Exact Algorithms for Solving Stochastic Games*

Kristoffer Arnsfelt Hansen† Michal Koucký‡ Niels Lauritzen§
Peter Bro Miltersen¶ and Elias P. Tsigaridas‖

February 20, 2012

Abstract

Shapley's *discounted stochastic games*, Everett's *recursive games* and Gillette's *undiscounted stochastic games* are classical models of game theory describing two-player zero-sum games of potentially infinite duration. We describe algorithms for exactly solving these games. When the number of positions of the game is constant, our algorithms run in polynomial time.

1 Introduction

Shapley's model of finite *stochastic games* [34] is a classical model of game theory describing two-player zero-sum games of (potentially) infinite duration. Such a game is given by a finite set of positions $1, \ldots, N$, with a $m_k \times n_k$ *reward* matrix (a^k_{ij}) associated to each position k, and an $m_k \times n_k$ *transition* matrix (p^{kl}_{ij}) associated to each pair of positions k and l. The game is played in rounds, with some position k being the *current* position in each round. At each such round, Player I chooses an action $i \in \{1, 2, \ldots, m_k\}$ while simultaneously, Player II chooses an action $j \in \{1, 2, \ldots, n_k\}$, after which the (possibly negative) *reward* a^k_{ij} is paid by Player II to Player I, and with probability p^{kl}_{ij} the current position becomes l for the next round.

During play of a stochastic game, a sequence of rewards is paid by Player II to Player I. There are three standard ways of associating a *payoff* to Player I from such a sequence, leading to three different variants of the stochastic game model:

Shapley games. In Shapley's original paper, the payoff is simply the sum of rewards. While this is not well-defined in general, in Shapley's setting it is required that for all positions k, $\sum_l p^{kl}_{ij} < 1$,

*An extended abstract of this paper was presented at STOC'11. Hansen, Miltersen and Tsigaridas acknowledge support from the Danish National Research Foundation and The National Science Foundation of China (under the grant 61061130540) for the Sino-Danish Center for the Theory of Interactive Computation, within which this work was performed. They also acknowledge support from the Center for Research in Foundations of Electronic Markets (CFEM), supported by the Danish Strategic Research Council.

†Computer Science Department, Aarhus University, Denmark.

‡Institute of Mathematics of Czech Academy of Sciences. Partially supported by GA ČR P202/10/0854, project No. 1M0021620808 of MŠMT ČR, Institutional Research Plan No. AV0Z10190503 and grant IAA100190902 of GA AV ČR.

§Mathematics Department, Aarhus University, Denmark.

¶Computer Science Department, Aarhus University, Denmark.

‖Computer Science Department, Aarhus University, Denmark. Partially supported by an individual postdoctoral grant from the Danish Agency for Science, Technology and Innovation.

with the remaining probability mass resulting in termination of play. Thus, no matter which actions are chosen by the players, play eventually ends with probability 1, making the payoff well-defined except with probability 0. We shall refer to this original variant of the stochastic games model as *Shapley games*. Shapley observed that an alternative formulation of this payoff criterion is to require $\sum_l p_{ij}^{kl} = 1$, but *discounting* rewards, i.e., penalizing a reward accumulated at time t by a factor of γ^t where γ is a *discount factor* strictly between 0 and 1. Therefore, Shapley games are also often referred to as *discounted* stochastic games. Using the Banach fixed point theorem in combination with the von Neumann minimax theorem for matrix games, Shapley showed that all Shapley games have a value, or, more precisely, a *value vector*, one value for each position. Also, the values can be guaranteed by both players by a *stationary strategy*, i.e., a strategy that associates a fixed probability distribution on actions to each position and therefore does not take history of play into account.

Gillette games. Gillette [23] requires that for all k, i, j, $\sum_l p_{ij}^{kl} = 1$, i.e., all plays are infinite. The total payoff to Player I is $\liminf_{T\to\infty}(\sum_{t=1}^{T} r_i)/T$ where r_t is the reward collected at round t. Such games are called *undiscounted* or *limiting average* stochastic games. In this paper, for coherence of terminology, we shall refer to them as *Gillette games*. It is much harder to see that Gillette games have values than that Shapley games do. In fact, it was open for many years if the concrete game *The Big Match* with only three positions that was suggested by Gillette has a value. This problem was resolved by Blackwell and Ferguson [8], and later, Mertens and Neyman [29] proved in an ingenious way that all Gillette games have value vectors, using the result of Bewley and Kohlberg [7]. However, the values can in general only be approximated arbitrarily well by strategies of the players, not guaranteed exactly, and non-stationary strategies (taking history of play into account) are needed even to achieve such approximations. In fact, *The Big Match* proves both of these points.

Everett games. Of generality between Shapley games and Gillette games is the model of *recursive games* of Everett [21]. We shall refer to these games as *Everett games*, also to avoid confusion with the largely unrelated notion of recursive games of Etessami and Yannakakis [19]. In Everett's model, we have $a_{ij}^k = 0$ for all i, j, k, i..e, rewards are *not* accumulated during play. For each particular k, we can have either $\sum_l p_{ij}^{kl} < 1$ or $\sum_l p_{ij}^{kl} = 1$. In the former case, a prespecified payoff b_{ij}^k is associated to the termination outcome. Payoff 0 is associated with infinite play. The special case of Everett games where $b_{ij}^k = 1$ for all k, i, j has been studied under the name of *concurrent reachability games* in the computer science literature [17, 11, 25, 24]. Everett showed that Shapley games can be seen as a special case of Everett games. Also, it is easy to see Everett games as a special case of Gillette games. It was shown in Everett's original paper that all Everett games have value vectors. Like Gillette games, the values can in general only be approximated arbitrarily well, but unlike Gillette games, stationary strategies are sufficient for guaranteeing such approximations.

For formal definitions and proofs of some of the facts above, see Section 2.

Our Results

In this paper we consider the problem of exactly solving Shapley, Everett and Gillette games, i.e., computing the value of a given game. The variants of these two problems for the case of *perfect information* (a.k.a. *turn-based*) games are well-studied by the computer science community, but not known to be polynomial time solvable: The tasks of solving perfect information Shapley, Everett

and Gillette games and the task of solving Condon's *simple stochastic games* [13] are polynomial time equivalent [1]. Solving simple stochastic games in polynomial time is by now a famous open problem. As we consider algorithms for the more general case of imperfect information games, we, unsurprisingly, do not come up with polynomial time algorithms. However, we describe algorithms for all three classes of games that run in polynomial time when the number of positions is constant and our algorithms are the first algorithms with this property. As the values of all three kinds of games may be irrational but algebraic numbers, our algorithms output real algebraic numbers in *isolating interval representation,* i.e., as a square-free polynomial with rational coefficients for which the value is a root, together with an (isolating) interval with rational endpoints in which this root is the only root of the polynomial. To be precise, our main theorem is:

Theorem. *For any constant N, there is a polynomial time algorithm that takes as input a Shapley, Everett or Gillette game with N positions and outputs its value vector using isolating interval encoding. Also, for the case of a Shapley games, an optimal stationary strategy for the game in isolating interval encoding can be computed in polynomial time. Finally, for Shapley as well as Everett games, given an additional input parameter $\epsilon > 0$, an ϵ-optimal stationary strategy using only (dyadic) rational valued probabilities can be computed in time polynomial in the representation of the game and* $\log(1/\epsilon)$.

We remark that when the number of positions N is constant, what remains to vary is (most importantly) the number of actions m for each player in each position and (less importantly) the bitsize τ of transition probabilities and payoffs. We also remark that Etessami and Yannakakis [20] showed that the bitsize of the isolating interval encoding of the value of a discounted stochastic game as well as the value of a recursive game may be exponential in the number of positions of the game and that Hansen, Koucký and Miltersen [25] showed that the bitsize of an ϵ-optimal strategy for a recursive game using binary representation of probabilities may be exponential in the number of positions of the game. Thus, merely from the size of the output to be produced, there can be no polynomial time algorithm for the tasks considered in the theorem without some restriction on N. Nevertheless, the time complexity of our algorithm has a dependence on N which is very bad and not matching the size of the output. For the case of Shapley games, the exponent in the polynomial time bound is $O(N)^{N^2}$ while for the case of Everett games and Gillette games, the exponent is $N^{O(N^2)}$. Thus, getting a better dependence on N is a very interesting open problem.

Prior to our work, algorithms for solving stochastic games relied either on generic reductions to decision procedures for the first order theory of the reals [20, 12], or, for the case of Shapley games and concurrent reachability games on value or strategy iteration [33, 11]. For all these algorithms, the complexity is at least exponential *even when the number of positions is a constant and even when only a crude approximation is required [24].* Nevertheless, as is the case for the algorithms based on reductions to decision procedures for the first order theory of the reals, our algorithms rely on the theory of semi-algebraic geometry [3], but in a more indirect way as we explain below.

Our algorithms are based on a simple recursive bisection pattern which is in fact a very natural and in retrospect unsurprising approach to solving stochastic games. However, in order to set the parameters of the algorithm in a way that makes it correct, we need *separation bounds* for values of stochastic games of given type and parameters; lower bounds on the absolute value of games of non-zero value. Such bounds are obtained by bounding the algebraic degree and coefficient size of the defining univariate polynomial and applying standard arguments, so the task at hand boils down to determining as good bounds on degree and coefficient size as possible; with better bounds leading to faster algorithms. To get these bounds, we apply the general machinery of real

algebraic geometry and semi-algebraic geometry following closely the techniques of the seminal work of Basu, Pollack and Roy [3]. That is, for each of the three types of games, we describe how for a given game G to derive a formula in the first order theory of the real numbers uniquely defining the value of G. This essentially involves formalizing statements proved by Shapley, Everett, and Mertens and Neyman together with elementary properties of linear programming. Now, we apply the powerful tools of *quantifier elimination* [3, Theorem 14.16] and *sampling* [3, Theorem 13.11] to show the appropriate bounds on degree and coefficient size. We stress that these procedures are only carried out in our proofs; they are not carried out by our algorithms. Indeed, if they were, the time complexity of the algorithms would be exponential, even for a constant number of positions. While powerful, the semi-algebraic approach has the disadvantage of giving rather imprecise bounds. Indeed, as far as we know, all published versions of the quantifier elimination theorem and the sampling theorem have unspecified constants ("big-Os"), leading to unspecified constants in the code of our algorithms. Only for the case of Shapley games, are we able to do somewhat better, their mathematics being so simple that we can avoid the use of the general tools of quantifier elimination and sampling and instead base our bounds on solutions to the following very natural concrete problem of real algebraic geometry that can be seen as a very special case of the sampling problem:

Given a system of m polynomials in n variables (where m is in general different from n) of degree bounded by d, whose coefficients have bitsizes at most τ, and an isolated *(in the Euclidean topology) real root of the system, what is an upper bound on its algebraic degree as a function of d and n? What is a bound on the bitsizes of the coefficients of the defining polynomial?*

Basu, Pollack and Roy [3, Corollary 13.18] stated the upper bound $O(d)^n$ on the algebraic degree as a corollary of the sampling theorem. We give a constructive bound of $(2d+1)^n$ on the algebraic degree and we derive an explicit bound on the coefficients of the defining polynomial. We emphasize that our techniques for doing this are standard in the context of real algebraic geometry; in particular the deformation method and u-resultants are used. However, we find it surprising that (to the best of our knowledge) no explicit constant for the big-O was previously stated for this very natural problem. Also, we do not believe that $(2d+1)^n$ is the final answer and would like to see an improvement. We hope that by stating some explicit bound we will stimulate work improving it. We note that for the case of isolated complex roots, explicit bounds appeared recently, see Emiris, Mourrain and Tsigaridas [18] and references therein.

The degree bounds for the algebraic problem lead to upper bounds on the algebraic degree of the values of Shapley games as a function of the combinatorial parameters of the game. We also provide corresponding lower bounds by proving that polynomials that have among their real roots the value of certain Shapley games are irreducible. We prove irreducibility based on Hilbert's irreducibility theorem and a generalization of the Eisenstein criterion, As these bounds may be of independent interest, we state them explicitly:

The value of any Shapley game with N positions, m actions for each player in each position, and rational payoffs and transition probabilities, is an algebraic number of degree at most $(2m+5)^N$. Also, for any $N, m \geq 1$ there exists a game with these parameters such that its value is an algebraic number of degree m^{N-1}.

The lower bound strengthens a result of Etessami and Yannakakis [20] who considered the case of $m = 2$ and proved a $2^{\Omega(N)}$ lower bound. For the more general case of Everett games and Gillette games, we are only able to get an upper bound on the degree of the form $m^{O(N^2)}$ and consider getting improved bounds for this case an interesting problem (we have no lower bounds better than

for the case of Shapley games). As explained above, replacing the big-Os with explicit constants requires "big-O-less" versions of the quantifier elimination theorems and sampling theorems of semi-algebraic geometry. We acknowledge that it is a straightforward but also probably quite work-intensive task to understand exactly which constants are implied by existing proofs. Clearly, we would be interested in such results, and are encouraged by recent work of the real algebraic geometry community [4] essentially providing a big-O-less version of the very related Theorem 13.15 of Basu, Pollack and Roy. We do hypothesize that the constants will be much worse that the constant of our big-O-less version of Corollary 13.18 of Basu, Pollack and Roy and that merely stating some constants would stimulate work improving them.

As a final byproduct to our techniques, we give a new upper bound on the complexity of the strategy iteration algorithm for concurrent reachability games [11] that matches the known lower bound [24]. We show: *The strategy improvement algorithm of Chatterjee, de Alfaro and Henzinger [11] computes an ϵ-optimal strategy in a concurrent reachability game with N actions, m actions for each player in each position after at most $(1/\epsilon)^{m^{O(N)}}$ iterations.* Prior to this paper only a doubly exponential upper bound on the complexity of strategy iteration was known, even for the case of a constant number of positions [24]. The proof uses a known connection between the *patience* of concurrent reachability games and the convergence rate of strategy iteration [24] combined with a new bound on the patience proved using a somewhat more clever use of semi-algebraic geometry than in the work leading to the previous bound [25].

Structure of the paper

Section 2 contains background material and notation. Section 3 contains a description of our algorithms. Section 4 contains the upper bounds on degree of values and lower bounds on coefficient sizes of defining polynomials and resulting separation bounds of values needed for the algorithm, for the case of Shapley, Everett and Gillete games. The proof of the exact bounds, big-O-less version, of the algebraic degree and the separation bounds of the isolated real solutions of a polynomial system is presented in Section 5. Section 6 presents the lower bound construction on the Shapley games and the algebraic tools needed for this. Finally, Section 7 contains the consequences of our results for the strategy improvement algorithm for concurrent reachability are explained.

