Origami Theorem Proving

Bruno Buchberger[1] , Tetsuo Ida[2]

□[1] Research Institute for Symbolic Computation (RISC), Johannes Kepler University, Linz, Austria,
□[2] Symbolic Computation Research Group (SCORE), University of Tsukuba, Japan.

Acknowledgement: Sponsored by Austrian FWF (Österreichischer Fonds zur Förderung der Wissenschaftlichen Forschung), Project 1302 in the frame of the SFB (Special Research Area) 013 "Scientific Computing".

■ Abstract

Origami paper folding has a long tradition in Japan's culture and education. The second author has recently developed a software system, based on functional logic programming and web-technology, for *simulating* origami paper folding on the computer (the "origami *computing* problem" or the "forward origami problem"). This system is based on the implementation of the six fundamental origami folding steps ("origami axioms") formulated by Huzita. In this paper, we consider the problem of automatically *proving* general theorems on the result of origami folding sequences (the "origami *proving* problem") using algebraic methods, in particular the first author's Gröbner bases method. We also give some comments on *finding* origami folding steps that result in a desired object (the "origami *solving* problem" or "*inverse* origami problem").

■ Introduction

■ The Forward Origami Problem

The origami software system developed by the second author allows to study the effect of sequences of origami folding steps on the computer, see [Ida 2003]. This system is implemented in Mathematica, see [Wolfram 1999] and can also be accessed over the web.

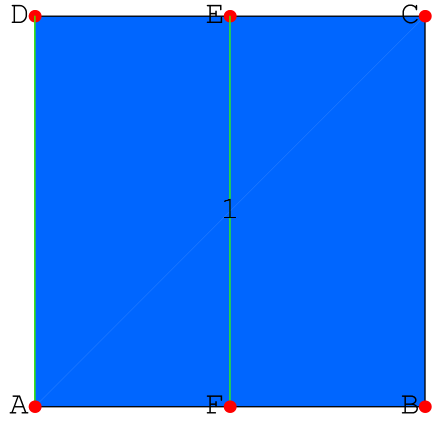
Here is a typical session, which illustrates part of a sequence of origami steps that construct an equilateral triangle starting from a square. (In the interactive web-based version of the system, the input is driven by a user−friendly menu, which is not shown here.) The input commands and the respective visualization of the folded 2−dobject should be self−explanatory:

```
DefOrigami[4, 4, MarkPoints → {"A", "B", "C", "D"}, Context → "MaxTriangle‘"];

FoldBring[1, A, B, MarkCrease → True]; ToStep[1, $markSymbols];
```

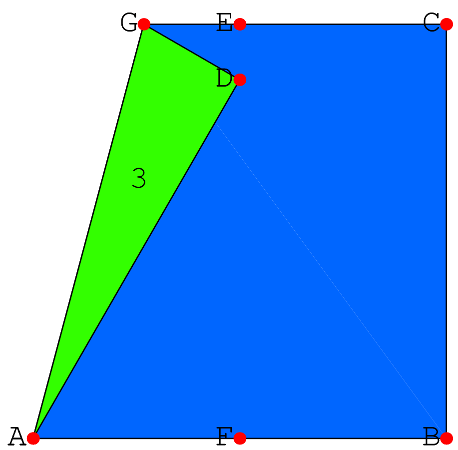
ShowOrigami[More → Graphics3D[{Hue[0.3], GraphicsLine[A, D], GraphicsLine[E, F]}]]

ShowOrigami::id : 1



FoldBrTh[1, D, Segment[E, F], A, 2, MarkCrease → True]; ShowOrigami[]

ShowOrigami::id : 2

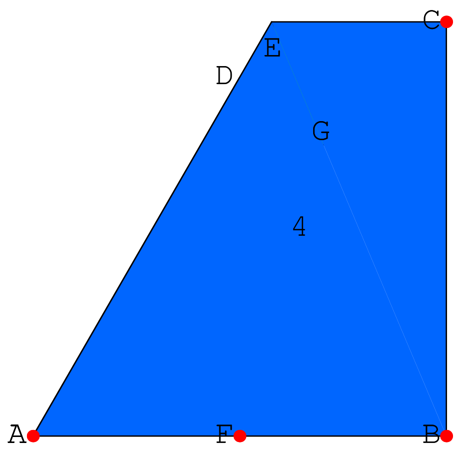


- Graphics3D -

FoldByLine[2, SegmentToLine[Segment[A, D]], G, Direction -> "Mountain"];

ShowOrigami[];

ShowOrigami::id : 3



etc.

