Uniform Approximation and Bernstein Polynomials with Coefficients in the Unit Interval

Weikang Qian and Marc D. Riedel
Electrical and Computer Engineering,
University of Minnesota
200 Union St. S.E.
Minneapolis, MN 55455, USA
{qianx030, mriedel}@umn.edu

Ivo Rosenberg
Mathematics and Statistics
University of Montreal
C.P. 6128, Succ. Centre-Ville
Montreal, Quebec, Canada H3C 3J7
rosenb@DMS.UMontreal.CA

Abstract

This paper presents two main results. The first result pertains to uniform approximation with Bernstein polynomials. We show that, given a power-form polynomial g, we can obtain a Bernstein polynomial of degree m with coefficients that are as close as desired to the corresponding values of g evaluated at the points $0, \frac{1}{m}, \ldots, 1$, provided that m is sufficiently large. The second result pertains to a subset of Bernstein polynomials: those with coefficients that are all in the unit interval. We show that polynomials in this subset map the open interval $(0,1)$ into the open interval $(0,1)$ and map the points 0 and 1 into the closed interval $[0,1]$. The motivation for this work is our research on probabilistic computation with digital circuits. Our design methodology, called stochastic logic, is based on Bernstein polynomials with coefficients that correspond to probability values; accordingly, the coefficients must be values in the unit interval. The mathematics presented here provide a necessary and sufficient test for deciding whether polynomial operations can be implemented with stochastic logic.

1 Introduction

The Weierstrass approximation theorem is a famous theorem in mathematical analysis. It asserts that every continuous function defined on a closed interval can be uniformly approximated as closely as desired by a polynomial function [1].

The Weierstrass Approximation Theorem: *Let f be a continuous function defined on the closed interval $[a,b]$. For any $\epsilon > 0$, there exists a polynomial function p such that for all x in $[a,b]$, we have*

$$|f(x) - p(x)| < \epsilon. \qquad \square$$

The theorem can be proved by a transformation with Bernstein polynomials [2]. By a linear substitution, the interval $[a,b]$ can be transformed into the unit interval $[0,1]$. Thus, the original statement of the theorem holds if and only if the theorem holds for every continuous function f defined on the interval $[0,1]$.

A *Bernstein polynomial* of degree n is a polynomial expressed in the following form [3]:

$$\sum_{k=0}^{n} \beta_{k,n} b_{k,n}(x), \tag{1}$$

where each $\beta_{k,n}$, $k = 0, 1, \ldots, n$, is a real number and

$$b_{k,n}(x) = \binom{n}{k} x^k (1-x)^{n-k}. \tag{2}$$

The coefficients $\beta_{k,n}$ are called *Bernstein coefficients* and the polynomials $b_{0,n}(x), b_{1,n}(x), \ldots, b_{n,n}(x)$ are called *Bernstein basis polynomials* of degree n. Define the n-th Bernstein polynomial for f to be

$$B_n(f;x) = \sum_{k=0}^{n} f\left(\frac{k}{n}\right) b_{k,n}(x).$$

In 1912, Bernstein showed the following result [4, 5]:

The Bernstein Theorem: *Let f be a continuous function defined on the closed interval $[0,1]$. For any $\epsilon > 0$, there exists a positive integer M such that for all x in $[0,1]$ and integer $m \geq M$, we have*

$$|f(x) - B_m(f;x)| < \epsilon. \qquad \square$$

Note that the function $B_m(f;x)$ is a polynomial on x. Thus, based on the Bernstein Theorem, the Weierstrass Approximation Theorem holds. Given a power-form polynomial g of degree n, it is well known that for any $m \geq n$, g can be uniquely converted into a Bernstein polynomial of degree m [6]. Combining this fact with the Bernstein Theorem, we have the following corollary.

Corollary 1
Let g be a polynomial of degree n. For any $\epsilon > 0$, there exists a positive integer $M \geq n$ such that for all x in $[0,1]$ and integer $m \geq M$, we have

$$\left| \sum_{k=0}^{m} \left(\beta_{k,m} - g\left(\frac{k}{m}\right) \right) b_{k,m}(x) \right| < \epsilon,$$

where $\beta_{0,m}, \beta_{1,m}, \ldots, \beta_{m,m}$ satisfy $g(x) = \sum_{k=0}^{m} \beta_{k,m} b_{k,m}(x)$. $\square$

In the first part of the paper, we prove a stronger result than this:

Theorem 1
Let g be a polynomial of degree $n \geq 0$. For any $\epsilon > 0$, there exists a positive integer $M \geq n$ such that for all integers $m \geq M$ and $k = 0, 1, \ldots, m$, we have

$$\left| \beta_{k,m} - g\left(\frac{k}{m}\right) \right| < \epsilon,$$

where $\beta_{0,m}, \beta_{1,m}, \ldots, \beta_{m,m}$ satisfy $g(x) = \sum_{k=0}^{m} \beta_{k,m} b_{k,m}(x)$. $\square$

(Combining Theorem 1 with the fact that $\sum_{k=0}^{m} b_{k,m}(x) = 1$, we can easily prove Corollary 1.)

In the second part of the paper, we consider a subset of Bernstein polynomials: those with coefficients that are all in the unit interval $[0,1]$.

Definition 1
Define U to be the set of Bernstein polynomials with coefficients that are all in the unit interval $[0,1]$:

$$U = \left\{ p(x) \mid \exists\ n \geq 1, 0 \leq \beta_{0,n}, \beta_{1,n}, \ldots, \beta_{n,n} \leq 1,\ \textit{such that}\ p(x) = \sum_{k=0}^{n} \beta_{k,n} b_{k,n}(x) \right\}. \qquad \square$$

The question we ask is: which polynomials can be converted into Bernstein polynomials in U?

Definition 2
Define the set V to be the set of polynomials which are either identically equal to 0 or equal to 1, or map the open interval $(0,1)$ into $(0,1)$ and the points 0 and 1 into the closed interval $[0,1]$, i.e.,

$$V = \{p(x) \mid p(x) \equiv 0,\ \textit{or}\ p(x) \equiv 1,\ \textit{or}\ 0 < p(x) < 1, \forall x \in (0,1)\ \textit{and}\ 0 \leq p(0), p(1) \leq 1\}. \quad \square$$

We prove that the two sets are equivalent:

Theorem 2

$$V = U. \qquad \square$$

In what follows, we will refer to a Bernstein polynomial of degree n converted from a polynomial g as "the Bernstein polynomial of degree n of g". When we say that a polynomial is of degree n, we mean that the power-form of the polynomial is of degree n.

Example 1
Consider the polynomial $g(x) = 3x - 8x^2 + 6x^3$. It maps the open interval $(0,1)$ into $(0,1)$ with $g(0) = 0, g(1) = 1$. Thus, g is in the set V. Based on Theorem 2, we have that g is in the set U. We verify this by considering Bernstein polynomials of increasing degree.

- *The Bernstein polynomial of degree 3 of g is*

$$g(x) = b_{1,3}(x) - \frac{2}{3} b_{2,3}(x) + b_{3,3}(x).$$

  Note that here the coefficient $\beta_{2,3} = -\frac{2}{3} < 0$.

- *The Bernstein polynomial of degree 4 of g is*

$$g(x) = \frac{3}{4} b_{1,4}(x) + \frac{1}{6} b_{2,4}(x) - \frac{1}{4} b_{3,4}(x) + b_{4,4}(x).$$

  Note that here the coefficient $\beta_{3,4} = -\frac{1}{4} < 0$.

- *The Bernstein polynomial of degree 5 of $g(x)$ is*

$$g(x) = \frac{3}{5} b_{1,5}(x) + \frac{2}{5} b_{2,5}(x) + b_{5,5}(x).$$

  Note that here all the coefficients are in $[0,1]$.