2 Preliminaries

(Parameterized) Matrix Games

A matrix game is given by a real $m \times n$ matrix A of payoffs a_{ij}. When Player I plays action $i \in \{1, 2, \ldots, m\}$ and Player II simultaneously plays action $j \in \{1, 2, \ldots, n\}$, Player I receives a payoff a_{ij} from Player II. A strategy of a player is a probability distribution over the player's actions, i.e. a stochastic vector. Given strategies x and y for the two players, the expected payoff to player I is $x^{\mathsf{T}}Ay$. We denote by $\mathrm{val}(A)$ the maximin value of the game. As is well-known the value as well as an optimal mixed strategy for Player I can be found by the following linear program, in variables $x_1, \ldots, x_m$ and v. By f_n we denote the vector of dimension n with all entries being 1.

$$\begin{array}{lrcl} \max & v & & \\ s.t. & f_n v - A^{\mathsf{T}} x & \leq & 0 \\ & x & \geq & 0 \\ & f_m^{\mathsf{T}} x & = & 1 \end{array} \tag{1}$$

The following easy lemma of Shapley is useful.

Lemma 1 ([34], equation (2))**.** *Let $A = (a_{ij})$ and $B = (b_{ij})$ be $m \times n$ matrix games. Then*

$$|\operatorname{val}(A) - \operatorname{val}(B)| \leq \max_{i,j} |a_{ij} - b_{ij}|$$

In the following we will find it convenient to use terminology of Bertsimas and Tsitsiklis [6]. We say that a set of linear constraints are linearly independent if the corresponding coefficient vectors are linearly independent.

Definition 2. *Let P be a polyhedron in $\mathbb{R}^n$ defined by linear equality and inequality constraints and let $x \in \mathbb{R}^n$.*

1. *x is a* basic solution *if all equality constraints of P are satisfied by x, and there are n linearly independent constraints of P that are satisfied with equality by x.*
2. *x is a* basic feasible solution *(bfs) if x is a basic solution and furthermore satisfies all the constraints of P.*

The polyhedron defined by LP (1) is given by 1 equality constraint and $n + m$ inequality constraints, in $m+1$ variables. Since the polyhedron is bounded, the LP obtains its optimum value at a bfs. To each bfs, (x, v), we may thus associate a set of $m + 1$ linearly independent constraints such that turning all these constraints into linear equations yields a linear system where (x, v) is the unique solution. Furthermore we may express this solution using Cramer's rule. We order the variables as $x_1, \ldots, x_m, v$, and we also order the constraints so that the equality constraint is the last one. Let B be a set of $m + 1$ constraints of the linear program, including the equality constraint. We shall call such a set B a *potential basis set*. Define M_B^A to be the $(m+1) \times (m+1)$ matrix consisting of the coefficients of the constraints in B. The linear system described above can thus be succinctly stated as follows:

$$M_B^A \begin{bmatrix} x \\ v \end{bmatrix} = e_{m+1} \ .$$

We summarize the discussion above by the following lemma.

Lemma 3. *Let $v \in \mathbb{R}$ and $x \in \mathbb{R}^m$ be given.*

1. *The pair $(x, v)^\mathsf{T}$ is a basic solution of (1) if and only if there is a potential basis set B such that $\det(M_B^A) \neq 0$ and $(x, v)^\mathsf{T} = (M_B^A)^{-1} e_{m+1}$.*
2. *The pair $(x, v)^\mathsf{T}$ is a bfs of (1) if and only if there is a potential basis set B such that $\det(M_B^A) \neq 0$, $(x, v)^\mathsf{T} = (M_B^A)^{-1} e_{m+1}$, $x \geq 0$ and $f_n v - A^\mathsf{T} x \leq 0$.*

By Cramer's rule we find that $x_i = \det((M_B^A)_i)/\det(M_B^A)$ and $v = \det((M_B^A)_{m+1})/\det(M_B^A)$. Here $(M_B^A)_i$ is the matrix obtained from M_B^A by replacing column i with e_{m+1}.

We shall be interested in *parameterized* matrix games. Let A be a mapping from $\mathbb{R}^N$ to $m \times n$ matrix games. Given a potential basis set B we will be interested in describing the sets of parameters for which B gives rise to a bfs as well as an optimal bfs for LP (1). We let F_B^A denote the set of $w \in \mathbb{R}^N$ such that B defines a bfs for the matrix game $A(w)$, and we let O_B^A denote the set of $w \in \mathbb{R}^N$ such that B defines an optimal bfs for the matrix game $A(w)$. Let $\overline{B_1} \subseteq \{1, \ldots, n\}$ be

the set of indices of the first n constraints that are not in B. Similarly, let $\overline{B_2} \subseteq \{1, \ldots, m\}$ be the indices of the next m constraints that are not in B. We may describe the set F_B^A as a union $F_B^{A+} \cup F_B^{A-}$. Here F_B^{A+} is defined to be the set of parameters w that satisfy the following $m+1$ inequalities:

$$\det(M_B^{A(w)}) > 0 \ ,$$

$$\det((M_B^{A(w)})_{m+1}) - \sum_{i=1}^{m} a_{ij} \det(((M_B^{A(w)})_i)) \leq 0 \text{ for } j \in \overline{B_1},$$

$$\det((M_B^{A(w)})_i) \geq 0 \text{ for } i \in \overline{B_2}.$$

The set F_B^{A-} is defined analogously, by reversing all inequalities above. With these in place we can describe O_B^A as the sets of parameters $w \in F_B^A$ for which

$$\det((M_B^{A(w)})_{m+1}) = \mathrm{val}(A(w)) \det(M_B^{A(w)}) \ .$$

Shapley and Everett games

We will define stochastic games in a general form, following Everett [21], to capture both Shapley games as well as Everett games (but not Gillette games) as direct specializations. Everett in fact defined his games abstractly in terms of "game elements". We shall restrict ourselves to game elements that are given by matrix games (cf. [32]). Because of this, our precise notation will differ slightly from the one of Everett.

For that purpose a stochastic game Γ is specified as follows. We let N denote the number of *positions*, numbered $\{1, \ldots, N\}$. In every position k, the two players have m_k and n_k *actions* available, numbered $\{1, \ldots, m_k\}$ and $\{1, \ldots, n_k\}$. If at position k Player I chooses action i and Player II simultaneously chooses action j, Player I receives reward a_{ij}^k from player II. After this, with probability $s_{ij}^k \geq 0$ the game stops, in which case Player I receives an additional reward b_{ij}^k from player II. With probability $p_{ij}^{kl} \geq 0$, play continues at position l. We demand $s_{ij}^k + \sum_{l=1}^{N} p_{ij}^{kl} = 1$ for all positions k and all pairs of actions (i, j). A *strategy* of a player is an assignment of a probability distribution on the actions of each position, for each possible history of the play, a history being the sequence of positions visited so far as well as the sequences of actions played by both players in those rounds. A strategy is called *stationary* if it only depends on the current position.

Given a pair of strategies x and y as well as a starting position k, let r_i be the random variable denoting the reward given to Player I during round i (if play has ended we define this as 0). We define the expected total payoff by $\tau^k(x, y) = \lim_{n \to \infty} E\left[\sum_{i=1}^{n} r_i\right]$, where the expectation is taken over actions of the players according to their strategies x and y, as well as the probabilistic choices of the game (In the special cases of Shapley and Everett games the limit always exist). We define the *lower value*, $\underline{v}^k$, and *upper value*, $\overline{v}^k$, of the game Γ, starting in position k by $\underline{v}^k = \sup_x \inf_y \tau^k(x, y)$, and $\overline{v}^k = \inf_y \sup_x \tau^k(x, y)$. In case that $\underline{v}^k = \overline{v}^k$ we define this as the *value* v^k of the game, starting at position k. Assuming Γ has a value, starting at position k, we say that a strategy x is *optimal* for Player I, starting at position k if $\inf_y \tau^k(x, y) = v^k$, and for a given $\epsilon > 0$, we say the strategy x is ϵ-optimal starting at position k, if $\inf_y \tau^k(x, y) \geq v^k - \epsilon$. We define the notions of optimal and ϵ-optimal analogously for Player II.

A Shapley game [34] is a special case of the above defined stochastic games, where $s_{ij}^k > 0$ and $b_{ij}^k = 0$ for all positions k and all pairs of actions (i, j). Given *valuations* $v_1, \ldots, v_N$ for

the positions and a given position k we define $A^k(v)$ to be the $m_k \times n_k$ matrix game where entry (i,j) is $a^k_{ij} + \sum_{l=1}^N p^{kl}_{ij} v_l$. The *value iteration* operator $T : \mathbb{R}^N \to \mathbb{R}^N$ is defined by $T(v) = \big(\mathrm{val}(A^1(v)), \ldots, \mathrm{val}(A^N(v))\big)$. The following theorem of Shapley characterizes the value and optimal strategies of a Shapley game.

Theorem 4 (Shapley)**.** *The value iteration operator T is a contraction mapping with respect to supremum norm. In particular, T has a unique fixed point, and this is the value vector of the stochastic game Γ. Let x^* and y^* be the stationary strategies for Player I and player II where in position k an optimal strategy in the matrix game $A^k(v^*)$ is played. Then x^* and y^* are optimal strategies for player I and player II, respectively, for play starting in any position.*

An Everett game [21] is a special case of the above defined stochastic games, where $a^k_{ij} = 0$ for all k, i, j. In contrast to Shapley games, we may have that $s^k_{ij} = 0$ for some k, i, j. Everett points out that his games generalize the class of Shapley games. Indeed, we can convert Shapley game Γ to Everett game Γ' by letting $b^k_{ij} = a^k_{ij}/s^k_{ij}$, recalling that $s^k_{ij} > 0$.

Given *valuations* $v_1, \ldots, v_N$ for the positions and a given position k we define $A^k(v)$ to be the $m_k \times n_k$ matrix game where entry (i,j) is $s^k_{ij} b^k_{ij} + \sum_{l=1}^N p^{kl}_{ij} v_l$. The *value mapping* operator $M : \mathbb{R}^N \to \mathbb{R}^N$ is then defined by $M(v) = \big(\mathrm{val}(A^1(v)), \ldots, \mathrm{val}(A^N(v))\big)$. Define relations $\succcurlyeq$ and $\preccurlyeq$ on $\mathbb{R}^N$ as follows:

$$u \succcurlyeq v \quad \text{if and only if} \quad \begin{cases} u_i > v_i & \text{if } v_i > 0 \\ u_i \geq v_i & \text{if } v_i \leq 0 \end{cases}, \quad \text{for all } i \ .$$

$$u \preccurlyeq v \quad \text{if and only if} \quad \begin{cases} u_i < v_i & \text{if } v_i < 0 \\ u_i \leq v_i & \text{if } v_i \geq 0 \end{cases}, \quad \text{for all } i \ .$$

Next, we define the regions $C_1(\Gamma)$ and $C_2(\Gamma)$ as follows:

$$C_1(\Gamma) = \{v \in \mathbb{R}^N \mid M(v) \succcurlyeq v\},$$
$$C_2(\Gamma) = \{v \in \mathbb{R}^N \mid M(v) \preccurlyeq v\}.$$

A *critical vector* of the game is a vector v such that $v \in \overline{C_1(\Gamma)} \cap \overline{C_2(\Gamma)}$. That is, for every $\epsilon > 0$ there exists vectors $v_1 \in C_1(\Gamma)$ and $v_2 \in C_2(\Gamma)$ such that $\|v - v_1\|_2 \leq \epsilon$ and $\|v - v_2\|_2 \leq \epsilon$.

The following theorem of Everett characterizes the value of an Everett game and exhibits near-optimal strategies.

Theorem 5 (Everett)**.** *There exists a unique critical vector v for the value mapping M, and this is the value vector of Γ. Furthermore, v is a fixed point of the value mapping, and if $v_1 \in C_1(\Gamma)$ and $v_2 \in C_2(\Gamma)$ then $v_1 \leq v \leq v_2$. Let $v_1 \in C_1(\Gamma)$. Let x be the stationary strategy for player I, where in position k an optimal strategy in the matrix game $A^k(v_1)$ is played. Then for any k, starting play in position k, the strategy x guarantees expected payoff at least $v_{1,k}$ for player I. The analogous statement holds for $v_2 \in C_2(\Gamma)$ and Player II.*

Gillette Games

While the payoffs in Gillette's model of stochastic games cannot be captured as a special case of the general formalism above, the general setup is the same, i.e., the parameters $N, m_k, n_k, a^k_{ij}, p^{kl}_{ij}$

is as above and the game is played as in the case of Shapley games and Everett games. In Gillette's model, we have $b_{ij}^k = 0$ and $s_{ij}^k = 0$ for all k, i, j. The payoff associated with an infinite play of a Gillette game is by definition $\liminf_{T\to\infty}(\sum_{t=1}^{T} r_i)/T$ where r_t is the reward collected at round t. Upper and lower values are defined analogously to the case of Everett and Shapley games, but with the expectation of the payoff defined in this way replacing $\tau^k(x, y)$. Again, the value of position k is said to exist if its upper and lower value coincide. An Everett game can be seen as a special case of a Gillette game by replacing each termination outcome with final reward b with an absorbing position in which the reward b keeps recurring. The central theorem about Gillette games is the theorem of Mertens and Neyman [29], showing that all such games have a value. The proof also yields the following connection to Shapley games that is used by our algorithm: For a given Gillette game Γ, let Γ_λ be the Shapley game with all stop probabilities s_{ij}^k being λ and each transition probability being the corresponding transition probability of Γ multiplied by $1 - \lambda$. Let v^k be the value of position k in Γ and let v_λ^k be the value of position k in Γ_λ. Then, the following holds.

Theorem 6 (Mertens and Neyman)**.**

$$v^k = \lim_{\lambda\to 0+} \lambda v_\lambda^k$$

Real Algebraic Numbers

Let $p(x) \in \mathbb{Z}[x]$ be a nonzero polynomial with integer coefficients of degree d. Write $p(x) = \sum_{i=1}^{d} a_i x^i$, with $a_d \neq 0$. The *content* $\mathrm{cont}(p)$ of p is defined by $\mathrm{cont}(p) = \gcd(a_0, \ldots, a_d)$, and we say that p is *primitive* if $\mathrm{cont}(p) = 1$. We can view the coefficients of p as a vector $a \in \mathbb{R}^{d+1}$. We then define the *length* $|p|$ of p by $|p| = \|a\|_2$ as well as the *height* $|p|_\infty$ of p by $|p|_\infty = \|a\|_\infty$.

An algebraic number $\alpha \in \mathbb{C}$ is a root of a polynomial in $\mathbb{Q}[x]$. The *minimal polynomial* of α is the unique monic polynomial in $q \in \mathbb{Q}[x]$ of least degree with $q(\alpha) = 0$. Given an algebraic number α with minimal polynomial q, there is a minimal integer $k \geq 1$ such that $p = kq \in \mathbb{Z}[x]$. In other words p is the unique polynomial in $\mathbb{Z}[x]$ of least degree with $p(\alpha) = 0$, $\mathrm{cont}(p) = 1$ and positive leading coefficient. We extend the definitions of degree and height to α from p. The *degree* $\deg(\alpha)$ of α is defined by $\deg(\alpha) = \deg(p)$ and *height* $|\alpha|_\infty$ of α is defined by $|\alpha|_\infty = |p|_\infty$.

