a knot is a torus knot, a satellite, hyperbolic, cabled, or a connected sum, as follows.

Theorem 1.1. *The torus knot recognition problem is in $\text{NP} \cap \text{co-NP}$, assuming GRH. Moreover, for any fixed torus knot $T_{r,s}$, the $T_{r,s}$ recognition problem is also in $\text{NP} \cap \text{co-NP}$, assuming GRH.*

Remark 1.2. The claim that TORUS-KNOT \in NP is proved unconditionally in Theorem 4.3, so only the membership in co-NP requires GRH. The same is true for the $T_{r,s}$ recognition problem.

Theorem 1.3. *The satellite knot recognition problem is in NP, assuming GRH.*

Corollary 1.4. *The hyperbolic knot recognition problem is in co-NP, assuming GRH.*

Proof. We can certify that a knot diagram does not represent a hyperbolic knot by providing a certificate that it is either an unknot, a torus knot, or a satellite knot, since all three recognition problems are in NP (assuming GRH in the case of a satellite knot). \square

Theorem 1.5. *The cabled knot and composite knot recognition problems are in NP.*

Our proofs of Theorems 1.1 and 1.3 (which appears later as Theorem 6.4) combine aspects of both Kuperberg's and Lackenby's proofs that UNKNOT \in co-NP. In order to recognize a torus knot, a cabled knot, a composite knot, or a satellite knot, we must decompose the knot exterior along essential annuli or tori, certify the incompressibility of the tori in the latter case, and efficiently triangulate what remains; all of this is accomplished in [Lac16]. In order to certify a torus knot, we must then check that what remains is a pair of solid tori, and this can be certified by work of Ivanov [Iva08]. Similarly, for Theorem 1.5 (a combination of Theorems 7.2 and 7.3) we must certify that some of the components are nontrivial knot complements.

The part where Kuperberg's techniques, and hence GRH, play a role in the certification of satellite knots is the verification that the incompressible tori are not boundary parallel. For this we need to check that some component of their complement has boundary $T^2 \sqcup T^2$ but is not $T^2 \times I$, which we verify using the following result.

Theorem 1.6 (Theorem 6.2). *Let $P \subset S^1 \times D^2$ be a knot. There is a representation*

$$\pi_1((S^1 \times D^2) \setminus P) \rightarrow \text{SL}_2(\mathbb{C})$$

with nonabelian image if and only if P is not isotopic to a core of the solid torus.

Theorem 1.6 is analogous to the theorem of Kronheimer and Mrowka [KM04] that nontrivial knots in S^3 admit nonabelian $SU(2)$ representations, which Kuperberg used to certify knottedness. (Our proof relies on recent work of Zentner [Zen18], which in turn depends on [KM04].) In both cases, these representations are complex points of algebraic varieties defined over \mathbb{Z} , and the use of GRH allows Kuperberg and us to assert that these varieties also have \mathbb{F}_p -points where p is a reasonably small prime. Our certificate that some component is not $T^2 \times I$ is then a nonabelian $SL_2(\mathbb{F}_p)$ representation of its fundamental group.

The proof that $TORUS\text{-}KNOT \in \text{co-NP}$ assuming GRH follows similar lines and in fact makes use of Theorem 1.3. We have already shown how to certify that a nontorus knot K is a satellite knot, but it might be hyperbolic instead. We use the fact that the peripheral element $\mu^{rs}\lambda$ belongs to the center of the knot group of the torus knot $T_{r,s}$, whereas nontorus knots have trivial center [BZ66]. We can therefore certify that a knot is not $T_{r,s}$ by finding an $SL_2(\mathbb{F}_p)$ representation ρ of its knot group for which $\rho(\mu^{rs}\lambda)$ is not in the center of the image. Theorem 5.3 asserts that hyperbolic knots admit such certificates: we can find $SL_2(\mathbb{C})$ representations of this form, e.g. any faithful representation, and then the same appeal to GRH provides an $SL_2(\mathbb{F}_p)$ representation as well.

The above argument relies on the specific pair (r, s) , but this turns out to not be a problem if we wish to certify that an n -crossing diagram D does not represent any torus knot at all, since D can only represent $T_{r,s}$ if $|rs| < 3n$ (see Lemma 2.1). We thus need only rule out at most $O(n \log n)$ torus knots $T_{r,s}$ to conclude that D does not represent any torus knot. In fact, given a polynomial-time method to distinguish any two distinct torus knots (see Lemma 2.2 and Proposition 2.6), this observation shows that the two halves of Theorem 1.1 are equivalent: the torus knot recognition problem is in NP if and only if each $T_{r,s}$ recognition problem is in NP, and likewise for co-NP.

Finally, in order to certify that a knot is cabled or composite, after decomposing along an essential annulus we must verify that one or both of the remaining components are nontrivial knot complements rather than solid tori. In this case we can use Lackenby's work [Lac16, Theorem 1.5] to certify that they have nonzero Thurston norm, and this shows that they are not solid tori as needed.

Organization. In Section 2 we show that the Alexander polynomial and signature uniquely determine each torus knot among the set of all torus knots and that they can be computed in polynomial time. After a review of some facts about normal surfaces in Section 3, Section 4 proves half of Theorem 1.1, namely, that the torus knot recognition problem is in NP. Section 5 shows how to certify that hyperbolic knots are not torus knots; we explain in detail the role played by representation varieties and GRH, following [Kup14]. In Section 6 we combine techniques from Sections 4 and 5 to prove Theorem 1.3 and complete the proof of Theorem 1.1. Finally, in Section 7 we prove Theorem 1.5, showing that the cable and composite knot recognition problems are also in NP.

2. ALEXANDER POLYNOMIALS AND SIGNATURES OF TORUS KNOTS

In this section we show that two torus knots are isotopic if and only if they have the same Alexander polynomial and signature and that given a diagram for K there is a polynomial time algorithm to either find the unique torus knot T such that $\Delta_K(t) = \Delta_T(t)$ and $\sigma(K) = \sigma(T)$ or determine that T does not exist.

This will imply that the two claims of Theorem 1.1 are equivalent, namely, that TORUS-KNOT is in $\text{NP} \cap \text{co-NP}$ if and only if the $T_{r,s}$ recognition problem is for each pair r, s because of the following bound.

Lemma 2.1. *If $\Delta_K(t) = \Delta_{T_{r,s}}(t)$ for some integers $r > s \geq 2$, then $rs < 3 \text{cr}(K)$ where cr denotes crossing number.*

Proof. To see this, we use the well-known fact that $2 \deg(\Delta_K(t)) \leq \text{cr}(K)$ (see Exercise 4 of [CF63, Chapter VIII]), which in this case gives $(r - 1)(s - 1) \leq \text{cr}(K)$. Combining $rs \leq \text{cr}(K) + r + s - 1$ with $r + s \leq \frac{1}{2}rs + 2$ (which is equivalent to $(r - 2)(s - 2) \geq 0$) gives $rs \leq \text{cr}(K) + \frac{1}{2}rs + 1$ or $rs \leq 2 \text{cr}(K) + 2$. But K is nontrivial since $\Delta_K(t) \neq 1$, so its crossing number is at least 3, and hence the right-hand side is less than $3 \text{cr}(K)$. \square

As explained in the introduction, Lemma 2.1 reduces the torus knot recognition problem to the collection of $T_{r,s}$ recognition problems, since we can just check that a given n -crossing diagram does or does not represent $T_{r,s}$ for each pair of coprime integers (r, s) with $|r| > s \geq 2$ and $|rs| < 3n$. There are only $O(n \log n)$ such pairs, since for each value of r there are at most $\frac{3n}{|r|}$ possible values of s , so if each one can be checked individually in polynomial time, then so can all of them.

Lemma 2.2. *If K and K' are torus knots with the same Alexander polynomial and signature, then K is isotopic to K' .*

Proof. We first claim that K is determined up to chirality by its Alexander polynomial. Supposing that $K = T_{r,s}$ for some relatively prime $r, s \geq 2$, it is well-known (see e.g. [Lic97]) that $T_{r,s}$ has genus $g = \frac{(r-1)(s-1)}{2}$ and Alexander polynomial

$$\Delta_K(t) = \frac{1}{t^g} \frac{(t^{rs} - 1)(t - 1)}{(t^r - 1)(t^s - 1)},$$

whose leading term is t^g . Thus $\Delta_K(t)$ determines both rs , since the least value of $\theta > 0$ for which $\Delta_K(e^{i\theta}) = 0$ is $\theta = \frac{2\pi}{rs}$, and $(r - 1)(s - 1)$, as twice the degree of its leading term. From these we can deduce the value of

$$r + s = rs - (r - 1)(s - 1) + 1$$

as well, and then r and s are uniquely determined as the roots of $x^2 - (r + s)x + rs$.

The Alexander polynomial does not distinguish between a torus knot $T_{r,s}$ and its mirror $T_{-r,s}$, but the signature does; we adopt the sign convention for which the right-handed trefoil has signature -2 . Rudolph [Rud82] showed that braid-positive knots have negative signature, so if K is a torus knot with $\Delta_K(t) = \Delta_{T_{r,s}}(t)$ for some $r, s \geq 2$, then it follows that $K = T_{r,s}$ if $\sigma(K) < 0$ and $K = T_{-r,s}$ if $\sigma(K) > 0$. \square

Here and throughout the rest of this paper, we write “ $y = \text{poly}(x_1, \dots, x_n)$ ” to indicate that the value of y is bounded above by some fixed polynomial in x_1 through x_n .

Since we are using the Alexander polynomial and signature to distinguish torus knots, we need to know that they can be computed from a diagram D with n crossings in $\text{poly}(n)$ time. We first recall some facts from computational algebra. Given a polynomial $f \in \mathbb{Z}[t]$, we will write $\|f\|_\infty$ to denote the largest absolute value of any of its coefficients.

Lemma 2.3. *Let A be a $k \times k$ matrix with entries $a_{ij} \in \mathbb{Z}[t]$, each of which has degree at most $d \geq 1$ and satisfies $\|a_{ij}\|_\infty \leq C$ for some constant C . Then $\det(A)$ can be computed in $\text{poly}(dk, \log C)$ time.*

Proof. For each $i = 0, 1, \dots, dk$, we let $A_i = A|_{t=i}$ denote the matrix obtained from A by substituting $t = i$; then each entry of A_i has absolute value at most

$$(d + 1)Ci^d \leq (d + 1)C(dk)^d.$$

The determinant of a $k \times k$ integer matrix with all entries between $-C'$ and C' can be computed in $\text{poly}(k, \log C')$ time; see e.g. [vzGG99, Theorem 5.12]. Thus $\det(A_i)$ can be computed in $\text{poly}(k, \log((d + 1)C(dk)^d)) = \text{poly}(dk, \log C)$ time. Hadamard’s inequality [vzGG99, Theorem 16.6] says that

$$|\det(A_i)| \leq k^{k/2}((d + 1)Ci^d)^k,$$

so that $\log |\det(A_i)| = O(dk \log dk)$ for $0 \leq i \leq dk$.