■ The Inverse Origami Problem and the Origami Proving Problem

As we have seen, the current origami system of [Ida 2003] can simulate and visualize, by algebraic calculations that correspond to the six basic origami operations, the effect of any origami folding sequence, i.e. it solves what we call the "origami computing problem" or the "**origami forward problem**" (in analogy to the "**forward kinematics problem**" in robotics). In contrast, in this paper, we would like to discuss (and partly solve) the expansion of the capability of the system into the following two natural directions:

- The "**origami solving problem**" (or "**inverse origami problem**"): For a given initial origami shape and a final origami shape with certain desired properties, find a sequence of origami steps that transforms the initial into the final shape (or report "not origami solvable" if such a sequence does not exist).

- The "**origami proving problem**": For a given sequence of origami steps and a given property (out of a certain class of properties), *prove* that the resulting shape will satisfy the property (or disprove the property).

We will give a complete answer to the origami proving problem (for a well-defined wide class of theorems) and some preliminary remarks on the origami solving problem.

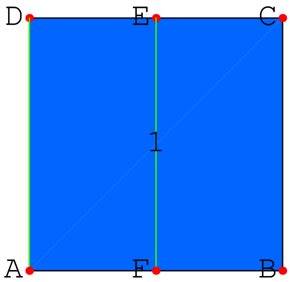
The algorithmics of origami, in itself, is an interesting research area. In addition, in the frame of the SFB (Sonderforschungsbereich = Special Research Area) "Scientific Computing" of the Austrian FWF funding agency, the algorithmics of origami is an excellent example of the fundamental and general three algorithmic aspects "computing (simplifying, forward solving, equivalence transforming, ...)", "solving (inverse solving, existential proving,...)", and "proving (universal proving, truth deciding, ...)", which have been chosen as the structuring principle for the various subprojects of the entire SFB.

An Example of an Origami Proving Problem and Its Solution by the Gröbner Bases Method

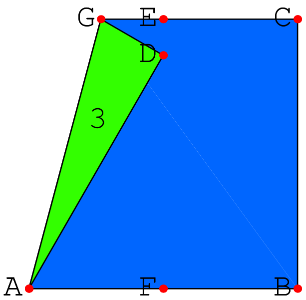
A Simple Solve Problem and a Simple Prove Problem

We start with the following simple origami solving problem: Starting from a square A, B, C, D, find a sequence of origami steps such that, finally, we arrive at an equilateral triangle.

Here is a first solution to the problem (which, however, does not yield maximum edge length): We first fold the square along the middle line EF. (This is a legal origami operation.)



Then we fix the point A and fold so that point D will lie on line EF. (This is a legal origami operation.)



Now we can do the analogous step with corner C, fixing B and bringing C onto the current position of D.

Then the triangle ADB is an equilateral triangle with edge length $\overline{AB}$. We could add a few easy origami operations that would result in hiding the areas that extend over the triangle ADB but we do not show these easy steps because we would like now to pose a simple proving problem:

Prove that, for all squares ABCD, $\overline{GD} = 2\,\overline{ED}$.

The Translation into a Prove Problem on Equalities

For deciding whether, for all ABCD, $\overline{GD} = 2\,\overline{ED}$, we first translate the question into a statement consisting of equalities:

First, note that $\overline{AB} = \overline{BC} = \overline{CD} = \overline{DA}$, since we start from a square. Hence, whenever the length of one of these four edges occurs, we replace it by $\overline{AB}$.

