HAL open science

Cake cutting: Explicit examples for impossibility results

Guillaume Chèze

▶ To cite this version:

Guillaume Chèze. Cake cutting: Explicit examples for impossibility results. Mathematical Social Sciences, 2019, 102, pp.68-72. hal-01953971v2

HAL Id: hal-01953971
https://hal.science/hal-01953971v2

Submitted on 28 Jun 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

CAKE CUTTING: EXPLICIT EXAMPLES FOR IMPOSSIBILITY RESULTS

GUILLAUME CHÈZE

Abstract. In this article we suggest a model of computation for the cake cutting problem. In this model the mediator can ask the same queries as in the Robertson-Webb model but he or she can only perform algebraic operations as in the Blum-Shub-Smale model. All existing algorithms described in the Robertson-Webb model can be described in this new model.
We show that in this model there exist explicit couples of measures for which no algorithm outputs an equitable fair division with connected parts.
We also show that there exist explicit set of measures for which no algorithm in this model outputs a fair division which maximizes the utilitarian social welfare function.
The main tool of our approach is Galois theory.

Introduction

In 1837, Pierre Wantzel has shown that there exists no general construction using only compass and straightedge which divides an angle into three equal angles. The proof relies on algebra and field theory. The angle trisection problem can be seen as a fair division problem: we have a portion of pizza and we want to divide it in a fair way between three friends (by using only compass and straightedge constructions...). Wantzel's theorem says that this problem has no solution.

In this article, we are going to study a similar fair division problem and we are going to use similar tools.

In the following, we consider an heterogeneous good, for example: a cake, land, time or computer memory, represented by the interval $X = [0, 1]$ and n players with different points of view. We associate to each player a non-atomic probability measure μ_i on the interval $X = [0; 1]$. These measures represent the utility functions of the player. This means that if $[a, b] \subset X$ is a part of the cake then $\mu_i([a, b])$ is the value associated by the i-th player to this part of the cake. As μ_i are probability measures, we have $\mu_i(X) = 1$ for all i.
A division of X is a partition $X = \sqcup_i X_i$ where X_i is the part given to the i-th player. A division is *simple* when each X_i is an interval.

Several notions of fair division exists.
We say that a division is *proportional* when $\mu_i(X_i) \geq 1/n$.

Guillaume Chèze: Institut de Mathématiques de Toulouse, UMR 5219, Université de Toulouse ; CNRS, UPS IMT, F-31062 Toulouse Cedex 9, France
E-mail address: guillaume.cheze@math.univ-toulouse.fr.
Date: June 28, 2019.

We say that a division is *envy-free* when for $i \neq j$, we have $\mu_i(X_i) \geq \mu_i(X_j)$.
We say that a division is *equitable* when for all $i \neq j$, we have $\mu_i(X_i) = \mu_j(X_j)$.

We say that the division $X = \sqcup_i X_i$ *maximizes the utilitarian social welfare function* when

$$\sum_{i=1}^{n} \mu_i(X_i) \geq \sum_{i=1}^{n} \mu_i(Y_i),$$

for all partition $X = \sqcup_i Y_i$.

The problem of fair division (theoretical existence of fair division and construction of algorithms) has been studied in several papers [Ste48, DS61, EP84, EP11, BT95, RW97, Pik00, Tho06, Pro13, BJK13, AM16], and books about this topic, see e.g. [RW98, BT96, Pro16, Bar05]. These results appear in the mathematics, economics, political science, artificial intelligence and computer science literature. Recently, the cake cutting problem has been studied intensively by computer scientists for solving resource allocation problems in multi agents systems, see e.g. [CDE$^+$06, CLPP13, KPS13, BM15].

A practical problem is the computation of fair divisions. In order to describe algorithms we thus need a model of computation. There exist two main classes of cake cutting algorithms: discrete and continuous protocols (also called moving knife methods). Here, we study only discrete algorithms. These kinds of algorithms can be described thanks to the classical model introduced by Robertson and Webb and formalized by Woeginger and Sgall in [WS07]. In this model we suppose that a mediator interacts with the agents. The mediator asks two type of queries: either cutting a piece with a given value, or evaluating a given piece. More precisely, the two type of queries allowed are:

(1) $eval_i(x, y)$: Ask agent i to evaluate the interval $[x, y]$. This means compute $\mu_i([x, y])$.
(2) $cut_i(x, a)$: Asks agent i to cut a piece of cake $[x, y]$ such that $\mu_i([x, y]) = a$. This means: for given x and a, solve $\mu_i([x, y]) = a$.

