CYCLOTOMIC POINTS AND ALGEBRAIC PROPERTIES OF POLYGON DIAGONALS

Thomas Grubb
Department of Mathematics, University of California San Diego, San Diego, California, United States
tgrubb@ucsd.edu

Christian Wolird
Department of Mathematics, University of California San Diego, San Diego, California, United States
christianwolird@gmail.com

Received: 4/21/20, Accepted: 3/30/21, Published: 4/20/21

Abstract

By viewing the regular N-gon as the set of Nth roots of unity in the complex plane we transform several questions regarding polygon diagonals into when a polynomial vanishes when evaluated at roots of unity. To study these solutions we implement algorithms in Sage as well as examine a trigonometric diophantine equation. In doing so we classify when a metallic ratio can be realized as a ratio of polygon diagonals, answering a question raised in a PBS Infinite Series broadcast. We then generalize this idea by examining the degree of the number field generated by a given ratio of polygon diagonals.

1. Introduction

The study of rational solutions to (possibly several) polynomial equations has a long history and needs no introduction. Lately there has been interest in extending this line of study to other types of algebraic numbers. In particular, one may ask the following. Given k multivariate polynomials $f_1, \ldots, f_k$ from $\mathbb{Q}[x_1, \ldots, x_n]$, does there exist a point $(\zeta_1, \ldots, \zeta_n)$ with both

- ζ_j a root of unity for all j, and
- $f_i(\zeta_1, \ldots, \zeta_n) = 0$ for all i?

Such a solution will be called a *cyclotomic point* or *cyclotomic solution* to the equations defined by the f_i. Lang had conjectured that such solutions can be given in terms of finitely many parametric families [16]. This has since been verified via work of Ihara, Serre, and Tate [16] and Laurent [17]. Recent work has been centered around developing methods for computing the parametric families of cyclotomic solutions to a given set of equations. In doing so one finds applications to properties of regular polgyons [21] and to solving trigonometric diophantine equations [6].

The easiest paradigm of this question involves finding zeroes of univariate polynomials which are roots of unity; this was carried out by Bradford and Davenport [2], who gave a concise algorithm for finding such factors. This has since been extended by Beukers and Smyth to the setting of algebraic plane curves [4], and generalized to arbitrary dimensions by Aliev and Smith [1]. These papers will form the backbone of our results; those interested in further constructive results and explicit methods may additionally explore [18], [22], and [23].

Our main contribution is to apply existing algorithms to explicitly compute the cyclotomic solutions to two specific polynomials. In doing so we are able to solve two classification problems.

The first of our main results regards metallic means, which are extensions of the well known golden ratio $\phi_1 = \frac{1+\sqrt{5}}{2}$. The golden ratio is ubiquitous in combinatorics and other areas, making appearances with respect to the Fibonacci sequence, irrationality and Diophantine approximation [13], and even topological entropy [10]. Naturally the golden ratio has been extended to *metallic means*; for an integer $n \geq 1$ define the nth metallic mean by

$$\phi_n = \frac{n + \sqrt{n^2 + 4}}{2}.$$

The formula comes from the generalized Fibonacci recursion

$$F_k^{(n)} = nF_{k-1}^{(n)} + F_{k-2}^{(n)}$$

with appropriate initial conditions; see [12] or [11] for analysis of metallic means.

It is well known that both the golden ratio ϕ_1 and the *silver ratio* ϕ_2 can be expressed as a ratio of diagonals in a regular polygon:

By *diagonal* we mean the distance between any two distinct vertices of a polygon, so side lengths are allowed. In a PBS Infinite Series broadcast, Perez-Giz raised the question of whether or not the same statement is true for ϕ_n for any $n \geq 3$ [20]. This question was in fact answered negatively by Buitrago for the *bronze ratio* ϕ_3 several years previously [5]. The methods used were entirely numeric, and did not extend to $n \geq 4$. Our first contribution is to answer Perez-Giz's question for a more general class of metallic means, which we now define.

Let c be a real number with $c^2 \in \mathbb{Q}$. Define the *generalized metallic mean* ϕ_c to be the larger root of the quadratic equation $x^2 - cx - 1 = 0$. That is to say,

$$\phi_c = \frac{c + \sqrt{c^2 + 4}}{2}.$$

Note that this formula returns a standard metallic mean if c happens to be an integer. We now present our first classification theorem regarding these numbers.

Theorem 1. *Let c be a real number with $c^2 \in \mathbb{Q}$ and let ϕ_c be the corresponding generalized metallic mean as above. Then ϕ_c can be realized as a ratio of diagonals in a regular polygon if and only if*

$$c \in \{0, \pm 1, \pm \tfrac{3}{2}, \pm 2, \pm\sqrt{2}, \pm\sqrt{5}, \pm\sqrt{12}, \pm\tfrac{\sqrt{2}}{2}, \pm\tfrac{\sqrt{6}}{6}, \pm\tfrac{2\sqrt{3}}{3}, \pm\tfrac{\sqrt{12}}{12}\}.$$

Explicit constructions are given in Section 3, and the proof framework is simple to describe. By viewing the regular N-gon as the set of Nth roots of unity in the complex plane, one can translate the question of Theorem 1 into writing ϕ_c as a ratio

$$\phi_c = \frac{|1 - \zeta_N^a|}{|1 - \zeta_N^b|}$$

for some primitive root of unity ζ_N and for two integers a, b. With simple algebraic manipulations one can translate this into finding a polynomial $f(t, x, y)$ such that equation (1) holds if and only if $f(c, \zeta_N^a, \zeta_N^b) = 0$. To finish, we use elimination theory and the algorithmic tools for finding cyclotomic points on curves mentioned above to classify when solutions of this form exist.

After proving Theorem 1 we will discuss a generalization of the realization of metallic means as ratios of polygon diagonals. For a given Nth root of unity ζ_N, let $\mathbb{Q}(\zeta_N)^+$ denote the maximal totally real subfield of the extension $\mathbb{Q}(\zeta_N)/\mathbb{Q}$; explicitly, $\mathbb{Q}(\zeta_N)^+ = \mathbb{Q}(\zeta_N + \zeta_N^{-1})$. Given diagonals of a regular polygon $d_1 = |1 - \zeta_N^a|$ and $d_2 = |1 - \zeta_N^b|$, a simple manipulation shows that the d_i lie inside the real cyclotomic field $\mathbb{Q}(\zeta_{4N})^+$. Should a ratio $\frac{d_1}{d_2}$ equal a metallic mean, then $\frac{d_1}{d_2}$ will generate at most a degree four subextension of $\mathbb{Q}(d_1, d_2)/\mathbb{Q}$. Thus it is natural to ask more generally, can one classify all pairs of diagonals d_1, d_2 for which $\frac{d_1}{d_2}$ generates at most a degree C extension of $\mathbb{Q}$, for some constant $C > 0$? Towards this end, we offer the following.

Theorem 2. *Let $d_1 = |1 - \zeta_N^a|$ and $d_2 = |1 - \zeta_N^b|$ be diagonals of a regular N-gon, with $\gcd(a, b) = 1$. Letting ϕ denote Euler's totient function, we have:*

- *If N is odd, then $[\mathbb{Q}(\frac{d_1}{d_2}) : \mathbb{Q}] = \frac{\phi(4N)}{4}$.*
- *If N is even, then $[\mathbb{Q}(\frac{d_1}{d_2}) : \mathbb{Q}] \geq \frac{\phi(4N)}{10}$.*

A direct consequence of this is that, for any $C > 0$, there are only finitely many ratios of diagonals which generate an extension of degree at most C. Moreover, these ratios can be listed explicitly using simple bounds on the totient function ϕ. As an example of this, we will use Theorem 2 to give an alternate proof of Theorem 1 at the end of Section 4.

Theorem 2 will be proven in Section 4 as a consequence to Proposition 1, in which we analyze the index of $\mathbb{Q}(\frac{d_1}{d_2})$ inside $\mathbb{Q}(\zeta_{4N})^+$. This analysis is similar to the proof of Theorem 1 in that it reduces to solving equations in roots of unity. However, due to an increased number of parameters, it is infeasible to use the same computational proof. We get around this by reducing our original equation to a trigonometric diophantine equation, to which we can apply results of Włodarski [27] and Conway and Jones [6].

The rest of this paper is outlined as follows. In Section 2 we give a brief review of the algorithmic tools developed in [1], [2], and [4]. The theoretical background will allow us to implement an algorithm in Sage [26] in order to solve Theorem 1; the discussion of this will take place in Section 3. The methods used to prove Theorem 1 do not extend to a proof of Theorem 2, as it is computationally infeasible to apply the techniques of Section 2 to this question. Section 4 will be dedicated to solving this problem by using a trigonometric diophantine equation; we end the section with an analytic question that could provide an interesting future avenue of research.

2. Tools for Finding Cyclotomic Points

In this section we will discuss algorithms for finding cyclotomic points on various objects. We will start with the simplest case: finding cyclotomic roots to a univariate polynomial. From there we will build up to finding cyclotomic points on families of curves. We emphasize that much of the theory discussed here may be found in [4]; the only minor novelty that we require is to allow for a rational parameter instead of solely looking for cyclotomic solutions.

2.1. Preliminary Definitions and Lemmas

Given a univariate polynomial $f(x) \in \mathbb{C}[x]$ we define the (squarefree) *cyclotomic part* of f to be

$$Cf(x) = \prod_{f(\zeta)=0} (x - \zeta)$$

where the product runs over all roots of unity on which f vanishes.