Since $\det(A)$ is a polynomial $f(t)$ of degree at most dk , it is determined by the values $f(i) = \det(A_i)$ for $i = 0, \dots, dk$. We can compute each of these in a total of $\text{poly}(dk, \log(C))$ time, and then we reconstruct $\det(A) = f(t)$ by Lagrange interpolation, using a total of $O((dk)^3)$ arithmetic operations on integers $\det(A_i)$ with $O(dk \log dk)$ digits each. □

Lemma 2.3 implies that the characteristic polynomial of a $k \times k$ integer matrix A with entries between $-C$ and C can be computed as $\det(tI - A)$ in $\text{poly}(k, \log C)$ time.

Lemma 2.4. *Let A be a symmetric $k \times k$ matrix with integer entries between $-C$ and C . Then there is an algorithm which computes the signature of A in $\text{poly}(k, \log C)$ time.*

Proof. By hypothesis, the eigenvalues of A are all real. We can compute the characteristic polynomial

$$f(\lambda) = \det(\lambda I - A) = \lambda^k + a_1\lambda^{k-1} + \dots + a_{k-1}\lambda + a_k$$

in time $\text{poly}(k, \log C)$. Dividing by a power of λ so that the constant term is nonzero, we can assume that all of the roots of f (which are now the nonzero eigenvalues of M) are nonzero.

We let k_+ denote the number of sign changes in the sequence $a_0 = 1, a_1, \dots, a_k$, meaning the number of indices i such that $a_i a_j < 0$ for some $j > i$ and all intermediate terms a_{i+1}, \dots, a_{j-1} are zero; likewise we let k_- denote the number of sign changes in $(-1)^k a_0, (-1)^{k-1} a_1, (-1)^{k-2} a_2, \dots, a_k$. Since all k roots of $f(\lambda)$ are real and nonzero and the total number of sign changes in both sequences is easily seen to be at most k , we have

$$k = \#\{\text{positive roots}\} + \#\{\text{negative roots}\} \leq k_+ + k_- \leq k,$$

where the first inequality is Descartes’ rule of signs. These inequalities must then be equalities, so $f(\lambda)$ has exactly k_\pm roots of either sign, and thus $\text{sign}(A) = k_+ - k_-$. □

Lemma 2.5. *Let $f_1, \dots, f_k \in \mathbb{Z}[t]$ be polynomials of degree at most $d \geq 1$ and with $\|f_i\|_\infty \leq C$ for some constant C . Then $\text{gcd}(f_1, \dots, f_k)$ can be computed in $\text{poly}(k, d, \log C)$ time.*

Proof. In the case $k = 2$, we can compute $\gcd(f_1, f_2)$ in $\text{poly}(d, \log C)$ time according to [vzGG99, Theorem 6.62]. We would like to apply this algorithm repeatedly in the general case by computing $g_i := \gcd(f_1, \dots, f_i)$ as the greatest common divisor of $g_{i-1} = \gcd(f_1, \dots, f_{i-1})$ and f_i for each $i = 2, \dots, k$, but we need to ensure that the intermediate norms $\|g_{i-1}\|_\infty$ stay reasonably small.

To that end, suppose we have polynomials $p, q, r \in \mathbb{Z}[t]$ of degrees $a \geq 1, b, c$, where qr divides p and hence $b + c \leq a$. Then Mignotte’s bound [vzGG99, Corollary 6.33] says that

$$\|q\|_\infty \|r\|_\infty \leq (a + 1)^{1/2} 2^{b+c} \|p\|_\infty.$$

In the above case, since g_{i-1} divides f_1 , we have $\deg(g_{i-1}) \leq d$ and $\|g_{i-1}\|_\infty \leq (d + 1)^{1/2} 2^d C$, and so we can compute $g_i = \gcd(g_{i-1}, f_i)$ in

$$\text{poly}\left(d, \log\left((d + 1)^{1/2} 2^d C\right)\right) = \text{poly}(d, \log C)$$

time. This is independent of i , so after k steps we can determine g_k in the claimed time. □

Proposition 2.6. *Given a diagram D with n crossings representing the knot K , there is an algorithm which computes $\Delta_K(t)$ and $\sigma(K)$ in time $\text{poly}(n)$.*

Proof. In order to compute $\Delta_K(t)$, we take the Wirtinger presentation associated to D and compute the associated $n \times n$ matrix of Fox derivatives in $O(n^2)$ time. We abelianize this to get a matrix with entries in $\mathbb{Z}[t^{\pm 1}]$, and then $\Delta_K(t)$ is the greatest common divisor of the determinants of the $(n - 1) \times (n - 1)$ minors of this matrix. We multiply the minors by a power of t so their entries lie in $\mathbb{Z}[t]$ and compute their determinants using Lemma 2.3. The greatest common divisor can then be computed in time $\text{poly}(n)$ by Lemma 2.5, since all of the coefficients and degrees of polynomials which occur along the way have length at most $\text{poly}(n)$. We then normalize $\Delta_K(t)$ so that it is a symmetric Laurent polynomial and $\Delta_K(1) = 1$.

For $\sigma(K)$, we use Gordon and Litherland’s signature formula [GL78], which says that $\sigma(K) = \text{sign}(G) - \mu$, where G is a Goeritz matrix for D and μ is a certain correction term. To construct these, we orient D and choose a checkerboard coloring of D , label the white regions X_0, \dots, X_k , and assign each crossing c a sign $\eta(c) = \pm 1$ and a type (I or II) as shown below:



We then build a $(k + 1) \times (k + 1)$ matrix G' whose off-diagonal entries g_{ij} , $0 \leq i, j \leq k$, are defined as $-\sum \eta(c)$ over all crossings c incident to both X_i and X_j and for which $g_{ii} = -\sum_{j \neq i} g_{ij}$. The Goeritz matrix G is the $k \times k$ submatrix $(g_{ij})_{1 \leq i, j \leq k}$, and then we let $\mu = \sum \eta(c)$ over all type II crossings c .

From the construction we see that $k \leq n$: forgetting the crossing information turns D into a planar 4-valent graph with n vertices and hence $2n$ edges and $2n - n + 2 = n + 2$ regions in its complement, so at most $n + 1$ are white. The entries of G have magnitude at most n , since each $|g_{ij}|$ or $|g_{ii}|$ is bounded by the number of crossings incident to X_i , and clearly $|\mu| \leq n$ as well. Both G and μ are easily computable in polynomial time, and then the signature $\text{sign}(G)$ is

computable in $\text{poly}(k, \log n) = \text{poly}(n)$ time as well by Lemma 2.4, hence so is $\sigma(K) = \text{sign}(G) - \mu$. \square

Proposition 2.7. *Given a diagram D for a knot K , there is an algorithm which returns the unique pair (r, s) of coprime integers with $|r| > s \geq 2$ such that $\Delta_K(t) = \Delta_{T_{r,s}}(t)$ and $\sigma(K) = \sigma(T_{r,s})$ if such a pair exists, and the empty set otherwise. If D has n crossings, then this algorithm runs in time $\text{poly}(n)$.*

Proof. We use D to compute the Alexander polynomial $\Delta_K(t)$ and signature $\sigma(K)$ in $\text{poly}(n)$ time, by Proposition 2.6. If $\Delta_K(t) = \Delta_{T_{a,b}}(t)$ where $a > b \geq 2$, then $\Delta_K(t)$ has maximal degree $d = \frac{(a-1)(b-1)}{2}$. Lemma 2.1 says that $ab < 3n$, so $b < \sqrt{3n}$. Thus for each b in the range $2 \leq b < \sqrt{3n}$, we set $a = \frac{2d}{b-1} + 1$, and if this is an integer greater than b , then we compute

$$(t^a - 1)(t^b - 1)\Delta_K(t) - (t^{ab} - 1)(t - 1).$$

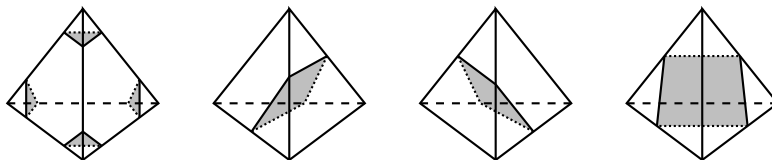
If this is zero for some such pair (a, b) , then $\Delta_K(t) = \Delta_{T_{a,b}}(t)$; and if not, then $\Delta_K(t)$ is not the Alexander polynomial of a torus knot, and so we return \emptyset . This requires $O(\sqrt{n})$ operations on polynomials of degree at most $ab < 3n$, and hence can also be done in $\text{poly}(n)$ time.

Next, assuming that $\Delta_K(t) = \Delta_{T_{a,b}}(t)$ as above, we compute $\sigma(T_{a,b})$ using Litherland’s formula [Lit79]. This requires only $O(ab)$ operations on integers of size at most $O(ab)$; we note that $O(ab)$ is in fact $O(n)$ if we reach this step, since $ab < 3n$. If $\sigma(K) = \pm\sigma(T_{a,b})$, then we return $(r, s) = (\pm a, b)$, and otherwise we return \emptyset . \square

3. NORMAL SURFACES AND ESSENTIAL ANNULI

Our recognition algorithms will rely heavily on being able to identify annuli and tori in knot complements which are essential, meaning that they are incompressible and boundary-incompressible. In this section we review key results which will allow us to do so. We first recall what it means to be a normal surface in a triangulated 3-manifold.

Let \mathcal{T} be a triangulation of a compact 3-manifold Y . A properly embedded surface $S \subset Y$ is *normal* if it intersects each tetrahedron of \mathcal{T} in a disjoint union of finitely many *elementary disks*, which are properly embedded triangles or quadrilaterals. There are seven types of elementary disks, one triangle per vertex and one quadrilateral per pair of opposite edges:



If there are t tetrahedra, then we can describe a normal surface S by a vector $v(S) \in \mathbb{Z}^{7t}$ with nonnegative coordinates, counting the number of parallel copies of each type of elementary disk in each tetrahedron. In fact, a vector $v \in \mathbb{Z}^{7t}$ describes an embedded surface if and only if its entries are nonnegative; it satisfies the *matching equations*, linear equations asserting that when we glue tetrahedra together along a pair of faces, the edges of the elementary disks in each tetrahedron

form the same pattern of line segments on either face; and at most one type of quadrilateral appears in each tetrahedron.

The set of all vectors in \mathbb{R}^{7t} satisfying the nonnegativity and matching conditions is a polyhedral cone, called the *Haken normal cone* of the triangulation. The *carrier* of a normal surface S is the minimal face $\mathcal{C}(S)$ of the Haken normal cone containing $v(S)$, and S is said to be a *vertex surface* if it is connected and two-sided and its carrier is a 1-dimensional face. We say a vertex surface S is *minimal* if $v(S)$ is not a nontrivial integral multiple of another integral point on this face. In this case there is a bound on its complexity, due to Hass, Lagarias, and Pippenger [HLP99].