Theorem 7 (Kannan, Lenstra and Lovász)**.** *There is an algorithm that computes the minimal polynomial of a given algebraic number α of degree n_0 when given as input d and H such that $\deg(\alpha) \leq d$ and $|\alpha|_\infty \leq H$ and $\overline{\alpha}$ such that $|\alpha - \overline{\alpha}| \leq 2^{-s}/(12d)$, where*

$$s = \lceil d^2/2 + (3d + 4)\log_2(d + 1) + 2d\log_2(H)\rceil \ .$$

The algorithm runs in time polynomial in n_0, d and $\log H$.

3 Algorithms

In this section we describe our algorithms for solving Shapley, Everett and Gillette games. The algorithms for Shapley and Everett games proceed along the same lines, using the fact that Shapley games can be seen as a special case of Everett games explained above. The algorithm for Gillette games is a reduction to the case of Shapley games using Theorem 6. We proceed by first constructing the algorithms for Everett and Shapley games and explain the algorithm for Gillette games at the end of this section.

Reduced games

Let Γ be an Everett game with $N+1$ positions. Denote by $V(\Gamma)$ the critical vector of Γ. Given a valuation v for position $N+1$ we consider the *reduced game* $\Gamma^r(v)$ with N positions, obtained from Γ in such a way that whenever the game would move to position $N+1$, instead the game would stop and player 1 would receive a payoff v.

Denote by $V^r(v)$ the critical vector of the game $\Gamma^r(v)$. We have the following basic lemma shown by Everett.

Lemma 8. *For every $\delta > 0$, for all v and for all positions k: $(V^r(v))_k - \delta \leq (V^r(v-\delta))_k \leq (V^r(v))_k \leq (V^r(v+\delta))_k \leq (V^r(v))_k + \delta$. In particular, $V^r(v)$ is a continuous monotone function of v in all components. The first and last inequalities are strict inequalities, unless $(V^r(v))_k = v$.*

Let $\widetilde{V}(v)$ denote the value $\mathrm{val}(A^{N+1}(V^r(v), v))$ of the parameterized game for position $N+1$, where the first N positions are given valuations according to $V^r(v)$ and position $N+1$ is given valuation v.

Lemma 9. *Denote by v^* component $N+1$ of $V(\Gamma)$. Then the following equivalences hold.*

1. *Suppose $v^* > 0$ and $v \geq 0$. Then, $\widetilde{V}(v) > v \Leftrightarrow v < v^*$.*
2. *Suppose $v^* < 0$ and $v \leq 0$. Then, $\widetilde{V}(v) < v \Leftrightarrow v^* < v$.*

Proof. We shall prove only the first equivalence. The proof of the second equivalence is analogous. Assume first that $\widetilde{V}(v) > v$. Since $\widetilde{V}$ is continuous we can find $z \in C_1(\Gamma^r(v))$ such that $\mathrm{val}(A^{N+1}(z, v)) > v$ as well. This implies that $(z, v) \in C_1(\Gamma)$ and by definition of $C_1(\Gamma)$ we obtain that $v \leq v^*$. By Theorem 5, $\widetilde{V}(v^*) = \mathrm{val}(A^{N+1}(V^r(v^*), v^*)) = \mathrm{val}(A^{N+1}(V(\Gamma))) = v^*$. Since $\widetilde{V}(v) > v$ we have $v < v^*$.

The other part of the equivalence was shown by Everett as a part of his proof of Theorem 5. We present the argument for completeness. Everett in fact shows that v^* is the fixpoint of $\widetilde{V}$ of minimum absolute value. That is, $\widetilde{V}(v^*) = v^*$ and whenever $\widetilde{V}(v) = v$ we have $|v| \geq |v^*|$. Now assume that $v < v^*$, and let $\delta = v^* - v$. From Lemma 8 we have $\widetilde{V}(v) = \widetilde{V}(v^* - \delta) \geq \widetilde{V}(v^*) - \delta = v^* - \delta = v$. Since $v \geq 0$, from minimality of $|v^*|$ we have the strict inequality $\widetilde{V}(v) > v$. □

Recursive bisection algorithm

Based on Lemma 9 we may construct an idealized bisection algorithm Bisect (Algorithm 1) for approximating the last component of the critical vector, unrealistically assuming we can compute the critical vector of a reduced game exactly. For convenience and without loss of generality, we will assume throughout that the payoffs in the game Γ we consider have been normalized to belong to the interval $[-1, 1]$. The correctness of the algorithm follows directly from Lemma 9. Given that we have obtained a sufficiently good approximation for the last component of the critical vector we may reconstruct the exact value using Theorem 7. What "sufficiently good" means depends on the algebraic degree and size of coefficients of the defining polynomial of the algebraic number to be given as output, so we shall need bounds on these quantities for the game at hand.

To get an algorithm implementable as a Turing machine we will have to compute with approximations throughout the algorithm but do so in a way that simulates Algorithm 1 exactly, i.e., so that the same branches are followed in the if-statements of the algorithm. For this, we need separation bounds for values of stochastic games. Fortunately, these follow from the bounds on degree

Algorithm 1: Bisect(Γ, k)

Input: Game Γ with $N+1$ positions, all payoffs between -1 and 1, accuracy parameter $k \geq 2$.

Output: v such that $|v - v^*| \leq 2^{-k}$.

if $\widetilde{V}(0) = 0$ **then**
  return 0
else
  $v_l \leftarrow 0$
  $v_r \leftarrow \mathrm{sgn}(\widetilde{V}(0))$
  for $i \leftarrow 1$ **to** $k-1$ **do**
    $v \leftarrow (v_l + v_r)/2$
    if $|\widetilde{V}(v)| > |v|$ **then**
      $v_l \leftarrow v$
    else
      $v_r \leftarrow v$
  return $(v_l + v_r)/2$

Algorithm 2: ApproxBisect(Γ, k)

Input: Game Γ with $N+1$ positions, m actions per player in each position, all payoffs rationals between -1 and 1 and of bitsize L, accuracy parameter $k \geq 2$.

Output: v such that $|v - v^*| < 2^{-k}$.

$\epsilon \leftarrow \mathrm{sep}(N, m, L, 0)/5$
$v \leftarrow \mathrm{val}(A^{N+1}([\mathrm{ApproxVal}(V^r(0), \lceil -\log \epsilon \rceil)]_{\lceil -\log \epsilon \rceil}, 0))$
if $|v| \leq 2\epsilon$ **then**
  return 0
else
  $v_l \leftarrow 0$
  $v_r \leftarrow \mathrm{sgn}(v)$
  for $i \leftarrow 1$ **to** $k-1$ **do**
    $v \leftarrow (v_l + v_r)/2$
    $\epsilon \leftarrow \mathrm{sep}(N, m, \max(L, i), i)/5$
    $v' \leftarrow \mathrm{val}(A^{N+1}([\mathrm{ApproxVal}(V^r(v), \lceil -\log \epsilon \rceil)]_{\lceil -\log \epsilon \rceil}, v))$
    if $|v'| > |v|$ **then**
      $v_l \leftarrow v$
    else
      $v_r \leftarrow v$
  return $(v_l + v_r)/2$

Algorithm 3: ApproxVal(Γ, k)

Input: Game Γ with N positions, payoffs between -1 and 1, accuracy parameter $k \geq 2$.
Output: Value vector v such that $|v_i - v_i^*| < 2^{-k}$ for all positions i.

```
if N = 0 then
    return The empty vector
else
    for i ← 1 to N do
        v_i = ApproxBisect(Γ, k), where position i is swapped with position N
    Return v
```

and coefficient size needed anyway to apply Theorem 7. Consider a class $\mathcal{C}$ of Everett games (In fact $\mathcal{C}$ will be either all Everett games or the subset consisting of Shapley games). Let $\mathrm{sep}(N, m, L, j)$ denote a positive real number so that if v is the value of game $\Gamma \in \mathcal{C}$ with N positions, m actions to each player in every position, and every rational occurring in the description in the game having bitsize at most L, and v is not an integer multiple of 2^{-j}, then v differs by at least $\mathrm{sep}(N, m, L, j)$ from every integer multiple of 2^{-j}. Also, we let $[v]_k$ denote the function that rounds all entries in the vector v to the nearest integer multiple of 2^{-k}. Our modified algorithm ApproxBisect (for approximate Bisect) is given as Algorithm 2. The procedure ApproxVal invoked in the code simply computes approximations to the values of all positions in a game using ApproxBisect.

The correctness of ApproxBisect follows from the correctness of Bisect by observing that the former emulates the latter, in the sense that the same branches are followed in the if-statements. For the latter fact, Lemma 1 and Lemma 9 are used.

The complexity of the algorithm is estimated by the inequalities

$$T_{\mathrm{ApproxVal}}(N, m, L, k) \leq N T_{\mathrm{ApproxBisect}}(N, m, L, k),$$

and

$$\begin{aligned} T_{\mathrm{ApproxBisect}}(N, m, L, k) \leq {} & \lceil -\log \epsilon \rceil (T_{\mathrm{LP}}(m+1, \lceil -\log \epsilon \rceil) \\ & + T_{\mathrm{ApproxVal}}(N-1, m, \max\{L, k\}, \lceil -\log \epsilon \rceil), \end{aligned}$$

where $\epsilon = \mathrm{sep}(N-1, m, \max\{L, k\}, k)/5$, and $T_{\mathrm{LP}}(m+1, k)$ is a bound on the complexity of computing the value of a $m \times m$ matrix game with entries of bitsize k.

Plugging in the separation bound for Shapley games of Proposition 12, we get a concrete algorithm without unspecified constants. Also, to get an algorithm that outputs the exact algebraic answer in isolating interval encoding we need to call the algorithm with parameter k appropriately chosen to match the quantities stated in Theorem 7, taking into account the degree and coefficient bounds given in Proposition 12. Finally, plugging in a polynomial bound for T_{LP}, the above recurrences is now seen to yield a polynomial time bound for constant N. However, the exponent in this polynomial bound is $O(N)^{N^2}$, i.e., the complexity is doubly exponential in N. We emphasize that the fact that the exact value is reconstructed in the end only negligibly changes the complexity of the algorithm compared to letting the algorithm return a crude approximation. Indeed, an approximation algorithm following our approach would have to compute with a precision in its recursive calls similar to the precision necessary for reconstruction. Only for games with only one position (and hence no recursive calls) would an approximation version of ApproxBisect be faster.

For the case of Everett games, the degree, coefficient and separation bounds of Proposition 16 similarly yields the existence of a polynomial time algorithm for the case of constant N, with an exponent of $N^{O(N^2)}$.

Computing strategies

We now consider the task of computing ϵ-optimal strategies to complement our algorithm for computing values. For Shapley games the situation is simple. By Theorem 4, once we have obtained the value v^* of the game, we can obtain *exactly* optimal stationary strategies x^* and y^* by finding optimal strategies in the matrix games $A^k(v^*)$. Also, if we only have an approximation $\tilde{v}$ to v^*, such that $\|v^* - \tilde{v}\|_\infty \leq \epsilon$, consider the stationary strategies $\tilde{x}^*$ and $\tilde{y}^*$ given by optimal strategies in the matrix games $A^k(\tilde{v})$. In every round of play, these strategies may obtain ϵ less than the optimal strategies. But this deficit is *discounted* in every round by a factor $1 - \lambda$ where $\lambda = \min(s^k_{ij}) > 0$ is the minimum stop probability. Hence $\tilde{x}$ and $\tilde{y}$ are in fact (ϵ/λ)-optimal strategies.

For Everett games the situation is more complicated, since the actual values v^* may in fact give absolutely no information about ϵ-optimal strategies. We shall instead follow the approach of Everett and show how to find points $v_1 \in C_1$ and $v_2 \in C_2$ that are ϵ-close to v^*. Then, using Theorem 5 we can compute ϵ-optimal strategies by finding optimal strategies in the matrix games $A^k(v_1)$ and $A^k(v_2)$, respectively.

Let Γ be an Everett game with $N + 1$ positions. We first describe how to exactly compute $v_1 \in C_1$, given the ability to exactly compute the values; the case of $v_2 \in C_2$ is analogous. Let v^* be the critical vector of Γ. In case that $v^*_i \leq 0$ for all i, then by definition of C_1 we have $v^* \in C_1$. Otherwise at least one entry of v^* is positive, so assume $v^*_{N+1} > 0$. As in Section 3 we consider the reduced game $\Gamma^r(v)$, taking payoff v for position $N + 1$. By Lemma 9, whenever $0 \leq v < v^*_{N+1}$ we have $\widetilde{V}(v) > v$. Suppose in fact that we pick v so that $v^*_{N+1} - v \leq \epsilon/2$. Now let $\delta = \widetilde{V}(v) - v$. Recall $\widetilde{V}(v) = \mathrm{val}(A^{N+1}(V^r(v), v))$. Now recursively compute $z \in C_1(\Gamma^r(v))$ such that $\|V^r(v) - z\|_\infty \leq \min(\delta/2, \epsilon)$. Then by Lemma 1 we have that $|\mathrm{val}(A^{N+1}(V^r(v), v)) - \mathrm{val}(A^{N+1}(z, v))| \leq \delta/2$, which means $\mathrm{val}(A^{N+1}(z, v)) > v$. This means that $v_1 = (z, v) \in C_1$, and by our choices we have $\|v_1 - v^*\|_\infty \leq \epsilon$, as desired. We now have an exact representation of an algebraic vector v_1 in C_1, ϵ-approximating the critical vector. The size of the representation in isolating interval representation is polynomial in the bitsize of Γ (for constant N). From this we may compute the optimal strategies of $A^k(v_1)$ which also form an ϵ-optimal strategy of Γ. The polynomial size bound on v_1 implies that all non-zero entries in this strategy have magnitude at least 2^{-l} where l is polynomially bounded in the bitsize of Γ. We now show how to get a rational valued 2ϵ-optimal strategy in polynomial time. For this, we apply a rounding scheme described in Lemmas 14 and 15 of Hansen, Koucký and Miltersen [25]. For each position, we now round all probabilities, except the largest, *upwards* to L significant digits where L is a somewhat larger polynomial bound than l, while the largest probability at each position is rounded downwards to L significant digits. Using Lemma 14 (see also the proof of Lemma 15) of Hansen, Koucký and Miltersen [25], we can set L so that the resulting strategy is 2ϵ-optimal in Γ. This concludes the description of the procedure.

The case of Gillette games

To compute the value of a given Gillette game, we proceed as follows. Based on Theorem 6 we can similarly to the case of Shapley games and Everett games give degree, coefficient, and separation bounds for the values of the given game. These are given in Proposition 20. Furthermore, and also

based on Theorem 6, we can for a given ϵ give an explicit upper bound on the value of λ necessary for v^k_λ to approximate v^k within ϵ. This expression for such λ, given in Proposition 22, is of the form $\lambda_\epsilon = \epsilon^{\tau m^{O(N^2)}}$. Our algorithm proceeds simply by setting ϵ so small that an ϵ-approximation to the value allows an exact reconstruction of the value using Theorem 7. Such ϵ can be computed as we have derived degree and coefficient bounds for the value of the Gillette game at hand. We then run our previously constructed algorithm on the Shapley game Γ_λ, where $\lambda = \lambda_\epsilon$.

