ACTA ARITHMETICA
129.4 (2007)

Determinants of knots and Diophantine equations

by

A. Stoimenow (Kyoto)

1. Introduction. The problem of solving an equation $P(x_1,\dots,x_n)=0$ for some polynomial $P\in\mathbb{Z}[x_1,\dots,x_n]$ in integers x_i is one of the most fundamental in the whole mathematics. A general theory is developed only for P of small degree, having few variables, or of a special type, like quadratic forms [Z], the Fermat equation [W], elliptic curves [Hu] or Waring's class of problems [Ho]. See e.g. [Sm].

The aim of this paper is to give an application of the theory of knots [Ka1] to Diophantine equations, by means of a knot-theoretic obstruction to the solvability of certain types of such equations. Of central importance will be the work of Kauffman [Ka2], Murasugi [Mu1], and the following theorem on the signature $\sigma(K)$ and determinant $\det(K)$ of a knot K.

Theorem 1.1. *There is no knot K with* $\det(K)=1$ *and* $\sigma(K)\equiv 4 \pmod 8$.

Theorem 1.1 is a consequence of a signature theorem for even unimodular quadratic forms. A brief proof will be given in the next section. This theorem will be used to show the non-solvability of certain Diophantine equations $P(x_1,\dots,x_n,k,l)=\pm1$ in non-negative integers x_i. *Inter alia*, we can associate to any diagram D of a knot K whose canonical genus $g(D)$ satisfies $2g(D)=\sigma(K)\equiv 6 \pmod 8$, a polynomial P_D such that any solution of $P_D=\pm1$ contains at least three integers of a given sign. Moreover the number of variables of P_D is equal to the number of crossings of D, and hence can be arbitrarily augmented. The simplest type of such a polynomial P_D is the elementary symmetric polynomial of second highest degree. We have in particular:

2000 *Mathematics Subject Classification*: 11D72, 57M27, 11D41, 11B37, 11D79, 15A63.

Key words and phrases: knots, signature, determinant, Jones polynomial, Diophantine equation, quadratic form.

Research supported by 21st Century COE Program.

THEOREM 1.2. *Let $\sigma_{n-1,n}$ be the elementary symmetric polynomial of degree $n-1$ in n variables and $n \equiv 7 \pmod 8$. Then any solution of $\sigma_{n-1,n} = -1$ in odd integers contains at least three negative* (*and three positive*) *ones.*

The polynomials we will consider are of some special types, but they arise from the particular families of knots we study, and one can build many more. The non-negativity condition on the x_i in P_D can be removed by suitable substitutions (and also by appropriate modification of the knots under consideration), yielding polynomials of even degree in all but two of their variables. By substitutions one also obtains many low degree polynomials. In other cases, including examples of cubic curves [Ma], one can show that the signs of continued fractions related to integer solutions satisfy certain congruences. One can also obtain results about linear recurrent sequences.

It is unlikely that (and unclear how) one can study a given particular equation by such a procedure. The statements that one obtains with our approach, however, may well go beyond the scope of state-of-the-art methods (using the apparatus from algebraic geometry). It is at least unlikely that our results can be recovered by known methods in such a direct way.

Acknowledgements. The work in this paper was mostly carried out during a stay at MPI Bonn. I would like to thank B. Poonen, V. Protsak and D. Zagier for some helpful remarks and discussions. Most of all, however, I wish to thank F. Hirzebruch, who pointed out Theorem 1.1 to me, and without whose support this work would not have been possible.

2. Knots, signature and determinant

2.1. *Relation to Seifert forms.* A *knot* (resp. n-component *link*) is an S^1 (resp. n copies of it), oriented or not, smoothly embedded in $\mathbb{R}^3$. We need some basic facts about knots, which are explained in detail for example in [Ro].

Knots and links are represented by *diagrams*, plane curves with transverse self-intersections, called *crossings*, at each of which an over- and underpassing strand is distinguished. A diagram is called *connected* if its plane curve is connected. A link is *split* if it has a diagram which is not connected; otherwise it is *non-split.* (A knot is always non-split.)

Every oriented knot or link L bounds a compact surface S embedded in $\mathbb{R}^3$, so that the orientation of $L = \partial S$ matches the one induced from S. Such a surface S is called a *Seifert surface* of L. The minimal genus, resp. the maximal Euler characteristic of all Seifert surfaces of L is called the *genus* $g(L)$, resp. the *Euler characteristic* $\chi(L)$ of L. From each diagram D of L one can obtain a Seifert surface $S(D)$ of L by means of an algorithm due to Seifert. We call the genus $g(S(D)) = g(D)$, resp. the Euler characteristic

$\chi(S(D)) = \chi(D)$ of $S(D)$ the *canonical genus*, resp. the *canonical Euler characteristic* of D.

Each Seifert surface of L gives rise to a *Seifert matrix*. Here it is enough to understand that this is a square matrix with integer entries. A knot K has many Seifert surfaces, and each Seifert surface defines many Seifert matrices. Still there are invariants of K derived from the Seifert matrix.

The results that follow will be obtained by extensively using properties of the *signature* and *determinant* of knots and links. These invariants have been around for a long time in knot theory (see, e.g., [H, Ro]). Originally they were defined in terms of Seifert matrices. More precisely, $\det(K)$ is the order of the homology group of the double cover of S^3 branched over the knot (or link), and obtained its name from its expression as the determinant of a Seifert matrix (which is a representation matrix for this homology group), and $\sigma(K)$ is the signature of the symmetric pairing given by the Seifert matrix.

The definition of signature and determinant by means of Seifert matrices leads to Theorem 1.1.

Proof of Theorem 1.1. Consider the Seifert form of K given by $A + A^T$, where A is a Seifert matrix of K. Then $\det(K) = \det(A + A^T) = \pm 1$, and $A + A^T$ has only even entries on the diagonal.

For any bilinear form S over $\mathbb{Z}^n$ the map

$$x \mapsto S(x, x) \bmod 2$$

is linear, and if $S \bmod 2$ is non-degenerate ($\Leftrightarrow \det(S)$ is odd), then

$$\exists w : S(x, w) \equiv S(x, x) \pmod{2}$$

for all $x \in \mathbb{Z}^n$. We have the following theorem on the norm of w and the signature $\sigma(S)$ of S (see [HNK, Theorem 3.10]).

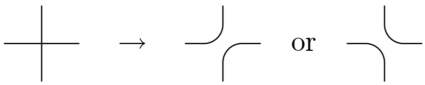
Theorem 2.1. *If* $\det(S) = \pm 1$, *then* $S(w, w) \equiv \sigma(S) \pmod{8}$ *for any such* w.

If $S = A + A^T$ has only even entries on the diagonal, then $S(x, x) \equiv 0 \pmod{2}$, and thus we can choose $w = 0$. Then the theorem shows $\sigma(K) = \sigma(S) \equiv 0 \pmod{8}$. ∎

Once Theorem 1.1 is proved, the Seifert form, however, will no longer be of interest to us for studying the determinant and signature. It will be more convenient to follow other approaches to these two invariants, using properties of their behaviour under certain knot diagrammatic operations.

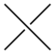
2.2. *The determinant via state model and braiding sequences.* For the determinant we follow an approach which was developed from the Kauffman state model [Ka2] for the Jones polynomial [J1]. It uses the property that $\det(K) = |\Delta_K(-1)| = |V_K(-1)| = |\langle D\rangle(\sqrt{i})|$, where Δ is the Alexander polynomial, V is the Jones polynomial, $\langle D\rangle$ is the Kauffman bracket of some diagram D of K, and $\sqrt{i}$ is a primitive 8th root of unity (see [J2, (12.3)]). The state model allows one to give a combinatorial definition of the determinant of alternating diagrams.

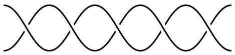
A diagram is *alternating* if each strand exiting a crossing from above enters the next crossing from below and vice versa. A connected alternating diagram D can be identified (up to mirror image, which preserves the determinant) with its plane curve $\widehat{D}\subset\mathbb{R}^2$. Then each of the n crossings (self-intersections) of $\widehat{D}$ can be *spliced* in two ways

(1) ,

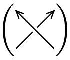
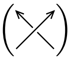
giving 2^n *states*, and $\det(D)$ is the number of states whose resulting collection of disjoint circles has only one component, i.e., is one single circle ("monocyclic state" [Kr]).

From this the definition of $\det(D)$ can be extended to arbitrary diagrams using the approach of braiding sequences [St2] (which was originally introduced for the study of Vassiliev invariants, but serves equally well also for any particular value of $\varDelta(t)$, not only $t=-1$).