We will need the following lemma of Beukers and Smyth which characterizes roots of unity and polynomials vanishing on roots of unity.

Lemma 1 (BS02, Lemma 1). *If $g(x) \in \mathbb{C}[x]$ with $g(0) \neq 0$ is a polynomial with the* *property that for every zero α of g, at least one of $\pm\alpha^2$ is a zero of g, then all zeroes of g are roots of unity. Furthermore, if ω is a root of unity, then it is conjugate (over $\mathbb{Q}$) to exactly one of $-\omega$, ω^2, or $-\omega^2$.*

From this two important lemmas follow.

Lemma 2. *Suppose $g(t,x) \in \mathbb{Z}[t,x]$ vanishes at (t_0,ω) with $t_0 \in \mathbb{Q}$ and ω a root of unity. Then one of*

$$\begin{aligned} g_1(t,x) &:= g(t,-x) \\ g_2(t,x) &:= g(t,x^2) \\ g_3(t,x) &:= g(t,-x^2) \end{aligned}$$

also vanishes at (t_0,ω). □

Lemma 3. *Suppose $g(t,x) \in \mathbb{Z}[t,x]$ is an irreducible polynomial which is nonconstant in both t and x. Then $g(t,x) \nmid g(t,\pm x^2)$.*

Proof. Suppose $g(t,x)$ divides $g(t,\pm x^2)$. For any fixed t_0, Lemma 1 thus implies that the roots of $g(t_0,x)$ are all roots of unity. It is known that there are only finitely many monic polynomials of a given degree whose zeroes are all on the unit circle; these are the so-called *Kronecker polynomials*. See [15] for the original reference, or [9] for a modern treatment. Since for any t_0, $g(t_0,x)$ is a scalar multiple of a Kronecker polynomial we may conclude by the pigeonhole principle that there is a Kronecker polynomial $K(x)$ and infinitely many distinct constants t_k for which $g(t_k,x) = c_k K(x)$ for some real numbers c_k.

We finish by writing

$$g(t,x) = \sum_{j=0}^{N} C_j(t)x^j$$

for some coefficient polynomials $C_j(t)$. The previous paragraph shows that the $C_j(t_k) = C_{j'}(t_k)$ for all k, and hence the coefficient polynomials are all identical. This gives a factorization $g(t,x) = C_N(t)K(x)$; the assumption that $g(t,x)$ is nonconstant in both t and x guarantees that $C_N(t)$ and $K(x)$ are nonconstant and hence we have a proper factorization of $g(t,x)$, contradicting our hypothesis. □

Finally we give a trivariate analog of Lemma 2.

Lemma 4. *Suppose $f(t,x,y) \in \mathbb{Z}[t,x,y]$ vanishes at (t_0,ω,τ) with $t_0 \in \mathbb{Q}$ and ω,τ roots of unity. Then one of*

- $f_1(t,x,y) := f(t,-x,y)$,
- $f_2(t,x,y) := f(t,x,-y)$,

- $f_3(t, x, y) := f(t, -x, -y)$,
- $f_4(t, x, y) := f(t, x^2, y^2)$,
- $f_5(t, x, y) := f(t, -x^2, y^2)$,
- $f_6(t, x, y) := f(t, x^2, -y^2)$,
- $f_7(t, x, y) := f(t, -x^2, -y^2)$

vanishes at (t_0, ω, τ) *as well.*

Proof. Pick a root of unity ζ for which $\omega = \zeta^a$ and $\tau = \zeta^b$ for coprime integers a and b. Define $g(t, z) := f(t, z^a, z^b)$, so that $g(t_0, \zeta) = 0$. By taking into account the parity of a and b, we see that

$$\begin{aligned} g(t, -z) &\in \{f_1(t, x, y), f_2(t, x, y), f_3(t, x, y)\} \\ g(t, z^2) &= f_4(t, x, y) \\ g(t, -z^2) &\in \{f_5(t, x, y), f_6(t, x, y), f_7(t, x, y)\} \end{aligned}$$

and hence by Lemma 2 we are done. □

The last prerequisite we will need is a method to find the cyclotomic part of a polynomial $f \in \mathbb{C}[x]$. We will treat the existence of such an algorithm as a black box; for details one may read [2] or Section 2 of [4].

2.2. Finding Cyclotomic Points for Families of Polynomials

We now describe how to find cyclotomic solutions to families of polynomials indexed by a rational parameter. That is to say, given $f(t, x) \in \mathbb{Q}[t, x]$ we find pairs (t_0, ω) with $t_0 \in \mathbb{Q}$ and ω a root of unity for which $f(t_0, \omega) = 0$.

We start by recalling some properties of the *resultant* of two polynomials. The resultant is a classical tool in elimination theory, and we will refer the reader to Chapter 3, Section 6 of [8] as opposed to going into details here. For the purposes of this paper one may take the following crude and incomplete description: given two polynomials $f(t, x), g(t, x) \in \mathbb{Q}[t, x]$, there exists a polynomial $\mathrm{Res}(f, g, x) \in \mathbb{Q}[t]$, read "the resultant of f and g with respect to x," with the property that if (t_0, x_0) is a common zero of f and g, then t_0 is a zero of $\mathrm{Res}(f, g, x)$. Importantly, the resultant of two low degree polynomials may be calculated in many modern computer algebra systems. The use of resultants lowers the number of variables in question at each step, making it ideal for the classification problems we are interested in.

We now describe an algorithm based on [2] and [4] for finding cyclotomic points on families of polynomials. We will maintain the notation of Lemma 2, i.e., if $f(t, x) \in \mathbb{Q}[t, x]$ then

$$f_1(t, x) = f(t, -x), f_2(t, x) = f(t, x^2), f_3(t, x) = f(t, -x^2).$$

Algorithm 1 Pseudocode

Input: A polynomial $f(t,x) \in \mathbb{Q}[t,x]$.

Output: All pairs (t_0, ω) with $t_0 \in \mathbb{Q}$ and ω a root of unity for which $f(t_0, \omega) = 0$.

1. Check if $f(t,x)$ is irreducible. If not, factor f and run the algorithm on irreducible components of f.

2. Check if $f(t,x)$ is a polynomial in x^m for an integer $m \geq 2$. If so, define $g(t,x)$ so that $g(t,x^m) = f(t,x)$ and run the algorithm on $g(t,x)$. It is simple to translate zeroes of $g(t,x)$ into zeroes of $f(t,x)$.

3. Check if $f(t,x)$ is constant in t. If so, find the cyclotomic roots of $f(1,x)$ to find zeroes $\omega_1, \ldots, \omega_k$. Output (t_0, ω_i) for any rational t_0.

4. Check if $f(t,x)$ is constant in x. If so, use the Rational Roots Theorem to find the rational roots $t_1, \ldots, t_s$ of $f(t,1)$. Output the parametric family $\{(t_j, \omega)\}$ where ω is any root of unity.

5. For $i \in \{1,2,3\}$:

   (a) Compute $h_i(t) = \mathrm{Res}(f, f_i, x)$.

   (b) Using the Rational Roots Theorem, find the rational roots of h_i. Call them $r_{i,1}, \ldots, r_{i,k_i}$.

   (c) For each $r_{i,j}$, find cyclotomic roots of $f(r_{i,j}, x)$. For each ω output $(r_{i,j}, \omega)$.

End Algorithm

We now discuss the validity of the code. This entails ensuring that we find *all* desired solutions, as well as ensuring we do not find any extraneous solutions. Suppose $t_0 \in \mathbb{Q}$, ω is a root of unity, and $f(t_0, \omega) = 0$. By Lemma 2, we also have $f_i(t_0, \omega) = 0$ for some $i \in \{1,2,3\}$. Thus the resultant $\mathrm{Res}(f, f_i, x)$ will vanish at t_0. We can easily find this by applying the Rational Root Theorem to $\mathrm{Res}(f, f_i, x)$. Once we find t_0 the work of [2] and [4] ensures we can find ω by finding the cyclotomic roots of $f(t_0, x)$. Thus (t_0, ω) will be output in Step 5 of the algorithm.

Now suppose we have found an extraneous solution. This would occur if we had $\mathrm{Res}(f, f_i, x) = 0$ for some i. For $i = 2, 3$ this is ruled out by Lemma 3, since Step 1 has the effect of ensuring we always work with irreducible polynomials. If $\mathrm{Res}(f, f_1, x) = 0$, then $f(t,x)$ and $f(t,-x)$ share a factor. In this case it must be that $f(t,x)$ is a rational multiple of $f(t,-x)$. This can only occur if $f(t,x)$ is a polynomial in x^2, or if $f(t,x) = x \cdot g(t,x)$ where $g(t,x)$ is a polynomial in x^2. These cases are both ruled out by Steps 1 and 2.

2.3. Finding Cyclotomic Points for Families of Curves

We now bootstrap the previous algorithm to finding cyclotomic points on families of curves. Our argument in this section relies heavily upon [4].