In the Robertson-Webb model the mediator can adapt the queries from the previous answers given by the players. In this model, the complexity counts the finite number of queries necessary to get a fair division. For a rigorous description of this model we can consult: [WS07, BN17].

The result of a query is a real number and thus the mediator has to manipulate real numbers. There exist two possible models of computation which allows this task.
First, we can consider computable real numbers. Roughly speaking a real number is said to be computable if there exists a Turing machine which writes digit by digit the (infinite) decimal expansion of this number. Unfortunately, this model of computation is not natural in our setting because we cannot decide in this model if a computable number is equal to 0. This means that we cannot decide if two computable numbers are equal. Thus, with this model, the mediator cannot check if a fair division is equitable.

Second, we can consider the BSS model of computation. This model has been developed by Blum, Shub and Smale (BSS). It allows to study algorithms over a ring. Roughly speaking a BSS machine has registers which can hold arbitrary elements of the studied ring (here $\mathbb{R}$), and perform exact arithmetic $(+, -, \times, \div)$ and can branch on conditions based on exact comparisons $(=, <, >, \leq, \geq)$. Furthermore, with this theory when the ring is $\mathbb{Z}/2\mathbb{Z}$ then we recover the classical theory of Turing machine. For a detailed description of this model see [BSS89, BCSS98].

In this article we are going to suppose that the mediator use a BSS machine. We call this new model of computation the BSSRW model (Blum-Shub-Smale-Robertson-Webb model) and we are going to prove impossibilty results.

In the fair division literature some impossibility results have been already given. Stromquist in [Str08] has proved that there exists no algorithm giving a simple and envy-free fair division for $n \geq 3$ players. When $n = 2$, the classical "Cut and Choose" algorithm gives a simple and envy-free fair division.
Cechlárová et al. have shown, in [CP12], that there exists no algorithm computing a simple and equitable fair division for $n \geq 3$ players in the Roberston-Webb model.

The strategy used in these articles is the following: they suppose that an algorithm computing the desired division exists and then by an iteration process they construct from this algorithm a set of measures giving a contradiction. Thus they obtain a result of this kind: for all algorithms in the Roberston-Webb model there exists a set of measures for which the desired fair division cannot be given.
It must be noticed that this approach gives for each algorithm a set of measures leading to a contradiction. Thus the set of measures is related to the algorithm. Moreover, the measures are not explicitly given. Therefore, we can imagine that these sets of measure correspond to very complicated situations not appearing in practice and that for "reasonable" sets of measures the contradiction does not occur.

Procaccia and Wang have also given an impossibility result for equitable fair division in [PW17]. As a corollary of a theorem about a lower bound for equitable division they deduce that there exists no algorithm giving an equitable fair division. However, with this approach we still cannot give an explicit example of measures such that no algorithm in the Robertson-Webb model returns an equitable division with this input.

In the first part of this article, we are going to study simple equitable fair divisions. This topic has been less studied than proportional and envy-free divisions. However, there exist some results showing the existence of such fair divisions [CDP13, SHS18, Chè17]. Furthermore, if we consider a continous protocol, it is possible to get an equitable fair division (not necessarily simple) thanks to Austin's moving knife procedure, see [Aus82].
Here, we are going to give explicit examples where two players cannot get an equitable fair division with connected parts if we use our suggested model of computation.

Theorem 1. *In the BSSRW model of computation no algorithm returns a simple and equitable division when the measures* (μ_1, μ_2) *are given by*

$$\mu_1\big([0,x]\big) = x, \quad \mu_2\big([0,x]\big) = x^5.$$

The strategy used to prove this theorem is the following: We are going to show that if there exists an equitable and simple division $X = [0,t] \sqcup [t,1]$ then the final cutpoint t must satisfy a polynomial equation. Then, with elementary field theory, we can show that t cannot be computed with the BSSRW model.

Now, if we use Abel's impossibility theorem and Galois' theory showing that some polynomials are not solved by radicals, then we obtain other examples as stated in the next theorem:

Theorem 2. *In the BSSRW model of computation there exist measures* (μ_1, μ_2) *such that no algorithm returns a simple and equitable division for these measures. Furthermore, we can take* (μ_1, μ_2) *in the following way:*

$$\mu_1\big([0,x]\big) = x, \quad \mu_2\big([0,x]\big) = x^d$$

where

- $d \geq 5$ *is even,*
- *or* $d \geq 5$ *is odd with* $d \not\equiv 2\,[3]$*,*
- *or* $d \geq 5$ *is prime and* $d \equiv 2\,[3]$*.*

Thus, when we have two players, we can give *easy and explicit* couples of measures for which no algorithm in the BSSRW model gives a simple and equitable fair division.