Since the Bernstein polynomial of degree 5 of g satisfies Definition 1, we conclude that g is in the set U. $\square$

Example 2

Consider the polynomial $g(x) = \frac{1}{4} - x + x^2$. *Since* $g(0.5) = 0$, *thus* g *is not in the set* V. *Based on Theorem 2, we have that* g *is not in the set* U. *We verify this. By contraposition, suppose that there exist* $n \geq 1$ *and* $0 \leq \beta_{0,n}, \beta_{1,n}, \ldots, \beta_{n,n} \leq 1$ *such that*

$$g(x) = \sum_{k=0}^{n} \beta_{k,n} b_{k,n}(x).$$

Since $g(0.5) = 0$, *therefore,* $\sum_{k=0}^{n} \beta_{k,n} b_{k,n}(0.5) = 0$. *Note that for all* $k = 0, 1, \ldots, n$, $b_{k,n}(0.5) > 0$. *Thus, we have that for all* $k = 0, 1, \ldots, n$, $\beta_{k,n} = 0$. *Therefore,* $g(x) \equiv 0$, *which contradicts the original assumption about* g. *Thus,* g *is not in the set* U. $\Box$

The remainder of the paper is organized as follows. In Section 2, we present some mathematical preliminaries pertaining to Bernstein polynomials. In Section 3, we prove Theorem 1. Based on this theorem, in Section 4, we prove Theorem 2. Finally, we conclude the paper with a discussion on applications of these theorems to our research in probabilistic computation with digital circuits.

2 Properties of Bernstein Polynomials

We list some pertinent properties of Bernstein polynomials.

(a) The *positivity* property:

For all $k = 0, 1, \ldots, n$ and all x in $[0, 1]$, we have

$$b_{k,n}(x) \geq 0. \tag{3}$$

(b) The *partition of unity* property:

The binomial expansion of the left-hand side of the equality $(x + (1-x))^n = 1$ shows that the sum of all Bernstein basis polynomials of degree n is the constant 1, i.e.,

$$\sum_{k=0}^{n} b_{k,n}(x) = 1. \tag{4}$$

(c) Converting power-form coefficients to Bernstein coefficients:

The set of Bernstein basis polynomials $b_{0,n}(x), b_{1,n}(x), \ldots, b_{n,n}(x)$ forms a basis of the vector space of polynomials of real coefficients and degree no more than n [6]. Each power basis function x^j can be uniquely expressed as a linear combination of the $n+1$ Bernstein basis polynomials:

$$x^j = \sum_{k=0}^{n} \sigma_{jk} b_{k,n}(x), \tag{5}$$

for $j = 0, 1, \ldots, n$. To determine the elements of the transformation matrix σ, we write

$$x^j = x^j (x + (1-x))^{n-j}$$

and perform a binomial expansion on the right hand side. This gives

$$x^j = \sum_{k=j}^{n} \frac{\binom{k}{j}}{\binom{n}{j}} b_{k,n}(x),$$

for $j = 0, 1, \ldots, n$. Therefore, we have

$$\sigma_{jk} = \begin{cases} \sigma_{jk} = \binom{k}{j}\binom{n}{j}^{-1}, & \text{for } j \leq k \\ 0, & \text{for } j > k. \end{cases} \tag{6}$$

Suppose that a power-form polynomial of degree no more than n is

$$g(x) = \sum_{k=0}^{n} a_{k,n} x^k \tag{7}$$

and the Bernstein polynomial of degree n of g is

$$g(x) = \sum_{k=0}^{n} \beta_{k,n} b_{k,n}(x). \tag{8}$$

Substituting Equations (5) and (6) into Equation (7) and comparing the Bernstein coefficients, we have

$$\beta_{k,n} = \sum_{j=0}^{n} a_{j,n}\sigma_{jk} = \sum_{j=0}^{k} \binom{k}{j}\binom{n}{j}^{-1} a_{j,n}. \tag{9}$$

Equation (9) provide a means for obtaining Bernstein coefficients from power-form coefficients.

(d) Degree elevation:

Based on Equation (2), we have that for all $k = 0, 1, \ldots, m$,

$$\begin{aligned} &\frac{1}{\binom{m+1}{k}} b_{k,m+1}(x) + \frac{1}{\binom{m+1}{k+1}} b_{k+1,m+1}(x) = x^k(1-x)^{m+1-k} + x^{k+1}(1-x)^{m-k} \\ =&x^k(1-x)^{m-k} = \frac{1}{\binom{m}{k}} b_{k,m}(x), \end{aligned}$$

or

$$\begin{aligned} b_{k,m}(x) &= \frac{\binom{m}{k}}{\binom{m+1}{k}} b_{k,m+1}(x) + \frac{\binom{m}{k}}{\binom{m+1}{k+1}} b_{k+1,m+1}(x) \\ &= \frac{m+1-k}{m+1} b_{k,m+1}(x) + \frac{k+1}{m+1} b_{k+1,m+1}(x). \end{aligned} \tag{10}$$

Given a power-form polynomial g of degree n, for any $m \geq n$, g can be uniquely converted into a Bernstein polynomial of degree m. Suppose that the Bernstein polynomials of degree m and degree $m+1$ of g are $\sum_{k=0}^{m} \beta_{k,m} b_{k,m}(x)$ and $\sum_{k=0}^{m+1} \beta_{k,m+1} b_{k,m+1}(x)$, respectively. We have

$$\sum_{k=0}^{m} \beta_{k,m} b_{k,m}(x) = \sum_{k=0}^{m+1} \beta_{k,m+1} b_{k,m+1}(x). \tag{11}$$

Substituting Equation (10) into the left-hand side of Equation (11) and comparing the Bernstein coefficients, we have

$$\beta_{k,m+1} = \begin{cases} \beta_{0,m}, & \text{for } k = 0 \\ \frac{k}{m+1}\beta_{k-1,m} + \left(1 - \frac{k}{m+1}\right)\beta_{k,m}, & \text{for } 1 \leq k \leq m \\ \beta_{m,m}, & \text{for } k = m+1. \end{cases} \tag{12}$$

Equation (12) provides a means for obtaining the coefficients of the Bernstein polynomial of degree $m+1$ of g from the coefficients of the Bernstein polynomial of degree m of g. We will call this procedure *degree elevation*.

For convenience, given a Bernstein polynomial $g(x) = \sum_{k=0}^{n} \beta_{k,n} b_{k,n}(x)$, we can also express it as

$$g(x) = \sum_{k=0}^{n} c_{k,n} x^k (1-x)^{n-k}, \tag{13}$$

where

$$c_{k,n} = \binom{n}{k} \beta_{k,n}, \tag{14}$$

for $k = 0, 1, \ldots, n$. Substituting Equation (14) into Equation (12), we have

$$c_{k,m+1} = \begin{cases} c_{0,m}, & \text{for } k = 0 \\ c_{k-1,m} + c_{k,m}, & \text{for } 1 \le k \le m \\ c_{m,m}, & \text{for } k = m+1. \end{cases} \tag{15}$$

3 A Proof of Theorem 1

Suppose that the polynomial g is of degree n. Applying Equation (15) recursively, we can express $c_{k,m}$ as a linear combination of $c_{0,n}, c_{1,n}, \ldots, c_{n,n}$.

Lemma 1
Let g be a polynomial of degree n. For any $m \ge n$, suppose that the Bernstein polynomial of degree m of g is $g(x) = \sum_{k=0}^{m} c_{k,m} x^k (1-x)^{m-k}$. Let $c_{k,m} = 0$ for all $k < 0$ and all $k > m$. Then for all $k = 0, 1, \ldots, m$, we have

$$c_{k,m} = \sum_{i=0}^{m-n} \binom{m-n}{i} c_{k-m+n+i,n}. \qquad \square \tag{16}$$

Proof: We prove the lemma by induction on $m - n$.

