A Probabilistic Algorithm for Verification of Geometric Theorems

Mingyan Chen and Zhenbing Zeng(✉)

Department of Mathematics, Shanghai University, Shanghai 200444, China
yetibetan@sina.com, zbzeng@shu.edu.cn

Abstract. In this paper we combine the Schwartz-Zippel theorem with statistical inference theory and develop a new probabilistic algorithm instead of deterministic algorithms for geometry theorem proving. Our work includes an improved algorithm for estimating the upper bounds in the pseudo-remainder, and three selection criteria for statistical populations.

Keywords: Geometric theorems proving · Probabilistic algorithm · Selection criterion for statistical population · Statistical inference

1 Introduction

The common approaches of automated geometric theorem proving can be divided into three categories: algebraic methods, vector methods and search methods based on deductive database. Algebraic methods can be classified into two types, symbolic computation type which includes Wu's method [1,2], Gröbner bases method [3,4], resultant elimination method [5], etc.), and numerical computation type which includes the single-instance numerical verification method [6], and parallel numerical verification method [7,8,21,22]. All methods mentioned above belong to deterministic algorithms which will always get deterministic results if calculated by correct steps. However, when it comes to complicated problems, the complexity of deterministic algorithms can be very high which will seriously affect the efficiency of problem-solving. Thus, "probabilistic" algorithms (also called "non-deterministic" algorithms) are proposed which perform efficiently within a short time. Probabilistic algorithms have a wide range of applications in the field of computer algebra, such as prime number judgment and solving the largest invariant factor, etc. Probabilistic algorithms have two significant features: the algorithms are executed within the specified time and returning the computational results; the computational results may be incorrect but can control them within a small scope of 0. So the key question is that can we adopt a fast probabilistic algorithm instead of deterministic algorithms to improve the efficiency of geometric theorem proving?

This work is supported by the Project 11471209 of the National Natural Science Foundation of China.

D.-Z. Du et al. (Eds.): AAIM 2019, LNCS 11640, pp. 29–41, 2019.
https://doi.org/10.1007/978-3-030-27195-4_3

The answer is affirmative. In 1997, Carrá et al. [10] developed a probabilistic algorithm based on Schwartz-Zippel theorem [9] and Wu's method to prove constructive geometric theorems (see [1,2] for the definition) by verifying a number of random instances, the probability of incorrect result is also provided. They combined the bounds of the exponent of a polynomial in the radical of an ideal given by Brownawell and Kollar [11,12] with the bounds of the degree of Wu-Ritt's characteristic sets given by Gallo and Mishra [13,14] to estimate the upper bound about the total degree of the pseudo-remainder. The following is their research result. If a constructive geometric theorem (see Sect. 2) is constructed by C points and P circles or straight lines, then the bound calculated by their algorithm is $D = c \cdot 2^{C^3} 3^{C^3} C^{C^2}$ where c is a constant. Select N instances randomly from J where the J is a set of $2D$ different real number, then the probability that the result is correct is larger than $1 - 2^{-N}$ if the N instances all satisfy the geometric theorem. Unfortunately, this enormous bound D led Carrá et al. to fail to implement their algorithm on a computer. Besides, the extended characteristic sets and the pseudo-remainder are needed to be calculated if instance meets the degenerative conditions, which will increase the complexity of their algorithm inevitably.

Tulone et al. [15] proposed a probabilistic test for the vanishing of radical expression, and soon they developed the Core Library which was designed as a general C++ package and support the Exact Geometric Computation approach to robust algorithms. In 2001, they developed a geometry theorem prover based on probabilistic algorithm and the Core Library [16]. Their result can be summarized as follows.

Theorem 1. *Suppose $g(u, x)$ is the polynomial about the conclusion of a constructive geometric theorem with $\deg(g) = d$, and $G(u)$ be any of the 2^r radical expressions derived from $g(u, x)$ after eliminating dependent variables. If the theorem is constructed by k steps of ruler and compass constructions and $g(u, x)$ contains t terms, then $r \deg_u(G) \leq td2^r 85^k$ holds. Select the independent variables from J randomly, where J is a set formed by $td2^{c+2r}85^k (c \geq 1)$ real numbers, if the geometric theorem is false, then the probability that and the instance satisfies the theorem is at most 2^{-c}.* □

The above bound is much better, but when it comes to the class of non-linear constructive geometric theorems, the efficiency is still not satisfied. To refine the probabilistic algorithm of geometric theorems proving, we have improved the algorithm in this paper for estimating the upper bounds about the degrees of the pseudo-remainder in each independent variable, proposed three selection criteria for statistical population and apply two checking methods to verify instances, and designed a combined probabilistic checking model for mechanical geometry theorem proving on the basis of statistical error analysis and significance test.

This paper is organized as follows. In Sect. 2 we introduce the methods for representation of geometric theorems and related concepts of irreducible ascending sets. In Sect. 3 we give an improved algorithm to estimate the upper bounds of the pseudo-remainder. In Sect. 4 we introduce two checking methods for instances

verification and propose a new probabilistic algorithm for geometry theorem proving based on Schwartz-Zippel Theorem with three selection criteria for statistical population. In Sect. 5 we discuss the statistical error analysis and significance test.