In a second part, we show that in the BSSRW model we cannot obtain a fair division which maximizes the utilitarian social welfare function. In this last situation, we will consider n players and we will not suppose the division $X = \sqcup_i X_i$ to be simple.

Theorem 3. *In the BSSRW model of computation there exists measures* $\mu_1, \mu_2, \ldots, \mu_n$ *such that no algorithm returns a division which maximizes the utilitarian social welfare function.*
Furthermore, we can take $\mu_1, \mu_2, \ldots, \mu_n$ *in the following way:*

$$\mu_1([0,x]) = \cdots = \mu_{n-1}([0,x]) = x, \quad \mu_n([0,x]) = x^p$$

where $p \geq 3$ *is a prime number.*

Now, in order to state our results, we introduce our model of computation.

1. The BSSRW model

In the Robertson-Webb model of computation the computational power of the mediator is not specified. It is not mentioned what kind of computations the mediator can perform with the results of the queries. Furthermore, the number of elementary operations done by the mediator (equality and inequality tests and arithmetic operations $+, -, \times, \div$) is not taken into account in the complexity. This point has been discussed in [Chè18].
Here, we suppose as in the classical model that the mediator can use the cut_i and

$eval_i$ queries. However, we also suppose that the mediator can *only* perform equality and inequality tests and the usual algebraic operations: $+, -, \times, \div$ on the results of queries. We also suppose that the mediator can use freely the rational numbers. This means that the mediator uses a Blum-Shub-Smale machine.

These assumptions are not restrictive. Indeed, no known algorithm uses the computation of a logarithm or of an exponential by the mediator or more generally the computation of a transcendental function.
Furthermore, when the mediator needs a constant during the algorithm this constant is always a rational number. Indeed, in practice the mediator never asks a query of the form $cut_i(0, \frac{e}{4}\mu_i(X))$, where $e = 2,718\ldots$ is Napier's constant. Queries have the form $cut_i\big(0, \frac{\mu_i(X)}{n}\big)$ or $cut_i\big(0, \frac{p}{q}\mu_i(X)\big)$, where p, q, n are integers.

Therefore, if we suppose that the answer to the first three queries are denoted by $\alpha_1, \alpha_2, \alpha_3$, then in this new model, the fourth query is of the form $cut_i(\beta_1, \beta_2)$ or $eval_i(\beta_1, \beta_1)$ where $\beta_1, \beta_2 \in \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$. This means that β_1 and β_2 are rational expressions in terms of $\alpha_1, \alpha_2, \alpha_3$.

The algebraic assumption is not restrictive and to author's knowledge all algorithms written in the classical Robertson-Webb model can be written in this Blum-Shub-Smale-Robertson-Webb model (BSSRW model). However, these precisions are important for our study. Indeed, if the algorithm uses k queries with answers $\alpha_1, \ldots, \alpha_k$ for computing a fair division, then the cutpoints used in the output of the algorithm must belong to $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_k)$. This gives an algebraic condition for the final cutpoints. Using this algebraic condition, we can prove our impossibility theorems.

Notations and elementary results. For given measures $\mu_1, \mu_2, \ldots, \mu_n$ we denote by f_i, $i = 1, \ldots, n$ the function

$$f_i(x) = \mu_i\big([0, x]\big).$$

Let α_j be the result of the j-th query, then we set

$$\mathbb{K}_j = \mathbb{Q}(\alpha_1, \ldots, \alpha_j).$$

We thus have $\mathbb{K}_j = \mathbb{K}_{j-1}(\alpha_j)$ and $\mathbb{K}_0 = \mathbb{Q}$.

