PRIME FACTORIZATION OF KNOTS

ALLEN LIN

1. Introduction and Motivation

Now that we have a notion of combining two oriented knots through the connected sum, it is natural to ask the reverse on the decomposition of any knot into a connected sum of fundamental knots. By fundamental we mean that these knots are no longer decomposable. This motivates the definition of a prime knot. This was first determined by Schubert [2] in 1949. In the sequel, we denote the connected sum by $+$, though the symbol $\#$ is also used in the literature.

Definition 1. A knot K is a *prime knot* if it is not the unknot and any decomposition $K = K_1 + K_2$ implies that either K_1 or K_2 is the unknot.

One may recognize that this definition is analogous to that of a prime number: a number $p \in \mathbb{N}$ is prime if $p \neq 1$ and any decomposition $p = ab$ implies either $a = 1$ or $b = 1$.

Of course, the notion of a composite knot is defined in the most natural way.

Definition 2. A knot K is a *composite knot* if it is not prime.

Similar to the convention in number theory that 1 is neither prime nor composite, we make the following convention.

Remark 1. The unknot is neither prime nor composite.

Now that we have a notion of prime knots, the next natural questions are

(I) whether a prime knot exists,
(II) whether any knot can be decomposed into a connected sum of prime knots, and
(III) whether the decomposition is unique if it exists.

The answer to these questions is in the affirmative, analogous to the Fundamental Theorem of Arithmetic from number theory.

Theorem 1. *Any knot can be expressed uniquely as a finite connected sum of prime knots up to order.*

To prove this theorem, we freely make use of the following result on the addivity of the genus g of a knot over a connected sum.

Theorem 2. *For any two knots K_1 and K_2, $g(K_1 + K_2) = g(K_1) + g(K_2)$.*

2. Existence of Prime Decomposition

In this section, we prove that for any knot there exists a prime decomposition. We first answer (I) and show that prime knots exist.

Lemma 1. *Let K be a knot. If $g(K) = 1$, then K is prime.*

Proof. Let $K = K_1 + K_2$ be a decomposition. Theorem 2 then implies

$$1 = g(K) = g(K_1) + g(K_2).$$

Without loss of generality, suppose $g(K_1) = 0$. Then K_1 is the unknot, which implies K is prime. □

Now we answer (II) and prove the existence of a prime decomposition of a knot.

Theorem 3. *Any knot K can be expressed as a finite sum of prime knots.*

Proof. We induct on the genus g. If $g(K) = 1$, then we are done by Lemma 1. Suppose that all knots with genus $g < k$ have a finite prime decomposition, and let K be a knot of genus $g(K) = k$. If K itself is prime, then we are done. Then suppose K is not prime, and so $K = K_1 + K_2$ for nontrivial K_1 and K_2. By the inductive hypothesis,

$$K_1 = P_1 + \cdots + P_n,$$
$$K_2 = Q_1 + \cdots + Q_m,$$

for prime knots $P_1, \ldots, P_n, Q_1, \ldots, Q_m$. Thus,

$$K = K_1 + K_2 = P_1 + \cdots + P_n + Q_1 + \cdots + Q_m,$$

which proves the result. □

One might recognize that this style of proof is similar to the proof of the existence of the prime factorization of any natural number.

3. Uniqueness of Prime Decomposition

In this section we answer (III) and prove that the prime decomposition of a knot constructed in Theorem 3 is unique. We first present the following result.

Theorem 4 (Lickorish [1])**.** *Suppose $K = P + Q = K_1 + K_2$ and P is a prime knot. Then either*

(a) $K_1 = P + K_1'$ for some K_1' and $Q = K_1' + K_2$, or
(b) $K_2 = P + K_2'$ for some K_2' and $Q = K_1 + K_2'$.

For a proof of this result, we refer the reader to [1]. The proof is mainly topological in nature.

Theorem 4 allows us to prove the following useful lemma.

Lemma 2. *Suppose P is prime and $P + Q = P + K_2$. Then $Q = K_2$.*

Proof. Let $K_1 = P$ and apply Theorem 4. Therefore, there are two possibilities. The first is that $K_1 = P + K_1'$ for some K_1' and $Q = K_1' + K_2$, where applying Theorem 2 to the first decomposition gives

$$g(P) = g(K_1) = g(P) + g(K_1').$$

This implies $g(K_1') = 0$, so K_1' is the unknot, and applying this to the second decomposition gives $Q = K_2$. The second possibility is that $K_2 = P + K_2'$ for some K_2' and $Q = K_1 + K_2' = P + K_2'$, so $Q = K_2$. □

We now prove the uniqueness result using Lemma 2.

Theorem 5. *Any knot K can be expressed uniquely as a finite sum of prime knots.*

Proof. Suppose

$$K = P_1 + P_2 + \cdots + P_m = Q_1 + Q_2 + \cdots + Q_n \tag{1}$$

are two prime decompositions of K. Let

$$\begin{aligned} P &= P_1, \\ Q &= P_2 + \cdots + P_m, \\ K_1 &= Q_1, \\ K_2 &= Q_2 + \cdots + Q_n, \end{aligned}$$

so that

$$K = P + Q = K_1' + K_2'.$$

Applying Theorem 4 gives us two possibilities. The first is that $Q_1 = P_1 + K_1'$ for some K_1'. However, Q_1 is prime, so $Q_1 = P_1$ by definition. We apply Lemma 2 to (1) to get

$$P_2 + \cdots + P_m = Q_2 + \cdots + Q_n,$$

and one can repeat this process to conclude that $m = n$ and the prime decompositions are indeed the same. In the second case we have $Q_2 + \cdots + Q_n = P_1 + K_2'$ for some K_2'. This occurs only when $Q_j = P_1 + K^*$ for some $j \in \{2, \ldots, n\}$ and some K^*. This immediately implies $Q_j = P_1$ by definition, and one uses Lemma 2 to (1) in the same vein as in the first case. □

One might recognize that this style of proof is similar to the proof of the uniqueness of the prime factorization of any natural number.

References

[1] W. B. R. Lickorish, *An Introduction to Knot Theory*, Springer-Verlag, 1997.
[2] H. Schubert, Die eindeutige Zerlegbarkeit eines Knotens in Primknoten, *S.-B Heidelberger Akad. Wiss. Math.-Nat. Kl.* (1949) 57–104.

Massachusetts Institute of Technology, 77 Massachusetts Ave, Cambridge, MA 02139-4301
Email address: allenees@mit.edu