# Arithmetic of infinite Dedekind-finite sets

Jing-Yi Liu
Mentor: Andreas Blass

24 June 2022

## Contents

**1 Introduction** **1**

**2 Infinite Dedekind-finite sets are transcendental** **3**

**3 Polynomials in more than one variable** **4**

**4 Possible extensions** **6**

**5 References** **7**

## 1 Introduction

We say a set is "Dedekind-finite" if there is no bijection between it and a proper subset. A set is "Dedekind-infinite" if it is not Dedekind-finite. If we assume the Axiom of Choice, being Dedekind-finite is equivalent to being in 1-1 correspondence with a natural number. However, without the Axiom of Choice, there may exist infinite Dedekind-finite sets; Dedekind-finite sets that contain more than $n$ elements for all $n \in \mathbb{N}$.

These infinite Dedekind-finite sets behave much like very large finite sets when it comes to polynomials. In this paper, assume polynomials have finitely many terms and natural number coefficients and exponents unless otherwise specified. Addition in this context means taking the disjoint union and multiplication means taking the Cartesian product. Coefficients are repeated addition and exponents are repeated multiplication.

First, the following lemma allows us to use another useful definition of Dedekind-finite:

**Lemma 1.1.** Let $X$ be a set. The following are equivalent definitions for "$X$ is Dedekind-finite":

1. There is no 1-1 correspondence between $X$ and a proper subset of $X$.
2. $X$ has no countably infinite subset.

**Proof:** We proceed by proof by contrapositive.

**(1) $\implies$ (2):** Suppose there exists a countably infinite subset $S$ of $X$. Since $S$ is countable, there exists a bijection $g : S \to \mathbb{N}$. Let $f : X \to X$ where $f(x) = \begin{cases} x & x \notin S \\ g^{-1}(2g(x)) & x \in S \end{cases}$. It suffices to show that $f$ is injective but not surjective because then it is a bijection between $X$ and its image, which is a proper subset of $X$.

Suppose $f(x) = f(y)$. If $x, y \notin S$, then we have $x = y$. If $x, y \in S$, then $g^{-1}(2g(x)) = g^{-1}(2g(y))$, so we can apply $g$ to both sides to get $2g(x) = 2g(y)$. Since $g$ and multiplication by 2 are injective, so is $2g$, so $x = y$. If $x \in S, y \notin S$, then $f(x)$ is in the image of $g^{-1}$, which is $S$, and $f(y) = y \notin S$, which contradicts $f(x) = f(y)$. The same goes if $x \notin S, y \in S$. Thus $f(x) = f(y) \implies x = y$, so $f$ is injective.

Consider $g^{-1}(1) \in S$. For all $x \notin S$, $f(x) = x \notin S$, so $f(x) \neq g^{-1}(1)$. For all $x \in S$, there exists some $n \in \mathbb{N}$ such that $g^{-1}(n) = x$ because $g$ is bijective. Then,

$$f(x) = f(g^{-1}(n)) = g^{-1}(2g(g^{-1}(n)))$$

since $g, g^{-1}$ are inverses,

$$= g^{-1}(2n)$$

Since $2n \neq 1$ for all $n \in \mathbb{N}$ and $g^{-1}$ is bijective, $g^{-1}(2n) \neq g^{-1}(1)$ for all $n \in \mathbb{N}$. Thus $f(x) \neq g^{-1}(1)$. Then $g^{-1}(1)$ is never in the image of $f$, so $f$ is not surjective.

**(2) $\implies$ (1):** Suppose there exists a bijection $f : X \to S$ where $S \subset X$. Let $x_0 \in X \backslash S$, which is possible because $S$ is a proper subset. I claim that $g : \mathbb{N} \to S$ where $g(n) = f^n(x_0)$ (i.e. applying $f$ to $x_0$, $n$ times) is injective. Then $g[\mathbb{N}]$ is a countably infinite subset of $S$ (and therefore of $X$).