We recall that when a field $\mathbb{F}$ is a subfield of a field $\mathbb{K}$ then we say that we have a field extension and this is denoted by $\mathbb{K}/\mathbb{F}$. Furthermore, the dimension of $\mathbb{K}$ seen as a $\mathbb{F}$-vector space is called the degree of the extension and is denoted by $[\mathbb{K} : \mathbb{F}]$. When the degree is finite we say that the extension is finite. Moreover, when we have the inclusion $\mathbb{F} \subset \mathbb{K} \subset \mathbb{L}$, this gives two extensions $\mathbb{L}/\mathbb{K}$ and $\mathbb{K}/\mathbb{F}$. If the degree of these two extensions are finite then the extension $\mathbb{L}/\mathbb{F}$ is also finite and we have the following equality: $[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}]$, see e.g. [Tig01, Lemma 15.3].
Furthermore, we recall that if α is a root of an irreducible polynomial in $\mathbb{K}[T]$ with degree d then $[\mathbb{K}(\alpha) : \mathbb{K}] = d$, see [Tig01, Proposition 12.15].

Now, we recall some classical results which will be useful in our proofs.

Lemma 4. *Let p be a prime number and let b be an element of some field $\mathbb{F}$, which is not a p-th power in $\mathbb{F}$.*
The polynomial $T^p - b$ is irreducible over $\mathbb{F}$.

Proof. For a proof see [Tig01, Lemma 13.9]. □

Lemma 5. *If $f_1(x) = \cdots = f_{n-1}(x) = x$, and $f_n(x) = x^p$ with $p \geq 3$ a prime number then the degree of the field extension $\mathbb{K}_j/\mathbb{K}_{j-1}$ is equal to p or 1.*

Proof. By definition we have $\mathbb{K}_j = \mathbb{K}_{j-1}(\alpha_j)$.
Two situations appear:
First, $\alpha_j = eval_i(x, y)$, where $x, y \in \mathbb{K}_{j-1}$.
As, $eval_1(x, y) = \cdots = eval_{n-1}(x, y) = y - x$ and $eval_2(x, y) = y^p - x^p$, we deduce that in this case $\alpha_j \in \mathbb{K}_{j-1}$. Thus $\mathbb{K}_j = \mathbb{K}_{j-1}$ and the degree of the extension is equal to one.
Second, $\alpha_j = cut_i(x, a)$, where $x, a \in \mathbb{K}_{j-1}$.
If $i = 1, \ldots, n-1$ then α_j is the solution of $\alpha_j - x = a$ then $\alpha_j \in \mathbb{K}_{j-1}$ and the degree of the field extension is equal to one.
If $i = n$ then α_j is the solution of $\alpha_j^p - x^p = a$.
If this equation has a solution in $\mathbb{K}_{j-1}$, this means $\alpha_j \in \mathbb{K}_{j-1}$ and the degree of $\mathbb{K}_j/\mathbb{K}j - 1$ is equal to one.
If the equation $\alpha_j^p - x^p = a$ has no solution in $\mathbb{K}_{j-1}$, then $a + x^p$ is not a p-th power in $\mathbb{K}_{j-1}$. Thus by Lemma 4 the polynomial $T^p - x^p - a \in \mathbb{K}_{j-1}[T]$ is irreducible over $\mathbb{K}_{j-1}$. In this last case, the degree of the extension $\mathbb{K}_j/\mathbb{K}_{j-1}$ is equal to p, see [Tig01, Proposition 12.15]. □

2. Impossible equitable fair divisions

2.1. **Proof of Theorem 1.** The idea used to prove our theorems is the following: If there exists a simple and equitable fair division $X = [0, t] \sqcup [t, 1]$, then we have

$$\mu_1\big([0, t]\big) = \mu_2\big([t, 1]\big) \text{ or } \mu_2\big([0, t]\big) = \mu_1\big([t, 1]\big).$$

This gives

$$f_1(t) = 1 - f_2(t) \text{ or } f_2(t) = 1 - f_1(t).$$

These two equations are equivalent to the following one:

$$(E) \quad f_1(t) + f_2(t) - 1 = 0.$$

This equation gives an algebraic condition on t which cannot be satisfied when we use the BSSRW model. The following proof explains why.

Proof of Theorem 1. If an algorithm in the algebraic Robertson-Webb model computes an equitable and simple fair division in k steps then the final cutpoint t belongs to $\mathbb{K}_k = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$. We have thus the inclusion $\mathbb{Q} \subset \mathbb{Q}(t) \subset \mathbb{K}_k$.
As t satisfies the equation (E) we have here

$$t^5 + t - 1 = 0.$$

We can factorize this expression and we obtain:

$$t^5 + t - 1 = (t^2 - t + 1)(t^3 + t^2 - 1) = 0.$$

As the polynomial $T^2 - T + 1$ has no real roots we deduce that we have

$$t^3 + t^2 - 1 = 0.$$

Furthermore, the polynomial T^3+T^2-1 is irreducible in $\mathbb{Q}[T]$. Indeed, it suffices to remark that T^3+T^2-1 has no rational roots. This a consequence of the rational roots theorem. In our situation, this theorem says that if T^3+T^2-1 has a rational root then it must be ± 1. Thus T^3+T-1 has no rational root and this polynomial is irreducible over $\mathbb{Q}$.