Base case: For $m - n = 0$, the right-hand side of Equation (16) reduces to $\binom{0}{0} c_{k,n} = c_{k,m}$, so the equation holds.

Inductive step: Suppose that Equation (16) holds for some $m \ge n$ and all $k = 0, 1, \ldots, m$. Consider $m+1$. Since we assume that $c_{-1,m} = c_{m+1,m} = 0$, Equation (15) can be written as

$$c_{k,m+1} = c_{k-1,m} + c_{k,m}, \tag{17}$$

for all $k = 0, \ldots, m+1$. With our convention that $c_{i,n} = 0$ for all $i < 0$ and $i > n$, it is easily seen that

$$c_{-1,m} = 0 = \sum_{i=0}^{m-n} \binom{m-n}{i} c_{-1-m+n+i,n}, \quad c_{m+1,m} = 0 = \sum_{i=0}^{m-n} \binom{m-n}{i} c_{m+1-m+n+i,n}.$$

Together with the induction hypothesis, we conclude that for all $k = -1, 0, \ldots, m, m+1$

$$c_{k,m} = \sum_{i=0}^{m-n} \binom{m-n}{i} c_{k-m+n+i,n}. \tag{18}$$

Based on Equations (17) and (18), for all $k = 0, 1, \ldots, m+1$, we have

$$c_{k,m+1} = \sum_{i=0}^{m-n} \binom{m-n}{i} c_{k-1-m+n+i,n} + \sum_{j=0}^{m-n} \binom{m-n}{j} c_{k-m+n+j,n}.$$

In the first sum, we change the summation index to $j = i - 1$. We obtain

$$\begin{aligned} c_{k,m+1} &= \sum_{j=-1}^{m-n-1} \binom{m-n}{j+1} c_{k-m+n+j,n} + \sum_{j=0}^{m-n} \binom{m-n}{j} c_{k-m+n+j,n} \\ &= \binom{m-n}{0} c_{k-m+n-1,n} + \sum_{j=0}^{m-n-1} \left[\binom{m-n}{j+1} + \binom{m-n}{j} \right] c_{k-m+n+j,n} + \binom{m-n}{m-n} c_{k,n}. \end{aligned}$$

Applying the basic formula $\binom{r}{q} = \binom{r-1}{q-1} + \binom{r-1}{q}$, we obtain

$$c_{k,m+1} = c_{k-m+n-1,n} + \sum_{j=0}^{m-n-1} \binom{m+1-n}{j+1} c_{k-m+n+j,n} + c_{k,n} = \sum_{i=0}^{m+1-n} \binom{m+1-n}{i} c_{k-m-1+n+i,n}.$$

Thus Equation (16) holds for $m+1$. By induction, it holds for all $m \geq k$. □

Remark: Equation (16) can be formulated as

$$c_{k,m} = \sum_{i=\max\{0,k-m+n\}}^{\min\{k,n\}} \binom{m-n}{k-i} c_{i,n}, \tag{19}$$

for all $m \geq n$ and $k = 0, 1, \ldots, m$. Indeed, in Equation (16), first use the basic formula $\binom{r}{q} = \binom{r}{r-q}$ and then change the summation index to $j = k - m + n + i$ to obtain

$$c_{k,m} = \sum_{i=0}^{m-n} \binom{m-n}{m-n-i} c_{k-m+n+i,n} = \sum_{j=k-m+n}^{k} \binom{m-n}{k-j} c_{j,n}.$$

Note that $c_{j,n} \neq 0$ implies $0 \leq j \leq n$. This yields Equation (19). □

Lemma 2
Let n be a positive integer. For all integer m, k and i such that

$$m > n, \quad 0 \leq k \leq m, \quad \max\{0, k-m+n\} \leq i \leq \min\{k, n\}, \tag{20}$$

we have

$$\left| \left(\frac{k}{m}\right)^i \left(1 - \frac{k}{m}\right)^{n-i} - \frac{\binom{m-n}{k-i}}{\binom{m}{k}} \right| \leq \frac{n^2}{m}. \qquad \square \tag{21}$$

Proof: For simplicity, we define $\delta = \left(\frac{k}{m}\right)^i \left(1 - \frac{k}{m}\right)^{n-i} - \frac{\binom{m-n}{k-i}}{\binom{m}{k}}$. Now

$$\begin{aligned}
\frac{\binom{m-n}{k-i}}{\binom{m}{k}} &= \frac{(m-n)!}{(k-i)!(m-n-k+i)!} \cdot \frac{k!(m-k)!}{m!} \\
&= \frac{k(k-1)\cdots(k-i+1)(m-k)(m-k-1)\cdots(m-n-k+i+1)}{m(m-1)\cdots(m-n+1)} \\
&= \prod_{j=0}^{i-1} \frac{k-j}{m-j} \cdot \prod_{j=0}^{n-i-1} \frac{m-k-j}{m-i-j} = \prod_{j=0}^{i-1} \left(1 - \frac{m-k}{m-j}\right) \cdot \prod_{j=0}^{n-i-1} \left(1 - \frac{k-i}{m-i-j}\right).
\end{aligned} \tag{22}$$

We obtain an upper bound for $\frac{\binom{m-n}{k-i}}{\binom{m}{k}}$ by replacing j in Equation (22) with its least value, 0:

$$\frac{\binom{m-n}{k-i}}{\binom{m}{k}} \leq \prod_{j=0}^{i-1} \left(1 - \frac{m-k}{m}\right) \cdot \prod_{j=0}^{n-i-1} \left(1 - \frac{k-i}{m-i}\right) = \left(\frac{k}{m}\right)^i \left(\frac{m-k}{m-i}\right)^{n-i}.$$

We need the following simple inequality: for real numbers $0 \leq x \leq y \leq 1$ and a non-negative integer l,

$$y^l - x^l = (y-x) \sum_{j=0}^{l-1} y^j x^{l-1-j} \leq (y-x)l. \tag{23}$$

From Equation (20), we obtain $0 \leq i \leq \min\{k, n\} \leq k \leq m$ and so we can use Equation (23) for

$$0 \leq x = \frac{m-k}{m} \leq \frac{m-k}{m-i} = y \leq 1, \quad l = n-i \geq 0.$$

We obtain

$$\begin{aligned}
\delta &= \left(\frac{k}{m}\right)^i \left(1 - \frac{k}{m}\right)^{n-i} - \frac{\binom{m-n}{k-i}}{\binom{m}{k}} \geq \left(\frac{k}{m}\right)^i \left(\left(\frac{m-k}{m}\right)^{n-i} - \left(\frac{m-k}{m-i}\right)^{n-i}\right) \\
&= -\left(\frac{k}{m}\right)^i \left(\left(\frac{m-k}{m-i}\right)^{n-i} - \left(\frac{m-k}{m}\right)^{n-i}\right) \\
&\geq -\left(\frac{k}{m}\right)^i \left(\frac{m-k}{m-i} - \frac{m-k}{m}\right)(n-i) = -\left(\frac{k}{m}\right)^i \frac{(m-k)i(n-i)}{(m-i)m}.
\end{aligned}$$

Since $0 \leq \frac{k}{m} \leq 1$, $0 \leq \frac{m-k}{m-i} \leq 1$, and $0 \leq i \leq n$, we obtain

$$-\left(\frac{k}{m}\right)^i \frac{(m-k)i(n-i)}{(m-i)m} \geq -\frac{i(n-i)}{m} > -\frac{n^2}{m}.$$

Therefore,

$$\delta = \left(\frac{k}{m}\right)^i \left(1 - \frac{k}{m}\right)^{n-i} - \frac{\binom{m-n}{k-i}}{\binom{m}{k}} > -\frac{n^2}{m}. \tag{24}$$