Suppose for the sake of induction that $g(1), \cdots, g(n-1)$ are all pairwise distinct. Then $g(n) = f(g(n-1))$, and $g(1) = f(x_0)$. Since the image of $g$ is contained in $S$ and $x_0 \notin S$, $g(n-1) \neq x_0$, and since $f$ is bijective, $g(n) \neq g(1)$. Note that $g(k) = f(g(k-1))$ for all $k = 2, \cdots, n-1$. By the inductive hypothesis, $g(n-1) \neq g(k-1)$ for all $k = 2, \cdots, n-1$, so since $f$ is bijective, $g(n) \neq g(k)$ for all $k = 2 \cdots, n-1$. Thus $g(1), \cdots, g(n)$ are all pairwise distinct. Then by induction on $n$, $g$ is injective. □

If we assume the Axiom of Choice, infinite cardinal polynomials are very simple: if at least one of $\kappa, \lambda$ is infinite, then $\kappa + \lambda = \max(\kappa, \lambda)$. If at least one of $\kappa, \lambda$ is infinite and neither is 0, then $\kappa \cdot \lambda = \max(\kappa, \lambda)$. Then any polynomial that has an infinite term simplifies down to the largest infinite cardinal that is the value of one of the variables.

However, we can show that unlike Dedekind-infinite sets, infinite Dedekind-finite sets behave like sufficiently large finite sets when it comes to polynomials. In particular, if some polynomial is larger than another for sufficiently large finite inputs, that inequality will also hold for infinite Dedekind-finite sets. The following theorems formalize that intuition.

## 2 Infinite Dedekind-finite sets are transcendental

**Lemma 2.1.** Let $p, q$ be distinct finite polynomials in one variable with natural number coefficients and exponents. Then without loss of generality, there exists some $N \in \mathbb{N}$ such that for all $n \geqslant N$, $p(n) > q(n)$. If $p(X) \leqslant q(X)$ for some infinite $X$, then $X$ is Dedekind-infinite. In other words, $p(x) > q(x)$ for all sufficiently large Dedekind-finite sets $x$.

**Proof:** Suppose $p, q$ are distinct polynomials in one variable and for all $n \geqslant N$, $p(n) > q(n)$. Let $X$ be an infinite set such that $p(X) \leqslant q(X)$. Since $X$ is infinite, choose $N$ elements from $X$ and order them into a list of length $N$: $x_1, \cdots, x_N$. Since $p(X) \leqslant q(X)$, let $f : p(X) \to q(X)$ be an injection.

With $N$ elements from $X$, we can generate $p(N)$ points in $p(X)$; for example, if the coefficient on the $X^2$ term in $p(X)$ is 2 and $N = 2$, then $(0, x_1, x_2)$ and $(1, x_2, x_1)$ are points in $p(X)$. We order these points from lowest degree term to highest, then by coefficient, then lexicographically in $X^j$ for each $X^j$ term in $p(X)$. Then we have an ordered list of $p(N)$ points in $p(X)$ using only combinations of $x_1, \cdots, x_N$.

Using $f$, map these $p(N)$ points to an ordered list of $p(N)$ points in $q(X)$, where the ordering comes from $f$. Since $p(N) > q(N)$, these $p(N)$ points must contain points that are not just combinations of $x_1, \cdots, x_N$ in $q(X)$ because there are only $q(N)$ such points. Then this ordered list of $p(N)$ points in $q(X)$ must include an element of $X$ that is not among $x_1, \cdots, x_N$. Pick the first new element of $X$ that shows up in the list and append it to the ordered list of $N$ elements from $x$ to get a list of length $N + 1$.

Again make an ordered list of $p(N + 1)$ points in $p(X)$, and use $f$ to get an ordered list of $p(N + 1)$ elements of $q(X)$. Then take the first new point in $X$ and extend the ordered list of $N + 1$ points in $X$ by that one element. Since

$p(n) > q(n)$ for all $n \geqslant N$, we can repeat inductively to get a countably infinite sequence of elements in $X$. Then, $X$ is Dedekind-infinite. □

**Theorem 2.1.** Suppose $X$ is an infinite Dedekind-finite set. Then for any finite polynomial $p$ with integer coefficients and natural number exponents, $p(X) \neq 0$. In other words, $X$ is transcendental.

**Proof:** Suppose for the sake of contradiction that $p(X) = 0$. We can add the negative terms to both sides of the equation so we have $q(X) = r(X)$ where $q, r$ are finite polynomials with natural number coefficients and natural number exponents. In particular, $q$ is the polynomial made of the terms of $p$ with positive coefficients and $r$ is the polynomial made of the terms of $p$ with negative coefficients.

Since each (nonzero) term of $p$ cannot have both positive and negative coefficient, $q, r$ do not share any terms of the same power. Then, $q, r$ are distinct finite polynomials in one variable with natural number coefficients and exponents. Since $q(X) = r(X)$ and $X$ is infinite, by lemma 2.1 $X$ is Dedekind-infinite, which contradicts $X$ being Dedekind-finite. □

# 3 Polynomials in more than one variable

In this paper, an equation has an "integer solution" if there is a solution where all the variables are integers. Likewise a "Dedekind-finite solution" is where all the variables are Dedekind-finite.

