University of Zurich

Department of Economics

Working Paper Series

ISSN 1664-7041 (print)
ISSN 1664-705X (online)

Working Paper No. 447

Solving the n-Player Tullock Contest

Christian Ewerhart

Revised version, January 2026

Solving the n-Player Tullock Contest*

Christian Ewerhart†

January 19, 2026

Abstract. The n-player Tullock contest with complete information is known to admit explicit solutions in special cases, such as (i) homogeneous valuations, (ii) constant returns, and (iii) two contestants. But can the model be solved more generally? In this paper, we show that key characteristics of the equilibrium, such as individual efforts, winning probabilities, and payoffs, cannot, in general, be expressed in terms of the primitives of the model using only basic arithmetic operations and the extraction of roots. In this sense, the Tullock contest is intractable. We argue that our formal concept of tractability captures the intuitive notion of the term.

Keywords. Tullock contest · pure-strategy Nash equilibrium · solution by radicals · Galois theory

JEL codes. C02, C72, D72

*) Two anonymous reviewers and a handling editor provided valuable comments on an earlier version. For useful discussions, I am indebted to Jörg Franke, Dan Kovenock, Bruno Mazorra, Dmitry Ryvkin, Marco Serena, Constantine Sorokin, and Cédric Wasser. This work has been presented at the Oligo Workshop in Cambridge, UK, the SAET Conference in Ischia, Italy, and the Econometric Society World Congress in Seoul, South Korea.

†) Department of Economics, University of Zurich, Schönberggasse 1, 8001 Zurich, Switzerland; christian.ewerhart@econ.uzh.ch.

1 Preliminaries

1.1 Introduction

In the standard n-player Tullock (1980) contest with complete information, each contestant $i \in I \equiv \{1, \ldots, n\}$ chooses an effort $x_i \geq 0$ so as to maximize her payoff

$$\Pi_i = \frac{x_i^R}{x_1^R + \ldots + x_n^R} V_i - x_i, \tag{1}$$

where $V_i > 0$ is contestant i's valuation of winning, and $R > 0$ is a parameter of the model that measures the extent to which effort, rather than luck, determines the winner of the contest.[1] As usual, the ratio in equation (1) is understood to assume the value $\frac{1}{n}$ if the denominator vanishes. Moreover, by renaming the contestants if necessary, it may be assumed w.l.o.g. that $V_1 \geq \ldots \geq V_n$. The game described above has found widespread applications in various areas such as marketing, lobbying, electoral competition, and sports (Konrad, 2009).[2]

One of the reasons why Tullock's model has been so fruitful is that its equilibrium in pure strategies admits a convenient representation in important special cases. Solution formulas are available if (i) valuations are homogeneous, i.e., $V_1 = \ldots = V_n$, (ii) returns from effort are constant (i.e., $R = 1$), and (iii) there are $n = 2$ contestants. In those cases, the system of necessary Karush–Kuhn–Tucker conditions for an optimal choice of effort,

$$\frac{\partial \Pi_i}{\partial x_i} = \frac{R x_i^{R-1}(x_1^R + \ldots + x_{i-1}^R + x_{i+1}^R + \ldots + x_n^R)}{(x_1^R + \ldots + x_n^R)^2} V_i - 1 \leq 0, \tag{2}$$

[1] Indeed, in the limit case $R \to 0$, each contestant wins with the same probability $\frac{1}{n}$ regardless of efforts, whereas in the other limit case $R \to \infty$, the highest effort wins with certainty, just as in the all-pay auction.

[2] Throughout the analysis, we will assume that contestants differ in valuations only. All our results can, however, be readily adapted to a setup where contestants differ, in addition, in abilities (i.e., individual weight factors put in front of the x_i^R terms) and marginal costs.

with equality if $x_i > 0$, turns out to be tractable under suitable restrictions on the exogenous parameters. However, it has remained an open question for some time if further generalization is feasible.[3]

This paper provides evidence showing that the search for further generalization is, in a sense, bound to be futile. To this end, we show that the n-player Tullock contest with heterogeneous valuations and non-constant returns cannot, in general, be *solved by radicals*. That is, it is not feasible to express endogenous characteristics of the equilibrium, such as individual efforts, winning probabilities, or payoffs, in terms of the primitives of the model using basic arithmetic operations such as addition, subtraction, multiplication, and division, plus the extraction of roots. We also argue, but cannot prove of course, that our formal definition of tractability is equivalent to what is intuitively understood by tractability.[4]

The derivation of our main result, the intractability of the Tullock contest, proceeds in two steps. The first step is simple. Recalling that the probabilistic contest is an aggregative game,[5] we combine the necessary first-order conditions to a single polynomial equation whose unique positive solution pins down the equilibrium values of individual efforts, winning probabilities, and payoffs for all players. The issue of tractability of the Tullock contest is thereby boiled down to the question of whether a specific class of polynomial equations can be solved by radicals.[6] The second step of the analysis,

[3] Cf. Ryvkin (2007). The lack of a complete solution complicates, in particular, the comparison with the standard all-pay auction for which a complete solution is available (Baye et al., 1996).

[4] The term "radical" appears also in Hilbert's Nullstellensatz (Kübler et al., 2014, Thm. 2.1). There, it refers to the radical of an ideal, whereas here, it corresponds to the extraction of a root.

[5] In an *aggregative* game, individual payoffs are functions of the player's own action and some aggregate of the actions of the other players. See, e.g., Corchón (1994).

[6] Thus, the initial step of our analysis is analogous to the application of the *Shape Lemma* (Kübler and Schmedders, 2010a) that finds, under general conditions, a single univariate polynomial equation from which the solutions to a whole system of polynomial equations in several variables can be derived in a straightforward way.

however, is based on tools from *Galois theory*, which is a core topic in abstract algebra (van der Waerden, 1937). Specifically, we construct an example with $n = 5$ contestants and parameter $R = \frac{1}{2}$, and show that the associated polynomial equation derived in the first step cannot be solved by radicals. That result is extended, first to general valuations, and then to an arbitrary number of contestants $n \geq 5$. As any general solution formula for n contestants must solve, in particular, the case $R = \frac{1}{2}$, we obtain our impossibility result.[7]

1.2 Galois theory

In the early 19th century, the French mathematician Évariste Galois developed the theory named after him, concomitantly with the theory of permutation groups, to address questions of tractability of polynomial equations of degree five and higher.[8] The idea of this theory is that the roots of a polynomial constitute a finite set whose elements can be permuted.[9] The *Galois group* of a polynomial consists of those permutations of the roots that leave all multivariate algebraic relationships with rational coefficients between the roots intact. The fundamental insight of Galois was that the structure of the Galois group of a polynomial $g(X)$ contains information about the solvability of the associated polynomial equation $g(X) = 0$ by radicals. That is, the Galois group encodes if, and if so how, the roots of a polynomial equation can be computed from the coefficients of the polynomial using the basic arithmetic operations of addition,

[7] While this settles the issue in the general case, we will also explain why it is unlikely that solution formulas for other values of R will be found.

[8] At the time, Galois' theory provided answers to other long-standing problems such as the trisection of an angle, the doubling of the cube, and the construction of regular polygons (Edwards, 1984). More recently, Galois representations featured prominently in Andrew Wiles' proof of Fermat's Last Theorem.

[9] As usual, a complex number $s \in \mathbb{C}$ is called a *root* of the polynomial $g(X)$ if $g(s) = 0$.

subtraction, multiplication, and division, plus the extraction of roots. To obtain a definite answer for a specific polynomial equation, it is crucial to check:

(i) if the polynomial is *irreducible*, i.e., it does not decompose into a product of simpler polynomials, and

(ii) provided that the polynomial is irreducible, the Galois group of the polynomial is *solvable*.[10]

Thus, if the relevant polynomial is irreducible and the Galois group lacks the property of solvability, then one may conclude that its roots cannot be represented "in explicit terms." In this paper, we use Galois theory to study the tractability of the n-player Tullock contest.

1.3 Contribution

To evaluate the contribution of the present paper, it is essential to understand why our main result, the intractability of the Tullock contest, is not a straightforward consequence of the *Abel-Ruffini Impossibility Theorem*.[11] In short, that result says that, in contrast to polynomials of degree at most four, there is no general solution to polynomial equations of degree five or higher. On a superficial level, that seems to settle our research question, because it is not too difficult to find specifications of the primitives of the n-player Tullock contest for which the equilibrium conditions can be combined into a polynomial equation of arbitrarily high degree. However, there do exist families of polynomial equations of degree five and above that admit an explicit

[10]Definitions will be provided below.

[11]Cf. Kübler et al. (2014, fn. 5). An accessible exposition of the Abel-Ruffini Theorem can be found in Rosen (1995). Dummit (1991) and Kobayashi and Nakagawa (1992) derived formulas for the roots of solvable equations of degree five. Spearman and Williams (1994) characterized such equations.

solution. And indeed, this matters in the case of the Tullock contest, as the following example illustrates.

Example 1 *Suppose that there are $n = 5$ contestants, with valuations given by*

$$(V_1, V_2, V_3, V_4, V_5) = (27, 18, 12, 7, 2).$$

Suppose also that $R = \frac{1}{2}$. Then, as detailed in Appendix A.1, the analysis of the first-order conditions leads to a quintic, *i.e., to a polynomial equation of degree five. Still, the unique equilibrium is given by $x_i^* = \frac{24}{(1+48/V_i)^2}$, or more explicitly, by*

$$\begin{aligned}(x_1^*, x_2^*, x_3^*, x_4^*, x_5^*) &= (\tfrac{1944}{625}, \tfrac{216}{121}, \tfrac{24}{25}, \tfrac{1176}{3025}, \tfrac{24}{625}) \\ &= (3.11, 1.79, 0.96, 0.39, 0.04).\end{aligned}$$

The example shows that there do exist tractable examples even in cases in which the analysis leads to a polynomial equation of degree greater than four. This point is not obvious because the set of polynomials that arise from the analysis of contests is, as follows from Equation (19) below, a *strict* subset of the set of all polynomials. In this sense, Example 1 is special.[12] Thus, the main result of the present paper indeed does not easily follow from the Abel-Ruffini theorem.

1.4 Related literature

The present paper lies on the intersection of two strands of literature. The first is the literature on *contests*. Since Tullock's (1980) seminal work, explicit solutions of the probabilistic contest model have been derived under various sets of assumptions.

[12] Example 1 is, in fact, the only such example that we found during our investigations. As will be explained, this is not surprising given our main result and quantitative versions of Hilbert's Irreducibility Theorem.

The main contributions identifying pure-strategy solutions in the basic model, such as Hillman and Riley (1989), Pérez-Castrillo and Verdier (1992), Nti (1999), Stein (2002), Cornes and Hartley (2005), and Ewerhart (2025a), will be reviewed in Section 3.[13] Most prominently, Ryvkin (2007) pointed out the lack of explicit solutions for the n-player Tullock contest with heterogeneous valuations and non-constant returns. To address the issue, he employed first-order Taylor approximations around the tractable case of homogeneous valuations.[14]

The second strand of literature concerns the use of *algebraic methods in game theory*. Dresher et al. (1949) studied polynomial zero-sum games. Nash and Shapley (1950) characterized equilibria in behavior strategies in terms of roots of polynomial equations. In seminal work, Blume and Zame (1994) pointed out that the set of sequential equilibria of a finite extensive-form game is semi-algebraic, i.e., it may be understood as the set of solutions of a system of polynomial equalities and inequalities. Nau et al. (2004) noted that an irrational Nash equilibrium of a finite normal-form game with rational coefficients cannot be a corner point of the set of correlated equilibria. Datta (2003) showed that any real algebraic variety may be understood as the set of totally mixed equilibria of some finite normal-form game. Kübler and Schmedders (2010a, 2010b) constructed Gröbner bases for semi-algebraic sets that characterize equilibria of various kinds. Nie and Tang (2023, 2024) obtained algorithmic solutions to Nash equilibrium problems that are given by polynomial functions. None of these papers, however, employed Galois theory. As far as we know, there have been very few applica-

[13]Pérez-Castrillo and Verdier (1992), Cornes and Hartley (2005), and Ewerhart (2025a) documented the possibility of multiple pure-strategy equilibria in Tullock contests with increasing returns and more than two players. Mixed-strategy equilibria of the n-player Tullock contest have been characterized by Baye et al. (1994), Alcalde and Dahm (2010), Wang (2010), Ewerhart (2015, 2017a, 2017b, 2025b), and Feng and Lu (2017).

