An Equivalence for Origami-Constructibility

Jialu Wang

Definition 1. Fix complex numbers $z_1, \ldots, z_n$ and set $F := \mathbb{Q}(z_1, \ldots, z_n) \subset \mathbb{C}$. A complex number z is *origami-constructible over* F if, after identifying $\mathbb{C} \cong \mathbb{R}^2$, the point corresponding to z can be obtained from the initial points $\{0, 1, z_1, \ldots, z_n\}$ after a finite sequence of constructions using the following Alperin's axioms (1)–(6). At each step we include the intersection point of two constructed lines.

(1) The line connecting two constructible points is a constructible line.

(2) The point of coincidence of two constructible lines is a constructible point.

(3) The perpendicular bisector of the segment connecting two constructible points is a constructible line.

(4) The line bisecting any given constructed angle can be constructed.

(5) Given a constructed line ℓ and constructed points P, Q, then whenever possible, the line through Q which reflects P onto ℓ can be constructed.

(6) Given constructed lines ℓ, m and constructed points P, Q, then whenever possible, any line which simultaneously reflects P onto ℓ and Q onto m can be constructed.

Lemma 1. *Let E/F be a finite field extension. Let $\overline{E}/F$ be the normal closure of E over F. If $[E : F] \in \{2, 3\}$, then $[\overline{E} : F] = 2^a 3^b$ for some $a, b \in \mathbb{Z}_{\geq 0}$.*

Proof. Since 2 and 3 are prime numbers, by the tower law, there is no proper middle field between F and E. This implies E is obtained by adjoining an element α where $\alpha \in E \setminus F$, so the normal closure $\overline{E}$ equals the splitting field L of f over F. Let f be the minimal polynomial of α with degree $n \in \{2, 3\}$.

When $n = 2$, f splits in E, then $E = \overline{E}$. Therefore, $[\overline{E} : F] = 2$.

When $n = 3$, set $G := \mathrm{Gal}(L/F)$. By the natural action of G on the three roots $\{\alpha, \beta, \gamma\}$ of f, we obtain an embedding $G \hookrightarrow S_3$. Since f is irreducible, the action is transitive, which implies G should be S_3 or A_3. Hence $|G| = [\overline{E} : F] \in \{3, 6\}$.

□

Theorem 1. *Fix points $z_1, \ldots, z_n \in \mathbb{C}$ and set $F = \mathbb{Q}(z_1, \ldots, z_n) \subset \mathbb{C}$. For any $z \in \mathbb{C}$ the following statements are equivalent:*

(1) *z is origami-constructible over F.*

(2) *There exists a chain of subfields of $\mathbb{C}$*

$$F = F_0 \subset F_1 \subset \cdots \subset F_r$$

such that $[F_{i+1} : F_i] \in \{2, 3\}$ for each i, and $z \in F_r$.

(3) *Let K/F be the splitting field of the minimal polynomial of z over F, and let $G = \mathrm{Gal}(K/F)$. Then there exist nonnegative integers a, b such that*

$$|G| = 2^a 3^b.$$

Proof. (1) $\Rightarrow$ (2) : Suppose F is closed under complex conjugation without loss of generality. Let O_F be the field of origami-constructible numbers, starting with the numbers $0, 1, z_1, \ldots, z_n$. By a proof similar to that of [1, Theorem 5.2], we can derive that O_F is the smallest subfield of $\mathbb{C}$ that contains F and closed under square roots, cube roots and complex conjugation.

Let O'_F be O_F ignoring closed under complex conjugation. If $z \in O'_F$, there exists a tower $F = E_0 \subset E_1 \cdots \subset E_m$ such that $[E_{i+1} : E_i] \in \{2, 3\}$ for each i, and $z \in E_m$. To make O'_F closed under conjugation, we add further extension $E_{i+1} \subset \overline{E_{i+1}}$ after each extension $E_i \subset E_{i+1}$ with $[E_{i+1} : E_i] \in \{2, 3\}$. Then we get a tower

$$F \subset F[a_1] \subset \overline{F[a_1]} \subset \overline{F[a_1]}[a_2] \subset \overline{\overline{F[a_1]}[a_2]} \subset \cdots \subset \overline{\overline{\overline{F[a_1]}[a_2]} \cdots [a_m]}$$

where the minimal polynomials of $a_1, a_2, \cdots, a_m$ have degree two or three. If $z \in O_F$, it is contained in the top field for such field tower.