Suppose $f(t,x,y)$ is a Laurent polynomial in x and y, i.e., $f \in \mathbb{Z}[t,x,y,x^{-1},y^{-1}]$. Write

$$f(t,x,y) = \sum_{a,b} c_{a,b}(t)x^a y^b.$$

We denote the *support* of f, $\operatorname{supp}(f)$, to be $\operatorname{supp}(f) := \{(a,b) : c_{a,b}(t) \neq 0\}$. For example,

$$\operatorname{supp}(3txy + t^2x^2 + xy^4) = \{(1,1),(2,0),(1,4)\}.$$

From this we may define $\mathcal{L}(f)$ to be the lattice generated by the differences of elements in $\operatorname{supp}(f)$. Continuing our example,

$$\begin{aligned}\mathcal{L}(3txy + t^2x^2 + xy^4) &= \mathbb{Z}\cdot(1,-1) + \mathbb{Z}\cdot(0,3) + \mathbb{Z}\cdot(1,-4)\\ &= \mathbb{Z}\cdot(1,-1) \oplus \mathbb{Z}\cdot(0,3).\end{aligned}$$

The following two observations are straightforward from the definition of $\mathcal{L}$. Suppose $\mathcal{L}(f)$ is rank 1, i.e., it is generated by a single vector (a,b). If we let $u = x^a y^b$, then $f(t,x,y)$ may be written as

$$f(n,x,y) = x^s y^{s'} g(n,u)$$

for some monomial $x^s y^{s'}$ and some Laurent polynomial $g \in \mathbb{Z}[t,u,u^{-1}]$. Alternatively, suppose $\mathcal{L}(f)$ is rank 2, generated freely by $\{(a,b),(c,d)\}$. Letting $u = x^a y^b$ and $v = x^c y^d$, one can find a Laurent polynomial $g \in \mathbb{Z}[t,u,u^{-1},v,v^{-1}]$ for which $\mathcal{L}(g) = \mathbb{Z}\oplus\mathbb{Z}$ and for which

$$f(x,y) = x^s y^{s'} g(t,u,v)$$

for some monomial $x^s y^{s'}$.

We now proceed with the algorithm, maintaining the notation developed in Lemma 4. Our objective is as follows. Given a polynomial $f(t,x,y) \in \mathbb{Q}[t,x,y]$, we wish to find solutions (t_0,ω,τ) with $t_0 \in \mathbb{Q}$ and ω,τ roots of unity.

Algorithm 2 Pseudocode

Input: A polynomial $f(t,x,y) \in \mathbb{Q}[t,x,y]$.

Output: All triples (t_0,ω,τ) with $t_0 \in \mathbb{Q}$ and ω,τ roots of unity for which $f(t_0,\omega,\tau) = 0$.

1. Check if $f(t,x,y)$ is irreducible. If not, factor f and run the algorithm on the irreducible factors of f.

2. Check if $\mathcal{L}(f)$ is rank 1. If so, chose $u = x^a y^b$ so that $g(t,x,y) = x^s y^{s'} g(t,u)$. Run Algorithm 1 on the polynomial $g(t,u)$. Translating solutions of $g(t,u)$ to roots of $f(t,x,y)$ is straightforward.

3. Check if $\mathcal{L}(f) = \mathbb{Z} \oplus \mathbb{Z}$. If not, find g for which $\mathcal{L}(g) = \mathbb{Z} \oplus \mathbb{Z}$ and $f(t, x, y) = x^s y^{s'} g(t, u, v)$. Continue the algorithm on g. For each solution obtained one can recover the solutions for f by following the steps of Section 3.7 in [4].

4. For $i \in \{1, 2, \ldots, 7\}$:
   (a) Compute $g_i = \text{Res}(f, f_i, y)$.
   (b) Run Algorithm 2 on g_i to obtain zeroes $(t_{i,1}, \omega_{i,1}), \ldots, (t_{i,j_i}, \omega_{i,j_i})$.
      i. For $l \in \{1, \ldots, j_i\}$, compute $G_l = f(t_{i,l}, \omega_{i,l}, y)$.
      ii. Compute the cyclotomic roots of G_l via Algorithm 1. For each such root τ, output $(t_{i,l}, \omega_{i,l}, \tau)$.

End Algorithm

Again we verify that the above code returns the expected result. Suppose $f(t_0, \omega, \tau) = 0$ for $t_0 \in \mathbb{Q}$ and ω, τ roots of unity. By Lemma 3, $f_i(t_0, \omega, \tau) = 0$ as well for some $i \in \{1, 2, \ldots, 7\}$. In particular the resultant g_i will vanish at (t_0, ω). The correctness of Algorithm 2 ensures that (t_0, ω) will be found in Step 4, (b). Once (t_0, ω) have been identified it is then a simple matter to find τ by examining the univariate polynomial $f(t_0, \omega, y)$.

Now suppose we have found an extraneous solution. We will be led to the same contradiction as [4]. As with Algorithm 2, this would occur if a resultant calculation $g_i = \text{Res}(f, f_i, y)$ resulted in $g_i(t, x) \equiv 0$. Since Step 1 ensures f is irreducible, this can only occur if f divides f_i for some $i \in \{1, 2, \ldots, 7\}$. Suppose f divides f_1. As with Algorithm 2, this can only occur if f is a Laurent polynomial in x^2. But this would imply that $\mathcal{L}(f) \neq \mathbb{Z} \oplus \mathbb{Z}$, contradicting Step 3. A similar argument shows that f does not divide f_2 or f_3. Suppose now that f divides f_i, for $i \in \{4, 5, 6, 7\}$. Applying the ring automorphisms $x \to -x$, $y \to -y$ to $\mathbb{Q}[t, x, y, x^{-1}, y^{-1}]$ shows that f_1, f_2, and f_3 also divide f_i. As f,f_1,f_2, and f_3 are coprime, we are led to the product $f \cdot f_1 \cdot f_2 \cdot f_3$ dividing f_i, which is clearly a contradiction in degree.

3. Metallic Means and Polygon Diagonals

We now apply the methods of the previous section to prove Theorem 1. Our calculations may be checked in the Sage code provided in the ancillary file.

Proof of Theorem 1. Suppose ϕ_{t_0} is a metallic mean which may be represented as a ratio of diagonals of a regular N-gon. By viewing the polygon as the set of points $\{\zeta_N^a : 1 \leq a \leq N\}$ in the complex plane, we obtain

$$\phi_{t_0} = \frac{|1 - \zeta_N^a|}{|1 - \zeta_N^b|}.$$

Noting that $\overline{\zeta_N} = \zeta_N^{-1}$ and squaring both sides, we obtain

$$\phi_{t_0}^2 = \frac{(1-\zeta_N^a)(1-\zeta_N^{-a})}{(1-\zeta_N^b)(1-\zeta_N^{-b})}.$$

Now for any metallic ratio ϕ_t we have $\phi_t^2 - 2 + \phi_t^{-2} = (\phi_t - \phi_t^{-1})^2 = t^2$. In particular, we obtain $\phi_t^2 + \phi_t^{-2} - t^2 - 2 = 0$. Thus via substitution we see that $(t_0^2, \zeta_N^a, \zeta_N^b)$ must be a zero of the following multivariate polynomial:

$$\begin{aligned} f(t,x,y) = -x^3y^3t^2 + x^4y^2 - 2x^3y^3 + x^2y^4 + 2x^3y^2t^2 + 2x^2y^3t^2 - x^3yt^2 \\ - 4x^2y^2t^2 - xy^3t^2 - 2x^3y + 4x^2y^2 - 2xy^3 \\ + 2x^2yt^2 + 2xy^2t^2 - xyt^2 + x^2 - 2xy + y^2. \end{aligned}$$

In particular, for the classification asserted in Theorem 1 we may run the algorithms of Section 2 to find all solutions to $f(t,x,y) = 0$ whose first coordinate is rational and last two coordinates are roots of unity. Given such a triple (a, τ, ω) we get the following two desired metallic means, corresponding to the positive and negative square roots of a:

$$\phi_{\sqrt{a}} = \frac{|1-\omega|}{|1-\tau|}$$
$$\phi_{-\sqrt{a}} = \frac{|1-\tau|}{|1-\omega|}. \qquad \square$$

Below we list explicit realizations of the metallic means as ratios of polygon diagonals. We omit the trivial solution for $t = 0$, and only list solutions for t positive. To obtain the negative solutions one merely needs to take reciprocals.

t	ϕ_t	Numerator Diagonal	Denominator Diagonal
1	$\frac{1+\sqrt{5}}{2}$	$\|1-\zeta_5^2\|$	$\|1-\zeta_5\|$
2	$1+\sqrt{2}$	$\|1-\zeta_8^3\|$	$\|1-\zeta_8\|$
$\frac{3}{2}$	2	$\|1-\zeta_6^3\|$	$\|1-\zeta_6\|$
$\sqrt{2}$	$\frac{\sqrt{2}+\sqrt{6}}{2}$	$\|1-\zeta_{12}^5\|$	$\|1-\zeta_{12}^2\|$
$\sqrt{5}$	$\frac{3+\sqrt{5}}{2}$	$\|1-\zeta_{10}^3\|$	$\|1-\zeta_{10}\|$
$\sqrt{12}$	$2+\sqrt{3}$	$\|1-\zeta_{12}^5\|$	$\|1-\zeta_{12}\|$
$\frac{\sqrt{2}}{2}$	$\sqrt{2}$	$\|1-\zeta_{24}^6\|$	$\|1-\zeta_{24}^4\|$
$\frac{\sqrt{6}}{6}$	$\frac{\sqrt{6}}{2}$	$\|1-\zeta_{12}^4\|$	$\|1-\zeta_{12}^3\|$
$\frac{2\sqrt{3}}{3}$	$\sqrt{3}$	$\|1-\zeta_6^2\|$	$\|1-\zeta_6\|$
$\frac{\sqrt{12}}{12}$	$\frac{2\sqrt{3}}{3}$	$\|1-\zeta_6^3\|$	$\|1-\zeta_6^2\|$

4. Generating Real Subfields of Cyclotomic fields

We now change our focus to the question of when a ratio of polygon diagonals generates an extension of $\mathbb{Q}$ of small degree. To simplify our discussion, we will restrict to the case in which $d_1 = |1-\zeta_N^a|$ and $d_2 = |1-\zeta_N^b|$ with a and b coprime. By doing so, we rule out the possibility of, for instance, treating a ratio of square diagonals as a ratio of octagon diagonals. This simplifies the exposition greatly.