2 Algebraic Representation of Geometry Theorems

It is well known that geometric theorems can be expressed as certain relations of algebraic equations using coordinates. For a large class of elementary geometric theorems, we can translate them into simple quadratic algebraic equations by adopting an appropriate coordinate system. A theorem is called a constructive geometric theorem if it is constructed according to some construction rules (e.g. ruler and compass constructions).

For a constructive geometric theorem, we can translate its hypotheses into a set of multivariate polynomial equations $H : \{f_i(u_1, u_2, \ldots, u_m, x_1, x_2, \ldots, x_n) = 0, i = 1, 2, \ldots, n\}$ and its conclusion is also a multivariate polynomial equation G: $g(u_1, u_2, \ldots, u_m, x_1, x_2, \ldots, x_n) = 0$ where $u_1, u_2, \ldots, u_m$ are independent variables (or parameters) and $x_1, x_2, \ldots, x_n$ are dependent variables, $f_1, f_2, \ldots, f_n$ and g are quadratic equations (i.e., the degree of each variable in each polynomial is not bigger than 2) in $Q(u_1, u_2, \ldots, u_m)[x_1, x_2, ..., x_n]$.

In what follows we use abbreviation $u = u_1, u_2, \ldots, u_m$, $x = x_1, x_2, \ldots, x_n$, $Q[u]$ denotes $Q[u_1, u_2, \ldots, u_m]$ and $Q(u)[x]$ the polynomial ring of $x_1, x_2, \ldots, x_n$ over the field of rational expressions $Q(u_1, u_2, \ldots, u_m)$.

A Maple package (EPSILON) developed by Wang in [17] can be used to translate a geometric theorem into algebraic form automatically by invoking the commands of `Load and Algebraic` in its submodule GEOTHER. The preparatory work is to formalize a geometric theorem as Theorem (H, G, X) where H is the hypotheses, G is the conclusion, and X is the set of dependent variables.

In general, the hypotheses H can be simplified into an equivalent ascending set (triangular form) by applying Wu-Ritt's algorithm, see [18–20]. Furthermore, based on the ascending set, following we will give the definition of irreducible ascending set as it plays an important role in this paper.

Definition 1. *If each polynomial f_i in an ascending set is irreducible in the ring $Q(u)[x_1, x_2, \ldots, x_i]/(f_1, f_2, \ldots, f_{i-1})$, then we'll call it an irreducible ascending set (IAS):*

$$IAS \begin{cases} f_1(u, x_1) = 0; \\ f_2(u, x_1, x_2) = 0; \\ \ldots \\ f_n(u, x_1, x_2, \ldots, x_n) = 0. \end{cases} \tag{1}$$

In order to describe the algebraic feature of the class of constructive geometric theorems as well as the linear class clearly, here we use the i-th element $D_f^{\,i}$ in the $n + m$-length array D_f to denote the degree of f in the i-th variable where $f \in Q_n(u)[x]$, and $m_f = \max\{D_f^{\,i}, 1 \le i \le m + n\}$. Define $Q_j(D)$ as a set of

specific polynomials and D^i denotes the i-th element in the n+m-length array D, for any $f \in Q_j(u)[x_1, x_2, \ldots, x_j]$, if f satisfies formula (2), then $f \in Q_j(D)$.

$$Q_j(D) = \{f \in Q_j | {D_f}^i \leq D^i, j = 1, 2, \ldots, m + j\} \tag{2}$$

For any constructive geometric theorem, each f_i in formula (1) satisfies either $D_{f_i}^{m+i} = 1, m_{f_i} \leq 2$ (suppose that there are l polynomials satisfy this condition, then $\frac{n}{2} \leq l \leq n$ will always hold) or $D_{f_i}^{m+i} = 2, m_{f_i} \leq 4$. If every polynomial f_i satisfies $D_{f_i}^{m+i} = 1$, then we call it a constructive geometric theorem of linear class.

3 Estimating the Degree Bounds for the Pseudo-remainder

Our goal in this section is to establish an algorithm of estimating the upper bounds of the degrees of the pseudo-remainder. We need the following result.

Theorem 2. *Let the i-th element $D_{g_j}^i$ in the $(m+j)$-length array D_{g_j} denote the degree of $g_j(u)[x_1, x_2, \ldots, x_j]$, in the i-th variable, then for any j-stage irreducible branch $\Re_j$ of formula (1), there exists a non-zero polynomial I on $\Re_j$ and*

$$g_{j-1}(u)[x_1, x_2, \ldots, x_{j-1}] \in Q_{j-1}(D_{f_j}^{m+j} D_{g_j} + D_{f_j}^{m+j} D_{g_j}^{m+j} D_{f_j}),$$

such that

$$I(u)[x_1, x_2, \ldots, x_j] \cdot g_j(u)[x_1, x_2, \ldots, x_j] = g_{j-1}(u)[x_1, x_2, \ldots, x_{j-1}] \tag{3}$$

holds on $\Re_j$, and $g_j \equiv 0$ on $\Re_j$ if and only if $g_{j-1} \equiv 0$. □

We refer the reader to the original paper [5] for the proof of this theorem. According to Theorem 2 and the n triangular polynomials in (1), we adopt inductive reasoning to deduce the following theorem.