Now observe that

$$\overline{DF}^2 = \overline{AD}^2 - \overline{AF}^2 = \overline{AB}^2 - (\overline{AB}/2)^2 = 3/4\,\overline{AB}^2.$$

and

$$\overline{GD}^2 = \overline{GE}^2 + \overline{ED}^2 = (\overline{DC}/2 - \overline{GD})^2 + (\overline{EF} - \overline{DF})^2 = (\overline{AB}/2 - \overline{GD})^2 + (\overline{AB} - \overline{DF})^2.$$

We want to decide whether, under these assumptions,

$$\overline{GD} = 2\,\overline{ED} = 2\,(\overline{EF} - \overline{DF}) = 2\,(\overline{AB} - \overline{DF}).$$

For abbreviation, let's write

$$a = \overline{AB},\ \ b = \overline{GD},\ f = \overline{DF}.$$

Then, what we want to prove is that

$$\underset{a,f,b}{\forall}\left(\begin{cases} f^2 = 3/4\,a^2 \\ b^2 = (a/2 - b)^2 + (a - f)^2 \end{cases} \Rightarrow (b = 2\,(a - f))\right)$$

where the variables 'a', 'f', 'b' range over the real numbers. However, in fact, we will prove that the theorem is even true for all complex numbers (with the exception of a=0).

■ A Proof by Gröbner Bases

In this easy example, it can be easily verified, by a sequence of simplification steps, that the conclusion is a consequence of the premises (with the exception of the case a=0). However, for proceeding towards a general (and completely automatic) proving method for such theorems, let us formulate the proving steps in a more general setting by saying that the theorem would be proved if we could show that the polynomial

$$b - 2\,(a - f)$$

was in the ideal generated by the polyomials

$$f^2 - 3/4\,a^2$$

and

$$b^2 - (a/2 - b)^2 - (a - f)^2,$$

because if this is true then the conclusion polynomial is a linear combination of the two premise polynomials and, hence, the conclusion polynomial vanishes for all values a, b, f, for which the premise polynomials vanish.

Now, questions about polynomial ideal membership can be answered by the Gröbner bases method. (The Gröbner bases theory and method was introduced in [Buchberger 1970]. The few notions and facts of Gröbner bases theory needed in this paper can be found in [Buchberger 1998].)

The Gröbner bases method by now is implemented in all computer algebra systems. For example, in Mathematica we can execute the necessary steps in the following way: We first compute the Gröbner basis for the two premise polynomials (w.r.t. to the lexical ordering of the variables 'b', 'f', 'a')

$$G = \text{GroebnerBasis}[\{f^2 - 3/4\, a^2,\ b^2 - (a/2 - b)^2 - (a - f)^2\},\ \{b, f, a\}]$$

$$\{-3\, a^2 + 4\, f^2,\ -2\, a^2 + a\, b + 2\, a\, f\}$$

Now, by Gröbner bases theory, for checking whether the conclusion polynomial is in the ideal generated by the hypotheses polynomials, it suffices to check whether the conclusion polynomials can be reduced to zero by using the polynomials in the Gröbner basis G. In fact,

$$b - 2\,(a - f)$$

is irreducible modulo G because its leading power product b is neither a multiple of the leading power product f^2 of the polynomial $-3\,a^2 + 4\,f^2$ nor of the leading power product ab of the polynomial $-2\,a^2 + a\,b + 2\,a\,f$. (Note that we are working over the pure lexical ordering determined by b>f>a.)

This reduction could, in principle, also be executed within Mathematica. However, the current implementation of the reduction operation in Mathematica has a bug that results in reporting, errouneously, that b-2(a-f) *is* reducible modulo the premise polynomials!

Hence, the conclusion polynomial is not in the ideal generated by the premise polynomials and we cannot conclude that the theorem is true.

