

A CHARACTERIZATION OF HOMEOMORPHIC BERNOULLI TRIAL MEASURES

ANDREW Q. YINGST

ABSTRACT. We give conditions which, given two Bernoulli trial measures, determine whether there exists a homeomorphism of Cantor space which sends one measure to the other, answering a question of Oxtoby. We then provide examples, relating these results to the notions of good and refinable measures on Cantor space.

1. INTRODUCTION

1.1. Homeomorphic measures. Two measures μ and ν defined on the Borel subsets of a topological space X are said to be *homeomorphic* or *topologically equivalent* provided there exists a homeomorphism h of X onto X such that μ is the image measure of ν under h : $\mu = \nu h^{-1}$. This means $\mu(E) = \nu(h^{-1}(E))$ for each Borel subset E of X .

One may be interested in the structure of these equivalence classes of measures or in a particular equivalence class. For example, a probability measure μ on $[0, 1]$ is topologically equivalent to Lebesgue measure if and only if μ gives every point measure 0 and every non-empty open set positive measure. (The distribution function of μ is a homeomorphism on $[0, 1]$ witnessing this equivalence.) This is a special case of a result of Oxtoby and Ulam [15], who characterized those probability measures μ on finite dimensional cubes $[0, 1]^n$ which are homeomorphic to Lebesgue measure. For this to be so, μ must give points measure 0, non-empty open sets positive measure, and the boundary of the cube measure 0. Later Oxtoby and Prasad [14] extended this result to the Hilbert cube. These results have been extended and applied to various manifolds. The book of Alpern and Prasad [2] is an excellent source for these developments. Oxtoby [13] also characterized those probability measures on the space of irrational numbers in $[0, 1]$ which are homeomorphic to Lebesgue measure as those which give points measure zero and open sets positive measure.

It turns out that the Cantor space is more rigid than the above spaces for measure homeomorphisms – it is not true that two probability measures on $\mathcal{C} = \{0, 1\}^{\mathbb{N}}$ which give points measure 0 and non-empty open sets positive measure are homeomorphic. Since \mathcal{C} has countably many clopen sets, the set of values taken on clopen sets by such a measure will be a countable dense subset of $[0, 1]$. We will refer to this set

Received by the editors July 17, 2006.

2000 *Mathematics Subject Classification.* Primary 28D05; Secondary 37B05, 28C15.

©2007 American Mathematical Society
Reverts to public domain 28 years from publication

as the *clopen values set* of such a measure. Even two well behaved measures on \mathcal{C} will typically have different clopen values sets, and so cannot be homeomorphic. A first conjecture at getting around this may be to ask whether any two measures on \mathcal{C} with the same clopen values sets are homeomorphic. This turns out to fail, and it appears unlikely that adding additional conditions will provide a satisfactory theorem, as in some sense there are just too many measures possible. We therefore restrict our attention to a particular class of measures which arise frequently.

1.2. Bernoulli trial measure. Regard $\mathcal{C} = \{0, 1\}^{\mathbb{N}}$ as the set of all infinite words on the alphabet $\{0, 1\}$, and for $e = e_1 e_2 \dots e_n$ a finite word, we let $[e]$ denote the set of all infinite words beginning with e . We refer to such sets as *cylinder sets*, and note they are clopen and they form a basis for \mathcal{C} . We say the *length* of such a set is the length of the word e .

If $0 \leq r \leq 1$, we let μ_r denote the Bernoulli trial measure with probability r of success, sometimes called the coin tossing measure. To be specific, μ_r is the unique measure for which the sets $\{\pi_n^{-1}(1)\}_{n \geq 1}$ are independent, and each has measure r . Note that if e is a word of length n having i occurrences of the letter 1, then $\mu_r([e]) = r^i(1-r)^{n-i}$.

When the measures μ_r and μ_s are homeomorphic, we say r and s are *topologically equivalent*, and we write $r \sim_{top} s$. In 1979, Oxtoby began to publish papers investigating this equivalence relation on $[0, 1]$. In this paper we give a complete characterization of when two such measures are homeomorphic, answering Oxtoby's question.

In Section 2 we define terminology, review some previous results, and prove a few preliminary lemmas, finally stating our main result, that four statements are equivalent. Sections 3 through 5 prove this result, each addressing one of the three non-trivial implications. Section 6 provides some examples and additional results, and raises some questions for further research.

2. THE MAIN THEOREM

2.1. Terminology. When discussing Bernoulli trial measures on \mathcal{C} , the following notation used by Austin [3] is valuable.

Definition 2.1. A polynomial p is said to be a *partition polynomial* if it is expressible in the form

$$p(x) = \sum_{i=0}^n a_i x^i (1-x)^{n-i},$$

where n is a non-negative integer and each a_i is an integer with $0 \leq a_i \leq \binom{n}{i}$. The class of all partition polynomials will be denoted as \mathcal{P} .

Any clopen set C in \mathcal{C} is expressible as a finite union of cylinder sets of the same length, say n , and the μ_r measure of one of these cylinder sets $[e_j]$ is $r^i(1-r)^{n-i}$, where i is the number of 1's in the string e_j defining this cylinder set. The maximum number of cylinder sets of length n in C having i 1's is $\binom{n}{i}$. This leads to the observation that, for any clopen set C in \mathcal{C} , there is a polynomial $p \in \mathcal{P}$ such that $\mu_r(C) = p(r)$ for all $r \in [0, 1]$. Likewise for any $p \in \mathcal{P}$, there are many clopen sets

which have this relationship. We will describe such a clopen set as *associated* with p , or say that this is the polynomial *associated* with this clopen set. For $r \in [0, 1]$, we will let $\mathcal{P}(r)$ denote $\{p(r) : p \in \mathcal{P}\}$. So $\mathcal{P}(r)$ is the clopen values set for the measure μ_r .

Note that if $0 < r < 1$, and C is a clopen set in \mathcal{C} , we may leave C fixed and vary r , in which case, $\mu_r(C)$ is the partition polynomial associated with C . On the other hand, we may leave r fixed and vary C , in which case we get the clopen values set for the measure μ_r . When we aren't giving a name to the partition polynomial of C , we refer to it as $\mu_x(C)$.

Definition 2.2. Let $0 < r, s < 1$. The number s is said to be *binomially reducible* to r when there is a partition polynomial p such that $s = p(r)$.

It is known that μ_s is *continuously reducible* to, or is a continuous image of, the measure μ_r (i.e., $\mu_s = \mu_r \circ g^{-1}$ for some continuous $g : \mathcal{C} \rightarrow \mathcal{C}$) if and only if s is binomially reducible to r [10]. Note that this property is transitive, giving us that binomial reducibility is transitive as well. (Theorem 2.6 will make it clear that partition polynomials are closed under composition for a more transparent argument of this fact.) Transitivity tells us that if s is binomially reducible to r , then every element of $\mathcal{P}(s)$ is as well. We collect these facts in the following theorem.

Theorem 2.3. Let $0 \leq r, s \leq 1$. The following are equivalent:

- (i) s is binomially reducible to r .
- (ii) $s \in \mathcal{P}(r)$.
- (iii) $\mathcal{P}(s) \subseteq \mathcal{P}(r)$.
- (iv) μ_s is continuously reducible to μ_r .

Thus, we have another natural equivalence relation on $[0, 1]$.

Definition 2.4. Let $0 \leq r, s \leq 1$. Then r is *binomially equivalent* to s , denoted $r \sim_{bin} s$, provided r is binomially reducible to s and s is binomially reducible to r , or, equivalently, each of the measures μ_r and μ_s is a continuous image of the other.

Since $\mathcal{P}(r)$ is the clopen values set for the measure μ_r , the previous theorem implies that r and s are binomially equivalent if and only if the measures μ_r and μ_s have the same clopen values set. Hence it is clear that binomial equivalence is a necessary condition for topological equivalence. (In symbols, $r \sim_{top} s \implies r \sim_{bin} s$.) In a paper to appear, Austin [3] provided a particular example witnessing that it is not sufficient. We discuss this example further in Section 6.

Notice that x and $1 - x$ are partition polynomials, so that if $r = s$ or if $r = 1 - s$ (and so $s = 1 - r$), then r and s are binomially equivalent. Also, r and s are topologically equivalent, in the first case by the identity homeomorphism, and in the second by the homeomorphism which switches 0's and 1's. When $r = s$ or $r = 1 - s$, we will say that r and s are *trivially* binomially equivalent, and are *trivially* topologically equivalent. We will also say μ_r and μ_s are *trivially* homeomorphic, even though there are many homeomorphisms witnessing their equivalence, for example, any permutation of indices.

Many cases of the homeomorphism problem have already been settled. If r and s are binomially equivalent, then there are partition polynomials f and g such that $r = f(s)$, and $s = g(r)$. If $r \neq s$ and $r \neq 1 - s$, then f is non-linear, as the only linear partition polynomials are x and $1 - x$. (This can be argued directly, but will

be clear after Theorem 2.6, which characterizes partition polynomials.) Hence $f \circ g$ is non-linear, and in particular is not the identity. So $r = f \circ g(r)$ is a non-trivial polynomial relation satisfied by r , and hence r and s must be algebraic. Also, in this case r and s have the same algebraic degree. Moreover, r is an algebraic integer if and only if s is. Huang [8] showed that if r is an algebraic integer of degree 2, and $r \sim_{bin} s$, then $r = s$ or $r = 1 - s$. In fact, Navarro-Bermudez [11] showed that if r is rational or transcendental and $r \sim_{bin} s$, then $r = s$ or $r = 1 - s$. We gather these facts in the following theorem.

Theorem 2.5 (various authors). *For r rational, transcendental, or an algebraic integer of degree 2, the \sim_{top} equivalence class containing r and the \sim_{bin} equivalence class containing r are both equal to $\{r, 1 - r\}$.*

On the other hand, it is known that for every $n \geq 3$, there are algebraic integers r of degree n such that the \sim_{bin} equivalence class containing r has at least 4 elements [8]. (In fact, Pinch [16] showed that, if $n = 2^{k+1}$, then there is an algebraic integer r of degree n with at least $2k$ distinct numbers binomially equivalent to it.) One example of these is the solution of

$$r^3 + r^2 - 1 = 0$$

lying in the open interval $(0, 1)$. For this value of r , it turns out that $s = r^2 \sim_{bin} r$, and Navarro-Bermudez and Oxtoby [12] proved that $r \sim_{top} s$ via a simple homeomorphism, actually, a block code map. This was the first non-trivial example of topologically equivalent Bernoulli trial measures.

Further examples were found by Dougherty, Mauldin and Yingst in [18], where it was argued that if r and s are binomially equivalent, and satisfy an additional property called *refinability*, then r and s are topologically equivalent. A simple algebraic characterization of refinability was proved, and this was used to provide examples of algebraic integers which are topologically equivalent to at least n distinct numbers, for any large n . These examples are reviewed in Section 6.

2.2. Partition polynomials. Recall that partition polynomials are those of the form $\sum_{i=0}^n a_i x^i (1-x)^{n-i}$, for some n and some integers $0 \leq a_i \leq \binom{n}{i}$. Further recall that partition polynomials correspond with clopen sets in \mathcal{C} in the sense that if U is clopen, $p(x) = \mu_x(U)$ is a partition polynomial.

The partition polynomials can be manipulated in much the same way as their associated clopen sets. A clopen set $C \subset \mathcal{C}$ can be written as a finite union of cylinder sets each of the same length n . We can then refine C into cylinder sets having a common length equal to any integer larger than n . We call the smallest such n the *minimal length* of C . Similarly, any partition polynomial p can be expressed in *partition form*, i.e. the form of the definition, for some degree n . By repeatedly multiplying by $(x) + (1-x)$, we can express p in partition form for any degree greater than n . The smallest such n will be called the *partition degree* of p .

Consider the matrix $A = (a_{ij})_{i,j=0}^n$ where a_{ij} is the coefficient of x^j in the expansion of $x^i(1-x)^{n-i}$. The matrix A is triangular with 1's on the diagonal. This matrix is invertible, so we have $\{x^i(1-x)^{n-i}\}_{i=0}^n$ is a basis of the space of polynomials of degree $\leq n$. Further, this is an integer matrix with determinant 1, so such a polynomial has integer coefficients if and only if it has integer coefficients when expressed as a linear combination of this basis. We therefore have that any polynomial $p \in \mathbb{Z}[x]$ of degree n or less can be expressed uniquely as an integer linear

combination of these. However, even if p is a partition polynomial, we can have no expectation that for this smallest possible choice of n , the coefficients will fall into the legal ranges for a partition polynomial. One example is $p(x) = 3x(1 - x)$. This would appear not to be a partition polynomial, as $3 > \binom{2}{1}$, but we may multiply by $(x) + (1 - x)$ once and write $p(x) = 3x(1 - x)^2 + 3x^2(1 - x)$, revealing that p actually is a partition polynomial. Indeed, the partition degree of a partition polynomial can be much larger than its actual degree. For example, the polynomial $q(x) = 6x^2(1 - x)$ is a partition polynomial, but its coefficients will not be in the correct ranges until expressed taking $n = 14$. Because of these difficulties, the following theorem characterizing partition polynomials is especially valuable. This theorem and the following one appeared previously in [18].

Theorem 2.6. *If p is a polynomial with integer coefficients, then p is a partition polynomial if and only if p maps $(0, 1)$ into $(0, 1)$, or p equals 0 or 1.*

This theorem follows easily from a result of Hausdorff (originally in [7], but it may be easier to find in [17], part 6 #49) that any polynomial which is positive on $(-1, 1)$ can be expressed as a finite sum $\sum c_i(1 + x)^j(1 - x)^k$ with positive coefficients c_i . The argument we present includes a modification of the proof in [17].

Proof. If $p(x) = \sum_{i=0}^n a_i x^i(1 - x)^{n-i}$ is a partition polynomial, then either $p = 0$, or one of the coefficients is positive, in which case p is positive on $(0, 1)$. The same is true of $(1 - p)(x) = \sum_{i=0}^n (\binom{n}{i} - a_i)x^i(1 - x)^{n-i}$, so that either $p < 1$ on $(0, 1)$, or $p = 1$. So one direction is proven.