Theorem 3. *Let the i-th element D_g^i in the $(m+n)$-length array D_g denote the degree of the i-th variable in the conclusion of a geometric theorem $g(u)[x]$, then for any n-stage irreducible branch $\Re$ of IAS (i.e., formula (1)) derived from its hypotheses, there exists a non-zero polynomial I on $\Re$ and $R \in Q_0(D_0)$, such that*

$$I(u)[x] \cdot g(u)[x] = R[u] \tag{4}$$

holds on $\Re$, and $g \equiv 0$ on $\Re$ if and only if $R \equiv 0$.

Proof. According to Theorem 2, for any n-stage irreducible branch $\Re_n$ of *IAS* (hypotheses) and conclusion $g(u)[x]$ of a given constructive geometric theorem, there exist a non-zero polynomial I_n on $\Re_n$ and $g_{n-1}(u)[x_1, x_2, ..., x_{n-1}] \in Q_{n-1}(D_{f_n}^{m+n} D_g + D_{f_n}^{m+n} D_g^{m+n} D_{f_n})$, such that

$$I_n(u)[x] \cdots g(u)[x] = g_{n-1}(u)[x_1, x_2, \ldots, x_{n-1}]$$

holds on $\Re_n$, and $g \equiv 0$ on $\Re_n$ if and only if $g_{n-1} \equiv 0$. Similarly, repeat applying Theorem 2 to eliminate the last i dependent variables, for any $(n-i+1)$-stage irreducible branch $\Re_{n-i+1}$ of IAS, there exists I_{n-i} and

$$g_{n-i}(u)[x_1, \ldots, x_{n-i}] \in Q_{n-i}(D_{f_{n-i+1}}^{m+n-i+1} D_{g_{n-i+1}} + D_{f_{n-i+1}}^{m+n-i+1} D_{g_{n-i+1}}^{m+n-i+1} D_{f_{n-i+1}}),$$

such that

$$g_{n-i} = I_{n-i} g_{n-i+1} = I_{n-i} I_{n-i+1} g_{n-i+1} = \ldots$$

$$= I_{n-i} I_{n-i+1} \cdots I_{n-1} g_{n-1} = I_{n-i} I_{n-i+1} \cdots I_n g$$

holds on $\Re_{n-i+1}$, and $g_{n-i+1} \equiv 0$ on $\Re_{n-i+1}$ if and only if $g_{n-i} \equiv 0$. Let $i = n$, i.e., have finished eliminating all the dependent variables, then for any 1-stage irreducible branch $\Re_1$ of IAS, there exists a non-zero polynomial I_1 and

$$g_0[u] \in Q_0(D_{f_1}^{m+1} D_{g_1} + D_{f_1}^{m+1} D_{g_1}^{m+1} D_{f_1}) = Q_0(D_0),$$

such that

$$g_0 = I_1 g_1 = I_1 I_2 g_2 = \ldots = I_1 I_2 \cdots I_n g$$

holds on $\Re_1$, and $g_1 \equiv 0$ on $\Re_1$ if and only if $g_0 \equiv 0$. Set $R = g_0$ and $I = I_1 I_2 \cdots I_n$, then $Ig = R$ holds. According to Theorem 2 and the recursive process of I and R, $g \equiv 0$ on $\Re$ if and only if $R \equiv 0$ holds. □

By Theorem 3 and the whole process of its proof, we can design the following algorithm to estimate the degrees of the polynomial R in every independent variables.

Algorithm 1. Estimate the upper bounds of the degrees of R in every independent variables.

Input: g, IAS, $ux = [u_1, u_2, \ldots, u_m, x_1, x_2, \ldots, x_n]$.

Output: An array D where the first m elements are the upper bounds of the degrees of R in every independent variables.

```
degreebounds:=proc(g, IAS, ux)
 n:=nops(IAS): m:=nops(ux)-n:
 D:=[seq(degree(G, op(i, ux)), i=1.. m+n)]:
  for i from n to 1 by -1 do
   FI:= IAS[i]: dFI:=[seq(degree(FI,op(j, ux)), j=1...m+n)]:
   D:=dFI[m+i]*D + dFI[m+i]*D[m+i]*dFI:
  end do:
 return D:
end proc:
```

By Theorem 3 and Algorithm 1, we have the following corollary.