However, under the assumption that a≠0, the Gröbner basis G can be brought into the form

$$G0 = \{-3\, a^2 + 4\, f^2,\ -2\, a + b + 2\, f\}.$$

Now we see that, of course, the polynomial

$$b - 2\,(a - f)$$

can be reduced to zero modulo G0. This means that we have proved the following slightly more restricted form of the theorem:

$$\underset{a \neq 0, f, b}{\forall} \left(\begin{cases} f^2 = 3/4\, a^2 \\ b^2 = (a/2 - b)^2 + (a - f)^2 \end{cases} \Rightarrow (b = 2\,(a - f)) \right).$$

It is telling to analyze the original variant of the proposition

$$\underset{a, f, b}{\forall} \left(\begin{cases} f^2 = 3/4\, a^2 \\ b^2 = (a/2 - b)^2 + (a - f)^2 \end{cases} \Rightarrow (b = 2\,(a - f)) \right)$$

and to give account why it does not hold for a=0: If a=0 then f must be 0 by the first hypothesis but, since the second hypothesis reduces to

$$b^2 = b^2,$$

any b satifies the second hypothesis but, then, for a b≠0 the conclusion does not hold!

■ A Decision by Gröbner Bases

The approach in the previous section gave us a sufficient condition (expressed in terms of Gröbner bases computation and reduction) that guaranteed that the theorem was true. One can go one step further for obtaining a sufficient *and* necessary condition (expressed in terms of Gröbner bases) for deciding whether the theorem is true. For this we transform the theorem in the following way:

$$\underset{a, f, b}{\forall} \left(\begin{cases} f^2 = 3/4\, a^2 \\ b^2 = (a/2 - b)^2 + (a - f)^2 \end{cases} \Rightarrow (b = 2\,(a - f)) \right)$$

is equivalent to

$$\underset{a,f,b}{\neg\exists}\left(\begin{cases} f^2 = 3/4\,a^2 \\ b^2 = (a/2 - b)^2 + (a - f)^2 \\ b \neq 2\,(a - f) \end{cases}\right),$$

which is equivalent to

$$\underset{a,f,b,\xi}{\neg\exists}\left(\begin{cases} f^2 = 3/4\,a^2 \\ b^2 = (a/2 - b)^2 + (a - f)^2 \\ (b - 2\,(a - f))\,\xi = 1 \end{cases}\right),$$

Now, by one of the fundamental properties of Gröbner bases, this question can be decided by computing the (reduced) Gröbner basis

$$H = \text{GroebnerBasis}[\{f^2 - 3/4\,a^2,\ b^2 - (a/2 - b)^2 - (a - f)^2,\ (b - 2\,(a - f))\,\xi - 1\},\ \{\xi, b, f, a\}]$$

$$\{a,\ f^2,\ -1 + b\,\xi + 2\,f\,\xi\}$$

and to check whether or not this Gröbner basis is equal to {1}. Since this is not the case, we know that the above version of the theorem is not true. (Note that this is much more than saying that we cannot prove that the above version of the theorem is true!)

Now we do the same for the slightly restricted version of the theorem:

$$\underset{a\neq 0,f,b}{\forall}\left(\begin{cases} f^2 = 3/4\,a^2 \\ b^2 = (a/2 - b)^2 + (a - f)^2 \end{cases} \Rightarrow (b = 2\,(a - f))\right)$$

is equivalent to

$$\underset{a,f,b}{\neg\exists}\left(\begin{cases} a \neq 0 \\ f^2 = 3/4\,a^2 \\ b^2 = (a/2 - b)^2 + (a - f)^2 \\ b \neq 2\,(a - f) \end{cases}\right),$$

which is equivalent to

$$\underset{a,f,b,\xi,\eta}{\neg\exists}\left(\begin{cases} a\,\eta = 1 \\ f^2 = 3/4\,a^2 \\ b^2 = (a/2 - b)^2 + (a - f)^2 \\ (b - 2\,(a - f))\,\xi = 1 \end{cases}\right),$$

Now, again, this question can be decided by computing the (reduced) Gröbner basis

$$J = \text{GroebnerBasis}[\{a\,\eta - 1,\ f^2 - 3/4\,a^2,\ b^2 - (a/2 - b)^2 - (a - f)^2,\ (b - 2\,(a - f))\,\xi - 1\},\ \{\xi, \eta, b, f, a\}]$$

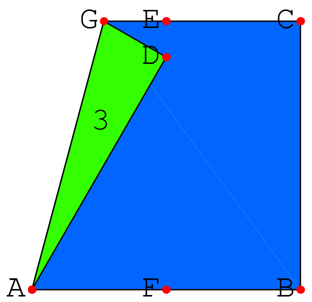
$$\{1\}$$

and to check whether or not this Gröbner basis is equal to {1}. Since this is the case, we know that the restricted version of the theorem is true.