Now, let p be a polynomial with integer coefficients which is positive on $(0, 1)$. Then p can be factored into linear and quadratic polynomials with real coefficients which are irreducible over $\mathbb{R}[x]$. None of these factors can have a root in $(0, 1)$, so by changing signs of pairs if necessary, we may assume each is positive on $(0, 1)$. We first argue that for each of these, there is an n for which it can be written as a linear combination of $\{x^i(1 - x)^{n-i}\}_{i=0}^n$ using non-negative (real) coefficients.

If f is a linear factor of p , say $f(x) = ax + b$. Then $f(x) = (a + b)x + b(1 - x)$. Since f is positive on $(0, 1)$, we will have that $f(0) = b$ and $f(1) = a + b$ are non-negative.

If f is a quadratic factor of p , say $f(x) = ax^2 + bx + c$, since f is irreducible over $\mathbb{R}[x]$, we know that 0 and 1 aren't roots of f . Therefore, f is positive on $[0, 1]$. We may find $\epsilon > 0$ such that f is greater than ϵ on $[0, 1]$. We multiply each term of f by a binomial expansion of 1:

$$\begin{aligned} f(x) &= \left(ax^2 \sum_{i=0}^{n-2} \binom{n-2}{i} x^{n-2-i}(1-x)^i \right) + \left(bx \sum_{i=0}^{n-1} \binom{n-1}{i} x^{n-1-i}(1-x)^i \right) \\ &\quad + \left(c \sum_{i=0}^n \binom{n}{i} x^{n-i}(1-x)^i \right) \\ &= \left[\sum_{i=0}^{n-2} \left(a \binom{n-2}{i} + b \binom{n-1}{i} + c \binom{n}{i} \right) x^{n-i}(1-x)^i \right] \\ &\quad + (b + nc)x^1(1-x)^{n-1} + cx^0(1-x)^n. \end{aligned}$$

We have that $c = f(0) > 0$, so that the final two coefficients will be non-negative for any sufficiently large n . For the remaining coefficients:

$$\begin{aligned} a \binom{n-2}{i} + b \binom{n-1}{i} + c \binom{n}{i} &= \binom{n}{i} \left(a \frac{(n-i)(n-1-i)}{n(n-1)} + b \frac{n-i}{n} + c \right) \\ &= \binom{n}{i} \left[f\left(\frac{n-i}{n}\right) + a \frac{n-i}{n} \left(\frac{n-1-i}{n-1} - \frac{n-i}{n} \right) \right] \\ &= \binom{n}{i} \left[f\left(\frac{n-i}{n}\right) - a \frac{n-i}{n} \frac{i}{n-1} \right] > \binom{n}{i} \left[f\left(\frac{n-i}{n}\right) - \frac{|a|}{n-1} \right], \end{aligned}$$

which will be positive for all i if n is so large that $\frac{|a|}{n-1} < \epsilon$.

Now note that if g_1 is a non-negative linear combination of elements of $\mathcal{B}_n = \{x^i(1-x)^{n-i}\}_{i=0}^n$, and if g_2 is a non-negative linear combination of \mathcal{B}_m , then $g_1 g_2$ is naturally a non-negative linear combination of \mathcal{B}_{m+n} . Thus p is expressible as a non-negative linear combination of \mathcal{B}_N for some large N , as we have so written the factors of p . Now, if p maps $(0, 1)$ into $(0, 1)$, then $1 - p$ is also positive on $(0, 1)$, and by the same argument we may express $1 - p$ as a linear combination of elements of \mathcal{B}_M for some large M . By repeatedly multiplying one of these by $(x) + (1 - x)$, we may assume $M = N$.

We have written $p(x) = \sum_{i=0}^N a_i x^i (1-x)^{N-i}$ and $(1-p)(x) = \sum_{i=0}^N b_i x^i (1-x)^{N-i}$, with $a_i, b_i \geq 0$. But $p(x) = 1 - (1-p)(x) = \sum_{i=0}^N (\binom{N}{i} - b_i) x^i (1-x)^{N-i}$. By linear independence, we must have $a_i = \binom{N}{i} - b_i$, and so $0 \leq a_i \leq \binom{N}{i}$. As mentioned before, p will have integer coefficients in the usual sense if and only if a_i is an integer for $0 \leq i \leq N$. \square

It's clear that if $C_2 \subseteq C_1$ are clopen sets in \mathcal{C} , then the measure properties of μ_r will give that the associated partition polynomials satisfy $p_2 \leq p_1$ on $(0, 1)$. With the above result, we verify a sort of converse to this.

Theorem 2.7. *If C_2 is a clopen set in \mathcal{C} whose associated polynomial is p_2 , and if p_1 is a polynomial with integer coefficients such that $0 < p_1 < p_2$ on $(0, 1)$, then there is a clopen set $C_1 \subset C_2$ whose associated polynomial is p_1 .*

Proof. Both p_1 and $p_2 - p_1$ are partition polynomials. Let n be greater than the minimal length of C_1 , and the partition degrees of p_1, p_2 and $p_2 - p_1$. So when written in partition form at level n (as a linear combination of $\{x^i(1-x)^{n-i}\}$), the coefficients of p_1 and of $p_2 - p_1$ add to make the coefficients of p_2 . In particular, the coefficients of p_1 are less than or equal to the coefficients of p_2 . But the terms of this expression of p_2 correspond with elements in the partition of C_2 into cylinder sets of length n . So we may construct C_1 by collecting some of these sets, the number of each type to be determined by the coefficients of p_1 . \square

2.3. The main theorem. Note that the partition polynomials x and $1 - x$ are somewhat special. They are the only linear partition polynomials, and further, if r and s are binomially equivalent via partition polynomials from the set $\{x, 1 - x\}$, then r and s are topologically equivalent. Strangely, it appears that the important properties of x and $1 - x$ are their behavior at 0 and 1.

Definition 2.8. We say that a partition polynomial f is *x-like* when:

$$f(0) = 0, f'(0) = 1, f(1) = 1, f'(1) = 1.$$

We say that a partition polynomial f is $(1 - x)$ -like when:

$$f(0) = 1, f'(0) = -1, f(1) = 0, f'(1) = -1.$$

We refer to the collection of all x -like partition polynomials as \mathcal{P}_x , and we refer to the collection of all $(1 - x)$ -like partition polynomials as \mathcal{P}_{1-x} .

Hence, \mathcal{P}_x and \mathcal{P}_{1-x} are rather small subsets of \mathcal{P} . It is worth noting that the sets \mathcal{P}_x and $\mathcal{P}_x \cup \mathcal{P}_{1-x}$ are each closed under composition, just as \mathcal{P} is.

By Definition 2.4, two numbers are binomially equivalent when they are expressible as partition polynomials in each other. By restricting this to x -like and $(1 - x)$ -like partition polynomials, we will obtain the stronger condition of topological equivalence. We will prove the following complete characterization at the end of the section.

Theorem 2.9. *Let $0 \leq r, s \leq 1$. Then r and s are topologically equivalent if and only if there are partition polynomials f and g , each of which is either x -like or $(1 - x)$ -like, such that $r = f(s)$, and $s = g(r)$.*

In this case, we will actually be able to construct a homeomorphism with some additional special properties, which require a definition.

Definition 2.10. A homeomorphism h of \mathcal{C} is said to *count 0's* if whenever w is a word in \mathcal{C} which is eventually 1, we have that $h(w)$ is eventually 1, and that w and $h(w)$ have the same finite number of 0's. We say h *counts 1's* if h acts similarly on the set of words which are eventually 0.

We say a homeomorphism h of \mathcal{C} *switch-counts 0's and 1's* if h sends words which are eventually 1 to words which are eventually 0, and sends words which are eventually 0 to words which are eventually 1, while similarly preserving the number of exceptional characters.

We now state the main result of this paper, which will be proved over the next three sections.

Theorem 2.11. *Let r and s be algebraic numbers in $(0, 1)$, and let R and S be their irreducible polynomials. Further, suppose f and g are partition polynomials such that $r = f(s)$ and $s = g(r)$. Then the following are equivalent:*

- (i) *The measures μ_r and μ_s are homeomorphic.*
- (ii) *If $R(0) \neq \pm 1$ and $g(0) = 0$, or if $R(1) \neq \pm 1$ and $g(1) = 1$, then*
 - (a) $R(0)|g'(0) - 1$,
 - (b) $R(1)|g'(1) - 1$,
 - (c) $S(0)|f'(0) - 1$,
 - (d) $S(1)|f'(1) - 1$.*If $R(0) \neq \pm 1$ and $g(0) = 1$, or if $R(1) \neq \pm 1$ and $g(1) = 0$, then*
 - (a) $R(0)|g'(0) + 1$,
 - (b) $R(1)|g'(1) + 1$,
 - (c) $S(0)|f'(0) + 1$,
 - (d) $S(1)|f'(1) + 1$.
- (iii) *There are partition polynomials \hat{f} and \hat{g} , either both x -like or both $(1 - x)$ -like, such that $r = \hat{f}(s)$ and $s = \hat{g}(r)$.*
- (iv) *There is a homeomorphism h of \mathcal{C} which either counts 0's and 1's or switch-counts 0's and 1's, such that $\mu_r = \mu_s \circ h$.*

In this paper, when we refer to the *irreducible polynomial* of an algebraic number, r , we mean irreducible over the ring $\mathbb{Z}[x]$. (That is, we mean the integer polynomial of minimal degree which r solves, whose coefficients have a greatest common divisor of 1. This polynomial is unique up to sign.) This implies that if R is the irreducible polynomial of r and if p is some integer polynomial with $p(r) = 0$, then by Gauss' lemma, $p = QR$ for some integer polynomial Q . We will frequently use this fact without comment in the arguments of this paper.

The above theorem gives us two tools for examining homeomorphisms. We may use the third statement to generate examples of topologically equivalent numbers by finding x -like partition polynomials f and g so that $f \circ g = id$ has non-trivial solutions in $(0, 1)$. On the other hand, given two binomially equivalent numbers (and given partition polynomials witnessing this), we may use the second statement to check whether they are topologically equivalent. Of course, this test only holds if we already know that r and s are binomially equivalent and we have partition polynomials witnessing this fact. Theorem 6.11 provides some clarification of this issue, telling us, given some f and g with integer coefficients having $r = f(s)$ and $s = g(r)$, when f and g can be replaced by partition polynomials. From this point, statement two tells us when they can be further replaced by x -like or $(1 - x)$ -like partition polynomials, and hence when $r \sim_{top} s$.

It is clear that the fourth statement implies the first. The other three necessary implications require many lemmas, and each has one of the three following sections devoted to its proof.

We now prove Theorem 2.9 assuming Theorem 2.11.

Proof. If f and g are either both x -like or both $(1 - x)$ -like, then the third part of Theorem 2.11 applies and we directly have that r and s are topologically equivalent. If one is x -like and the other is $(1 - x)$ -like, then we have that $(f \circ g - id)(r) = 0$, so $R|f \circ g - id$. In particular, we have $R(0)|f(g(0)) - 0 = 1$ and $R(1)|f(g(1)) - 1 = -1$. So $R(0) = \pm 1$ and $R(1) = \pm 1$. The second part of Theorem 2.11 holds trivially and so r and s are topologically equivalent. \square

It is worth noting that in the proof given above, we found that r and s were topologically equivalent because $R(0) = \pm 1$ and $R(1) = \pm 1$. In Section 6, we will see that this is the case when μ_r and μ_s are what will be called "refinable" measures. An alternate proof of Theorem 2.9 may be seen by noting that if f and g are an x -like and a $(1 - x)$ -like partition polynomial with $r = f(s)$ and $s = g(r)$, then $\hat{f} = f \circ g \circ f$ and $\hat{g} = g$ are partition polynomials with $r = \hat{f}(s)$ and $s = \hat{g}(r)$, and are either both x -like or both $(1 - x)$ -like.

3. ONE IMPLIES TWO

In this section, we prove the first of the necessary implications. The observation which motivates this proof is that for C a cylinder set, and U a clopen subset, that the associated partition polynomial p_U of U is of the form $p_C q$, where p_C is the partition polynomial associated with C , and q is some partition polynomial.

3.1. Proof.

Theorem 3.1. *Let r and s be algebraic numbers in $(0, 1)$, and let R and S be their irreducible polynomials. Further, suppose f and g are partition polynomials*

such that $r = f(s)$ and $s = g(r)$, and that h is a homeomorphism of \mathcal{C} such that $\mu_r = \mu_s \circ h$.

If $R(0) \neq \pm 1$ and $g(0) = 0$, or if $R(1) \neq \pm 1$ and $g(1) = 1$, then

- (i) $R(0)|g'(0) - 1$,
- (ii) $R(1)|g'(1) - 1$,
- (iii) $S(0)|f'(0) - 1$,
- (iv) $S(1)|f'(1) - 1$.

If $R(0) \neq \pm 1$ and $g(0) = 1$, or if $R(1) \neq \pm 1$ and $g(1) = 0$, then

- (i) $R(0)|g'(0) + 1$,
- (ii) $R(1)|g'(1) + 1$,
- (iii) $S(0)|f'(0) + 1$,
- (iv) $S(1)|f'(1) + 1$.

Proof. We view the strange conclusion of the theorem as sixteen statements: there are four if's, each giving four then's. We will use a number of symmetries to reduce the number of statements requiring proof. To help justify our simplifying hypotheses, we regard the theorem as a statement about a system (r, s, R, S, f, g, h) satisfying the first two sentences, which we will call a *homeomorphism system*. The next several paragraphs will reduce the problem to showing two of the sixteen statements, by cutting the number in half three times.

If (r, s, R, S, f, g, h) is a homeomorphism system, let $\hat{r} = 1 - r$, $\hat{s} = s$, $\hat{R}(x) = R(1 - x)$, $\hat{S} = S$, $\hat{f}(x) = 1 - f(x)$, and $\hat{g}(x) = g(1 - x)$. So \hat{r} , \hat{s} are algebraic numbers, \hat{R} and \hat{S} are their irreducible polynomials, and \hat{f} and \hat{g} are partition polynomials such that $\hat{r} = \hat{f}(\hat{s})$ and $\hat{s} = \hat{g}(\hat{r})$. Let Φ denote the homeomorphism of \mathcal{C} which switches 0's and 1's. So $\mu_x \circ \Phi = \mu_{1-x}$, for all x . In particular, $\mu_{\hat{r}} = \mu_r \circ \Phi = \mu_s \circ h \circ \Phi$. Let $\hat{h} = h \circ \Phi$. So $(\hat{r}, \hat{s}, \hat{R}, \hat{S}, \hat{f}, \hat{g}, \hat{h})$ is a homeomorphism system also. A straightforward but lengthy verification shows that the first eight of our sixteen statements (the first two large if's) will hold for the (r, s) system if and only if the last eight statements hold for our (\hat{r}, \hat{s}) system. Hence it suffices to show the first eight hold for all homeomorphism systems.