Corollary 1. *If there are* $l(\frac{n}{2} \leq l \leq n)$ *polynomials in the irreducible ascending set IAS of a constructive geometric theorem satisfy* $\deg(f_i, x_i) = 1$, $m_{f_i} \leq 2$ *and* $n-l$ *polynomials satisfy* $\deg(f_i, x_i) = 2$, $m_{f_i} \leq 4$, *then* $\deg(R, u_i) \leq 2 \cdot 3^l 10^{n-l} \leq 2 \cdot 30^{n/2} (i = 1, 2, ..., m)$ *and* $T\deg(R) \leq 2m \cdot 3^l \cdot 10^{n-l} \leq 2m \cdot 30^{n/2}$ *hold, i.e., the upper bound of the degree of* R *in each independent variable is not bigger than* $2 \cdot 30^{n/2}$ *and the upper bound of the total degree of* R *is not bigger than* $2m \cdot 30^{n/2}$. *Furthermore, if limited to the linear class, then the bounds can still be improved to* $T\deg(R) \leq 2m \cdot 3^n$ *and* $\deg(R, u_i) \leq 2 \cdot 3^n (i = 1, 2, \ldots, m)$.

Proof. We first prove the conclusion that $\deg(g_{n-t}, u_i) \leq 2 \cdot 3^{l'} 10^{t-l'}$ $(i = 1, 2, \ldots, m)$ holds for $1 \leq t \wedge t \leq n$ where g_{n-t} is derived by eliminating the last t dependent variables in g and l' denotes the number of polynomials that satisfy $D_{f_i}^{m+i} = 1$ in the last t polynomials of *IAS*. We use mathematical induction to prove the above conclusion.

When $h = 1$, i.e., we can eliminate the last independent variable x_n with f_n, then $g_{n-1} \in Q_{n-1}(D_{f_n}^{m+n} D_g + D_{f_n}^{m+n} D_g^{m+n} D_{f_n})$ holds according to Theorem 2. If $D_{f_n}^{m+n} = 1$, then $l' = 1$, $D_{f_n}^j \leq 2 (j = 1, 2, \ldots, m+n)$ holds. Since $D_g^m \leq 2$, then $D_{g_{n-1}}^i \leq D_{f_n}^{m+n} \cdot \max\limits_{1 \leq j \leq m} (D_g^j) + D_{f_n}^{m+n} \cdot \max\limits_{1 \leq j \leq m} (D_g^j) \cdot \max\limits_{1 \leq j \leq m} (D_{f_1}^j) = 1 \cdot 2 + 1 \cdot 2 \cdot 2 = 2 \cdot 3^{l'} \cdot 10^{1-l'}$ holds where $1 \leq i \leq m$, i.e., the conclusion holds. On the other hand, if $D_{f_n}^{m+n} = 2$, then $l' = 0, D_{f_n}^j \leq 4 (j = 1, 2, \ldots, m)$ holds. Similarly, the conclusion holds. Suppose that when $h = t (1 \leq t < n)$ the conclusion holds, following we will prove when $h = t + 1$ the conclusion also holds. According to Theorem 3, after eliminating x_{n-t} with f_{n-t}, $g_{n-t-1} \in Q_{n-t-1}(D_{f_{n-t}}^{m+n-t} D_{g_{n-t}} + D_{f_{n-t}}^{m+n-t} D_{g_{n-t}}^{m+n-t} D_{f_{n-t}})$ holds obviously. If $D_{f_{n-t}}^{m+n-t} = 1$, then $l' = l' + 1, D_{f_{n-t}}^j \leq 2 (j = 1, 2, \cdot, m)$ holds. Since $h = t$ the conclusion holds, then we have $D_{g_{n-t}}^i \leq 2 \cdot 3^{l'-1} 10^{t-l'-1} (i = 1, 2, \cdot, m)$ holds, now we can derive the upper bound of g_{n-t-1} as follows, $D_{g_{n-t-1}}^i \leq D_{f_{n-t}}^{m+n-t} \cdot \max\limits_{1 \leq j \leq m} (D_{g_{n-t}}^j) + D_{f_{n-t}}^{m+n-t} \cdot \max\limits_{1 \leq j \leq m} (D_{g_{n-t}}^j) \cdot \max\limits_{1 \leq j \leq m} (D_{f_{n-t}}^j) = 1 \cdot 2 \cdot 3^{l'-1} 10^{t-l'-1} + 1 \cdot 3^{l'-1} 10^{t-l'-1} \cdot 2 = 2 \cdot 3^{l'} \cdot 10^{t+1-l'}$, by this the conclusion holds obviously. If $\deg(f_{n-t}, x_{n-t}) = 2$, then $l' = l', D_{f_{n-t}}^{m+n-t} = 2, D_{f_{n-t}}^j \leq 4 (j = 1, 2, \cdot, m)$ holds, similarly, the conclusion also holds. That is, we have proven that the conclusion will also hold for $h = t + 1$ if $h = t$ the conclusion holds. By mathematical induction, the above conclusion holds for $1 \leq t \wedge t \leq n$. By Theorem 3, after eliminating all the dependent variables we will obtain a polynomial g_0 where $g_0 = R$. If there are l polynomials in *IAS* satisfy $\deg(f_i, x_i) = 1$, then claims that $\deg(R, u_i) \leq 2 \cdot 3^l 10^{n-l} (i = 1, 2, \cdot, m)$ holds obviously by the above conclusion. Since there are m independent variables in R and their degrees are not bigger than $2 \cdot 3^l 10^{n-l}$, so $T\deg(R) \leq 2m \cdot 3^l 10^{n-l}$ holds. Moreover, if limited to the linear class, i.e., every polynomials in *IAS* satisfy $\deg(f_i, x_i) = 1$, so $l = n$. Substitute $l = n$ into $\deg(R, u_i) \leq 2 \cdot 3^l 10^{n-l} (i = 1, 2, \ldots, m)$, the conclusion $\deg(R, u_i) \leq 2 \cdot 3^n (i = 1, 2, ..., m)$ holds immediately, similarly, $T\deg(R) \leq 2m \cdot 3^n$ also holds, i.e., Corollary 1 holds. □