Number the crossings of a diagram D by $c_1,\dots,c_n$. To each c_i one assigns an odd integer variable x_i. Then define $D(x_1,\dots,x_n)$ to be the diagram obtained from D by replacing each crossing c_i  in D by a tangle, called a *twist* below, of $|x_i|$ crossings like

(2) 

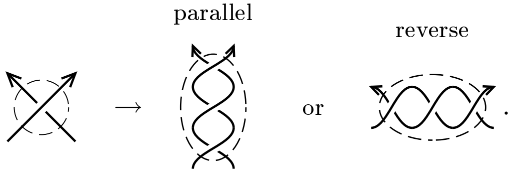
(for $x_i=\pm5$). To fix the signs, we demand that when orienting D, the crossings in this tangle have sign $\operatorname{sgn}(x_i)$, where the *sign* (or *writhe*) of a crossing is defined by

(3) sgn () $=-1$ and sgn () $=1$.

(We use here the fact that D is a knot diagram, and then any of the two orientations attaches the same sign to each crossing.) Then $D=D(x_1,\dots,x_n)$ for $x_i=\operatorname{sgn}(c_i)$.

The above tangle replacement is called *braiding*. When D is oriented, then for $|x_i|>1$ we call the twist of (2) *parallel* or *reverse* (*antiparallel*), depending on whether both strands enter from the same left/right side, or from both. (If $x_i=\pm1$, we can consider a single crossing as either a parallel or an antiparallel twist.) We actually have two ways of braiding, depending on whether in the oriented diagram the twist becomes parallel or reverse. For example, for $x_i=3$:

(4)



The choice between the two braidings is (for now) irrelevant, but should be kept fixed for each crossing c_i of D, independently of x_i. We call a twist parallel or antiparallel according to its braiding, and positive or negative according to the sign of its crossings.

On properly adjusting the signs of the x_i, $D(x_1, \dots, x_n)$ becomes alternating, and we have already defined $\det(D(x_1, \dots, x_n))$. It is easy to see that the map

$$(x_1, \dots, x_n) \mapsto \det(D(x_1, \dots, x_n))$$

for x_i signed this way is a ("braiding") polynomial P, linear in all variables. Define then $\det(D(x_1, \dots, x_n))$ for arbitrarily signed x_i to be $|\widetilde{P}(x_1, \dots, x_n)|$, where $\widetilde{P}$ is the unique extension of P to $(2\mathbb{Z}+1)^{\times n}$. This procedure in particular allows calculating the determinant $\det(D)$ for arbitrary D.

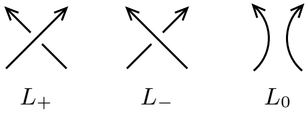
The determinant is an invariant of the underlying knot K, so its calculation does not depend on the choice of the diagram D, and hence we set $\det(K) := \det(D)$ for some diagram D of K. The advantage of using this method to determine $\det(K)$ is to remember that $\det(D)$ behaves (up to sign) linearly in all x_i.

Another important feature of the determinant is that it is odd if and only if the link is a knot, i.e. has only one component. More generally, the multiplicity of 2 in $\det(L)$ is at least (but not always equal to) $n-1$ for an n-component link L. (This can be seen from the identity $\det(L) = \pm\Delta_L(-1)$.)

Kauffman's model for the determinant was subsequently put into a nice language by Krebes [Kr], who showed how to calculate the determinant of arborescent knots (in the Conway [Co] sense), by showing that the "ratio" of the determinants of both closures of a 2-string (i.e. 4-end) tangle behaves additively under Conway's tangle sum operation. This method will be subsequently used, but we repeat below only a part of the formalism we need; see [Kr] for more details.

2.3. *Calculating the signature.* The signature σ is a $\mathbb{Z}$-valued invariant of knots and links. We know that $\sigma(L)$ has opposite parity to the number of components of the link L whenever $\Delta_L(-1) \neq 0$. This in particular always happens for L being a knot (remember that $\Delta_L(-1)$ is always odd in this case), so that σ takes only even values on knots. Most of the early work on the signature was done by Murasugi [Mu1], who showed several properties of this invariant.

Consider three links with diagrams differing just at one crossing:

(5) 

.

Then

$$\sigma(L_+) - \sigma(L_-) \in \{0, 1, 2\}, \tag{6}$$

$$\sigma(L_\pm) - \sigma(L_0) \in \{-1, 0, 1\}. \tag{7}$$

(Note: In the first property one can also have $\{0, -1, -2\}$ instead of $\{0, 1, 2\}$, since other authors, like Murasugi, take σ to be with opposite sign. Thus (6) not only defines a property, but also specifies our sign convention for σ.)

Further, Murasugi found the following important relation between $\sigma(K)$ and $\det(K)$ for a knot K:

$$\begin{aligned} \sigma(K) \equiv 0 \pmod 4 \;&\Leftrightarrow\; \det(K) \equiv 1 \pmod 4, \\ \sigma(K) \equiv 2 \pmod 4 \;&\Leftrightarrow\; \det(K) \equiv 3 \pmod 4. \end{aligned} \tag{8}$$

These conditions, together with the initial value $\sigma(\bigcirc) = 0$ for the unknot, and the additivity of σ under split union (denoted by "$\sqcup$") and connected sum (denoted by "#"),

$$\sigma(L_1 \# L_2) = \sigma(L_1 \sqcup L_2) = \sigma(L_1) + \sigma(L_2),$$

allow one to calculate σ for very many links. In particular, if we have a sequence of knots

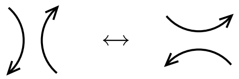
$$K_0 \to K_1 \to \cdots \to K_n$$

such that K_n is the unknot and K_i differs from K_{i-1} only by a crossing change, then (6) and (8) allow calculating $\sigma(K_i)$ inductively from $\sigma(K_{i+1})$ if $\det(K_i)$ is known.

From this the following property is evident for knots, which also holds for links: $\sigma(!L) = -\sigma(L)$, where $!L$ is the mirror image of L.

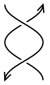
We will need the following operation (see also [Mu2]).

Definition 2.1. A *band-connecting* (or *plumbing of an annulus*) is the operation

(9) 
.

(Note that this always changes the number of components.)

Lemma 2.1. *If a link L_1 is obtained from a link L by band-connecting, then $|\sigma(L) - \sigma(L_1)| \le 1$.*

Proof. Use (7) and the fact that L_1 is obtained from L by smoothing out a crossing (replacement of $L_\pm$ by L_0 in (5)), when redrawing the l.h.s. of (9) as  . ■

2.4. *Tangle notation and families of links.* Some formulas for σ will be necessary, in particular those for both rational knots and links. We will describe them in some detail, since it will be important for what follows.

Conway [Co] introduced a notation for knot and link diagrams. Here it suffices to consider Conway notations which consist of a set of integers, to which two binary operations, named by Conway "sum" and "product", are applied, with various parenthesizations. Figure 1 shows how to obtain a diagram of a knot or link from its Conway notation. The diagram is the closure of the tangle with the same notation. The convention in composing the tangles is that a Conway notation with no negative integers gives an alternating diagram. The "product" (which is not associative!) is assumed to be left-associative, so that abc is understood to stand for $(ab)c$. We will often omit the product sign, but sometimes write it "$\cdot$" for clarity. Diagrams and their links describable in such a way are called *arborescent* or *Conway-algebraic*. For more details see [Ad, §2.3].

A *rational* knot or link is one with a rational diagram. Such a diagram is specified by a Conway notation that contains only a product with no parentheses, i.e. is a sequence of integers.

Let the *continued* (or *iterated*) *fraction* $[[s_1,\dots,s_m]]$ for integers s_i be defined inductively by $[[s]]=s$ and

$$[[s_1,s_2,\dots]] = s_1 - \frac{1}{[[s_2,\dots]]}.$$

The rational knot or link $S(p,q)$ in Schubert's [Sb] notation has the Conway notation

$$(-1)^{n-1}c_n \;\cdot\; (-1)^{n-2}c_{n-1} \;\cdot\; \dots \;\cdot\; -c_2 \;\cdot\; c_1, \tag{10}$$

when the c_i are chosen so that

$$[[c_1,\dots,c_n]] = \frac{p}{q}. \tag{11}$$

Without loss of generality one can assume that $(p,q)=1$, $|q|<|p|$, and that (exactly) one of p and q is even. (If both are odd, we replace q by $q\pm|p|$, the sign being determined by the condition $|q|<|p|$.) Note that $S(-p,-q)$ is the same knot or link as $S(p,q)$, while $S(-p,q)=S(p,-q)$ is its mirror image. $S(p,q)$ is a knot for p odd and a 2-component link for p even.