[14]See also Ryvkin (2013).

tions of Galois theory to game theory so far. Specifically, in response to the question by McKelvey and McLennan (1997) as to whether the computation of the equilibrium set could be simplified by starting from one equilibrium considered as known, Gandhi and Chatterji (2015) used Galois theory to construct new equilibria from a given sample equilibrium.[15] That approach led, in particular, to novel algorithms for the computation of mixed Nash equilibria in games with rational payoffs and irrational equilibria. However, those contributions are not directly related to our impossibility result.[16]

1.5 Overview

The remainder of the paper is structured as follows. Section 2 provides the necessary background on Galois theory. Section 3 reviews existing equilibrium characterizations for the Tullock contest. Section 4 presents our main result. Section 5 offers some discussion. Section 6 concludes. An Appendix contains material omitted from the body of the paper.

2 Background on Galois theory

This section provides the necessary background on Galois theory. We will discuss polynomial equations (Section 2.1), the Galois group (Section 2.2), and the Galois equivalence (Section 2.3).

[15] See also Gandhi (2011) and Chatterji and Gandhi (2011).

[16] The notion of *algebraic* tractability developed below also clearly differs from the widely used notion of *computational* tractability, which refers to deterministic computability in polynomial time in the context of the P vs. NP problem (e.g., von Stengel and Forges, 2008).

2.1 Polynomial equations

We consider equations of the type $g(X) = 0$, where

$$g(X) = a_N X^N + \ldots + a_1 X + a_0$$

is a *polynomial* with coefficients $a_0, \ldots, a_N$.[17] If $a_N \neq 0$, then N is the *degree* of $g(X)$.

A polynomial equation $g(X) = 0$ is *solvable by radicals* if its roots can be found from elements of the respective coefficient field by repeatedly taking sums, differences, products, and quotients, as well as by extracting roots. Here, the individual operations are understood to be finite in nature so that, e.g., infinite series are not allowed. Further, the extraction of roots refers to the inverse of the power map $s \mapsto s^K$, where $K \geq 2$ is an integer.[18]

For instance, the polynomial equation $X^5 - 2 = 0$ is solvable by radicals because one solution is given by $X = \sqrt[5]{2}$, and the other solutions can be easily found by multiplying the known solution with a fifth unit root. In contrast, $X^5 - X + 1 = 0$ is a classic example of a quintic not solvable by radicals. Proving that a specific equation is not solvable, however, requires the methods of Galois theory that will be reviewed below.

[17]Let $\mathbb{Q} = \{\frac{p}{q} : p, q \text{ integers}, q \neq 0\}$ denote the field of rational numbers. For *specific* valuations $V_1, \ldots, V_n \in \mathbb{Q}$, we will consider polynomials $g(X)$ over $\mathbb{Q}$. Hence, in this case, $a_0, \ldots, a_N \in \mathbb{Q}$. For *general* valuations, we will consider polynomials $g(X) \equiv g(X; V_1, \ldots, V_n)$ over the field of rational functions, $\mathbb{Q}(V_1, \ldots, V_n) = \{\frac{g_1(V_1,\ldots,V_n)}{g_2(V_1,\ldots,V_n)} : g_1, g_2 \text{ polynomials with integer coefficients}, g_2 \text{ is not identically zero}\}$. In that case, $a_0, \ldots, a_N \in \mathbb{Q}(V_1, \ldots, V_n)$.

[18]For $s \geq 0$, the inverse map is simply $s \mapsto \sqrt[K]{s}$. For complex s and $K \geq 2$, however, the power map is not globally invertible. Instead, any $s \neq 0$ admits precisely K pre-images that differ by powers of the Kth unit root. This multiplicity issue must be kept in mind when extracting roots from complex numbers. In those cases, solvability by radicals is understood in the most general sense, i.e., any pre-images in a given solution formula may be picked, if necessary (van der Waerden, 1937, § 56). For an illustration of this possibility, see the discussion of Equation (A.4) in the Appendix.

2.2 The Galois group

To decide if a polynomial equation is solvable, it is obviously sufficient to restrict attention to polynomials that cannot be easily factored. Formally, a polynomial over the field of rational numbers $\mathbb{Q}$, or similarly, over the function field $\mathbb{Q}(V_1, \ldots, V_n)$, is *irreducible* if it cannot be written as a product of two or more polynomials of degree at least one with coefficients in the same field.[19] To solve an irreducible equation by radicals, it suffices to be able to express a single root in this way (Edwards, 1984, p. 65, ex. 4). Another useful and well-known fact is that the roots of a polynomial $g(X)$ that is irreducible over $\mathbb{Q}$ have multiplicity one (Stewart, 2015, Prop. 9.14), and the same is true for polynomials irreducible over $\mathbb{Q}(V_1, \ldots, V_n)$. Thus, the number of distinct roots equals the degree of the polynomial in this case.

Consider an irreducible polynomial $g(X)$ of degree N with rational coefficients. Let $r_1, \ldots, r_N$ denote the different roots of $g(X)$. Given that $\{r_1, \ldots, r_N\}$ is a finite set, we may study its *permutations*, i.e., one-to-one mappings of this set. The set of all such permutations forms a group, known as the *symmetric group* S_N.[20] Now, the roots may jointly satisfy an algebraic relationship, say $h(r_1, \ldots, r_N) = 0$, where $h(Y_1, \ldots, Y_N)$ is a multivariate polynomial with rational coefficients. The *Galois group* of $g(X)$, denoted by $\mathcal{G}$, consists of those permutations π of the roots with the property that any algebraic

[19] While the irreducibility of a given polynomial may, with some luck, be verified using Gauss' lemma, parameter transformations, and Eisenstein's criterion, using computer algebra software is often more convenient. See Appendix A.8.

[20] In abstract algebra, a finite *group* consists of a finite set of elements (here: a set of permutations of the roots of a polynomial), a binary operation (here: the composition of permutations), and a neutral element (here: the trivial permutation that keeps all roots fixed) such that (i) the group operation is associative, (ii) every element has an inverse, and (iii) the group operation with the unit element has no effect. E.g., in $S_3 = \{e, (12), (13), (23), (123), (132)\}$, the neutral element is e, and the permutation (123) maps roots r_1 to r_2, r_2 to r_3, and r_3 to r_1. Moreover, the group operation corresponds to the execution of the permutations from right to left. E.g., in S_3, we have $(12)(123) = (23)$. It is important to realize that the group operation need not be commutative. And indeed, $(123)(12) = (13) \neq (23)$.

relationship $h(r_1, \ldots, r_N) = 0$ satisfied by the roots remains true after applying π to the roots, i.e., $h(r_{\pi(1)}, \ldots, r_{\pi(N)}) = 0$. We illustrate the concept with an example.

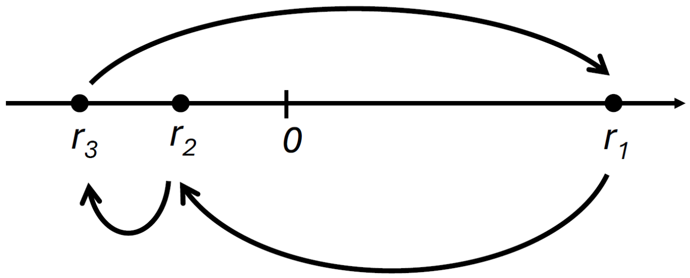

Figure 1: The permutation π_0 operates on the roots of the polynomial $g_0(X)$.

Example 2 *The polynomial $g_0(X) = X^3 - 9X - 9$ has the three real roots $r_1 = 3.41$, $r_2 = -1.18$, and $r_3 = -2.23$, as illustrated in Figure 1.*[21] *The Galois group $\mathcal{G}_0$ of $g_0(X)$ turns out to be the cyclic group of order three,*[22] *a generator of which is the permutation $\pi_0 = (123)$ that maps r_ν to $r_{\nu+1}$ if $\nu \in \{1, 2\}$ and r_3 to r_1. To understand why some permutations are members of the Galois group, while others are not, consider the following two illustrations. First, the algebraic relationship $(r_1 - r_2)(r_2 - r_3)(r_1 - r_3) = 27$ remains valid if π_0 is applied to the roots. One can show that this is actually true for any algebraic relationship in the three variables r_1, r_2, and r_3 with rational coefficients. This means by definition that π_0 is a member of $\mathcal{G}_0$. Second, the very same relationship becomes invalid if, for instance, the permutation $\pi_1 = (12)$ is applied, because*

$$(r_{\pi_1(1)} - r_{\pi_1(2)})(r_{\pi_1(2)} - r_{\pi_1(3)})(r_{\pi_1(1)} - r_{\pi_1(3)}) = (r_2 - r_1)(r_1 - r_3)(r_2 - r_3) = -27 \neq 27.$$

Thus, π_1 is not a member of $\mathcal{G}_0$.

[21]This polynomial happens to arise in the analysis of a three-player contest with valuation vector $(V_1, V_2, V_3) = (6, 3, 2)$ and parameter $R = \frac{1}{2}$. See Appendix A.4.

[22]The *order* of a finite group is the number of its elements.

This definition of the Galois group extends in a completely analogous way to polynomials with coefficients in $\mathbb{Q}(V_1, \ldots, V_n)$.

2.3 Galois' equivalence[23]

The gist of Galois theory is that the knowledge of the Galois group of an irreducible polynomial allows us to decide if the corresponding polynomial equation can be solved by radicals or not. In particular, for a polynomial $g(X)$ of degree five that is irreducible over the rationals, it suffices to show that the Galois group is, e.g., the full symmetric group S_5 to be able to deduce that $g(X) = 0$ cannot be solved by radicals.

By definition, the group $\mathcal{G}$ is *solvable* if there is a finite sequence of subgroups

$$\{1\} = \mathcal{G}^{(0)} \subsetneq \mathcal{G}^{(1)} \subsetneq \cdots \subsetneq \mathcal{G}^{(L)} = \mathcal{G}, \tag{3}$$

such that each $\mathcal{G}^{(l)}$ is a normal subgroup of $\mathcal{G}^{(l+1)}$, and all quotient groups $\mathcal{G}^{(l+1)}/\mathcal{G}^{(l)}$ are abelian.[24] Intuitively, a non-abelian quotient group in a maximally refined sequence (3) is a "smoking gun" for the existence of a root that cannot be found by basic arithmetic operations and the extraction of roots alone.

Lemma 1 (Galois Equivalence) *Let $g(X)$ be a polynomial that is irreducible over $\mathbb{Q}$ (or over $\mathbb{Q}(V_1, \ldots, V_n)$). Then, the following statements are equivalent:*

(i) $g(X) = 0$ is solvable by radicals;

(ii) the Galois group of $g(X)$ is solvable.

[23] The main result of Galois theory is the inclusion-reversing isomorphism between the lattice of intermediate fields of a finite Galois extension and the lattice of subgroups of its Galois group. That insight, known as Galois' correspondence, is used to derive Lemma 1 below.