Theorem 3.1 ([HLP99, Lemma 6.1]). *If S is a minimal vertex surface with respect to a triangulation \mathcal{T} with t tetrahedra, then each coordinate of $v(S) \in \mathbb{Z}^{7t}$ is at most 2^{7t-1} .*

The key fact we use to detect torus knots, cabled knots, and composite knots, proved originally by Simon [Sim73], is that a knot K lies in one of these classes if and only if its exterior $E_K = S^3 \setminus N(K)$ contains a properly embedded essential annulus. The annuli in question split E_K into two connected complements as follows:

- If K is a torus knot, then the complement is a pair of solid tori.
- If K is a cable, the complement is a solid torus and a nontrivial knot complement.
- If K is a composite knot, the complement is a pair of nontrivial knot complements.

By [BZ03, Lemma 15.26], if K is a torus knot or a cable, then every essential annulus is a cabling annulus: this means that there is a knot $K' \subset S^3$ such that K is a nonseparating curve in the torus $T = \partial N(K')$ (note that K' is unknotted if K is a torus knot), and the annulus is then the intersection $T \cap E_K$. Such annuli decompose E_K into the exterior $E_{K'}$ and the solid torus $N(K')$. If instead K is a connected sum, then every essential annulus has meridional boundary slope and thus decomposes E_K into a pair of nontrivial knot complements.

Essential annuli in the exterior of K are always isotopic to normal surfaces in any given triangulation of E_K by the following theorem; we take the statement from Jaco and Rubinstein [JR89, Theorem 2.4], who attribute it to Haken [Hak68].

Theorem 3.2. *Let S be a properly embedded, essential surface in an irreducible 3-manifold Y with incompressible boundary. If \mathcal{T} is any triangulation of Y and $\mathcal{T}^{(1)}$ its 1-skeleton, then S is isotopic to a normal surface S' of least weight, meaning that $\#(S' \cap \mathcal{T}^{(1)})$ is minimized among normal surfaces in its isotopy class.*

Theorem 3.2 is true for arbitrary essential surfaces, but for annuli we know significantly more: by work of Jaco and Tollefson [JT95], we can find essential annuli as above which are not just normal but vertex surfaces. The following result holds for annuli and tori in any orientable, compact, irreducible 3-manifold with incompressible boundary, though we only need it for annuli in knot complements.

Theorem 3.3 ([JT95, Corollary 6.8]). *Let A be a normal, two-sided, essential annulus of least weight in the exterior E_K of a nontrivial knot $K \subset S^3$. Then every vertex surface in the carrier of A is either an essential annulus or an essential torus.*

We combine all of these results to guarantee the existence of essential annuli with bounded weight in the complements of torus knots, cables, and connected sums of knots.

Proposition 3.4. *Let $K \subset S^3$ be a nontrivial knot, and let \mathcal{T} be a triangulation of its exterior $E_K = S^3 \setminus N(K)$, with t tetrahedra. If K is a torus knot, cable knot, or composite knot, then there is an essential annulus $A \subset E_K$ which is normal with respect to \mathcal{T} of total weight*

$$\|v(A)\|_{L^1} \leq 7t \cdot 2^{7t}.$$

The complement $E_K \setminus N(A)$ has two connected components, which are either a pair of solid tori, a solid torus and a nontrivial knot complement, or a pair of nontrivial knot complements depending on whether K is a torus, a cable knot, or a composite knot respectively.

Proof. By hypothesis E_K contains an essential annulus which is isotopic to a normal annulus A_0 of least weight by Theorem 3.2. Theorem 3.3 says that every vertex surface in $\mathcal{C}(A_0)$ is an essential annulus or an essential torus, and since $v(A_0)$ is a linear combination of the normal coordinates of these vertex surfaces, they cannot all be tori or else A_0 would not have nonempty boundary in ∂E_K .

We conclude that there is an essential normal annulus A which is a vertex surface, and since it is connected it must be either minimal or twice a minimal surface (which is then nonorientable, hence a Möbius band). The bound of Theorem 3.1 says that each of the $7t$ coordinates of $v(A)$ is then at most 2^{7t} , so that $\|v(A)\|_{L^1} \leq 7t \cdot 2^{7t}$ as claimed. Finally, the description of $E_K \setminus N(A)$ follows from [BZ03, Lemma 15.26] as described above. \square

Given normal surface coordinates for a properly embedded annulus A , the following lemma will help us verify that A is incompressible.

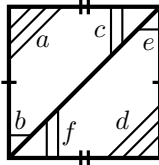
Lemma 3.5. *Let A be a properly embedded annulus in the exterior $E_K = S^3 \setminus N(K)$ of a nontrivial knot. The map $\pi_1(A) \rightarrow \pi_1(E_K)$ is injective if and only if each component of ∂A represents a nontrivial class in $H_1(\partial E_K)$.*

Proof. We note that the two components of ∂A represent the same class in $\pi_1(E_K)$, since A provides a homotopy between them. The map $\pi_1(\partial E_K) \rightarrow \pi_1(E_K)$ is injective since K is nontrivial, so the components must then also be identical in $\pi_1(\partial E_K) \cong H_1(\partial E_K)$.

Let γ be a component of ∂A . Then γ generates $\pi_1(A) \cong \mathbb{Z}$, so every class in $\pi_1(A)$ is represented by a curve γ^n in ∂E_K , and thus the map $\pi_1(A) \rightarrow \pi_1(E_K)$ factors as $\langle \gamma \rangle \rightarrow \pi_1(\partial E_K) \rightarrow \pi_1(E_K)$. Since the map $\pi_1(\partial E_K) \rightarrow \pi_1(E_K)$ is injective, we see that $\pi_1(A) \rightarrow \pi_1(E_K)$ is injective if and only if $\langle \gamma \rangle \rightarrow \pi_1(\partial E_K)$ is as well. But $\pi_1(\partial E_K) \cong H_1(\partial E_K)$ is torsion-free, so the latter map is injective if and only if $[\gamma]$ is a nonzero class in $H_1(\partial E_K)$. \square

We explain how to check that the criteria of Lemma 3.5 are satisfied. If E_K has a triangulation \mathcal{T} restricting to a one-vertex triangulation of the boundary torus and A is a properly embedded normal annulus A in E_K , then ∂A is naturally described as a normal curve in the surface ∂E_K with respect to $\mathcal{T}|_{\partial E_K}$. Normal curves in this triangulation were studied by Jaco and Sedgwick [JS03, Theorem 3.6]; they are described by three nonnegative integers per triangle, counting the number of arcs

around each vertex.



A normal curve satisfies one matching equation per edge of the triangulation, namely,

$$a + b = d + e, \quad a + c = d + f, \quad b + c = e + f.$$

These are equivalent to $a = d$, $b = e$, and $c = f$, so the curve is uniquely characterized by the triple (a, b, c) . Two curves in this triangulation are normally isotopic if and only if they are isotopic [JS03, Lemma 3.5], so if A is a normal annulus with boundary $\gamma_1 \cup \gamma_2$, then γ_1 is isotopic to γ_2 and so ∂A has normal coordinates of the form $(2a, 2b, 2c)$. If the γ_i are homologically nontrivial, then they each represent a primitive class since they are embedded, and hence each has odd intersection with some element of a basis of $H_1(\partial E_K; \mathbb{Z})$. In particular, they are homologically nontrivial if and only if ∂A has normal coordinates $(2a, 2b, 2c)$ with at least one of $a + b$ and $a + c$ being odd.

4. TORUS KNOT RECOGNITION IS IN NP

In this section we show how to certify that a knot diagram D represents a torus knot. We do not declare which torus knot it is, but this is unnecessary, since Proposition 2.7 allows us to determine this in polynomial time. Our certification relies on the fact that a knot $K \subset S^3$ is a torus knot if and only if there is an essential annulus A in the exterior of K whose complement is a pair of solid tori; the annulus is the intersection of the exterior with a Heegaard torus on which K lies.

Our certification is a straightforward combination of algorithms by others. After triangulating the knot complement, we present the annulus A as a normal surface with bounded weight, using Proposition 3.4; then we cut the knot complement along A and triangulate the remaining pieces using work of Lackenby [Lac16]. Finally, we certify that A is essential and that the remaining pieces are indeed solid tori using an algorithm of Ivanov [Iva08], and this verifies that we have a torus knot.

We now begin to construct the certificate in detail by producing a small triangulation of the knot exterior $E_K = S^3 \setminus N(K)$. We assume that every knot diagram has at least three crossings, since otherwise it is clearly a diagram of the unknot.

Proposition 4.1. *Let D be a diagram with n crossings of a knot K . There are a universal constant C and an algorithm which produces in $\text{poly}(n)$ time a triangulation \mathcal{T} of the exterior E_K such that \mathcal{T} has at most Cn tetrahedra and its restriction to the boundary torus ∂E_K consists of two triangles and a single vertex.*

Proof. Hass, Lagarias, and Pippenger [HLP99, Lemma 7.1] show how to triangulate S^3 with at most $440n + 2$ tetrahedra in $O(n \log n)$ time so that K lies in the 1-skeleton, and then in [HLP99, Lemma 7.2] they apply two barycentric subdivisions and remove a neighborhood of K to get a triangulation \mathcal{T}_0 of E_K with $t \leq 24^2(440n + 2)$ tetrahedra. The restriction of \mathcal{T}_0 to ∂E_K may be complicated, but following an algorithm of Lackenby [Lac16, Proposition 10.3] we can attach at most $4t$ tetrahedra to ∂E_K in $\text{poly}(t) = \text{poly}(n)$ time to reduce the number

of boundary vertices to one. The resulting triangulation \mathcal{T} of E_K has at most $5t \leq 5 \cdot 24^2(440n + 2)$ tetrahedra, so we take $C = 5 \cdot 24^2 \cdot 441$. \square

Supposing that \mathcal{T} has t tetrahedra, Proposition 3.4 provides an essential annulus $A \subset E_K$ which is normal of weight $\|v(A)\|_{L^1} \leq 7t \cdot 2^{7t}$ and which splits E_K into a pair of solid tori. In order to triangulate the complement of A in E_K , we use the following proposition, which is due to, but not explicitly stated by, Lackenby [Lac16].

Proposition 4.2. *Let M be a compact, irreducible, orientable 3-manifold with incompressible boundary, and let \mathcal{T} be a triangulation of M with t tetrahedra. If A is a properly embedded normal annulus in M with weight $w = \|v(A)\|_{L^1}$, then there is an algorithm which builds a triangulation of $M' = M \setminus N(A)$ with at most $200t$ tetrahedra in $\text{poly}(t \log(w))$ time.*

Proof. We repeat the proof of [Lac16, Theorem 11.4] verbatim. The algorithm converts \mathcal{T} into a handle structure, cuts along A , and converts the resulting handle structure back into a triangulation. This may produce at least $O(w)$ handles, but most of them are quite simple: they are 3-balls cut out by two parallel elementary disks of A inside a single handle of \mathcal{T} , and these fit into a union \mathcal{B} of I -bundles over subsurfaces of $A \sqcup A$, called “parallelity bundles”. So we triangulate the linearly many (in t) handles of $M' \setminus \mathcal{B}$, determine the topology of each component of \mathcal{B} by [Lac16, Theorem 9.3], and then use this to build a simpler triangulation of \mathcal{B} by hand which we glue to the triangulation of $M' \setminus \mathcal{B}$.