Similarly, we obtain a lower bound for $\frac{\binom{m-n}{k-i}}{\binom{m}{k}}$ by replacing the index j in Equation (22) with i in the first product and with $n-i$ in the second product, obtaining

$$\begin{aligned}\frac{\binom{m-n}{k-i}}{\binom{m}{k}} &= \prod_{j=0}^{i-1}\left(1-\frac{m-k}{m-j}\right)\cdot\prod_{j=0}^{n-i-1}\left(1-\frac{k-i}{m-i-j}\right) \geq \prod_{j=0}^{i-1}\left(1-\frac{m-k}{m-i}\right)\cdot\prod_{j=0}^{n-i-1}\left(1-\frac{k-i}{m-n}\right)\\ &= \left(\frac{k-i}{m-i}\right)^i\left(\frac{m-n-k+i}{m-n}\right)^{n-i} \geq \left(\frac{k-i}{m-i}\right)^i\left(\frac{m-n-k+i}{m-n+i}\right)^{n-i}.\end{aligned}$$

Thus, proceeding as above, we have

$$\begin{aligned}\delta &= \left(\frac{k}{m}\right)^i\left(1-\frac{k}{m}\right)^{n-i} - \frac{\binom{m-n}{k-i}}{\binom{m}{k}} \leq \left(\frac{k}{m}\right)^i\left(\frac{m-k}{m}\right)^{n-i} - \left(\frac{k-i}{m-i}\right)^i\left(\frac{m-n-k+i}{m-n+i}\right)^{n-i}\\ &= \left[\left(\frac{k}{m}\right)^i - \left(\frac{k-i}{m-i}\right)^i\right]\left(\frac{m-k}{m}\right)^{n-i} + \left[\left(\frac{m-k}{m}\right)^{n-i} - \left(\frac{m-n-k+i}{m-n+i}\right)^{n-i}\right]\left(\frac{k-i}{m-i}\right)^i.\end{aligned}$$

Due to Equation (20), we have

$$0 \leq \frac{k-i}{m-i} \leq \frac{k}{m} \leq 1, \quad 0 \leq \frac{m-n-k+i}{m-n+i} \leq \frac{m-k}{m} \leq 1,$$

and so we obtain

$$\delta \leq \left(\frac{k}{m}\right)^i - \left(\frac{k-i}{m-i}\right)^i + \left(\frac{m-k}{m}\right)^{n-i} - \left(\frac{m-n-k+i}{m-n+i}\right)^{n-i}. \tag{25}$$

Applying Equation (23) twice to the right-hand side of Equation (25), we obtain

$$\begin{aligned}\delta &\leq i\left(\frac{k}{m}-\frac{k-i}{m-i}\right) + (n-i)\left(\frac{m-k}{m}-\frac{m-n-k+i}{m-n+i}\right)\\ &= \frac{i^2}{m}\cdot\frac{m-k}{m-i} + \frac{(n-i)^2}{m}\cdot\frac{k}{m-n+i}.\end{aligned}$$

From Equation (20), we have

$$0 \leq \frac{m-k}{m-i} \leq 1, \quad 0 \leq \frac{k}{m-n+i} \leq 1.$$

Therefore,

$$\delta = \left(\frac{k}{m}\right)^i\left(1-\frac{k}{m}\right)^{n-i} - \frac{\binom{m-n}{k-i}}{\binom{m}{k}} \leq \frac{i^2+(n-i)^2}{m} \leq \frac{ni+n(n-i)}{m} = \frac{n^2}{m}. \tag{26}$$

Equations (24) and (26) together yield Equation (21). □

Now we give a proof of Theorem 1.

Theorem 1
Let g be a polynomial of degree $n \geq 0$. For any $\epsilon > 0$, there exists a positive integer $M \geq n$ such that for all integer $m \geq M$ and $k = 0, 1, \ldots, m$, we have

$$\left|\beta_{k,m} - g\left(\frac{k}{m}\right)\right| < \epsilon,$$

where $\beta_{0,m}, \beta_{1,m}, \ldots, \beta_{m,m}$ *satisfy that* $g(x) = \sum_{k=0}^{m} \beta_{k,m} b_{k,m}(x)$. $\square$

Proof: For $n = 0$, g is a constant polynomial. Suppose that $g(x) = y$, where y is a constant value. We select $M = 1$. Then, for all integers $m \geq M$ and all integers $k = 0, 1, \ldots, m$, we have $\beta_{k,m} = y = g\left(\frac{k}{m}\right)$. Thus, the theorem holds.

For $n > 0$, we select M such that $M > \max\left\{\frac{n^2}{\epsilon}\sum_{i=0}^{n}|c_{i,n}|, 2n\right\}$, where the real numbers $c_{0,n}, c_{1,n}, \ldots, c_{n,n}$ satisfy

$$g(x) = \sum_{i=0}^{n} c_{i,n} x^i (1-x)^{n-i}. \tag{27}$$

Now consider any $m \geq M$. Since

$$2n \leq \max\left\{\frac{n^2}{\epsilon}\sum_{i=0}^{n}|c_{i,n}|, 2n\right\} < M \leq m,$$

we have $m - n > n$. Consider the following three cases for k.

1. The case where $n \leq k \leq m - n$. Here $\max\{0, k - m + n\} = 0$ and $\min\{k, n\} = n$. Thus, the summation indices in Equation (19) range from 0 to n. Therefore,

$$\beta_{k,m} = \frac{c_{k,m}}{\binom{m}{k}} = \sum_{i=0}^{n} \frac{\binom{m-n}{k-i}}{\binom{m}{k}} c_{i,n}. \tag{28}$$

   Substituting x with $\frac{k}{m}$ in Equation (27), we have

$$g\left(\frac{k}{m}\right) = \sum_{i=0}^{n} c_{i,n}\left(\frac{k}{m}\right)^i \left(1 - \frac{k}{m}\right)^{n-i}. \tag{29}$$

   By Lemma 2, since $0 < n < m$ and $0 \leq k \leq m$, Equation (21) holds for all $0 = \max\{0, k - m + n\} \leq i \leq \min\{k, n\} = n$. Thus, by Equations (21), (28), (29) and the well-known inequality $|\sum x_i| \leq \sum |x_i|$, we have

$$\begin{aligned}\left|\beta_{k,m} - g\left(\frac{k}{m}\right)\right| &= \left|\sum_{i=0}^{n}\left[\frac{\binom{m-n}{k-i}}{\binom{m}{k}} - \left(\frac{k}{m}\right)^i\left(1 - \frac{k}{m}\right)^{n-i}\right] c_{i,n}\right| \\ &\leq \sum_{i=0}^{n}\left|\frac{\binom{m-n}{k-i}}{\binom{m}{k}} - \left(\frac{k}{m}\right)^i\left(1 - \frac{k}{m}\right)^{n-i}\right| |c_{i,n}| \leq \frac{n^2}{m}\sum_{i=0}^{n}|c_{i,n}|.\end{aligned}$$

   Since $\frac{n^2}{\epsilon}\sum_{i=0}^{n}|c_{i,n}| < M \leq m$, we have

$$\frac{n^2}{m}\sum_{i=0}^{n}|c_{i,n}| < \epsilon. \tag{30}$$

   Therefore, for all $n \leq k \leq m - n$, we have $\left|\beta_{k,m} - g\left(\frac{k}{m}\right)\right| < \epsilon$.