We will start by analyzing the complementary question of when a ratio $\frac{d_1}{d_2}$ fails to generate the extension $\mathbb{Q}(d_1, d_2)$. From our assumption on d_1 and d_2 it is straightforward to show $\mathbb{Q}(d_1, d_2) = \mathbb{Q}(\zeta_{4N}^+)$, and thus the degree of $\mathbb{Q}(d_1, d_2)$ over $\mathbb{Q}$ is $\frac{\phi(4N)}{2}$. This quantity diverges as $N \to \infty$. The tower law for field extensions then states that

$$\frac{\phi(4N)}{2} = [\mathbb{Q}(d_1, d_2) : \mathbb{Q}(\tfrac{d_1}{d_2})] \cdot [\mathbb{Q}(\tfrac{d_1}{d_2}) : \mathbb{Q}].$$

This reduces Theorem 2 to finding an explicit upper bound on $[\mathbb{Q}(d_1, d_2) : \mathbb{Q}(\frac{d_1}{d_2})]$. As with the previous result, our approach will involve finding cyclotomic solutions to a (Laurent) polynomial.

Let us call a ratio of polygon diagonals $\frac{d_1}{d_2}$ for which $\mathbb{Q}(\frac{d_1}{d_2}) \neq \mathbb{Q}(d_1, d_2)$ *defective*. In the same vein as the previous section, write

$$\begin{aligned} d_1 = |1-\zeta_N^a| = \sqrt{(1-\zeta_N^a)(1-\zeta_N^{-a})} &= \sqrt{-\zeta_N^{-a}(1-\zeta_N^a)^2} \\ &= \zeta_{4N}^N \zeta_{2N}^{-a}(1-\zeta_N^a) \\ &= \zeta_{4N}^{N-2a} + \zeta_{4N}^{3N+2a}. \end{aligned}$$

We note in passing that the product of the two summands above equals 1; this will be crucial in what follows. We now know that a ratio of two diagonals in a regular N-gon may be written as

$$\frac{d_1}{d_2} = \frac{\zeta_{4N}^{N-2a} + \zeta_{4N}^{3N+2a}}{\zeta_{4N}^{N-2b} + \zeta_{4N}^{3N+2b}}.$$

Suppose $\frac{d_1}{d_2}$ is defective, and let σ be a nontrivial automorphism in $\mathrm{Gal}(\mathbb{Q}(d_1, d_2)/\mathbb{Q})$ fixing the ratio. Let $\hat{\sigma}$ be a lift of σ to $\mathrm{Gal}(\mathbb{Q}(\zeta_{4N})/\mathbb{Q})$. We have

$$\frac{\zeta_{4N}^{N-2a} + \zeta_{4N}^{3N+2a}}{\zeta_{4N}^{N-2b} + \zeta_{4N}^{3N+2b}} = \hat{\sigma}\left(\frac{\zeta_{4N}^{N-2a} + \zeta_{4N}^{3N+2a}}{\zeta_{4N}^{N-2b} + \zeta_{4N}^{3N+2b}}\right) \tag{1}$$

$$= \frac{\hat{\sigma}(\zeta_{4N}^{N-2a}) + \hat{\sigma}(\zeta_{4N}^{3N+2a})}{\hat{\sigma}(\zeta_{4N}^{N-2b}) + \hat{\sigma}(\zeta_{4N}^{3N+2b})}. \tag{2}$$

We are naturally led to search for cyclotomic solutions to the equation

$$\frac{x_1 + x_1^{-1}}{x_2 + x_2^{-1}} = \frac{y_1 + y_1^{-1}}{y_2 + y_2^{-1}}.$$

A simple algebraic manipulation reduces this to finding cyclotomic solutions to

$$f(x_1,x_2,y_1,y_2) = (x_1y_2 + x_1^{-1}y_2^{-1}) + (x_1y_2^{-1} + x_1^{-1}y_2) \\ + (x_2y_1 + x_2^{-1}y_1^{-1}) + (x_2y_1^{-1} + x_2^{-1}y_1).$$

One might hope to find the cyclotomic solutions to f by iteratively taking resultants, as in the previous section. From a computational perspective this is a much more challenging problem. This would require first scaling f by the monomial $x_1x_2y_1y_2$ to yield a sextic polynomial in four variables. Then one would hope to take successive resultants $r_1(x_2,y_1,y_2)$, $r_2(y_1,y_2)$, and $r_3(y_2)$ to reduce the problem to the univariate case. Due to the heightened degree and number of variables compared to Section 3, even the computations of these resultants are nontrivial. In general the degree of a resultant of two polynomials is *multiplicative* in the degrees of the input polynomials, and the computation itself is often achieved through the calculation of a large determinant.

Even if one could achieve these resultant calculations, one would then be left with the problem of lifting zeroes of $r_3(y_2)$ to zeroes of f. Should we find a zero ζ_N of $r_3(y_2)$, one first has to lift this to a zero of $r_2(y_1,\zeta_N)$. To find the cyclotomic zeroes of $r_2(y_1,\zeta_N)$, one first computes the image of $r_2(y_1,\zeta_N)$ under the *norm map* $\mathbb{Q}(\zeta_N)[y_1] \to \mathbb{Q}[y_1]$ so that we may obtain a polynomial with strictly rational coefficients. The norm map is defined by sending

$$r_2(y,\zeta_N) \to \prod_{\sigma\in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})} \sigma(r_2(y_1,\zeta_N)).$$

This increases the degree of the polynomials in question and hence increases the possible solution space. This process would then be repeated to lift to a zero of r_1 and finally to f itself. The combination of these difficulties made it impossible for our computers to prove Theorem 2 in this fashion. Fortunately we can work around this as follows.

Note that f is comprised of eight monomials which appear in complex conjugate pairs when the variables are specialized to roots of unity (explaining the authors' choice of writing parentheses around certain terms). Thus while the computational techniques of the previous sections fail, we can still solve the problem by using the techniques of Włodarski [27] and of Conway and Jones [6] for solving trigonometric diophantine equations. Namely, the identity

$$2\cos(\tfrac{2\pi a}{b}) = \zeta_b^a + \zeta_b^{-a}$$

suggests first finding rational solutions to the equation

$$F(A,B,C,D) = \cos(\pi A) + \cos(\pi B) + \cos(\pi C) + \cos(\pi D) = 0.$$

This is in part the content of [27] and [6].

Lemma 5 ([27] Theorem 1, [6] Theorem 6). *The rational solutions to*

$$\cos(\pi A) + \cos(\pi B) + \cos(\pi C) + \cos(\pi D) = 0$$

come in two parametric families and 10 'sporadic' solutions. The parametric families have one of the two following forms:

$$\{A, B, C, D\} = \{\alpha, \beta, 1 - \alpha, 1 - \beta\}$$

$$\{A, B, C, D\} = \left\{\alpha, \frac{2}{3} - \alpha, \frac{2}{3} + \alpha, \frac{1}{2}\right\}.$$

The ten sporadic solutions occur in 5 pairs which are negations of one another; in these cases, $\{A, B, C, D\}$ is one of the following:

$$\begin{array}{ll}
\left\{\frac{2}{5}, \frac{1}{2}, \frac{4}{5}, \frac{1}{3}\right\} & \left\{\frac{3}{5}, \frac{1}{2}, \frac{1}{5}, \frac{2}{3}\right\} \\
\left\{1, \frac{1}{5}, \frac{3}{5}, \frac{1}{3}\right\} & \left\{0, \frac{4}{5}, \frac{2}{5}, \frac{2}{3}\right\} \\
\left\{\frac{2}{5}, \frac{7}{15}, \frac{13}{15}, \frac{1}{3}\right\} & \left\{\frac{3}{5}, \frac{8}{15}, \frac{2}{15}, \frac{2}{3}\right\} \\
\left\{\frac{4}{5}, \frac{1}{15}, \frac{11}{15}, \frac{1}{3}\right\} & \left\{\frac{1}{5}, \frac{14}{15}, \frac{4}{15}, \frac{2}{3}\right\} \\
\left\{\frac{2}{7}, \frac{4}{7}, \frac{6}{7}, \frac{1}{3}\right\} & \left\{\frac{1}{7}, \frac{3}{7}, \frac{5}{7}, \frac{2}{3}\right\}.
\end{array}$$

□

This allows us to find the cyclotomic solutions of our Laurent polynomial in question as follows. Note that not every solution will be germane to the question of when the ratio of two diagonals is defective, since we are only interested in solutions which satisfy an appropriate Galois relationship (see Equations (1) and (2)). However, for completeness we will not restrict ourselves by this condition just yet.