Case 1: If $E_i \subset E_{i+1}$ has degree 2 by adjoining α where the minimal polynomial of α is $x^2 + px + q$ for $p, q \in E_i$, we add further extension $E_{i+1} \subset \overline{E_{i+1}}$. Observe that $E_{i+1} = \{a + b\alpha \mid a, b \in E_i\}$, and we suppose E_i is closed under complex conjugation (Induction from F), then the complex conjugate of $a + b\alpha$ is $\overline{a} + \overline{b}\,\overline{\alpha}$ where $\overline{a}, \overline{b} \in E_i$, which gives $\overline{E_{i+1}} \cong E_{i+1}(\overline{\alpha})$. And since $\alpha^2 + p\alpha + q = 0$, $\overline{\alpha}$ satisfies $x^2 + \overline{p}x + \overline{q}$ where $\overline{p}, \overline{q} \in E_i \subset E_{i+1}$, thus $E_{i+1} \subset \overline{E_{i+1}}$ has degree less than or equal to two depending on whether $x^2 + \overline{p}x + \overline{q}$ is irreducible over E_{i+1}.

Case 2: Similar to Case 1, if $E_i \subset E_{i+1}$ has degree 3, $E_{i+1} \subset \overline{E_{i+1}}$ has degree less than or equal to three.

Therefore, the further extension for conjugation has degree one, two or three, consistent with statement (2).

(2) $\Rightarrow$ (3) : Suppose there exists a tower $F = F_0 \subset F_1 \subset \cdots \subset F_r$ such that $[F_i : F_{i-1}] \in \{2, 3\}$. Let $z \in F_r$ with the minimal polynomial f over F. Let K be the splitting field of f over F. Let $\overline{F_r}/F$ be the normal closure of F_r over F. Since $[F_i : F_{i-1}] \in \{2, 3\}$, by lemma, $[\overline{F_i} : F_{i-1}] = 2^{a_i} 3^{b_i}$ for some $a_i, b_i \in \mathbb{Z}_{\geq 0}$. Note that $\overline{F_{i-1}}$ is the minimal normal closure that contain F_{i-1}, then $F_{i-1} \subset \overline{F_{i-1}} \subset \overline{F_i}$, which implies $[\overline{F_i} : \overline{F_{i-1}}]$ divides $[\overline{F_i} : F_{i-1}]$. So $[\overline{F_i} : \overline{F_{i-1}}] = 2^c 3^d$ for some $c, d \in \mathbb{Z}_{\geq 0}$. We get

$$F \subset \overline{F_1} \subset \cdots \subset \overline{F_r}$$

with $[\overline{F_i} : \overline{F_{i-1}}] = 2^{a_i} 3^{b_i}$ for some $a_i, b_i \in \mathbb{Z}_{\geq 0}$ for each i. Therefore, by tower law $[\overline{F_r} : F] = 2^a 3^b$ for some $a, b \in \mathbb{Z}_{\geq 0}$. Since $F \subset K \subset \overline{F_r}$, then $[K : F]$ divides $[\overline{F_r} : F]$, so $[K : F] = 2^{a'} 3^{b'}$ for some nonnegative numbers a', b'.

(3) $\Rightarrow$ (2) : Suppose group G has order $2^a 3^b$ for some nonnegative numbers a, b, then by Burnside's theorem, G is solvable, so there exists

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright \{1\}$$

such that $G_i / G_{i+1} \cong C_2$ or C_3 (Lagrange's theorem). By Galois theory, there exists a chain of fixed field:

$$F = K^{G_0} \subset F_1 = K^{G_1} \subset \cdots \subset F_m = K$$

with $[F_{i+1} : F_i] = [G_i : G_{i+1}] \in \{2, 3\}$. Since K/F is the splitting field of the minimal polynomial of z over F, $z \in K$.