We deduce then

$$[\mathbb{Q}(t):\mathbb{Q}]=3.$$

However, by Lemma 5 with $n=2$, we have

$$[\mathbb{K}_k:\mathbb{Q}]=5^l,$$

with $l\leq k$. Therefore, the equality

$$5^l=[\mathbb{K}_k:\mathbb{Q}]=[\mathbb{K}_k:\mathbb{Q}(t)][\mathbb{Q}(t):\mathbb{Q}]=[\mathbb{K}_k:\mathbb{Q}(t)]\times 3$$

is impossible and this concludes the proof. □

Remark 6. We can remark that with the measures given in Theorem 1 even if the mediator can compute square roots then we still have an impossibility result.
Indeed, if the mediator use a square root after the j-th query then this means that during the algorithm the mediator uses a number $\alpha=\sqrt{\beta}$, where $\beta\in\mathbb{K}_j$. Then, we must consider some extensions $\mathbb{K}'_j=\mathbb{K}_j(\alpha)$ where $\alpha^2=\beta\in\mathbb{K}_j$. Therefore, the degree of some extensions $\mathbb{K}_j/\mathbb{K}_{j-1}$ can be equal to two. Thus, in the previous proof the degree $[\mathbb{K}_k:\mathbb{Q}]$ has the following form $[\mathbb{K}_k:\mathbb{Q}]=2^m5^l$ and the conclusion is still valid.

2.2. **Proof of Theorem 2.** In order to prove Theorem 2, we need some tools.

Lemma 7. *If $f_i(x)=x^{e_i}$, for $i=1,2$ then for all $j\geq 1$, $\mathbb{K}_j=\mathbb{K}_{j-1}$ or $\mathbb{K}_j$ is a radical extension of $\mathbb{K}_{j-1}$.*

Roughly speaking, this lemma says that the field $\mathbb{K}_j$ is of the following form: $\mathbb{K}_{j-1}(\sqrt[n]{\alpha})$, where n is an integer and $\alpha\in\mathbb{K}_{j-1}$.

Proof. If the j-th query is of the form $eval_i\big([x,y]\big)$ with $x,y\in\mathbb{K}_{j-1}$ then $eval_i\big([x,y]\big)$ is equal to $y^{e_i}-x^{e_i}$. Thus the result to this query $\alpha_j=y^{e_i}-x^{e_i}\in\mathbb{K}_{j-1}$. In this situation we have then $\mathbb{K}_j:=\mathbb{K}_{j-1}$.
If the j-th query is of the form $cut_i\big(x,a\big)$ with $x,a\in\mathbb{K}_{j-1}$ then the result α_j to this query is the unique solution in $[0,1]$ of the following equation:

$$\alpha_j^{e_i}-x^{e_i}=a.$$

This implies $\alpha_j=\sqrt[e_i]{a+x^{e_i}}$ and $\mathbb{K}_j:=\mathbb{K}_{j-1}(\sqrt[e_i]{a+x^{e_i}})$.
The extension $\mathbb{K}_j/\mathbb{K}_{j-1}$ is thus a radical extension.

□

As $\mathbb{Q}\subset\mathbb{K}_1\subset\cdots\subset\mathbb{K}_k$ we have by definition of a radical extension, see [Tig01, Chapter 13], the following corollary:

Corollary 8. *For all $j\geq 1$, the extension $\mathbb{K}_j/\mathbb{Q}$ is radical.*

Now, we recall a result about the irreducibility and the Galois group of certain trinomials.

Proposition 9 (Selmer [Sel56])**.** *The polynomials $T^d - T - 1$ are irreducible in $\mathbb{Q}[T]$ for all d.*
The polynomials $T^d + T + 1$ are irreducible in $\mathbb{Q}[T]$ for $d \not\equiv 2\,[3]$, but have a factor $T^2 + T + 1$ when $d \equiv 2\,[3]$. In the latter case, $T^d + T + 1$ has another factor which is irreducible.