Given a solution $f(\omega_1, \omega_2, \tau_1, \tau_2) = 0$, where ω_i and τ_i are roots of unity, we are led to a solution of the trigonometric diophantine equation above as discussed. Write the solution as

$$F(2\tfrac{a_1}{b_1}, 2\tfrac{a_2}{b_2}, 2\tfrac{a_3}{b_3}, 2\tfrac{a_4}{b_4}) = 0,$$

for integers a_i, b_i. This can be rewritten as

$$\zeta_{b_1}^{a_1} + \zeta_{b_1}^{-a_1} + \zeta_{b_1}^{a_2} + \zeta_{b_2}^{-a_2} + \zeta_{b_3}^{a_3} + \zeta_{b_3}^{-a_3} + \zeta_{b_4}^{a_4} + \zeta_{b_4}^{-a_4} = 0.$$

It follows that for some permutation $\pi : \{1,2,3,4\} \to \{1,2,3,4\}$,

$$\begin{aligned}
\omega_1\tau_2 + \omega_1^{-1}\tau_2^{-1} &= \zeta_{b_{\pi(1)}}^{a_{\pi(1)}} + \zeta_{b_{\pi(1)}}^{-a_{\pi(1)}} \\
\omega_1\tau_2^{-1} + \omega_1^{-1}\tau_2 &= \zeta_{b_{\pi(2)}}^{a_{\pi(2)}} + \zeta_{b_{\pi(2)}}^{-a_{\pi(2)}} \\
\omega_2\tau_1 + \omega_1^{-1}\tau_2^{-1} &= \zeta_{b_{\pi(3)}}^{a_{\pi(3)}} + \zeta_{b_{\pi(3)}}^{-a_{\pi(3)}} \\
\omega_2\tau_1^{-1} + \omega_2^{-1}\tau_2 &= \zeta_{b_{\pi(4)}}^{a_{\pi(4)}} + \zeta_{b_{\pi(4)}}^{-a_{\pi(4)}}.
\end{aligned}$$

To simplify this further, note this implies there is a function sign : $\{1,2,3,4\} \to \{1,-1\}$ for which

$$\begin{aligned}
\omega_1\tau_2 &= \zeta_{b_{\pi(1)}}^{\mathrm{sign}(1)a_{\pi(1)}} \\
\omega_1\tau_2^{-1} &= \zeta_{b_{\pi(2)}}^{\mathrm{sign}(2)a_{\pi(2)}} \\
\omega_2\tau_1 &= \zeta_{b_{\pi(3)}}^{\mathrm{sign}(3)a_{\pi(3)}} \\
\omega_2\tau_1^{-1} &= \zeta_{b_{\pi(4)}}^{\mathrm{sign}(4)a_{\pi(4)}}.
\end{aligned}$$

Once we have reduced to these 4 equalities it is simple to solve for $\omega_1, \omega_2, \tau_1, \tau_2$ up to negation using, for instance,

$$\begin{aligned}
\omega_1^2 &= \zeta_{b_{\pi(1)}}^{\mathrm{sign}(1)a_{\pi(1)}} \cdot \zeta_{b_{\pi(2)}}^{\mathrm{sign}(2)a_{\pi(2)}} \\
\omega_2^2 &= \zeta_{b_{\pi(3)}}^{\mathrm{sign}(3)a_{\pi(3)}} \cdot \zeta_{b_{\pi(4)}}^{\mathrm{sign}(4)a_{\pi(4)}}.
\end{aligned}$$

As we are solving a quadratic equation for ω_i, each choice of π and sign will lead to 4 solutions. Thus a priori, for each solution

$$F(2\tfrac{a_1}{b_1}, 2\tfrac{a_2}{b_2}, 2\tfrac{a_3}{b_3}, 2\tfrac{a_4}{b_4}) = 0$$

we should expect $4! \cdot 2^4 \cdot 4 = 1,536$ solutions $f(\omega_1, \omega_2, \tau_1, \tau_2) = 0$. For the sake of brevity in this paper we will reduce this in three ways. Note that f admits the following symmetries:

1. $f(x_1, x_2, y_1, y_2) = f(x_2, x_1, y_2, y_1)$,
2. $f(x_1, x_2, y_1, y_2) = f(x_1^{-1}, x_2, y_1, y_2)$,
3. $f(x_1, x_2, y_1, y_2) = f(x_1, x_2^{-1}, y_1, y_2)$,
4. $f(x_1, x_2, y_1, y_2) = f(y_2, x_2, y_1, x_1)$,
5. $f(x_1, x_2, y_1, y_2) = f(x_1, y_1, x_2, y_2)$,
6. $f(x_1, x_2, y_1, y_2) = f(y_2^{-1}, x_2, y_1, x_1^{-1})$,
7. $f(x_1, x_2, y_1, y_2) = f(x_1, y_1^{-1}, x_2^{-1}, y_2)$.

The first three operations allow us to reduce the number of permutations that we need to check; for instance, if we have a permutation assigning

$$\begin{aligned}\omega_1\tau_2+\omega_1^{-1}\tau_2^{-1}&=\zeta_{b_1}^{a_1}+\zeta_{b_1}^{-a_1}\\ \omega_1\tau_2^{-1}+\omega_1^{-1}\tau_2&=\zeta_{b_2}^{a_2}+\zeta_{b_2}^{-a_2}\\ \omega_2\tau_1+\omega_1^{-1}\tau_2^{-1}&=\zeta_{b_3}^{a_3}+\zeta_{b_3}^{-a_3}\\ \omega_2\tau_1^{-1}+\omega_2^{-1}\tau_2&=\zeta_{b_4}^{a_4}+\zeta_{b_4}^{-a_4},\end{aligned}$$

then applying the first listed symmetry gives a solution for which

$$\begin{aligned}\omega_1\tau_2+\omega_1^{-1}\tau_2^{-1}&=\zeta_{b_3}^{a_3}+\zeta_{b_3}^{-a_3}\\ \omega_1\tau_2^{-1}+\omega_1^{-1}\tau_2&=\zeta_{b_4}^{a_4}+\zeta_{b_4}^{-a_4}\\ \omega_2\tau_1+\omega_1^{-1}\tau_2^{-1}&=\zeta_{b_1}^{a_1}+\zeta_{b_1}^{-a_1}\\ \omega_2\tau_1^{-1}+\omega_2^{-1}\tau_2&=\zeta_{b_2}^{a_2}+\zeta_{b_2}^{-a_2}.\end{aligned}$$

Thus, by composing operations 1 thru 3 we can generate eight distinct permutations, and hence we will only list three representatives explicitly which generate all 24 under these operations. Similarly, operations 4 thru 7 allow us to change the sign function arbitrarily; again, by way of example if we have a solution for which

$$\begin{aligned}\omega_1\tau_2&=\zeta_{b_1}^{a_1}\\ \omega_1\tau_2^{-1}&=\zeta_{b_2}^{a_2}\\ \omega_2\tau_1&=\zeta_{b_3}^{a_3}\\ \omega_2\tau_1^{-1}&=\zeta_{b_4}^{a_4},\end{aligned}$$

then after applying operation 4 we will have a solution for which

$$\begin{aligned}\omega_1\tau_2&=\zeta_{b_1}^{a_1}\\ \omega_1\tau_2^{-1}&=\zeta_{b_2}^{-a_2}\\ \omega_2\tau_1&=\zeta_{b_3}^{a_3}\\ \omega_2\tau_1^{-1}&=\zeta_{b_4}^{a_4}.\end{aligned}$$

Thus for a fixed permutation there is no need to worry about a sign function as long as we allow for arbitrary composition of operations 4 thru 7. Finally, we will rampantly use the plus or minus sign $\pm$ to simplify the solutions to quadratic equations. We hope no confusion arises from these simplifications.

With this discussion in mind, we have the following classification. The proof is immediate given Lemma 5 and the previous discussion.

Lemma 6. *Let $(\omega_1,\omega_2,\tau_1,\tau_2)$ be a cyclotomic solution to f. Then $(\omega_1,\omega_2,\tau_1,\tau_2)$ can be obtained via the seven listed symmetries from one of the following families of solutions:*

- *For any root of unity* ζ_b^a*, one of the following three parametric families:*

  1. $(x_1, y_2) = \pm(\zeta_3^2\zeta_b^a, \zeta_3)$, $(x_2, y_1) = \pm(\zeta_{24}^{11}\zeta_{2b}^a, \zeta_{24}^5\zeta_{2b}^a)$.
  2. $(x_1, y_2) = \pm(\zeta_3\zeta_b^a, \zeta_3^2)$, $(x_2, y_1) = \pm(\zeta_{24}^7\zeta_{2b}^a, \zeta_{24}\zeta_{2b}^a)$.
  3. $(x_1, y_2) = \pm(\zeta_8\zeta_{2b}^a, \zeta_8^7\zeta_{2b}^a)$, $(x_2, y_1) = \pm(\zeta_b^a, \zeta_3)$.