Then we can choose all c_i in (11) to be even (and non-zero). It is known that, with this choice of c_i, their number $n=1-\chi(S(p,q))$ is equal to twice the genus of $S(p,q)$ or twice the genus plus one, depending on whether $S(p,q)$

is a knot (i.e. p is odd and n even) or a 2-component link (p even, n odd). The primitive tangles in Figure 1 also specify a mirroring convention. When n and all c_i in the Conway notation are even, then the writhe, according to (3), of the crossings corresponding to the entry $(-1)^{i-1}c_i$ in (10) is $\mathrm{sgn}(c_i)$.

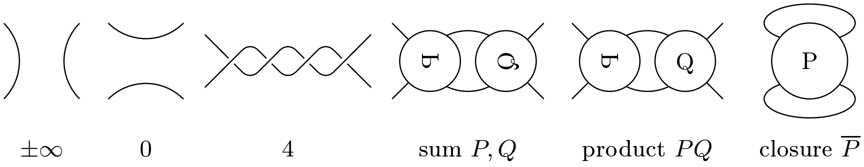


Fig. 1. Conway's primitive tangles and tangle operations

Theorem 2.2. *When c_i in* (10) *are even* (*and non-zero*), *we have*

$$\sigma(S(p,q)) = \sum_{i=1}^{1-\chi(S(p,q))} \mathrm{sgn}(c_i).$$

This formula follows from [HNK, p. 71]. Later, however, we will be able to give a brief independent proof. The formula will allow us to give statements on the distribution of signs in continued fractions related to integer points on some cubic curves.

In the case of links (p even), the interchange $q \leftrightarrow q \pm |p|$ corresponds to reversing the orientation of one of the components. For example, the Conway notation "2 -2 2" with $[[2,2,2]] = 4/3$ corresponds to the positive $(2,4)$-torus link with parallel orientation and signature $\sigma = \mathrm{sgn}(2) + \mathrm{sgn}(2) + \mathrm{sgn}(2) = 3$, while the Conway notation "4" with $[[4]] = 4/1$ corresponds to the positive $(2,4)$-torus link with reverse orientation and signature $\sigma = \mathrm{sgn}(4) = 1$.

For the purpose of calculating with continued fractions, it will be helpful to extend the operations "+" and "$1/\cdot$" to $\mathbb{Q} \cup \{\infty\}$ by $1/0 = \infty$, $1/\infty = 0$, $k + \infty = \infty$ for any $k \in \mathbb{Q}$. The reader may think of ∞ as the fraction $1/0$, to which one applies the usual rules of fraction arithmetic and reducing. In particular reducing tells that $-1/0 = 1/0$ so that for us $-\infty = \infty$. This may appear strange at first glance, but has a natural interpretation in the rational tangle context.

Rational knots with Conway notation $n\,2$ (with $n \neq 0$), or Schubert notation $S(p,2)$ (p odd) are called *twist knots.*

Montesinos knots/links (see e.g. [LT]) are generalizations of rational knots/links and special types of arborescent knots/links. They are denoted by $M(p_1/q_1, \dots, p_l/q_l; n)$, where $(p_i, q_i) = 1$ and $|p_i| > q_i$. (Note: there is a variety of conventions for the notation in the literature; mostly they differ from ours in signs.) Here p_i/q_i are continued fractions of rational tangles $c_{n_i,i} \dots c_{1,i}$ with $[[c_{1,i}, -c_{2,i}, c_{3,i}, \dots, (-1)^{n_i-1}c_{n_i,i}]] = p_i/q_i$. Then

$M(p_1/q_1, \ldots, p_l/q_l; n)$ corresponds to the Conway notation

$$(c_{n_1,1} \ldots c_{1,1}), (c_{n_2,2} \ldots c_{1,2}), \ldots, (c_{n_l,l} \ldots c_{1,l}), n0. \tag{12}$$

Note that for this to be a knot, at most one p_i can be even. If $l \le 2$, then the Montesinos knot or link is a rational knot/link.

The defining convention is that all $q_i > 0$, and if $p_i < 0$, then the tangle is composed so as to give a non-alternating sum with a tangle with $p_{i\pm1} > 0$. This defines the diagram up to mirror image, which is fixed by the choice of mirroring the primitive tangles in Figure 1. A typical example is shown in Figure 2.

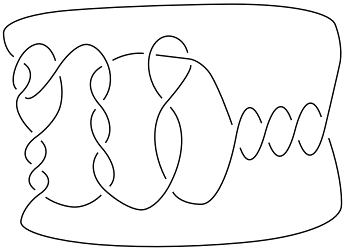


Fig. 2. The Montesinos knot $M(11/3, -4, 5/2; 4)$ with Conway notation $(213, -4, 22, 40)$

A *pretzel knot/link* is a special type of Montesinos knot/link, where all $q_i = 1$ (or equivalently all $n_i = 1$ in (12)).

A(n oriented) knot/link is called *positive* if it has a positive diagram. A positive diagram is one in which all crossings have sign 1, according to (3). See for example [N, St1]. Murasugi also proves special formulas for σ of alternating links L (see e.g. p. 437 of [Ka3]), which in case L is positive and non-split show $\sigma(L) = 1 - \chi(L)$, with $\chi(L)$ being the Euler characteristic of L. In particular, for the pretzel knot or link $(x_1, \ldots, x_l)$ with all x_i odd and positive, we have $\sigma = l - 1$.

3. Knot adjacency.

3. Knot adjacency. Before we start applying Theorem 1.1 to more general types of polynomials, we first consider the one variable case, which has some applications to knot theory and should help in understanding the multi-variable cases discussed later.

The original hope was to apply Theorem 1.1 to unknotting numbers. Although this has failed so far, the theorem has some applications to the more general concept of knot distance; see [DS, Mr, Ask]. (The *unknotting number* is the knot distance to the trivial knot.)

Definition 3.1. Two knots K_1 and K_2 have distance n if they can be interconverted by n, but not fewer, crossing changes. The knots are called *adjacent* if they have distance 1.

Recall that when considering a braiding at a particular crossing c_i of an oriented knot diagram D, we have in fact the two options of a parallel and an antiparallel braiding. In §2.2 we have intentionally abused the orientation when describing how to calculate the determinant. It behaves polynomially, independently of which particular choice of braiding is made at any crossing c_i (as long as this choice is kept fixed for different x_i).

However, now there is an important difference between the two braidings. In both cases the determinants form (up to sign) an arithmetic progression $a_1 + 2a_2x_i$, but in the case of the antiparallel braiding a_2 comes from the determinant of the link obtained by smoothing out c_i as in (5), while for the parallel braiding the other splicing (in the sense of (1)), yielding again a knot, must be applied. Thus a_2 is even in the antiparallel and odd in the parallel case, and we have

Lemma 3.1. *If at c_1 in D a parallel braiding is done*, *then*

$$\sigma(D(x_1+2,x_2,\dots,x_n)) - \sigma(D(x_1,x_2,\dots,x_n)) = 2$$

except exactly for one value of $x_1 \in 2\mathbb{Z}+1$ (*where the difference is* 0).

If at c_1 in D an antiparallel braiding is done, *then*

$$\sigma(D(x_1+2,x_2,\dots,x_n)) - \sigma(D(x_1,x_2,\dots,x_n)) = 0$$

except exactly for one value of $x_1 \in 2\mathbb{Z}+1$ (*where the difference is* 2) *if*

$$\det(D(x_1+2,x_2,\dots,x_n)) \neq \det(D(x_1,x_2,\dots,x_n)),$$

and without any exception otherwise.

This lemma will play a central role in all the considerations to follow, and will often be used without explicit reference.

Proof. Use (8) and (6). Note that for knots σ is even, so 1 cannot occur on the r.h.s. of (6). The exceptional value of x_1 occurs when the arithmetic progression of the determinants changes sign. ∎

An application of this lemma and of Theorem 1.1 yields a condition obstructing certain knots to be adjacent.