Proposition 10 (Osada [Osa87])**.** *Let $f(T) = T^d + aT + b \in \mathbb{Z}[T]$, where $a = a_0c^d$ and $b = b_0c^d$ for some integer c. Then the Galois group over $\mathbb{Q}$ of this polynomial is isomorphic to the symmetric group $\mathcal{S}_d$ if the following conditions are satisfied:*

(1) *$f(T)$ is irreducible over $\mathbb{Q}$,*
(2) $\gcd\big(a_0c(d-1), db_0\big) = 1$.

These propositions allow us to show the following lemma.

Lemma 11. *If d is even or if $d \geq 5$ is odd with $d \not\equiv 2[3]$, then the Galois group over $\mathbb{Q}$ of $T^d + T - 1$ is isomorphic to the symmetric group $\mathcal{S}_d$.*
If $d \geq 5$ is prime and $d \equiv 2[3]$ then $T^d + T - 1$ is reducible over $\mathbb{Q}$: it has an irreducible factor with degree 2 and another one with degree $d - 2$.

Proof. When d is even, the change of variables $Y = -T$ gives

$$T^d + T - 1 = (-T)^d - (-T) - 1 = Y^d - Y - 1.$$

We deduce that $T^d + T - 1$ is irreducible since, by Proposition 9, $Y^d - Y - 1$ is irreducible.
When $d \geq 5$ is odd with $d \not\equiv 2\,[3]$, the change of variables $Y = -T$ gives

$$T^d + T - 1 = -(-T)^d - (-T) - 1 = -Y^d - Y - 1 = -(Y^d + Y + 1).$$

As before, thanks to Proposition 9, we deduce that $T^d + T - 1$ is irreducible since $Y^d + Y + 1$ is irreducible.

Therefore, in the two previous cases $T^d + T - 1$ is irreducible over $\mathbb{Q}$.
Proposition 10 with $a_0 = c = 1$ and $b = -1$ entails in these situations that the Galois group of $T^d + T - 1$ is isomorphic to $\mathcal{S}_d$.

When $d \geq 5$ is prime and $d \equiv 2[3]$, the change of variables $Y = -T$ gives as before $T^d + T - 1 = -(Y^d + Y + 1)$ and Proposition 9 gives the desired result. □

Now, we can prove Theorem 2.

Proof of Theorem 2. We suppose that there exists an algorithm in the BSSRW model computing an equitable and simple fair division $X = [0, t] \cup [t, 1]$. Then, t must satisfy the equation (E). Here, this equation is:

$$t^d + t - 1 = 0.$$

First, we suppose that d satisfies the hypothesis of one of the first two items.

As t must belong to $\mathbb{K}_k$ and, by Corollary 8, $\mathbb{K}_k$ is a radical extension of $\mathbb{Q}$, we deduce that t has a radical expression over $\mathbb{Q}$. Thus as the polynomial $T^d + T - 1$ is irreducible then it can be solved by radicals over $\mathbb{Q}$, see [Tig01, Proposition 14.33]. However, by Lemma 11, the Galois group of $T^d + T - 1$ is isomorphic to $\mathcal{S}_d$. Then Galois' theory implies that this polynomial cannot be solved by radicals over $\mathbb{Q}$,

see [Tig01, Chapter 14]. This gives the desired contradiction.

Now, we suppose that $d \geq 5$ is prime and $d \equiv 2\,[3]$.
In this case, the proof is a generalization of the proof of Theorem 1.

By Lemma 11, the polynomial $T^d + T - 1$ has an irreducible factor with degree 2 and another one with degree $d-2$. This gives

$$[\mathbb{Q}(t) : \mathbb{Q}] = 2 \text{ or } [\mathbb{Q}(t) : \mathbb{Q}] = d - 2.$$

Furthermore, thanks to Lemma 5 we have

$$[\mathbb{K}_k : \mathbb{Q}] = d^l,$$

where $l \in \mathbb{N}$.
The equality

$$[\mathbb{K}_k : \mathbb{Q}] = [\mathbb{K}_k : \mathbb{Q}(t)][\mathbb{Q}(t) : \mathbb{Q}]$$

is then impossible since d is prime. This concludes the proof. □

3. Impossibility to maximize the social welfare function

Theorem 3. *In the BSSRW model of computation there exists measures $\mu_1, \mu_2, \ldots, \mu_n$ such that no algorithm returns a division which maximizes the utilitarian social welfare function.*
Furthermore, we can take $\mu_1, \mu_2, \ldots, \mu_n$ in the following way:

$$\mu_1([0,x]) = \cdots = \mu_{n-1}([0,x]) = x, \quad \mu_n([0,x]) = x^p$$

where $p \geq 3$ is a prime number.