(2) $\Rightarrow$ (1) : Suppose there exists a tower

$$F = F_0 \subset F_1 \subset \cdots \subset F_r$$

such that $[F_{i+1} : F_i] \in \{2, 3\}$ for each i, and $z \in F_r$. Note that the field of origami-constructible numbers O_F is still closed under the square roots and the cubic roots though the starting point set is enlarged from $\{0, 1\}$ to $\{0, 1, z_1, \ldots, z_n\}$; the argument is the same as in [1, §§4–5, esp. pp. 127–129].

If $[F_{i+1} : F_i] = 2$, $F_{i+1} \cong F_i(\alpha)$ where α satisfies a minimal polynomial of degree two over F_i. By quadratic formula, α can be expressed using field operation and square roots over F_i, so the elements in $F_i(\alpha)$ are origami-constructible.

If $[F_{i+1} : F_i] = 3$, $F_{i+1} \cong F_i(\beta)$ where β satisfies a minimal polynomial of degree three over F_i. By Cardano's formula, β can be expressed using field operation, square roots and cubic roots over F_i, so the elements in $F_i(\beta)$ are origami-constructible.

Therefore, $z \in F_r$ is origami-constructible over F. $\square$

Question 1. *If z is a two-fold constructible number (see [2, §4] for two-fold axioms), what constraint can be imposed on the step degrees $[F_{i+1} : F_i]$ in a tower of fields*

$$F = F_0 \subset F_1 \subset \cdots \subset F_r$$

with $z \in F_r$?

Proposition 1 (Answer to Question 1)**.** *Let $F \subset \mathbb{C}$ be a base field and let $z \in \mathbb{C}$ be a two-fold constructible number over F. Then there exists a tower of subfields*

$$F = F_0 \subset F_1 \subset \cdots \subset F_r$$

with $z \in F_r$ and $[F_i : F_{i-1}] \leq 192$ for every i.

Proof. Consider a single two-fold step whose data lie in a field $F \subset \mathbb{C}$. Its construction yields a polynomial system in four unknowns consisting of four equations, each of degree at most 4. The all-degree-4 pattern (alignment type AL8, AL9) has Jacobian of rank < 4 in general, hence it does not generically determine the two folds finitely. Therefore, in any realizable two-fold step at least one equation has degree ≤ 3.

Write the four unknowns as $u = (u_1, u_2, u_3, u_4)$. By the discussion preceding, we have a system

$$f_1(u) = f_2(u) = f_3(u) = f_4(u) = 0, \qquad f_j \in F[u_1, u_2, u_3, u_4],\ \deg f_1 \leq 3,\ \deg f_2, \deg f_3, \deg f_4 \leq 4.$$

Set $A := F[u_1, u_2, u_3, u_4]/(f_1, f_2, f_3, f_4)$. Realizability implies that this system has finitely many solutions (counted with multiplicities), hence A is finite-dimensional. By Bézout's theorem,

$$\dim_E A \ \leq\ \prod_{j=1}^{4} \deg(f_j) \ \leq\ 3 \cdot 4 \cdot 4 \cdot 4 \ =\ 192.$$

Let $P = (P_1, P_2, P_3, P_4)$ be any solution of the system in some field extension of F. Define a homomorphism

$$\phi : A \twoheadrightarrow F(P_1, P_2, P_3, P_4) =: F_1, \qquad u_i \mapsto P_i.$$

It is well-defined because it sends f_1, f_2, f_3, f_4 to zero. And it is surjective. Hence

$$[F_1 : F] = \dim_F F_1 \ \leq\ \dim_F A \ \leq\ 192.$$

Thus a single two-fold step enlarges the field by a finite extension of degree at most 192. Iterating over the n steps of the construction we obtain fields

$$F \subset F_1 \subset \cdots \subset F_r, \qquad [F_i : F_{i-1}] \leq 192 \ \ (1 \leq i \leq r),$$

with the constructed number $z \in F_r$. $\square$

References

[1] Roger C. Alperin. A mathematical theory of origami constructions and numbers. *New York Journal of Mathematics*, 6:119–133, 2000.

[2] Roger C. Alperin and Robert J. Lang. One-, two-, and multi-fold origami axioms. In Robert J. Lang, editor, *Origami^4: Fourth International Meeting of Origami Science, Mathematics, and Education*, pages 371–393. A K Peters, Natick, MA, 2009.