2. The case where $0 \leq k < n$. Since $m > 2n$, we have $k - m + n < k - n < 0$. Thus, $\max\{0, k-m+n\} = 0$ and $\min\{k, n\} = k$. Thus, the summation indices in Equation (19) range from 0 to k. Therefore,

$$\beta_{k,m} = \frac{c_{k,m}}{\binom{m}{k}} = \sum_{i=0}^{k} \frac{\binom{m-n}{k-i}}{\binom{m}{k}} c_{i,n}. \tag{31}$$

When $k + 1 \leq i \leq n$, we have that $1 \leq k + 1 \leq i$ and so

$$\left| \left(\frac{k}{m}\right)^i \left(1 - \frac{k}{m}\right)^{n-i} \right| = \left(\frac{k}{m}\right) \left| \left(\frac{k}{m}\right)^{i-1} \left(1 - \frac{k}{m}\right)^{n-i} \right| \leq \frac{k}{m} < \frac{n}{m} \leq \frac{n^2}{m}. \tag{32}$$

By Lemma 2, since $0 < n < m$ and $0 \leq k \leq m$, Equation (21) holds for all $0 = \max\{0, k-m+n\} \leq i \leq \min\{k, n\} = k$. Thus, by Equations (21), (29), (30), (31), (32) and the inequality $|\sum x_i| \leq \sum |x_i|$, we have

$$\begin{aligned}
\left|\beta_{k,m} - g\left(\frac{k}{m}\right)\right| &= \left| \sum_{i=0}^{k} \frac{\binom{m-n}{k-i}}{\binom{m}{k}} c_{i,n} - \sum_{i=0}^{n} \left(\frac{k}{m}\right)^i \left(1 - \frac{k}{m}\right)^{n-i} c_{i,n} \right| \\
&= \left| \sum_{i=0}^{k} \left[\frac{\binom{m-n}{k-i}}{\binom{m}{k}} - \left(\frac{k}{m}\right)^i \left(1 - \frac{k}{m}\right)^{n-i} \right] c_{i,n} - \sum_{i=k+1}^{n} \left(\frac{k}{m}\right)^i \left(1 - \frac{k}{m}\right)^{n-i} c_{i,n} \right| \\
&\leq \sum_{i=0}^{k} \left| \frac{\binom{m-n}{k-i}}{\binom{m}{k}} - \left(\frac{k}{m}\right)^i \left(1 - \frac{k}{m}\right)^{n-i} \right| |c_{i,n}| + \sum_{i=k+1}^{n} \left| \left(\frac{k}{m}\right)^i \left(1 - \frac{k}{m}\right)^{n-i} \right| |c_{i,n}| \\
&\leq \frac{n^2}{m} \sum_{i=0}^{n} |c_{i,n}| < \epsilon.
\end{aligned}$$

3. The case where $m - n < k \leq m$. Since $m > 2n$, we have $n < m - n < k$. Thus, $\max\{0, k-m+n\} = k - m + n$ and $\min\{k, n\} = n$. Now, the summation indices in Equation (19) range from $k - m + n$ to n. Therefore,

$$\beta_{k,m} = \frac{c_{k,m}}{\binom{m}{k}} = \sum_{i=k-m+n}^{n} \frac{\binom{m-n}{k-i}}{\binom{m}{k}} c_{i,n}. \tag{33}$$

When $0 \leq i \leq k - m + n - 1$, we have that $1 \leq m + 1 - k \leq n - i$. Thus,

$$\left| \left(\frac{k}{m}\right)^i \left(1 - \frac{k}{m}\right)^{n-i} \right| = \left(1 - \frac{k}{m}\right) \left| \left(\frac{k}{m}\right)^{i} \left(1 - \frac{k}{m}\right)^{n-i-1} \right| \leq \frac{m-k}{m} < \frac{n}{m} \leq \frac{n^2}{m}. \tag{34}$$

By Lemma 2, since $0 < n < m$ and $0 \leq k \leq m$, Equation (21) holds for all $k - m + n = \max\{0, k-m+n\} \leq i \leq \min\{k, n\} = n$. Thus, by Equations (21), (29), (30), (33), (34) and the inequality $|\sum x_i| \le \sum |x_i|$, we have

$$\left|\beta_{k,m} - g\left(\frac{k}{m}\right)\right| = \left|\sum_{i=k-m+n}^{n} \frac{\binom{m-n}{k-i}}{\binom{m}{k}} c_{i,n} - \sum_{i=0}^{n} \left(\frac{k}{m}\right)^i \left(1-\frac{k}{m}\right)^{n-i} c_{i,n}\right|$$

$$= \left|\sum_{i=k-m+n}^{n} \left[\frac{\binom{m-n}{k-i}}{\binom{m}{k}} - \left(\frac{k}{m}\right)^i \left(1-\frac{k}{m}\right)^{n-i}\right] c_{i,n} - \sum_{i=0}^{k-m+n-1} \left(\frac{k}{m}\right)^i \left(1-\frac{k}{m}\right)^{n-i} c_{i,n}\right|$$

$$\le \sum_{i=k-m+n}^{n} \left|\frac{\binom{m-n}{k-i}}{\binom{m}{k}} - \left(\frac{k}{m}\right)^i \left(1-\frac{k}{m}\right)^{n-i}\right| |c_{i,n}| + \sum_{i=0}^{k-m+n-1} \left|\left(\frac{k}{m}\right)^i \left(1-\frac{k}{m}\right)^{n-i}\right| |c_{i,n}|$$

$$\le \frac{n^2}{m} \sum_{i=0}^{n} |c_{i,n}| < \epsilon.$$

In conclusion, if $m \ge M$, then for all $k = 0, 1, \ldots, m$, we have

$$\left|\beta_{k,m} - g\left(\frac{k}{m}\right)\right| < \epsilon. \qquad \square$$

4 A Proof of Theorem 2

We demonstrate that the sets U and V defined in the introduction – see Definitions 1 and 2 – are one and the same. We demonstrate that $U \subseteq V$ and $V \subseteq U$ separately. First, we prove the former – the easier one. Then we use Theorem 1 to prove the latter.

Theorem 3

$$U \subseteq V. \qquad \square$$

Proof: Let $n \ge 1$ and $\beta_{k,n} = 0$, for all $0 \le k \le n$. Then the polynomial $p(x) = \sum_{k=0}^{n} \beta_{k,n} b_{k,n}(x) = 0$.

Let $n \ge 1$ and $\beta_{k,n} = 1$, for all $0 \le k \le n$. Then, by Equation (4), the polynomial $p(x) = \sum_{k=0}^{n} \beta_{k,n} b_{k,n}(x) = 1$.

Thus $0 \in U$ and $1 \in U$. From the definition of V, $0 \in V$ and $1 \in V$.

Now consider any polynomial $p \in U$ such that $p \not\equiv 0$ and $p \not\equiv 1$. There exist $n \ge 1$ and $0 \le \beta_{0,n}, \beta_{1,n}, \ldots, \beta_{n,n} \le 1$ such that

$$p(x) = \sum_{k=0}^{n} \beta_{k,n} b_{k,n}(x).$$

From Equations (3), (4) and the fact that $0 \le \beta_{0,n}, \beta_{1,n}, \ldots, \beta_{n,n} \le 1$, for all x in $[0, 1]$, we have

$$0 \le p(x) = \sum_{k=0}^{n} \beta_{k,n} b_{k,n}(x) \le \sum_{k=0}^{n} b_{k,n}(x) = 1.$$

We further claim that for all x in $(0, 1)$, we must have $0 < p(x) < 1$. By contraposition, we assume that there exists a $0 < x_0 < 1$, such that $p(x_0) \le 0$ or $p(x_0) \ge 1$. Since for $0 < x_0 < 1$, we have $0 \le p(x_0) \le 1$, thus $p(x_0) = 0$ or 1.