It must be noticed that the division is not supposed to be simple.

The previous theorem deals with a problem involving an inequality about the utilitarian social welfare function. Our strategy will be to reduce this problem to a problem involving an equation.
In general, fair division problems are stated with inequalities, see e.g. envy-free division and proportional division. We can always reduce these problems to problems involving equalities. For example, the condition $\mu_i(X_i) \geq 1/n$ becomes $\mu_i(X_i) = 1/n + e^2$, where $e \in \mathbb{R}$. However, with this method we introduce new variables and the problem do not become necessarily easier with these equalities.

Proof. Let $X = \sqcup_{i=1}^n X_i$ be a division of X constructed with m cuts.
This means that each X_i can be written in the following way $X_i = \sqcup_{j \in I_i} [x_j, x_{j+1}]$, and we have m different x_j: $x_1 \leq x_2 \leq \cdots \leq x_m$.

The value of the utilitarian social welfare function associated to this division is

$$\mathcal{F}(x_1, \ldots, x_m) = \sum_{i=1}^{n-1} \sum_{j \in I_i} (x_{j+1} - x_j) + \sum_{j \in I_n} (x_{j+1}^p - x_j^p).$$

Now, we consider an index $j_0 \in I_n$.
We remark that

$$\mathcal{F}(x_1, \ldots, x_m) = g(x_1, \ldots, x_{j_0-1}, x_{j_0+1}, \ldots, x_m) + x_{j_0} - x_{j_0}^p,$$

where g is a function independent of x_{j_0}.
If this division maximizes the social welfare function then we must have

$$\partial_{x_{j_0}} \mathcal{F}(x_1, \ldots, x_m) = 1 - p x_{j_0}^{p-1} = 0.$$

Then $x_{j_0} = \sqrt[p-1]{1/p}$. As $p \geq 3$ is a prime number we deduce that $x_{j_0} \notin \mathbb{Q}$. Furthermore, as x_{j_0} is a root of the polynomial $pT^{p-1} - 1$ we get

$$1 < [\mathbb{Q}(x_{j_0}) : \mathbb{Q}] < p.$$

Now, suppose that an algorithm in the BSSRW model computes in k steps a division which maximizes the utilitarian social welfare function. Then, $x_{j_0} \in \mathbb{K}_k$. However, by Lemma 5, we have

$$[\mathbb{K}_k : \mathbb{Q}] = p^l,$$

with $l \leq k$. Therefore, the equality

$$[\mathbb{K}_k : \mathbb{Q}] = [\mathbb{K}_k : \mathbb{Q}(x_{j_0})][\mathbb{Q}(x_{j_0}) : \mathbb{Q}]$$

is impossible since p is prime. This concludes the proof. □

Acknowledgement The author thanks Erel Segal-Halevi for his precious remarks about a preliminary version of this article.

References

[AM16] H. Aziz and S. Mackenzie. A discrete and bounded envy-free cake cutting protocol for any number of agents. In *IEEE 57th Annual Symposium on Foundations of Computer Science, FOCS 2016, 9-11 October 2016*, pages 416–427, 2016.

[Aus82] A. K. Austin. Sharing a cake. *The Mathematical Gazette*, 66(437):212–215, 1982.

[Bar05] J. Barbanel. *The geometry of efficient fair division*. Cambridge University Press, 2005.

[BCSS98] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and real computation*. Springer-Verlag, New York, 1998. With a foreword by Richard M. Karp.

[BJK13] S. Brams, M. Jones, and C. Klamler. N-person cake-cutting: There may be no perfect division. *The American Mathematical Monthly*, 120(1):35–47, 2013.

[BM15] S. Brânzei and P. Miltersen. A dictatorship theorem for cake cutting. In Qiang Yang and Michael Wooldridge, editors, *Proceedings of the Twenty-Fourth International Joint Conference on Artificial Intelligence, IJCAI 2015, Buenos Aires, Argentina, July 25-31, 2015*, pages 482–488. AAAI Press, 2015.

[BN17] S. Brânzei and N. Nisan. The query complexity of cake cutting. *ArXiv e-prints*, abs/1705.02946, 2017.

[BSS89] L. Blum, M. Shub, and S. Smale. On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. *Bull. Amer. Math. Soc. (N.S.)*, 21(1):1–46, 1989.