4 Degree and separation bounds for Stochastic Games

4.1 Shapley Games

Our bounds on degree, coefficient size, and separation for Shapley games are obtained by a reduction to the same question about isolated solutions of polynomial systems. The latter is treated in Section 5. In this section we present the reduction as well as stating the consequences obtained from this and Theorem 23 of Section 5. To analyse our reduction we also need the following simple fact.

Proposition 10 ([3], Proposition 8.12)**.** *Let M be an $m \times m$ matrix, whose entries are integer polynomials in variables $x_1, \ldots, x_n$ of degree at most d and coefficients of bitsize at most τ. Then $\det(M)$, as a polynomial in variables $x_1, \ldots, x_n$ is of degree at most dm and has coefficients of bitsize at most $(\tau + \mathrm{bit}(m))m + n\,\mathrm{bit}(md+1)$, where $bit(z) = \lceil \lg z \rceil$.*

Also, denote by $\mathrm{B}(v, \epsilon)$ the ball around $v \in \mathbb{R}^N$ of radius $\epsilon > 0$, $\{v' \in \mathbb{R}^N \mid \|v - v'\|_2 \leq \epsilon\}$. We are now in position to present the reduction.

Theorem 11. *Let Γ be a Shapley game, with N positions. Assume that in position k, the two players have m_k and n_k actions available. Assume further that all payoffs and probabilities in Γ are rational numbers with numerators and denominators of bitsize at most τ.*

Then there is a system $\mathcal{S}$ of polynomials in variables $v_1, \ldots, v_N$, for which the value vector v^* of Γ is an isolated root. Furthermore the system $\mathcal{S}$ consists of at most $\sum_{k=1}^{N} \binom{n_k+m_k}{m_k}$ polynomials, each of degree at most $m+2$ and having integer coefficients of bitsize at most $2(N+1)(m+1)^2\tau+1$, where $m = \max_{k=1}^{N} (\min(n_k, m_k))$.

Proof. Let $v^* \in \mathbb{R}^n$ be the fixpoint of T given by Theorem 4. For all positions k, and for all potential basis sets B^k corresponding to the parameterized matrix game A^k we consider the closures $\overline{O^{A^k}_{B^k}}$ of the sets $O^{A^k}_{B^k}$. Since there are finitely many positions and for each position finitely many potential basis sets, we may find $\epsilon > 0$ such that whenever $\mathrm{B}(v^*, \epsilon) \cap \overline{O^{A^k}_{B^k}} \neq \emptyset$ we have $v^* \in \overline{O^{A^k}_{B^k}}$ for all positions k and all potential basis sets B^k. For a given position k, let $\mathcal{B}^k$ be the set of such potential basis sets. Then, for every $B^k \in \mathcal{B}^k$ define the polynomial

$$P_{B^k}(w) = \det((M^{A^k(w)}_{B^k})_{m_k+1}) - w_k \det(M^{A^k(w)}_{B^k}) \ .$$

Let $\mathcal{P}$ be the system of polynomials consisting of all such polynomials for all positions k. We claim that v^* is an isolated root of the system $\mathcal{P}$. First we show that v^* is in fact a solution. Consider any position k and any polynomial $P_{B^k} \in \mathcal{P}$. By construction we have $v^* \in \overline{O^{A^k}_{B^k}}$, and we may thus find a sequence $(w^i)_{i=1}^{\infty}$ in $O^{A^k}_{B^k}$ converging to v^*. Since for every i, $w^i \in O^{A^k}_{B^k}$ we have that $\det((M_B^{A^k(w^i)})_{m+1}) - \mathrm{val}(A^k(w^i)) \det(M_B^{A(w^i)}) = 0$, and thus by continuity of the functions

det, val, and the entries of A^k, we obtain $\det((M_B^{A^k(v^*)})_{m+1}) - \mathrm{val}(A^k(v^*))\det(M_B^{A^k(v^*)}) = 0$. But $\mathrm{val}(A^k(v^*)) = v_k^*$ and hence $P_{B^k}(v^*) = 0$.

Next we show that v^* is unique. Indeed, suppose that $v' \in \mathrm{B}(v^*, \epsilon)$ is a solution to the system $\mathcal{P}$. For each position k pick a potential basis set B^k such that B^k describes an optimal bfs for $A^k(v')$. Now since $v' \in \mathrm{B}(v^*, \epsilon)$ as well as $v' \in O_{B^k}^{A^k}$ we have by definition that $B^k \in \mathcal{B}^k$ and hence $P_{B^k} \in \mathcal{P}$. As a consequence v' must be a root of P_{B^k}. Now, since B^k in particular is a basic solution we have $\det(M_{B^k}^{A^k(v')}) \neq 0$. Combining these two facts we obtain

$$v'_k = \det((M_{B^k}^{A^k(v')})_{m_k+1}) / \det(M_{B^k}^{A^k(v')}) \ ,$$

and since B^k is an optimal bfs for $A^k(v')$ we have that $\mathrm{val}(A^k(v'))_k = v'_k$. Since this holds for all k, we obtain that v' is a fixpoint of T, and Theorem 4 then gives that $v' = v^*$.

To get the system $\mathcal{S}$ we take (smallest) integer multiples of the polynomials in $\mathcal{S}$ such that all polynomials have integer coefficients. For a given position k, we have $\binom{n_k+m_k}{m_k}$ potential basis sets, giving the bound on the number of polynomials. Assume now that $m_k \leq n_k$ (In case $m_k > n_k$ we can consider the dual of the linear program in Lemma 3). Fix a potential basis set B^k.

Using Proposition 10 the degree of $P_{B^k}(w)$ is at most $1 + (m_k + 1)$. Further to bound the bitsize of the coefficients, note that using linearity of the determinant we may multiply each row of the matrices $(M_{B^k}^{A^k(w)})_{m_k+1}$ and $M_{B^k}^{A^k(w)}$ by the product of the denominators of all the coefficients of entries in the same row in the matrix $M_{B^k}^{A^k(w)}$. This product is an integer of bitsize at most $(N+1)(m_k+1)\tau$. Hence, doing this, both matrices will have entries where all the coefficients are integers of bitsize at most $(N+1)(m_k+1)\tau$ as well. Now by Proposition 10 again the bitsize of the coefficients of both determinants is at most

$$((N+1)(m_k+1)\tau + \mathrm{bit}(m_k))(m_k+1) + N\,\mathrm{bit}(m_k+2) \leq$$
$$2(N+1)(m_k+1)^2\tau$$

From this the claimed bound follow. □

We can now state the degree and separation bounds for Shapley games.

Proposition 12. *Let Γ be a Shapley game with N positions and m actions for each player in each position and all rewards and transition probabilities being rational numbers with numerators and denominators of bitsize at most τ, and let v be the value vector of Γ. Then, each entry of v is an algebraic number of degree at most $(2m+5)^N$ and the defining polynomial has coefficients of bitsize at most $21m^2N^2\tau(2m+5)^{N-1}$. Finally, if an entry of v is not an integer multiple of 2^{-j}, it differs from any such multiple by at least $2^{-22m^2N^2\tau(2m+5)^{N-1}-j(2m+5)^N-1}$.*

Proof. From Theorem 11 the value of Γ is among the isolated real solutions of a system of $\sum_{i=1}^{N}\binom{2m}{m} \leq 4^m$ polynomials, of degree at most $m+2$ and bitsize at most $2(N+1)(m+1)^2\tau+1 \leq 4Nm^2\tau$. Theorem 23 implies that the algebraic degree of the solutions is $(2(m+2)+1)^N = (2m+5)^N$ and the defining polynomial has coefficients of magnitude at most

$$2^{(8m^2N^2\tau+8Nm+5N\lg(m))(2m+5)^{N-1}} \leq 2^{21m^2N^2\tau(2m+5)^{N-1}} \ .$$

For a position k, let the defining polynomial be $A(v_k)$. To compute a lower bound on the difference between a root of A and a number 2^{-j}, it suffices to apply the map $v_k \mapsto v_k + 2^{-j}$ to A

and compute a lower bound for the roots of the shifted polynomial. The shifted polynomial also has degree $(2m+5)^N$, but its maximum coefficient bitsize is now bounded by $21m^2N^2\tau(2m+5)^{N-1} + j(2m+5)^N + 4\lg(2m+5)^N \leq 22m^2N^2\tau(2m+5)^{N-1} + j(2m+5)^N$. By applying Lemma 26 we get the result. □

4.2 Everett Games

Our bounds on degree, coefficient size, and separation for Everett games are obtained by a reduction to the more general results about the first-order theory of the reals.

Theorem 13. *Let Γ be an Everett game, with N positions. Assume that in position k, the two players have m_k and n_k actions available. Assume further that all payoffs and probabilities in Γ are rational numbers with numerators and denominators of bitsize at most τ.*

Then there is a quantified formula with N free variables that describes whether a vector v^* is the value vector of Γ. The formula has two blocks of quantifiers, where the first block consists of a single variable and the second block consists of $2N$ variables. Furthermore the formula uses at most $(2N+3) + 2(m+2)\sum_{k=1}^{N}\binom{n_k+m_k}{m_k}$ different polynomials, each of degree at most $m+2$ and having coefficients of bitsize at most $2(N+1)(m+2)^2\,\mathrm{bit}(m)\tau$, where $m = \max_{k=1}^{N}(\min(n_k, m_k))$.

Proof. By Theorem 5 we may express the value vector v^* by the following first-order formula with free variables v: $(\forall\epsilon)(\exists v_1, v_2)\ (\epsilon \leq 0) \vee (\|v - v_1\|^2 < \epsilon \wedge \|v - v_2\|^2 < \epsilon \wedge v_1 \in C_1(\Gamma) \wedge v_2 \in C_2(\Gamma))$. Here the expressions $v_1 \in C_1(\Gamma)$ and $v_2 \in C_2(\Gamma)$ are shorthands for the quantifier free formulas of polynomial inequalities implied by the definitions of $C_1(\Gamma)$ and $C_2(\Gamma)$. We provide the details below for the case of $C_1(\Gamma)$. The case of $C_2(\Gamma)$ is analogous. By definition $v_1 \in C_1(\Gamma)$ means $M(v_1) \succcurlyeq v_1$, which in turn is equivalent to $\wedge_{k=1}^{N}((\mathrm{val}(A^k(v_1)) > v_{1k} \wedge v_{1k} > 0) \vee (\mathrm{val}(A^k(v_1)) \geq v_{1k} \wedge (v_{1k} \leq 0)))$. Now we can rewrite the predicate $\mathrm{val}(A^k(v_1)) > v_{1k}$ to the following expression: $\vee_{B^k}((v_1 \in F_{B^k}^{A^k+} \wedge \det((M_{B^k}^{A^k(v_1)})_{m_k+1}) > v_{1k}\det(M_{B^k}^{A^k(v_1)}))) \vee ((v_1 \in F_{B^k}^{A^k-} \wedge \det((M_{B^k}^{A^k(v_1)})_{m_k+1}) < v_{1k}\det(M_{B^k}^{A^k(v_1)})))$, where the disjunction is over all potential basis sets, and each of the expressions $v_1 \in F_{B^k}^{A^k+}$ and $v_1 \in F_{B^k}^{A^k-}$ are shorthands for the conjunction of the m_k+1 polynomial inequalities describing the corresponding sets.

By a similar analysis as in the proof of Theorem 11 we get the following bounds, assuming without loss of generality that $m_k \leq n_k$: The predicates $v_1 \in F_{B^k}^{A^k+}$ and $v_1 \in F_{B^k}^{A^k-}$ can be written as a quantifier free formulas using at most m_k+1 different polynomials, each of degree at most m_k+2 and having coefficients of bitsize at most $2(N+1)(m_k+2)^2\,\mathrm{bit}(m_k)\tau$. Also, the predicate $\mathrm{val}(A^k(v_1)) > v_{1k}$ can be written as a quantifier free formula using at most $(m_k+2)\binom{n_k+m_k}{m_k}$ different polynomials, each of degree at most m_k+2 and having coefficients of bitsize at most $2(N+1)(m_k+2)^2\,\mathrm{bit}(m_k)\tau$.

Combining these further, for all positions we have the following statement (that shall be used also in our upper bound for strategy iteration for concurrent reachability games in Section 7).

Lemma 14. *The predicate $v_1 \in C_1(\Gamma)$ can be written as a quantifier free formula using at most $\sum_{k=1}^{N} 1 + (m+2)\binom{n_k+m_k}{m_k}$ different polynomials, each of degree at most $m+2$ and having coefficients of bitsize at most $2(N+1)(m+2)^2\,\mathrm{bit}(m)\tau$, where $m = \max_{k=1}^{N}(\min(n_k, m_k))$.*

From this the statement of the theorem easily follows. □

We shall also need the following basic statement about univariate representations.

Lemma 15. *Let α be a root of $f \in \mathbb{Z}[x]$, which is of degree d and maximum coefficient bitsize at most τ. Moreover, let $g(x) = p(x)/q(x)$ where $p, q \in \mathbb{Z}[x]$ are of degree at most d, have maximum coefficient bitsize at most τ, and $q(\alpha) \neq 0$. Then the minimal polynomial of $g(\alpha)$ is a univariate polynomial of degree at most $2d$ and maximum coefficient bitsize at most $2d\tau + 7d \lg d$.*

Proof. The minimal polynomial of $g(\alpha)$ is among the square-free factors of the following (univariate) resultant with respect to y:

$$r(x) = \mathrm{res}_y(f(y), q(y)x - p(y)) \in \mathbb{Z}[x].$$

The degree of r is bounded by d and its maximum coefficient bitsize is at most $2d\tau + 5d \lg d$ [3, Proposition 8.46]. Any factor of r has maximum coefficient bitsize at most $2d\tau + 7d \lg d$, due to the Landau-Mignotte bound, see, e.g., Mignotte [30]. □

We can now apply the machinery of semi-algebraic geometry to get the desired bounds on degree and the separation bounds.

Proposition 16. *Let Γ be an Everett game with N positions, m actions for each player in each position, and rewards and transition probabilities being rational numbers with numerators and denominators of bitsize at most τ, and let v be the value vector of Γ. Then, each entry of v is an algebraic number of degree at most $m^{O(N^2)}$ and the defining polynomial has coefficients of bitsize at most $\tau m^{O(N^2)}$. Finally, if an entry of v is not a multiple of 2^{-j}, it differs from any such multiple by at least $2^{-\max\{\tau, j\} m^{O(N^2)}}$.*

Proof. We use Theorem 14.16 (Quantifier Elimination) of Basu, Pollack and Roy [3] on the formula of Theorem 13 to find a quantifier free formula expressing that v is the value vector of the game. Next, we use Theorem 13.11 (Sampling) of [3] to this quantifier free formula to find a univariate representation of the value vector v satisfying the formula from Lemma 13. That is, we obtain polynomials $f, g_0, \ldots, g_{2N}$, with f and g_0 coprime, such that $v = (g_1(t)/g_0(t), \ldots, g_{2N}(t)/g_0(t))$, where t is a root of f. These polynomials are of degree $m^{O(N^2)}$ and their coefficients have bitsize $\tau m^{O(N^2)}$. We apply Lemma 15 to the univariate representation to obtain the desired defining polynomials. Finally, we obtain the separation bound using Lemma 26 in the same way as in the proof of Proposition 12 □

4.3 Gillette's Stochastic Games

Our bounds on degree, coefficient size, and separation for Gillette games are obtained, as in the case of Everett games but in a more involved way, by a reduction to the more general results about the first-order theory of the reals.