Consider $\bar{r} = 1 - r$, $\bar{s} = 1 - s$, $\bar{R}(x) = R(1 - x)$, $\bar{S}(x) = S(1 - x)$, $\bar{f}(x) = 1 - f(1 - x)$, $\bar{g}(x) = 1 - g(1 - x)$, and $\bar{h} = \Phi \circ h \circ \Phi$. Then as before, we have $(\bar{r}, \bar{s}, \bar{R}, \bar{S}, \bar{f}, \bar{g}, \bar{h})$ is a homeomorphism system, and it can be verified that the first four statements (the "if $R(0) \neq \pm 1$ and $g(0) = 0$ " statements) hold for the (r, s) system, if and only if the second set of four statements (the "if $R(1) \neq \pm 1$ and $g(1) = 1$ " statements) hold for the (\bar{r}, \bar{s}) system. Hence it suffices to show the first four statements hold for all homeomorphism systems.

Suppose (r, s, R, S, f, g, h) is a homeomorphism system with $R(0) \neq \pm 1$, and $g(0) = 0$. We have that $S(s) = S(g(r)) = 0$. So $S \circ g$ is an integer polynomial with r as a root. It must therefore be a multiple of R . That is, $R|S \circ g$. In particular, $R(0)|S \circ g(0) = S(0)$. So we must have $S(0) \neq \pm 1$. We also have that $r = f(s) = f(g(r))$. Therefore, $(f \circ g - id)(r) = 0$. Again, this tells us that $R|f \circ g - id$, and in particular, $R(0)|(f(g(0)) - 0 = f(0))$. But f is a partition polynomial, and so $f(0)$ is either 0 or 1. Since $R(0) \neq \pm 1$, we must have that $f(0) = 0$. We have argued that the assumptions of $R(0) \neq \pm 1$ and $g(0) = 0$ give two further statements that $S(0) \neq \pm 1$ and $f(0) = 0$, and the argument is symmetric so that the two are actually equivalent. This explains the apparent

asymmetry of the sixteen statements: Each of the four if's concerning g and R is equivalent to some similar statements about f and S .

For clarity, we restate that we have now reduced the problem to showing that for a homeomorphism system with $R(0) \neq \pm 1$ and $g(0) = 0$, we have

- (i) $R(0)|g'(0) - 1$,
- (ii) $R(1)|g'(1) - 1$,
- (iii) $S(0)|f'(0) - 1$,
- (iv) $S(1)|f'(1) - 1$.

We have also argued that a homeomorphism system satisfies $R(0) \neq \pm 1$ and $g(0) = 0$ if and only if it satisfies $S(0) \neq \pm 1$ and $f(0) = 0$. Because of this, we see that the homeomorphism system (r, s, R, S, f, g, h) satisfies the $R(0) \neq \pm 1, g(0) = 0$ hypotheses if and only if the homeomorphism system obtained by exchanging the roles of r and s does. (This system is $(s, r, S, R, g, f, h^{-1})$.) Also, it is clear that the first two of the conclusions above hold for the (r, s) system if and only if the last two hold for the (s, r) system. Hence it suffices to show that the first two conclusions hold for every homeomorphism system with $R(0) \neq \pm 1, g(0) = 0$. We will actually only argue one of these, and indicate how the proof of the second is similar.

Let (r, s, R, S, f, g, h) be a homeomorphism system with $R(0) \neq \pm 1$ and $g(0) = 0$. Let $w_0 = 1\bar{0} = 1000\dots \in \mathcal{C}$, and let $w_1 = 01\bar{0}$. We have that h is a homeomorphism, and so $h(w_0)$ and $h(w_1)$ cannot both be $\bar{0}$. Assume $h(w_0) \neq \bar{0}$. (The other case is similar.) We know therefore that there is some n such that $\pi_n(h(w_0)) = 1$. Let $A = \{w \in \mathcal{C} : \pi_n(w) = 1\}$. Then A is a clopen set whose associated partition polynomial is $\mu_x(A) = x$.

We know that $w_0 \in h^{-1}(A)$. By continuity, we know some cylinder set about w_0 is properly contained in $h^{-1}(A)$. That is, $[100\dots 0] \subsetneq h^{-1}(A)$. This gives that $h([100\dots 0]) \subsetneq A$, and if we let $q(x)$ denote the partition polynomial of $h([100\dots 0])$, we know that $0 < q(x) < x$ on $(0, 1)$. In particular, we know that $q(0) = 0$. So x is a factor of $q(x)$, and $\frac{q(x)}{x}$ is a polynomial with integer coefficients satisfying $0 < \frac{q(x)}{x} < 1$ on $(0, 1)$. So $\frac{q(x)}{x}$ is a partition polynomial. This gives us that $\frac{q(s)}{s} \in \mathcal{P}(s)$. But, calculating $q(s)$:

$$\frac{q(s)}{s} = \frac{\mu_s(h([100\dots 0]))}{s} = \frac{\mu_r([100\dots 0])}{g(r)} = \frac{r(1-r)^j}{g(r)} \in \mathcal{P}(s) = \mathcal{P}(r),$$

for some $j \geq 0$. (We know that $\mathcal{P}(s) = \mathcal{P}(r)$ by binomial equivalence.)

We therefore know that there is some partition polynomial p such that $r(1-r)^j = g(r)p(r)$. This implies that the polynomials $x(1-x)^j$ and $g(x)p(x)$ are congruent modulo $R(x)$, and we may write

$$x(1-x)^j = g(x)p(x) + Q(x)R(x)$$

for some integer polynomial $Q(x)$. Observe now that x divides the left hand side of the above equation. Also, we are under the assumption that $g(0) = 0$, so that x divides $g(x)$. This gives us that x divides $Q(x)R(x)$. Since R is irreducible and isn't x itself (since R has a root in $(0, 1)$), we have that x divides $Q(x)$. This gives $-R(x)\frac{Q(x)}{x} = \frac{g(x)}{x}p(x) - (1-x)^j$. Letting x go to zero gives that

$$-R(0)Q'(0) = g'(0)p(0) - 1.$$

But p is a partition polynomial, and $p(0) = 0$ gives a contradiction, since $R(0) \neq \pm 1$. So it must be that $p(0) = 1$ and $R(0)|g'(0) - 1$.

The argument that $R(1)|g'(1) - 1$ is similar to the one above, beginning by taking $w_0 = 0\bar{1}$ and $w_1 = 10\bar{1}$. □

4. TWO IMPLIES THREE

4.1. Lemmas. In this section we argue that if we have the divisibility properties of the second statement, then the partition polynomials f and g of the theorem may be replaced by partition polynomials which are either both x -like or both $(1 - x)$ -like. Note that the definitions of x -like and $(1 - x)$ -like describe local properties that f and g have at 0 and 1. Hence, our strategy to replace f and g with x -like and $(1 - x)$ -like polynomials will be to work one side at a time. We will describe properties which assure us that we may replace g with a polynomial which is x -like at 0, without affecting whether g is x -like at 1, and similarly when we may replace g with a polynomial which is x -like at 1, without affecting whether g is x -like at 0. (The same arguments will also apply to f .)

Each of these is again divided into two parts: we first must be able to assure that g takes the correct value at 0, and then must be able to assure that g takes the correct derivative at 0. (We will then use symmetry to apply these to the value and derivative of g at 1.) First we examine the value of g .

Lemma 4.1. *If $g \in \mathcal{P}$ with $g(0) = 1$, if R is an integer polynomial with $R(0) = \pm 1$, and if $0 < r < 1$ with $R(r) = 0$, then there is $\hat{g} \in \mathcal{P}$ such that $\hat{g}(0) = 0$, $\hat{g}(r) = g(r)$, $\hat{g}(1) = g(1)$, and $\hat{g}'(1) = g'(1)$.*

Proof. Define g_n as

$$g_n(x) = g(x) - R(0)R(x)(1 - x)^n.$$

Then if $n \geq 2$, we have that $g_n(0) = 0$, $g_n(r) = g(r)$, $g_n(1) = g(1)$, and $g'_n(1) = g'(1)$. It only remains to verify that for some large n , g_n is a partition polynomial. (Let \hat{g} be this g_n .) It is clear that g_n is a polynomial with integer coefficients, so by Theorem 2.6 it suffices to show that for large n we have $0 < g_n < 1$ on $(0, 1)$.

A simple computation verifies that $g'_n(0) \rightarrow \infty$, and so for some large n_1 , $g'_{n_1}(0) > 0$, and $g_{n_1}(0) = 0$. Hence, there is $\delta_1 > 0$ such that $0 < g_{n_1}(x)$ and $R(0)R(x) > 0$ for all x in $(0, \delta_1]$. On this interval, we have that g_n increases pointwise to g as n increases, and so for $n > n_1$ we have $0 < g_{n_1} < g_n < g < 1$ on $(0, \delta_1]$.

As $x \rightarrow 1$, we have that g increases to 1 or decreases to 0 at a polynomial rate. There are some constants c and m such that $\min\{g(x), 1 - g(x)\} = c(1 - x)^m + O((1 - x)^{m+1})$ as $x \rightarrow 1$. Fixing $n_2 > m$, we have that $|R(0)R(x)(1 - x)^{n_2}| < \min\{g(x), 1 - g(x)\}$ for $x \in [1 - \delta_2, 1)$, for some $\delta_2 > 0$. This implies that $|R(0)R(x)(1 - x)^n| < \min\{g(x), 1 - g(x)\}$ on $[1 - \delta_2, 1)$ for all $n > n_2$. From this, we get that $0 < g_n < 1$ on $[1 - \delta_2, 1)$.

Finally, since g is a partition polynomial, there is some $\epsilon > 0$ such that $\epsilon < g < 1 - \epsilon$ on the interval $[\delta_1, 1 - \delta_2]$. Also, R is bounded on $[0, 1]$, so there is $n_3 > 0$ such that $|R(0)R(x)(1 - x)^{n_3}| < \epsilon$ on $[\delta_1, 1 - \delta_2]$. For $n > n_3$, we will have that $0 < g_n < 1$ on $[\delta_1, 1 - \delta_2]$. Combining all of these, we have that if $n > n_1, n_2, n_3$, then $0 < g_n < 1$ on $(0, 1)$. □

Next we give conditions under which we may force g to have the correct derivative at 0.

Lemma 4.2. *If $g \in \mathcal{P}$ with $g(0) = 0$, if R is an integer polynomial with $R(0)|g'(0) - 1$, and if $0 < r < 1$ with $R(r) = 0$, then there is $\hat{g} \in \mathcal{P}$ such that $\hat{g}(0) = 0$, $\hat{g}'(0) = 1$, $\hat{g}(r) = g(r)$, $\hat{g}(1) = g(1)$, and $\hat{g}'(1) = g'(1)$.*

Proof. Define g_n as

$$g_n(x) = g(x) - \frac{g'(0) - 1}{R(0)}R(x)x(1 - x)^n.$$

(If $R(0) = 0$, then the theorem is trivial as $R(0)|g'(0) - 1$ implies $g'(0) = 1$. Take $\hat{g} = g$.) Then if $n \geq 2$, it's easy to verify that $g_n(0) = 0$, $g'_n(0) = 1$, $g_n(r) = g(r)$, $g_n(1) = g(1)$, and $g'_n(1) = g'(1)$. It only remains to verify that for some large n , g_n is a partition polynomial. As before, it is clear that g_n is a polynomial with integer coefficients, so by Theorem 2.6 it suffices to show that for large n we have $0 < g_n < 1$ on $(0, 1)$.

Let $n_1 = 2$. Since $g'_{n_1}(0) = 1$, we may find $\delta_1 > 0$ such that $0 < g_{n_1}(x) < 1$, and $\frac{R(x)}{R(0)} > 0$ for x in $(0, \delta_1]$. On this interval, g_n either decreases to g pointwise if $g'(0) - 1 < 0$, or g_n increases to g pointwise if $g'(0) - 1 > 0$. (If $g'(0) = 1$, then let $\hat{g} = g$ and we're done.) In either of these cases, we have for $n > n_1$ that g_n lies between g_{n_1} and g on $(0, \delta_1]$, each of which is between 0 and 1 on $(0, \delta_1]$. Hence, we have for $n > n_1$, that $0 < g_n < 1$ on $(0, \delta_1]$.

The remainder of the argument is similar to the argument of the previous lemma. There are constants c and m such that $\min\{g(x), 1 - g(x)\} = c(1 - x)^m + O((1 - x)^{m+1})$ as $x \rightarrow 1$. If $n_2 > m$, we have that there is a constant $\delta_2 > 0$ such that $|\frac{g'(0)-1}{R(0)}R(x)x(1 - x)^{n_2}| < \min\{g(x), 1 - g(x)\}$ for $x \in [1 - \delta_2, 1)$. This inequality will also hold for $n > n_2$, and so for $n > n_2$, we have $0 < g_n < 1$ on $[1 - \delta_2, 1)$.

Finally, there is $\epsilon > 0$ such that $\epsilon < g < 1 - \epsilon$ on $[\delta_1, 1 - \delta_2]$. We can find n_3 such that $|\frac{g'(0)-1}{R(0)}R(x)x(1 - x)^{n_3}| < \epsilon$ on $[\delta_1, 1 - \delta_2]$. This will also hold for $n > n_3$, and so for $n > n_3$ we have that $0 < g_n < 1$ on $[\delta_1, 1 - \delta_2]$. Combining all these, we get that if $n > n_1, n_2, n_3$, then $0 < g_n < 1$ on $(0, 1)$, and we're done. \square

The previous two lemmas adjusted the behaviour of g at 0. We use the same symmetries we exploited in the last section to describe how to adjust g at 1.