- *For any two roots of unity* ζ_b^a, ζ_c^d*, one of the following three parametric families:*

  1. $(x_1, y_2) = \pm(\zeta_4\zeta_b^a, \zeta_4^3)$, $(x_2, y_1) = \pm(\zeta_4, \zeta_c^d, \zeta_4^3)$.
  2. $(x_1, y_2) = \pm(\zeta_{2bd}^{ad+bc}, \zeta_{2bd}^{ad-bc})$, $(x_2, y_1) = \pm(\zeta_{2bd}^{-ad-bc}, \zeta_{2bd}^{-ad+bc})$.
  3. $(x_1, y_2) = \pm(\zeta_4\zeta_{2bd}^{ad+bc}, \zeta_4^3\zeta_{2bd}^{ad-bc})$, $(x_2, y_1) = \pm(\zeta_4\zeta_{2bd}^{-ad-bc}, \zeta_4^3\zeta_{2bd}^{-ad+bc})$.

- *Any entry from the following table:*

$x_1y_2 + \frac{1}{x_1y_2}$	$\frac{x_1}{y_2} + \frac{y_2}{x_1}$	$x_2y_1 + \frac{1}{x_2y_1}$	$\frac{x_2}{y_1} + \frac{y_1}{x_2}$	(x_1, y_2)	(x_2, y_1)
$\zeta_5 + \zeta_5^4$	$\zeta_4 + \zeta_4^3$	$\zeta_5^2 + \zeta_5^3$	$\zeta_6 + \zeta_6^5$	$\pm(\zeta_{40}^9, \zeta_{40}^{39})$	$\pm(\zeta_{60}^{17}, \zeta_{60}^7)$
$\zeta_5 + \zeta_5^4$	$\zeta_5^2 + \zeta_5^3$	$\zeta_4 + \zeta_4^3$	$\zeta_6 + \zeta_6^5$	$\pm(\zeta_{10}^3, \zeta_{10}^9)$	$\pm(\zeta_{24}^5, \zeta_{24})$
$\zeta_5 + \zeta_5^4$	$\zeta_6 + \zeta_6^5$	$\zeta_4 + \zeta_4^3$	$\zeta_5^2 + \zeta_5^3$	$\pm(\zeta_{60}^{11}, \zeta_{60})$	$\pm(\zeta_{40}^{13}, \zeta_{40}^{37})$
$\zeta_{10}^3 + \zeta_{10}^7$	$\zeta_4 + \zeta_4^3$	$\zeta_{10} + \zeta_{10}^9$	$\zeta_3 + \zeta_3^2$	$\pm(\zeta_{40}^{11}, \zeta_{40})$	$\pm(\zeta_{60}^{13}, \zeta_{60}^{53})$
$\zeta_{10}^3 + \zeta_{10}^7$	$\zeta_{10} + \zeta_{10}^9$	$\zeta_4 + \zeta_4^3$	$\zeta_3 + \zeta_3^2$	$\pm(\zeta_{10}^2, \zeta_{10})$	$\pm(\zeta_{24}^7, \zeta_{24}^{23})$
$\zeta_{10}^3 + \zeta_{10}^7$	$\zeta_3 + \zeta_3^2$	$\zeta_4 + \zeta_4^3$	$\zeta_{10} + \zeta_{10}^9$	$\pm(\zeta_{60}^{19}, \zeta_{60}^{59})$	$\pm(\zeta_{40}^7, \zeta_{40}^3)$
$\zeta_2 + \zeta_2$	$\zeta_{10} + \zeta_{10}^9$	$\zeta_{10}^3 + \zeta_{10}^7$	$\zeta_6 + \zeta_6^5$	$\pm(\zeta_{10}^3, \zeta_{10}^2)$	$\pm(\zeta_{60}^{14}, \zeta_{60}^4)$
$\zeta_2 + \zeta_2$	$\zeta_{10}^3 + \zeta_{10}^7$	$\zeta_{10} + \zeta_{10}^9$	$\zeta_6 + \zeta_6^5$	$\pm(\zeta_{10}^4, \zeta_{10})$	$\pm(\zeta_{60}^8, \zeta_{60}^{58})$
$\zeta_2 + \zeta_2$	$\zeta_6 + \zeta_6^5$	$\zeta_{10} + \zeta_{10}^9$	$\zeta_{10}^3 + \zeta_{10}^7$	$\pm(\zeta_6^2, \zeta_6)$	$\pm(\zeta_{10}^2, \zeta_{10}^9)$
$\zeta_2^0 + \zeta_2^0$	$\zeta_5^2 + \zeta_5^3$	$\zeta_5 + \zeta_5^4$	$\zeta_3 + \zeta_3^2$	$\pm(\zeta_5, \zeta_5^4)$	$\pm(\zeta_{15}^4, \zeta_{15}^{14})$
$\zeta_2^0 + \zeta_2^0$	$\zeta_5 + \zeta_5^4$	$\zeta_5^2 + \zeta_5^3$	$\zeta_3 + \zeta_3^2$	$\pm(\zeta_{10}, \zeta_{10}^9)$	$\pm(\zeta_{30}^{11}, \zeta_{30})$
$\zeta_2^0 + \zeta_2^0$	$\zeta_3 + \zeta_3^2$	$\zeta_5^2 + \zeta_5^3$	$\zeta_5 + \zeta_5^4$	$\pm(\zeta_6, \zeta_6^5)$	$\pm(\zeta_{10}^3, \zeta_{10})$
$\zeta_5 + \zeta_5^4$	$\zeta_{30}^7 + \zeta_{30}^{23}$	$\zeta_{30}^{13} + \zeta_{30}^{17}$	$\zeta_6 + \zeta_6^5$	$\pm(\zeta_{60}^{13}, \zeta_{60}^{59})$	$\pm(\zeta_{30}^9, \zeta_{30}^4)$
$\zeta_5 + \zeta_5^4$	$\zeta_{30}^{13} + \zeta_{30}^{17}$	$\zeta_{30}^7 + \zeta_{30}^{23}$	$\zeta_6 + \zeta_6^5$	$\pm(\zeta_{60}^{19}, \zeta_{60}^{53})$	$\pm(\zeta_{30}^6, \zeta_{30})$
$\zeta_5 + \zeta_5^4$	$\zeta_6 + \zeta_6^5$	$\zeta_{30}^7 + \zeta_{30}^{23}$	$\zeta_{30}^{13} + \zeta_{30}^{17}$	$\pm(\zeta_{60}^{11}, \zeta_{60})$	$\pm(\zeta_{30}^{10}, \zeta_{30}^{27})$
$\zeta_{10}^3 + \zeta_{10}^7$	$\zeta_{15}^4 + \zeta_{15}^{11}$	$\zeta_{15} + \zeta_{15}^{14}$	$\zeta_3 + \zeta_3^2$	$\pm(\zeta_{60}^{17}, \zeta_{60}^{59})$	$\pm(\zeta_{30}^6, \zeta_{30}^{26})$
$\zeta_{10}^3 + \zeta_{10}^7$	$\zeta_{15} + \zeta_{15}^{14}$	$\zeta_{15}^4 + \zeta_{15}^{11}$	$\zeta_3 + \zeta_3^2$	$\pm(\zeta_{60}^{11}, \zeta_{60}^7)$	$\pm(\zeta_{30}^9, \zeta_{30}^{29})$
$\zeta_{10}^3 + \zeta_{10}^7$	$\zeta_3 + \zeta_3^2$	$\zeta_{15}^4 + \zeta_{15}^{11}$	$\zeta_{15} + \zeta_{15}^{14}$	$\pm(\zeta_{60}^{19}, \zeta_{60}^{59})$	$\pm(\zeta_{30}^5, \zeta_{30}^3)$
$\zeta_5^2 + \zeta_5^3$	$\zeta_{30} + \zeta_{30}^{29}$	$\zeta_{30}^{11} + \zeta_{30}^{19}$	$\zeta_6 + \zeta_6^5$	$\pm(\zeta_{60}^{13}, \zeta_{60}^{11})$	$\pm(\zeta_{30}^8, \zeta_{30}^3)$
$\zeta_5^2 + \zeta_5^3$	$\zeta_{30}^{11} + \zeta_{30}^{19}$	$\zeta_{30} + \zeta_{30}^{29}$	$\zeta_6 + \zeta_6^5$	$\pm(\zeta_{60}^{23}, \zeta_{60})$	$\pm(\zeta_{30}^3, \zeta_{30}^{28})$
$\zeta_5^2 + \zeta_5^3$	$\zeta_6 + \zeta_6^5$	$\zeta_{30} + \zeta_{30}^{29}$	$\zeta_{30}^{11} + \zeta_{30}^{19}$	$\pm(\zeta_{60}^{17}, \zeta_{60}^7)$	$\pm(\zeta_{30}^6, \zeta_{30}^{25})$
$\zeta_{10} + \zeta_{10}^9$	$\zeta_{15}^7 + \zeta_{15}^8$	$\zeta_{15}^2 + \zeta_{15}^{13}$	$\zeta_3 + \zeta_3^2$	$\pm(\zeta_{60}^{17}, \zeta_{60}^{11})$	$\pm(\zeta_{30}^7, \zeta_{30}^{27})$
$\zeta_{10} + \zeta_{10}^9$	$\zeta_{15}^2 + \zeta_{15}^{13}$	$\zeta_{15}^7 + \zeta_{15}^8$	$\zeta_3 + \zeta_3^2$	$\pm(\zeta_{60}^7, \zeta_{60}^{59})$	$\pm(\zeta_{30}^{12}, \zeta_{30}^2)$
$\zeta_{10} + \zeta_{10}^9$	$\zeta_3 + \zeta_3^2$	$\zeta_{15}^7 + \zeta_{15}^8$	$\zeta_{15}^2 + \zeta_{15}^{13}$	$\pm(\zeta_{60}^{13}, \zeta_{60}^{53})$	$\pm(\zeta_{30}^9, \zeta_{30}^5)$
$\zeta_7 + \zeta_7^6$	$\zeta_7^2 + \zeta_7^5$	$\zeta_7^3 + \zeta_7^4$	$\zeta_6 + \zeta_6^5$	$\pm(\zeta_{42}^9, \zeta_{42}^{39})$	$\pm(\zeta_{84}^{25}, \zeta_{84}^{11})$
$\zeta_7 + \zeta_7^6$	$\zeta_7^3 + \zeta_7^4$	$\zeta_7^2 + \zeta_7^5$	$\zeta_6 + \zeta_6^5$	$\pm(\zeta_{42}^{12}, \zeta_{42}^{36})$	$\pm(\zeta_{84}^{19}, \zeta_{84}^5)$
$\zeta_7 + \zeta_7^6$	$\zeta_6 + \zeta_6^5$	$\zeta_7^2 + \zeta_7^5$	$\zeta_7^3 + \zeta_7^4$	$\pm(\zeta_{84}^{13}, \zeta_{84}^{83})$	$\pm(\zeta_{42}^{15}, \zeta_{42}^{39})$
$\zeta_{14} + \zeta_{14}^{13}$	$\zeta_{14}^3 + \zeta_{14}^{11}$	$\zeta_{14}^5 + \zeta_{14}^9$	$\zeta_3 + \zeta_3^2$	$\pm(\zeta_{42}^6, \zeta_{42}^{39})$	$\pm(\zeta_{84}^{29}, \zeta_{84})$
$\zeta_{14} + \zeta_{14}^{13}$	$\zeta_{14}^5 + \zeta_{14}^9$	$\zeta_{14}^3 + \zeta_{14}^{11}$	$\zeta_3 + \zeta_3^2$	$\pm(\zeta_{42}^9, \zeta_{42}^{36})$	$\pm(\zeta_{84}^{23}, \zeta_{84}^{79})$
$\zeta_{14} + \zeta_{14}^{13}$	$\zeta_3 + \zeta_3^2$	$\zeta_{14}^3 + \zeta_{14}^{11}$	$\zeta_{14}^5 + \zeta_{14}^9$	$\pm(\zeta_{84}^{17}, \zeta_{84}^{73})$	$\pm(\zeta_{42}^{12}, \zeta_{42}^{39})$