We first consider the case that $p(x_0) = 0$. Since $0 < x_0 < 1$, it is not hard to see that for all $k = 0, 1, \ldots, n$, $b_{k,n}(x_0) > 0$. Thus, $p(x_0) = 0$ implies that for all $k = 0, 1, \ldots, n$, $\beta_{k,n} = 0$. In this case, for any real number x, $p(x) = \sum_{k=0}^{n} \beta_{k,n} b_{k,n}(x) = 0$, which contradicts the assumption that $p(x) \not\equiv 0$.

Similarly, in the case that $p(x_0) = 1$, we can show that $p(x) \equiv 1$, which contradicts the assumption that $p(x) \not\equiv 1$. In both cases, we get a contradiction; this proves the claim that for all x in $(0, 1)$, $0 < p(x) < 1$.

Therefore, for any polynomial $p \in U$ such that $p \not\equiv 0$ and $p \not\equiv 1$, we have $p \in V$. Since we showed at the outset that $0 \in U$, $1 \in U$, $0 \in V$ and $1 \in V$, thus, for any polynomial $p \in U$, we have $p \in V$. Therefore, $U \subseteq V$. □

Next we prove the claim that $V \subseteq U$. We will first show that each of four possible different categories of polynomials in the set V are in the set U. The different categories are tackled in Theorems 4 and 5 and Corollaries 2 and 3.

Theorem 4
Let g be a polynomial of degree n mapping the open interval $(0, 1)$ into $(0, 1)$ with $0 \leq g(0), g(1) < 1$. Then $g \in U$. □

Proof: Since g is continuous on the closed interval $[0, 1]$, it attains its maximum value M_g on $[0, 1]$. Since $g(x) < 1$, for all $x \in [0, 1]$, we have $M_g < 1$.

Let $\epsilon_1 = 1 - M_g > 0$. By Theorem 1, there exists a positive integer $M_1 \geq n$ such that for all integers $m \geq M_1$ and $k = 0, 1, \ldots, m$, we have $\left|\beta_{k,m} - g\left(\frac{k}{m}\right)\right| < \epsilon_1$, where $\beta_{0,m}, \beta_{1,m}, \ldots, \beta_{m,m}$ satisfy that $g(x) = \sum_{k=0}^{m} \beta_{k,m} b_{k,m}(x)$. Thus, for all $m \geq M_1$ and all $k = 0, 1, \ldots, m$,

$$\beta_{k,m} < g\left(\frac{k}{m}\right) + \epsilon_1 \leq M_g + 1 - M_g = 1. \tag{35}$$

Denote by r the multiplicity of 0 as a root of $g(x)$ (where $r = 0$ if $g(0) \neq 0$) and by s the multiplicity of 1 as a root of $g(x)$ (where $s = 0$ if $g(1) \neq 0$). We can factorize $g(x)$ as

$$g(x) = x^r (1 - x)^s h(x), \tag{36}$$

where $h(x)$ is a polynomial, satisfying that $h(0) \neq 0$ and $h(1) \neq 0$.

We show that $h(0) > 0$. By the way of contraposition, suppose that $h(0) \leq 0$. Since $h(0) \neq 0$, we have $h(0) < 0$. By the continuity of the polynomial $h(x)$, there exists some $0 < x^* < 1$, such that $h(x^*) < 0$. Thus, $g(x^*) = x^{*r}(1 - x^*)^s h(x^*) < 0$. However, $g(x) > 0$, for all $x \in (0, 1)$. Therefore, $h(0) > 0$. Similarly, we have $h(1) > 0$.

Since $g(x) > 0$ for all x in $(0, 1)$, we have $h(x) = \dfrac{g(x)}{x^r (1 - x)^s} > 0$ for all x in $(0, 1)$. In view of the fact that $h(0) > 0$ and $h(1) > 0$, we have $h(x) > 0$, for all x in $[0, 1]$. Since $h(x)$ is continuous on the closed interval $[0, 1]$, it attains its minimum value m_h on $[0, 1]$. Clearly, $m_h > 0$.

Let $\epsilon_2 = m_h > 0$. By Theorem 1, there exists a positive integer $M_2 \geq n - r - s$, such that for all integers $d \geq M_2$ and $k = 0, 1, \ldots, d$, we have $\left|\gamma_{k,d} - h\left(\frac{k}{d}\right)\right| < \epsilon_2$, where $\gamma_{0,d}, \gamma_{1,d}, \ldots, \gamma_{d,d}$ satisfy that

$$h(x) = \sum_{k=0}^{d} \gamma_{k,d} b_{k,d}(x). \tag{37}$$

Thus, for all $d \geq M_2$ and all $k = 0, 1, \ldots, d$,

$$\gamma_{k,d} > h\left(\frac{k}{d}\right) - \epsilon_2 \geq m_h - m_h = 0.$$

Combining Equations (36) and(37), we have

$$\begin{aligned} g(x) &= x^r(1-x)^s h(x) = x^r(1-x)^s \sum_{k=0}^{d} \gamma_{k,d} b_{k,d}(x) = x^r(1-x)^s \sum_{k=0}^{d} \gamma_{k,d} \binom{d}{k} x^k (1-x)^{d-k} \\ &= \sum_{k=0}^{d} \frac{\gamma_{k,d}\binom{d}{k}}{\binom{d+r+s}{k+r}} \binom{d+r+s}{k+r} x^{k+r}(1-x)^{d+s-k} = \sum_{k=r}^{d+r} \frac{\gamma_{k-r,d}\binom{d}{k-r}}{\binom{d+r+s}{k}} b_{k,d+r+s}(x) \\ &= \sum_{k=0}^{d+r+s} \beta_{k,d+r+s} b_{k,d+r+s}(x), \end{aligned}$$

where $\beta_{k,d+r+s}$ are the coefficients of the Bernstein polynomial of degree $d+r+s$ of g and

$$\beta_{k,d+r+s} = \begin{cases} 0, & \text{for } 0 \leq k < r \text{ and } d+r < k \leq d+r+s \\ \frac{\gamma_{k-r,d}\binom{d}{k-r}}{\binom{d+r+s}{k}} > 0, & \text{for } r \leq k \leq d+r. \end{cases}$$

Thus, when $m = d + r + s \geq M_2 + r + s$, we have for all $k = 0, 1, \ldots, m$,

$$\beta_{k,m} \geq 0. \tag{38}$$

According to Equations (35) and (38), if we select an $m_0 \geq \max\{M_1, M_2 + r + s\}$, then $g(x)$ can be expressed as a Bernstein polynomial of degree m_0:

$$g(x) = \sum_{k=0}^{m_0} \beta_{k,m_0} b_{k,m_0}(x),$$

with $0 \leq \beta_{k,m_0} \leq 1$, for all $k = 0, 1, \ldots, m_0$. Therefore, $g \in U$. □

Theorem 5
Let g be a polynomial of degree n mapping the open interval $(0, 1)$ into $(0, 1)$ with $g(0) = 0$ and $g(1) = 1$. Then $g \in U$. □

Proof: Denote by r the multiplicity of 0 as a root of $g(x)$. We can factorize $g(x)$ as

$$g(x) = x^r h(x), \tag{39}$$

where $h(x)$ is a polynomial satisfying $h(0) \neq 0$. By a similar reasoning as in the proof of Theorem 4, we obtain $h(0) > 0$. Since for all x in $(0, 1]$, $h(x) = \dfrac{g(x)}{x^r} > 0$, we have for all x in $[0, 1]$, $h(x) > 0$. Since $h(x)$ is continuous on the closed interval $[0, 1]$, it attains its minimum value m_h on $[0, 1]$. Clearly, $m_h > 0$.