Lemma 4.3. *Let $g \in \mathcal{P}$, and let R be an integer polynomial with $R(r) = 0$ for some $0 < r < 1$.*

There is $\hat{g} \in \mathcal{P}$ with $\hat{g}(0) = 0$, $\hat{g}'(0) = 1$, $\hat{g}(r) = g(r)$, $\hat{g}(1) = g(1)$, and $\hat{g}'(1) = g'(1)$, provided either $R(0) = \pm 1$, or $g(0) = 0$ and $R(0)|g'(0) - 1$.

There is $\hat{g} \in \mathcal{P}$ with $\hat{g}(1) = 1$, $\hat{g}'(1) = 1$, $\hat{g}(r) = g(r)$, $\hat{g}(0) = g(0)$, and $\hat{g}'(0) = g'(0)$, provided either $R(1) = \pm 1$, or $g(1) = 1$ and $R(1)|g'(1) - 1$.

Proof. The first statement is just a combination of the two previous lemmas. The second follows directly from applying the first statement to the partition polynomial $1 - g(1 - x)$ and the polynomial $R(1 - x)$ which has a root of $1 - r$. \square

Now we use the above lemma to give conditions under which we may replace g with an x -like or $(1 - x)$ -like partition polynomial.

Theorem 4.4. *Let $g \in \mathcal{P}$, and let R be an integer polynomial with $R(r) = 0$ for some $0 < r < 1$.*

There is an x -like partition polynomial \hat{g} with $\hat{g}(r) = g(r)$, provided the following two statements hold.

- (i) *Either we have $R(0) = \pm 1$ or we have $g(0) = 0$ and $R(0)|g'(0) - 1$.*
- (ii) *Either we have $R(1) = \pm 1$ or we have $g(1) = 1$ and $R(1)|g'(1) - 1$.*

There is a $(1 - x)$ -like partition polynomial \hat{g} with $\hat{g}(r) = g(r)$, provided the following two statements hold.

- (i) Either we have $R(0) = \pm 1$ or we have $g(0) = 1$ and $R(0)|g'(0) + 1$.
- (ii) Either we have $R(1) = \pm 1$ or we have $g(1) = 0$ and $R(1)|g'(1) + 1$.

Proof. The first statement is simply a combining of the two parts of the previous theorem. The second statement can be derived by applying the first statement to the partition polynomial $1 - g(x)$, noting that $g(x)$ is x -like if and only if $1 - g(x)$ is $(1 - x)$ -like. □

Of course we have written the above theorem in terms of the polynomials g and R , but they can also be applied to f and S which satisfy the same hypotheses. We now show the next implication of Theorem 2.11, that two implies three.

4.2. Proof.

Theorem 4.5. *Let r and s be algebraic numbers in $(0, 1)$, and let R and S be their irreducible polynomials. Further, suppose f and g are partition polynomials such that $r = f(s)$ and $s = g(r)$.*

Suppose also that if $R(0) \neq \pm 1$ and $g(0) = 0$, or if $R(1) \neq \pm 1$ and $g(1) = 1$, then

- (i) $R(0)|g'(0) - 1$,
- (ii) $R(1)|g'(1) - 1$,
- (iii) $S(0)|f'(0) - 1$,
- (iv) $S(1)|f'(1) - 1$.

Finally, suppose that if $R(0) \neq \pm 1$ and $g(0) = 1$, or if $R(1) \neq \pm 1$ and $g(1) = 0$, then

- (i) $R(0)|g'(0) + 1$,
- (ii) $R(1)|g'(1) + 1$,
- (iii) $S(0)|f'(0) + 1$,
- (iv) $S(1)|f'(1) + 1$.

Then there are partition polynomials \hat{f} and \hat{g} , either both x -like or both $(1 - x)$ -like, such that $r = \hat{f}(s)$ and $s = \hat{g}(r)$.

Proof. As mentioned before, since $S(g(r)) = 0$ we know $R|S \circ g$. We also have that $(f \circ g - id)(r) = 0$, which implies $R|f \circ g - id$. Similar arguments give two more statements:

$$R|S \circ g, \quad R|f \circ g - id, \quad S|R \circ f, \quad S|g \circ f - id.$$

We will repeatedly use these facts in what follows. We split into cases, first considering whether $R(0)$ or $R(1)$ is ± 1 , and then splitting into subcases, considering whether $g(0)$ is 0 or 1.

- (i) $R(0) = \pm 1, R(1) = \pm 1$: Using that $S|R \circ f$, and f is 0 or 1 valued at 0 and 1, we have that $S(0)|\pm 1$ and $S(1)|\pm 1$. So by Theorem 4.4, we may replace f and g by two x -like or two $(1 - x)$ -like partition polynomials. Note that in this case, we may choose whether we want to use x -like or $(1 - x)$ -like polynomials.
- (ii) $R(0) \neq \pm 1, R(1) = \pm 1$:
 - (a) $g(0) = 0$: We are in the case that $R(0) \neq \pm 1$ and $g(0) = 0$, so the first long hypothesis of the theorem applies. We therefore know that $R(0)|g'(0) - 1$, as well as that $g(0) = 0$, and that $R(1) = \pm 1$. By

Theorem 4.4, we know that we may also replace g with an x -like partition polynomial.

We know that $R|f \circ g - id$, so $R(0)|f(0)$. We cannot have $f(0) = 1$, and so it must be the case that $f(0) = 0$. We also claim that $S(1)|\pm 1$: In the case that $f(1) = 1$, this follows from $S(1)|R(f(1))$, while in the case that $f(1) = 0$ it follows from $S(1)|g(f(1)) - 1$. We have that $f(0) = 0$, $S(1) = \pm 1$, and that $S(0)|f'(0) - 1$, by the hypothesis of the theorem again. So we may replace f with an x -like partition polynomial as well.

- (b) $g(0) = 1$: In this case, we have $R(0) \neq \pm 1$, and $g(0) = 1$, so the second long hypothesis of the theorem applies, and we know $R(0)|g'(0) + 1$. We may therefore replace g with a $(1-x)$ -like partition polynomial. We know that $R|f \circ g - id$, so $R(0)|f(1) - 0$. We cannot have $f(1) = 1$, so it must be that $f(1) = 0$. We also claim that $S(0)|\pm 1$: This follows from $S(0)|R(f(0))$ if $f(0) = 1$, or it follows from $S(0)|g(f(0)) - 0$ if $f(0) = 0$. We have therefore that $f(1) = 0$, $S(0) = \pm 1$, and that $S(1)|f'(1) + 1$. So by Theorem 4.4, we may replace f with a $(1-x)$ -like partition polynomial as well.
- (iii) $R(0) = \pm 1$, $R(1) \neq \pm 1$: This case reduces to case (ii). Let $\bar{r} = 1 - r$, $\bar{R}(x) = R(1-x)$, $\bar{s} = s$, $\bar{S}(x) = S(x)$, $\bar{f}(x) = 1 - f(x)$, and $\bar{g}(x) = g(1-x)$. We have that $(\bar{r}, \bar{s}, \bar{R}, \bar{S}, \bar{f}, \bar{g})$ satisfy the hypotheses of the theorem if and only if (r, s, R, S, f, g) do, as mentioned in the previous section. Since $\bar{R}(0) \neq \pm 1$ and $\bar{R}(1) = \pm 1$, case two applies here. There are therefore partition polynomials \hat{f} and \hat{g} , either both x -like or both $(1-x)$ -like, such that $r = \hat{f}(s)$ and $s = \hat{g}(r)$. Then, we may take $\hat{f}(x) = 1 - \hat{f}(x)$, and $\hat{g}(x) = \hat{g}(1-x)$. (It is easy to verify that these will be either both $(1-x)$ -like or both x -like as well.)
- (iv) $R(0) \neq \pm 1$, $R(1) \neq \pm 1$:
- (a) $g(0) = 0$: Again, $R(0)|f(g(0)) - 0$ gives us that $f(0) = 0$. Further, we have that $R(1)|f(g(1)) - 1$. This will yield a contradiction unless $f(g(1)) = 1$, which can only happen if $g(1) = 1$ and $f(1) = 1$. We are in the case of the first long hypothesis of the theorem, so we have that $R(0)|g'(0) - 1$, and three similar statements. Using all of these, Theorem 4.4 lets us replace f and g with x -like partition polynomials.
- (b) $g(0) = 1$: As before, $R(0)|f(g(0)) - 0$ gives that $f(1) = 0$. Also, we have that $R(1)|f(g(1)) - 1$. It must be that $f(g(1)) = 1$, but this can only happen if $g(1) = 0$ and $f(0) = 1$. Also, we are in the case of the second long hypothesis, so we have $R(0)|g'(0) + 1$, as well as three more statements. Theorem 4.4 therefore lets us replace f and g with $(1-x)$ -like partition polynomials.

□

In the next section, we will see that x -like partition polynomials yield homeomorphisms which count 0's and 1's, while $(1-x)$ -like partition polynomials yield homeomorphisms which switch-count. We may like to do something similar here, and keep track of which conditions yield x -like partition polynomials and which yield $(1-x)$ -like partition polynomials. A formal statement is cumbersome, but an inspection of the proof shows: If the first half of the condition holds non-trivially

(the hypothesis and conclusions are both true), then we get x -like partition polynomials. If the second half holds non-trivially, we get $(1-x)$ -like partition polynomials. If both hold trivially, it must be the case that $R(0) = \pm 1$ and $R(1) = \pm 1$, and we may find either x -like or $(1-x)$ -like partition polynomials.

Furthermore, it turns out that it is impossible for both halves to hold non-trivially. For example, if the hypothesis of the first statement were true because $R(0) \neq \pm 1$ and $g(0) = 0$, then the hypothesis of the second could only hold by $R(1) \neq \pm 1$ and $g(1) = 0$. As we've argued before, $R(0)|f(g(0)) - 0$ implies $f(0) = 0$. But now $R(1)|f(g(1)) - 1$, yielding $R(1) = 1$, a contradiction.

5. THREE IMPLIES FOUR

In this section we prove the final non-trivial implication, using the x -like or $(1-x)$ -like partition polynomials to construct a homeomorphism sending μ_r to μ_s , which also either counts or switch-counts 0's or 1's.

5.1. Lemmas. First, we state a result which describes the extent to which we may approximate a continuous function on $[0, 1]$ by a polynomial with integer coefficients. Lorentz proved most of the following theorem in his book on Bernstein polynomials [9], but only stated that such polynomials are dense in $C[\delta, 1 - \delta]$.

Lemma 5.1. *Let f be a continuous function on $[0, 1]$. Given $\epsilon, \delta > 0$, there is a polynomial p with integer coefficients so that $|f(x) - p(x)| < \epsilon$ for $x \in [\delta, 1 - \delta]$, and $|f(x) - p(x)| < \frac{1}{2} + \epsilon$ for $x \in [0, \delta] \cup [1 - \delta, 1]$.*

Proof. It is well known that the Bernstein polynomials of a continuous function f , $B_n^f(x) = \sum_{i=0}^n f(\frac{i}{n}) \binom{n}{i} x^i (1-x)^{n-i}$, converge uniformly to f on $[0, 1]$. So for large n , we have $|f - B_n^f| < \epsilon/2$ on $[0, 1]$. Let $c_{i,n}$ be the nearest integer to $f(\frac{i}{n}) \binom{n}{i}$. Then $|B_n^f(x) - \sum_{i=0}^n c_{i,n} x^i (1-x)^{n-i}| \leq \sum_{i=0}^n \frac{1}{2} x^i (1-x)^{n-i} = \frac{1}{2} \frac{x^{n+1} - (1-x)^{n+1}}{2x-1}$. This function converges to zero uniformly on $[\delta, 1 - \delta]$ while staying less than $\frac{1}{2}$ on $[0, \delta] \cup [1 - \delta, 1]$. \square

We will actually need to use this lemma in a particular way. This will be clearer at the time if we state the following lemma now.

Lemma 5.2. *Suppose f and g are functions continuous on $[0, 1]$, except possibly for finitely many poles, and that at such poles of g , we have $g \rightarrow +\infty$, while at poles of f we have $f \rightarrow -\infty$. Further suppose that $f < g$ on their common domain, and that $g(1) - f(1) > 1$, and $g(0) - f(0) > 1$, if these values are defined. Then there is a polynomial Q with integer coefficients having $f < Q < g$ on $[0, 1]$.*

Proof. We may find a continuous function \hat{Q} on $[0, 1]$ with $f < \hat{Q} < g$ everywhere, and with $f + \frac{1}{2} < \hat{Q} < g - \frac{1}{2}$ on some neighborhoods of 0 and 1. We could, for example take \hat{Q} to be $\frac{f+g}{2}$ except near poles of f and g , where we use a continuous linear patch. Now an approximation of \hat{Q} by a polynomial with integer coefficients using the previous lemma with sufficiently small ϵ and δ will satisfy the desired requirements. \square

We now use this theorem to prove our main technical requirement, which we may view as an extension lemma. We are given "behaviors" (of p_1 and p_2) at 0, r , and 1, which sum to the corresponding "behaviors" of q at these points. We extend these behaviors to polynomials q_1 and q_2 which now sum to q everywhere.

Lemma 5.3. *If r is an algebraic number in $(0, 1)$, and if p_1, p_2 , and q are partition polynomials such that $p_1(r) + p_2(r) = q(r)$ and such that $\frac{p_1+p_2}{q}(x) \rightarrow 1$ as x goes to 0 and 1, then there are partition polynomials q_1 and q_2 such that $q_1 + q_2 = q$, such that $q_i(r) = p_i(r)$ for $i = 1, 2$, and such that $\frac{p_i}{q_i}(x) \rightarrow 1$ as x goes to 0 or 1, for $i = 1, 2$.*

Proof. Since the p_i 's are integer polynomials, there are unique integers $a_i, b_i > 0$ and $m_i, n_i \geq 0$ such that $p_i(x) = a_i x^{m_i} + O(x^{m_i+1})$ as $x \rightarrow 0$, and such that $p_i(x) = b_i(1-x)^{n_i} + O((1-x)^{n_i+1})$ as $x \rightarrow 1$, for $i = 1, 2$. Let $m = \min\{m_1, m_2\}$, $n = \min\{n_1, n_2\}$, $M = \max\{m_1, m_2\}$, and $N = \max\{n_1, n_2\}$. Then our assumption that $\frac{p_1+p_2}{q} \rightarrow 1$ as $x \rightarrow 0, 1$ gives us that $q(x) = p_1(x) + p_2(x) + O(x^{m+1})$ as $x \rightarrow 0$, and $q(x) = p_1(x) + p_2(x) + O((1-x)^{n+1})$ as $x \rightarrow 1$.