Theorem 17. *Let Γ be a Gillette game, with N positions. Assume that in position k, the two players have m_k and n_k actions available. Assume further that all payoffs and probabilities in Γ are rational numbers with numerators and denominators of bitsize at most τ.*

Then there is a quantified formula with N free variables that describes whether a vector v^* is the value vector of Γ. The formula has four blocks of quantifiers, where the first three blocks consists of a single variable and the fourth block consists of N variables. Furthermore the formula uses at most $4 + 2(m+2)\sum_{k=1}^{N} \binom{n_k+m_k}{m_k}$ different polynomials, each of degree at most $2(m+2)$ and having coefficients of bitsize at most $2(N+1)(m+2)^2 \,\mathrm{bit}(m)\tau$, where $m = \max_{k=1}^{N} (\min(n_k, m_k))$.

Proof. By Theorem 6 we may express the value vector v^* by the following first-order formula with free variables v.

$$(\forall \epsilon > 0)(\exists \lambda_\epsilon > 0)(\forall \lambda, 0 < \lambda \leq \lambda_\epsilon)(\exists v')(v' = \lambda \operatorname{val}(\Gamma_\lambda) \wedge \|v' - v\|^2 < \epsilon) \ .$$

Here Γ_λ is the $(1-\lambda)$-discounted version of Γ, and the expression $v' = \lambda \operatorname{val}(\Gamma_\lambda)$ is a shorthand for a quantifier free formula of polynomial equalities and inequalities expressing that v' is the normalized vector of values of Γ_λ, and may be expressed as

$$\bigwedge_{k=1}^{N} \left(\bigvee_{B^k} \left(\left(v' \in F_{B^k}^{A_\lambda^k +} \vee v' \in F_{B^k}^{A_\lambda^k -} \right) \wedge \det((M_{B^k}^{A_\lambda^k(v')})_{m_k+1}) = \lambda v'_k \det(M_{B^k}^{A_\lambda^k(v')}) \right) \right) \ ,$$

using Theorem 4 and where A_λ^k is the parameterized matrix game corresponding to Γ_λ obtained as explained in Section 2. Here, as in the last section, the disjunction is over all potential basis sets, and each of the expressions $v' \in F_{B^k}^{A_\lambda^k +}$ and $v' \in F_{B^k}^{A_\lambda^k -}$ are shorthands for the conjunction of the $m_k + 1$ polynomial inequalities describing the corresponding sets.

We next analyze the bounds in the following. By a similar analysis as in the proof of Theorem 13 and Theorem 11 we get the following bounds, assuming without loss of generality that $m_k \leq n_k$.

Lemma 18. *The predicates $v' \in F_{B^k}^{A_\lambda^k +}$ and $v' \in F_{B^k}^{A_\lambda^k -}$ can be written as a quantifier free formulas using at most $m_k + 1$ different polynomials, each of degree at most $2(m_k + 2)$ and having coefficients of bitsize at most $2(N+1)(m_k+2)^2 \operatorname{bit}(m_k)\tau$.*

The larger degree compared to the case of Everett games is due to the additional variable λ. The same is true for the remaining predicate, hence we obtain the following.

Lemma 19. *The predicate $v' = \lambda \operatorname{val}(\Gamma_\lambda)$ can be written as a quantifier free formula using at most $\sum_{k=1}^{N} (m+2)\binom{n_k+m_k}{m_k}$ different polynomials, each of degree at most $2(m+2)$ and having coefficients of bitsize at most $2(N+1)(m+2)^2 \operatorname{bit}(m)\tau$, where $m = \max_{k=1}^{N} (\min(n_k, m_k))$.*

From this the statement easily follows. □

Proceeding exactly as in the proof of Proposition 16, we may now prove the following proposition, giving the exact same statement for Gillette games as for Everett games. Note, however, that since more blocks of quantifiers have to be eliminated, the constants in the big-O's are likely worse.

Proposition 20. *Let Γ be a Gillette game with N positions, m actions for each player in each position, and payoffs and transition probabilities being rational numbers with numerators and denominators of bitsize at most τ, and let v be the value vector of Γ. Then, each entry of v is an algebraic number of degree at most $m^{O(N^2)}$, and the defining polynomial has coefficients of bitsize at most $\tau m^{O(N^2)}$. Finally, if an entry of v is not a multiple of 2^{-j}, it differs from any such multiple by at least $2^{-\max\{\tau, j\} m^{O(N^2)}}$.*

Next we will obtain a bound on the discount factor for guaranteeing a sufficient approximation of the undiscounted game by the discounted one. We will consider the same formula, strip away the first two quantifiers, replacing the variable ϵ by a fixed constant and letting λ_ϵ be a free variable. Next binding the previous free variables v and expressing that these take the values of the value vector of Γ we in effect obtain a first order formula expressing a sufficient condition for whether a given discount factor $\gamma = 1 - \lambda$ ensures that the values vectors of Γ and Γ_λ are ϵ-close in every coordinate.

Theorem 21. *Let Γ be a Gillette game, with N positions. Assume that in position k, the two players have m_k and n_k actions available. Assume further that all payoffs and probabilities in Γ are rational numbers with numerators and denominators of bitsize at most τ.*

Let $\epsilon = 2^{-j}$. Then there is a quantified formula with one free variable that gives a sufficient condition for whether a given discount factor $\gamma = 1 - \lambda_\epsilon$ guarantees that $\|\mathrm{val}(\Gamma) - \lambda_\epsilon \mathrm{val}(\Gamma_{\lambda_\epsilon})\|^2 \leq \epsilon$.

The formula has five blocks of quantifiers, where the first block consists of N variables, second of 1 variable, third and fourth of 2 variables and the fifth of $2N$ variables. Furthermore the formula uses at most $6 + 4(m+2)\sum_{k=1}^{N} \binom{n_k+m_k}{m_k}$ different polynomials, each of degree at most $2(m+2)$ and having coefficients of bitsize at most $\max\{j, 2(N+1)(m+2)^2 \,\mathrm{bit}(m)\tau\}$, where $m = \max_{k=1}^{N} (\min(n_k, m_k))$.

Proof. Following the proof of Theorem 17 above, we may express the condition by the following first-order formula with free variable λ_ϵ.

$$(\exists v)(\forall \lambda, 0 < \lambda \leq \lambda_\epsilon)(\exists v')(v' = \lambda \,\mathrm{val}(\Gamma_\lambda) \wedge \|v' - v\|^2 < \epsilon \wedge v = \mathrm{val}(\Gamma)) \ ,$$

and letting $v = \mathrm{val}(\Gamma)$ be a shorthand for the entire formula guaranteed by Theorem 17. We obtain the formula as claimed by converting the above formula into prenex normal form. The rest of the analysis follows closely the proof of Theorem 17 and is hence omitted. □

We can now apply again the machinery of semi-algebraic geometry to get a bound on λ_ϵ above as a function of ϵ.

Proposition 22. *Let Γ be a Gillette game with N positions, m actions for each player in each position, and payoffs and transition probabilities being rational numbers with numerators and denominators of bitsize at most τ, and let $\epsilon = 2^{-j}$. Then there exists $\lambda_\epsilon = \epsilon^{\tau m^{O(N^2)}}$, such that $\|\mathrm{val}(\Gamma) - \lambda_\epsilon \mathrm{val}(\Gamma_{\lambda_\epsilon})\|^2 \leq \epsilon$.*

Proof. First we use Theorem 14.16 (Quantifier Elimination) of Basu et al.[3] to the formula of Theorem 21 to obtain an equivalent quantifier free formula. The (univariate) polynomials in this formula are of degree $m^{O(N^2)}$ and has coefficients of bitsize $\max\{\tau, j\} m^{O(N^2)} = \log(1/\epsilon)\tau m^{O(N^2)}$. We can then again use Theorem 13.11 (Sampling) of [3], Lemma 15, and Lemma 26 to obtain the lower bound $\lambda_\epsilon = \epsilon^{\tau m^{O(N^2)}}$. □

5 Degree and separation bounds for isolated real solutions

In this section we prove general results about the coordinates of isolated solutions of polynomial systems. The result as stated below provides concrete bounds on the algebraic degree, coefficient size and separation.

Theorem 23. *Consider a polynomial system of equations*

$$(\Sigma) \qquad g_1(x_1, \ldots, x_n) = \cdots = g_m(x_1, \ldots, x_n) = 0 \ , \tag{2}$$

with polynomials of degree at most d and integer coefficients of magnitude at most 2^τ.

Then, the coordinates of any isolated *(in Euclidean topology) real solutions of the system are real algebraic numbers of degree at most $(2d+1)^n$, and their defining polynomials have coefficients*

of magnitude at most $2^{2n(\tau+4n\lg(dm))(2d+1)^{n-1}}$. *Also, if* $\gamma_j = (\gamma_{j,1}, \cdots, \gamma_{j,n})$ *is an isolated solution of* (Σ), *then for any* i, *either*

$$2^{-2n(\tau+2n\lg(dm))(2d+1)^{n-1}} < |\gamma_{j,i}| \quad or \quad \gamma_{j,i} = 0 \ . \tag{3}$$

Moreover, given coordinates of isolated solutions of two such systems, if they are not identical, they differ by at least

$$\mathrm{sep}(\Sigma) \geq 2^{-3n(\tau+2n\lg(dm))(2d+1)^{2n-1}-\frac{1}{2}\lg(n)} \ . \tag{4}$$

Before the proof of the theorem we will need to establish some preliminary results.

5.1 Isolated solutions, minimizers and the u-resultant

We will use ideas from [26] used for for global minimization of polynomial functions in order to reach an appropriate system to analyze. The solutions of the system (Σ), which consists of real polynomials of total degree at most d, are the minimizers of the polynomial

$$G(x_1, \ldots, x_n) = g_1(x_1, \ldots, x_n)^2 + \cdots + g_m(x_1, \ldots, x_n)^2 \tag{5}$$

in $\mathbb{R}^n$. Furthermore, if z is an isolated real solution of (Σ), then z is an isolated minimizer for (5). Let $G_i(\mathbf{x}) = \frac{\partial G(\mathbf{x})}{\partial x_i}$. The critical points of $G(\mathbf{x})$ are among the solution set of the system

$$G_1(\mathbf{x}) = \cdots = G_n(\mathbf{x}) = 0. \tag{6}$$

If the number solutions of the system above is finite, then we can use the multivariate resultant[1] [15, 9] to compute them. We homogenize the polynomials using a new variable x_0 and introduce the linear form $G_0 = u_0x_0 + u_1x_1 + \cdots + u_nx_n$. We then compute the multivariate resultant of $G_1, \ldots, G_n$ and G_0 with respect to the variables $x_0, x_1, \ldots, x_n$, and a homogeneous polynomial with degree equal to the product of the degrees of G_i is obtained. This is called the u-resultant [38], see also [9]. If the number of solutions is finite then the resultant is non-vanishing for almost all linear forms G_0, and if we factorize it to linear forms over the complex numbers then we can recover the solutions of the system.

To compute, or as in our case to bound, the ℓ-th coordinates of the solution set, we may assume $u_\ell = -1$ and $u_i = 0$, for all i different from 0 and ℓ. Then the u-resultant is a univariate polynomial in u_0, and its solutions correspond to the ℓ-th coordinates of the solutions of the system.

However, the multivariate resultant vanishes identically if the system has an infinite number of solutions. This is the case when the variety has positive dimension or, simply, the variety has a component of positive dimension at infinity, also known as *excess component*.

5.2 Gröbner bases and Deformations

First we recall the following fundamental results from the theory of Gröbner bases. Let k be a field and $R = k[x_1, \ldots, x_n]$. For an extension field $K \supset k$ and an ideal $I \subset R$ we let $V_K(I) := \{x \in K^n \mid f(x) = 0, \forall f \in I\}$.

[1] Following closely [9], for n homogeneous polynomials $f_1, \ldots, f_n$ in n variables $x_1, \ldots, x_n$, of degrees $d_1, \ldots, d_n$ respectively, the multivariate resultant is a single polynomial in the coefficient of f_i, the vanishing of which is the necessary and sufficient condition for the polynomials to have a common non-trivial solution in the algebraic closure of the field of their coefficients. The resultant is of degree $d_1d_2 \cdots d_{i-1}d_{i+1} \cdots d_n$ in the coefficients of f_i.

Lemma 24. *Consider an ideal $I \subset R$, such that $d := \dim_k R/I < \infty$.*

(i) If $(z_1, \ldots, z_n) \in V_K(I)$. Then $z_j \in K$ is algebraic over k of degree at most d.

(ii) Suppose that $I = (f_1, \ldots, f_n)$ with

$$\begin{aligned} f_1(\mathbf{x}) &= x_1^{d_1} + h_1(\mathbf{x}) \\ &\vdots \\ f_n(\mathbf{x}) &= x_n^{d_n} + h_n(\mathbf{x}), \end{aligned}$$

where $\deg(h_j) < d_j$. Then $\dim_k R/I = d_1 \cdots d_n$.

Here item (i) follows from the proof of Theorem 6, Chapter 5 of [14] (more precisely, the proof of (v) $\Rightarrow$ (i)). Item (ii) follows from Proposition 4, also from Chapter 5 of [14], noting that $(f_1, \ldots, f_n)$ is a Gröbner basis with respect to the graded lexicographic order.

Next, in order to apply the u-resultant as described above, we will symbolically *perturb* the system. We need to do it in such a way that the perturbed system becomes 0-dimensional and also that from the solutions of this perturbed system we can recover the isolated real solutions of the original system. In [26] the deformation

$$G_\lambda(x) = G(x) + \lambda(x_1^{2(d+1)} + \cdots + x_n^{2(d+1)}),$$

where $\lambda > 0$ is introduced. By Lemma 24(ii)

$$\dim_{\mathbb{R}} R/\nabla I(G_\lambda) \leq (2d+1)^n$$

for $\lambda > 0$, where $\nabla I(G)$ is the gradient ideal $(\frac{\partial G_\lambda}{\partial x_1}, \ldots, \frac{\partial G_\lambda}{\partial x_n})$. Let

$$X_\lambda = V(\nabla I(G_\lambda)) \subset \mathbb{R}^n.$$

Notice that $|X_\lambda| \leq \dim_k R/\nabla I(G_\lambda) = (2d+1)^n$. We wish to reason about the "limit" $L = \lim_{\lambda \to 0} X_\lambda$. To make this more precise we define

$$L = \{x \in \mathbb{R}^n \mid \forall \epsilon > 0\, \exists \lambda_\epsilon > 0 : B(x, \epsilon) \cap X_\lambda \neq \emptyset, \text{ for every } \lambda \,\text{with}\, 0 < \lambda < \lambda_\epsilon\}.$$

It is rather difficult to decide if a given point is in L. For one thing the polynomial system may have several bigger components not related to the limit. In our case, we have the following result, which allows us to recover the real solution if we solve the system in the limit, that is as $\lambda \to 0$.