Corollary 1 shows that, if the *IAS* of a constructive geometric theorem contains n polynomials, then the upper bound of the degree of R in each independent variable is at most $B = 2 \cdot 3^l 10^{n-l}$. The bound can be improved to $2 \cdot 3^n$ if limited to the linear class. For constructive geometric theorems, l always satisfies $\frac{n}{2} \leq l \leq n$, so the bound can generalized as $\deg(R, u_i) \leq 2 \cdot 30^{n/2}$. That is, for a constrictive geometric theorem, its bounds B_1 satisfy $B_1 \leq 2 \cdot 30^{n/2}$, and for the linear class, the bounds B_2 can be improved to $B_2 \leq 2 \cdot 3^n$.

4 Probabilistic Estimates of Truth and Selection Criteria For statistical Population

Many geometric theorems can be transformed into the following form of conjunct logic relationship:

$$(\forall u, x)[(f_1 = 0 \wedge f_2 = 0 \wedge \ldots \wedge f_n = 0) \Rightarrow (g = 0)] \tag{5}$$

Thus, if a geometric theorem is true, then we can claim that remainder R (obtained in Theorem 3) is identically zero. It is certain that we can prove a theorem by calculating R from *IAS* and g according to Theorem 3 and then checking whether $R \equiv 0$ holds. We can also avoid calculating R directly via estimating the degrees of R by using Corollary 1. Then the key question is how to judge whether an instance satisfies the geometric theorem. Two kinds of checking methods are given in [6].

Checking Method 1: Numerical checking method, which uses a specific numerical instance to check whether $R \equiv 0$ holds. By Theorem 3, $g \equiv 0$ on $\Re$ if and only if $R \equiv 0$, i.e., for any $\tilde{u} = \tilde{u}_1, \tilde{u}_2, \ldots, \tilde{u}_m$ and $\tilde{x} = \tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_n$ satisfy formula (1), if $I(\tilde{u})[\tilde{x}] \neq 0$, then $g(\tilde{u})[\tilde{x}] = 0$ holds generically. The following steps show the checking process: (1)Select a numerical instance $\tilde{u} = \tilde{u}_1, \tilde{u}_2, \ldots, \tilde{u}_m$ randomly from the statistical population; (2) Substitute $\tilde{u}$ into the *IAS*, solve all the numerical solutions of the dependent variables $\tilde{x} = \tilde{x}_1, \tilde{x}_2, \ldots, \tilde{x}_n$; (3) Substitute $\tilde{u}$ and $\tilde{x}$ into the conclusion polynomial g, if $g(\tilde{u})[\tilde{x}] = 0$, then claims $R[\tilde{u}] = 0$, i.e., this instance satisfies the geometric theorem; if the dependent variables cannot be determined, which indicates that $I(\tilde{u})[\tilde{x}] = 0$ holds, according to formula (4), $R[\tilde{u}] = 0$ still holds. (4) If the instance does not satisfy $g(\tilde{u})[\tilde{x}] = 0$, i.e., $g(\tilde{u})[\tilde{x}] = 0$ does not hold, then claims that R is not identically zero, i.e., the geometric theorem is not true absolutely.

Checking Method 2: Successive pseudo division checking method which means that do not solve the numerical solutions about the dependent variables after substituting $\tilde{u}$ into the *IAS* but calculates R according to the instantiated *IAS* and g by formula (4) by using successive pseudo division algorithm. If $R = 0$, then claims that this instance satisfies the geometric theorem and the geometric theorem is true generically, else claims that the geometric theorem is false absolutely.

Remark. More rigorously, a geometric theorem may be expressed as the following conjunct logic relationship with non-degenerate conditions.

$$(\forall u, x)[(f_1 = 0 \wedge f_2 = 0 \wedge \ldots \wedge f_n = 0, \Delta_1, \Delta_2, \ldots, \Delta_k) \Rightarrow (g = 0)], \quad (6)$$

where $\Delta_1, \Delta_2, \ldots, \Delta_k$ denote the algebraic form of non-degenerate cases. Non-degenerate cases can be divided into two kinds: $\Delta \neq 0$ and $\Delta > 0$. Almost all prover now available can only deal with the first kind non-degenerate cases, following we also discuss the first kind of non-degenerate cases only.

As the results obtained by probabilistic algorithms are not always true, it is very essential to make probabilistic algorithms more reliable by providing the probability that the result is true (or false).