It is sufficient to find $q_1 \in \mathbb{Z}[x]$ such that:

- (i) $q_1(r) = p_1(r)$,
- (ii) $0 < q_1 < q$ on $(0, 1)$,
- (iii) $q_1(x) = p_1(x) + O(x^{m_1+1})$ as $x \rightarrow 0$, and $(q - q_1)(x) = p_2(x) + O(x^{m_2+1})$ as $x \rightarrow 0$,
- (iv) $q_1(x) = p_1(x) + O((1-x)^{n_1+1})$ as $x \rightarrow 1$, and $(q - q_1)(x) = p_2(x) + O((1-x)^{n_2+1})$ as $x \rightarrow 1$.

We know that $p_1(x) = (q - p_2)(x) + O(x^{m+1})$ as $x \rightarrow 0$, so one of the two statements of (iii) implies the other, depending on whether m_1 or m_2 is larger. Accordingly, let $e_L = p_1$ if $m_1 \geq m_2$, and let $e_L = q - p_2$ if $m_1 < m_2$. Then e_L is associated with the stronger of the two statements, and for (iii) to hold, it is sufficient that $q_1(x) = e_L(x) + O(x^{M+1})$ as $x \rightarrow 0$. Notice that e_L has exactly m_1 factors of x , the same number that p_1 has.

Similarly, we let $e_R = p_1$ if $n_1 \geq n_2$, and let $e_R = q - p_2$ if $n_1 < n_2$. Then for (iv) to hold, it is sufficient that $q_1(x) = e_R(x) + O((1-x)^{N+1})$ as $x \rightarrow 1$. Again, we may notice that e_R has exactly n_1 factors of $(1-x)$, the same as p_1 .

We now claim that $q - e_L > 0$ on $(0, \delta_1)$, and that $q - e_R > 0$ on $(1 - \delta_2, 1)$, for some $\delta_1, \delta_2 > 0$. These require the following cases:

- (i) If $m_1 < m_2$, then $q - e_L = p_2 \in \mathcal{P}$.
- (ii) If $m_1 \geq m_2$, then $(q - e_L)(x) = (q - p_1)(x) = p_2(x) + O(x^{m+1}) = a_2 x^{m_2} + O(x^{m_2+1})$ as $x \rightarrow 0$, and so $q - e_L$ is positive near 0.

The argument for $q - e_R$ near 1 is similar.

Next we claim that $e_L > 0$ on $(0, \delta'_1)$, and that $e_R > 0$ on $(1 - \delta'_2, 1)$, for some $\delta'_1, \delta'_2 > 0$. Again, there are two cases:

- (i) If $m_1 < m_2$, then $e_L(x) = (q - p_2)(x) = p_1(x) + O(x^{m+1}) = a_1 x^{m_1} + O(x^{m_1+1})$, which is positive near 0.
- (ii) If $m_1 \geq m_2$, then $e_L = p_1 \in \mathcal{P}$.

The argument for e_R near 1 is similar.

Let $\phi(x) = (1 - x^{M+1})^{N+1}$. Note that ϕ is a partition polynomial, that $\phi(x)$ has a root of multiplicity $N + 1$ at 1, while $1 - \phi(x)$ has a root of multiplicity $M + 1$ at 0. (The second statement can be seen by considering the first two terms of the binomial expansion of $\phi(x)$.) Let $R(x)$ be the irreducible polynomial of r , and consider choosing

$$q_1(x) = e_L(x)\phi(x) + e_R(x)(1 - \phi(x)) + Q(x)R(x)^2 x^{M+1}(1-x)^{N+1},$$

where Q is some polynomial with integer coefficients. We then have that

$$(q_1 - e_L)(x) = (e_R - e_L)(x)(1 - \phi(x)) + Q(x)R(x)^2x^{M+1}(1 - x)^{N+1} = O(x^{M+1})$$

as $x \rightarrow 0$, and also that

$$(q_1 - e_R)(x) = (e_L - e_R)(x)\phi(x) + Q(x)R(x)^2x^{M+1}(1 - x)^{N+1} = O((1 - x)^{N+1})$$

as $x \rightarrow 1$. This implies that the needed properties (iii) and (iv) hold. It is also easy to verify that $q_1(r) = p_1(r)$, using that $e_L(r) = e_R(r) = p_1(r)$. It only remains to verify that Q can be chosen so that q_1 is a partition polynomial and so that (ii) holds. Since q_1 has integer coefficients, we need only that $0 < q_1 < q$ on $(0, 1)$. This holds if and only if the following holds on $(0, 1)$:

$$\frac{-e_L(x)\phi(x) - e_R(x)(1 - \phi(x))}{R(x)^2x^{M+1}(1 - x)^{N+1}} < Q(x) < \frac{(q - e_L)(x)\phi(x) + (q - e_R)(x)(1 - \phi(x))}{R(x)^2x^{M+1}(1 - x)^{N+1}}.$$

We will now verify that the bounds above satisfy the hypotheses of Lemma 5.2, which will imply that such a polynomial $Q(x)$ with integer coefficients exists.

We are under the hypothesis that $p_1(r) + p_2(r) = q(r)$. This implies that $R|q - p_1 - p_2$, and therefore that $p_1(\bar{r}) + p_2(\bar{r}) = q(\bar{r})$ whenever \bar{r} is a root of R . If such a root is in $(0, 1)$, we will have that $0 < p_1(\bar{r}) < q(\bar{r})$. We will also have that $e_L(\bar{r}) = e_R(\bar{r}) = p_1(\bar{r})$. Thus, at a root \bar{r} of R in $(0, 1)$, the numerator of the left-hand side is $-p_1(\bar{r}) < 0$, and the denominator decreases to 0, while the right hand side has a numerator of $(q - p_1)(\bar{r}) > 0$ and the denominator decreases to 0. This gives that at any pole in $(0, 1)$ which arises as a root of R , the lower bound goes to $-\infty$ while the upper bound goes to $+\infty$, as required. Also it is clear that both bounds are continuous except at finitely many poles. The difference between the two has a numerator of $q(x)$, which is positive on $(0, 1)$. This will give that the upper bound is strictly greater than the lower bound on $(0, 1)$, as the denominators are always positive or 0. All that remains is to verify that the bounds have the correct behavior at 0 and 1. (Note that since R is irreducible, neither 0 nor 1 is a root of R .)

The lower bound can be expressed as

$$-\frac{e_L(x)\phi(x)}{R(x)^2x^{M+1}(1 - x)^{N+1}} - \frac{e_R(x)(1 - \phi(x))}{R(x)^2x^{M+1}(1 - x)^{N+1}}.$$

Recall that $1 - \phi(x)$ has a root of multiplicity $M + 1$ at 0, and so all the factors of x in the second term can be cancelled and the second term stays finite near 0. We have verified that e_L is positive near 0 on the right, and it is clear that ϕ , $R(x)^2$, and $x^{M+1}(1 - x)^{N+1}$ are positive near 0. So the first term is negative near 0. Also, when we defined e_L , we noticed that it had exactly m_1 factors of x . The denominator of the first term has $M + 1$ factors of x , a larger number, so the first term has a pole at 0. Since this term stays negative, it must go to $-\infty$ as $x \rightarrow 0^+$. The second term stayed finite near 0, and so the lower bound goes to $-\infty$ as $x \rightarrow 0^+$. A similar argument verifies that the lower bound goes to $-\infty$ as $x \rightarrow 1^-$, this time because the second term goes to $-\infty$ and the first term stays finite. This will ensure that the difference between the upper bound and lower bound is greater than 1 near 0^+ and 1^- , as long as the upper bound does not go to $-\infty$ near 0^+ or 1^- . We verify this now.

The upper bound can be expressed as

$$\frac{(q - e_L)(x)\phi(x)}{R(x)^2x^{M+1}(1-x)^{N+1}} + \frac{(q - e_R)(x)(1 - \phi(x))}{R(x)^2x^{M+1}(1-x)^{N+1}}.$$

We verified that $q - e_L$ is positive near zero on the right, and all other components of the first term are positive there also. The first term must stay positive as $x \rightarrow 0^+$, possibly going to $+\infty$. In the second term, we have seen that $1 - \phi(x)$ has $M + 1$ factors of x , so the second term stays bounded as $x \rightarrow 0^+$. So the sum of the two terms cannot go to $-\infty$, as neither term does. A similar argument applies as $x \rightarrow 1^-$, with the roles of the two terms reversed. \square

In the above lemma, we split a polynomial q into two pieces. A straightforward induction, which we omit, provides the following generalization: that we may split q into several pieces.

Lemma 5.4. *If r is an algebraic number in $(0, 1)$, and if p_1, \dots, p_k and q are partition polynomials such that $\sum_{i=1}^k p_i(r) = q(r)$ and such that $\frac{p_1 + \dots + p_k}{q}(x) \rightarrow 1$ as x goes to 0 or 1, then there are partition polynomials q_1, \dots, q_k such that $\sum_{i=1}^k q_i = q$, such that $q_i(r) = p_i(r)$ for $1 \leq i \leq k$, and such that $\frac{p_i}{q_i}(x) \rightarrow 1$ as x goes to 0 or 1, for $1 \leq i \leq k$.*

5.2. Counting 0's and 1's. Next, we examine the structure of the set of infinite words having exactly k 0's. Note that there is exactly one word with no 0's, namely $\bar{1}$. There are countably many words with exactly one 0, and the only limit point of this set is $\bar{1}$. Similarly, we have that the set of words with exactly k 0's is countably infinite if $k \geq 1$, and the limit points of this set are precisely the words with fewer than k 0's. On the other hand, the collection of all words with finitely many 0's is dense in \mathcal{C} .

If C is a non-empty clopen set in \mathcal{C} , density gives us that C must contain a word with finitely many 0's. Let k be the smallest number of 0's appearing in a word in C . Then C cannot contain infinitely many words with k 0's, as C would then contain a limit point of this set, which would have fewer than k 0's. Also, C contains a word with exactly k 0's, which is a limit point of the set of words with $k + 1$ 0's, and so C must contain infinitely many such points. Of course, similar statements hold when we count 1's, and we collect these statements:

Proposition 5.5. *Let C be a non-empty clopen set in \mathcal{C} . Then there are unique integers $a, b \geq 1, m, n \geq 0$ so that the following two statements hold: The number of words in C having exactly k 1's is 0 if $k < m$, is a if $k = m$, and is ∞ if $k > m$. The number of points in C having exactly k 0's is 0 if $k < n$, is b if $k = n$, and is ∞ if $k > n$.*

Next we observe that these characteristics of a clopen set C can be determined by examining the partition polynomial associated with C . Recall that any non-empty clopen set C can be written in the form $C = \bigcup_{i=0}^k [w_i]$, where the w_i 's are distinct words of the same length, N . It is clear that the smallest number, m , of 1's appearing in an element of C , is the smallest number of 1's appearing in one of the words w_i , and that the number, a , of such elements in C is the number of words w_i having that smallest number of 1's. The partition polynomial associated with C is $p(x) = \sum_{i=0}^k x^{a_i}(1-x)^{N-a_i}$, where a_i is the number of 1's in w_i . We have that there are exactly a terms which are $x^m(1-x)^{N-m}$, and all other terms

have a higher power of x . Since $x^m(1-x)^{N-m} = x^m + O(x^{m+1})$ as $x \rightarrow 0$, we can write $p(x) = ax^m + O(x^{m+1})$ as $x \rightarrow 0$. We may further note that any non-zero polynomial with integer coefficients has a unique $a \neq 0$ and $m \geq 0$ for which this equality holds, and so a and m can be determined uniquely by properties of p . Similar statements hold when we count 0's, and we collect these below:

Proposition 5.6. *Let C be a non-empty clopen set in \mathcal{C} , and let $p(x)$ be the partition polynomial associated with C . There are unique integers $a, b > 0$ and $m, n \geq 0$ such that C has exactly a words containing exactly m 1's, and C has exactly b words containing exactly n 0's. These are also the unique integers $a, b > 0$ and $m, n \geq 0$ such that $p(x) = ax^m + O(x^{m+1})$ as $x \rightarrow 0$, and such that $p(x) = b(1-x)^n + O((1-x)^{n+1})$ as $x \rightarrow 1$.*

5.3. Proof. We now prove the objective of the section. Note that we are actually stating something a little stronger: x -like partition polynomials yield homeomorphisms which count 0's and 1's, and $(1-x)$ -like partition polynomials yield homeomorphisms which switch-count.

Theorem 5.7. *Suppose r and s are numbers in $[0, 1]$, and f and g are partition polynomials such that $r = f(s)$ and $s = g(r)$. If f and g are x -like, then there is a homeomorphism h of \mathcal{C} which counts 0's and 1's such that $\mu_r = \mu_s \circ h$. If f and g are $(1-x)$ -like, then there is a homeomorphism h of \mathcal{C} which switch-counts 0's and 1's, such that $\mu_r = \mu_s \circ h$.*

Proof. First we note that it is sufficient to prove the first statement. If f and g are $(1-x)$ -like, then $\bar{f}(x) = 1 - f(x)$ and $\bar{g}(x) = g(1-x)$ are x -like, having $\bar{f}(s) = 1-r$, and $\bar{g}(1-r) = s$. If the first statement holds, there is a homeomorphism \bar{h} of \mathcal{C} which counts 0's and 1's, such that $\mu_{1-r} = \mu_s \circ \bar{h}$. If Φ again denotes the homeomorphism of \mathcal{C} which switches 0's and 1's, then we have $\mu_r = \mu_{1-r} \circ \Phi = \mu_s \circ \bar{h} \circ \Phi$, and so $h \circ \Phi$ is the desired homeomorphism. (It is easily verified to switch-count 0's and 1's.) So suppose f and g are x -like.