Proposition 25. *If $z = (z_1, \ldots, z_n)$ is an isolated solution of (Σ), eq. (2), then $z \in L$.*

Proof. By the isolation of z there exists $\delta > 0$, such that $G(x) > 0$ for every $x \in B(z, \delta) \setminus \{z\}$. Therefore $m = \min\{G(x) \mid x \in \partial B(z, \delta)\} > 0$. Pick $\lambda > 0$ so that

$$G_\lambda(z) = \lambda(z_1^{2(d+1)} + \cdots + z_n^{2(d+1)}) < m$$

Since

$$m \leq \min\{G_\lambda(x) \mid x \in \partial B(z, \delta)\},$$

we know that the minimum of G_λ on $B(z, \delta)$ is attained in $B(z, \delta)^\circ$. Thus, $X_\lambda \cap B(z, \delta) \neq \emptyset$. $\square$

5.3 Proof of Theorem 23

For the proof of Theorem 23 we additionally need the following fundamental bounds.

Lemma 26. *[3, 30, 39] Let $f \in \mathbb{Z}[x]$ of degree d, then for any non-zero root γ it holds*

$$(2\|f\|_\infty)^{-1} \leq |\gamma| \leq 2\|f\|_\infty \ .$$

If $\operatorname{sep} f$ *is the separation bound, that is the minimum distance between the roots, then*

$$\operatorname{sep} f = \min_{i \neq j} |\gamma_i - \gamma_j| \geq d^{-(d+2)/2} \|f\|_2^{1-d} \ .$$

Proof of Theorem 23. Let $\gamma_j = (\gamma_{j,1}, \cdots, \gamma_{j,n})$ be isolated real solutions of the system (Σ). As above, we consider

$$G(x_1, \ldots, x_n) = g_1(x_1, \ldots, x_n)^2 + \cdots + g_m(x_1, \ldots, x_n)^2$$

and its pertubation

$$G_\lambda(x) = G(x) + \lambda(x_1^{2(d+1)} + \cdots + x_n^{2(d+1)}),$$

Form the system of partial derivatives

$$f_i = G_i + (2d+2)\lambda x_i^{2d+1} \ ,$$

where $G_i(\mathbf{x}) = \frac{\partial G(\mathbf{x})}{\partial x_i}$. We homogenize the polynomials using a new variable x_0 and introduce the linear form $u_0 x_0 + \cdots + u_n x_n$ specialized to the lth coordinate as describe above. That is we add the polynomial

$$f_0 = u x_0 - x_1$$

Let the resulting system be (Σ_0).

For a polynomial f, let $\mathcal{L}(f)$ be the maximum coefficient bitsize, that is $\mathcal{L}(f) = \lceil \lg \|f\|_\infty \rceil$. We have $\deg(G) \leq 2d$ and $\mathcal{L}(G) \leq 2\tau + 2n \lg(dm)$. Write G_i on the form

$$G_i(\mathbf{x}) = \sum_{j=1}^{2d-1} c_{i,j} \mathbf{x}^{a_{i,j}} \in \mathbb{Z}[\mathbf{x}],$$

where $1 \leq i \leq n$, and let $\mathbf{c}$ be the set of all coefficients $c_{i,j}$. It holds that $\deg(G_i) = 2d-1$, $\|G_i\|_\infty \leq 2d\|G\|_\infty$.

Let $D = (2d+1)^n$ and $D_1 = (2d+1)^{n-1}$. For the system (Σ_0) we consider the multivariate resultant R in the variables $x_0, x_1, \ldots, x_n$. It is a polynomial in the coefficients of G, u and λ, that is $R \in (\mathbb{Z}[\mathbf{c}, \lambda])[u]$, [15]. It has degree D_1 in the coefficients of G_i, where $1 \leq i \leq n$, and degree D in the coefficients of G_0, which are 1 and u. To be more specific, R is of the form

$$R = \cdots + \varrho_k \, u^k \, \widetilde{\mathbf{c}}_{1,k}^{D_1} \, \widetilde{\mathbf{c}}_{2,k}^{D_1} \cdots \widetilde{\mathbf{c}}_{n,k}^{D_1} + \ldots,$$

where $\varrho_k \in \mathbb{Z}$, and $\widetilde{\mathbf{c}}_{i,k}^{D_1}$ is of the form $\lambda^\mu {\mathbf{c}_{i,k}}^{D_1-\mu}$ where the second factor corresponds to a monomial in the coefficients c_{ij}, of total degree $D_1 - \mu$, for some μ smaller than D_1.

The lowest-degree nonzero coefficient of R, R_u, seen as univariate polynomial in λ, is a projection operator: it vanishes on the projection of any 0-dimensional component of the algebraic set defined

by (Σ_0) [9, 16, 18]. In our case the ℓ-th coordinates of the isolated solutions of (6) are among the roots of R_u.

It holds that $R_u \in \mathbb{Z}[\mathbf{c}][u]$, and $\deg(R_u) \leq D$. Notice that the bound on the degree of R_u, that is $D = (2d+1)^n$, is also an upper bound on the algebraic degree on the coordinates of the solutions of (2). Which proves the first assertion of the theorem.

To compute the bounds on the roots of R_u, and thus bounds on the isolated solutions of (6), we should bound the magnitude of its coefficients. For the latter, it suffices to bound the coefficients of R. Let

$$\|R\|_\infty \leq \max_k |\varrho_k \, {\mathbf{c}_{1,k}}^{D_1} \, {\mathbf{c}_{2,k}}^{D_1} \, \cdots {\mathbf{c}_{n,k}}^{D_1}| \leq \max_k |\varrho_k| \cdot \max_k |{\mathbf{c}_{1,k}}^{D_1} \, {\mathbf{c}_{2,k}}^{D_1} \, \cdots {\mathbf{c}_{n,k}}^{D_1}| = h \cdot C \ .$$

To bound ϱ_k we need a bound on the number of integer points of the Newton polygons of f_i [35], which we denote by $(\#Q_i)$. We refer to [18] for details. For all k we have

$$|\varrho_k| \leq h = (n+1)^D \prod_{i=1}^{n} (\#Q_i)^{D_1} \leq 2^{nD_1} D^{nD_1} \ .$$

Moreover

$$\max_k |{\mathbf{c}_{1,k}}^{D_1} \, {\mathbf{c}_{2,k}}^{D_1} \, \cdots {\mathbf{c}_{n,k}}^{D_1}| = \prod_{i=1}^{n} \|G_i\|_\infty^{D_1} \leq (d\|G\|_\infty)^{nD_1} = C \ .$$

Hence

$$\|R_u\|_\infty \leq \|R\|_\infty \leq hC = (2Dd\|G\|)^{nD_1} \leq 2^{2n(\tau+2n\lg(dm))(2d+1)^{n-1}} \ .$$

Using Cauchy's bound (Lemma 26) any of the non-zero roots $\gamma_{j,i}$ of R_u satisfies

$$|\gamma_{j,i}| > \|R_u\|_\infty^{-1} \geq (hC)^{-1} \geq 2^{-2n(\tau+2n\lg(dm))(2d+1)^{n-1}} \ .$$

Notice that the defining polynomial of $\gamma_{j,i}$ is the square-free part of R_u, which has bitsize at most $2n(\tau + 2n\lg(dm))(2d+1)^{n-1} + (2d+1)^{n-1} + 2\lg(2d+1)^{n-1} \leq 2n(\tau + 4n\lg(dm))(2d+1)^{n-1}$.

To bound the minimum distance between the isolated roots of (Σ), we notice that

$$\sqrt{n}\,\operatorname{sep}(\Sigma) \geq \sqrt{n} \min_{i\neq j} \|\gamma_i - \gamma_j\|_\infty \geq \min_{i\neq j} \|\gamma_i - \gamma_j\|_2 \geq \min_{i\neq j} |\gamma_{i,\ell} - \gamma_{j,\ell}|,$$

for any $1 \leq \ell \leq n$ and where the last minimum is considered over all $\gamma_{i,\ell} \neq \gamma_{j,\ell}$.

Using the separation bound for univariate polynomials (Lemma 26), we get

$$\operatorname{sep}(R_u) = \min_{i\neq j} |\gamma_{i,\ell} - \gamma_{j,\ell}| \geq D^{-\frac{D+2}{2}} \|R_u\|_2^{1-D} \geq D^{-\frac{D+2}{2}} (\sqrt{D}\|R_u\|_\infty)^{1-D},$$

and so

$$\operatorname{sep}(R_u) = \min_{i\neq j} |\gamma_{i,\ell} - \gamma_{j,\ell}| \geq 2^{-3n(\tau+2n\lg(dm))(2d+1)^{2n-1}} \ .$$

Finally

$$\operatorname{sep}(\Sigma) \geq \operatorname{sep}(R_u)/\sqrt{n} \geq 2^{-3n(\tau+2n\lg(dm))(2d+1)^{2n-1} - \frac{1}{2}\lg(n)} \ .$$

This completes the proof. □

Better bounds should be possible for the algebraic degree of Theorem 23, based for example on Oleinik-Petrovskii, Milnor-Thom's [31, 37] bound for the sum of Betti numbers of a set of real zeros of a polynomial system, or on improved estimates by Basu [2] on individual Betti numbers; see also [5]. This should lead to improved separation bounds, if used in conjunction with neat deformation techniques and bounds on parametric Gröbner basis, e.g. [5, 27], and/or bounds based on the Generalized Characteristic Polynomial and sparse multivariate resultants [10, 18]. Nevertheless, it is not possible to beat the single exponential nature of the bound, and only improvements in the constants involved are expected.

6 Degree lower bounds for values of Shapley games

In this section we give a construction of a Shapley game $\Gamma_{N,m}$ with $N+1$ positions each having at most m actions, such that the algebraic degree of the value of one of the positions is at least m^N.

Previously, Etessami and Yannakakis [20] gave a reduction from the so-called square-root sum problem to the quantitative decision problem of Shapley games. In fact from this reduction one can obtain a Shapley game with N positions where the algebraic degree of the value of one of the positions is $2^{\Omega(N)}$.

Our results below can be viewed as a considerable extension of this, showing how the number of actions can affect the algebraic degree. Comparing with the upper bound $m^{O(N)}$ shows that our result is close to optimal. The idea of the game we construct is very simple. The game consists of a dummy game position that just gives rise to a probability distribution over the remaining N positions. Each of the remaining N positions are by themselves independent Shapley games consisting of a single position with m actions. We will construct these N games in such a way that their values are independent algebraic numbers each of degree m. Then a suitable linear combination of these, corresponding to the probability distribution, will cause the dummy position to have a value which is an algebraic number of degree m^N.

Actually implementing this approach seems to bring significant challenges when $m > 2$. However using the powerful Hilbert's irreducibility theorem we are able to give a simple existence proof of a Shapley game with the properties as stated above. Next, we will also give an explicit proof of existence using elementary but more involved arguments.

6.1 The single position game

Let $\alpha_1, \ldots, \alpha_m > 0$ be arbitrary positive numbers and $0 \leq \beta < 1$. Consider the Shapley game $\Gamma(\alpha, \beta)$ consisting of a single position where each player has m actions, and the payoffs are $a_{ii} = \alpha_i$ and $a_{ij} = 0$ for $i \neq j$, and transition probabilities $p_{ii}^{11} = \beta$ and $p_{ij}^{11} = 0$ for $i \neq j$. Thus to $\Gamma(\alpha, \beta)$ corresponds the parameterized matrix game given by the diagonal matrix $\mathrm{diag}(\alpha_1+\beta v, \ldots, \alpha_m+\beta v)$.

By Theorem 4, and since the game is given by a diagonal matrix with strictly positive entries on the diagonal, we find that the value of the game v satisfies the equation

$$\sum_{i=1}^{m} \frac{v}{\alpha_i + \beta v} = 1 \ . \tag{7}$$

More precisely, consider a diagonal matrix game $\mathrm{diag}(a_1, \ldots, a_m)$ with strictly positive entries $a_1, \ldots, a_m > 0$ on the diagonal, and let p and q be optimal strategies for the row and column player, respectively, and let $v > 0$ be the value of the game. Firstly, all $p_i > 0$ as otherwise the column

player could ensure payoff 0 by playing strategy i. Thus $v = a_i q_i$ for all i, and hence also $q_i > 0$ for all i. But then similarly we have $v = a_i p_i$ for all i. Rearranging to $p_i = v/a_i$ and doing summation over i gives the claimed equation.

Define the polynomial $f_m(v) = \prod_{i=1}^{m}(\alpha_i + \beta v)$. Then $f'_m(v) = \beta \sum_{i=1}^{m} \prod_{j\neq i}(\alpha_j + \beta v)$. Multiplying by $f_m(v)$ on both sides of equation 7 we obtain the following.

$$f_m(v) = v \sum_{i=1}^{m} \prod_{j\neq i}(\alpha_j + \beta_j v) = \frac{1}{\beta} v f'_m(v) \ .$$

In the following we will specialize $\beta = 1/c$, for some $c > 1$. We then obtain that v is a root in the univariate polynomial

$$F_m(v) = f_m(v) - cv f'_m(v) \ .$$

6.2 Existence using Hilbert's irreducibility theorem

We next present the simple existence proof using (a version) of Hilbert's irreducibility theorem.

Lemma 27. *If $c > 1$ is rational, then*

$$F_m(v, \alpha_1^2, \ldots, \alpha_m^2) \in \mathbb{Q}[v, \alpha_1, \ldots, \alpha_m]$$

is irreducible as a multivariate polynomial in $v, \alpha_1, \ldots, \alpha_m$.

Proof. This uses induction on m. For $m = 1$ we have $F_1 = (1 + 1/c)v + \alpha_1^2$ which is irreducible in $\mathbb{Q}[v, \alpha_1]$. The induction step proceeds as follows.

$$\begin{aligned}
F_m = f_m - cv f'_m &= (\alpha_m^2 + \frac{1}{c}v) f_{m-1} - cv \frac{d}{dv}\left((\alpha_m^2 + \frac{1}{c}v) f_{m-1}\right) \\
&= f_{m-1}\alpha_m^2 + \frac{1}{c} v f_{m-1} - cv(\frac{1}{c} f_{m-1} + (\alpha_m^2 + \frac{1}{c}v) f'_{m-1}) \\
&= f_{m-1}\alpha_m^2 + \frac{1}{c} v f_{m-1} - v f_{m-1} - cv\alpha_m^2 f'_{m-1} - v^2 f'_{m-1} \\
&= (f_{m-1} - cv f'_{m-1})\alpha_m^2 + v((\frac{1}{c} - 1) f_{m-1} - v f'_{m-1}) \\
&= F_{m-1}\alpha_m^2 + v\left((1/c - 1) f_{m-1} - v f'_{m-1}\right).
\end{aligned}$$

If F_{m-1} is associated to $F := (\frac{1}{c} - 1) f_{m-1} - v f'_{m-1}$ in the polynomial ring $\mathbb{Q}[v, \alpha_1, \ldots, \alpha_{m-1}]$, then we would have $(\frac{1}{c} - 1) F_{m-1} = F$ leading to the contradiction $(\frac{1}{c} - 1)c = 1$. Since F_{m-1} is irreducible by induction, it follows that

$$\gcd(F_{m-1}, (1/c - 1) f_{m-1} - v f'_{m-1}) = 1$$

and therefore that

$$F_m = F_{m-1}\alpha_m^2 + v((1/c - 1) f_{m-1} - v f'_{m-1}) \in \mathbb{Q}[v, \alpha_1, \ldots, \alpha_{m-1}][\alpha_m]$$

is irreducible. □

We recall the following version of Hilbert's irreducibility theorem (see [22], Corollary 11.7) sufficient for our purposes.