Theorem 3.1. *Let $K_{1,2}$ be knots with* $\det(K_1) > \det(K_2)$. *Assume one of the following three conditions is satisfied*:

(a) $\sigma(K_1) = \sigma(K_2) \equiv 4 \pmod 8$, $\det(K_1) \equiv 1 \pmod{\det(K_1) - \det(K_2)}$,

(b) $\sigma(K_1) = \sigma(K_2) \pm 2$, *there is a* $k \in \mathbb{N}$ *with* $\det(K_1) = k(\det(K_1) - \det(K_2)) + 1$ *and* $\sigma(K_1) \equiv \pm 2k + 4 \pmod 8$ (*the choice of* $+$ *or* $-$ *in the two "$\pm$" options being the same*),

(c) $\sigma(K_1) = \sigma(K_2) \pm 2$, *there is a* $k \in \mathbb{N}$ *with* $\det(K_1) = k(\det(K_1) - \det(K_2)) - 1$ *and* $\sigma(K_1) \equiv \pm 2(k-1) + 4 \pmod 8$ (*again with the same choice of signs*).

Then K_1 cannot be obtained from K_2 by one crossing change.

Note in particular the following special case of (a).

Corollary 3.1. *If* $\sigma(K) \equiv 4 \pmod 8$, *then K cannot be turned by one crossing change into a knot K' with* $\det(K') = \det(K) \pm 4$. ■

Proof of Theorem 3.1. This is an application of the lemma with $K_{1,2}$ represented by diagrams $D(\pm 1, x_2, \ldots, x_n)$ for fixed $x_2, \ldots, x_n$. Then consider the sequence $D(x_1) = D(x_1, x_2, \ldots, x_n)$ for odd x_1. The conditions are adjusted so that for suitable x_1 we get $\det(D(x_1)) = 1$ and $\sigma(D(x_1)) \equiv 4 \pmod 8$, giving a contradiction to Theorem 1.1. Note that among the two braidings in (4) at most one may produce a determinant 1 knot. In case (a) this is the antiparallel braiding, and in cases (b) and (c) the parallel one. In case (b) a determinant 1 knot is realized (when successively increasing $|x_i|$ by 2) just before the non-switch of the signature (in Lemma 3.1), and in (c) just after it. ■

Example 3.1. The simplest example is the pair of the trefoil and the figure-8-knot. We have thus an easy proof that they have distance two. Note that, similarly to rational knots of unknotting number 1 [KM], pairs of distance 1 rational knots can be described by applying the Culler–Gordon–Luecke–Shalen theorem about cyclic surgeries [CGLS], as done in [Mr]. This settles the distance 1 problem for many low crossing knots. However, compared to that heavy tool, our proof in this special case is almost elementary.

Example 3.2. If a knot K_1 of determinant 13 has $\sigma = 0$, like 6_3 (in the standard Rolfsen [Ro, appendix] notation), then by one crossing change it cannot be turned into any knot K_2 of determinant 7 or 11. If $\sigma(K_1) = 4$, like for $K_1 = 7_3$, then the same statement holds for (knots K_2 of) determinant 9. In the same way the distance from 7_5 to 8_{15} and $!8_5$ is not 1, partially solving two of the open entries in the table of [DS].

Example 3.3. If a knot has $\sigma = 0$ and determinant 41, like 10_{17}, then it cannot be turned into a knot of determinant 27 by one crossing change.

The arguments applied can also be used to show a similar non-existence result for links.

Corollary 3.2. *There is no* 2*-component link L with* $\det(L) = 2$ *and* $\sigma(L) \equiv \pm 3 \pmod 8$.

Proof. Connect the two components of such a link L by a half-twisted band, obtaining a knot K. By adding further (possibly reverse) twists to the band, one obtains a family of knots with determinants $\pm(4k+1)$. Thus this family contains a knot K' with determinant 1. However, $\sigma(K') = \sigma(L) \pm 1 \not\equiv 0 \pmod 8$, a contradiction. ■

Finally, we remark that Lemma 3.1 can be used to show Theorem 2.2.

Proof of Theorem 2.2. Consider the diagram of the rational link with Conway notation of even integers c_i. For all c_i positive, the diagram, and hence the rational link, is positive. Then by [N] it is special alternating, and we have the claim from the result $\sigma = 1 - \chi$ of [Mu1]. Changing the sign of some c_i corresponds to undoing positive/creating negative reverse twists at the same crossing. Lemma 3.1 implies that σ changes at most once under such a sequence of operations, and then by -2. This shows the formula with "$=$" replaced by "$\geq$". The reverse inequality follows by applying the same argument on the mirror images. ∎

4. Diophantine equations. Now we are going to apply the previous considerations to Diophantine equations. One simple series of examples concern the second highest elementary symmetric polynomial.

4.1. *Pretzel knots and elementary symmetric polynomials.* Let

$$\sigma_{p,q}(x_1, \ldots, x_q) = \Big[\prod_{i=1}^{q}(1 + tx_i)\Big]_{t^p} \tag{13}$$

be the elementary symmetric polynomial of degree p in q variables (here "$[\text{polynomial}]_{\text{monomial}}$" denotes the coefficient of "monomial" in "polynomial").

We will be concerned with the equation $\sigma_{l-1,l} = \pm 1$, because it turns out that $\sigma_{l-1,l}$ is the determinant of pretzel knots and links. We shall derive this relationship explicitly here, in order to give an idea how Krebes's method works. At a later stage we will content ourselves just with presenting the formulas for the determinants of the knots we consider.

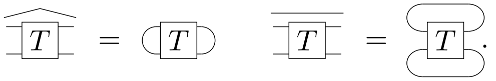
PROPOSITION 4.1. *$\sigma_{l-1,l}(x_1, \ldots, x_l)$ is the determinant of the $(x_1, \ldots, x_l)$ pretzel knot (or link).*

Proof. Krebes's invariant $\mathrm{Kr}(T)$ for a tangle T lies in the space $\Phi = \mathbb{Z} \times \mathbb{Z}/[(p,q) \sim (-p,-q)]$. We write p/q for $(p,q) \in \Phi$. Indeed, p/q can be thought of as a "fraction", apart from the more restrictive rule of reduction, since Φ is equipped with a binary operation $\oplus$ given by

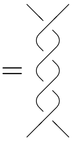
$$(p,q) \oplus (r,s) = (ps + qr, qs),$$

which is as the usual fraction addition (and will be named so below; though e.g. $1/3 \oplus 1/3 = 6/9 \neq 2/3$).

Krebes's invariant is defined by $\mathrm{Kr}(T) = \det(\overline{T})/\det(\widehat{T})$, where $\overline{T}$ and $\widehat{T}$ are the two closures of T:



Accordingly these closures are called the *denominator* and *numerator closure.* The latter is the (standard) closure shown in Figure 1. Take

$T_i =$  $\Bigg\}\, x_i$ half-twists.

(A negative number of half-twists means half-twists of opposite sign. We can, however, first consider just $x_i > 0$, in which case the pretzel tangle $(x_1, \dots, x_l)$ is alternating; the correctness of the formula for arbitrary x_i then follows from the above braiding sequence arguments.) We have $\mathrm{Kr}(T_i) = 1/x_i$. Now Kr is "additive":

$$\mathrm{Kr}((T_i0, T_j0)) = \mathrm{Kr}(T_i) \oplus \mathrm{Kr}(T_j),$$

where "," is Conway's tangle sum operator, and $\oplus$ is the above "fraction" addition in Φ. By iterating this rule, we obtain

$$\mathrm{Kr}(T_10, \dots, T_l0) = \frac{\sigma_{l-1,l}(x_1, \dots, x_l)}{\sigma_{l,l}(x_1, \dots, x_l)}.$$

The numerator on the right is the determinant of the closure of the $(x_1, \dots, x_l)$ pretzel tangle that gives the pretzel knot/link, and we are done. ∎

Clearly at most one of the x_i can be even in a solution of the equation $\sigma_{l-1,l} = \pm 1$. We start with a statement for the case when all x_i are odd, which has a particularly closed form.

THEOREM 4.1. *If* $l \equiv 5 \pmod 8$, *then the equation* $\sigma_{l-1,l}(x_1, \dots, x_l) = 1$ *has no solutions in odd* x_i *with at most one of them being of opposite sign to the others. The same holds if* $l \equiv 7 \pmod 8$ *for the equation* $\sigma_{l-1,l}(x_1, \dots, x_l) = -1$, *this time at most two of the* x_i *being allowed to have opposite sign to the others.*

REMARK 4.1. Note that in fact the second part of the statement implies the first (set $x_l = 1$, $x_{l-1} = -1$). Also, the solutions $x_i = \pm(-1)^i$ (with the same choice of ± for all $i = 1, \dots, l$) show that the number of negative x_i cannot be further restricted at least for $l = 5, 7$.