We construct partitions P_n and Q_n of \mathcal{C} into clopen sets for $n \geq 0$ and bijections $\pi_n : P_n \rightarrow Q_n$ satisfying the following properties:

- (i) P_{n+1} is a refinement of P_n and Q_{n+1} is a refinement of Q_n ,
- (ii) each member of P_{2n-1} and each member of Q_{2n} is a cylinder set of length at least n ,
- (iii) for any $C \in P_n$ we have $\mu_s(\pi_n(C)) = \mu_r(C)$,
- (iv) for any $C \in P_n$, and any $l \geq 0$, we have that the number of elements in C having exactly l 0's is the same as the number of elements in $\pi_n(C)$ having exactly l 0's,
- (v) for any $C \in P_n$, and any $l \geq 0$, we have that the number of elements in C having exactly l 1's is the same as the number of elements in $\pi_n(C)$ having exactly l 1's, and
- (vi) if $C \in P_{n+1}$ and $C \subseteq C' \in P_n$, then $\pi_{n+1}(C) \subseteq \pi_n(C')$.

Given the above sequence, define $h : \mathcal{C} \rightarrow \mathcal{C}$ by: for each $\alpha \in \mathcal{C}$, let C_n be the unique member of P_n containing α and let $f(\alpha)$ be the unique element of $\bigcap_n \pi_n(C_n)$. It is straightforward to verify that h is a well-defined homeomorphism of \mathcal{C} (defining f^{-1} by an analogous method from Q_n to P_n), and $h(C) = \pi_n(C)$ for all $C \in P_n$, so that $\mu_s(h(X)) = \mu_r(X)$ for $X \in \bigcup_n P_n$. Since every clopen set is a finite disjoint union of sets each in $\bigcup_n P_n$, h maps μ_r to μ_s . Finally, for any word w

in \mathcal{C} which contains exactly l 0's or 1's, w is the only such point in any sufficiently small neighborhood of w . Letting C_n again be the unique member of P_n containing w , we have that for sufficiently large n , C_n contains only one such point. This gives that $\pi_n(C_n)$ contains exactly one such point, and $\{h(w)\} = \bigcap_n \pi_n(C_n)$ must be this point. So h counts 0's and 1's.

We build P_n, Q_n , and π_n by a back-and-forth recursive construction. Let $P_0 = Q_0 = \{\mathcal{C}\}$ with $\pi_0(\mathcal{C}) = \mathcal{C}$. Given P_{2n}, Q_{2n}, π_{2n} , let P_{2n+1} be a refinement of P_{2n} into cylinder sets of length at least $n+1$. Fix $Y \in Q_{2n}$, a cylinder set, and let q be its associated partition polynomial. Also, let p be the partition polynomial associated with $\pi_{2n}^{-1}(Y)$. Now, $\pi_{2n}^{-1}(Y) \in P_{2n}$ is a union of cylinder sets $X_1, \dots, X_k \in P_{2n+1}$. Let the associated partition polynomial of X_i be p_i . We have therefore that

$$\sum_{i=1}^k (p_i \circ f)(s) = \sum_{i=1}^k p_i(r) = \sum_{i=1}^k \mu_r(X_i) = \mu_r(\pi_{2n}^{-1}(Y)) = \mu_s(Y) = q(s).$$

We also have that $\sum_{i=1}^k (p_i \circ f) = p \circ f$. Since f is x -like, we get that $p(f(x))/p(x)$ goes to 1 as x goes to 0, 1. (This statement is easy to verify, for example using L'Hôpital's rule and induction. Note that this is precisely where the fact that f is x -like is used.) Further, since p and q are the partition polynomials of $\pi_{2n}^{-1}(Y)$ and Y , respectively, and since these two sets have the same counting behavior, Proposition 5.6 gives us that $p(x)/q(x) \rightarrow 1$ as $x \rightarrow 0, 1$. Combining these gives us that $(\sum_{i=1}^k (p_i \circ f)(x))/q(x) \rightarrow 1$ as $x \rightarrow 0, 1$. We may therefore use Theorem 5.4 to find $q_1, \dots, q_k \in \mathcal{P}$ such that $\sum_{i=1}^k q_i = q$, such that $(p_i \circ f)(s) = q_i(s)$ for $1 \leq i \leq k$, and such that $\frac{p_i \circ f}{q_i}(x) \rightarrow 1$ as $x \rightarrow 0, 1$, for $1 \leq i \leq k$. Now by Theorem 2.7, there is a partition $\{Y_1, \dots, Y_k\}$ of Y into clopen sets whose associated partition polynomials are q_1, \dots, q_k , respectively.

Using $(p_i \circ f)(s) = q_i(s)$ gives us that $\mu_r(X_i) = \mu_s(Y_i)$. Knowing $\frac{p_i \circ f}{q_i}(x) \rightarrow 1$ as $x \rightarrow 0, 1$ and that f is x -like gives us that p_i and q_i have the same first order behavior at 0 and 1, which with Proposition 5.6 tells us that X_i and Y_i have the same number of words with exactly l 0's or 1's for all $l \geq 0$. We may therefore let $\pi_{2n+1}(X_i) = Y_i$, and let Q_{2n+1} include all these Y_i . Once this is done for all $Y \in Q_{2n}$, we will have the desired partition Q_{2n+1} and map π_{2n+1} .

We have finished refining the partition on the P side, and we must now refine the Q side. So let Q_{2n+2} be a refinement of Q_{2n+1} into cylinder sets of length $\geq n+1$, and apply the above procedure with r and s interchanged to get P_{2n+2} and π_{2n+2} (the map from Q_{2n+2} to P_{2n+2} will be π_{2n+2}^{-1}). This will complete the back-and-forth recursive step. □

6. FURTHER RESULTS AND EXAMPLES

6.1. Refinability. One consequence of Theorem 2.11 is that if r and s are binomially equivalent algebraic numbers, and if the irreducible polynomial R of r satisfies $R(0) = \pm 1$, and $R(1) = \pm 1$, then r and s are topologically equivalent. This gives a condition on R alone, which implies that every number binomially equivalent to r is topologically equivalent to r . This condition on r was shown in [18] by Dougherty, Mauldin and Yingst to be equivalent to a property of the measure μ_r , called refinability. (Versions of the results of this section and the following one appeared previously in that paper.) We discuss refinability now.

Definition 6.1. If μ is a measure on \mathcal{C} , we say that a clopen set C is *refinable* with respect to μ if whenever D_1, D_2, \dots, D_k are clopen sets in \mathcal{C} with $\sum_{i=1}^k \mu(D_i) = \mu(C)$, there is a partition $\{C_1, \dots, C_k\}$ of C into clopen sets, such that $\mu(C_i) = \mu(D_i)$ for $1 \leq i \leq k$. We say that the measure μ is refinable when every clopen set is refinable with respect to μ .

This definition is essentially what is required to replicate the proof of Theorem 5.7, and show that μ and ν are homeomorphic.

Theorem 6.2. *Let μ and ν be two refinable measures on \mathcal{C} with the same clopen values set. Then μ and ν are homeomorphic.*

Proof. As in the proof of Theorem 5.7, we construct partitions P_n and Q_n of \mathcal{C} into clopen sets for $n \geq 0$ and bijections $\pi_n : P_n \mapsto Q_n$ satisfying the following properties:

- (i) P_{n+1} is a refinement of P_n and Q_{n+1} is a refinement of Q_n ,
- (ii) each member of P_{2n+1} and each member of Q_{2n} is a cylinder set of length at least n ,
- (iii) for any $C \in P_n$ we have $\mu(\pi_n(C)) = \nu(C)$, and
- (iv) if $C \in P_{n+1}$ and $C \subseteq C' \in P_n$, then $\pi_{n+1}(C) \subseteq \pi_n(C')$.

As before, given the above sequence, we can construct a homeomorphism $h : \mathcal{C} \rightarrow \mathcal{C}$ with $\nu = \mu \circ h$ by: given $\alpha \in \mathcal{C}$, let C_n be the unique member of P_n with $\alpha \in P_n$, and let h map α to the unique element of $\bigcap_{n=0}^\infty \pi_n(C_n)$.

We build P_n, Q_n , and π_n by a back-and-forth recursive construction. Let $P_0 = Q_0 = \{\mathcal{C}\}$ with $\pi_0(\mathcal{C}) = \mathcal{C}$. Given P_{2n}, Q_{2n}, π_{2n} , let P_{2n+1} be a refinement of P_{2n} into cylinder sets of length $\geq n+1$. Fix $Y \in Q_{2n}$, a cylinder set. Now, $\pi_{2n}^{-1}(Y) \in P_{2n}$ is a union of cylinder sets $X_1, \dots, X_k \in P_{2n+1}$. Since μ and ν have the same clopen values set, for each X_i , there is some clopen Z_i with $\mu(Z_i) = \nu(X_i)$.

We have therefore that

$$\sum_{i=1}^k \mu(Z_i) = \sum_{i=1}^k \nu(X_i) = \nu(\pi_{2n}^{-1}(Y)) = \mu(Y).$$

Since Y is refinable with respect to μ , we have that there is a partition of Y , $\{Y_1, \dots, Y_k\}$ with $\mu(Y_i) = \mu(Z_i)$ for $1 \leq i \leq k$. We may let $\pi_{2n+1}(X_i) = Y_i$, and let Q_{2n+1} include all these Y_i . Once this is done for all $Y \in Q_{2n}$, we will have the desired partition Q_{2n+1} and map π_{2n+1} . We may apply a similar procedure to the Q side to complete the back-and-forth recursive step. □

We are interested in the case that $\mu = \mu_r$ is a Bernoulli trial measure. The following is a restatement of the definition of refinability in terms of partition polynomials. The proof is omitted and is trivial using the definition of associated partition polynomials and Theorem 2.7. Note that in the property below, we are requiring that a sum of values of functions be extendable to a sum of functions, similar to Lemma 5.3.

Proposition 6.3. *Let $0 \leq r \leq 1$. Then μ_r is refinable if and only if whenever q, p_1, \dots, p_k are partition polynomials with $q(r) = \sum_{i=0}^k p_i(r)$, there are partition polynomials q_1, \dots, q_k with $q = \sum_{i=0}^n q_i$, and with $q_i(r) = p_i(r)$ for $0 \leq i \leq k$.*

It's easy to note that μ_r is trivially refinable if r is transcendental, or if r is 0 or 1. (If r is transcendental, then $q(r) = \sum_{i=0}^k p_i(r)$ implies $q = \sum_{i=0}^k p_i$.) The following theorem from [18] characterizes the remaining cases.

Theorem 6.4. *Let r be an algebraic number in $(0, 1)$, and let R be its irreducible polynomial. Then μ_r is refinable if and only if $R(0) = \pm 1$ and $R(1) = \pm 1$.*

The proof is fairly complicated. Showing that refinability implies $R(0) = \pm 1$ and $R(1) = \pm 1$ is straightforward, but the other direction is messy. A large part depends on the following application of Theorem 5.2, which we state as a lemma.

Lemma 6.5. *Suppose $g \in \mathcal{P}$ with $g \neq 0$, f is a polynomial with real coefficients which is positive on $(0, 1)$, and R is a polynomial with integer coefficients with $|R(0)| = |R(1)| = 1$, such that $g < f$ at all roots of R in $(0, 1)$. Then there is a partition polynomial h such that $h(r) = g(r)$ for each root r of R in $(0, 1)$, and with $0 < h < f$ on $(0, 1)$.*

Proof. We first search for $\hat{g} \in \mathbb{Z}[x]$ with $\hat{g}(\bar{r}) = g(\bar{r})$ for every root \bar{r} of R in $(0, 1)$, and with $0 < \hat{g} < f$ on some intervals $(0, \delta) \cup (1 - \delta, 1)$. This property will be assured if \hat{g} has roots of 0 and 1 with higher multiplicity than those of f . Hence it suffices to show that g can be replaced by some $g^\# \in \mathbb{Z}[x]$ with its multiplicity at 0 and 1 each increased, but still retaining that $g > 0$ on $(0, \delta) \cup (1 - \delta, 1)$, and $g^\#(r) = g(r)$ for every root r of R in $(0, 1)$. For this, consider taking

$$g^\#(x) = g(x) [1 - R(x)^2 (1 - x(1 - x))^n].$$

The additional factor will clearly provide an additional root at 0 and 1, will not affect the value of g at roots of R , and is easily checked to be positive on $(0, \delta) \cup (1 - \delta, 1)$ for sufficiently large n . (Even though $a(x) = (1 - x(1 - x))^n$ and $b(x) = \frac{1}{R(x)^2}$ take the same value at 0 and 1, calculating the derivative of $a(x)$ at 0 and 1 verifies that $a < b$ on $(0, \delta) \cup (1 - \delta, 1)$ for large n .) Repeating this process sufficiently many times gives the desired \hat{g} .

We now search for a polynomial of the form $h(x) = \hat{g}(x) + x^N(1 - x)^N Q(x)R(x)^2$ where $Q \in \mathbb{Z}[x]$, and with $0 < h < f$. This is equivalent to solving

$$\frac{-\hat{g}(x)}{x^N(1 - x)^N R(x)^2} < Q(x) < \frac{f(x) - \hat{g}(x)}{x^N(1 - x)^N R(x)^2}.$$

If N is chosen sufficiently large so that the lower bound goes to $-\infty$ as $x \rightarrow 0^+$ or 1^- , and so that the upper bound goes to $+\infty$ as $x \rightarrow 0^+$ or 1^- , then the existence of such Q will be assured by Theorem 5.2. (That the bounds will behave this way for large N is assured since $0 < \hat{g} < f$ near 0^+ and 1^- .) It's easy to verify that h will have all the desired properties. \square

We now prove Theorem 6.4.

Proof. Let R be an irreducible polynomial with $|R(0)| = 1$, $|R(1)| = 1$, and let r be a root of R in $(0, 1)$. We will show that μ_r is refinable.

Suppose that f, g_1, g_2, \dots, g_k are partition polynomials with the property that $f(r) = \sum_{i=1}^k g_i(r)$. If some g_i 's are zero-valued anywhere in $(0, 1)$, then they are identically zero and we may take the corresponding h_i 's to be zero and still satisfy the requirements of refinability. Likewise, if there is only one g_i which is not zero, we can take $h_i = f$ and satisfy refinability. So assume $k > 1$, and each g_i is positive-valued at each root of R in $(0, 1)$. But $f - \sum g_i$ is an integer polynomial which is zero-valued at r , so is a polynomial multiple of R , and hence is zero-valued at all roots of R in $(0, 1)$. We may conclude that $0 < g_i < f$ at all roots of R in $(0, 1)$.