[BT95] S. Brams and A. Taylor. An envy-free cake division protocol. *The American Mathematical Monthly*, 102(1):9–18, 1995.

[BT96] S. Brams and A. Taylor. *Fair division - from cake-cutting to dispute resolution*. Cambridge University Press, 1996.

[CDE+06] Y. Chevaleyre, P. Dunne, U. Endriss, J. Lang, M. Lemaître, N. Maudet, J. Padget, S. Phelps, J. Rodríguez-Aguilar, and P. Sousa. Issues in multiagent resource allocation. *INFORMATICA*, 30:3–31, 2006.

[CDP13] K. Cechlárová, J. Doboš, and E. Pillárová. On the existence of equitable cake divisions. *Information Sciences*, 228(Supplement C):239 – 245, 2013.

[Chè17] G. Chèze. Existence of a simple and equitable fair division: A short proof. *Mathematical Social Sciences*, 87:92 – 93, 2017.

[Chè18] G. Chèze. Don't cry to be the first! symmetric fair division algorithms exist. *Arxiv*, http://arxiv.org/abs/1804.03833, 2018.

[CLPP13] Y. Chen, J. Lai, D. Parkes, and A. Procaccia. Truth, justice, and cake cutting. *Games and Economic Behavior*, 77(1):284 – 297, 2013.

[CP12] K. Cechlárová and E. Pillárová. On the computability of equitable divisions. *Discrete Optimization*, 9(4):249 – 257, 2012.

[DS61] L.E. Dubins and E. H. Spanier. How to cut a cake fairly. *The American Mathematical Monthly*, 68(1):1–17, 1961.

[EP84] S. Even and A. Paz. A note on cake cutting. *Discrete Applied Mathematics*, 7(3):285 – 296, 1984.

[EP11] J. Edmonds and K. Pruhs. Cake cutting really is not a piece of cake. *ACM Trans. Algorithms*, 7(4):51, 2011.

[KPS13] I. Kash, A. Procaccia, and N. Shah. No agent left behind: dynamic fair division of multiple resources. In *International conference on Autonomous Agents and Multi-Agent Systems, AAMAS '13, Saint Paul, MN, USA, May 6-10, 2013*, pages 351–358, 2013.

[Osa87] H. Osada. The Galois groups of the polynomials $X^n + aX^l + b$. *J. Number Theory*, 25(2):230–238, 1987.

[Pik00] O. Pikhurko. On envy-free cake division. *The American Mathematical Monthly*, 107(8):736–738, 2000.

[Pro13] A. Procaccia. Cake cutting: Not just child's play. *Commun. ACM*, 56(7):78–87, July 2013.

[Pro16] A. Procaccia. Cake cutting algorithms. In F. Brandt, V. Conitzer, U. Endriss, J. Lang, and A. D. Procaccia, editors, *Handbook of Computational Social Choice*, chapter 13. Cambridge University Press, 2016.

[PW17] A. Procaccia and J. Wang. A lower bound for equitable cake cutting. In *Proceedings of the 2017 ACM Conference on Economics and Computation*, EC '17, pages 479–495, New York, NY, USA, 2017. ACM.

[RW97] J. Robertson and W. Webb. Near exact and envy-free cake division. *Ars Combinatoria*, 45:97–108, 1997.

[RW98] J. Robertson and W. Webb. *Cake-cutting algorithms - be fair if you can*. A K Peters, 1998.

[Sel56] E. Selmer. On the irreducibility of certain trinomials. *Math. Scand.*, 4:287–302, 1956.

[SHS18] E. Segal-Halevi and B. Sziklai. Resource-monotonicity and population-monotonicity in connected cake-cutting. *Mathematical Social Sciences*, 95:19 – 30, 2018.

[Ste48] H. Steinhaus. The problem of fair division. *Econometrica*, 16(1):101–104, January 1948.

[Str08] W. Stromquist. Envy-free cake divisions cannot be found by finite protocols. *Electr. J. Comb.*, 15(1), 2008.

[Tho06] W. Thomson. Children crying at birthday parties. Why? *Economic Theory*, 31(3):501–521, 2006.

[Tig01] J.-P. Tignol. *Galois' theory of algebraic equations*. World Scientific Publishing Co., Inc., River Edge, NJ, 2001.

[WS07] G. Woeginger and J. Sgall. On the complexity of cake cutting. *Discrete Optimization*, 4(2):213 – 220, 2007.