Proof. For l and x_i odd and positive the pretzel knot $(x_1, \dots, x_l)$ has signature $l - 1$, and the twists corresponding to the x_i are antiparallel. Thus changing the sign of some x_i reduces σ at most by two by Lemma 3.1. ∎

In the case that one x_i is even, the twists corresponding to the odd x_i are parallel, and the ones corresponding to the even ones among the x_i are parallel or antiparallel, depending on the parity of l. This time the congruence restriction we obtain is not on the number of variables but on their sum.

Theorem 4.2. *Let $l \in \mathbb{N}$, and x_0 be even and $x_1, \dots, x_l$ be odd integers. Then any solution of $\sigma_{l,l+1}(x_0, x_1, \dots, x_l) = \pm 1$ with $\sum_{i=1}^{l} x_i \equiv l+2 \pmod 8$ for l even, or $\sum_{i=0}^{l} x_i \equiv l+2 \pmod 8$ for l odd contains at least three negative integers.*

Proof. Let l be even and all $x_i > 0$. Then the signature of the $(x_0, x_1, \dots, x_l)$-pretzel link is $\sigma = \sum_{i=1}^{l}(x_i - 1)$ by the formula for σ of alternating links (see end of §2.4). The twists corresponding to x_i for $i > 0$ are parallel, and positive for $x_i > 0$. Therefore, if we let x_i decrease successively by 2, σ decreases every time by 2, except once. The twists corresponding to x_0 are antiparallel and negative for $x_0 > 0$. Therefore, if we let x_0 decrease successively by 2, σ increases at most once, by 2, and remains constant otherwise. Thus if at most two of the x_i $(0 \le i \le l)$ are negative, we have

$$\sum_{i=1}^{l}(x_i - 1) \le \sigma \le \sum_{i=1}^{l}(x_i - 1) + 4,$$

so that σ remains non-divisible by 8.

Similarly let l be odd. If all $x_i > 0$, the signature of the $(x_0, x_1, \dots, x_l)$-pretzel link is $\sigma = \sum_{i=0}^{l}(x_i - 1) + 1$. Now the twists corresponding to any x_i, $0 \le i \le l$, are parallel, and the crossings are positive for $x_i > 0$. Then the same argument applies. ∎

4.2. *Montesinos knots and iterated fractions.* In many situations in which we can address the problem $P(x_1, \dots, x_l) = \pm 1$, we can also say something about the more general equation

$$q_1 \cdot \ldots \cdot q_k P(p_1/q_1, \dots, p_k/q_k, x_{k+1}, \dots, x_l) = \pm 1,$$

where $(p_i, q_i) = 1$ and $1 \le k \le l$.

This situation occurs on the knot side when replacing twist(tangle)s by rational tangles. Sometimes, it is still possible to control σ after this replacement, which then depends on the signs of the (unique) non-zero even integers, expressing p_i/q_i as continued fractions, or some slight modification thereof, if both p_i and q_i are odd. We give some applications in the simplest situation, when replacing the twist tangles of the pretzel knots by rational tangles and obtaining Montesinos knots.

Let us consider $M(p_1/q_1, \dots, p_l/q_l; n)$, where p_i, q_i are all odd except p_1, which should be even, and l is odd (the p_i need *not* be positive).

Proposition 4.2. *Let $\sigma = \sigma(M(p_1/q_1, \dots, p_l/q_l; 2k)) \equiv 4, 6 \pmod 8$ be such that l and all p_i, q_i are odd except p_1. Then*

$$\sum_{i=1}^{l} p_i \prod_{i \ne j} q_j + 2m \prod_{j=1}^{l} q_j \ne \pm 1 \tag{14}$$

for $m \le k$. The same property holds for $m \ge k$ if $\sigma \equiv 2, 4 \pmod 8$.

Proof. The l.h.s. in (14) is the determinant of $M(p_1/q_1,\dots,p_l/q_l;2m)$. If we had equality in (14), then $M(p_1/q_1,\dots,p_l/q_l;2m)$ would have determinant 1. However, the twists corresponding to $2k$ are reverse, and so (by Lemma 3.1)

$$\sigma(M(p_1/q_1,\dots,p_l/q_l;2m))-\sigma(M(p_1/q_1,\dots,p_l/q_l;2k))\in\{0,2\operatorname{sgn}(m-k)\},$$

and $\sigma(M(p_1/q_1,\dots,p_l/q_l;2m))\not\equiv 0 \pmod 8$, a contradiction. ∎

If we write

$$\begin{aligned}\frac{p_1}{q_1}&=[[a_{1,1},\dots,a_{n_1,1}]], & \frac{p_2}{|p_2|-q_2}&=[[a_{1,2},\dots,a_{n_2,2}]],\\ \frac{p_3}{|p_3|-q_3}&=[[a_{1,3},\dots,a_{n_3,3}]], \quad \dots, & \frac{p_l}{|p_l|-q_l}&=[[a_{1,l},\dots,a_{n_l,l}]],\end{aligned}\tag{15}$$

with all $a_{i,j}$ even and non-zero (note that n_1 is odd, while all the other n_i are even), then using Lemma 2.1 we have

$$\sigma(M(p_1/q_1,\dots,p_l/q_l;2k))=-\sum_{i=1}^{n_1}\operatorname{sgn}(a_{1,i})+\sum_{i=2}^{l}\sum_{j=1}^{n_i}\operatorname{sgn}(a_{i,j})\pm 1,\tag{16}$$

because by plumbing an annulus (9) the twists of $2k$ can be made trivial, and one obtains the connected sum of $l-1$ rational knots and one rational link, $S(p_1,q_1)$, the latter being mirrored opposite to the defining (mirroring) convention for its notation. Thus the condition on the signature can be rewritten as

$$-\sum_{j=1}^{n_1}\operatorname{sgn}(a_{1,j})+\sum_{i=2}^{l}\sum_{j=1}^{n_i}\operatorname{sgn}(a_{i,j})\equiv\pm 3 \pmod 8.\tag{17}$$

PROPOSITION 4.3. *Let p_i,q_i and l be odd except p_1. If for the $a_{i,j}$ in* (15) *we have* (17), *then* (14) *holds for any $m\in\mathbb{Z}$.* ∎

Similar statements hold if l is even. Then the formulas become even more coherent. First, "$p_1/q_1=[[\dots]]$" must be replaced by "$\frac{p_1}{|p_1|-q_1}=[[\dots]]$" in (15). (This corresponds to reversing the orientation of one of the components of the rational link.) Moreover, the formula (16) requires the sign of $\sum_{j=1}^{n_1}\operatorname{sgn}(a_{1,j})$ to be reversed, as in the alternating diagram the sign of the crossings in the p_1/q_1 tangle is altered. So we obtain:

PROPOSITION 4.4. *Let p_i,q_i be odd except p_1, and l be even. Write*

$$\frac{p_i}{|p_i|-q_i}=[[a_{1,i},\dots,a_{n_i,i}]]$$

for $i=1,\dots,l$ (with n_i even except n_1, all $a_{i,j}\neq 0$ and even). If

$$\sum_{i=1}^{l}\sum_{j=1}^{n_i}\operatorname{sgn}(a_{i,j})\equiv\pm 3 \pmod 8,\tag{18}$$

then

$$\sum_{i=1}^{l} p_i \prod_{i\neq j} q_j \not\equiv \pm 1 \left(\bmod 2\prod_{j=1}^{l} q_j\right).$$

Here is an example to the last proposition showing how the signature can be applied to deduce properties of continued fractions related to integer points on special types of cubic curves [Ma].

Example 4.1. Consider $M(2x^3/3, y^2/5, x/7, -15/11; 0)$ for x, y odd. The determinant is the cubic curve $C(x,y) = 770x^3 + 231y^2 + 165x - 1575$. If for some odd integers $x, y > 0$ we have

$$770x^3 + 231y^2 + 165x - 1575 \equiv \pm 1 \pmod{2310},$$

and we write

$$\frac{2x^3}{2x^3-3} = [[a_{1,1}, \dots, a_{n_1,1}]], \qquad \frac{y^2}{y^2-5} = [[a_{1,2}, \dots, a_{n_2,2}]],$$
$$\frac{x}{x-7} = [[a_{1,3}, \dots, a_{n_3,3}]],$$

then because of $\frac{-15}{15-11} = [[-4, -4]]$ we have $\sum_{i<4,j} \operatorname{sgn}(a_{i,j}) \equiv 1, 3 \pmod 8$.

Similar considerations can also be made if p_1 and l are both odd, only that in this case a nice formula for the signature as (16) is *a priori* lacking, as the $2k$ twists have parallel orientation, and the plumbing cannot be applied.