[24] A subgroup $\mathcal{N}$ of a group $\mathcal{G}$ is called *normal* if $\pi \mathcal{N} \pi^{-1} = \mathcal{N}$ for all elements $\pi \in \mathcal{G}$. It is a basic result in group theory that the cosets $\pi \mathcal{N}$ form a group, known as the *quotient group*. A group $\mathcal{G}$ is called *abelian* if the group operation is commutative.

Proof. See Stewart (2015, Thms. 15.8 and 18.21). □

We illustrate Lemma 1 by returning to our earlier example.

Example 2 (continued) *The cyclic group of order three,* $\mathcal{C}_3 \subseteq S_3$*, which is generated by the permutation* $\pi_0 = (123)$*,*[25] *admits the trivial decomposition*

$$\begin{array}{ccc} \mathcal{G}^{(0)} & \subseteq & \mathcal{G}^{(1)} \\ \shortparallel & & \shortparallel \\ \{e\} & \subseteq & \mathcal{C}_3. \end{array}$$

Thus, $\mathcal{C}_3$ *is solvable. By Lemma 1, this is equivalent to the statement that the equation* $g_0(X) = 0$ *is solvable by radicals. And indeed, an application of Cardano's formula yields* $r_{1,2,3} = \sqrt[3]{\frac{9+\sqrt{-27}}{2}} + \sqrt[3]{\frac{9-\sqrt{-27}}{2}}$*, where the three solutions result from choosing different values for the cubic roots (see Appendix A.3). Thus, the solutions of* $g_0(X) = 0$ *may indeed be represented using basic arithmetic operations and the extraction of roots alone.*[26]

In the example, we of course knew about the existence of an explicit formula before, because the degree of $g_0(X)$ is just three, but the point is that Lemma 1 holds for polynomials of any degree.

3 Tractable cases of the Tullock contest

This section reviews the main results in the literature that provide an explicit solution to the Tullock contest. For convenience, we will restrict attention to equilibria in pure strategies, emphasizing cases in which the equilibrium is unique.

[25] Thus, $\mathcal{C}_3 = \{e, (123), (132)\}$.

[26] Contrary to what one might expect, the explicit representation in this and similar examples may require (i) extracting roots from complex numbers even if the polynomial has only real roots (van der Waerden, 1937, pp. 188-189), and (ii) taking repeated radicals even if the extension is cyclic and of prime degree (Kang, 2000, Thm. 1).

3.1 Homogeneous valuations

Suppose first that $V_1 = \ldots = V_n \equiv V > 0$, i.e., all contestants possess the same positive valuation of winning. Assuming, for the moment, a symmetric strategy profile with $x_1 = \ldots = x_n > 0$, the necessary first-order condition for contestant $i \in I$ simplifies and yields an equilibrium effort of

$$x_i^* = \frac{(n-1)RV}{n^2}. \tag{4}$$

Clearly, contestant i wins with equal probability $p_i^* = \frac{1}{n}$. The corresponding equilibrium payoff is, therefore, given by

$$\Pi_i^* = \frac{(n-(n-1)R)V}{n^2}. \tag{5}$$

It turns out that these formulas characterize the unique symmetric Nash equilibrium if and only if $R \leq \frac{n}{n-1}$.

However, as noted by Pérez-Castrillo and Verdier (1992, Prop. 3), there may also be asymmetric equilibria. In any such equilibrium, a strict subset of the players exerts the same positive effort while the remaining players exert a zero effort. Since the Tullock contest does not admit equilibria in which only one contestant exerts a positive effort, an asymmetric equilibrium requires $n \geq 3$ players (under the present assumptions). More specifically, an asymmetric equilibrium with precisely $m \in \{2, \ldots, n-1\}$ active contestants can be shown to exist if and only if $R \in [R_*(m), R^*(m)]$, where $R^*(m) = \frac{m}{m-1}$ and $R_*(m) \in (1, R^*(m))$ are threshold values (Ewerhart, 2025a, Prop. 2).

The following result summarizes the discussion.

Proposition 1 *Suppose that $V_1 = \ldots = V_n \equiv V > 0$ and that either (i) $n = 2$ and $R \leq 2$, or (ii) $n \geq 3$ and $R < R_*(n-1)$. Then, the pure-strategy Nash equilibrium is* *unique, symmetric, interior, and characterized by (4) and (5).*[27]

Proof. By Pérez-Castrillo and Verdier (1992, Prop. 4), the symmetric equilibrium exists, is interior, and satisfies (4) and (5) if $R \leq \frac{n}{n-1}$. For $n = 2$, this equilibrium is always unique (cf. Prop. 3 below). For $n \geq 3$, the equilibrium is unique if and only if $R < R_*(n-1)$, where $R_*(n-1) < \frac{n}{n-1}$ (Ewerhart, 2025a, Prop. 5 & Appendix). □

3.2 Constant returns

Suppose next that $R = 1$. Then, the necessary first-order condition for a contestant i exerting a positive effort $x_i > 0$ simplifies to

$$\frac{X - x_i}{X^2} V_i - 1 = 0,$$

where $X = x_1 + \ldots + x_n$ is the aggregate effort.[28] Solving for x_i and subsequently adding over the n contestants, one obtains the equilibrium value

$$X^* = \frac{(n-1)\bar{V}_n}{n}, \tag{6}$$

where $\bar{V}_n = n\left(V_1^{-1} + \ldots + V_n^{-1}\right)^{-1}$ denotes the harmonic mean of contestants' valuations. Individual efforts, winning probabilities, and payoffs may be computed from X^*

[27]For $n \geq 3$ and $R \in [R_*(n-1), 2]$, there are multiple asymmetric equilibria. In that case, the number of contestants m exerting a positive effort may vary, but the equilibrium efforts and payoffs of those active contestants are characterized as above with n replaced by m. For $R > 2$, there is no equilibrium in pure strategies. See Cornes and Hartley (2005, Thm. 7), Ryvkin (2007, Sec. 3), and Ewerhart (2025a).

[28]For convenience, we use X to denote both a formal indeterminate and aggregate effort in the contest analysis.

via the relationships

$$x_i^* = X^*\left(1-\frac{X^*}{V_i}\right), \tag{7}$$

$$p_i^* = 1-\frac{X^*}{V_i}, \tag{8}$$

$$\Pi_i^* = \left(1-\frac{X^*}{V_i}\right)^2 V_i. \tag{9}$$

An analysis of optimal entry shows that this characterizes an interior Nash equilibrium in pure strategies if and only if $V_n > \frac{n-1}{n}\bar{V}_n$ (or equivalently, if and only if $V_n > \frac{n-2}{n-1}\bar{V}_{n-1}$).

Proposition 2 *Suppose that $R=1$ and $V_n > \frac{n-2}{n-1}\bar{V}_{n-1}$. Then, the pure-strategy Nash equilibrium is unique, interior, and characterized by (7)-(9).*

Proof. The equilibrium property has been established by Hillman and Riley (1989, Prop. 5). The observation that the equilibrium is unique has been made at various places in the literature (Gibbens and Kelly, 1999; Stein, 2002; Matros, 2006). □

If the condition on the valuations is not satisfied, contestant n exerts zero effort, and the characterization applies analogously with $(n-1)$ replacing n. By iterating this argument, one determines the set of contestants that exert positive effort. In this case, the unique equilibrium is a boundary equilibrium.

3.3 Two active contestants

Suppose finally that $n=2$. In this case, the two first-order conditions read

$$\frac{Rx_1^{R-1}x_2^R}{(x_1^R+x_2^R)^2}V_1 = 1,$$

$$\frac{Rx_2^{R-1}x_1^R}{(x_1^R+x_2^R)^2}V_2 = 1.$$

Dividing the two equations yields

$$x_2 = \lambda x_1,$$

with $\lambda = V_2/V_1 \in (0,1]$, which allows eliminating x_2 in the first-order condition of contestant 1. Rearranging, one arrives at equilibrium efforts

$$x_1^* = \frac{RV_1^{R+1}V_2^R}{(V_1^R + V_2^R)^2} \text{ and } x_2^* = \frac{RV_1^R V_2^{R+1}}{(V_1^R + V_2^R)^2}. \tag{10}$$

From this, we obtain winning probabilities $p_i^* = V_i^R/(V_1^R + V_2^R)$, as well as payoffs

$$\Pi_1^* = \frac{V_1^{R+1}\left(V_1^R + (1-R)V_2^R\right)}{(V_1^R + V_2^R)^2}, \tag{11}$$

$$\Pi_2^* = \frac{V_2^{R+1}\left((1-R)V_1^R + V_2^R\right)}{(V_1^R + V_2^R)^2}. \tag{12}$$

It can now be checked that these equations characterize the unique Nash equilibrium in pure strategies if and only if $R \leq 1 + \lambda^R$.[29]

Proposition 3 *Suppose that $n = 2$ and that $R \leq 1 + (V_2/V_1)^R$. Then, the pure-strategy Nash equilibrium is unique, interior, and characterized by (10)-(12).*

Proof. See Nti (1999). □

It apparently went unnoticed in the literature that, in the case of strictly increasing returns to scale, Proposition 3 admits an extension to the case of $n \geq 3$ contestants. Specifically, for $R \in (1, 1 + \lambda^R]$ and V_3/V_1 not too large, there exists an equilibrium in which only contestants 1 and 2 are active, choosing their efforts as if there were no other contestants. Depending on the vector of valuations, there may also be multiple equilibria in this case, with another pair of players being active.[30]

[29] For $R > 1 + \lambda^R$, there are no equilibria in pure strategies. If $R \in (1 + \lambda^R, 2]$, then contestant 1 uses a pure strategy while contestant 2 uses a mixed strategy (this case requires $V_2 < V_1$). See Wang (2010), Ewerhart (2017b), and Feng and Lu (2017). For $R > 2$, the equilibrium is in mixed strategies (Baye et al., 1994; Alcalde and Dahm, 2010; Wang, 2010; Ewerhart, 2015, 2017a) and unique (Ewerhart, 2025b).

[30] For further details, see Appendix A.2.

Apart from the cases surveyed above, we are not aware of any explicit characterizations of the pure-strategy Nash equilibrium in the literature. It is known, however, that the solution is unique and interior for any $R \in (0, 1)$ and any $V_1 \geq \ldots \geq V_n > 0$ (Szidarovszky and Okuguchi, 1997). We will therefore focus on this case in the sequel.

4 A limitation of tractability

This section outlines our main contribution. We start by providing a formal definition of tractability (Section 4.1), illustrate it with an example (Section 4.2), and finally, present the main result of the paper (Section 4.3).

4.1 A formal definition of tractability

Fix $n \geq 2$ and let $R \in (0, 1)$. The *primitives of the model* are the exogenous parameters $V_1 \geq \ldots \geq V_n > 0$. We define tractability as follows.

Definition 1 *We say that the n-player Tullock contest with parameter R is* ***solvable by radicals*** *if its key equilibrium characteristics, including individual efforts, winning probabilities, and payoffs, may be determined from the primitives of the model by repeatedly taking sums, differences, products, and quotients, as well as extracting roots.*

For the applied economist, the definition might seem restrictive. For example, additional functions could be added to the set of admissible operations. However, as will be discussed below, there are good reasons to assume that the definition captures what is intuitively understood by tractability within the considered class of games. Definition 1 also seems to be the first formal definition of algebraic tractability in the economics literature, and might therefore be of independent interest.

The tractable cases surveyed in Section 3 all satisfy the definition. A particular case is Proposition 3, which features the term $\lambda^R = (V_2/V_1)^R$ in the solution formulas. If $R = \frac{p}{q}$ is rational, however, then $\lambda^R = \lambda^{p/q} = \sqrt[q]{\lambda^p}$, which is representable using radicals. Thus, recalling that the set of rational numbers is dense in the reals, there is little that is lost.

Our main result (Theorem 1 below) says that the n-player Tullock contest is, in general, not solvable by radicals. It even shows that *none* of the equilibrium characteristics mentioned in Definition 1 can be determined using basic arithmetic operations and root extractions alone.