Randomization procedure is an essential part of our probabilistic algorithm, which means that instances should be randomly selected from the statistical population while checking. If a random instance does not match with the theorem, then the program will terminate and return the running result that the theorem is false, and the probability that the result is incorrect is 0. If N instances all match with the theorem, then the program will return a running result that the theorem is true. If R is not identically zero and all the N random instances are the zeros of R, then the running result will be incorrect. Can we control and obtain the upper bound of the probability that the result is incorrect? To solve this problem, we first introduce the famous Schwartz-Zippel Theorem proposed by Schwartz in 1980 [9] by which the upper bound of the number of the zeros of a nonzero polynomial in a specific sets can be determined.

Theorem 4. *Suppose that $G \in F[x_1, x_2, ..., x_n]$ and G is not identically zero. Let G_1 be the standard simplified form of G and d_1 be the degree of G_1 in x_1, G_2 be the coefficient of x_1^d in G_1. Then, inductively, let d_i be the degree of G_i in x_i and G_{i+1} be the coefficient of $x_i^{d_i}$ in G_i where $1 \leq i \leq n$.For any $x_i (1 \leq i \leq n)$, if $x_i \in I_i$ (here, $I_i \subset F$ and $|I_i| < d_i$), then in the set $I_1 \times I_2 \times \ldots \times I_n$, G has at most*

$$|I_1 \times I_2 \times \ldots \times I_n| \left(\frac{d_1}{|I_1|} + \frac{d_2}{|I_2|} + \ldots + \frac{d_n}{|I_n|} \right) \quad (7)$$

zeros. □

The following corollary is obtained immediately from Schwartz-Zippel Theorem.

Corollary 2. *Suppose that $G \in Q[x_1, x_2, \ldots, x_n]$ and G is not identically zero. If $x_1, x_2, \ldots, x_n$ are picked randomly from I where $I \subset Q$, then the probability that G is not identically zero in at most $\frac{d}{|I|}$, here d denotes the total degree of G and $|I| < d$.* □

Together with Algorithm 1, Schwartz-Zippel Theorem enables us to estimate the upper bound of the probability that the result is incorrect. In the rest of this section, we will propose three selection criteria for statistical population according to the Schwartz-Zippel Theorem and Corollary 2.

The First Selection Criterion. Select $c \times m \times d_i$ distinct positive integers to form a finite set U_i, e.g., $U_i = (1, 2, \ldots, cmd_i)$ where c is a positive integer and $i = 1, 2, \ldots, m$. Then an instance (called individual in statistical terminology) is formed by selecting an element from each U_i. Statistical population $S1$ is made up of all the instances, i.e., $S1 = U_1 \times U_2 \times \ldots \times U_m$, then the statistical population size $\# S1$ equal to the number of instances (individuals), i.e., $\# S1 = c^m m^m \prod_{i=1}^{m} d_i$. If R is not identically zero, then according to Theorem 4 we have:

$$|U_1 \times U_2 \times \ldots \times U_m| \left(\frac{d_1}{|U_1|} + \frac{d_2}{|U_2|} + \ldots + \frac{d_m}{|U_m|} \right)$$
$$= (cm)^m \prod_{i=1}^{m} d_i \cdot \left(\frac{d_1}{cmd_1} + \frac{d_2}{cmd_2} + \ldots + \frac{d_m}{cmd_m} \right) = c^{m-1} m^m \prod_{i=1}^{m} d_i \qquad (8)$$

By formula (8), we can claim that the number of instances in $S1$ that are zeros of R is at most $c^{m-1} m^m \prod_{i=1}^{m} d_i$. Therefore, the probability that the instance $\tilde{u} = \tilde{u}_1, \tilde{u}_2, \ldots, \tilde{u}_m$ selected randomly from $S1$ satisfies $R[\tilde{u}] = 0$ can be deduced as follows:

$$\text{Prob1}(R[\tilde{u}] = 0 | R \neq 0) \leq \frac{c^{m-1} m^m \prod_{i=1}^{m} d_i}{\# S1} = \frac{c^{m-1} m^m \prod_{i=1}^{m} d_i}{c^m m^m \prod_{i=1}^{m} d_i} = c^{-1} \qquad (9)$$

That is, if a geometric theorem is not true, then the probability that $R[\tilde{u}] = 0$ is at most c^{-1}, where $\tilde{u} = \tilde{u}_1, \tilde{u}_2, \ldots, \tilde{u}_m$ is an instance selected randomly from the statistical population $S1$.

The Second Selection Criterion. Let $D = \sum_{i=1}^{m} d_i$ where $d_1, d_2, \ldots, d_m$ are calculated by Algorithm, it is easy to see that the total degree of R in all the independent variables is at most D. Select cD distinct positive integers to form a finite set U, e.g., $U = (1, 2, \ldots, cD)$ where c is also a positive integer. Similarly, we obtain the statistical population: $S2 = \underbrace{U \times U \times \ldots \times U}_{\text{the number of } U \text{ is } m}$, and its size $\# S2$ as following:

$$\# S2 = c^m D^m = c^m (\sum_{i=1}^{m} d_i)^m = c^m m^m (\sum_{i=1}^{m} d_i \ / \ m)^m = c^m m^m (\bar{d})^m \qquad (10)$$

Repeat m times that select an element from U randomly can form an random instance $\tilde{u} = \tilde{u}_1, \tilde{u}_2, \ldots, \tilde{u}_m$, if R is not identically zero, then the probability that $R[\tilde{u}] = 0$ satisfies the following formula:

$$\text{Prob2}(R[\tilde{u}] = 0 | R \neq 0) \leq \frac{D}{\# U} = \frac{D}{cD} = c^{-1} \qquad (11)$$

according to Corollary 2, which implies that, if a geometric theorem is not true, then the probability that $R[\tilde{u}] = 0$ is at most c^{-1}, where $\tilde{u}$ is an instance selected randomly from the statistical population $S2$.