■ Another Example of Origami Proving by Gröbner Bases

■ An Alternative Construction of an Equilateral Triangle

We start the construction in the same way as in the first example:



Now we do the same construction once more, this time starting from the edge $\overline{AB}$, yielding a point H instead of G.

Then the assertion is that AGH is an equilateral triangle, i.e. that $\overline{AG} = \overline{GH}$. For this it suffices to prove that

$$a^2 + b^2 = 2\,(a - b)^2.$$

■ The Translation into a Prove Problem on Equalities

By translation into the algebraic language of equalities, the following theorem has to be proved:

$$\underset{a,f,b}{\forall}\left(\begin{cases} a \neq 0 \\ f^2 = 3/4\,a^2 \\ b^2 = (a/2 - b)^2 + (a - f)^2 \end{cases} \Rightarrow (a^2 + b^2 = 2\,(a - b)^2)\right)$$

Here, we already added the restriction

$$a \neq 0.$$

■ Decision of the Problem by the Gröbner Bases Method

$$\underset{a,f,b}{\forall}\left(\begin{cases} a \neq 0 \\ f^2 = 3/4\,a^2 \\ b^2 = (a/2 - b)^2 + (a - f)^2 \end{cases} \Rightarrow (a^2 + b^2 = 2\,(a - b)^2)\right)$$

is equivalent to

$$\underset{a,f,b}{\neg\exists}\left(\begin{cases} a \neq 0 \\ f^2 = 3/4\,a^2 \\ b^2 = (a/2 - b)^2 + (a - f)^2 \\ a^2 + b^2 \neq 2\,(a - b)^2 \end{cases}\right),$$

which is equivalent to

$$\underset{a,f,b,\xi,\eta}{\neg\exists}\left(\begin{cases} a\,\eta - 1 = 0 \\ f^2 = 3/4\,a^2 \\ b^2 = (a/2 - b)^2 + (a - f)^2 \\ (a^2 + b^2 - 2\,(a - b)^2)\,\xi = 1 \end{cases}\right).$$

Now, again, this question can be decided by computing the (reduced) Gröbner basis

$$K = \text{GroebnerBasis}[\{a\,\eta - 1,\ f^2 - 3/4\,a^2,\ b^2 - (a/2 - b)^2 - (a - f)^2,\ (a^2 + b^2 - 2\,(a - b)^2)\,\xi - 1\},\ \{\xi, \eta, b, f, a\}]$$

{1}

K is {1}. This shows that the theorem is true.

A General Decision Algorithm for the Origami Proving Problem and Its Implementation in Mathematica / *Theorema*

The Decision Problem

Once again we want to emphasize that, of course, for the two easy example theorems above the proof can be established straightforwardly by high-school mathematics. Similarly, the proof of many such theorems could be given by ad hoc invention of appropriate proof steps. The point is that we want to establish a *general algorithm* which, for any such proposition about the result of a sequence of origami steps, decides whether or not the proposition is true and, in case it is true, establishes a proof. The algorithm can already be read from the two easy examples above.

First of all, let us specify which class of propositions are in the scope of the decision algorithm:

It is clear that the result of any of the admissible six origami operations (according to the origami axiom system by Huzita) can be described by a polynomial equality in the coordinates of the points in an origami construction. Now let $\mathcal{O}$ be the class of propositions of the following structure:

$$\underset{a,b,c,\ldots}{\forall}\ (C \Rightarrow (p = q))$$

where C is a conjunction of equalities between arithmetical expressions in numerical constants and the variables a, b, c, ... that denote coordinates of points corresponding to the operations in an origami construction and p and q are also arithmetical expressions.