4.2 An intractable example

The following example illustrates that the n-player Tullock contest may fail to be solvable by radicals for specific values of the primitives.

Example 3 *Suppose that there are $n = 5$ contestants, with valuations*

$$(V_1, V_2, V_3, V_4, V_5) = (5, 4, 3, 2, 1).$$

Suppose, in addition, that $R = \frac{1}{2}$. Then there is a unique Nash equilibrium in pure strategies

$$\begin{aligned} x^* &= (x_1^*, x_2^*, x_3^*, x_4^*, x_5^*) \\ &= (0.53, 0.38, 0.25, 0.13, 0.04). \end{aligned}$$

However, for none of the players can the equilibrium efforts, winning probabilities, or payoffs be derived from the primitives of the model using basic arithmetic operations and the extraction of roots alone.

Next, we explain why Example 3 is not tractable. For $R = \frac{1}{2}$, while keeping $n \geq 2$ and $V_1 \geq \ldots \geq V_n > 0$ general, the system of necessary first-order conditions (2) reads

$$\frac{\sqrt{X} - \sqrt{x_i}}{2\sqrt{x_i}X} V_i - 1 = 0,$$

where $X = (\sqrt{x_1} + \ldots + \sqrt{x_n})^2$ is a *generalized aggregate* of individual efforts. These conditions are also sufficient because the marginal return is infinite at zero effort, so that all contestants choose a positive effort.[31] Solving for $\sqrt{x_i}$ yields

$$\sqrt{x_i} = \frac{\sqrt{X}V_i}{2X + V_i}. \tag{13}$$

Summing over all contestants, and subsequently dividing by $\sqrt{X} > 0$, one obtains

$$\frac{V_1}{2X + V_1} + \ldots + \frac{V_n}{2X + V_n} = 1. \tag{14}$$

Given that the left-hand side assumes the value n for $X = 0$ and is continuously diminishing to zero for large X, this equation uniquely characterizes the equilibrium value $X^* > 0$. Moreover, given X^*, we arrive at

$$x_i^* = \frac{X^* V_i^2}{(2X^* + V_i)^2}, \tag{15}$$

$$p_i^* = \frac{V_i}{2X^* + V_i}, \tag{16}$$

$$\Pi_i^* = \frac{(X^* + V_i)V_i^2}{(2X^* + V_i)^2}. \tag{17}$$

Conversely, if for some $i \in \{1, \ldots, n\}$, only one of the endogenous characteristics x_i^*, p_i^*, or Π_i^* is known, then we can derive X^* by solving, in the worst case, a quadratic equation.

[31] Indeed, using a suitable substitution (e.g., Szidarovszky and Okuguchi, 1997), this case may be rephrased as a Tullock contest with constant returns and quadratic costs.

From the above, the generalized aggregate X in our example satisfies

$$\frac{5}{2X+5} + \frac{4}{2X+4} + \frac{3}{2X+3} + \frac{2}{2X+2} + \frac{1}{2X+1} = 1.$$

Multiplying through and collecting terms, we obtain the polynomial equation

$$g(X) = 8X^5 - 170X^3 - 450X^2 - 411X - 120 = 0. \tag{18}$$

Ignoring negative solutions,[32] one numerically finds the root $X^* = 5.72$.

Our discussion so far may be summarized as follows.

Lemma 2 *The following statements are equivalent:*

(i) For some player i, the equilibrium effort x_i^* is solvable by radicals.[33]

(ii) For some i, the equilibrium winning probability p_i^* is solvable by radicals.

(iii) For some i, the equilibrium payoff Π_i^* is solvable by radicals.

(iv) $g(X) = 0$ is solvable by radicals.

Proof. See the text above. $\square$

We will now show that $g(X)$ is not solvable by radicals. In view of Lemma 1, it suffices to check the following facts.

Lemma 3 *The following statements are true:*

(i) $g(X)$ is irreducible over $\mathbb{Q}$;

[32] Indeed, in addition to the unique positive solution, equation (14) has a total of $(n-1)$ negative solutions, each of which lies strictly between a pair of neighboring poles.

[33] Note the abuse of terminology. We mean here that x_i^*, etc., may be expressed by repeatedly applying basic arithmetic operations and roots.

(ii) the Galois group of $g(X)$ is the full symmetric group S_5;

(iii) S_5 is not solvable.

Proof. Parts (i) and (ii) have been established using *Sage*. For details, see Appendix A.8. Part (iii) is well-known. See, e.g., Stewart (2015, Cor. 14.8). □

Thus, $g(X)$ is indeed not solvable by radicals, and the contest in Example 3 is intractable.

4.3 A general result

The following theorem is the main result of this paper.

Theorem 1 *For $n \geq 5$ and $R = \frac{1}{2}$, the n-player Tullock contest with general valuations $V_1 \geq \ldots \geq V_n > 0$ is not solvable by radicals.*

Proof. See Appendix A.5. □

The theorem above may be understood as an impossibility result. Indeed, if a formula existed for the equilibrium in the n-player contest, given valuations $V_1 \geq \ldots \geq V_n > 0$ and a parameter $R > 0$, possibly with case distinctions, then it should specialize, in particular, to a formula in the case $R = \frac{1}{2}$. Since such a formula is not available by the theorem, a *general* solution of the Tullock contest is not feasible.[34]

To understand what Theorem 1 entails, it is important to distinguish solvability over $\mathbb{Q}$ and solvability over $\mathbb{Q}(V_1, \ldots, V_n)$. In the analysis of Example 3, we checked that $g_5(X)$ is not solvable over $\mathbb{Q}$. In contrast, Theorem 1 says for the case $n \geq 5$ that the polynomial $g_n(X; V_1, \ldots, V_n)$ that characterizes the generalized aggregate

[34]For an explicit discussion of contests with $R \neq \frac{1}{2}$, see Section 5.

X as a function of the valuation vector is not solvable over $\mathbb{Q}(V_1, \ldots, V_n)$.[35] This result is stronger than the example for two reasons. First, it allows us to extend the impossibility captured by Example 3 to larger contests. Thus, for any $n \geq 5$, no general solution formula exists that would allow to compute the solution for all valuation vectors $(V_1, \ldots, V_n)$.

Second, the reformulation allows us to assess how "typical" the intractability property is for, say, randomly selected primitives. By *Hilbert's Irreducibility Theorem*, a fundamental result in diophantine geometry, there are infinitely many valuation vectors $(V_1, \ldots, V_n) \in \mathbb{Q}^n$ such that the Galois group of the polynomial with coefficients in $\mathbb{Q}(V_1, \ldots, V_n)$ does not change when specific values are plugged in and the polynomial is considered over $\mathbb{Q}$ instead. Quantitative versions of this result, such as given by Cohen (1981), imply that such valuation vectors can always be found in the economically relevant domain, i.e., when $V_1 \geq V_2 \geq \ldots \geq V_n > 0$. In fact, there is a sense in which "almost all" such vectors with rational components have this property.

Corollary 2 *Consider the n-player Tullock contest with $n \geq 5$ and $R = \frac{1}{2}$. Let $V^{\max} > 0$ be a rational number, and $\varepsilon > 0$. Then, for any sufficiently small grid step $\delta > 0$ that divides the interval $[0, V^{\max}]$ evenly into $M = \frac{V^{\max}}{\delta}$ subintervals, the share of the tractable cases within the set of valuation vectors $(V_1, \ldots, V_n)$ such that $V_1 \geq \ldots \geq V_n > 0$ and such that each V_i is taken from the grid $\{\delta, 2\delta, 3\delta, \ldots, (M-1)\delta, M\delta = V^{\max}\}$ is smaller than ε.*

Proof. See Appendix A.6. □

[35] This polynomial will be determined explicitly below. For example, for $n = 5$, it reads

$$g_5(X; V_1, \ldots, V_5) = 32X^5 - 8\,\sigma_2\,X^3 - 8\,\sigma_3\,X^2 - 6\,\sigma_4\,X - 4\,\sigma_5,$$

where the σ_k are elementary symmetric functions in $V_1, \ldots, V_5$. See Footnote 36.

Thus, Theorem 1 implies that the n-player Tullock contest is intractable for any $n \geq 5$ and the vast majority of specifications of the valuation vector.

Theorem 1 is obtained by contradiction. In the Appendix, we determine the general form of equation (18) as

$$g_n(X; V_1, \ldots, V_n) = \sum\nolimits_{k=0}^{n} (1-k)\sigma_k(V_1, \ldots, V_n)(2X)^{n-k}, \tag{19}$$

where $\sigma_k \equiv \sigma_k(V_1, \ldots, V_n)$ denotes the *elementary symmetric polynomial* of degree k in the variables $V_1, \ldots, V_n$.[36] As discussed above, for any economically meaningful choice of the valuation vector, $g_n(X; V_1, \ldots, V_n)$ has n distinct roots of multiplicity one, and the generalized aggregate $X^* = X^*(V_1, \ldots, V_n)$ as its sole positive root. We show that the Galois group of $g_n(X; V_1, \ldots, V_n)$ over the function field $\mathbb{Q}(V_1, \ldots, V_n)$ contains the Galois group of $g_{n-1}(X; V_1, \ldots, V_{n-1})$ as a subgroup. That result is obtained using the concept of *specialization* in Galois theory (van der Waerden, 1937, §61). Intuitively, we replace V_n by the value zero, which amounts to a well-defined mapping from the integral domain of parameterized polynomials $\mathbb{Q}(V_1, \ldots, V_n)[X]$ onto its subring $\mathbb{Q}(V_1, \ldots, V_{n-1})[X]$, even though we cannot do this in any solution formula.[37] Hence, by induction, we can make our way down to $g_5(X; V_1, \ldots, V_5)$. The Galois group of that polynomial over $\mathbb{Q}(V_1, \ldots, V_5)$, however, can be shown to be the full symmetric group S_5, because it specializes to Example 3. As S_5 is not solvable, we may use Lemma 1 to deduce that $g_n(X; V_1, \ldots, V_n)$ is not solvable by radicals over $\mathbb{Q}(V_1, \ldots, V_n)$, for any $n \geq 5$.

In fact, for a rigorous application of Lemma 1, we also need to show that $g_n(X) \equiv$

[36] Thus, $\sigma_0 = 1$, $\sigma_1 = V_1 + \ldots + V_n$, $\sigma_2 = V_1 V_2 + \ldots + V_{n-1} V_n$, and so on, up to $\sigma_n = V_1 \cdot \ldots \cdot V_n$. Cf. Stewart (2015, Sect. 18.2).

[37] Indeed, V_n might occur in the denominator of the solution formula, so that setting $V_n = 0$ may not be a well-defined operation.

$g_n(X; V_1, \ldots, V_n)$ is irreducible over $\mathbb{Q}(V_1, \ldots, V_n)$. Noting that the leading coefficient of the corresponding polynomial in $Z = 2X$ is one, Gauss' lemma implies that it suffices to check that $g_n(X)$ is irreducible over the unique factorization domain $\mathbb{Z}[V_1, \ldots, V_n]$. We show that $g_n(X)$ does not admit a linear factor for any $n \geq 2$. Moreover, we prove that

$$g_n(X; V_1, \ldots, V_{n-1}, 0) = (2X) \cdot g_{n-1}(X; V_1, \ldots, V_{n-1}). \tag{20}$$

The proof now proceeds by induction. Clearly, $g_2(X; V_1, V_2) = 4X^2 - V_1V_2$ is irreducible over $\mathbb{Z}[V_1, V_2]$. Moreover, if $g_n(X)$ was reducible for some $n \geq 3$, then each factor would be quadratic at least, and hence, by relationship (20), the decomposition would be inherited by $g_{n-1}(X)$, completing the argument.