The only difference is that [Lac16, Theorem 11.4] is stated for A a union of tori, and so the base of each parallelity bundle has genus at most 1. In our setting the genus is zero since A is an annulus, so the same estimates as in Lackenby’s original proof still hold. \square

We combine the above results to conclude that TORUS-KNOT is in NP.

Theorem 4.3. *Given a diagram D with n crossings of a knot K , if K is a torus knot, then there is a certificate which can be used to verify this in $\text{poly}(n)$ time.*

Proof. Using Proposition 4.1, we produce a triangulation \mathcal{T} of the exterior $E_K = S^3 \setminus N(K)$ with $t = O(n)$ tetrahedra. Given a properly embedded normal annulus $A \subset E_K$, we can use Proposition 4.2 to triangulate its complement with $O(n)$ tetrahedra in polynomial time as well. Our certificate therefore consists of:

- (1) normal coordinates $v(A)$ for an essential annulus A in E_K , with $\|v(A)\| \leq 7t \cdot 2^{7t}$;
- (2) certificates that the two triangulated components of $E_K \setminus N(A)$ are both solid tori, as provided by Ivanov [Iva08, Theorem 3].

To verify the certificate, we do the following:

- (1) Verify that $\Delta_K(t) \neq 1$, as described in Proposition 2.6.
- (2) Verify that A is an annulus and that the components of ∂A are homologically nontrivial in ∂E_K .
- (3) Apply Proposition 4.2 to triangulate $E_K \setminus N(A)$ and verify that it has two connected components, say M_1 and M_2 .
- (4) Verify the certificates that the given triangulations of M_1 and M_2 produce solid tori, following [Iva08].

Step (1) ensures that K is not the unknot, and hence it will help us show that A is essential. Indeed, if K is knotted, then step (2) will show that the map $\pi_1(A) \rightarrow \pi_1(E_K)$ is injective by Lemma 3.5, so it is either essential or boundary-parallel. But if A is boundary-parallel, then one component of its complement is homeomorphic to E_K , which can only be a solid torus if K is the unknot. Therefore, once we know that $E_K \setminus N(A)$ is a disjoint union of two solid tori, we can conclude that A is essential and K is indeed a torus knot. Moreover, torus knots do not have Alexander polynomial 1, so step (1) will not incorrectly eliminate any torus knots.

To verify that A is an annulus, we first check that the vector $v(A)$ solves the normal surface equations and that it produces a properly embedded surface of Euler characteristic zero with nonempty boundary. We can then use Agol-Hass-Thurston's orbit-counting algorithm to check in $\text{poly}(t \log \|v(A)\|_{L^1})$ time that A is connected [AHT06, Corollary 14], and we check that it is orientable by using the same algorithm to see that the surface with normal coordinates $2v(A)$ is not connected, as in [AHT06, Proof of Theorem 2]. Since A is connected and orientable with $\chi(A) = 0$ and $\partial A \neq \emptyset$, it must be an annulus, and this verification takes a total of $\text{poly}(t \log \|v(A)\|_{L^1})$ time. Similarly, we can verify that the components of ∂A are homologically nontrivial as described following Lemma 3.5 in $O(t + \log \|v(A)\|_{L^1})$ time, since we can read off the normal components of ∂A immediately once we identify the tetrahedra adjacent to ∂E_K .

To see that each of these steps can be done in $\text{poly}(n)$ time, we now observe that $t \leq Cn$, where C is a universal constant, and that $\|v(A)\|_{L^1} \leq 7t \cdot 2^{7t}$ by Proposition 3.4. Thus $\text{poly}(t \log \|v(A)\|_{L^1}) = \text{poly}(n)$, and we can construct the triangulation of $M_1 \sqcup M_2$, which has at most $200t = O(n)$ tetrahedra, in $\text{poly}(n)$ time. Finally, since M_1 and M_2 each has $O(n)$ tetrahedra we can verify their solid torus certificates in $\text{poly}(n)$ time as well. \square

5. CERTIFYING THAT HYPERBOLIC KNOTS ARE NOT TORUS KNOTS

Let D be a diagram with n crossings which represents a hyperbolic knot K . Assuming the generalized Riemann hypothesis, we will provide a certificate, verifiable in $\text{poly}(n)$ time, that K is not a torus knot. The construction of these certificates follows the same ideas as Kuperberg's certificates for knottedness [Kup14]. As in [Kup14], we need GRH to show that these certificates exist, but once they are known to exist they can be verified unconditionally. This will be a key step in the proof of Theorem 1.1, specifically the assertion that $\text{TORUS-KNOT} \in \text{co-NP}$, because it suffices to either certify that a given nontorus knot is hyperbolic or certify that it is a satellite knot; we will discuss certificates for satellite knots in Section 6.

The diagram D determines a Wirtinger presentation

$$\pi_1(S^3 \setminus K) = \langle g_1, \dots, g_n \mid r_1, \dots, r_n \rangle$$

of the knot group, in which each generator g_i is a meridian around some strand and the relations r_i all have the form $g_{m_i} g_{n_i} g_{m_i}^{-1} = g_{p_i}$ for some m_i, n_i, p_i . Using D , we fix peripheral elements $\mu = g_1$ and λ , representing a meridian and a longitude. We observe that λ can be expressed as a product of at most $2n$ of the generators g_i and their inverses: to see this, we use Seifert's algorithm to find a Seifert surface Σ consisting of some number of disks connected by n bands (one per crossing), take a parallel copy of K inside Σ , and observe that as this copy passes through each band twice it contributes a total of two generators (or their inverses) to λ .

Definition 5.1. *An uncentered certificate that D is not a diagram of a torus knot consists of:*

- (1) *a pair of relatively prime integers r, s with $|rs| < 3n$ such that K has the same Alexander polynomial and signature as $T_{r,s}$ or \emptyset if no such pair exists;*
- (2) *if we have integers r, s instead of \emptyset :*
 - *a prime p , with $\log(p) = \text{poly}(n)$;*
 - *a collection of 2×2 matrices $M_1, M_2, \dots, M_n \in \text{SL}_2(\mathbb{F}_p)$, defining a representation*

$$\rho : \pi_1(S^3 \setminus K) \rightarrow \text{SL}_2(\mathbb{F}_p)$$

by $\rho(g_i) = M_i$, such that $\rho(\mu^{rs}\lambda)\rho(g_i) \neq \rho(g_i)\rho(\mu^{rs}\lambda)$ for some i .

To verify an uncentered certificate, we do the following:

- (1) Using Proposition 2.7, check in $\text{poly}(n)$ time that the choice of (r, s) or \emptyset was made correctly. If we have \emptyset , then we stop; otherwise $|rs| < 3n$ by Lemma 2.1.
- (2) Verify that $\det(M_i) = 1$ for all i and that the M_i satisfy the relations r_1, \dots, r_n .
- (3) Compute $\rho(\mu^{rs}\lambda)$ and verify that it does not commute with some M_i .

It is mostly clear that if the certificate exists, then it can be verified in $\text{poly}(n)$ time. The only part which requires some additional thought is the computation of $\rho(\mu^{rs}\lambda)$. Since $\mu^{rs}\lambda$ can be written as a word of length at most $|rs| + 2n < 5n$ in the generators $g_1^{\pm 1}, \dots, g_n^{\pm 1}$, we can express $\rho(\mu^{rs}\lambda)$ as a product of the matrices $M_1^{\pm 1}, \dots, M_n^{\pm 1}$ of length at most $5n$, and so it can also be computed in polynomial time. We also remark that we do not actually need to verify that p is prime: even if it is not, the representation ρ still certifies that $\mu^{rs}\lambda$ is not central, which is all that matters.

Proposition 5.2. *If D has an uncentered certificate, then it is not a diagram of a torus knot.*

Proof. Suppose that D is a diagram of $T_{r,s}$. We can take the standard genus-1 Heegaard splitting of S^3 and embed $T_{r,s}$ in the Heegaard torus. Then $\pi_1(S^3 \setminus T_{r,s})$ is generated by the cores of the two genus-1 handlebodies, and $\mu^{rs}\lambda$ is a curve parallel to $T_{r,s}$ in the Heegaard torus, so it commutes with each generator. Since $\mu^{rs}\lambda$ is central, its image under any representation $\rho : \pi_1(S^3 \setminus T_{r,s}) \rightarrow \text{SL}_2(\mathbb{F}_p)$ must commute with everything in the image of ρ . \square

In contrast, we will prove that hyperbolic knots have such certificates, assuming GRH.

Theorem 5.3. *Assume the generalized Riemann hypothesis. If D is a diagram of a hyperbolic knot, then it admits an uncentered certificate.*

Remark 5.4. It is entirely possible that satellite knots also admit uncentered certificates, but we do not know a proof of this. In Section 6 we will use a different strategy to certify satellite knots.

Lemma 5.5. *Let D be a knot diagram with $n > 0$ crossings representing a knot K , and fix an integer m with $|m| < 3n$. There is an algebraic variety which is nonempty if and only if there is a representation*

$$\rho : \pi_1(S^3 \setminus K) \rightarrow \text{SL}_2(\mathbb{C})$$

such that $\rho(\mu^m \lambda)$ does not commute with some other element $\rho(g)$ of the image. Moreover, we can define such a variety using $8n$ variables and $5n + 1$ polynomials, each of which has maximum degree at most $5n + 2$ and integer coefficients bounded by 2^{5n+1} in absolute value.

Proof. We use D to construct a Wirtinger presentation

$$\pi_1(S^3 \setminus K) = \langle g_1, g_2, \dots, g_n \mid r_1, r_2, \dots, r_n \rangle,$$

in which each g_i is a meridional loop around a strand of D and each crossing produces a relation r_i of the form $g_{m_i} g_{n_i} g_{m_i}^{-1} = g_{p_i}$. We will take $\mu = g_1$ and let λ be a longitude.

We can construct the $SL_2(\mathbb{C})$ representation variety $R(K)$ from this presentation as an algebraic subset of \mathbb{C}^{4n} by using $4n$ generators a_i, b_i, c_i, d_i , packaged into matrices $M_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}$. Then $R(K)$ is defined by a total of $5n$ polynomial equations: we require that $\det(M_i) = a_i d_i - b_i c_i = 1$ for each i , and each relation r_i of the form $g_{m_i} g_{n_i} g_{m_i}^{-1} = g_{p_i}$ ($1 \leq i \leq n$) contributes four polynomial equations coming from the entries of the 2×2 matrix equation $M_{m_i} M_{n_i} = M_{p_i} M_{m_i}$.

We must now select only those representations ρ for which $\rho(\mu^m \lambda)$ does not commute with some M_i , so we first introduce some notation. As explained above, we can write λ as a word of length $l \leq 2n$ in the generators $g_1^{\pm 1}, \dots, g_n^{\pm 1}$, say $\lambda = g_{i_1}^{\epsilon_1} g_{i_2}^{\epsilon_2} \dots g_{i_l}^{\epsilon_l}$ where $\epsilon_j = \pm 1$ for each j . We will let $\epsilon = \text{sign}(m) \in \{\pm 1\}$ and write

$$A_m = (M_1^\epsilon)^{|m|} M_{i_1}^{\epsilon_1} M_{i_2}^{\epsilon_2} \dots M_{i_l}^{\epsilon_l},$$

where for any j we interpret M_j^{-1} as the matrix $\begin{pmatrix} d_j & -b_j \\ -c_j & a_j \end{pmatrix}$. This is a product of at most $|m| + l < 5n$ matrices $M_j^{\pm 1}$, so a simple induction says that its entries are sums of at most 2^{5n-1} monomials of degree at most $5n$ each in the generators a_j, b_j, c_j, d_j . Moreover, if a_j, b_j, c_j, d_j correspond to a representation $\rho \in R(K)$, then we have $A_m = \rho(\mu^m \lambda)$.