Choose positive numbers δ, ϵ so small that: for any root \bar{r} of R in $(0, 1)$ and any $x \in [\bar{r} - \delta, \bar{r} + \delta]$, we have $f(x) > (k-1)\epsilon + \sum_{i=2}^k g_i(\bar{r})$, and the distance between any two such roots is greater than 2δ . For each $i \geq 2$, we can find a polynomial p_i with real coefficients such that: for any root \bar{r} of R in $(0, 1)$, we have $p_i(\bar{r}) > g_i(\bar{r})$ but $0 < p_i(x) < g_i(\bar{r}) + \epsilon$ for all $x \in [\bar{r} - \delta, \bar{r} + \delta]$, and, for any $x \in (0, 1)$ not in any of the intervals $[\bar{r} - \delta, \bar{r} + \delta]$, we have $0 < p_i(x) < f(x)/(k-1)$. (Since the polynomials are dense in $C[0, 1]$, we may find a polynomial ϕ_i with $\phi_i(\bar{r}) > g_i(\bar{r})/f(\bar{r})$, $0 < \phi_i < (g_i(\bar{r}) + \epsilon)/f$ on each interval $[\bar{r} - \delta, \bar{r} + \delta]$, and $0 < \phi_i < 1/(k-1)$ off those intervals. Take $p_i = f\phi_i$.)

We have that $g_i < p_i$ at roots of R , and $p_i > 0$ on $(0, 1)$ for $i \geq 2$. So Lemma 6.5 applies, and we may find $h_i < p_i$, a partition polynomial which agrees with g_i at roots of R , for $i \geq 2$.

Let $h_1 = f - \sum_{i=2}^k h_i$. The properties in the preceding paragraphs ensure that $\sum_{i=2}^k p_i < f$ on $(0, 1)$, so $h_1 > 0$ on $(0, 1)$. The sum of the polynomials h_i is f , so each h_i lies below f and hence below 1. Therefore, each h_i is a partition polynomial. We have $h_i(r) = g_i(r)$ for $i \geq 2$, and $h_1(r) = f(r) - \sum_{i=2}^k h_i(r) = f(r) - \sum_{i=2}^k g_i(r) = g_1(r)$. This completes the proof that μ_r is refinable, by Proposition 6.3.

Now, suppose μ_r is refinable, and let R be the irreducible polynomial of r . Let $M = \sup_{x \in [0, 1]} R(x)^2$. Let k be such that $\left(\frac{1}{x(1-x)}\right)^k > M + 1$ on $[0, 1]$.

Next, let $j > k$ be sufficiently large that $(1-x)^{j-k} - x < R(x)^2$ on $(0, 1)$. (We know R is irreducible, so $R(0) \neq 0$. If $R(0)^2 = 1$, we'll have to find j sufficiently large that the derivative of the left hand side is less than that of the right at 0, so that the inequality holds on $(0, \delta)$ for some positive δ . For even larger j , the inequality will hold off of $(0, \delta)$, because the left hand side will be negative, and will still hold on $(0, \delta)$ because the left hand side decreases as j increases.)

So on $(0, 1)$ we have:

$$(1-x)^{j-k} - x < R(x)^2 < \frac{1}{x^k(1-x)^k} - 1 < \frac{1}{x^k(1-x)^k} - x.$$

Manipulating this gives

$$0 < x^{k+1}(1-x)^k - x^k(1-x)^j + x^k(1-x)^k R(x)^2 < 1 - x^k(1-x)^j.$$

Let $g(x)$ be the middle expression in the above inequality. By Theorem 2.6, $g(x)$ is a partition polynomial. We also have $r^{k+1}(1-r)^k = r^k(1-r)^j + g(r)$. By refinability, we have that there are partition polynomials h_1, h_2 , with $h_1(r) = r^k(1-r)^j$, $h_2(r) = g(r)$, and $h_1(x) + h_2(x) = x^{k+1}(1-x)^k$. In particular, we have $0 < h_1(x) < x^{k+1}(1-x)^k$ for x near 0 and 1. So h_1 must have a root of 0 with multiplicity at least $k+1$, and a root at 1 with multiplicity at least k . We can write $h_1(x) = x^{k+1}(1-x)^k p(x)$, for p a polynomial with integer coefficients.

Then we have $r^{k+1}(1-r)^k p(r) = r^k(1-r)^j$. So $rp(r) = (1-r)^{j-k}$. This implies that $xp(x)$ and $(1-x)^{j-k}$ are congruent modulo R , and we can write $xp(x) = (1-x)^{j-k} + Q(x)R(x)$ for some polynomial $Q \in \mathbb{Z}[x]$. Evaluating this at zero gives $0 = 1 + Q(0)R(0)$. Therefore $R(0) = \pm 1$.

One can argue that $R(1) = \pm 1$ by symmetry. If μ_r is refinable, then μ_{1-r} is as well, and the irreducible polynomial of $1-r$ is $R(1-x)$, and the above argument shows this polynomial satisfies $R(1-0) = \pm 1$. \square

As we have noted at the beginning of the section, if r and s are binomially equivalent, we only need that r has $R(0) = \pm 1$ and $R(1) = \pm 1$ to ensure that r and s are topologically equivalent. That is, we only need that μ_r be refinable. We observe now that Theorem 6.2 does apply in this case, and that μ_r and μ_s are actually both refinable.

Theorem 6.6. *If r and s are binomially equivalent numbers in $(0, 1)$, and if μ_r is refinable, then μ_r and μ_s are homeomorphic, and in particular, μ_s is refinable.*

Proof. If r is transcendental or is 0 or 1, then $s = r$ or $s = 1 - r$, and so μ_r and μ_s are trivially homeomorphic. If r is algebraic in $(0, 1)$, then by Theorem 6.4, we have $R(0) = \pm 1$, $R(1) = \pm 1$, and so Theorem 2.11 gives that μ_r and μ_s are homeomorphic. (For an alternative proof, we could use $S|R \circ f$ to find $S(0) = \pm 1$ and $S(1) = \pm 1$, showing that μ_s is refinable, and then Theorem 6.2 would give topological equivalence.) \square

6.2. Goodness. Following Akin [1], we refer to a probability measure μ on \mathcal{C} as *good* if given U and V clopen in \mathcal{C} such that $\mu(U) < \mu(V)$, there is $U' \subseteq V$, clopen with $\mu(U') = \mu(U)$. Good measures are significant for a variety of reasons given in [1], most notably because there is a uniquely ergodic minimal homeomorphism T on \mathcal{C} for which μ is the unique ergodic measure precisely when μ is good. (Glasner and Weiss showed in [4] that such measures are good, while Akin shows in [1] that good measures have this property.)

It is elementary to verify that all good measures on \mathcal{C} are refinable. From this it follows (using Theorem 6.2) that two good measures with the same clopen values set are topologically equivalent. The techniques of this paper give us a complete characterization of when the measure μ_r is good.

Theorem 6.7. *Let $r \in (0, 1)$ be algebraic. Then μ_r is good if and only if its irreducible polynomial R satisfies $R(0) = \pm 1$, $R(1) = \pm 1$, and R has exactly one root in $(0, 1)$.*

Proof. Suppose r satisfies the second property. Let C_1, C_2 be clopen sets in \mathcal{C} with $\mu_r(C_1) < \mu_r(C_2)$. Then their corresponding partition polynomials p_1, p_2 have the property that $p_1 < p_2$ at the only root of R in $(0, 1)$. Then Lemma 6.5 applies, and we may find \hat{p}_1 with integer coefficients such that $0 < \hat{p}_1 < p_2$ on $(0, 1)$, and $\hat{p}_1(r) = p_1(r)$. So $\hat{p}_1 \in \mathcal{P}$, and by Theorem 2.7 there is a corresponding clopen set $\hat{C}_1 \subseteq C_2$ such that $\mu_r(\hat{C}_1) = \mu_r(C_1)$. So μ_r is good and one direction is proven.

Now suppose μ_r is good. Then μ_r is refinable, and so by Theorem 6.4, $R(0) = \pm 1$ and $R(1) = \pm 1$. Now, if $\bar{r} \in (0, 1)$ is a root of the minimal polynomial of r , then any two clopen sets with the same μ_r measure will have the same $\mu_{\bar{r}}$ measure also. If U, V are clopen sets in \mathcal{C} with $\mu_r(U) < \mu_r(V)$, there is a clopen subset W of V with $\mu_r(W) = \mu_r(U)$. So $\mu_{\bar{r}}(U) = \mu_{\bar{r}}(W) < \mu_{\bar{r}}(V)$. That is, for U, V clopen sets, if $\mu_r(U) < \mu_r(V)$, then $\mu_{\bar{r}}(U) < \mu_{\bar{r}}(V)$. But if $\bar{r} \neq r$, we can clearly find two partition polynomials p_U, p_V with $p_U(r) < p_V(r)$ and $p_U(\bar{r}) > p_V(\bar{r})$, yielding a contradiction. \square

6.3. Examples. First we point out that there are large (finite) topological equivalence classes in $(0, 1)$. This example was earlier given in [18].

Theorem 6.8. *Given any $k \geq 0$ there are k distinct numbers in $(0, 1)$ which are topologically equivalent.*

Proof. Let n be a positive integer with at least k factors. Let r be the root of $x^n + x - 1$ in $(0, 1)$. If d is a factor of n , and $s = r^d$, we have $r = 1 - s^{n/d}$. These are partition polynomials, so r and s are binomially equivalent. The irreducible polynomial R of r is a factor of $x^n + x - 1$, and so has $R(0) \mid -1$ and $R(1) \mid 1$. So r and s are topologically equivalent, either by refinability or by the second part of Theorem 2.11. We have k such choices of s , and they are clearly distinct. \square

We have established implications between goodness, refinability, binomial equivalence, and topological equivalence. The following theorem collects some of these and asserts that these implications are sharp. The first part was established by Dougherty, Mauldin and Yingst in [18] and the third by Austin in [3].

Theorem 6.9. *Let $0 < r, s < 1$.*

- (i) *That μ_r is good is sufficient to assure that μ_r is refinable, but is not necessary, even among those r with a non-trivial \sim_{top} equivalence class.*
- (ii) *If r and s are binomially equivalent, then the refinability of μ_r is sufficient to assure that $r \sim_{top} s$, but is not necessary, even among non-trivially binomially equivalent r and s .*
- (iii) *The topological equivalence of r and s is sufficient to assure the binomial equivalence of r and s , but is not necessary.*

Proof. All three implications have been established previously, and we need only provide the counterexamples.

- (i) Let $R(x) = -14x^6 + 21x^4 - 8x^2 - x + 1$. It can be verified that R is irreducible, and R has three roots in $(0, 1)$. Let r be any one of these, and let $s = r^2$. Then $r = -14s^3 + 21s^2 - 8s + 1$. The polynomial $-14x^3 + 21x^2 - 8x + 1$ maps $(0, 1)$ into $(0, 1)$, and so is a partition polynomial, so we have that r and s are binomially equivalent. Also, $R(0) = 1$ and $R(1) = -1$, so r and s are topologically equivalent either by refinability or the second part of Theorem 2.11. It is also easy to verify that $r \neq s$ and $r \neq 1 - s$, so this equivalence is non-trivial.
- (ii) Let $f(x) = x + 5x^2(1 - x)^2$ and let $g(x) = x - 3x^2(1 - x)^2$. There is a unique root of $f \circ g - id$ in $(0, 1)$. Let r be this root, and let $s = g(r)$. We then have that $r = f(s)$. Both f and g map $(0, 1)$ into $(0, 1)$, so are partition polynomials, and both are x -like. Therefore by Theorem 2.11, r and s are topologically equivalent, and it's easy to see they are not trivially so. Using Maple, we can verify that $R(x) = \frac{f(g(x)) - x}{x^2(1-x)^2}$ is irreducible, and so is the irreducible polynomial of r . This polynomial has $R(0) = 2$, so r is not refinable, and by Theorem 6.6, s isn't refinable either.
- (iii) Let $f(x) = 3x(1 - x)$ and let $g(x) = 2x(1 - x)$. Let r and s be the unique solution of $r = f(s)$ and $s = g(r)$ in $(0, 1)$. Then f and g are partition polynomials, so $r \sim_{bin} s$. The irreducible polynomial of r can be verified to be $R(x) = \frac{f \circ g(x) - x}{x} = -12x^3 + 24x^2 - 18x + 5$. Now $R(0) \neq \pm 1$ and $g(0) = 0$, but $R(0) = 5$ does not divide $g'(0) - 1 = 1$. So by the second part of Theorem 2.11, r and s are not topologically equivalent. \square

6.4. Further results. One of the problems which has remained open in the area is whether a \sim_{top} equivalence class, or a \sim_{bin} equivalence class can be infinite. The following is a combination of known results pointed out by Joe Buhler, which shows that equivalence classes are finite for algebraic integers.

Theorem 6.10. *Let $0 < r < 1$ be an algebraic integer. There are only finitely many values in $(0, 1)$ which are binomially equivalent to r .*

Proof. If $r \sim_{bin} s$, then $r \in \mathcal{P}(s)$ and $s \in \mathcal{P}(r)$. So $r \in \mathbb{Z}[s]$ and $s \in \mathbb{Z}[r]$. From this it follows that $\mathbb{Z}[r] = \mathbb{Z}[s]$. For algebraic integers it is known that this implies that r and s have the same discriminant. We briefly argue this now.