The Third Selection Criterion. As indicated in Corollary 1, if the *IAS* of a geometric theorem contains n polynomials, then the upper bounds satisfy $\deg(R, u_i) \leq 2 \cdot 3^l 10^{n-l} \leq 2 \cdot 30^{n/2} (i = 1, 2, \ldots, m)$. In other words, if the *IAS* is too difficult to calculate, then the upper bounds can still be estimated quickly in accordance with Corollary 1. Let $d_i = 2 \cdot 30^{n/2}$ and $D = \sum_{i=1}^{m} d_i = 2m \cdot 30^{n/2}$, then the statistical population $S3$ can be obtained in accordance with Corollary 2 and its size as following:

$$\# \ S3 = c^m D^m = c^m (2m \cdot 30^{n/2})^m = 2^m c^m m^m 30^{nm/2} \tag{12}$$

Similarly, the probability that $R[\tilde{u}] = 0$ is at most c^{-1} if the geometric theorem is false and $\tilde{u}$ is selected randomly from $S3$, i.e.,

$$\text{Prob3}(R[\tilde{u}] = 0 | R \neq 0) \leq c^{-1}.$$

5 Statistical Error Analysis and Significance Test

In this section, we compare the three selection criteria for statistical population, and then discuss statistical error analysis and significance test of our method. We have seen that all three selection criteria satisfy $\text{Prob}(R[\tilde{u}] = 0 | R \neq 0) \leq c^{-1}$, which means that, if a geometric theorem is false, then the probability of the checking result that theorem is true is at most c^{-1}. Their main differences lie in the value ranges of the instances and the statistical populations sizes.

If the statistical population is collected by the first selection criterion, then the statistical population size is $\# \ S1 = c^m \cdot m^m \prod_{i=1}^{m} d_i$. The second selection criterion can determine $S2$ and $\# \ S2 = c^m m^m (\bar{d})^m$. And therefore,

$$P = \frac{\# \ S1}{\# \ S2} = \frac{c^m m^m \prod_{i=1}^{m} d_i}{c^m m^m (\bar{d})^m} = \frac{d_1 d_2 \ldots d_m}{(\sum_{i=1}^{m} d_i \ / \ m)^m} \leq 1 \tag{13}$$

where m, c, $d_i (1 \leq i \leq m)$ are all positive integers. By formula (13)shows that adopting the first selection criterion to collect statistical population will more precise than the second one. Moreover, the complexity of the algorithm will decrease with the refined statistical population and more compact value ranges of instances, thus to avoid data-overrun error caused by the limited precision of computation and achieve our goal that to prove geometric theorems fast and accurately.

After simplifying H into *IAS*, the upper bounds of the degrees of R in the independent variables can be estimated by Algorithm 1. However, for some high-complexity geometric theorems, such as the Five-Circles Theorem and Miquel's Theorem, H will be very complicated which will inevitably lead to wasting lots of time and consuming large amounts of memory in the process of simplifying H into *IAS*, and this will contrary to our original intention that design a probabilistic algorithm with high efficiency to prove geometric theorems. Can we avoid

calculating the IAS before instantiation if the geometric theorem is very complicated? To achieve this is easy by the Corollary 1 and it is also the reason why we propose the third selection criterion to collect the statistical population. That is, for some high-complexity geometric theorems, in the circumstance that data-overrun error will not occur during the whole actual operation, we can avoid calculating the irreducible ascending set before instantiation, and estimate the upper bounds crudely by Corollary 1 instead of Algorithm 1, thus to avoid failing to get the running result within the specified time or program interruption for out of memory.

The core content of mathematical statistics is the study of the relationship between statistical population and sample, and statistical inference is to infer statistical population in accordance with sample. In general, statistical inference can be divided into two categories: parameter estimation and significance test. The main researched in this paper belongs to inferring statistical population by sample which involves significance test only. We refer the reader to [23] for the general concept and terminology of significant test.

Statistical significance test is a common method of statistical inference whose principle judge whether there exists significant difference between the statistical population and the null hypothesis $H0$ by the sample information. Its essence is the "small probability theory" and logic approach of the "reductio ad absurdum". First of all, define the null hypothesis $H0$, and then calculate the probability that $H0$ holds base on the sample information by the corresponding statistical methods. If the probability is small enough (i.e., less than the significance level $a = 0.01$), then judge that $H0$ does not hold and reject the null hypothesis. Otherwise, accept the null hypothesis.