5 Discussion

This section offers additional perspective on our findings. We first argue that, for the considered class of games, our concept of tractability is unlikely to be affected even if we were to add further functions as admissible operations (Section 5.1). Next, we note that, whatever definition we ultimately choose, there will always be a need for a postulate ensuring that the preferred definition captures the intuitive notion of tractability (Section 5.2). Then, we explain why explicit solutions cannot, in general, be expected for parameter values other than $R = \frac{1}{2}$ (Section 5.3). Finally, we discuss the implications for numerical analysis (Section 5.4).

5.1 Adding elementary functions

As noted before, one might argue that the notion of tractability promoted in this study is of limited interest because economists are familiar with a number of special functions, such as the exponential, the logarithm, and various trigonometric functions. Upon reflection, however, it seems very unlikely that the addition of such functions would resolve the tractability issue for the Tullock contest. After all, this would imply, for instance, that the quintic constructed in the discussion of Example 3 is tractable by allowing for additional operations. But the properties of unsolvable quintics have been studied very thoroughly by mathematicians for more than two centuries, making this indeed a very remote possibility. Thus, even if our definition of tractability excludes the use of elementary functions, it seems to capture quite accurately which polynomial equations are tractable in a practical sense and which are not.[38]

5.2 The need for a postulate

There is, however, another problem that cannot be wiped away so easily, viz. that the tractability of a model is a rather vague concept. The situation is reminiscent of the problem of defining effective computability in computer science. It requires a *postulate*, such as the Church-Turing thesis, to assert that computability in the intuitive sense (i.e., by a scientist) is equivalent to computability in the formal sense (e.g., by a Turing machine). Similarly here, it seems to require such a postulate to assert that tractability in the practical sense is equivalent to tractability in the formal sense.[39]

[38] The mathematical literature has identified ways to deal with the implications of Galois' theory. According to a survey poster (Wolfram Research, 2005), there are solution approaches for general polynomial equations based on continued fractions, modular forms, theta functions, infinite series representations, Mellin integrals, hypergeometric functions, and elliptic Siegel functions. Such approaches, however, tend to add a multivariate transcendental function to the set of admissible operations (Umemura, 2007). The extent to which those methods are suitable for economic analysis is, therefore, still to be explored.

[39] Conversely, one might also argue that Definition 1 is too generous in some cases, e.g., if the resulting formulas are difficult to interpret or to work with. Given the purpose of the present paper, however, which is an impossibility result, we are on the safe side with respect to that concern.

5.3 Alternative values of R

Theorem 1 is a partial result in the sense that there might exist values of the parameter R different from $\frac{1}{2}$ for which a solution formula exists. However, as we argue below, that possibility is likewise unlikely. For rational $R = \frac{p}{q}$, with integers $q > p > 0$, the unique vector of equilibrium efforts solves a system of algebraic equations. As seen above for $p = 1$ and $q = 2$, that system can be reduced by hand to a single polynomial equation for the generalized aggregate X. In general, that simplification is still available, as we show in Appendix A.7. However, the polynomial quickly becomes more complex. Table I illustrates this by reporting the degree d of the minimal polynomial produced by *Mathematica* for a three-player Tullock contest with valuations $(V_1, V_2, V_3) = (3, 2, 1)$. For the considered cases with $p > 1$, the problem could be reduced to solving a polynomial of degree $d' = d/p$ using the substitution $Z = X^p$.

p/q	1/2	1/3	2/3	1/4	3/4	1/5	2/5	3/5	4/5
d	3	7	14	13	39	21	38	57	84
d'	3	7	7	13	13	21	19	19	21

Table I: The degrees of the respective minimal polynomials of X and $Z = X^p$

Cases in which we were able to determine a Galois group include $p \in \{1, 2\}$ and $q = 3$, corresponding to $R = \frac{1}{3}$ and $R = \frac{2}{3}$. In those cases, the polynomial is of degree $d = d' = 7$, irreducible, and of Galois group S_7, which is unsolvable. In all other cases, the degree of the minimal polynomial is so large that, even if an example could be found in which the Galois group is solvable, the resulting explicit formula might either never be found or, if it can be found, would be of little practical value.[40]

[40] A story that might come to mind is that, at the end of the 19th century, the German mathematician Johann Gustav Hermes spent a decade showcasing the construction of the regular 65537-gon with straightedge and compass.

5.4 Implications for numerical analysis

One might wonder to what extent Equation (19) can be generalized to any $R = \frac{p}{q}$ with integers $q \geq p \geq 1$. This might yield an interesting representation that is amenable to numerical analysis and could be useful, for example, for contest experiments. The generalized aggregate X is indeed always algebraic over $\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$. In fact, we have the following result.

Proposition 4 *Suppose that $R = \frac{p}{q}$, with $0 < p < q$ integers, and let $n \geq 2$. Then, the generalized aggregate $X = (x_1^{p/q} + \ldots + x_n^{p/q})^{q/p}$ is the root of a nonzero polynomial whose coefficients are taken from $\mathbb{Z}[\sigma_1, \ldots, \sigma_n]$.*

Proof. See Appendix A.7. □

Once such a polynomial is found by symbolic manipulation, X can be numerically obtained for any given vector $(V_1, \ldots, V_n)$. From there, equilibrium efforts can be derived via the first-order conditions. The following example illustrates this approach.

Example 4 *For $n = 3$ and $R = \frac{1}{3}$, the generalized aggregate*

$$X = (x_1^{1/3} + x_2^{1/3} + x_3^{1/3})^3$$

is a root of the irreducible polynomial[41]

$$\begin{aligned} g_3(X; V_1, V_2, V_3) = \ & (3X)^7 - 6\sigma_2(3X)^5 - \big(2\sigma_1\sigma_2 + 58\sigma_3\big)(3X)^4 \\ & + \big(-79\sigma_1\sigma_3 + 9\sigma_2^2\big)(3X)^3 + \big(-32\sigma_1^2\sigma_3 + 6\sigma_1\sigma_2^2 - 22\sigma_2\sigma_3\big)(3X)^2 \\ & + \big(-4\sigma_1^3\sigma_3 + \sigma_1^2\sigma_2^2 - 13\sigma_1\sigma_2\sigma_3 + 8\sigma_3^2\big)(3X) \\ & + \big(-2\sigma_1^2\sigma_2\sigma_3 + 2\sigma_1\sigma_3^2\big). \end{aligned}$$

Specializing to $V_1 = 3$, $V_2 = 2$, $V_3 = 1$ *yields* $\sigma_1 = 6$, $\sigma_2 = 11$, $\sigma_3 = 6$, *and*

$$g_3(X) = 2187X^7 - 16038X^5 - 38880X^4 - 47385X^3 - 36072X^2 - 17064X - 4320.$$

The unique real root of $g(X)$ *is* $X = 3.74$. *Plugging this into the first-order conditions*

$$x_i = \frac{1}{216X^2}\left(-V_i + \sqrt{V_i^2 + 12V_iX}\right)^3$$

gives equilibrium efforts $x_1 = 0.240$, $x_2 = 0.150$, *and* $x_3 = 0.064$.

6 Concluding remarks

In this paper, we have shown that the pure-strategy Nash equilibrium of the n-player Tullock contest cannot, in general, be expressed in terms of the primitives of the model using only basic arithmetic operations and root extractions. We have also explained why this limitation of the model cannot be overcome by introducing familiar functions such as the exponential or the logarithm. Thus, our analysis clearly delineates the boundaries of tractability for an important workhorse model.

[41] This polynomial was found using *Mathematica*. To verify that $g_3(X; V_1, V_2, V_3)$ is irreducible over $\mathbb{Q}(V_1, V_2, V_3)$, we checked via *Sage* that $g_3(X; 3, 2, 1)$ is irreducible over $\mathbb{Q}$. For $V_3 = 0$, the polynomial $g_3(X; V_1, V_2, 0) = 3X\left(27X^3 - 9X\sigma_2 - \sigma_1\sigma_2\right)^2$ has a unique positive root, of multiplicity two, at $X^* = \frac{1}{3}(V_1V_2)^{1/3}(V_1^{1/3} + V_2^{1/3})$, linking the example back to Proposition 3.

What is the broader scope of the methods developed here? We believe that our formal definition of tractability applies naturally to other economic environments. Specifically, in models such as Bertrand pricing, Walrasian exchange, and arms races with incomplete information, equilibria can be characterized as solutions of systems of polynomial equations, possibly complemented by inequality constraints (Judd et al., 2012). Applications of the Shape Lemma, followed by an analysis along the lines developed in the present paper, might then allow researchers to determine, once and for all, whether such models are solvable by radicals. As in the case of the Tullock contest studied above, such an approach could settle recurring speculations regarding the possibility of extending tractable cases in economic theory.

A Appendix

This appendix contains material that has been omitted from the body of the paper.

A.1 Details on Example 1

We first check the equilibrium property directly. Given that $R < 1$, it is never optimal for any contestant to exert an effort of zero. Moreover, payoff functions are globally strictly concave in own effort in the interior. It therefore suffices to check the first-order conditions. Indeed, define the generalized aggregate

$$\begin{aligned} X^* &= (\sqrt{x_1^*} + \sqrt{x_2^*} + \sqrt{x_3^*} + \sqrt{x_4^*} + \sqrt{x_5^*})^2 \\ &= \left(\sqrt{\tfrac{1944}{625}} + \sqrt{\tfrac{216}{121}} + \sqrt{\tfrac{24}{25}} + \sqrt{\tfrac{1176}{3025}} + \sqrt{\tfrac{24}{625}} \right)^2 \\ &= 24. \end{aligned}$$

One may now check mechanically that the claimed value for each x_i^* satisfies the first-order condition

$$\frac{\sqrt{X^*} - \sqrt{x_i^*}}{2X^* \sqrt{x_i^*}} V_i - 1 = 0.$$

This shows that we have indeed identified an equilibrium.

To understand why this special case is tractable, we aggregate the five first-order conditions into the single polynomial equation (cf. the details on Example 3 provided in the body of the paper)

$$\hat{g}(X) = 4X^5 - 1553X^3 - 15864X^2 - 50139X - 40824 = 0.$$

But $\hat{g}(X)$ fails to be irreducible. In fact, one can check that

$$\hat{g}(X) = (X - 24)\,(4X^4 + 96X^3 + 751X^2 + 2160X + 1701),$$

so that $X^* = 24$ is a solution for the generalized aggregate.

A.2 Extension of Proposition 3

Recall that $\lambda = V_2/V_1 \in (0, 1]$ denotes the ratio of the second-highest to the highest valuation. We did not find a reference for the following result.

Proposition A.1 *Suppose that $V_1 \geq \ldots \geq V_n > 0$ with $n \geq 3$. Suppose also that $R \in (1, 1 + \lambda^R]$, and that*

$$V_3 \leq V_1 \frac{\lambda^R}{(1 + \lambda^R)^{2-1/R}} \frac{R^2}{(R-1)^{1-1/R}}. \tag{A.1}$$

Then, the n-player Tullock contest admits a pure-strategy Nash equilibrium characterized by (10)-(12) for contestants $i \in \{1, 2\}$, and by $x_i^* = p_i^* = \Pi_i^* = 0$ for contestants $i \in \{3, \ldots, n\}$.

Proof. It follows from Proposition 3 that contestants 1 and 2 play a best response. To establish that none of the contestants $i \in \{3, \ldots, n\}$ have an incentive to deviate, it certainly suffices to consider contestant $i = 3$. By Cornes and Hartley (2005, Prop. 4), the zero bid is a best response for contestant 3 given efforts $x_1 = x_1^*$, $x_2 = x_2^*$, and $x_j = 0$ for any $j \geq 4$, if and only if

$$(x_1^*)^R + (x_2^*)^R \geq V_3^R \frac{(R-1)^{R-1}}{R^R}.$$

Using (10), this transforms into (A.1). □

In the constant-returns case $R = 1$, we have $(R-1)^{1-1/R} = 0^0 = 1$, so that inequality (A.1) becomes $V_3 \leq \frac{1}{2}\bar{V}_2$. Thus, this simply brings us back to the case dealt with in Proposition 2.