Another version with the role of the product n of denominators (above $n = 1155$) and the value of the cubic curve $C(x,y)$ swapped can be obtained by considering tangles of the form Mn, where M is a Montesinos tangle and n is a primitive Conway tangle with n even. This time we obtain statements for the solutions of $C(x,y) \mid (n \pm 1)/2$.

4.3. *More general equations.* Pretzel and Montesinos knots are special types of knots, and thus the method can be applied in more generality. In particular, by the calculus of Krebes [Kr] one can very easily calculate the determinant for arborescent knots in terms of their Conway notation. We demonstrate by a few exemplary statements how to proceed, giving some applications to polynomials involving various combinations of $\sigma_{l-1,l}$'s. (Even the restriction to consider arborescent knots is not necessary, but chosen for simplicity.)

Theorem 4.3. *Let $k, l \in \mathbb{N}$ be integers with $k - l \equiv 2 \pmod 4$. Set*

$$\sigma_{n,2k} = \sigma_{n,2k}(a_1, \dots, a_{2k}) \quad \textit{and} \quad \sigma_{m,2l} = \sigma_{m,2l}(b_1, \dots, b_{2l}).$$

Then

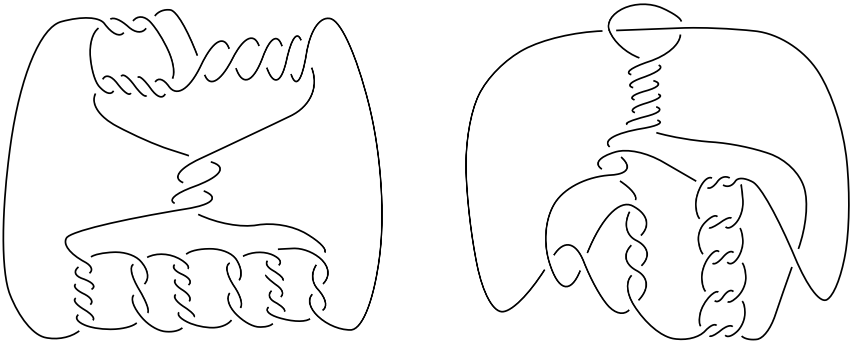
$$(19) \qquad \sigma_{2k-1,2k}\sigma_{2l-1,2l} + [\sigma_{2k,2k} + (2m+1)\sigma_{2k-1,2k}][\sigma_{2l,2l} + (2n+1)\sigma_{2l-1,2l}] = \pm 1$$

has no solutions in odd positive integers $a_1, \dots, a_{2k}, b_1, \dots, b_{2l}$ *and* $m, n \in \mathbb{Z}$. *The same statement holds for odd positive integers* $a_1, \dots, a_{2k}$ *and odd negative integers* $b_1, \dots, b_{2l}$ *if the condition* $k - l \equiv 2 \pmod 4$ *is replaced by* $k + l \equiv 3 \pmod 4$.

Proof. Consider the arborescent knot

$$K = ((a_1, \dots, a_{2k})\, 2m + 1)\, (2n + 1\, (b_1, \dots, b_{2l}))$$

(see Figure 3(a), where the example for $k = 3$, $l = 1$, $a_1 = a_3 = a_5 = b_2 = 5$, $a_2 = a_4 = a_6 = b_1 = 3$, $m = -2$ and $n = -3$ is shown). By plumbing two bands, the twists corresponding to the $2m+1$ and $2n+1$ can be trivialized, and one obtains a 3-component link L, which is the connected sum of two pretzel links $(a_1, \dots, a_{2k})$ and $(b_1, \dots, b_{2l})$ of opposite sign, oriented so that the twists of the a_i and b_j are antiparallel. We have $\sigma(L) = 2(k - l) \equiv 4 \pmod 8$, and thus (as plumbing of an annulus changes σ at most by ± 1) $\sigma(K) \equiv 2, 4, 6 \pmod 8$.



(a) (b)

Fig. 3

The determinant of K is found to be (up to sign) the l.h.s. of (19) by the calculus of Krebes. The + sign between the two products needs to be taken because we compose the tangles $(a_1, \dots, a_{2k})\, 2m + 1$ and $2n + 1\, (b_1, \dots, b_{2l})$, so that for a proper sign choice of m and n the diagram is alternating. The formula then follows for arbitrarily signed m and n, because the determinant behaves polynomially in m and n.

Taking the b_j to be negative means that we now consider a knot K as above, but this time L is the connected sum of two positive (or two negative) pretzel links, and thus $\sigma(L) = \pm(2k - 1 + 2l - 1) = \pm 2(k + l - 1)$. By the new congruence imposed, again $\sigma(L) \equiv 4 \pmod 8$, and the same argument applies. ∎

Remark 4.2. It should be noted that in this theorem the assumption that all a_i and b_j are positive/negative is essential. For example, $a_i = b_i =$

$(-1)^i$ gives a solution (which corresponds to unknotting the knot). Thus in particular the theorem cannot be proved by congruences.

Another result is shown in similar way by considering rational instead of pretzel tangles.

Definition 4.1. Define $P_i, Q_i \in \mathbb{Z}[x_1, \ldots, x_i]$ by $(P_i, Q_i) = 1$ and

$$[[x_1, \ldots, x_i]] = \frac{P_i(x_1, \ldots, x_i)}{Q_i(x_1, \ldots, x_i)}.$$

Alternatively, P_i and Q_i are defined recursively by

$$P_1(a_1) = a_1, \quad Q_1(a_1) = 1,$$
$$P_n(a_1, \ldots, a_n) = a_1 P_{n-1}(a_2, \ldots, a_n) - Q_{n-1}(a_2, \ldots, a_n),$$
$$Q_n(a_1, \ldots, a_n) = P_{n-1}(a_2, \ldots, a_n).$$

Proposition 4.5. *Let $a_1, \ldots, a_{2m}, b_1, \ldots, b_{2n}$ be non-zero even integers with*

$$\sum_{i=2}^{2m} \operatorname{sgn}(a_i) \equiv \sum_{i=2}^{2n} \operatorname{sgn}(b_i) \pmod 8.$$

Let $l \equiv 5 \pmod 8$, and write $P_m = P_{2m}(a_1, \ldots, a_{2m})$, $Q_m = Q_{2m}(a_1, \ldots, a_{2m})$, $P_n = P_{2n}(b_1, \ldots, b_{2n})$, $Q_n = Q_{2n}(b_1, \ldots, b_{2n})$, and $\sigma_{p,l} = \sigma_{p,l}(x_1, \ldots, x_l)$, with $\sigma_{p,l}$ as in (13)*. Then*

$$[P_m \sigma_{l-1,l} + Q_m \cdot (\sigma_{l,l} + \sigma_{l-1,l})] P_n + Q_m Q_n \sigma_{l-1,l} = \pm 1$$

has no solutions in odd integers $x_1, \ldots, x_l$ all positive or all negative, and a_i, b_j as above.

Proof. This time we consider the knot

$$K = ((x_1, \ldots, x_l)(-a_{2m}\, a_{2m-1} \ldots -a_2\, a_1 + 1))(-b_{2n}\, b_{2n-1} \ldots -b_2\, b_1)$$

(see Figure 3(b), where the example for $l = 5$, all $x_i = 3$ for $1 \le i \le 5$, $m = 2$, $n = 1$, $a_1 = a_2 = a_3 = -2$, $a_4 = 4$, $b_1 = 6$ and $b_2 = -2$ is shown). Again by plumbing two annuli, K can be turned into the connected sum of the rational links $L_1 = -a_{2m}\, a_{2m-1} \ldots -a_2$ and $L_2 = -b_{2n}\, b_{2n-1} \ldots -b_2$ with the pretzel knot $(x_1, \ldots, x_l)$. From the signature formula for rational knots (see §2) we have

$$\sigma(L_1 \# L_2) = -\sum_{i=2}^{2m} \operatorname{sgn}(a_i) + \sum_{i=2}^{2n} \operatorname{sgn}(b_i) \equiv 0 \pmod 8,$$

and the pretzel knot has signature $\pm(l-1) \equiv 4 \pmod 8$ (the sign according to whether all x_i are positive or negative). The rest of the argument is the same as before. ∎

Remark 4.3. It is clear that the conditions of the theorem can be relaxed. For example, it may be of interest to have more than two variables to range over both positive and negative numbers. In this direction we can allow one of the x_i to have a different sign from the others, as long as $\sigma_{l-1,l} > 0$. If at most one x_i has a different sign, then the pretzel has $\sigma = \pm(l-1)$ or $\sigma = \pm(l-3)$, depending on $|\sigma_{l-1,l}| \bmod 4$. But $\sigma_{l-1,l} \equiv 1 \pmod 4$ for odd x_i and $l \equiv 5 \pmod 8$, and thus $\sigma = \pm(l-1)$ is equivalent to the condition on the sign of $\sigma_{l-1,l}$.