Let $\epsilon_1 = m_h > 0$. By Theorem 1, there exists a positive integer $M_1 \geq n - r$ such that for all integers $d \geq M_1$ and $k = 0, 1, \ldots, d$, we have $\left|\gamma_{k,d} - h\left(\dfrac{k}{d}\right)\right| < \epsilon_1$, where $\gamma_{0,d}, \gamma_{1,d}, \ldots, \gamma_{d,d}$ satisfy

$$h(x) = \sum_{k=0}^{d} \gamma_{k,d} b_{k,d}(x). \tag{40}$$

Thus, for all $d \geq M_1$ and all $k = 0, 1, \ldots, d$,

$$\gamma_{k,d} > h\left(\frac{k}{d}\right) - \epsilon_1 \geq m_h - m_h = 0.$$

Combining Equations (39) and (40), we have

$$\begin{aligned} g(x) &= x^r h(x) = x^r \sum_{k=0}^{d} \gamma_{k,d} b_{k,d}(x) = x^r \sum_{k=0}^{d} \gamma_{k,d} \binom{d}{k} x^k (1-x)^{d-k} \\ &= \sum_{k=0}^{d} \frac{\gamma_{k,d}\binom{d}{k}}{\binom{d+r}{k+r}} \binom{d+r}{k+r} x^{k+r}(1-x)^{d-k} = \sum_{k=r}^{d+r} \frac{\gamma_{k-r,d}\binom{d}{k-r}}{\binom{d+r}{k}} b_{k,d+r}(x) = \sum_{k=0}^{d+r} \beta_{k,d+r} b_{k,d+r}(x), \end{aligned}$$

where $\beta_{k,d+r}$ are the coefficients of the Bernstein polynomial of degree $d+r$ of g and

$$\beta_{k,d+r} = \begin{cases} 0, & \text{for } 0 \leq k < r \\ \frac{\gamma_{k-r,d}\binom{d}{k-r}}{\binom{d+r}{k}} > 0, & \text{for } r \leq k \leq d+r. \end{cases}$$

Thus, when $m = d + r \geq M_1 + r$, we have for all $k = 0, 1, \ldots, m$,

$$\beta_{k,m} \geq 0. \tag{41}$$

Let

$$g^*(x) = 1 - g(x). \tag{42}$$

Then g^* maps the open interval $(0,1)$ into $(0,1)$ with $g^*(0) = 1$, $g^*(1) = 0$. Denote by s the multiplicity of 1 as a root of $g^*(x)$. Thus, we can factorize $g^*(x)$ as

$$g^*(x) = (1-x)^s h^*(x), \tag{43}$$

where $h^*(x)$ is a polynomial satisfying that $h^*(1) \neq 0$. As in the proof of Theorem 4, we obtain $h^*(1) > 0$. Since for all x in $[0,1)$, $h^*(x) = \dfrac{g^*(x)}{(1-x)^s} > 0$, we have for all $x \in [0,1]$, $h^*(x) > 0$. Since $h^*(x)$ is continuous on the closed interval $[0,1]$, it attains its minimum value m_h^* on $[0,1]$. Clearly, $m_h^* > 0$.

Let $\epsilon_2 = m_h^* > 0$. By Theorem 1, there exists a positive integer $M_2 \geq n - s$ such that for all integers $q \geq M_2$ and $k = 0, 1, \ldots, q$, we have $\left|\gamma_{k,q}^* - h^*\left(\frac{k}{q}\right)\right| < \epsilon_2$, where $\gamma_{0,q}^*, \gamma_{1,q}^*, \ldots, \gamma_{q,q}^*$ satisfy

$$h^*(x) = \sum_{k=0}^{q} \gamma_{k,q}^* b_{k,q}(x). \tag{44}$$

Thus, for all $q \geq M_2$ and all $k = 0, 1, \ldots, q$,

$$\gamma_{k,q}^* > h^*\left(\frac{k}{q}\right) - \epsilon_2 \geq m_h^* - m_h^* = 0.$$

Combining Equations (42), (43) and (44), we have

$$\begin{aligned} g(x) &= 1 - g^*(x) = 1 - (1-x)^s h^*(x) = 1 - (1-x)^s \sum_{k=0}^{q} \gamma_{k,q}^* b_{k,q}(x) \\ &= 1 - (1-x)^s \sum_{k=0}^{q} \gamma_{k,q}^* \binom{q}{k} x^k (1-x)^{q-k} = 1 - \sum_{k=0}^{q} \frac{\gamma_{k,q}^*\binom{q}{k}}{\binom{q+s}{k}} \binom{q+s}{k} x^k (1-x)^{q+s-k}. \end{aligned}$$

Further using (4), we obtain

$$g(x) = \sum_{k=0}^{q+s} b_{k,q+s}(x) - \sum_{k=0}^{q} \frac{\gamma^*_{k,q}\binom{q}{k}}{\binom{q+s}{k}} b_{k,q+s}(x) = \sum_{k=0}^{q+s} \beta_{k,q+s} b_{k,q+s}(x),$$

where the $\beta_{k,q+s}$'s are the coefficients of the Bernstein polynomial of degree $q+s$ of g:

$$\beta_{k,q+s} = \begin{cases} 1 - \frac{\gamma^*_{k,q}\binom{q}{k}}{\binom{q+s}{k}} < 1, & \text{for } 0 \leq k \leq q \\ 1, & \text{for } q < k \leq q+s. \end{cases}$$

Thus, when $m = q + s \geq M_2 + s$, we have for all $k = 0, 1, \ldots, m$,

$$\beta_{k,m} \leq 1. \tag{45}$$

According to Equations (41) and (45), if we select an $m_0 \geq \max\{M_1 + r, M_2 + s\}$, then $g(x)$ can be expressed as a Bernstein polynomial of degree m_0:

$$g(x) = \sum_{k=0}^{m_0} \beta_{k,m_0} b_{k,m_0}(x),$$

with $0 \leq \beta_{k,m_0} \leq 1$, for all $k = 0, 1, \ldots, m_0$, Therefore, $g \in U$. □

Lemma 3
If a polynomial p is in the set U, then the polynomial $1 - p$ is also in the set U. □

Proof: Since p is in the set U, there exist $n \geq 1$ and $0 \leq \beta_{0,n}, \beta_{1,n}, \ldots, \beta_{n,n} \leq 1$ such that

$$p(x) = \sum_{k=0}^{n} \beta_{k,n} b_{k,n}(x).$$

By Equation (4), we have

$$1 - p(x) = \sum_{k=0}^{n} b_{k,n}(x) - \sum_{k=0}^{n} \beta_{k,n} b_{k,n}(x) = \sum_{k=0}^{n} (1 - \beta_{k,n}) b_{k,n}(x) = \sum_{k=0}^{n} \gamma_{k,n} b_{k,n}(x),$$

where $\gamma_{k,n} = 1 - \beta_{k,n}$ satisfying $0 \leq \gamma_{k,n} \leq 1$, for all $k = 0, 1, \ldots, n$. Therefore, $1-p$ is in the set U. □

Corollary 2
Let g be a polynomial of degree n mapping the open interval $(0,1)$ into $(0,1)$ with $0 < g(0), g(1) \leq 1$. Then $g \in U$. □

Proof: Let polynomial $h = 1 - g$. Then h maps $(0,1)$ into $(0,1)$ with $0 \leq h(0), h(1) < 1$. By Theorem 4, $h \in U$. By Lemma 3, $g = 1 - h$ is also in the set U. □

Corollary 3
Let g be a polynomial of degree n mapping the open interval $(0,1)$ into $(0,1)$ with $g(0) = 1$ and $g(1) = 0$. Then $g \in U$. □

Proof: Let the polynomial $h = 1 - g$. Then h maps $(0, 1)$ into $(0, 1)$ with $h(0) = 0, h(1) = 1$. By Theorem 5, $h \in U$. By Lemma 3, $g = 1 - h$ is also in the set U. □

Combining Theorem 4, Theorem 5, Corollary 2 and Corollary 3, we show that $V \subseteq U$.