The equilibrium identified in Proposition A.1 need not be unique, however. To see this, it suffices to consider the case where $R = 1 + \lambda^R$. Then, inequality (A.1) reads $V_3 \leq V_2 R^{1/R}$, which is automatically fulfilled. Thus, by continuity, for R close to $1+\lambda^R$ and valuations close to identical, there are multiple pure-strategy equilibria, viz. one for each pair of active contestants.

A.3 The principal value of the Kth root

This section provides further background regarding the Kth root. It also prepares the analysis of the case $K = 3$ and $R = \frac{1}{2}$ dealt with in the next section. As discussed in the body of the paper, the Kth root $\sqrt[K]{s}$ of a complex number $s \in \mathbb{C}\backslash\{0\}$ is defined up to a unit-root factor. Thus, any $s \neq 0$ admits precisely K pre-images that differ by powers of the Kth unit root $\zeta_K = \exp(2\pi\sqrt{-1}/K)$. To resolve the resulting ambiguity, one may refer to the *principal value* of $\sqrt[K]{s}$, which is defined as follows. Given $s \neq 0$, we find unique polar coordinates $r > 0$ and $\varphi \in (-\pi, \pi]$ such that $s = r \exp(\varphi\sqrt{-1})$. Then, using de Moivre's identity,

$$\sqrt[K]{s} = \sqrt[K]{r} \exp\left(\frac{\varphi}{K}\sqrt{-1}\right)$$

is a Kth root of s, known as the principal value.

A special case of interest is a root of a complex number with positive real part.

Lemma A.1 *Let $s = \sigma + \tau\sqrt{-1}$, with $\sigma > 0$ and τ real. In this case, the principal value of the Kth root of s is given by*

$$\sqrt[K]{s} = \sqrt[2K]{\sigma^2 + \tau^2}\left(\cos(\frac{1}{K}\arctan(\frac{\tau}{\sigma})) + \sqrt{-1}\sin(\frac{1}{K}\arctan(\frac{\tau}{\sigma}))\right).$$

Proof. In the considered case, $r = \sqrt{\sigma^2 + \tau^2}$ and $\varphi = \arctan(\tau/\sigma)$. Hence, the principal value is given as

$$\sqrt[K]{s} = \sqrt[2K]{\tau^2 + \sigma^2}\exp\left(\frac{\sqrt{-1}}{K}\arctan(\frac{\tau}{\sigma})\right).$$

The claim follows now from Euler's formula $\exp(\varphi\sqrt{-1}) = \cos\varphi + \sqrt{-1}\sin\varphi$. □

A.4 The case $n = 3$ and $R = \frac{1}{2}$

It follows from the present analysis that the case $R = \frac{1}{2}$ is tractable for any $n \geq 2$, provided that valuations are taken from at most four different values. For example, the Tullock contest with $n = 5$ players, where $V_1 = V_2 > V_3 > V_4 > V_5 > 0$ and $R = \frac{1}{2}$, admits an explicit solution, because the analysis of first-order conditions leads to a polynomial equation of degree four, which can always be solved using radicals (van der Waerden, 1937, §58). Below, we derive a comparably simple solution for $n = 3$, exploiting that all roots of the minimal polynomial of X are real.[42]

[42]Using the approach outlined in Krvavica (2019), similar expressions appear feasible for $n \geq 4$, under the conditions just explained.

Proposition A.2 *Suppose that there are $n = 3$ contestants, with valuations $V_1 \geq V_2 \geq V_3 > 0$. Suppose also that $R = \frac{1}{2}$. Then, the solution of the Tullock contest is given by equations (15-17) in the body of the paper, where*

$$X^* = \sqrt{\frac{c_a}{c_g^3}} \cdot \cos\left(\frac{1}{3}\arctan\sqrt{\left(\frac{c_a}{c_g}\right)^3 - 1}\right), \tag{A.2}$$

c_a and c_g denote, respectively, the arithmetic and geometric means of the reciprocal valuations $\frac{1}{V_1}$, $\frac{1}{V_2}$, and $\frac{1}{V_3}$.

Proof. Suppose first that valuations are homogeneous, i.e., $V_1 = V_2 = V_3 \equiv V$. Then, from Proposition 1, $x_1^* = x_2^* = x_3^* = \frac{V}{9}$. Hence,

$$X^* = \left(\sqrt{x_1^*} + \sqrt{x_2^*} + \sqrt{x_3^*}\right)^2 = V.$$

But equation (A.2) delivers the same result because $c_a = c_g = \frac{1}{V}$ in that case. This proves the claim in the case of homogeneous valuations. Suppose next that not all valuations are identical. Then, $c_g < c_a$ (Hardy et al., 1934, p. 17). Under the assumptions made, equation (14) reads

$$\frac{V_1}{2X + V_1} + \frac{V_2}{2X + V_2} + \frac{V_3}{2X + V_3} = 1.$$

Multiplying through with the common denominator and collecting terms, we obtain a depressed[43] cubic equation

$$X^3 + aX + b = 0, \tag{A.3}$$

where $a = -\frac{3c_a}{4c_g^3}$ and $b = -\frac{1}{4c_g^3}$. The discriminant is

$$D = -4a^3 - 27b^2 = \frac{27}{16c_g^6}\left(\left(\frac{c_a}{c_g}\right)^3 - 1\right) > 0.$$

[43] A cubic equation is called *depressed* if there is no quadratic term.

Thus, the cubic has three real solutions, one of which is positive and two of which are negative. We are in the *casus irreducibilis*, i.e., any explicit solution by radicals requires the extraction of roots from complex numbers. The solution is $X^* = C - \frac{a}{3C}$, with a total of six possibilities for

$$C = \sqrt[3]{-\frac{b}{2} + \sqrt{\frac{b^2}{4} + \frac{a^3}{27}}} = \frac{1}{2c_g}\sqrt[3]{1 \pm \sqrt{1 - (c_a/c_g)^3}}.$$

Hence,

$$X^* = \frac{1}{2c_g}\left(\sqrt[3]{1 \pm \sqrt{1 - (c_a/c_g)^3}} + \frac{(c_a/c_g)}{\sqrt[3]{1 \pm \sqrt{1 - (c_a/c_g)^3}}}\right), \tag{A.4}$$

where the $\pm$ in front of the square roots assume the same value and the cubic roots take the same value. To select the values of the roots, one notes first that the right-hand side of equation (A.4) does not depend on the sign in front of the square root. Indeed, regardless of the choice of the cubic root, the first term in the large brackets can be easily seen to be the complex conjugate of the second term. We may therefore, without loss of generality, select the positive sign in front of the square root. Further, we know that X^* is the unique positive solution of equation (A.3). But the only way to arrive at a positive value in equation (A.4) is to select the principal value for the cubic root. It now suffices to apply Lemma A.1 to obtain the claimed formula for X^*. □

Equation (A.2) uses trigonometric functions to circumvent the extraction of roots from complex numbers. This approach goes back to Viète, who proposed it to avoid the use of complex numbers in the casus irreducibilis of Cardano's analysis (cf. Plante, 2018).

We illustrate the use of Proposition A.2 with an example.

Example A.1 *Suppose that* $(V_1, V_2, V_3) = (6, 3, 2)$. *Then,* $c_a = \frac{1}{3}(\frac{1}{V_1} + \frac{1}{V_2} + \frac{1}{V_3}) = 0.33$ *and* $c_g = 1/\sqrt[3]{V_1 V_2 V_3} = 0.30$. *Hence,* $X^* = 3.411$. *Individual efforts are, therefore,* *given by* $x_1^* = 0.75$*,* $x_2^* = 0.32$*, and* $x_3^* = 0.18$*. Winning probabilities are* $p_1^* = 0.47$*,* $p_2^* = 0.31$*, and* $p_3^* = 0.23$*. Payoffs are* $\Pi_1^* = 2.06$*,* $\Pi_2^* = 0.60$*, and* $\Pi_3^* = 0.28$*.*

For completeness, we mention that, in the case dealt with by Proposition A.2, the discriminant D is known to determine the Galois group. Specifically, if D is *not* a square of a rational number, then the Galois group is S_3. An example is $(V_1, V_2, V_3) = (3, 2, 1)$. Then, $D = 359/2^4$ is not a square. And indeed, the minimal polynomial $g(X) = X^3 - \frac{11}{4}X - \frac{3}{2}$ is irreducible with Galois group S_3. If, however, D happens to be square, then the Galois group is the cyclic group of order three, i.e., $\mathcal{C}_3$. An example is $(V_1, V_2, V_3) = (6, 3, 2)$. Then, $D = 3^6$ is a square. And indeed, the minimal polynomial $g(X) = X^3 - 9X - 9$ is irreducible with cyclic Galois group $\mathcal{C}_3$ (cf. Example A.1 above and Example 2 in the body of the paper).

A.5 Proof of Theorem 1

Fix $n \geq 5$. To provoke a contradiction, suppose that there exists an explicit formula

$$x_i^* = f_{n,R}(V_1, \ldots, V_n)$$

for the equilibrium effort of some player $i \in \{1, \ldots, n\}$, computable from the primitives $V_1, \ldots, V_n$ using basic arithmetic operations and by taking roots. From the discussion in the body of the paper, we know that

$$x_i^* = \frac{X^* V_i^2}{(2X^* + V_i)^2},$$

where X^* is the unique positive solution of

$$\frac{V_1}{2X + V_1} + \ldots + \frac{V_n}{2X + V_n} - 1 = 0.$$

Rewriting yields

$$\frac{\left\{\sum_{i=1}^{n} V_i \prod_{j\neq i}(2X+V_j)\right\} - \prod_{i=1}^{n}(2X+V_i)}{\prod_{i=1}^{n}(2X+V_i)} = 0. \tag{A.5}$$

Recall that the system of elementary symmetric polynomials in n variables satisfies the recursive relationship

$$\sigma_k(V_1,\ldots,V_n) = \sigma_k(V_1,\ldots,V_{n-1}) + V_n\sigma_{k-1}(V_1,\ldots,V_{n-1}),$$

for $k \in \{1,\ldots,n\}$. Using this relationship, straightforward induction arguments show that

$$\begin{aligned}\prod_{i=1}^{n}(2X+V_i) &= \sum\nolimits_{k=0}^{n}\sigma_k(V_1,\ldots,V_n)(2X)^{n-k},\\ \sum_{i=1}^{n} V_i\prod_{j\neq i}(2X+V_j) &= \sum\nolimits_{k=0}^{n} k\sigma_k(V_1,\ldots,V_n)(2X)^{n-k}.\end{aligned}$$

Up to a negative sign, the numerator in (A.5) is, therefore, given by

$$g_n(X;V_1,\ldots,V_n) = \sum\nolimits_{k=0}^{n}(1-k)\sigma_k(V_1,\ldots,V_n)(2X)^{n-k}.$$

The following lemma is commonly used to compute Galois groups modulo prime numbers, but it can be used also in our setting.

Lemma A.2 (Specialization) *Let $\mathfrak{R}$ be a unique factorization domain and let $\mathfrak{P}$ be a prime ideal of $\mathfrak{R}$. If $g(X)$ is a polynomial with coefficients in $\mathfrak{R}$, and the image $\bar{g}(X)$ of $g(X)$ under the canonical epimorphism $\mathfrak{R} \to \bar{\mathfrak{R}} = \mathfrak{R}/\mathfrak{P}$ has no multiple roots, then the Galois group of $\bar{g}(X)$ is a subgroup of the Galois group of $g(X)$.*

Proof. See van der Waerden (1937, §61). □

The next lemma completes the proof of Theorem 1.