Theorem 28 (Hilbert)**.** *Let K be a finite extension field of $\mathbb{Q}$ and $f \in K[x, y_1, \ldots, y_n]$ an irreducible polynomial. Then there exists $(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}^n$, such that*

$$f(x, \alpha_1, \ldots, \alpha_n) \in K[x]$$

is an irreducible polynomial.

We are now in position to show existence of the Shapley game $\Gamma_{N,m}$.

Theorem 29. *For any $N, m \geq 1$ there exists a Shapley game with $N+1$ positions each having m actions for each player, such that the value position $N+1$ in the game is an algebraic number of degree m^N.*

Proof. We shall construct the first N positions as independent Shapley games described as above. For the base case of $N = 1$, using Lemma 27 we simply invoke Theorem 28 on the polynomial $F_m(v, \alpha_1^2, \ldots, \alpha_m^2)$ with $c = 2$, say. This gives a specialization of $\alpha_1, \ldots, \alpha_m \in \mathbb{Q}$ such that the value of the game $\Gamma((\alpha_1^2, \ldots, \alpha_m^2), 1/2)$ is an algebraic number v_1 of degree m.

Now assume by induction that we have constructed $N-1$ single-position Shapley games with values $v_1, \ldots, v_{N-1}$ together with positive integer coefficients $k_1, \ldots, k_{N-1}$ such that $v' = k_1 v_1 + \cdots + k_{N-1} v_{N-1}$ is an algebraic number of degree m^{N-1}. Invoke Theorem 28 on the polynomial $F_m(v, \alpha_1^2, \ldots, \alpha_m^2)$ as before, but now over the extension field $\mathbb{Q}(v')$. This again gives a specialization of $\alpha_1, \ldots, \alpha_m \in \mathbb{Q}$ such that the value of the game $\Gamma((\alpha_1^2, \ldots, \alpha_m^2), 1/2)$ is an algebraic number v_N of degree m, but now over $\mathbb{Q}(v')$. We may now find a positive integer k such that $v' + k_N v_N$ is an algebraic number of degree $m^{N-1} m = m^N$ over $\mathbb{Q}$.

Now we may construct the $N+1$ position game as follows. Let $K = k_1 + \cdots + k_N$. In position $N+1$, regardless of the players actions, with probability $1/2$ the game ends, and with probability $1/2k_i$ the play proceeds in position i. No payoff is awarded. Clearly the value of position $N+1$ is exactly $(k_1 v_1 + \cdots + k_N v_N)/2$ and is thus an algebraic number of degree m^N. □

6.3 An explicit specialization

Write $E_k(\alpha) = E_k(\alpha_1, \ldots, \alpha_m)$ for the kth elementary symmetric polynomial in $\alpha_1, \ldots, a_m$ i.e.

$$E_k(\alpha) = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq m} \alpha_{i_1} \cdots \alpha_{i_k}$$

for $1 \leq k \leq m$. For notational convenience we define $E_0(\alpha) = 1$. We have not been able to find a reference in the literature for the following lemma. For a complete factorization of $S_k(x)$ we refer to Lemma 35.

Lemma 30. *Let $S_k(x) = E_k(1, x, \ldots, x^{m-1})$, where x is a variable. Then*

$$\gcd(S_1(x), \ldots, S_{m-1}(x)) = \Phi_m(x),$$

where Φ_m is the m-th cyclotomic polynomial.

Proof. Define

$$\begin{aligned} f(t,x) &= (t-1)(t-x)(t-x^2)\cdots(t-x^{m-1}) \\ &= t^m - S_1(x)t^{m-1} + \cdots + (-1)^{m-1}S_{m-1}(x)t + (-1)^m S_m(x). \end{aligned}$$

If ξ is a primitive m-th root of unity, then $f(t,\xi) = t^m - 1$ and therefore $S_j(\xi) = 0$ for $j = 1,\ldots,m-1$. If ξ is not a primitive m-th root of unity, then $f(t,\xi)$ has multiple roots showing that $S_j(\xi) \neq 0$ for some $j = 1,\ldots,m-1$. Thus the greatest common divisor of $S_1(x),\ldots,S_{m-1}(x)$ is the product of $(x-\xi)$, where ξ runs through the primitive m-th roots of unity. This polynomial is precisely Φ_m. □

We now derive the following formula for F_m giving the coefficients explicitly.

Lemma 31.

$$F_m(v) = \sum_{k=0}^{m} E_{m-k}(\alpha)(1-ck)(v/c)^k \ .$$

Proof. First we have

$$f_m(v) = \prod_{i=1}^{m}(a_i + v/c) = \sum_{k=0}^{m} E_{m-k}(\alpha)(v/c)^k \ ,$$

and thus

$$f'_m(v) = \sum_{k=0}^{m} E_{m-k}(\alpha)kv^{k-1}(1/c)^k \ .$$

We can then conclude

$$F_m(v) = \sum_{k=0}^{m} E_{m-k}(\alpha)((v/c)^k - cv(kv^{k-1}(1/c)^k)) = \sum_{k=0}^{m} E_{m-k}(\alpha)((1-ck)(v/c)^k) \ .$$

□

Lemma 32. *The polynomial*

$$F(v) = \sum_{k=0}^{m} E_{m-k}(\alpha)(1-ck)c^{m-k}v^k = c^m F_m(v) \ , \tag{8}$$

is irreducible for an infinite number of specializations of α and c.

Proof. We consider the polynomial $G(v) = v^m F(1/v)$. Obviously $F(v)$ is irreducible if and only if $G(v)$ is. Moreover, we let $\alpha_i = x^{i-1}$, for $1 \leq i \leq m$, for $x \in \mathbb{Z}_+$ to be specified in the sequel. By abuse of notation we also denote this polynomial as $G(v)$, which is

$$G(v) = \sum_{k=0}^{m} (1-(m-k)c)c^k \cdot S_k(x) \cdot v^k.$$

By Lemma 30 all the coefficients of $G(v)$, except the leading and the trailing coefficient, have $\Phi_m(x)$ as a common divisor. Now specialize to $x = \ell m$ with $\ell \gg 0$ and $\ell \in \mathbb{N}$. Let p be a prime

divisor in $\Phi_m(x)$. Then $p \nmid x$. There exists infinitely many $c \in \mathbb{N}$, such that $p \mid 1 - mc$, since $p \nmid m$. By possibly replacing c by $c + p$ we may assume that $1 - mc = bp$, where $p \nmid b$.

With this choice of c, $p \nmid c$ and p divides the constant term of $G(v)$ precisely once. Moreover, p is not a divisor of the leading coefficient of $G(v)$, which is $x^{m(m-1)/2}c^m$.

We conclude using Eisenstein's criterion (Theorem 36) all but that $G(v)$, and hence $F(v)$, is irreducible for this class of (infinite) specializations. □

Lemma 33. *Let $F_j(v)$ as in (8), i.e.*

$$F_j(v) = \sum_{k=0}^{m} E_{m-k}(a_{1j}, \ldots, a_{mj})(1 - c_j k)c_j^{m-k} v^k \ , \tag{9}$$

where $1 \leq j \leq n$. Let γ_j be any root of $F_j(v)$, then there is an infinite number of specializations of a_{ij} and c_j, such that

$$[\mathbb{Q}(\gamma_1, \ldots, \gamma_n) : \mathbb{Q}] = m^n.$$

Proof. We consider the specialization $a_{ij} = x^{i-1}$, where $1 \leq i \leq m$, $1 \leq j \leq n$, for a $x \in \mathbb{Z}_+$ to be specified in the sequel.

As before, we let $S_k(m) = E_k(1, x, \ldots, x^{m-1})$, and we perform the transformations $G_j(v) = v^m F_j(1/v)$, where $1 \leq j \leq n$, and we obtain the polynomials

$$G_j(v) = \sum_{k=0}^{m} (1 - (m-k)c_j)\, c_j^k \cdot S_k(m) \cdot v^k.$$

We pick a $x \in \mathbb{Z}_+$ so that $\Phi_m(x)$ has at least n distinct prime factors, $p_1, \ldots, p_n$, that are relative prime to m. For such a procedure we refer to Lemma 39. For $1 \leq j \leq n$, we choose c_j so that the equation $1 - mc_j = b_j p_j$ is satisfied for an integer b_j, and p_j is not a divisor of b_j.

All, but the leading and trailing, coefficients of G_j have $\Phi_m(x)$ as their common GCD, according to Lemma 30, and hence they are $0 \mod p_j$, for $1 \leq j \leq n$.

To summarize, for the n primes, p_j, it holds:

- None of them divides any of the leading coefficients of G_j.
- For each j, p_j divides the constant term of $G_j(v)$, p_j^2 does not, and p_j does not divide any of the constant term of the other polynomials.
- For all G_j, all the coefficients but the leading and the constant term, are divided by p_j.

Hence, according to Theorem 37, if γ_j is a root of G_j, then

$$[\mathbb{Q}(\gamma_1, \ldots, \gamma_n) : \mathbb{Q}] = m^n.$$

□

Lemma 34. *Let $F_j(v)$ as in (9), and let γ_j be any root of $F_j(v)$, then there is an infinite number of specializations of a_{ij} and c_j, such that for all but a finite number of $k_j \in \mathbb{Q}$, it holds*

$$[\mathbb{Q}(\gamma_1 + k_2\gamma_2 + \cdots + k_n\gamma_n) : \mathbb{Q}] = m^n \ ,$$

where $1 \leq j \leq n$.

Proof. The existence of k_i is guaranteed from the existence of primitive element [38]. That is for all but a finite number of values of $k_j \in \mathbb{Q}$ it holds $\mathbb{Q}(\gamma_1, \ldots, \gamma_n) = \mathbb{Q}(\gamma_1 + k_2\gamma_2 + \cdots + k_n\gamma_n)$, and from Lemma 33 we conclude for the degree.

To find explicit values for k_i we modify slightly the proof of the existence of primitive element [38]. Let γ_{ji} be all the roots of $F_j(v)$, where $1 \leq i \leq m$. It is without loss of generality to assume that $\gamma_i = \gamma_{j1}$.

Let $\beta_2 = \gamma_1 + k_2\gamma_2$. For $\mathbb{Q}(\beta_2) = \mathbb{Q}(\gamma_1, \gamma_2)$ to hold, it should be

$$k_2 \neq \frac{\gamma_{11} - \gamma_{1i}}{\gamma_{2\ell} - \gamma_{21}} \ ,$$

for all $1 \leq i \leq m$ and $1 < \ell \leq m$, and hence there are at most $(m-1)m$ forbidden values for k_2. This means that there is at least one positive integer between 0 and m^2, that we can assign k_2 to, so that $\mathbb{Q}(\gamma_1 + k_2\gamma_2) = \mathbb{Q}(\beta_2) = \mathbb{Q}(\gamma_1, \gamma_2)$.

If we let $\beta_3 = \beta_2 + k_3\gamma_3 = \gamma_1 + k_2\gamma_2 + k_3\gamma_3$, then for $\mathbb{Q}(\beta_3) = \mathbb{Q}(\gamma_1, \gamma_2, \gamma_3)$ to hold, it should be

$$k_3 \neq \frac{\beta_{21} - \beta_{2i}}{\gamma_{3\ell} - \gamma_{31}} = \frac{(\gamma_{11} - \gamma_{1,i_1}) + k_2(\gamma_{21} - \gamma_{2,i_2})}{\gamma_{3\ell} - \gamma_{31}} \ ,$$

for all $1 \leq i \leq m^2$, $1 < i_1 \leq m$, $1 < i_2 \leq m$ and $1 < \ell \leq m$. Hence there are at most $(m-1)m^2)$ forbidden values for k_3, and so there at least two integers between 0 and $(m-1)m + (m-1)m^2 = (m-1)^2 m$, that k_2 and k_3 could be assign to, so that $\mathbb{Q}(\beta_3) = \mathbb{Q}(\gamma_1, \gamma_2, \gamma_3)$.

We continue similarly, and eventually we let

$$\beta = \beta_n = \beta_{n-1} + k_n\gamma_n = \gamma_1 + k_2\gamma_2 + \cdots + k_n\gamma_n \ .$$

We consider

$$k_n \neq \frac{\beta_{n-1,1} - \beta_{n-1,i}}{\gamma_{n\ell} - \gamma_{n1}} = \frac{(\gamma_{11} - \gamma_{1,i_1}) + k_2(\gamma_{21} - \gamma_{2,i_2}) + \cdots + k_{n-1}(\gamma_{n-1,1} - \gamma_{n-1,i_{n-1}})}{\gamma_{n\ell} - \gamma_{n1}} \ ,$$

for all $1 \leq i \leq m^{n-1}$, $1 \leq i_\ell \leq m$, and $1 < \ell \leq m$. There are at $m^{n-1}(m-1)$ forbidden values for k_n.

Overall, there is at least $n-1$ integers between 0 and $m(m^{n-1}-1) \sim m^n$ that $k_2, \ldots, k_n$, could be assigned to, so that

$$\mathbb{Q}(\gamma_1, \ldots, \gamma_n) = \mathbb{Q}(\gamma_1 + k_2\gamma_2 + \cdots + k_n\gamma_n) \ .$$

Using the previous lemma we conclude for the degree. □

Now combining Lemma 33 and Lemma 34 we can immediately turn the proof of Theorem 29 into an explicit proof of existence.

6.3.1 Auxiliary results

A similar lemma appears in [36].

Lemma 35. *Let E_k be the elementary symmetric polynomials in n variables $a_1, \ldots, a_n$, where $0 \leq k \leq n$, that is $E_k(a_1, \ldots, a_n) = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} a_{i_1} \cdots a_{i_k}$.*

Let $S_k(n) = E_k(1, x, \ldots, x^{n-1})$, where $1 \le k \le n$, then it holds that

$$\begin{aligned} S_k(n) &= x^{k(k-1)/2} \prod_{\ell=1}^{k} (x^{n-\ell+1} - 1)/\Phi_\ell^{\lfloor k/\ell \rfloor}(x) \\ &= x^{k(k-1)/2} \prod_{i_1 | n} \Phi_{i_1}(x) \prod_{i_2 | (n-1)} \Phi_{i_2}(x) \cdots \prod_{i_k | (n-k+1)} \Phi_{i_k}(x) / \left(\prod_{\ell=1}^{k} \Phi_\ell^{\lfloor k/\ell \rfloor}(x) \right), \end{aligned}$$

where $\Phi_\ell = \Phi_\ell(x)$ is the ℓ-th cyclotomic polynomial.