Thus for example, the above two theorems are in $\mathcal{O}$ but the proposition stating that the second construction above yields the equilateral triangle of maximum length inscribed in the initial square is *not* in $\mathcal{O}$ because the maximum operation cannot be described in a purely equational theory. Still, $\mathcal{O}$ is a very big class of statements that includes a huge class of interesting properties of the result of origami constructions.

In fact, it is known, see e.g. [Buchberger 1998] that the following class $\mathcal{B}$ of statements that contains $\mathcal{O}$ as a proper subclass admits a decision algorithm: $\mathcal{B}$ is the class of statements of the form

$$\underset{a,b,c,\ldots}{\forall}\ M$$

or of the form

$$\underset{a,b,c,\ldots}{\exists}\ M$$

where M is a Boolean combination of equalities between arithmetical expressions in numerical constants and the variables a, b, c, ... We give a short summary of the decision algorithm for $\mathcal{B}$ in the next section.

A Decision Algorithm for the Class $\mathcal{B}$

The Algorithm

The decision algorithm, roughly, proceeds as follows:

- Bring all equalities in M into the form p=0 where p is a polynomial.
- By de Morgan, bring the formula always into the form

$$\underset{a,b,c,...}{\forall} N.$$

- Then bring M into conjunctive normal form and distribute $\forall$ over the conjunctive parts. Treat each of the parts

$$\underset{a,b,c,...}{\forall} P$$

separately. Note that P is now a disjunction

$$E_1 = 0 \vee ... \vee E_k = 0 \vee N_1 \neq 0 \vee ... \vee N_m \neq 0$$

of equalities and negations of equalities.

- Now

$$\underset{a,b,c,...}{\forall} (E_1 = 0 \vee ... \vee E_k = 0 \vee N_1 \neq 0 \vee ... \vee N_m \neq 0)$$

is transformed into

$$\neg \underset{a,b,c,...}{\exists} (E_1 \neq 0 \wedge ... \wedge E_k \neq 0 \wedge N_1 = 0 \wedge ... \wedge N_m = 0)$$

and further on to

$$\neg \underset{a,b,c,...,\xi_1,...,\xi_k}{\exists} (E_1\, \xi_1 - 1 = 0 \wedge ... \wedge E_k\, \xi_k - 1 = 0 \wedge N_1 = 0 \wedge ... \wedge N_m = 0)$$

with new variables $\xi_1, \ldots, \xi_k$ ("Rabinovich trick").

- Now, the latter question is a question on the solvability of a system of polynomial equations, which can be decided by computing the reduced Gröbner basis of $\{E_1\, \xi_1 - 1, \ ..., \ E_k\, \xi_k - 1, N_1, \ ..., \ N_m\}$. Namely, one of the fundamental theorems of Gröbner bases theory tells us that this Gröbner basis will be {1} iff the system is unsolvable (i.e. has no common zeros), which was first proved in [Buchberger 1970], see also [Buchberger 1998].

▫ The Implementation in *Theorema*

The decision algorithm is already implemented within *Theorema* [Buchberger et al. 2000] using the implementation of the author's Gröbner bases algorithm in Mathematica [Wolfram 1999]. In the *Theorema* implementation, one can call the algorithm by, first, specifying the formula which one wants to prove

Formula["Origami", any[a, f, b],
$$\underset{b,f,a}{\forall} \left(a \neq 0 \wedge \left(a^2 - f^2 - (\tfrac{a}{2})^2 = 0\right) \wedge \left(b^2 - (\tfrac{a}{2} - b)^2 - (a-f)^2 = 0\right) \Rightarrow (2 * (a - f) = b)\right) \qquad \text{"(1)"}$$
]

and then calling the Gröbner bases prover by

Prove[Formula["Origami Theorem"], using → {}, by → GroebnerBasesProver].

The result will be the following proof (including the intermediate English explanations), which will be stored in an extra Mathematica notebook:

Prove:

(Formula (Origami): (1))

$$\underset{b,f,a}{\forall}\left(a \neq 0 \bigwedge \left(a^2 - f^2 - (\frac{a}{2})^2 = 0\right) \bigwedge \left(b^2 - (\frac{a}{2} - b)^2 - (a-f)^2 = 0\right) \Rightarrow (2 * (a - f) = b)\right),$$

with no assumptions.