In order to select only the desired representations, we need only check that A_m does not commute with the image M_i of some generator g_i . We accomplish this by the Rabinowitsch trick, following Kuperberg [Kup14]: namely, we add another $4n$ generators t_{ijk} with $1 \leq i \leq n$ and $1 \leq j, k \leq 2$, and we add a single equation

$$\sum_{i,j,k} t_{ijk} (A_m M_i - M_i A_m)_{j,k} = 1,$$

where $(M)_{j,k}$ denotes the (j, k) th entry of the matrix M . It is clear that this equation is satisfiable for some values of the t_{ijk} if and only if $A_m M_i \neq M_i A_m$ for some i , i.e., if and only if the corresponding representation ρ satisfies $\rho(\mu^m \lambda) \rho(g_i) \neq \rho(g_i) \rho(\mu^m \lambda)$. Then every term in this equation has degree at most $5n + 2$ and integer coefficients bounded in absolute value by 2^{5n+1} , since $A_m M_i$ and $M_i A_m$ are each sums of at most 2^{5n} monomials of degree at most $5n + 1$, and so the lemma follows. □

In order to produce an $SL_2(\mathbb{F}_p)$ representation from the $SL_2(\mathbb{C})$ representation variety, we use the following theorem, which is a combination of results of Koiran [Koi96] and Lagarias-Odlyzko and Weinberger [LO77, Wei84].

Theorem 5.6 ([Kup14, Theorem 3.3]). *Let $f_1, \dots, f_m \in \mathbb{Z}[x_1, \dots, x_n]$ be non-constant integer polynomials with degree at most d and all coefficients having absolute value at most r , and suppose that the system $f_1 = f_2 = \dots = f_m = 0$ has a solution in \mathbb{C}^n . Assuming the generalized Riemann hypothesis, there is a prime p with $\log(p) = \text{poly}(n, m, \log(d), \log(r))$ such that the system has a solution in $(\mathbb{Z}/p\mathbb{Z})^n$.*

We remark that the generalized Riemann hypothesis is used in [LO77, Wei84] to provide an effective version of the Chebotarev density theorem, guaranteeing that we can take p with at most polynomially many digits. The basic result we need to assume (and which is implied by GRH) is stated as [Kup14, Theorem 3.2]; it asserts that an irreducible polynomial $h \in \mathbb{Z}[x]$ with degree d and all coefficients between $-r$ and r has a root in $\mathbb{Z}/p\mathbb{Z}$ for some prime $p = \text{poly}(d, \log r)$. Without GRH, Koiran's work [Koi96] plus the classical Chebotarev density theorem says unconditionally that we can take any p in some positive-density subset of the primes, but it does not provide a small enough bound on the minimal value of p .

Proof of Theorem 5.3. We may assume that K has the same Alexander polynomial and signature as the torus knot $T_{r,s}$, since otherwise our certificate does not require an actual $\text{SL}_2(\mathbb{F}_p)$ representation. In this case Lemma 2.1 says that $|rs| < 3n$.

Since K is hyperbolic, there is a discrete, faithful representation $\rho_0 : \pi_1(S^3 \setminus K) \rightarrow \text{SL}_2(\mathbb{C})$, as proved in [CS83, Proposition 3.1.1] and attributed to Thurston. A theorem of Burde and Zieschang [BZ66] says that $\pi_1(S^3 \setminus K)$ has trivial center since K is not a torus knot, so $\mu^{rs}\lambda$ does not commute with some element g of the knot group. But then $\rho_0(\mu^{rs}\lambda)$ does not commute with $\rho_0(g)$ since ρ_0 is faithful, so if we set $m = rs$, then the variety of Lemma 5.5 is nonempty. We apply Theorem 5.6 to conclude that the system of equations defining this variety has a solution mod p , where

$$\log(p) = \text{poly}(8n, 5n + 1, \log(5n + 2), \log(2^{5n+1})) = \text{poly}(n).$$

This solution gives the desired prime p and representation $\pi_1(S^3 \setminus K) \rightarrow \text{SL}_2(\mathbb{F}_p)$. \square

6. SATELLITE KNOT RECOGNITION IS IN NP

A knot $K \subset S^3$ is a satellite knot if and only if its exterior contains some incompressible, non-boundary-parallel tori. In this case the JSJ decomposition [JS79, Joh79] of the knot exterior is nontrivial, with $E_K = S^3 \setminus N(K)$ being cut along such incompressible tori into atoroidal and Seifert fibered pieces. In particular, we can certify that a K is a satellite knot by providing the JSJ tori and efficiently checking that they are incompressible and not all boundary-parallel.

In the first part of this certification, we specify the JSJ tori as a union T of normal surfaces, using exponential bounds on their weight due to Mijatović [Mij05], and then use Lackenby's work [Lac16] to certify that they are incompressible and to triangulate their complement. The incompressibility certificate is a crucial part of Lackenby's Thurston norm certificate [Lac16, Section 13], which we explain very briefly here.

The complement $E_K \setminus N(T)$ can be written $M'_1 \sqcup M'_2$, where M'_1 consists of the atoroidal components and M'_2 the Seifert fibered components. We certify using [Lac16, Theorem 12.3] that M'_2 has incompressible boundary. We then turn

M'_1 into a sutured manifold with empty sutures and certify that $\partial M'_1$ is incompressible by providing a certain sutured manifold hierarchy for (M'_1, \emptyset) , of length linear in the number of tetrahedra. The certificate thus includes handle structures for every other manifold in the hierarchy, denoted (M_i, γ_i) , and normal surface vectors for the decomposing surfaces $S_i \subset M_i$. (The remaining sutured manifolds are decomposed along annuli which can be determined algorithmically; see [Lac16, Theorem 10.1].) The certificate also includes proof that the last manifold in the hierarchy is a product, using the theorem of Schleimer [Sch11] and Ivanov [Iva08] that 3-ball recognition is in NP. Much of the difficulty comes from needing to decompose each (M_i, γ_i) efficiently along the corresponding S_i and subsequent annuli, so that a handle structure on the resulting (M_{i+1}, γ_{i+1}) can be constructed and verified in polynomial time.

Taking the incompressibility of the JSJ tori for granted at the moment, we can understand the components of their complement as follows.

Lemma 6.1. *Let $K \subset S^3$ be a knot with exterior $E_K = S^3 \setminus N(K)$, and let $T \subset E_K$ be a union of finitely many disjoint incompressible tori. Then one component of $E_K \setminus N(T)$ is the complement of some knot $K' \subset S^3$, and every other component is the complement of a knot in $S^1 \times D^2$.*

Proof. If T consists of a single torus, then we note that T bounds a solid torus $S^1 \times D^2$ in S^3 , and since T is incompressible in E_K it follows that K must lie in this solid torus. If we let $K' \subset S^3$ be the core of this solid torus, then $E_K \setminus N(T)$ consists of two components, one of which is the exterior of K' and the other of which is $(S^1 \times D^2) \setminus N(K)$.

Now suppose that T consists of n tori T_1, \dots, T_n , where $n \geq 2$. As above, each T_i separates E_K into a knot exterior E_{K_i} , with boundary T_i , and $(S^1 \times D^2) \setminus N(K)$. We define a total ordering of the tori by $T_i < T_j$ if $T_i \subset E_{K_j}$, and we relabel the tori so that $T_1 < T_2 < \dots < T_n$. Then T_n divides $S^3 \setminus N(K)$ into two components, one of which is $(S^1 \times D^2) \setminus N(K)$. The other component is the exterior E_{K_n} , and it contains the incompressible tori T_1, \dots, T_{n-1} , so the lemma follows by induction on n . \square

The component which is a knot complement cannot be an unknot complement since its boundary is incompressible, so in order to see that we have a satellite, we just need to show that one of the remaining components is not $T^2 \times I$. Since these components are all complements of knots in $S^1 \times D^2$, we use the following criterion, originally stated as Theorem 1.6.

Theorem 6.2. *Let $P \subset S^1 \times D^2$ be a knot, and let $E_P = (S^1 \times D^2) \setminus N(P)$ be its exterior. There is a representation*

$$\pi_1(E_P) \rightarrow \mathrm{SL}_2(\mathbb{C})$$

with nonabelian image if and only if P is not isotopic to the core $S^1 \times \{0\}$.

Proof. If P is a core of the solid torus, then $\pi_1(E_P) = \mathbb{Z}^2$ is abelian, so the claim follows immediately. If P lies in a 3-ball, then we can write $E_P = (S^1 \times D^2) \# (S^3 \setminus N(P))$, whose fundamental group surjects onto $\mathbb{Z} * H_1(S^3 \setminus P) = \mathbb{Z} * \mathbb{Z}$. This has a nonabelian representation for any pair of noncommuting elements of $\mathrm{SL}_2(\mathbb{C})$, so we can assume from now on that P does not lie in a 3-ball. We let $M = \{\mathrm{pt}\} \times \partial D^2$ and $L = S^1 \times \{\mathrm{pt}\}$ be generators of $H_1(S^1 \times \partial D^2)$, and we let

$\mu, \lambda \in \partial N(P)$ denote a meridian and a longitude of P respectively. If P has winding number w , then these satisfy $[\mu] = w[\lambda]$ and $[\lambda] = w[L]$ in $H_1(E_P; \mathbb{Z})$, which is generated by $[\mu]$ and $[L]$.

We now fix an integer $r \neq 0$ and construct 3-manifolds Y_n for any $n \in \mathbb{Z}$ by Dehn filling the exterior of P along a pair of curves: we fill $\partial N(P)$ along the slope $\mu + r\lambda$, and then we fill $S^1 \times \partial D^2$ along $nM + (nrw^2 + 1)L$. The filling curves belong to the homology classes $[\mu] + rw[L]$ and $nw[\mu] + (nrw^2 + 1)[L]$, which span all of $H_1(E_P)$, so Y_n is a homology sphere. If Y_n is not homeomorphic to S^3 , then Zentner [Zen18] proved that $\pi_1(Y_n)$ admits an irreducible $SL_2(\mathbb{C})$ representation, and since $\pi_1(Y_n)$ is a quotient of $\pi_1(E_P)$, the composition

$$\pi_1(E_P) \rightarrow \pi_1(Y_n) \rightarrow SL_2(\mathbb{C})$$

is the desired representation.