We can also generalize Theorem 4.1 as follows. Let $g(D)$ be the (canonical) genus of D (see §2.1).

THEOREM 4.4. *To any diagram D of a knot K with $2g(D) = \sigma(K) \equiv 6 \pmod 8$ we can associate a polynomial P_D in $n = c(D)$ variables such that any solution of $P_D(x_1, \ldots, x_n) = \pm 1$ in odd integers contains at least three negative ones.*

Proof. Let P_D be the braiding polynomial of the determinant on D with antiparallel twists, the x_i parametrized to be positive on positive twists. Then clearly $2g(D) = \sigma(K)$ and the invariance of $g(D)$ under antiparallel twists implies that σ cannot increase anymore under positive twists, while it decreases at most once under negative twists at the same crossing. ■

The polynomials P_D for the maximal generators of genus g considered in [SV] contain all the other polynomials as special cases, i.e. by specializing values of some x_i. However, these values are not always positive, so that the statement for the maximal generators does not imply it for all other generators. Moreover, we know from [SV] that the number of maximal generators grows at least like 400^g, so that there is a large wealth of polynomials to which the theorem applies.

4.4. *Linear recurrent sequences.* Such sequences are the subject of intensive study. General results on properties like the number of realizations of a given integer [SS] require application of deep results in algebraic geometry [Ev, Fa], and are still far from being optimal.

Linear recurrent sequences can be made to enter our picture in a way explained in [St3] by considering determinants of rational knots whose Conway notation contains iterative patterns. The following theorem is certainly not the most general possible, but chosen so that its proof indicates how one can proceed in other cases. (Setting $i = 0$ specializes it to statements of the sort of Theorem 1.2.)

THEOREM 4.5. *Let $l > 0$ be odd, $x_1, \ldots, x_l$ be odd integers, and write $\widehat{\sigma} = \sigma_{l,l}(x_1, \ldots, x_l)$ and $\overline{\sigma} = \sigma_{l-1,l}(x_1, \ldots, x_l)$. Fix two non-zero even integers a_1 and a_2. Define a linear recurrent sequence $\{q_i\}$ for $i \geq 0$ by*

$$q_0 = 4\widehat{\sigma} + 11\overline{\sigma}, \quad q_1 = q_0(1 + a_1a_2) + 4a_2\overline{\sigma}, \quad q_{i+2} = (2 + a_1a_2)q_{i+1} - q_i.$$

Assume now that $|q_i| = 1$ *for some* i. *Let*

$$\sigma_i = i \cdot (\mathrm{sgn}(a_2) - \mathrm{sgn}(a_1)) + l + 1.$$

Then if $\sigma_i \equiv 6 \pmod 8$, *at least three of the* x_k *are negative. If* $\sigma_i \equiv 4 \pmod 8$, *at least two of the* x_k *are negative.*

Proof. Consider the rational knot K_i with notation $4\, -4\, -a_1\, -a_2\, -a_1\, -a_2\, \ldots\, -a_1\, -a_2$, with the subsequence $(-a_1\, -a_2)$ repeated i times. Since all numbers are even, the twists in each group are reverse. (They correspond to a Hopf plumbing of K_i.) In the group of "-4" we replace one crossing by a flipped $(-x_1, \ldots, -x_l)$ pretzel tangle, so that the twists counted by the $-x_l$ are reverse. The Conway notation then becomes

$$4 \cdot ((-x_1, \ldots, -x_l) \cdot -3) \cdot -a_1 \ldots - a_2.$$

Figure 4 shows the example for $l = 3$, $x_k = 3$ $(k = 1, 2, 3)$, $a_1 = -2$, $a_2 = 2$ and $i = 1$.

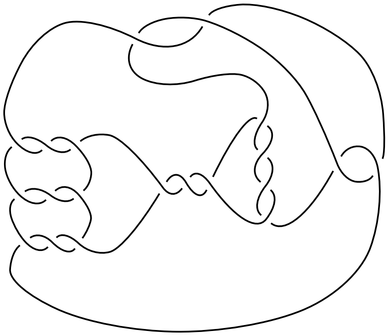


Fig. 4

Call the arborescent knot thus obtained $\overline{K}_i$. Then $\det(\overline{K}_i) = q_i$. To see this, first note that K_i corresponds to the iterated fraction $[[a_2, -a_1, \ldots, a_2, -a_1, 4, 4]]$. Then $\det(\overline{K}_i)$ is given by the numerator of

$$\left[\left[a_2, -a_1, \ldots, a_2, -a_1, \frac{11}{4} + \frac{\widehat{\sigma}}{\sigma}\right]\right].$$

Now one verifies the first three values for q_i, and uses an argument as in the proof of Theorem 7.4 in [St3] to establish the recurrence. (Unlike there, only three initial values are necessary, since the eigenvalues of the matrix appear only in powers 0 and $\pm i$, but not $\pm 2i$.) Now, if all x_i are positive, one can still turn the diagram of $\overline{K}_i$ into an alternating one, by a variant of the tangle isotopy that makes the rational tangle closing to K_i alternating. Then one sees that $\sigma_i = -\sigma(\overline{K}_i)$, and the rest of the argument is as before. ■

One can obtain statements about deeper (in length) recurrences by adding sequences under tangle composition, or by incorporating more iterative subsequences.

5. Problems. It would be interesting to see to what extent the above method can find applications to number theory, in particular to cubic curves. We have presented just a part of the situations in which it can be applied; there are several possibilities for extension. One can e.g. also consider non-arborescent knots, or 2-component links, applying Corollary 3.2 (in which case only one variable of the polynomial can be made to take either signs, as only two consecutive values of the signature are excluded). On the other hand, a combination with number-theoretic work may be desirable.

We conclude with two more specific problems.

5.1. *Determinants of signature 4 knots.* One can ask whether ±1 plays a special role in Theorem 1.1 and cannot be replaced by another integer. This is important at least because it could lead to another series of results of the above type.

The question whether each pair $(d, s) \in (2\mathbb{N}+1) \times 2\mathbb{N}$ satisfying the Murasugi condition (8) occurs as $(\det(K), \sigma(K))$ for some knot K was considered by Shinohara in [Sh] and observed to have a positive solution if $s \not\equiv 4 \pmod 8$ or $s \equiv 4 \pmod 8$ and $d \equiv 5 \pmod 8$. While a general positive answer seems natural and likely, Theorem 1.1 shows the difficulty of the case $s \equiv 4 \pmod 8$. One cannot obtain it by twisting arguments if twists are performed at only one place in the diagram, as in the proof of Theorem 3.1. Here is a point where knot theory fails and more sophisticated number theory may find its application.

Question 5.1. Let $S \subset 1 + 4\mathbb{N}$ be given by

$$S := \{\det(K) : \sigma(K) = 4\}.$$

Is $S = 5 + 4\mathbb{N}$?

Remark 5.1. Note that for any other value of $\sigma \equiv 4 \pmod 8$ the problem is equivalent because of connected sums with knots like 10_{124} (the $(3,5)$-torus knot) and their mirror images. Also the question for *prime* examples can be settled by the "KT grabber" method of [Bl], once (possibly composite) examples are found.

We summarize some simple properties of S.

Proposition 5.1. *S has the following properties.*

1) *If $p = 4l + 1$ and $4k + 3 \,|\, p$ with $k \geq 0$, then $p \in S$.*
2) *If $p \in S$, then $(4k + 1)p \in S$ for each $k \geq 0$.*

3) *S contains the value range of $\sigma_{l-1,l}$ with $l \equiv 5 \pmod 8$ on odd positive arguments.*
4) $1 \notin S$.
5) *S contains (besides further specific values) all integers $p = 4l+1$ with $1 < p < 2209$.*
6) *S contains infinitely many arithmetic progressions, for example $5+8k$, $5+12k$, $9+12k$ $(k \geq 0)$.*

Proof. 1) Consider connected sums of two positive twist knots.

2) Consider connected sum with a non-positive twist knot.

3) Consider the (generalized) pretzel knots $(x_1, \dots, x_l)$.

4) This is Theorem 1.1.

5) This is the outcome of a computer experiment, compiling the determinants of the knots of [HT] with $\sigma \equiv 4 \pmod 8$.