Proved.

The Theorem is proved by the Groebner Bases method.

The formula in the scope of the universal quantifier is transformed into an equivalent formula that is a conjunction of disjunctions of equalities and negated equalities. The universal quantifier can then be distributed over the individual parts of the conjunction. By this, we obtain:

Independent proof problems:

(Formula (Origami): (1).1)

$$\underset{a,b,f}{\forall}\ ((a = 0) \bigvee (2 * a + (-b) + (-2) * f = 0) \bigvee \frac{3}{4} * a^2 + (-f^2) \neq 0 \bigvee \frac{-5}{4} * a^2 + a * b + 2 * a * f + (-f^2) \neq 0)$$

We now prove the above individual problems separately:

Proof of (Formula (Origami): (1).1):

This proof problem has the following structure:

(Formula (Origami): (1).1.structure)

$$\underset{a,b,f}{\forall}\ (\text{Poly3}[1] \neq 0 \vee \text{Poly3}[2] \neq 0 \vee (\text{Poly3}[3] = 0) \vee (\text{Poly3}[4] = 0)),$$

where

$$\begin{aligned} \text{Poly3}[1] &= \frac{3}{4} * a^2 + (-f^2) \\ \text{Poly3}[2] &= \frac{-5}{4} * a^2 + a * b + 2 * a * f + (-f^2) \\ \text{Poly3}[3] &= a \\ \text{Poly3}[4] &= 2 * a + (-b) + (-2) * f \end{aligned}$$

(Formula (Origami): (1).1.structure) is equivalent to

(Formula (Origami): (1).1.implication)

$$\underset{a,b,f}{\forall}\ ((\text{Poly3}[1] = 0) \wedge (\text{Poly3}[2] = 0) \Rightarrow (\text{Poly3}[3] = 0) \vee (\text{Poly3}[4] = 0)).$$

(Formula (Origami): (1).1.implication) is equivalent to

(Formula (Origami): (1).1.not–exists)

$$\underset{a,b,f}{\nexists}\ (((\text{Poly3}[1] = 0) \wedge (\text{Poly3}[2] = 0)) \wedge (\text{Poly3}[3] \neq 0 \wedge \text{Poly3}[4] \neq 0)).$$

By introducing the slack variable(s)

$\{\xi 7, \xi 8\}$

(Formula (Origami): (1).1.not-exists) is transformed into the equivalent formula

(Formula (Origami): (1).1.not−exists−slack)

$$\nexists_{a,b,f,\xi 7,\xi 8} (((\text{Poly3}[1] = 0) \wedge (\text{Poly3}[2] = 0)) \wedge \{-1 + \xi 7\, \text{Poly3}[3] = 0,\ -1 + \xi 8\, \text{Poly3}[4] = 0\}).$$

Hence, we see that the proof problem is transformed into the question on whether or not a system of polynomial equations has a solution or not. This question can be answered by checking whether or not the (reduced) Groebner basis of

$$\{\text{Poly3}[1], \text{Poly3}[2], -1 + \xi 7\, \text{Poly3}[3], -1 + \xi 8\, \text{Poly3}[4]\}$$

is exactly $\{1\}$.

Hence, we compute the Groebner basis for the following polynomial list:

$$\left\{-1 + a\,\xi 7,\ -1 + 2\,a\,\xi 8 + (-1)\,b\,\xi 8 + (-2)\,f\,\xi 8,\ \frac{3\,a^2}{4} + (-1)\,f^2,\ \frac{-5\,a^2}{4} + a\,b + 2\,a\,f + (-1)\,f^2\right\}$$

The Groebner basis:

$$\{1\}$$

Hence, (Formula (Origami): (1).1) is proved.

Since all of the individual subtheorems are proved, the original formula is proved.