If we did not get a representation out of this construction, then we must have $Y_n \cong S^3$ for all n . Letting $K \subset Y_0 \cong S^3$ denote the core of the filling along L , we note that the nontrivial surgery on K corresponding to filling along $M + (rw^2 + 1)L$ produces $Y_1 \cong S^3$. Gordon and Luecke’s solution to the knot complement problem [GL89] therefore says that K is the unknot. Its complement is a solid torus which we constructed by filling E_P along the curve $\mu + r\lambda \subset \partial N(P)$, so P has a nontrivial $S^1 \times D^2$ surgery of slope $\mu + r\lambda$. In other words, P must be a Berge-Gabai knot [Ber91, Gab89], meaning it is either a torus knot (i.e., isotopic into $S^1 \times \partial D^2$) or a 1-bridge braid.

Since we chose r arbitrarily at the beginning, the above argument shows that if there are no nonabelian representations $\pi_1(E_P) \rightarrow SL_2(\mathbb{C})$, then any $\mu + r\lambda$ is an $S^1 \times D^2$ surgery slope for P . But Berge [Ber91] and Gabai [Gab90] showed that 1-bridge braids have at most two nontrivial $S^1 \times D^2$ surgeries, so P must be isotopic into $S^1 \times \partial D^2$. Suppose that P represents the class $p[M] + q[L]$ for some coprime integers p, q with $q \geq 2$, since if $q = 0$, then P lies in a 3-ball and if $q = 1$, then P is isotopic to a core. If $|p| \geq 2$ as well, then we can Dehn fill E_P along the curves L and $\mu + \lambda$ to get 1-surgery on the (p, q) torus knot in S^3 . Then $\pi_1(E_P)$ surjects onto $\pi_1(S^3_1(T_{p,q}))$, which admits a nonabelian $SU(2) \subset SL_2(\mathbb{C})$ representation by [KM04, Theorem 1]; hence $\pi_1(E_P)$ does as well.

The only remaining case is the torus knot with $(p, q) = (1, q)$, whose exterior has fundamental group

$$\pi_1(E_P) = \mathbb{Z}^2 *_{(1,q) \sim q} \mathbb{Z} = \langle x, y, t \mid xy = yx, xy^q = t^q \rangle,$$

as can be seen by splitting E_P along an essential annulus (whose core is parallel to P) into $T^2 \times I$ and $S^1 \times D^2$, and its mirror, which has $(p, q) = (-1, q)$ and the same fundamental group. We use the second relation above to write $x = t^q y^{-q}$ and then substitute this into $xy = yx$ to get $t^q y^{1-q} = y t^q y^{-q}$ or, equivalently,

$$\pi_1(E_P) = \langle y, t \mid t^q y = y t^q \rangle.$$

This group has an $SL_2(\mathbb{C})$ representation defined by $t \mapsto \begin{pmatrix} e^{i\pi/q} & \\ 0 & e^{-i\pi/q} \end{pmatrix}$, $y \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and this is nonabelian since $q \geq 2$, so this completes the proof. \square

Corollary 6.3. *Let $P \subset S^1 \times D^2$ be a knot whose exterior $E_P = (S^1 \times D^2) \setminus N(P)$ can be triangulated with t tetrahedra. Assuming the generalized Riemann hypothesis, there is a prime p with $\text{poly}(t)$ digits and a representation*

$$\pi_1(E_P) \rightarrow SL_2(\mathbb{F}_p)$$

with nonabelian image if and only if P is not isotopic to the core $S^1 \times \{0\}$.

Proof. If P is isotopic to the core, then again E_P has abelian fundamental group, so no such representation exists. Otherwise there is a presentation of $\pi_1(E_P)$ with $O(t)$ generators and relations, since these are determined by the 1-skeleton and 2-dimensional faces of the triangulation respectively, and moreover each relation can be taken to have polynomial length in t . Then Theorem 6.2 says that there is a representation $\pi_1(E_P) \rightarrow \text{SL}_2(\mathbb{C})$ with nonabelian image, so [Kup14, Theorem 3.4] guarantees the existence of such an $\text{SL}_2(\mathbb{F}_p)$ representation as well by using the Rabinowitsch trick to discard the representations with abelian image and then applying Theorem 5.6. \square

We can now prove Theorem 1.3, which asserts that SATELLITE-KNOT is in NP, assuming GRH. Again we remark that GRH is required only for the existence of a certificate; any given certificate can be unconditionally verified in polynomial time.

Theorem 6.4. *Assume the generalized Riemann hypothesis. Given a diagram D of a satellite knot K with n crossings, there is a certificate which can be used to verify in $\text{poly}(n)$ time that K is a satellite knot.*

Proof. We triangulate the exterior $E_K = S^3 \setminus N(K)$ with $t = O(n)$ tetrahedra using Proposition 4.1. Then the JSJ tori T of E_K can be realized as normal surfaces with total weight $\|v(T)\|_{L^1} \leq 2^{80t^2}$ by [Mij05, Proposition 2.4], so by [Lac16, Theorem 11.4] we can triangulate $E_K \setminus N(T)$ with at most $200t = O(n)$ tetrahedra in $\text{poly}(t \log \|v(T)\|_{L^1}) = \text{poly}(n)$ time.

If K is a nontrivial satellite, then by Lemma 6.1 some component C of $E_K \setminus N(T)$ will be the complement of a knot in $S^1 \times D^2$ which is not isotopic to a core, so by Corollary 6.3 there will be a prime p with $\log(p) = \text{poly}(n)$ and a representation $\pi_1(C) \rightarrow \text{SL}_2(\mathbb{F}_p)$ with nonabelian image. We can determine a presentation

$$\pi_1(C) = \langle g_1, \dots, g_k \mid r_1, \dots, r_m \rangle$$

in $\text{poly}(t) = \text{poly}(n)$ time from the 2-skeleton of the given triangulation of C . Our certificate therefore consists of:

- (1) the normal coordinates $v(T)$ for the JSJ tori of E_K ;
- (2) a certificate that T is incompressible, from [Lac16];
- (3) a choice of component C of $E_K \setminus T$;
- (4) a prime number p with $\text{poly}(n)$ digits;
- (5) a representation $\rho : \pi_1(C) \rightarrow \text{SL}_2(\mathbb{F}_p)$ with nonabelian image, specified as a list of k matrices $M_i = \rho(g_i) \in \text{SL}_2(\mathbb{F}_p)$.

To verify the certificate, we do the following:

- (1) Verify that T is a union of tori by using the work of Agol-Hass-Thurston [AHT06, Corollary 17].
- (2) Verify the certificate that asserts the incompressibility of T , as in [Lac16].
- (3) Verify that the boundary of C has two connected components.
- (4) Verify that the matrices M_i satisfy $\det(M_i) = 1$ and each of the relations r_j .
- (5) Verify that $M_i M_j \neq M_j M_i$ for some $i \neq j$.

This verification can clearly be done in polynomial time; we need only observe that for the first step, the algorithm of [AHT06, Corollary 17] requires time $\text{poly}(t \log \|v(T)\|_{L^1}) = \text{poly}(n)$. If successful, it shows that the specified component

C of $E_K \setminus T$ has boundary a pair of incompressible tori but is not $T^2 \times I$, since the representation ρ shows that $\pi_1(C)$ is nonabelian. This implies that E_K contains an incompressible torus which is not boundary-parallel, and so K is indeed a satellite knot. \square

Theorem 6.4 finally allows us to complete the proof of Theorem 1.1.

Proof of Theorem 1.1. We already showed in Theorem 4.3 that TORUS-KNOT \in NP, so we wish to show that it is in co-NP, assuming GRH. Given a diagram of a knot K which is not a torus knot, we know that K is either the unknot, a satellite knot, or a hyperbolic knot. If it is an unknot or a satellite knot, then we can certify this using Hass-Lagarias-Pippenger’s unknottedness certificates [HLP99] or Theorem 6.4 respectively. Otherwise, K is a hyperbolic knot, and in this case we can certify that it is not a torus knot by using an uncentered certificate, whose existence is guaranteed by Theorem 5.3.

As for the $T_{r,s}$ recognition problem, given a knot diagram we can certify that it represents $T_{r,s}$ by first certifying that it is a torus knot and then verifying in polynomial time (via Proposition 2.7) that it has the same Alexander polynomial and signature as $T_{r,s}$. If instead it does not represent $T_{r,s}$, then we can certify this by either certifying that it is not a torus knot or by checking that it does not have the same Alexander polynomial and signature as $T_{r,s}$. Assuming GRH, these certificates exist and can be verified in polynomial time since TORUS-KNOT \in NP \cap co-NP, so this establishes that the $T_{r,s}$ recognition problem is in NP \cap co-NP as well. \square

7. CABLE RECOGNITION AND COMPOSITE KNOT RECOGNITION ARE IN NP

In this section we produce certificates, verifiable in polynomial time, which prove that a knot diagram represents a nontrivial cable or composite knot. The arguments are very similar to our proof in Section 4 that TORUS-KNOT \in NP, in that we use Proposition 3.4 to provide an essential normal annulus and check the components of its complement.

More precisely, if K is cabled or composite, then an essential annulus separates the exterior $E_K = S^3 \setminus N(K)$ into two components. Then K is cabled if and only if one component is a solid torus and the other is a nontrivial knot complement $E_{K'}$, where K' is the companion knot, and K is composite if and only if both components are nontrivial knot complements, say E_{K_1} and E_{K_2} , where $K = K_1 \# K_2$. In either case we can recognize solid tori using Ivanov’s work [Iva08], and we can recognize nontrivial knot complements by certifying their Thurston norm as done by Lackenby [Lac16].

In order to check that the Thurston norm of some triangulated knot complement is nonzero, we first need to find a simplicial 1-cocycle with bounded coefficients which represents a nonzero cohomology class.

Proposition 7.1. *Let Y be a compact, connected 3-manifold with $H^1(Y; \mathbb{Z}) = \mathbb{Z}$ and possibly nonempty boundary, and let \mathcal{T} be a triangulation of Y with t tetrahedra. Then there is a simplicial 1-cocycle ϕ , with integer coefficients in the basis of $C^1(Y; \mathbb{Z})$ dual to the edges of \mathcal{T} , such that $\|\phi\|_{L^1} \leq \frac{1}{3}(18t)^{6t}$ and the class $[\phi]$ is a generator of $H^1(Y; \mathbb{Z})$.*

Proof. We write the simplicial cochain complex corresponding to \mathcal{T} as

$$C^0(Y; \mathbb{Z}) \xrightarrow{\delta^0} C^1(Y; \mathbb{Z}) \xrightarrow{\delta^1} C^2(Y; \mathbb{Z}) \xrightarrow{\delta^2} C^3(Y; \mathbb{Z}).$$

Labeling the edges of \mathcal{T} as e_1, \dots, e_n , where $n \leq 6t$, the dual elements e_1^*, \dots, e_n^* defined by $e_i^*(e_j) = \delta_{ij}$ generate $C^1(Y; \mathbb{Z}) \cong \mathbb{Z}^n$. Likewise we let v_1, \dots, v_m and f_1, \dots, f_k be the vertices and faces of \mathcal{T} , with $k, m \leq 4t$, and then the dual elements v_i^* and f_j^* generate $C^0(Y; \mathbb{Z})$ and $C^2(Y; \mathbb{Z})$.