Statistical significance test involves two types of errors: Type I error and type II error. Type I error is the incorrect rejection of a true null hypothesis and type II error is the failure to reject a false null hypothesis. Unlike many statistical problem, the major research problem in this paper involves Type I error only and Type II error will not exist. If a geometric theorem is false and a counter example is found successfully, then the program will terminate and return the running result that the theorem is false absolutely, and the probability that the result is incorrect is 0. If N random instances all match the theorem, then the program will reject the null hypothesis and return the running result that the theorem is true. In this case, Type I error will occur unluckily. In view of this, we use the statistical significance test which has no relationship with type II error to control the probability that the occurrence of Type I error.

6 Conclusions

In this paper we presented a new probabilistic algorithm for automated geometry theorem proving which combined the Schwartz-Zippel theorem with statistical inference theory. Our main work includes an improved algorithm for estimating the upper bounds of the pseudo-remainder and three selection criteria for statistical populations. We have implemented the prover with Maple and verified

the performance with experiments. Due to the page limit of this paper, more results on the experiment results and the prover implementation detail will be published in forthcoming papers.

References

1. Chou, S.C.: Proving elementary geometry theorem using Wu's Algorithm. Department of Mathematics, University of Texas at Austin, Ph.D. thesis (1985)
2. Wu, W.T.: Basic principles of mechanical theorem proving in elementary geometries. J. Symb. Comput. **2**(4), 221–25 (1986)
3. Kapur, D.: Using Grobner bases to reason about geometry problems. J. Symb. Comput. **2**, 399–408 (1986)
4. Kutzler, B., Stifter, S.: Automated geometry theorem proving using Buchberger's algorithm. In: On Symbolic and Algebraic Computation, pp. 209–214. ACM Press (1986)
5. Kapur, D., Saxena, T., Yang, L.: Algebraic and geometric reasoning using Dixon resultant. In: Proceedings of ISSAC 1994, vol. 7, pp. 97–107 (1994)
6. Hong, J.W.: Can we prove geometry theorem by computing an example? Sci. China Math. (Ser. A) **16**(3), 234–243 (1986)
7. Zhang, J.Z., Yang, L., Deng, M.K.: The parallel numerival methods in mechanical theorem proving. Theoret. Comput. Sci. **74**, 253–271 (1990)
8. Bellman, R.E.: On Proving Theorems in Plane Geometry via Digital Computer. RAND Corporation, Santa Monica (1965)
9. Schwartz, J.T.: Fast probabilistic algorithms for verification of polynomical identities. J. ACM **27**, 701–717 (1980)
10. Carrá Ferro, G., Gallo, G., Gennaro, R.: Probabilistic verification of elementary geometry statements. In: Wang, D. (ed.) ADG 1996. LNCS, vol. 1360, pp. 87–101. Springer, Heidelberg (1997). https://doi.org/10.1007/BFb0022721
11. Brownawell, W.D.: Bounds for the degrees in the Nullstellensatz. Ann. Math. **126**, 577–591 (1987)
12. Kollar, J.: Sharp effective Nullstellensatz. J. Am. Math. Soc. **1**, 963–975 (1988)
13. Gallo, G., Mishra, B.: Efficient algorithm and bounds for Wu-Ritt characteristic sets. In: Mora, T., Traverso, C. (eds.) Effective Methods in Algebraic Geometry. Progress in Mathematics, vol. 94, pp. 119–142. Birkhauser, Boston (1990). https://doi.org/10.1007/978-1-4612-0441-1_8
14. Gallo, G., Mishra, B.: Wu-Ritt characteristic sets and their complexity. DIMACS Ser. **6**, 111–136 (1991)
15. Tulone, D., Yap, C., Li, C.: Randomized xero testing of radical expressions and elementary geometry theorem proving. In: Richter-Gebert, J., Wang, D. (eds.) ADG 2000. LNCS (LNAI), vol. 2061, pp. 58–82. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45410-1_5
16. Tulone, D., Yap, C., Li, C.: Core Library. http://cs.nye.edu/exact/cpre/
17. Wang, D.M.: EPSILON. http://www-calfor.lip6.fr/wang/epsilon/
18. Chou, S.C.: An introduction to Wu's method for mechanical theorem proving in geometry. J. Autom. Reason. **4**, 237–267 (1988)
19. Wang, D.M.: A new theorem discovered by computer prover. J. Geom. **36**, 173–182 (1989)
20. Gao, X.-S., Lin, Q.: MMP/Geometer – a software package for automated geometric reasoning. In: Winkler, F. (ed.) ADG 2002. LNCS (LNAI), vol. 2930, pp. 44–66. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24616-9_4

21. Deng, M.K.: The parallel numerical method of proving the construction geometric theorem. Chin. Sci. **34**, 1066–1070 (1989)
22. Yang, L., Zhang, J.Z., Li, C.Z.: A prover for papallel numerical verification to a class of constructive geometirc theorem. J. Guangzhou Univ. (Nat. Sci. Ed.) **1**(3), 29–34 (2002)
23. Casella, G., Berger, R.L.: Statistical Inference, 2nd edn. Duxbury Press, Duxbury (2001)