□

Note that the proof automatically generated by the Gröbner bases prover of *Theorema* also contains the explanation of the method and does not only give the "yes" or "no" decision. This is desirable for didactical purposes so that each call of the prover for a concrete example proposition also explains the general strategy in the concrete example. We do not show, in the proof text, the individual steps of the Gröbner bases computation, which corresponds to the didactic and logical principle that a proof in some area of mathematics should only contain the proof steps on the highest level, specific to the particular area, and should leave out the details on lower levels, which at this stage are considered to be "routine". In fact, in our case, the actual computation of the Gröbner basis could consist of thousands and even millions of steps depending on the proposition to be decided.

■ An Implementation of Origami Proving in *Theorema* / Mathematica

Combining the Origami Simulation Software by [Ida 2003], which is written in Mathematica, the implementation of the Gröbner bases algorithm of [Buchberger 1970] in Mathematica, the implementation of the above decision algorithm in *Theorema* [Buchberger et al. 2000] (which is also implemented in Mathematica), and a new tool in *Theorema*, which can translate geometrical descriptions of configurations into the corresponding polynomial equalites, developed in the recent PhD thesis [Robu 2002] and also implemented in Mathematica, we will soon be able to offer a coherent tool written in Mathematica that can

- ○ simulate arbitrary origami sequences both algebraically and graphically,
- ○ translate conjectures about properties of the results of origami sequences into statements in the form of universally quantified boolean combinations of polynomial equalities,
- ○ decide the truth of such conjectures and produce a proof or refutation of the conjecture fully automatically.

■ Approaches to the Origami Solving Problem

We did not yet study the Origami solving problem, which asks for *finding* a sequence of origami steps that will lead to a origami object with a desired property. However, it is clear that this problem is analogous to the problem of finding geometric objects with desired properties using only compass and ruler. Note, however, that the two problems – origami construction and compass / ruler construction – are *not* equivalent. In fact origami operations are more powerful than compass / ruler operations. For example, trisection of angles is possible by origami but not by compass / ruler. However, in analogy to the compass / ruler construction problem, Galois theory suggests itself as the main approach to solving the origami construction problem.

■ References

[Buchberger 1970] B. Buchberger.
Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems (An Algorithmical Criterion for the Solvability of Algebraic Systems of Equations).
Aequationes mathematicae 4/3, 1970, pp. 374–383.
(English translation in: B. Buchberger, F. Winkler (eds.), Gröbner Bases and Applications, Proceedings of the International Conference "33 Years of Groebner Bases", 1998, RISC, Austria, London Mathematical Society Lecture Note Series, Vol. 251, Cambridge University Press, 1998, pp. 535 –545.)

[Buchberger 1998] B. Buchberger.
Introduction to Groebner Bases.
In: Groebner Bases and Applications (B. Buchberger, F. Winkler, eds.),
Cambridge University Press, 1998, pp.3–31.

[Buchberger et al. 2000] B. Buchberger, C. Dupre, Tudor Jebelean, F. Kriftner, Koji Nakagawa, D. Vasaru, W. Windsteiger.
The *Theorema* Project: A Progress Report.
In: Symbolic Computation and Automated Reasoning (Proceedings of CALCULEMUS 2000, Symposium on the Integration of Symbolic Computation and Mechanized Reasoning, August 6–7, 2000, St. Andrews, Scotland), M. Kerber and M. Kohlhase (eds.), A.K. Peters, Natick, Massachusetts, pp. 98–113.

[Ida 2003] T. Ida.ko
Constructing Origami on the Internet.
In: D. Petcu, V. Negru, D. Zaharie, T. Jebelean (eds.), Symbolic and Numeric Algorithms for Scientific Computing (Proc. of the 5th International SYNASC Workshop, Oct. 1–4, 2003, Timisoara, Romania), Mirton Publishing Company, ISBN 973–661–104-3p. 40.

[Robu 2002] J. Robu.
Automated Geometric Theorem Proving.
PhD Thesis, RISC (Research Institute for Symbolic Computation), Johannes Kepler University Linz, Austria, 2002.s

[Wolfram 1999] S. Wolfram.
The Mathematica Book.
Wolfram Media and Cambridge University Press, 4th edition, 1999.