We now attempt to find an integral cocycle with bounded coefficients representing a nonzero class in $H^1(Y; \mathbb{Z})$. We observe that $\ker(\delta^0)$ has rank $b_0(Y) = 1$, so $\text{Im}(\delta^0)$ has rank $m - 1$ and then

$$\text{rank}(\ker(\delta^1)) = b_1(Y) + \text{rank}(\text{Im}(\delta^0)) = 1 + (m - 1) = m.$$

The operator δ^1 thus has rank $n - m$. Representing it as a $k \times n$ matrix A in the standard bases (e_i^*) and (f_j^*) of $C^1(Y; \mathbb{Z})$ and $C^2(Y; \mathbb{Z})$, we can renumber the f_j so that the first $n - m$ rows of A are linearly independent. Similarly, we can renumber the vertices v_i so that $\delta^0 v_1^*, \dots, \delta^0 v_{m-1}^*$ are linearly independent in $C^1(Y; \mathbb{Z})$. We now form an $(n - 1) \times n$ matrix B whose first $n - m$ rows are the first $n - m$ rows of A and whose remaining $m - 1$ rows are the coordinates of the vectors $\delta^0 v_1^*, \dots, \delta^0 v_{m-1}^*$.

By construction, a nonzero element $x \in \mathbb{Z}^n$ belongs to $\ker(B)$ if and only if it is in $\ker(A)$ and orthogonal to each of the $\delta^0 v_i^*$; the corresponding cocycle ϕ is not in $\text{Im}(\delta^0)$, so it represents a nontrivial cohomology class. The entries of B are bounded as follows: every entry in the first $n - m$ rows is an entry of A , so it has the form $a_{ij} = (\delta^1 e_j^*)(f_i) = e_j^*(\partial f_i)$, which has absolute value at most 3. Each entry in the last $m - 1$ rows has the form $(\delta^0 v_i^*)(e_j) = v_i^*(\partial e_j)$, which is ± 1 if exactly one endpoint of e_j is v_i and 0 otherwise. Thus B is an $(n - 1) \times n$ matrix whose entries are all integers between -3 and 3 , so Siegel’s lemma [Sie14, p. 213] says that $Bx = 0$ has a nonzero integer solution $x = \langle x_1, \dots, x_n \rangle$ satisfying

$$|x_i| \leq (3n)^{(n-1)/(n-(n-1))} = (3n)^{n-1}$$

for all i . In particular, this gives a cocycle $\phi \in C^1(Y; \mathbb{Z})$ with $[\phi] \neq 0$ in $H^1(Y; \mathbb{Z})$ and $\|\phi\|_{L^1} \leq (3n)^{n-1} \cdot n = \frac{1}{3}(3n)^n \leq \frac{1}{3}(18t)^{6t}$.

Now suppose that $[\phi] = d[\phi']$, where $[\phi']$ generates $H^1(Y; \mathbb{Z})$. If $d = 1$, then we are done, so we may assume that $d \geq 2$. Then we have integers c_1, \dots, c_m such that

$$\phi = d\phi' + \sum_{i=1}^m c_i(\delta_0 v_i^*).$$

Letting n_i be the closest integer to $\frac{c_i}{d}$ for each $i = 1, \dots, m$, we define a cocycle

$$\phi_0 = \phi' + \sum_{i=1}^m n_i(\delta_0 v_i^*) \in C^1(Y; \mathbb{Z})$$

and observe that $[\phi_0] = [\phi']$ generates $H^1(Y; \mathbb{Z})$, and also that

$$\left\| \phi_0 - \frac{1}{d}\phi \right\|_{L^1} = \left\| \sum_{i=1}^m \left(n_i - \frac{c_i}{d} \right) (\delta_0 v_i^*) \right\|_{L^1} \leq \frac{1}{2} \sum_{i=1}^m \|\delta_0 v_i^*\|_{L^1}$$

by the triangle inequality. Now $|(\delta_0 v_i^*)(e_j)| \leq 1$ as explained above, so $\|\delta_0 v_i^*\|_{L^1} \leq n$, and hence the right-hand side above is at most $\frac{1}{2}mn \leq 12t^2$. We conclude by the triangle inequality that

$$\|\phi_0\|_{L^1} \leq \left\| \phi_0 - \frac{1}{d}\phi \right\|_{L^1} + \frac{1}{d}\|\phi\|_{L^1} \leq 12t^2 + \frac{1}{2}(18t)^{6t},$$

which is clearly at most $\frac{1}{3}(18t)^{6t}$ for all $t \geq 1$, establishing the claim. \square

With the cocycles provided by Proposition 7.1 in hand, we can now certify the cabledness or compositeness of a given knot.

Theorem 7.2. *Given a diagram of a cabled knot K with n crossings, there is a certificate which can be used to verify in $\text{poly}(n)$ time that K is a nontrivial cable.*

Proof. We construct a triangulation \mathcal{T} of the exterior E_K with $t = O(n)$ tetrahedra, whose restriction to ∂E_K consists of two triangles and a single vertex, using Proposition 4.1. We can realize a cabling annulus A as a normal surface with $\|v(A)\|_{L^1} \leq 7t \cdot 2^{7t}$ by Proposition 3.4. We can use Proposition 4.2 to produce a triangulation of $E_K \setminus N(A)$ with at most $200t$ tetrahedra in $\text{poly}(t)$ time.

The complement $E_K \setminus N(A)$ consists of two components, one of which is a solid torus and the other of which is the complement of the companion K' ; we will call these C and E respectively. We can use the triangulation of E to find a presentation of $\pi_1(E)$ in $\text{poly}(t) = \text{poly}(n)$ time. Our certificate that K is cabled thus contains the following:

- (1) positive integers g and θ , with $1 \leq \theta < 2g - 1 \leq n$;
- (2) a certificate that K has Seifert genus g , as provided by Lackenby [Lac16];
- (3) normal coordinates $v(A)$ of a properly embedded, essential annulus $A \subset E_K$ with weight $\|v(A)\|_{L^1} \leq 7t \cdot 2^{7t}$;
- (4) a certificate that one component C of $E_K \setminus N(A)$ is a solid torus, as provided by Ivanov [Iva08];
- (5) for the other component E of $E_K \setminus N(A)$, a simplicial 1-cocycle ϕ with integer coefficients satisfying $\|\phi\|_{L^1} < \frac{1}{3}(18 \cdot 200t)^{6 \cdot 200t}$;
- (6) a certificate that the Poincaré dual of $[\phi]$ has Thurston norm θ , as provided by Lackenby [Lac16].

We verify the certificate as follows:

- (1) Verify the certificate that $g(K) = g$, as in [Lac16].
- (2) Verify that A is an annulus and that the components of ∂A are homologically nontrivial in ∂E_K .
- (3) Verify as in [Iva08] the certificate that $C \cong S^1 \times D^2$.
- (4) Verify the certification of the Thurston norm of $[\phi]$, as in [Lac16].

To see that this correctly proves that K is cabled, we note that if K is a (p, q) -cable of K' , then we have the relation

$$g(K) > g(K') \geq 1,$$

see [Shi89], and that $2g(K) - 1 \leq n$ by an easy application of Seifert's algorithm. Thus step (1) certifies that K is knotted without incorrectly eliminating any cables. Since K is knotted, step (2) proves that A is either essential or boundary-parallel. In the latter case, we would have $E \cong E_K$, so any nonzero class in $H^1(E) \cong \mathbb{Z}$ would have Thurston norm a positive multiple of $2g - 1$. In particular, the certificate verifies that A is essential.

Since A is an essential annulus, K must be a torus knot, a cable, or composite. If it is composite, then both components of $E_K \setminus N(A)$ are nontrivial knot exteriors, so C cannot be a solid torus. If instead K is a torus knot, then both components are solid tori, so the Thurston norm of E vanishes. Thus if the certificate exists, it proves that K is a cable.

Now we need to see that a certificate exists whenever $K = C_{p,q}(K')$ is a nontrivial cable of a nontrivial knot K' . The normal annulus A exists by Proposition 3.4, as does the certificate that $C \cong S^1 \times D^2$. Using Proposition 7.1, we know that there is a cocycle ϕ representing a generator of $H^1(E) \cong \mathbb{Z}$, where $\|\phi\|_{L^1}$ satisfies the given bounds since E has at most $200t$ tetrahedra. The Poincaré dual of ϕ then has Thurston norm $\theta = 2g(K') - 1 > 0$, where $g(K')$ is the Seifert genus of the companion K' . But we have

$$2g(K') - 1 \leq 2g(K) - 1 \leq n,$$

where $g(K') \leq g(K)$ by [Shi89] and $2g(K) - 1 \leq n$ by an easy application of Seifert’s algorithm, and so $1 \leq \theta \leq n$. Thus ϕ and θ exist as well.

Finally, it is mostly clear that each step of the verification requires only polynomial time in n , since $t = O(n)$. We recall that in step (2), we verify that A is an annulus using [AHT06] and that we determine that ∂A consists of essential curves in ∂E_K using their characterization as normal curves as in Section 3. Moreover, step (4) takes $\text{poly}(200t, \log(\theta), \log(\|\phi\|_{L^1}))$ time by [Lac16, Theorem 1.5], but $\log(\theta) = O(\log n)$ and $\log(\|\phi\|_{L^1}) = O(t \log t)$ and $t = O(n)$, so this is again $\text{poly}(n)$ as desired. \square

The construction of certificates proving that a knot K is composite and the algorithm which verifies them in polynomial time are nearly identical.

Theorem 7.3. *Given a diagram of a composite knot K with n crossings, there is a certificate which can be used to verify in $\text{poly}(n)$ time that K is a nontrivial connected sum.*

Proof. We produce a triangulation \mathcal{T} of the exterior E_K which restricts to a 1-vertex triangulation on ∂E_K by Proposition 4.1, and given a normal essential annulus A which splits E_K into a pair of nontrivial knot complements E_1 and E_2 we can triangulate $E_K \setminus N(A)$ with $O(n)$ tetrahedra in $\text{poly}(n)$ time by Proposition 4.2. We can arrange that $\|v(A)\|_{L^1} \leq 7t \cdot 2^{7t}$, where \mathcal{T} has $t = O(n)$ tetrahedra by Proposition 3.4. Using the triangulations of E_1 and E_2 , we can similarly produce presentations of $\pi_1(E_1)$ and $\pi_1(E_2)$ in $\text{poly}(n)$ time. All of this is accomplished exactly as in the proof of Theorem 7.2.

The compositeness certificate for the given diagram consists of:

- (1) a certificate that it represents a nontrivial knot, as specified by Lackenby [Lac16];
- (2) normal coordinates for an essential annulus A , with $\|v(A)\|_{L^1} \leq 7t \cdot 2^{7t}$;
- (3) for both $i = 1$ and $i = 2$:
 - (a) a simplicial 1-cocycle ϕ_i on E_i with integral coefficients satisfying $\|\phi_i\|_{L^1} < \frac{1}{3}(3600t)^{1200t}$;
 - (b) a positive integer $\theta_i < n$;
 - (c) a certificate that the Poincaré dual of $[\phi_i]$ has Thurston norm $[\theta_i]$, as provided by [Lac16].