6) This is obtained by checking what determinant changes occur under the change of a crossing in a $\sigma = 4$ knot diagram, and then applying the iterated twist argument as in Theorem 3.1. For example, $5+12k$ comes from the sequence $5_1, 7_5, 9_7, \dots$. ■

5.2. *Arithmetic progressions.* One can obtain more arithmetic progressions contained in S by the methods of §3. If a knot K_1 with $\sigma \equiv 4 \pmod 8$ turns into a knot K_2 by one crossing change, then S contains an arithmetic progression $a_1 + a_2 k$ for $k \in \mathbb{N}$, where

$$(a_1, a_2) = \begin{cases} (\det(K_1) \bmod |\det(K_1) - \det(K_2)|, |\det(K_1) - \det(K_2)|) \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } \sigma(K_1) = \sigma(K_2), \\ (\det(K_1), \det(K_1) + \det(K_2)) \quad \text{if } \sigma(K_1) \neq \sigma(K_2). \end{cases}$$

One has *a priori* no reason to expect any particular feature of the pairs (a_1, a_2) so obtained, except that $a_1 \neq 1$ (and $4 \mid a_2$). However, examination of a large number of knots reveals striking regularities in the distribution of such pairs. Consider only pairs representing *maximal* progressions, i.e. if $a_2 \mid a_2'$, then $\{a_1' + a_2' k\} \subset \{a_1 + a_2 k\}$ with $a_1 = a_1' \bmod a_2$, and call such pairs (a_1, a_2) *maximal.* Then experiments suggest in particular the following properties of maximal pairs (a_1, a_2).

- a_1 is never a perfect square except in $12k+9$, i.e. $a_1 = 9$, $a_2 = 12$.
- $a_2/4$ is always a prime.
- For fixed $a_2 \neq 8$ there are exactly $(a_2/4 + 1)/2$ different values of a_1 with (a_1, a_2) being a pair.
- $a_1 = 5$, i.e. $a_2 k + 5$ is a progression, if and only if $a_2/4 \not\equiv \pm 1 \pmod 5$.

I have no explanation for these phenomena.

The table below summarizes the values of a_1 I found for small a_2.

a_2	a_1
8	5
12	5, 9
20	5, 13, 17
28	5, 13, 17, 21
44	13, 17, 21, 29, 33, 41
52	5, 13, 21, 33, 37, 41, 45
68	5, 17, 29, 37, 41, 45, 57, 61, 65

Using these series, a small calculation, and Proposition 5.1, we have

COROLLARY 5.1. *If* $p \equiv 1 \pmod 4$ *with* $p \notin S$, *then all prime divisors of* p *are of the form* $24k+1$ *and are not smaller than* 33049. ■

One can do much better if one uses the full list of progressions (not only those given in the above table). Applying the resulting larger number of congruence conditions, a search through the primes up to $4 \cdot 10^9$ failed to find one violating all of them. (Thus in particular S contains all numbers $p = 4l + 1 \geq 5$ up to this limit.) However, Dirichlet teaches that for any number of congruence classes there exist primes outside these classes, and in fact they are infinitely many, so that such a procedure can never be exhaustive.

References

[Ad] C. C. Adams, *The Knot Book*, W. H. Freeman, New York, 1994.

[Ask] N. Askitas, *Multi-# unknotting operations: a new family of local moves on a knot diagram and related invariants of knots*, J. Knot Theory Ramif. 7 (1998), 857–871.

[Bl] S. A. Bleiler, *Realizing concordant polynomials with prime knots*, Pacific J. Math. 100 (1982), 249–257.

[Co] J. H. Conway, *On enumeration of knots and links*, in: Computational Problems in Abstract Algebra, J. Leech (ed.), Pergamon Press, 1969, 329–358.

[CGLS] M. Culler, C. McA. Gordon, J. Luecke and P. B. Shalen, *Dehn surgery on knots*, Bull. Amer. Math. Soc. (N.S.) 13 (1985), 43–45.

[DS] I. D. Darcy and D. W. Sumners, *A strand passage metric for topoisomerase action*, in: KNOTS '96 (Tokyo), World Sci., River Edge, NJ, 1997, 267–278.

[Ev] J.-H. Evertse, *An improvement of the quantitative subspace theorem*, Compos. Math. 101 (1996), 225–311.

[Fa] G. Faltings, *Diophantine approximation on abelian varieties*, Ann. of Math. 133 (1991), 549–576.

[H] F. Hirzebruch, *Singularities and exotic spheres*, in: Séminaire Bourbaki 10, exp. No. 314, Soc. Math. France, Paris, 1995, 13–32.

[HNK] F. Hirzebruch, W. D. Neumann and S. S. Koh, *Differentiable Manifolds and Quadratic Forms*, Lecture Notes in Pure Appl. Math. 4, Dekker, New York, 1971.

[Ho] C. Hooley, *On Waring's problem*, Acta Math. 157 (1986), 49–97.

[HT] J. Hoste and M. Thistlethwaite, *KnotScape*, a knot polynomial calculation and table access program, http://www.math.utk.edu/˜morwen.

[Hu] D. Husemoller, *Elliptic Curves*, with an appendix by R. Lawrence, Grad. Texts in Math. 111, Springer, New York, 1987.

[J1] V. F. R. Jones, *A polynomial invariant of knots and links via von Neumann algebras*, Bull. Amer. Math. Soc. 12 (1985), 103–111.

[J2] —, *Hecke algebra representations of braid groups and link polynomials*, Ann. of Math. 126 (1987), 335–388.

[KM] T. Kanenobu and H. Murakami, *2-bridge knots of unknotting number one*, Proc. Amer. Math. Soc. 96 (1986), 499–502.

[Ka1] L. H. Kauffman, *On Knots*, Ann. of Math. Stud. 115, Princeton Univ. Press, 1987.

[Ka2] —, *State models and the Jones polynomial*, Topology 26 (1987), 395–407.

[Ka3] —, *An invariant of regular isotopy*, Trans. Amer. Math. Soc. 318 (1990), 417–471.

[Kr] D. Krebes, *An obstruction to embedding 4-tangles in links*, J. Knot Theory Ramif. 8 (1999), 321–352.

[LT] W. B. R. Lickorish and M. B. Thistlethwaite, *Some links with non-trivial polynomials and their crossing numbers*, Comment. Math. Helv. 63 (1988), 527–539.

[Ma] Yu. I. Manin, *Cubic Forms. Algebra, Geometry, Arithmetic*, 2nd ed., North-Holland Math. Library 4, North-Holland, Amsterdam, 1986.

[Mr] H. Murakami, *Some metrics on classical knots*, Math. Ann. 270 (1985), 35–45.

[Mu1] K. Murasugi, *On a certain numerical invariant of link types*, Trans. Amer. Math. Soc. 117 (1965), 387–422.

[Mu2] —, *On closed 3-braids*, Mem. Amer. Math. Soc. 151 (1974).

[N] T. Nakamura, *Positive alternating links are positively alternating*, J. Knot Theory Ramif. 9 (2000), 107–112.

[Ro] D. Rolfsen, *Knots and Links*, Publish or Perish, 1976.

[SS] H. P. Schlickewei and W. M. Schmidt, *The number of solutions of polynomial-exponential equations*, Compos. Math. 120 (2000), 193–225.

[Sb] H. Schubert, *Knoten mit zwei Brücken*, Math. Z. 65 (1956), 133–170.

[Sh] Y. Shinohara, *On the signature of knots and links*, Trans. Amer. Math. Soc. 156 (1971), 273–285.

[Sm] N. P. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Math. Soc. Student Texts 41, Cambridge Univ. Press, Cambridge, 1998.

[St1] A. Stoimenow, *Positive knots, closed braids and the Jones polynomial*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. 2 (2003), 237–285.

[St2] —, *Gauß sum invariants, Vassiliev invariants and braiding sequences*, J. Knot Theory Ramif. 9 (2000), 221–269.

[St3] —, *Generating functions, Fibonacci numbers, and rational knots*, J. Algebra 310 (2007), 491–525.

[SV] A. Stoimenow and A. Vdovina, *Counting alternating knots by genus*, Math. Ann. 333 (2005), 1–27.

[W] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. 141 (1995), 443–551.

[Z] D. B. Zagier, *Zetafunktionen und quadratische Körper*, Springer, Berlin, 1981.

Research Institute for Mathematical Sciences
Kyoto University
Kyoto 606-8502, Japan
E-mail: stoimeno@kurims.kyoto-u.ac.jp
http://www.kurims.kyoto-u.ac.jp/~stoimeno/

Received on 15.3.2007 (5407)