Lemma A.3 *The following statements are true:*

(i) $g_n(X; V_1, \ldots, V_n)$ *does not have multiple roots; moreover,* $g_n(0; V_1, \ldots, V_n) \neq 0$*;*

(ii) $g_n(X; V_1, \ldots, V_{n-1}, 0) = 2X \cdot g_{n-1}(X; V_1, \ldots, V_{n-1})$*;*

(iii) the Galois group of $g_{n-1}(X; V_1, \ldots, V_{n-1})$ *over* $\mathbb{Q}(V_1, \ldots, V_{n-1})$ *is a subgroup of the Galois group of* $g_n(X; V_1, \ldots, V_n)$ *over* $\mathbb{Q}(V_1, \ldots, V_n)$*;*

(iv) $g_5(X; V_1, V_2, V_3, V_4, V_5)$ *has the Galois group* S_5 *over* $\mathbb{Q}(V_1, V_2, V_3, V_4, V_5)$*;*

(v) the Galois group of $g_n(X; V_1, \ldots, V_n)$ *over* $\mathbb{Q}(V_1, \ldots, V_n)$ *contains* S_5 *as a subgroup;*

(vi) $g_n(X; V_1, \ldots, V_n)$ *is irreducible over* $\mathbb{Q}(V_1, \ldots, V_n)$*.*

Proof. (i) This was shown in the body of the paper. (ii) By the recursive definition of the elementary symmetric polynomials,

$$\sigma_k(V_1, \ldots, V_{n-1}, 0) = \begin{cases} \sigma_k(V_1, \ldots, V_{n-1}) & \text{if } k < n \\ 0 & \text{if } k = n. \end{cases}$$

Hence,

$$\begin{aligned} g_n(X; V_1, \ldots, V_{n-1}, 0) &= \sum_{k=0}^{n} (1-k)\sigma_k(V_1, \ldots, V_{n-1}, 0)(2X)^{n-k} \\ &= \sum_{k=0}^{n-1} (1-k)\sigma_k(V_1, \ldots, V_{n-1})(2X)^{n-k} \\ &= 2X \cdot \sum_{k=0}^{n-1} (1-k)\sigma_k(V_1, \ldots, V_{n-1})(2X)^{n-1-k} \\ &= 2X \cdot g_{n-1}(X; V_1, \ldots, V_{n-1}), \end{aligned}$$

as has been claimed. (iii) Consider the integral domain $\mathfrak{R}_n = \mathbb{Q}[V_1, \ldots, V_n]$, i.e., the ring of polynomials in the variables $V_1, \ldots, V_n$ with rational coefficients. In $\mathfrak{R}_n$, we have the prime ideal $\mathfrak{P}_n = \langle V_n \rangle$ generated by the polynomial V_n. There is an isomorphism

$$\bar{\mathfrak{R}}_n = \mathfrak{R}_n/\mathfrak{P}_n \simeq \mathfrak{R}_{n-1}.$$

Moreover, the image of $g_n(X; V_1, \ldots, V_n)$ under the canonical epimorphism $\mathfrak{R}_n \to \bar{\mathfrak{R}}_n$ is

$$\bar{g}_n(X; V_1, \ldots, V_n) = g_n(X; V_1, \ldots, V_{n-1}, 0) = 2X \cdot g_{n-1}(X; V_1, \ldots, V_{n-1}).$$

Since $2X$ and $g_{n-1}(X)$ share no root by part (i), $\bar{g}_n(X)$ has no multiple zeros. By the specialization lemma (Lemma A.2), the Galois group of $g_{n-1}(X; V_1, \ldots, V_{n-1})$ is indeed a subgroup of the Galois group of $g_n(X; V_1, \ldots, V_n)$. (iv) We have seen above that $g_5(X)$ has the Galois group S_5 over $\mathbb{Q}$. By another application of the Lemma A.2, this implies that S_5 is a subgroup of the Galois group of $g_5(X; V_1, V_2, V_3, V_4, V_5)$ over $\mathbb{Q}(V_1, V_2, V_3, V_4, V_5)$. Given that $g_5(X; V_1, V_2, V_3, V_4, V_5)$ is of degree five in X, this implies the claim. (v) The claim follows via induction from the previous two parts. (vi) As explained in the body of the paper, it suffices to show that $g_n(X)$, considered as a polynomial in $Z = 2X$ over $\mathbb{Z}[V_1, \ldots, V_n]$ does not admit a linear factor for $n \geq 2$. The proof is by contradiction. Suppose that there is some $a \in \mathbb{Z}[V_1, \ldots, V_n]$ such that $(Z - a) \mid g_n(Z)$.[44] Then, a is a root of $g_n(Z)$, i.e.,

$$\begin{aligned} 0 &= \sum\nolimits_{k=0}^{n} (1-k)\sigma_k a^{n-k} \\ &= (1-n)\sigma_n + a \sum\nolimits_{k=0}^{n-1} (1-k)\sigma_k a^{n-k-1}. \end{aligned}$$

Hence, $a \mid (n-1)\sigma_n$. Suppose first that $a \in \mathbb{Z}$. Then, since $\sigma_0, \ldots, \sigma_n$ are linearly independent over $\mathbb{Z}$, we obtain $0 = 1 - n$, a contradiction. Suppose next that $a \notin \mathbb{Z}$. Then, from $a \mid (n-1)\sigma_n$, we have $V_i \mid a$ for some $i \in \{1, \ldots, n\}$. Moreover, $V_i^2 \nmid a$.

[44] As usual, the vertical bar $\mid$ refers to divisibility within the polynomial ring.

Therefore, $V_i^n \mid a^n$, but $V_i^n \nmid \sigma_k a^{n-k}$, for any $k \in \{2, \ldots, n\}$. Thus, a is not a root of $g_n(Z)$, in conflict with what has been assumed. □

It follows from the above that the equilibrium efforts of any player cannot be expressed from the valuation vector using basic arithmetic operations and by extracting roots. The derivation for the winning probability and equilibrium payoff of any individual contestant is entirely analogous and, therefore, omitted.

A.6 Proof of Corollary 2

We check the assumptions of Cohen (1981, Thm. 2.1). In our application, the field extension is trivial over the number field $\mathbb{Q}$. Let $f(Z, V_1, \ldots, V_n) \equiv g_n(X; V_1, \ldots, V_n)$, be specified by (19) and $Z = 2X$. When considered as a polynomial in the $(n+1)$ indeterminates $Z, V_1, \ldots, V_n$, f is non-zero, of *total* degree n (because σ_k is of degree k), and possesses integer coefficients. As seen in the proof of Theorem 1, the Galois group $\mathcal{G}$ of g_n over $\mathbb{Q}(V_1, \ldots, V_n)$ acts transitively on its n roots (from irreducibility, see van der Waerden (1937, p. 162)) and contains S_5 as a subgroup. The term of f with the largest coefficient in absolute value is $(1-n)\sigma_n(V_1, \ldots, V_n)$. Let $|f| = \max\{8, n-1\}$. Then, by Cohen's theorem, there exists some $c \equiv c(n)$, such that provided $M > |f|^c$, the number of $(V_1, \ldots, V_n) \in \{-M, \ldots, M\}^n$ for which $\mathcal{G}(V_1, \ldots, V_n)$, the Galois group of the specialized polynomial $g_n(X; V_1, \ldots, V_n)$ over $\mathbb{Q}$, differs from $\mathcal{G}$ does not exceed $|f|^{c/3} M^{n-\frac{1}{2}} \ln M$. One notes that $|f|^{c/3} M^{n-\frac{1}{2}} \ln M = o(M^n)$, where we consider the limit $M \to \infty$. Moreover, the number of economically meaningful valuation vectors $(V_1, \ldots, V_n) \in \{1, \ldots, M\}^n$ satisfying $V_1 \geq \ldots \geq V_n$ exceeds $\frac{M^n}{n!}$. Let now $\varepsilon > 0$, and $\bar{V} \in \mathbb{Q}$ with $\bar{V} > 0$ be given. By the above, there exists M_0 such that for any $M \geq M_0$, the number of $(V_1, \ldots, V_n) \in \{1, \ldots, M\}^n$ for which $\mathcal{G}(V_1, \ldots, V_n) \neq \mathcal{G}$ does not exceed

εM^n. Let $\delta_M = \bar{V}/M > 0$. Since f is homogeneous of degree n,

$$g_n(X\delta_M; V_1\delta_M, \ldots, V_n\delta_M) = \delta_M^n g_n(X; V_1, \ldots, V_n).$$

Therefore, the Galois group of $g_n(X; V_1\delta_M, \ldots, V_n\delta_M)$ over $\mathbb{Q}$, including its operation on the set of roots, is isomorphic to $\mathcal{G}(V_1, \ldots, V_n)$. This completes the proof of the corollary.

A.7 Proof of Proposition 4

Rearranging player i's first-order condition yields

$$V_i \;=\; \frac{q}{p}\,\frac{\xi_i^{q-p} S^2}{S - \xi_i^p} \tag{A.6}$$

where $\xi_i = x_i^{1/q}$ and $S = \xi_1^p + \cdots + \xi_n^p$. Consider the map $\Phi : (\xi_1, \ldots, \xi_n) \mapsto (V_1, \ldots, V_n)$ defined component-wise by the right-hand side of (A.6). Its Jacobian $J_\Phi(\xi_1, \ldots, \xi_n) = (\partial V_i/\partial \xi_j)_{i,j=1}^n$ is regular at $\xi_1 = \cdots = \xi_n = 1$.[45] Clearing denominators, (A.6) becomes a system of equations in the unknowns $\xi_1, \ldots, \xi_n$ with coefficients

[45] Indeed, a calculation shows that

$$\frac{\partial V_i}{\partial \xi_j}(1, \ldots, 1) = \begin{cases} D & \text{if } i = j, \\ B & \text{if } i \neq j, \end{cases}$$

with

$$D \;=\; \frac{q\,n\big((q-p)n + 2p\big)}{p(n-1)}, \qquad B \;=\; \frac{q\,n(n-2)}{(n-1)^2}.$$

Thus $J_\Phi(1, \ldots, 1)$ has constant diagonal D and constant off-diagonal B, so

$$\det J_\Phi(1, \ldots, 1) = (D - B)^{n-1}\big(D + (n-1)B\big).$$

Substituting D and B and simplifying gives

$$\det J_\Phi(1, \ldots, 1) = \frac{q^{n+1} n^{2n}\big((q-p)(n-1) + p\big)^{n-1}}{p^n (n-1)^{2n-1}} \neq 0$$

for all integers $n \geq 2$ and $0 < p < q$.

in $\mathbb{Q}(V_1, \ldots, V_n)$. For generic $(V_1, \ldots, V_n)$, this polynomial system has only finitely many solutions $(\xi_1, \ldots, \xi_n)$. Equivalently, each ξ_i is algebraic over $\mathbb{Q}(V_1, \ldots, V_n)$, and hence, $X = S^{q/p}$, is algebraic over $\mathbb{Q}(V_1, \ldots, V_n)$. Finally,

$$T^n - \sigma_1 T^{n-1} + \cdots + (-1)^n \sigma_n \in \mathbb{Q}(\sigma_1, \ldots, \sigma_n)[T]$$

has $V_1, \ldots, V_n$ as roots, so each V_i is algebraic over $\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$. Hence $\mathbb{Q}(V_1, \ldots, V_n)$ is an algebraic extension of $\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$. Thus X is algebraic over $\mathbb{Q}(\sigma_1, \ldots, \sigma_n)$: there exists a nonzero polynomial $h(T) \in \mathbb{Q}(\sigma_1, \ldots, \sigma_n)[T]$ such that $h(X) = 0$. Multiplying by a common denominator yields a nonzero polynomial $g(T) \in \mathbb{Z}[\sigma_1, \ldots, \sigma_n][T]$ with $g(X) = 0$. This completes the proof of the proposition.