Let n be the degree of r . This must be the degree of s also. Let $r = r_1, r_2, \dots, r_n$ be the algebraic conjugates of r . Each of $1, s, \dots, s^{n-1}$ is in $\mathbb{Z}[r]$ and so is an integer linear combination of powers of r . Since r is an algebraic integer, we may express them as an integer combination of $1, r, \dots, r^{n-1}$. The rational vector space $\mathbb{Q}(r) = \mathbb{Q}(s)$ has as bases both $\mathcal{B}_1 = \{1, r, \dots, r^{n-1}\}$ and $\mathcal{B}_2 = \{1, s, \dots, s^{n-1}\}$. The expressions described above give us that the change of basis matrix M , from \mathcal{B}_2 to \mathcal{B}_1 , has integer entries. By symmetry of argument, the inverse of this matrix also has integer entries, and so $\det M = \pm 1$. We have M^T maps the vector $(1, r, \dots, r^{n-1})$ to $(1, s, \dots, s^{n-1})$, and so maps $(1, r_i, \dots, r_i^{n-1})$ to $(1, s_i, \dots, s_i^{n-1})$, where $\{s_i\}_{i=1}^n$ are the algebraic conjugates of s . If $A = [a_{i,j}]$ and $B = [b_{i,j}]$ are given by $a_{i,j} = r_j^{i-1}$ and $b_{i,j} = s_j^{i-1}$, then $M^T A = B$ and

$$\text{disc } s = (\det B)^2 = (\det M^T)^2 (\det A)^2 = (\det A)^2 = \text{disc } r.$$

A result of Kálmán Györy, first proved in [5] and [6], is that if we regard two polynomials as equivalent when they differ by translation by an integer, then there are only finitely many monic polynomials of any given degree and discriminant. If r and s are binomially equivalent numbers in $(0, 1)$, and r is an algebraic integer of degree n and discriminant D , then s is an algebraic integer which is the root of some monic polynomial of discriminant D and degree n . There are only finitely many choices of such a polynomial up to translation by an integer, and only finitely many translates of such a polynomial will have a root in $(0, 1)$. □

It appears that this argument cannot be extended to non-integers. Versions of Györy’s theorem exist for non-integers with a more sophisticated notion of equivalent polynomials, but it doesn’t appear useful in this case, as binomially equivalent non-integers do not necessarily have the same discriminant. For instance, the example in the second part of the proof of Theorem 6.9 can be computed by Maple to have different (very large) discriminants.

Next, we present a theorem which we haven’t used in this paper, but may be a useful tool when searching for examples. The statement that s is binomially reducible to r is stronger than the statement that $s \in \mathbb{Z}[r]$. This result describes exactly how much stronger.

Theorem 6.11. *Let $0 < r, s < 1$ be algebraic, and let R be the irreducible polynomial of r . Suppose g is some polynomial with integer coefficients with $g(r) = s$. Then there is a partition polynomial \hat{g} with $\hat{g}(r) = s$ if and only if the following statements hold:*

- (i) *either $R(0) \mid g(0)$ or $R(0) \mid g(0) - 1$,*
- (ii) *either $R(1) \mid g(1)$ or $R(1) \mid g(1) - 1$,*
- (iii) *and $0 < g(\bar{r}) < 1$ for every root \bar{r} of R in $(0, 1)$.*

Proof. If such \hat{g} exists, it satisfies $\hat{g}(r) = g(r)$, and so g and \hat{g} are congruent modulo R in $\mathbb{Z}[x]$. So \hat{g} must be of the form $\hat{g} = g + QR$ for some $Q \in \mathbb{Z}[x]$. The

three statements now follow from the fact that $\hat{g}(0), \hat{g}(1)$ are each 0 or 1, and that $0 < \hat{g}(\bar{r}) < 1$ for any root \bar{r} of R in $(0, 1)$.

Now suppose g has the required properties. Then for some integers m and n , we have $g(0) + mR(0)$ and $g(1) + nR(1)$ are each 0 or 1. So, replacing $g(x)$ with $g(x) + nxR(x) + m(1 - x)R(x)$ lets us assume that $g(0)$ and $g(1)$ are each 0 or 1.

We search for a partition polynomial of the form $\hat{g}(x) = g(x) + x(1 - x)R(x)^2Q(x)$. This polynomial will have $\hat{g}(r) = g(r) = s$, and so we need only show that it can be chosen to be a partition polynomial. It has integer coefficients, so we need only verify that $0 < \hat{g} < 1$ on $(0, 1)$. This holds if and only if the following inequality holds on $(0, 1)$:

$$\frac{-g(x)}{x(1 - x)R(x)^2} < Q(x) < \frac{1 - g(x)}{x(1 - x)R(x)^2}.$$

We verify that the bounds for Q satisfy the hypotheses of Lemma 5.2, and so such a Q with integer coefficients exists. Both sides are clearly continuous with only finitely many poles in $(0, 1)$, and the difference is clearly positive so that the right-hand side is strictly greater than the left on $(0, 1)$. At any pole which is a root \bar{r} of R , we have that $0 < g(\bar{r}) < 1$, so that the numerator of the left-hand side is negative, and the numerator of the right-hand side is positive, which ensures that the lower bound goes to $-\infty$ and the upper bound goes to $+\infty$. At 0, we have either that $-g(0) = 0$ and $1 - g(0) = 1$, in which case the left hand side stays finite and the right-hand side goes to $+\infty$, or we have that $-g(0) = -1$ and $1 - g(0) = 0$, in which case the left hand side goes to $-\infty$ and the right hand side stays finite. In either case, the hypotheses are satisfied, and similar reasoning applies at 1. \square

This theorem directly gives the following corollary.

Corollary 6.12. *If r is an algebraic number in $(0, 1)$, and R is its irreducible polynomial, then the clopen values set of the measure μ_r is the set of all $g(r)$ where g is some integer polynomial satisfying $g(0) \equiv 0$ or 1 modulo $R(0)$, $g(1) \equiv 0$ or 1 modulo $R(1)$, and $0 < g(\bar{r}) < 1$ for each root \bar{r} of R in $(0, 1)$.*

We now use this result to characterize another property defined by Akin in [1]. A measure μ on \mathcal{C} is said to have a *grouplike clopen values set* if given any two clopen sets C and D in \mathcal{C} with $\mu(C) + \mu(D) < 1$, there is a clopen set E with $\mu(C) + \mu(D) = \mu(E)$. This occurs exactly when the clopen values set of the measure μ is of the form $G \cap [0, 1]$, where G is a subgroup of \mathbb{R} , or equivalently, when the clopen values set S of μ has the property that $S + \mathbb{Z}$ is a subgroup of \mathbb{R} . The preceding lemma makes it fairly simple to characterize the Bernoulli trial measures with grouplike clopen values set.

Corollary 6.13. *Let $0 < r < 1$. The measure μ_r has a grouplike clopen values set if and only if r is algebraic and its irreducible polynomial R satisfies $R(0) = \pm 1$ or ± 2 , $R(1) = \pm 1$ or ± 2 , and R has exactly one root in $(0, 1)$.*

Proof. Suppose that μ_r has a grouplike clopen values set. For some n , we have $r^n < \frac{1}{2}$. So $2r^n$ is a clopen value for the measure μ_r . There is some partition polynomial p with $p(r) = 2r^n$. Since $2x^n$ is not a partition polynomial, this is a non-trivial polynomial equation solved by r , so r is algebraic. Further, $2x^n - p(x)$ is a multiple of $R(x)$, so $R(1)$ divides $2 - p(1) = 2$ or 1 , so $R(1) = \pm 1$ or ± 2 . A similar argument using $2(1 - x)^n$ shows that $R(0) = \pm 1$ or ± 2 .

Now suppose that $R(x)$ has a root \bar{r} in $(0, 1)$ other than r . Further suppose $r < \bar{r}$. Then for some large n , we will have $2r^n < \bar{r}^n < \frac{1}{2}$. Let m be the largest integer such that $mr^n \leq 1$. If μ_r has a grouplike clopen values set, then using this property $m - 1$ times shows that mr^n is a clopen value for μ_r . There must be a partition polynomial p with $p(r) = mr^n$. This polynomial must also have $p(\bar{r}) = m\bar{r}^n > 2mr^n > (m + 1)r^n > 1$, a contradiction. Considering multiples of $(1 - r)^n$ handles the case when $\bar{r} < r$.

Now suppose r has the properties described. If C and D are clopen sets with $\mu_r(C) + \mu_r(D) < 1$, let p_C and p_D be their partition polynomials. We have that $0 < p_C + p_D < 1$ at the only root of R in $(0, 1)$, and we must have that $(p_C + p_D)(0) \equiv 0$ or 1 modulo $R(0)$, and $(p_C + p_D)(1) \equiv 0$ or 1 modulo $R(1)$, since every integer has these properties. By the above theorem, $p_C(r) + p_D(r)$ is a clopen value for the measure μ_r , and μ_r is good. \square

6.5. Related problems. We conclude by presenting a few directions in which research in this problem can be continued.

Problem. Is there an infinite \sim_{top} equivalence class? Is there an infinite \sim_{bin} equivalence class? We may weaken the question even further by saying r and s are *algebraically equivalent* when $\mathbb{Z}[r] = \mathbb{Z}[s]$, and asking if there is an infinite algebraic equivalence class in $(0, 1)$.

Problem. When are two Haar measures on \mathcal{C} homeomorphic? That is, given two topological groups whose topology is homeomorphic to \mathcal{C} , when are the associated Haar measures homeomorphic?

A partial answer is briefly described as follows: It is known that such a topological group must have a decreasing sequence, $\{C_n\}_{n=1}^\infty$, of clopen subgroups whose intersection is $\{e\}$. (Balls about the origin with respect to a translation invariant ultrametric will work.) Compactness gives that the space is a finite union of translates of C_n , so $\mu(C_n) = \frac{1}{a_n}$ for some integer a_n . The same argument applied to C_{n-1} gives us that $a_{n-1} | a_n$. We find by a simple homeomorphism that μ is homeomorphic to the product measure on $\prod_{n=1}^\infty F_n$, where each F_n is a finite set with $\frac{a_{n+1}}{a_n}$ elements, endowed with the uniform measure. By further factoring each of these F_n 's, we are able to express this measure as a product measure on $\prod_{n=1}^\infty P_n$ where each P_n is finite with prime size and uniform measure. We observe that two Haar measures are homeomorphic if and only if they yield the same “prime factorization,” meaning that every prime occurs in the resulting sequence the same (possibly infinite) number of times. This answer seems unsatisfactory however, and some deeper algebraic description might be desirable.

Problem. If (r_1, \dots, r_n) is a probability vector, let $\beta(r_1, \dots, r_n)$ be the corresponding product measure on $\{1, \dots, n\}^\mathbb{N}$. When are two of these measures homeomorphic?

Instead of increasing the size of the factors, we may be interested in increasing the number of factors. It turns out that this does not significantly complicate the issue: Let I be any infinite index set, possibly of very large cardinality, and ν_r denote the Bernoulli trial measure on the set $\{0, 1\}^I$. Then ν_r and ν_s are homeomorphic precisely when μ_r and μ_s on $\{0, 1\}^\mathbb{N}$ are. This is because clopen sets in $\{0, 1\}^I$ can only depend on finitely many indices, and so they correspond with partition polynomials in the same way, and all the same arguments apply, giving us that if

$\nu_r \approx \nu_s$, then r and s can be written as x -like or $(1-x)$ -like partition polynomials in each other. On the other hand, if $\mu_r \approx \mu_s$, then ν_r and ν_s are homeomorphic since they are expressible as products of copies of μ_r and μ_s , respectively.

ACKNOWLEDGEMENTS

I would like to thank the following people for their suggestions, contributions and support: Ethan Akin, Randy Dougherty, Kálmán Györy, Joe Buhler, Mik Laczkovich and Shems Alhaddad. This paper is based on my thesis at the University of North Texas: Special thanks go to my advisor, Dan Mauldin, for his encouragement and support.

REFERENCES

1. E. Akin, *Good measures on Cantor space*, Trans. Amer. Math. Soc. **357** (2005), 2681–2722. MR2139523 (2006e:37003)
2. S. Alpern and V. S. Prasad, *Typical dynamics of volume preserving homeomorphisms*, Cambridge Tracts in Mathematics **139** (2000). MR1826331 (2002i:37006)
3. T. D. Austin, *A pair of non-homeomorphic measures on the Cantor set*, Math. Proc. Camb. Phil. Soc. **142** (2007), 103–110. MR2296394
4. E. Glasner and B. Weiss, *Weak orbit equivalence of minimal Cantor systems*, Internat. J. Math. **6** (1995), 559–579. MR1339645 (96g:46054)
5. K. Györy, *Sur les polynômes à coefficients entiers et de discriminant donné*, Acta Arith. **23** (1973), 419–426. MR0437489 (55:10419a)
6. ———, *Sur les polynômes à coefficients entiers et de discriminant donné. II*, Publ. Math. Debrecen **21** (1974), 125–144. MR0437490 (55:10419b)
7. F. Hausdorff, *Summationsmethoden und Momentfolgen I*, Math. Z. **9** (1921), 74–109. MR1544453
8. K. J. Huang, *Algebraic numbers and topologically equivalent measures in the Cantor set*, Proc. Amer. Math. Soc. **96** (1986), 560–562. MR826481 (87b:11100)
9. G. G. Lorentz, *Bernstein Polynomials*, University of Toronto Press, Toronto, 1953. MR0057370 (15:217a)
10. R. D. Mauldin, *Problems in topology arising from analysis*, (1990), 617–629. MR1078668
11. F. J. Navarro-Bermudez, *Topologically equivalent measures in the Cantor space*, Proc. Amer. Math. Soc. **77** (1979), 229–236. MR542090 (80k:28017)
12. F. J. Navarro-Bermudez and J. C. Oxtoby, *Four topologically equivalent measures in the Cantor space*, Proc. Amer. Math. Soc. **104** (1988), 859–860. MR939966 (90c:28020)
13. J. C. Oxtoby, *Homeomorphic measures in metric spaces*, Proc. Amer. Math. Soc. **24** (1970), 419–423. MR0260961 (41:5581)
14. J. C. Oxtoby and V. S. Prasad, *Homeomorphic measures in the Hilbert cube*, Pac. J. Math. **77** (1978), 483–497. MR510936 (80h:28006)
15. J. C. Oxtoby and S. M. Ulam, *Measure preserving homeomorphisms and metrical transitivity*, Ann. Math. **42** (1941), 874–920. MR0005803 (3:211b)
16. R. G. E. Pinch, *Binomial equivalence of algebraic numbers*, J. Indian Math. Soc. (N.S.) **58** (1992), 33–37. MR1207024 (94a:11160)
17. G. Pólya and G. Szegő, *Problems and Theorems in Analysis II*, Springer, 1972.
18. R. D. Mauldin, R. Dougherty and A. Yingst, *On homeomorphic Bernoulli measures on the Cantor space*, to appear in Trans. Amer. Math. Soc., 16 pages.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTH CAROLINA, COLUMBIA, SOUTH CAROLINA 29208

E-mail address: andy.yingst@gmail.com

Current address: Department of Mathematics, University of South Carolina, P.O. Box 889, Lancaster, South Carolina 29721