We can now refine the previous lemma by taking into consideration Galois groups of real cyclotomic extensions.

Lemma 7. *Take two roots of unity, written as* ζ_{2N}^a *and* ζ_{2N}^b*. Then there exists a nontrivial automorphism* $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{2N})/\mathbb{Q})$ *for which*

$$\frac{\zeta_{2N}^a + \zeta_{2N}^{-a}}{\zeta_{2N}^b + \zeta_{2N}^{-b}} = \frac{\sigma(\zeta_{2N}^a) + \sigma(\zeta_{2N}^{-a})}{\sigma(\zeta_{2N}^b) + \sigma(\zeta_{2N}^{-b})}$$

if and only if either

- $\zeta_{2N}^a = \pm\zeta_{2N}^{\pm b}$, *or*
- *there exists a* $k \in (\mathbb{Z}/2N\mathbb{Z})^\times$ *which solves the simultaneous equations*

$$ak \equiv N + a \mod 2N$$
$$bk \equiv N + b \mod 2N.$$

Before giving the proof which, at this stage, follows quite simply from our buildup, we provide an example application of our theorem. Let us take $2N = 20$, $a = 1$, and $b = 3$. Then

$$k \equiv 10 + 1 \mod 20$$
$$3k \equiv 10 + 3 \mod 20$$

has the solution $k = 11$, telling us that $\frac{\zeta_{20}+\zeta_{20}^{19}}{\zeta_{20}^3+\zeta_{20}^{17}}$ fails to generate $\mathbb{Q}(\zeta_{20} + \zeta_{20}^{-1})$. However, the ratio $\frac{\zeta_{20}+\zeta_{20}^{19}}{\zeta_{20}^2+\zeta_{20}^{18}}$ does generate the extension, since if k is forced to be 11 then $2k \not\equiv 12 \mod 20$. In this simple case one could verify these observations by, for instance, computing the minimal polynomials of the previous two ratios. However, one could imagine that if N grows it will become much simpler to use the criterion given by Lemma 7.

We now proceed with the proof of Lemma 7.

Proof of Lemma 7. Suppose σ is a map as above. As a field automorphism, σ must respect multiplicative order when applied to any root of unity. By examining Lemma 6 we see that the only case in which this occurs is if $x_1 = \pm x_2^{\pm 1}$, in which case σ can be arbitrary, or if we can simultaneously solve $y_1 = \pm x_1^{\pm 1}$ and $y_2 = \pm x_2^{\pm 1}$. Thus we must find an automorphism σ for which $\sigma(\zeta_{2N}^a) = \pm\zeta_{2N}^{\pm a}$ and $\sigma(\zeta_{2N}^b) = \pm\zeta_{2N}^{\pm b}$. Now automorphisms of cyclotomic extensions will have the form $\zeta_{2N} \to \zeta_{2N}^k$ for k coprime to $2N$. In order for the automorphism to be nontrivial, we must be able to solve the following consistently for k:

$$ka \equiv N + a \mod 2N$$
$$kb \equiv N + b \mod 2N.$$

This completes the proof. □

Having classified the cyclotomic solutions to our Laurent polynomial of interest and then examined the relationship between these solutions and Galois groups of real cyclotomic fields, it is a simple matter to classify defective ratios of polygon diagonals.

Proposition 1. *Let d_1 and d_2 be diagonals of a regular N gon, with $d_1 = |1-\zeta_N^a|$ and $d_2 = |1-\zeta_N^b|$. Then the ratio $\frac{d_1}{d_2}$ is defective if and only if either of the following hold:*

- *$d_1 = d_2$, or*
- *there exists $k \in (\mathbb{Z}/4N\mathbb{Z})^\times$ which solves the simultaneous equation*

$$\begin{aligned} k(N-2a) &\equiv 3N-2a \mod 4N \\ k(N-2b) &\equiv 3N-2b \mod 4N. \end{aligned}$$

Proof. As discussed in the beginning of the section, if $\frac{d_1}{d_2}$ fails to generate the extension in question then we could find a nontrivial field automorphism σ of $\mathbb{Q}(d_1, d_2)$ fixing $\frac{d_1}{d_2}$. Writing

$$\frac{d_1}{d_2} = \frac{\zeta_{4N}^{N-2a} + \zeta_{4N}^{3N+2a}}{\zeta_{4N}^{N-2b} + \zeta_{4N}^{3N+2b}},$$

this would give a solution

$$f(\zeta_{4N}^{N-2a}, \zeta_{4N}^{N-2b}, \sigma(\zeta_{4N}^{N-2a}), \sigma(\zeta_{4N}^{N-2b}) = 0.$$

If $d_1 \neq d_2$ then Lemma 6 implies that $\sigma(\zeta_{4N}^{N-2a})$ is in $\{\pm\zeta_{4N}^{N-2a}, \pm\zeta_{4N}^{2a-N}\}$ and that $\sigma(\zeta_{4N}^{N-2b})$ is in $\{\pm\zeta_{4N}^{N-2b}, \pm\zeta_{4N}^{2b-N}\}$. As we are working in $\mathbb{Q}(\zeta_{4N})^+$, we can assume with no loss of generality that $\sigma(\zeta_{4N}^{N-2a}) = -\zeta_{4N}^{N-2a}$ and $\sigma(\zeta_{4N}^{N-2b}) = -\zeta_{4N}^{N-2b}$. This then implies that there exists a $k \in (\mathbb{Z}/4N\mathbb{Z})^\times$ for which $k(N-2a) \equiv 3N-2a \mod 4N$ and $k(N-2b) \equiv 3N-2b \mod 4N$ as in Lemma 7. □

Again by way of example, the golden ratio $\phi_1 = \frac{|1-\zeta_5^2|}{|1-\zeta_5|}$ is defective; this reduces to the example following Lemma 6, since

$$\phi_1 = \frac{|1-\zeta_5^2|}{|1-\zeta_5|} = \frac{\zeta_{20} + \zeta_{20}^{19}}{\zeta_{20}^3 + \zeta_{20}^{17}} = \frac{\zeta_{20}^{11} + \zeta_{20}^9}{\zeta_{20}^{13} + \zeta_{20}^7}.$$

An example of a non-defective ratio can also be found by taking, for instance, a ratio of two diagonals in a decagon. For example,

$$\frac{|1-\zeta_{10}|}{|1-\zeta_{10}^2|} = \frac{\zeta_{40}^8 + \zeta_{40}^{32}}{\zeta_{40}^6 + \zeta_{40}^6};$$

since ζ_{40}^8 reduces to a fifth root of unity it cannot be conjugated to its negative, which has multiplicative order 10. Hence this ratio is not defective.

We end the section by using Proposition 1 to prove Theorem 2, and then using Theorem 2 to give an alternate proof to Theorem 1.