A.8 Computer-assisted parts of the proofs

In the analysis of Example 3, we used *Sage*, which is a web application freely accessible at sagecell.sagemath.org. The following code checks that $g(X)$, defined in equation (18), is irreducible over $\mathbb{Q}$.

```
R.<X>=PolynomialRing(QQ)
(8*X^5-170*X^3-450*X^2-411*X-120).is_irreducible()
True
```

The final line is the output returned by Sage. Similarly, the code below computes the Galois group of $g_5(X)$, where again, the final line is the output.

```
R.<X> = PolynomialRing(QQ)
g(X) = 8*X^5-170*X^3-450*X^2-411*X-120
```

```
K.<a> = NumberField(g(X))
K.galois_group()
Galois group 5T5 (S5) with order 120
```

To replicate these derivations, it suffices to copy either of the two code snippets to the *Sage* prompt, delete the output as well as any leading spaces, and click "evaluate."

References

Alcalde, José and Matthias Dahm (2010) "Rent seeking and rent dissipation: A neutrality result," *Journal of Public Economics*, 94 (1), 1–7, 10.1016/j.jpubeco.2009.11.005. 7, 17

Baye, Michael R., Dan Kovenock, and Casper G. de Vries (1994) "The solution to the Tullock rent-seeking game when $R > 2$: Mixed-strategy equilibria and mean dissipation rates," *Public Choice*, 81 (3), 363–380, 10.1007/BF01053238. 7, 17

——— (1996) "The all-pay auction with complete information," *Economic Theory*, 8 (2), 291–305, 10.1007/BF01211819. 3

Blume, Lawrence E. and William R. Zame (1994) "The algebraic geometry of perfect and sequential equilibrium," *Econometrica*, 62 (4), 783–794, 10.2307/2951732. 7

Chatterji, Samaresh and Ratnik Gandhi (2011) "Computing equilibria with group actions," *ACM Communications in Computer Algebra*, 45 (1/2), 115–116, 10.1145/2016567.2016583. 8

Cohen, S. D. (1981) "The distribution of Galois groups and Hilbert's Irreducibility

Theorem," *Proceedings of the London Mathematical Society, 3rd Series*, 43 (2), 227–250, 10.1112/plms/s3-43.2.227. 23, 40

Corchón, Luis C. (1994) "Comparative statics for aggregative games: The strong concavity case," *Mathematical Social Sciences*, 28 (3), 151–165, 10.1016/0165-4896(94)90001-9. 3

Cornes, Richard and Roger Hartley (2005) "Asymmetric contests with general technologies," *Economic Theory*, 26 (4), 923–946, 10.1007/s00199-004-0566-5. 7, 15, 32

Datta, Ruchira S. (2003) "Universality of Nash equilibria," *Mathematics of Operations Research*, 28 (3), 424–432, 10.1287/moor.28.3.424.16397. 7

Dresher, M., S. Karlin, and L. S. Shapley (1949) "Polynomial Games," in *Contributions to the Theory of Games*, 161–180: Princeton University Press, 10.1515/9781400881727-015. 7

Dummit, D. S. (1991) "Solving solvable quintics," *Mathematics of Computation*, 57 (195), 387–401, 10.1090/S0025-5718-1991-1079014-X. 5

Edwards, Harold M. (1984) *Galois Theory*, New York: Springer, `http://drhuang.com/science/mathematics/book/`. 4, 10

Ewerhart, Christian (2015) "Mixed equilibria in Tullock contests," *Economic Theory*, 60 (1), 59–71, 10.1007/s00199-014-0835-x. 7, 17

——— (2017a) "Contests with small noise and the robustness of the all-pay auction," *Games and Economic Behavior*, 105, 195–211, 10.1016/j.geb.2017.07.003. 7, 17

——— (2017b) "Revenue ranking of optimally biased contests: The case of two players," *Economics Letters*, 157, 167–170, 10.1016/j.econlet.2017.05.012. 7, 17

——— (2025a) "On asymmetric equilibria in rent-seeking contests with strictly increasing returns," *Economic Theory Bulletin*, 10.1007/s40505-025-00301-4. 7, 14, 15

——— (2025b) "On the uniqueness of the mixed equilibrium in the Tullock contest," *Economics Letters*, 247, 112166, 10.1016/j.econlet.2025.112166. 7, 17

Feng, Xin and Jingfeng Lu (2017) "Uniqueness of equilibrium in two-player asymmetric Tullock contests with intermediate discriminatory power," *Economics Letters*, 159, 61–64, 10.1016/j.econlet.2017.07.017. 7, 17

Gandhi, Ratnik (2011) *Algebraic Approach to Nash Equilibria for Finite Normal Form Games* Ph.D. Thesis, Dhirubhai Ambani Institute of Information and Communication Technology, `http://drsr.daiict.ac.in//handle/123456789/314`. 8

Gandhi, Ratnik and Samaresh Chatterji (2015) "Applications of algebra for some game theoretic problems," *International Journal of Foundations of Computer Science*, 26 (01), 51–78, 10.1142/s0129054115500033. 8

Gibbens, Richard J and Frank P Kelly (1999) "Resource pricing and the evolution of congestion control," *Automatica*, 35 (12), 1969–1985. 16

Hardy, G.H., J.E. Littlewood, and G. Polya (1934) *Inequalities*: Cambridge University Press, `http://archive.org/details/in.ernet.dli.2015.278938`. 34

Hillman, Arye L. and John G. Riley (1989) "Politically contestable rents and transfers," *Economics & Politics*, 1 (1), 17–39, 10.1111/j.1468-0343.1989.tb00003.x. 7, 16

Judd, Kenneth L., Philipp Renner, and Karl Schmedders (2012) "Finding all pure-strategy equilibria in games with continuous strategies," *Quantitative Economics*, 3 (2), 289–331, 10.3982/QE165. 30

Kang, Ming-chang (2000) "Cubic fields and radical extensions," *American Mathematical Monthly*, 107 (3), 254–256, 10.1080/00029890.2000.12005188. 13

Kobayashi, Sigeru and Hiroshi Nakagawa (1992) "Resolution of solvable quintic equation," *Mathematica Japonica*, 37, 883–886, https://cir.nii.ac.jp/crid/1571698599899117952. 5

Konrad, Kai A. (2009) *Strategy and Dynamics in Contests*, London School of Economics Perspectives in Economic Analysis, Oxford, New York: Oxford University Press, https://doi.org/10.1093/oso/9780199549597.001.0001. 2

Krvavica, Nino (2019) "Explicit expressions for real roots of a quartic equation," *arXiv preprint arXiv:1902.08807*. 33

Kübler, Felix, Philipp Renner, and Karl Schmedders (2014) "Computing All Solutions to Polynomial Equations in Economics," in Schmedders, Karl and Kenneth L. Judd eds. *Handbook of Computational Economics*, 3, 599–652: Elsevier, 10.1016/B978-0-444-52980-0.00011-6. 3, 5

Kübler, Felix and Karl Schmedders (2010a) "Tackling multiplicity of equilibria with Gröbner bases," *Operations Research*, 58 (4-part-2), 1037–1050, 10.1287/opre.1100.0819. 3, 7

——— (2010b) "Competitive equilibria in semi-algebraic economies," *Journal of Economic Theory*, 145 (1), 301–330, 10.1016/j.jet.2009.10.004. 7

Matros, Alexander (2006) "Rent-seeking with asymmetric valuations: Addition or deletion of a player," *Public Choice*, 129 (3), 369–380, 10.1007/s11127-006-9037-9. 16

McKelvey, Richard D. and Andrew McLennan (1997) "The maximal number of regular totally mixed Nash equilibria," *Journal of Economic Theory*, 72 (2), 411–425, 10.1006/jeth.1996.2214. 8

Nash, John F. and Lloyd S. Shapley (1950) "A simple three-person poker game," in *Contributions to the Theory of Games (Annals of Mathematics Study No. 24), Volume I*, 105–116: Princeton University Press, 10.1515/9781400881727-011. 7

Nau, Robert, Sabrina Gomez Canovas, and Pierre Hansen (2004) "On the geometry of Nash equilibria and correlated equilibria," *International Journal of Game Theory*, 32 (4), 443–453, 10.1007/s001820300162. 7

Nie, Jiawang and Xindong Tang (2023) "Convex generalized Nash equilibrium problems and polynomial optimization," *Mathematical Programming*, 198 (2), 1485–1518, 10.1007/s10107-021-01739-7. 7

——— (2024) "Nash equilibrium problems of polynomials," *Mathematics of Operations Research*, 49 (2), 1065–1090, 10.1287/moor.2022.0334. 7

Nti, Kofi O. (1999) "Rent-seeking with asymmetric valuations," *Public Choice*, 98 (3), 415–430, 10.1023/A:1018391504741. 7, 17

Plante, Joseph (2018) "Cubic equations from an analytic point of view," *American Mathematical Monthly*, 125 (9), 845–849, 10.1080/00029890.2018.1507207. 35

Pérez-Castrillo, J. David and Thierry Verdier (1992) "A general analysis of rent-seeking games," *Public Choice*, 73 (3), 335–350, 10.1007/BF00140926. 7, 14, 15

Rosen, Michael I. (1995) "Niels Hendrik Abel and equations of the fifth degree," *American Mathematical Monthly*, 102, 495–505, 10.2307/2974763. 5

Ryvkin, Dmitry (2007) "Tullock contests of weakly heterogeneous players," *Public Choice*, 132 (1), 49–64, 10.1007/s11127-006-9133-x. 3, 7, 15

——— (2013) "Heterogeneity of players and aggregate effort in contests," *Journal of Economics & Management Strategy*, 22, 728–743, https://onlinelibrary.wiley.com/doi/full/10.1111/jems.12028. 7

Spearman, Blair K. and Kenneth S. Williams (1994) "Characterization of solvable quintics $x^5 + ax + b$," *American Mathematical Monthly*, 101 (10), 986–992, 10.2307/2975165. 5

Stein, William E. (2002) "Asymmetric rent-seeking with more than two contestants," *Public Choice*, 113 (3), 325–336, 10.1023/A:1020877410243. 7, 16

von Stengel, Bernhard and Françoise Forges (2008) "Extensive-form correlated equilibrium: Definition and computational complexity," *Mathematics of Operations Research*, 33 (4), 1002–1022, 10.1287/moor.1080.0340. 8

Stewart, Ian (2015) *Galois Theory*, New York: Chapman and Hall/CRC, 5th edition, 10.1201/9781003213949. 10, 13, 22, 24

Szidarovszky, Ferenc and Koji Okuguchi (1997) "On the existence and uniqueness of pure Nash equilibrium in rent-seeking games," *Games and Economic Behavior*, 18 (1), 135–140, 10.1006/game.1997.0517. 18, 20

Tullock, G. (1980) *Efficient Rent-Seeking*, College Station: Texas A&M Press, https://cir.nii.ac.jp/crid/1130282271486470912. 2, 6

Umemura, Hiroshi (2007) "Resolution of algebraic equations by theta constants," in Mumford, David ed. *Tata Lectures on Theta II*, 261–270, Boston, MA: Birkhäuser, 10.1007/978-0-8176-4578-6_18. 26

van der Waerden, B. L. (1937) *Moderne Algebra*, Berlin: Springer, 2nd edition, in German. 4, 9, 13, 24, 33, 37, 40

Wang, X. (2010) "Semi-mixed Equilibrium in Tullock Contests," *Journal of Public Economics*, 94 (1), 1–7, 10.1016/j.jpubeco.2009.10.005. 7, 17

Wolfram Research (2005) "Solving the Quintic with Mathematica – from Wolfram Library Archive," https://library.wolfram.com/infocenter/TechNotes/158/. 26