We use [Lac16] to verify that K is knotted and [AHT06] to verify that $v(A)$ indeed represents an annulus. We check that the components of ∂A are homologically essential in ∂E_K , which then proves that A is either essential or boundary-parallel. We then verify that the classes dual to $[\phi_i]$ on each E_i have the given Thurston norms. All of this can be done in $\text{poly}(n)$ time, as in Theorems 4.3 and 7.2.

To see that this correctly verifies that K is composite, we note that neither component of $E_K \setminus N(A)$ can be a solid torus, since then its Thurston norm would vanish. This implies that A cannot be boundary-parallel, so it must be essential, and then since neither component is a solid torus we conclude that K is composite. Moreover, if K is composite, then a certificate exists: the normal annulus exists by Proposition 3.4, and if E_i is the exterior of a knot K_i , then we have $g(K_1) + g(K_2) = g(K)$, so that

$$1 \leq 2g(K_i) - 1 \leq 2g(K) - 1 < n,$$

and hence the desired bounds on $\|\phi_i\|_{L^1}$ and θ_i follow as in Theorem 7.2. \square

ACKNOWLEDGMENT

We are grateful to the referee for providing useful feedback which improved the quality of the paper.

REFERENCES

- [AHT06] Ian Agol, Joel Hass, and William Thurston, *The computational complexity of knot genus and spanning area*, Trans. Amer. Math. Soc. **358** (2006), no. 9, 3821–3850, DOI 10.1090/S0002-9947-05-03919-X. MR2219001
- [Ber91] John Berge, *The knots in $D^2 \times S^1$ which have nontrivial Dehn surgeries that yield $D^2 \times S^1$* , Topology Appl. **38** (1991), no. 1, 1–19, DOI 10.1016/0166-8641(91)90037-M. MR1093862
- [BZ66] Gerhard Burde and Heiner Zieschang, *Eine Kennzeichnung der Torusknoten* (German), Math. Ann. **167** (1966), 169–176, DOI 10.1007/BF01362170. MR0210113
- [BZ03] Gerhard Burde and Heiner Zieschang, *Knots*, 2nd ed., De Gruyter Studies in Mathematics, vol. 5, Walter de Gruyter & Co., Berlin, 2003. MR1959408
- [CF63] Richard H. Crowell and Ralph H. Fox, *Introduction to knot theory*, based upon lectures given at Haverford College under the Philips Lecture Program, Ginn and Co., Boston, Mass., 1963. MR0146828
- [CL14] Alexander Coward and Marc Lackenby, *An upper bound on Reidemeister moves*, Amer. J. Math. **136** (2014), no. 4, 1023–1066, DOI 10.1353/ajm.2014.0027. MR3245186
- [CS83] Marc Culler and Peter B. Shalen, *Varieties of group representations and splittings of 3-manifolds*, Ann. of Math. (2) **117** (1983), no. 1, 109–146, DOI 10.2307/2006973. MR683804
- [Gab89] David Gabai, *Surgery on knots in solid tori*, Topology **28** (1989), no. 1, 1–6, DOI 10.1016/0040-9383(89)90028-1. MR991095
- [Gab90] David Gabai, *1-bridge braids in solid tori*, Topology Appl. **37** (1990), no. 3, 221–235, DOI 10.1016/0166-8641(90)90021-S. MR1082933
- [GL78] C. McA. Gordon and R. A. Litherland, *On the signature of a link*, Invent. Math. **47** (1978), no. 1, 53–69, DOI 10.1007/BF01609479. MR0500905
- [GL89] C. McA. Gordon and J. Luecke, *Knots are determined by their complements*, J. Amer. Math. Soc. **2** (1989), no. 2, 371–415, DOI 10.2307/1990979. MR965210
- [Hak61] Wolfgang Haken, *Theorie der Normalflächen* (German), Acta Math. **105** (1961), 245–375, DOI 10.1007/BF02559591. MR0141106
- [Hak62] Wolfgang Haken, *Über das Homöomorphieproblem der 3-Mannigfaltigkeiten. I* (German), Math. Z. **80** (1962), 89–120, DOI 10.1007/BF01162369. MR0160196
- [Hak68] Wolfgang Haken, *Some results on surfaces in 3-manifolds*, Studies in Modern Topology, Math. Assoc. Amer. (distributed by Prentice-Hall, Englewood Cliffs, N.J.), 1968, pp. 39–98. MR0224071
- [Hem79] Geoffrey Hemion, *On the classification of homeomorphisms of 2-manifolds and the classification of 3-manifolds*, Acta Math. **142** (1979), no. 1-2, 123–155, DOI 10.1007/BF02395059. MR512214
- [HLP99] Joel Hass, Jeffrey C. Lagarias, and Nicholas Pippenger, *The computational complexity of knot and link problems*, J. ACM **46** (1999), no. 2, 185–211, DOI 10.1145/301970.301971. MR1693203

- [Iva08] S. V. Ivanov, *The computational complexity of basic decision problems in 3-dimensional topology*, *Geom. Dedicata* **131** (2008), 1–26, DOI 10.1007/s10711-007-9210-4. MR2369189
- [Joh79] Klaus Johannson, *Homotopy equivalences of 3-manifolds with boundaries*, *Lecture Notes in Mathematics*, vol. 761, Springer, Berlin, 1979. MR551744
- [JR89] William Jaco and J. Hyam Rubinstein, *PL equivariant surgery and invariant decompositions of 3-manifolds*, *Adv. in Math.* **73** (1989), no. 2, 149–191, DOI 10.1016/0001-8708(89)90067-4. MR987273
- [JS79] William H. Jaco and Peter B. Shalen, *Seifert fibered spaces in 3-manifolds*, *Mem. Amer. Math. Soc.* **21** (1979), no. 220, viii+192, DOI 10.1090/memo/0220. MR539411
- [JS03] William Jaco and Eric Sedgwick, *Decision problems in the space of Dehn fillings*, *Topology* **42** (2003), no. 4, 845–906, DOI 10.1016/S0040-9383(02)00083-6. MR1958532
- [JT95] William Jaco and Jeffrey L. Tollefson, *Algorithms for the complete decomposition of a closed 3-manifold*, *Illinois J. Math.* **39** (1995), no. 3, 358–406. MR1339832
- [KM04] P. B. Kronheimer and T. S. Mrowka, *Dehn surgery, the fundamental group and $SU(2)$* , *Math. Res. Lett.* **11** (2004), no. 5–6, 741–754, DOI 10.4310/MRL.2004.v11.n6.a3. MR2106239
- [Koi96] Pascal Koiran, *Hilbert’s Nullstellensatz is in the polynomial hierarchy*, special issue for the Foundations of Computational Mathematics Conference (Rio de Janeiro, 1997), *J. Complexity* **12** (1996), no. 4, 273–286, DOI 10.1006/jcom.1996.0019. MR1422712
- [Kup14] Greg Kuperberg, *Knottedness is in NP, modulo GRH*, *Adv. Math.* **256** (2014), 493–506, DOI 10.1016/j.aim.2014.01.007. MR3177300
- [Lac15] Marc Lackenby, *A polynomial upper bound on Reidemeister moves*, *Ann. of Math. (2)* **182** (2015), no. 2, 491–564, DOI 10.4007/annals.2015.182.2.3. MR3418524
- [Lac16] Marc Lackenby, *The efficient certification of knottedness and Thurston norm*, arXiv:1604.00290, 2016.
- [Lic97] W. B. Raymond Lickorish, *An introduction to knot theory*, *Graduate Texts in Mathematics*, vol. 175, Springer-Verlag, New York, 1997. MR1472978
- [Lit79] R. A. Litherland, *Signatures of iterated torus knots*, *Topology of low-dimensional manifolds (Proc. Second Sussex Conf., Chelwood Gate, 1977)*, *Lecture Notes in Math.*, vol. 722, Springer, Berlin, 1979, pp. 71–84. MR547456
- [LO77] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, *Academic Press, London*, 1977, pp. 409–464. MR0447191
- [Mat03] Sergei Matveev, *Algorithmic topology and classification of 3-manifolds*, *Algorithms and Computation in Mathematics*, vol. 9, Springer-Verlag, Berlin, 2003. MR1997069
- [Mij05] Aleksandar Mijatović, *Triangulations of fibre-free Haken 3-manifolds*, *Pacific J. Math.* **219** (2005), no. 1, 139–186, DOI 10.2140/pjm.2005.219.139. MR2174223
- [Rud82] Lee Rudolph, *Nontrivial positive braids have positive signature*, *Topology* **21** (1982), no. 3, 325–327, DOI 10.1016/0040-9383(82)90014-3. MR649763
- [Sch11] Saul Schleimer, *Sphere recognition lies in NP*, *Low-dimensional and symplectic topology, Proc. Sympos. Pure Math.*, vol. 82, Amer. Math. Soc., Providence, RI, 2011, pp. 183–213, DOI 10.1090/pspum/082/2768660. MR2768660
- [Shi89] Tetsuo Shibuya, *Genus of torus links and cable links*, *Kobe J. Math.* **6** (1989), no. 1, 37–42. MR1023523
- [Sie14] Carl L. Siegel, *Über einige Anwendungen diophantischer Approximationen [reprint of Abhandlungen der Preußischen Akademie der Wissenschaften. Physikalisch-mathematische Klasse 1929, Nr. 1]* (German), *On some applications of Diophantine approximations, Quad./Monogr.*, vol. 2, Ed. Norm., Pisa, 2014, pp. 81–138. MR3330350
- [Sim73] Jonathan Simon, *An algebraic classification of knots in S^3* , *Ann. of Math. (2)* **97** (1973), 1–13, DOI 10.2307/1970874. MR0310861
- [Thu82] William P. Thurston, *Three-dimensional manifolds, Kleinian groups and hyperbolic geometry*, *Bull. Amer. Math. Soc. (N.S.)* **6** (1982), no. 3, 357–381, DOI 10.1090/S0273-0979-1982-15003-0. MR648524
- [vzGG99] Joachim von zur Gathen and Jürgen Gerhard, *Modern computer algebra*, *Cambridge University Press, New York*, 1999. MR1689167
- [Wei84] P. J. Weinberger, *Finding the number of factors of a polynomial*, *J. Algorithms* **5** (1984), no. 2, 180–186, DOI 10.1016/0196-6774(84)90025-7. MR744488

- [Zen18] Raphael Zentner, *Integer homology 3-spheres admit irreducible representations in $SL(2, \mathbb{C})$* , *Duke Math. J.* **167** (2018), no. 9, 1643–1712, DOI 10.1215/00127094-2018-0004. MR3813594

DEPARTMENT OF MATHEMATICS, BOSTON COLLEGE, MALONEY HALL, FIFTH FLOOR, BOSTON COLLEGE, CHESTNUT HILL, MASSACHUSETTS 02467-3806

Email address: `john.baldwin@bc.edu`

DEPARTMENT OF MATHEMATICS, IMPERIAL COLLEGE LONDON, HUXLEY BUILDING, 180 QUEEN'S GATE, LONDON SW7 2AZ, UNITED KINGDOM

Email address: `s.sivek@imperial.ac.uk`