Proof of Theorem 2. We can compute the index $[\mathbb{Q}(d_1, d_2) : \mathbb{Q}(\frac{d_1}{d_2})]$ by computing the size of the associated Galois group $\mathrm{Gal}(\mathbb{Q}(d_1, d_2)/\mathbb{Q}(\frac{d_1}{d_2}))$. As the second field is monogenic and our extensions are abelian, we may compute this by counting the number of automorphisms $\sigma \in \mathrm{Gal}(\mathbb{Q}(d_1, d_2)/\mathbb{Q})$ which fix $\frac{d_1}{d_2}$. Proposition 1 tells us that the number of nontrivial automorphisms which fix $\frac{d_1}{d_2}$ equals the one half the number of solutions to the simultaneous equation

$$\begin{aligned} k(N-2a) &\equiv 3N-2a \mod 4N \\ k(N-2b) &\equiv 3N-2b \mod 4N. \end{aligned}$$

We must divide by 2 to account for going from $\mathrm{Gal}(\mathbb{Q}(\zeta_{4N})/\mathbb{Q})$ to $\mathrm{Gal}(\mathbb{Q}(\zeta_{4N})^+/\mathbb{Q})$.

Reducing these equation mod N and rearranging shows that such a k must also solve

$$\begin{aligned} 2(k-1)a &\equiv 0 \mod N \\ 2(k-1)b &\equiv 0 \mod N. \end{aligned}$$

Since a and b are assumed to be coprime, this can only occur if $2(k-1) \equiv 0 \mod N$. If N is odd then this equation has the unique solution $k \equiv 1 \mod N$, and hence there are at most 4 solutions to the original solution, corresponding to the residue classes 1, $N+1$, $2N+1$, and $3N+1 \mod 4N$. A simple parity argument shows k must be odd, and hence there are in fact 2 solutions in this case.

Alternatively take N to be even; in this case there are fewer restrictions. The equation $2(k-1) \equiv 0 \mod N$ implies $k \equiv 1 \mod N$ or $k \equiv N/2+1 \mod N$, which lift to at most 8 solutions to the original equation.

Thus when N is odd there is a unique nontrivial map fixing $\frac{d_1}{d_2}$, and when N is even there are at most four such maps. After accounting for the identity morphism of the Galois group we obtain

$$[\mathbb{Q}(d_1, d_2) : \mathbb{Q}(\tfrac{d_1}{d_2})] \geq \begin{cases} 2 \text{ if } N \text{ is odd,} \\ 5 \text{ if } N \text{ is even.} \end{cases}$$

Using multiplicativity of degree in towers of field extensions then gives Theorem 2. □

We end by showing how Theorem 2 gives an alternate proof to Theorem 1.

Proof of Theorem 1. The proof of Theorem 2 implies that if d_1 and d_2 are diagonals of a regular N-gon, then the ratio $\frac{d_1}{d_2}$ generates an extension of $\mathbb{Q}$ of degree at least $\phi(4N)/16$. We employ a crude bound of $\phi(n) \geq 48 \cdot (n/210)^{12/13}$ for any integer n; for reference, see the Math StackExchange answer [14]. In particular, if $\frac{d_1}{d_2}$ generates an extension of degree ≤ 4, then $\phi(4N) \leq 64$, and hence $N \leq 286$.

To prove Theorem 1, all one has to do is iterate through the values $3 \leq N \leq 286$. For each such N one computes all possible pairs of coprime integers $1 \leq a, b \leq 286$, and for each pair computes the minimal polynomial of

$$\frac{\zeta_{4N}^{N-2a} + \zeta_{4N}^{3N+2a}}{\zeta_{4N}^{N-2b} + \zeta_{4N}^{3N+2b}}$$

using a computer algebra system such as Sage [26]. It is then a simple matter to classify which such minimal polynomials give rise to metallic ratios. □

We end our paper by noting that there has recently been much interest in examining vanishing sums of roots of unity. Apart from the work of Włodarski and of Conway and Jones mentioned in this section, one could explore [7], [19], [21], or [25]. It is feasible to imagine that the methods of this section, combined with these results, could lead to many more answers regarding generators of (subfields of) cyclotomic fields. We leave this area of exploration to the interested reader.

For an alternate avenue of study, one could examine analytical questions regarding polygon diagonals, instead of the algebraic ones examined here. For instance, we propose the following question.

Question 1. Let D denote the set of all ratios of regular polygon diagonals. What are the limit points of D?

For questions of a similar nature regarding Salem or Pisot numbers, see for instance [24] or Chapter 6 of [3].

Acknowledgements: We would like to thank Kiran Kedlaya for his patience and many helpful comments throughout this project. We would also like to thank an anonymous referee for numerous comments that improved the exposition of this article. The first listed author would like to gratefully acknowledge support from NSF Research Training Group grant DMS-1502651 and from NSF grant DMS-1849173.

References

[1] I. Aliev and C. J. Smyth, Solving algebraic equations in roots of unity, *Forum Math.* **24 (3)** (2012), 641-665.

[2] R. J. Bradford and J. H. Davenport. Effective tests for cyclotomic polynomials. In *Symbolic and Algebraic Computation (Rome, 1988)*, Volume 358 of *Lecture Notes in Comput. Sci.*, Springer, Berlin, 1989.

[3] M.-J. Bertin, A. Decomps-Guilloux, M. Grandet-Hugot, M. Pathiaux-Delefosse, and J.-P. Schreiber, *Pisot and Salem Numbers*, Birkhäuser Verlag, Basel, 1992. With a preface by David W. Boyd.

[4] F. Beukers and C. J. Smyth, Cyclotomic points on curves. In *Number Theory for the Millennium*, AK Peters, Natick, MA, 2002.

[5] A. Redondo Buitrago, Polygons, diagonals, and the bronze mean, *Nexus Network Journal* **9 (2)** (2007), 321-326.

[6] J. H. Conway and A. J. Jones, Trigonometric diophantine equations (On vanishing sums of roots of unity), *Acta Arith.* **30 (3)** (1976), 229-240.

[7] F. Calegari, S. Morrison, and N. Snyder, Cyclotomic integers, fusion categories, and subfactors, *Comm. Math. Phys.* **303 (3)** (2011) 845-896.

[8] J. Cox, D. Little, and D. O'Shea, *Ideals, Varieties, and Algorithms*, Undergrad. Texts Math., Springer-Verlag, New York, 1997.

[9] P. A. Damianou, Monic polynomials in $\mathbb{Z}[x]$ with roots in the unit disc, *Amer. Math. Monthly* **108 (3)** (2001), 253-257.

[10] D. D'Alessandro, M. Daleh, and I. Mezic, Control of mixing in fluid flow: a maximum entropy approach, *IEEE Trans. Automat. Control* **44 (10)** (1999) 1852-1863.

[11] V. W. de Spinadel, The family of metallic means, *Vis. Math.* **1 (3)** (1999) 1-16.

[12] J. B. Gil and A. Worley, Generalized metallic means, *arXiv e-prints* page arXiv:1901.02619, Jan 2019.

[13] A. Hurwitz, Ueber die angenäherte darstellung der zahlen durch rationale brüche, *Math. Ann.* **44 (2)** (1894) 417-436.

[14] W. Jagy, Is the Euler phi function bounded below, *Mathematics Stack Exchange* (2013) https://math.stackexchange.com/q/301856 (version: 2015-12-19).

[15] L. Kronecker, Zwei sätze über gleichungen mit ganzzahligen coefficienten, *J. Reine Angew. Math* **53** (1857) 173-175.

[16] S. Lang, Division points on curves, *Ann. Mat. Pura Appl.* **70** (1965) 229-234.

[17] M. Laurent, Équations diophantiennes exponentielles. In *Seminar on Number Theory*, Univ. Bordeaux I, Talence, 1984.

[18] L. Leroux, Computing the torsion points of a variety defined by lacunary polynomials, *Math. Comp.* **81 (279)** (2012) 1587-1607.

[19] T. Y. Lam and K. H. Leung, On vanishing sums of roots of unity, *J. Algebra* **224 (1)** (2000) 91-109.

[20] G. Perez-Giz, Beyond the golden ratio, *PBS Infinite Series Youtube Channel* hyperlink: https://www.youtube.com/watch?v=MIxvZ6jwTuA (2018).

[21] B. Poonen and M. Rubinstein, The number of intersection points made by the diagonals of a regular polygon, *SIAM J. Discrete Math.* **11 (1)** (1998) 135-156.

[22] J. M. Rojas, Efficiently detecting torsion points and subtori. In *Algebra, Geometry, and their Interactions*, Volume 448 of *Contemp. Math.*, 215-235. Amer. Math. Soc., Providence, RI, 2007.

[23] W. M. Ruppert, Solving algebraic equations in roots of unity *J. Reine Angew. Math.* **435** (1993) 119-156.

[24] C. J. Smyth, Seventy years of Salem numbers, *Bull. Lond. Math. Soc.* **47 (3)** (2015) 379-395.

[25] J. P. Steinberger, Minimal vanishing sums of roots of unity with large coefficients, *Proc. Lond. Math. Soc.* **97 (3)** (2008) 689-717.

[26] The Sage Developers, SageMath *The Sage Mathematics Software System (Version 8.8)* 2019 https://www.sagemath.org .

[27] Ł. Włodarski, On the equation $\cos\alpha_1+\cos\alpha_2+\cos\alpha_3+\cos\alpha_4 = 0$, *Ann. univ. Sci. Budapest. Eötvös Sect. Math.* **12** (1969) 147-155.