Theorem 6

$$V \subseteq U. \qquad \Box$$

Proof: Based on the definition of V, for any polynomial $p \in V$, we have one of following five cases.

1. The case where $p \equiv 0$ or $p \equiv 1$. In the proof of Theorem 3, we have shown that $0 \in U$ and $1 \in U$. Thus $p \in U$.
2. The case where p maps the open interval $(0, 1)$ into $(0, 1)$ with $0 \le p(0), p(1) < 1$. By Theorem 4, $p \in U$.
3. The case where p maps the open interval $(0, 1)$ into $(0, 1)$ with $0 < p(0), p(1) \le 1$. By Corollary 2, $p \in U$.
4. The case where p maps the open interval $(0, 1)$ into $(0, 1)$ with $p(0) = 0$ and $p(1) = 1$. By Theorem 5, $p \in U$.
5. The case where p maps the open interval $(0, 1)$ into $(0, 1)$ with $p(0) = 1$ and $p(1) = 0$. By Corollary 3, $p \in U$.

In summary, for any polynomial $p \in V$, we have $p \in U$. Thus, $V \subseteq U$. □

Based on Theorems 3 and 6, we have proved Theorem 2:

$$V = U. \qquad \Box$$

5 Discussion

We are interested in Bernstein polynomials with coefficients in the unit interval because this concept has applications in the area of digital circuit design. Specifically, the concept is a mathematical prerequisite for a design methodology that we have been advocating called *stochastic logic* [7–9]. We provide a brief overview of this application and point the reader to further sources.

Stochastic logic implements Boolean function with inputs that are *random* Boolean variables. A Boolean function f on n variables $x_1, x_2, \ldots, x_n$ is a mapping

$$f : \{0, 1\}^n \to \{0, 1\}.$$

With stochastic logic, the variables $x_1, x_2, \ldots, x_n$ are a set of independent random Boolean variables, i.e., for $1 \le i \le n$, x_i has a certain probability p_i $(0 \le p_i \le 1)$ of being one and a probability $1 - p_i$ of being zero. With random Boolean variables as inputs, the output is also a random Boolean variable: the function f has a certain probability p_o of being one and a probability $1 - p_o$ of being zero.

If implemented by digital circuitry, stochastic logic can be viewed as computation that transforms input probabilities into output probabilities [8]. Given an arbitrary Boolean function f and a set of input probabilities $p_1, p_2, \ldots, p_n$ that correspond to the probabilities of the input random Boolean variables being one, the output probability p_o is a function on $p_1, p_2, \ldots, p_n$. In fact, we have shown that the general form of the function is a multivariate polynomial on variables $p_1, \ldots, p_n$ with integer coefficients and with the degree of each variable no more than one [9].

Example 3
Consider stochastic logic based on the Boolean function

$$f(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee (\neg x_1 \wedge x_3),$$

where $\wedge$ means logical AND (conjunction), $\vee$ means logical OR (disjunction), and $\neg$ means logical negation.

The Boolean function f evaluates to one if and only if the 3-tuple (x_1, x_2, x_3) takes values from the set $\{(0,0,1), (0,1,1), (1,1,0), (1,1,1)\}$. The probability of the output being one is

$$\begin{aligned} p_o &= Pr(f = 1) = Pr\left(x_1, x_2, x_3 :\ (x_1, x_2, x_3) \in \{(0,0,1), (0,1,1), (1,1,0), (1,1,1)\}\right) \\ &= Pr(x_1 = 0, x_2 = 0, x_3 = 1) + Pr(x_1 = 0, x_2 = 1, x_3 = 1) \\ &+ Pr(x_1 = 1, x_2 = 1, x_3 = 0) + Pr(x_1 = 1, x_2 = 1, x_3 = 1). \end{aligned}$$

If x_1, x_2, and x_3 are independent random Boolean variables with probability p_1, p_2, and p_3 of being one, respectively, then we obtain

$$\begin{aligned} p_o &= (1 - p_1)(1 - p_2)p_3 + (1 - p_1)p_2p_3 + p_1p_2(1 - p_3) + p_1p_2p_3 \\ &= (1 - p_1)p_3 + p_1p_2 \\ &= p_1p_2 + p_3 - p_1p_3, \end{aligned} \tag{46}$$

which confirms that the function computed by stochastic logic is a multivariate polynomial on arguments p_1, p_2, and p_3 with integer coefficients and with the degree of each variable no more than 1. □

In design problems, we encounter univariate polynomials that have real coefficients and degree greater than 1. Sometimes it is possible to implement these by setting some of the probabilities p_i to be a common variable x and the others to be constants. For example, if we set $p_1 = p_3 = x$ and $p_2 = 0.75$ in Equation (46), then we obtain the polynomial $g(x) = 1.75x - x^2$. With different underlying Boolean functions and different assignments of probability values, we can implement many different univariate polynomials.

An interesting and yet practical question is: which univariate polynomials can be implemented by stochastic logic? Define the set W to be the set of (univariate) polynomials that can be implemented. We are interested in characterizing the set W.

In [9] we showed that $U \subseteq W$, i.e., if a polynomial can be expressed as a Bernstein polynomial with all coefficients in the unit interval, then the polynomial can be implemented by stochastic logic. In this paper, we proved that $V = U$. Thus, we have $V \subseteq W$.

Further, in [9] we showed that $W \subseteq V$, i.e., if a polynomial can be implemented by stochastic logic, then it is either identically equal to 0 or equal to 1, or it maps the open interval $(0, 1)$ into the open interval $(0, 1)$ and maps the points 0 and 1 into the closed interval $[0, 1]$. Therefore, we conclude that $W = V$, i.e., a polynomial can be implemented by stochastic logic if and only if it is either identically equal to 0 or equal to 1, or it maps the open interval $(0, 1)$ into the open interval $(0, 1)$ and maps the points 0 and 1 into the closed interval $[0, 1]$.

This necessary and sufficient conditions allows us to answer the question of whether any given polynomial can be implemented by stochastic logic. Based on the mathematics, we have proposed a constructive design method [9]. An overview of the method and its applications in circuit design will appear in a forthcoming "Research Highlights" article in Communications of the ACM [10].

References

[1] P. J. Davis, *Interpolation and Approximation.* Blaisdell Publishing Company, 1963.

[2] G. Lorentz, *Bernstein Polynomials.* University of Toronto Press, 1953.

[3] J. Berchtold and A. Bowyer, "Robust arithmetic for multivariate Bernstein-form polynomials," *Computer-Aided Design*, vol. 32, no. 11, pp. 681–689, 2000.

[4] S. N. Bernstein, "Démonstration du théorème de Weierstrass fondée sur le calcul des probabilités," *Communications of the Kharkov Mathematical Society*, vol. 13, pp. 1–2, 1912.

[5] K. M. Levasseur, "A probabilistic proof of the Weierstrass approximation theorem," *The American Mathematical Monthly*, vol. 91, no. 4, pp. 249–250, 1984.

[6] R. Farouki and V. Rajan, "On the numerical condition of polynomials in Bernstein form," *Computer Aided Geometric Design*, vol. 4, no. 3, pp. 191–216, 1987.

[7] B. Gaines, "Stochastic computing systems," in *Advances in Information Systems Science.* Plenum, 1969, vol. 2, ch. 2, pp. 37–172.

[8] B. Brown and H. Card, "Stochastic neural computation I: Computational elements," *IEEE Transactions on Computers*, vol. 50, no. 9, pp. 891–905, 2001.

[9] W. Qian and M. D. Riedel, "The synthesis of robust polynomial arithmetic with stochastic logic," in *Design Automation Conference*, 2008, pp. 648–653.

[10] ——, "The synthesis of stochastic logic," *Communications of the ACM (to appear)*, 2010.