Proof. We prove the formula using double induction.

Evidently the formula holds for $S_1(1)$, and we can easily prove that it holds for $S_1(n)$, for every n. It also holds for $S_k(k)$ for all k.

For the definition of the elementary symmetric polynomials it holds that $E_k(a_1, \ldots, a_n) = E_k(a_1, \ldots, a_{n-1}) + a_n E_{k-1}(a_1, \ldots, a_{n-1})$, and hence $S_k(n) = S_k(n-1) + x^{n-1} S_{k-}(n-1)$. We assume that the formula holds for $S_k(n-1)$ and $S_{k-1}(n-1)$ and we prove that it holds for $S_k(n)$.

$$\begin{aligned} S_k(n) &= S_k(n-1) + x^{n-1} S_{k-1}(n-1) \\ &= x^{k(k-1)/2} \prod_{\lambda=1}^{k} \frac{x^{n-\lambda} - 1}{\Phi_\lambda^{\lfloor k/\lambda \rfloor}} + x^{n-1} \cdot x^{(k-1)(k-2)/2} \prod_{\mu=1}^{k-1} \frac{x^{n-\mu} - 1}{\Phi_\mu^{\lfloor (k-1)/\mu \rfloor}} \\ &= x^{k(k-1)/2} \frac{\prod_{\lambda=1}^{k-1} (x^{n-\lambda} - 1)}{\prod_{\lambda=1}^{k} \Phi_\lambda^{\lfloor k/\lambda \rfloor}} (x^{n-k} - 1 + x^{n-k} \prod_{\mu | k} \Phi_\mu) \\ &= x^{k(k-1)/2} \frac{\prod_{\lambda=1}^{k-1} (x^{n-\lambda} - 1)}{\prod_{\lambda=1}^{k} \Phi_\lambda^{\lfloor k/\lambda \rfloor}} (x^{n-k} - 1 + x^{n-k} (x^k - 1)) \\ &= x^{k(k-1)/2} \prod_{\lambda=1}^{k} \frac{(x^{n-\lambda+1} - 1)}{\Phi_\lambda^{\lfloor k/\lambda \rfloor}}. \end{aligned}$$

The formula follows if we also consider that $x^n - 1 = \prod_{\ell | n} \Phi_\ell$. □

Theorem 36 (Eisenstein's criterion)**.** *Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients. Let p be a prime such that (i) p divides each a_i for $1 \le i < n$, (ii) p does not divide a_n, and (iii) p^2 does not divide a_0, then f is irreducible over the rational numbers.*

Theorem 37 (Generalized Eisenstein's criterion)**.** *[28] Let*

$$f_i(x) = x^{n_i} + a_{i,1} x^{n_i - 1} + \cdots + a_{i,n_i},$$

where $1 \le i \le s$ and all the coefficients of all the polynomials belong to O.

If there exists non-archimedean valuations $v_1, v_2, \ldots, v_s$ of K such that $t(v_1) = p_1, \ldots, t(v_s) = p_s$ are distinct primes, and that

$$v_i(a_{i,n_i}) = 1, \quad v_i(a_{j,n_j}) = 0, \text{ and } v_i(a_{k,r}) \ge 1,$$

where $1 \le i, j, k \le s$, $i \ne j$, $1 \le r \le n_k - 1$, then, for any choice of the roots of $f_i(x)$, say γ_i, $1 \le i \le s$, we have

$$[K(\gamma_1, \ldots, \gamma_s) : K] = n_1 n_2 \cdots n_s.$$

Remark 38 (A note on the leading coefficient)**.** *Theorem 37 is a generalization of Eisenstein's criterion. It assumes that all the polynomials are monic. However, it is without loss of generality to assume that the corresponding primes do not divide the leading coefficients. This is so because we can transform a non-monic polynomial to a monic one, such that the theorem holds, as follows: Given a polynomial*

$$g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_n \neq 1$*, we multiply all the coefficients by* a_n^{n-1} *then*

$$g_1(x) = a_n^n x^n + a_{n-1}a_n^{n-1}x^{n-1} + \cdots + a_n^{n-1}a_1 x + a_n^{n-1}a_0.$$

If we set $y = a_n x$*, then*

$$g_2(y) = y^n + a_{n-1}y^{n-1} + \cdots + a_n^{n-2}a_1 y + a_n^{n-1}a_0 = y^n + c_{n-1}y^{n-1} + \cdots + c_1 y + c_0$$

where in order Eisenstein's criterion, or its generalization, to hold, it suffices a prime p *not to divide the leading coefficient of* g*,* a_n*. If the roots of* g_2 *are* β_i*, then the roots of* g *are* $\gamma_i = \beta_i/a_n$*.*

Lemma 39. *Let* $f \in \mathbb{Z}[x]$ *be a non-constant polynomial and* a *an integer, such that* $f(a)$ *has the prime divisors* $p_1, \ldots, p_k$ *with* $k \geq 1$*. Then there exists an integer* b*, such that* $f(b)$ *is divisible by at least* $k+1$ *primes.*

Proof. We consider the polynomial

$$g(x) := f(f(a)^2 x + a) = f(a) + f(a)^2 x h(x) = f(a)(1 + f(a)xh(x)),$$

where $h(x) \in \mathbb{Z}[x]$ is non-zero. Notice that $g(x)$ is divisible by $p_1, \ldots, p_k$ for every $x \in \mathbb{Z}$. Now the result follows, since a prime dividing $1 + f(a)xh(x)$ for $x \in \mathbb{Z}$ cannot be among $p_1, \ldots, p_k$. □

7 Upper bounds for value and strategy iteration for concurrent reachability games

In this section we explain how the techniques of Section 4 as used for Everett games, also yields an improved analysis of the strategy improvement algorithm for concurrent reachability games.

Let Γ be an Everett game, with N positions. Assume that in position k, the two players have $m_k \leq m$ and $n_k \leq m$ actions available. Assume further that all payoffs and probabilities in Γ are rational numbers with numerators and denominators of bitsize at most τ. Further, let σ be a fixed positive integer.

From Lemma 14 we get the following statement.

Lemma 40. *There is a quantifier free formula with* $2N$ *free variables* v_1 *and* v_2 *that expresses* $v_1 \in C_1(\Gamma), v_2 \in C_2(\Gamma)$*, and* $\|v_1 - v_2\|^2 \leq 2^{-\sigma}$*.*

The formula uses at most $(2N+1) + 2(m+2)\sum_{k=1}^{N} \binom{n_k+m_k}{m_k}$ *different polynomials, each of degree at most* $m+2$ *and having coefficients of bitsize at most* $\max(\sigma, 2(N+1)(m+2)\tau)$*, where* $m = \max_{k=1}^{N}(\min(n_k, m_k))$*.*

Theorem 41. *Let* Γ *and* σ *be as above. Let* $\epsilon = 2^{-\sigma}$*. Then there exists* ϵ*-optimal strategy of* Γ *where each probability is a real algebraic number, defined by a polynomial of degree* $m^{O(N)}$ *and maximum coefficient bitsize* $\max(\sigma, \tau)m^{O(N)}$*.*

Proof. We use Theorem 13.11 of [3] to find a univariate representation of the pair (v_1, v_2) satisfying the formula from Lemma 40. That is we have polynomials $f, g_0, \ldots, g_{2N}$, with f and g_0 coprime, such that the points (v_1, v_2) are given as $(g_1(t)/g_0(t), \ldots, g_{2N}(t)/g_0(t))$, where t is a root of f. These polynomials are of degree $m^{O(N)}$ and their maximum coefficient bitsize is $\max(\sigma, \tau)m^{O(N)}$.

Now consider the matrix games $A^k(v_1)$ for all positions k. We find optimal strategies $p^1, \ldots, p^N$ that correspond to basic feasible solutions of the linear program LP (1). Notice that the elements of these matrix games are rational polynomial functions in $g_0, \ldots, g_N$. By Lemma 3 we have $p_i^k = \det((M_{B^k}^{A^k})_i)/\det(M_{B^k}^{A^k})$ for some potential basis sets $B^1, \ldots, B^k$. Using Lemma 10, each p_i^k is a rational polynomial function in $g_0, \ldots, g_N$ of degree $m^{O(N)}$ and maximum coefficient bitsize $\max(\sigma, \tau)m^{O(N)}$. Substituting the root t of f using Lemma 15 we obtain the statement. □

Using Lemma 26 we deduce:

Corollary 42. *An Everett game with coefficient bitsize bounded by τ has a $2^{-\sigma}$ optimal strategy where the probabilities are either zero or bounded from below by $2^{-\max(\sigma,\tau)m^{O(N)}}$.*

We now apply Lemma 3 of Hansen, Ibsen-Jensen and Miltersen [24] and conclude that value iteration and strategy iteration on a deterministic concurrent reachability game (where $\tau = O(1)$) will compute an ϵ-optimal strategy after at most $(\frac{1}{\epsilon})^{m^{O(N)}}$ iterations. This matches the lower bound obtained by Hansen, Ibsen-Jensen and Miltersen [24].

References

[1] D. Andersson and P.B. Miltersen. The complexity of solving stochastic games on graphs. In *Proc. of 20th ISAAC*, pages 112–121, 2009.

[2] S. Basu. Different bounds on the different Betti numbers of semi-algebraic sets. *Disc. & Comput. Geometry*, 30(1):65–85, 2003.

[3] S. Basu, R. Pollack, and M. Roy. *Algorithms in Real Algebraic Geometry.* Springer, 2nd edition, 2006.

[4] S. Basu and M. Roy. Bounding the radii of balls meeting every connected component of semi-algebraic sets. *J. Symb. Comp.*, 45:1270–1279, 2010.

[5] S. Basu and M. Roy. Bounding the radii of balls meeting every connected component of semi-algebraic sets. *J. Symb. Comp.*, 45(12):1270 – 1279, 2010. Special issue for MEGA'2009.

[6] D. Bertsimas and J.N. Tsitsiklis. *Introduction to Linear Optimization.* Athena Scientific, 1997.

[7] Truman Bewley and Elon Kohlberg. The asymptotic theory of stochastic games. *Mathematics of Operations Research*, 1(3):197–208, 1976.

[8] D. Blackwell and T.S. Ferguson. The big match. *Ann. Math. Statist.*, 39:159–163, 1968.

[9] J. Canny. *The Complexity of Robot Motion Planning.* ACM Doctoral Dissertation Award Series. MIT Press, 1987.

[10] J. Canny. Generalised characteristic polynomials. *J. Symb. Comp.*, 9(3):241–250, 1990.

[11] K. Chatterjee, L. de Alfaro, and T.A. Henzinger. Strategy improvement for concurrent reachability games. In *Third Int. Conf. on the Quant. Evaluation of Systems, QEST*, pages 291–300, 2006.

[12] K. Chatterjee, R. Majumdar, and T. Henzinger. Stochastic limit-average games are in EXPTIME. *Int. J. of Game Theory*, 37(2):219–234, 2008.

[13] A. Condon. The complexity of stochastic games. *Inf. and Comp.*, 96:203–224, 1992.

[14] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Springer-Verlag, New York, 1992.

[15] D. Cox, J. Little, and D. O'Shea. *Using algebraic geometry*, volume 185. Springer-Verlag, 1998.

[16] C. D'Andrea and I.Z. Emiris. Computing sparse projection operators. *Contemp. Math.*, 286:121–140, 2001.

[17] L. de Alfaro, T.A. Henzinger, and O. Kupferman. Concurrent reachability games. *Theor. Comput. Sci.*, 386(3):188–217, 2007.

[18] I.Z. Emiris, B. Mourrain, and E.P. Tsigaridas. The DMM bound: Multivariate (aggregate) separation bounds. In *Proc. ACM Int. Symp. on Symbolic & Algebraic Comp, ISSAC*, pages 243–250, 2010.

[19] K. Etessami and M. Yannakakis. Recursive concurrent stochastic games. In *Proc. of Int. Colloq. on Automata, Lang. and Prog., ICALP (2)*, volume 4052 of *LNCS*, pages 324–335. Springer, 2006.

[20] K. Etessami and M. Yannakakis. Recursive concurrent stochastic games. *Logical Methods in Comp. Sci.*, 4(4), 2008.

[21] H. Everett. Recursive games. In *Contributions to the Theory of Games Vol. III*, volume 39 of *Ann. Math. Studies*, pages 67–78. Princeton University Press, 1957.

[22] M.D. Fried and M. Jarden. *Field Arithmetic*. Springer-Verlag, New York, 1986.

[23] D. Gillette. Stochastic games with zero stop probabilities. In *Contributions to the Theory of Games III*, volume 39 of *Ann. Math. Studies*, pages 179–187. Princeton University Press, 1957.

[24] K.A. Hansen, R. Ibsen-Jensen, and P.B. Miltersen. The complexity of solving reachability games using value and strategy iteration. In *6th Int. Comp. Sci. Symp. in Russia, CSR*, LNCS. Springer, 2011.

[25] K.A. Hansen, M. Koucký, and P.B. Miltersen. Winning concurrent reachability games requires doubly exponential patience. In *Proc. of IEEE Symp. on Logic in Comp. Sci., LICS*, pages 332–341, 2009.

[26] B. Hanzon and D. Jibetean. Global minimization of a multivariate polynomial using matrix methods. *J. Global Optim.*, 27(1):1–23, 2003.

[27] G. Jeronimo and D. Perrucci. On the minimum of a positive polynomial over the standard simplex. *J. of Symb. Comp.*, 45(4):434 – 442, 2010.

[28] Z. Jian-Ping. On the degree of extensions generated by finitely many algebraic numbers. *J. Num. Theory*, 34(2):133 – 141, 1990.

[29] J.F. Mertens and A. Neyman. Stochastic games. *Int. J. of Game Theory*, pages 53–66, 1981.

[30] M. Mignotte. *Mathematics for Computer Algebra*. Springer-Verlag, New York, 1991.

[31] J. Milnor. On the Betti numbers of real varieties. *Proc. of the AMS*, 15(2):275–280, 1964.

[32] M. Orkin. Recursive matrix games. *J. App. Prob.*, 9(4):813–820, 1972.

[33] S.S. Rao, R. Chandrasekaran, and K.P.K. Nair. Algorithms for discounted games. *J. of Opt. Theory and App.*, pages 627–637, 1973.

[34] L.S. Shapley. Stochastic games. *Proc. Natl. Acad. Sci. U. S. A.*, 39:1095–1100, 1953.

[35] M. Sombra. The height of the mixed sparse resultant. *Amer. J. Math.*, 126:1253–1260, 2004.

[36] R.P. Stanley. *Enumerative Combinatorics: Volume 2*. Cambridge university press Cambridge;, 1999.

[37] R. Thom. Sur l'homologie des variétés algébriques réelles. *Differential and combinatorial topology*, pages 255–265, 1965.

[38] B.L. van der Waerden. *Modern Algebra*. F. Ungar Publishing Co., New York, 3rd edition, 1950.

[39] C. K. Yap. *Fundamental Problems of Algorithmic Algebra*. Oxford University Press, New York, 2000.