**Theorem 3.1.** Let $p, q$ be distinct finite polynomials in (up to) $m$ variables, $x_1, \cdots, x_m$ each. Suppose there are no integer solutions to $p(x_1, \cdots, x_m) = q(x_1, \cdots, x_m)$ where $x_{\alpha_1} \geqslant n_1, \cdots, x_{\alpha_k} \geqslant n_k$ where $1 \leqslant \alpha_1 < \cdots < \alpha_k \leqslant m$ and $n_1, \cdots, n_k \in \mathbb{N}$. Then there are no Dedekind-finite solutions where $x_{\alpha_1} \geqslant n_1, \cdots, x_{\alpha_k} \geqslant n_k$.

**Proof:** Order the terms in $p, q$ lexicographically by the powers on the variables. Suppose there exists a bijection $f : p(x_1, \cdots, x_m) \to q(x_1, \cdots, x_m)$. Pick $n_1$ elements from $x_{\alpha_1}$ and order them in a list, then pick $n_2$ elements from $x_{\alpha_2}$, and so on until we have $n_1, \cdots, n_k$ elements from $x_{\alpha_1}, \cdots, x_{\alpha_k}$ respectively. We also have lists of 0 points in the other $x$'s. Since there are no integer solutions in this case, we have one of the following cases:

$$p(0, \cdots, n_1, \cdots, n_k, \cdots, 0) < q(0, \cdots, n_1, \cdots, n_k, \cdots, 0)$$

$$p(0, \cdots, n_1, \cdots, n_k, \cdots, 0) > q(0, \cdots, n_1, \cdots, n_k, \cdots, 0)$$

Suppose the latter is true. Order the points in $p(x_1, \cdots, x_m)$ first by the order of the terms, then by coefficient, then by the order on the $x$'s, then lexicographically within $x_i^j$. Then we have an ordered list of $p(0, \cdots, n_1, \cdots, n_k, \cdots, 0)$ points in $p(x_1, \cdots, x_m)$, and we can send them via $f$ to $p(0, \cdots, n_1, \cdots, n_k, \cdots, 0)$

points in $q(x_1, \cdots, x_m)$. Since $p(0, \cdots, n_1, \cdots, n_k, \cdots, 0) > q(0, \cdots, n_1, \cdots, n_k, \cdots, 0)$, the points in $q(x_1, \cdots, x_m)$ must include at least one new point in one of $x_1, \cdots, x_m$, because they can't be only the combinations of the points we already have. Take the first such new point in the ordered list of $p(0, \cdots, n_1, \cdots, n_k, \cdots, 0)$ points and append it to the respective list of points in $x_1, \cdots, x_m$. Again since there are no integer solutions, we have an inequality:

$$p(0, \cdots, n_1, \cdots, 1, \cdots, n_k, \cdots, 0) < q(0, \cdots, n_1, \cdots, 1, \cdots, n_k, \cdots, 0)$$

$$p(0, \cdots, n_1, \cdots, 1, \cdots, n_k, \cdots, 0) > q(0, \cdots, n_1, \cdots, 1, \cdots, n_k, \cdots, 0)$$

If the former was true, we can use the same argument with $f^{-1}$ to lengthen one of the lists of elements in $x_1, \cdots, x_m$. Since at each stage we have ordered lists of elements with at least $n_1, \cdots, n_k$ elements from $x_{\alpha_1}, \cdots, x_{\alpha_k}$ respectively, we can repeat this step inductively to get countably infinite points in sequence. By the pigeonhole principle, at least one of the $x_1, \cdots, x_m$ must have countably infinitely many points, so at least one of them is Dedekind-infinite. □

As a special case, suppose we consider "trivial" solutions to be ones where at least one of $x_1, \cdots, x_m$ is 0. Then let $\alpha_1 = 1, \cdots, \alpha_k = m$ and $n_1 = \cdots = n_k = 1$, so by theorem 3.1 if there are no nontrivial integer solutions, there are no nontrivial Dedekind-finite solutions.

**Theorem 3.2.** Let $p, q$ be distinct finite polynomials in (up to) $m$ variables, $x_1, \cdots, x_m$ each. Suppose $p(x_1, \cdots, x_m) > q(x_1, \cdots, x_m)$ whenever $x_{\alpha_1} \geqslant n_1, \cdots, x_{\alpha_k} \geqslant n_k$. Then the same holds when we allow each of the $x_i$ to be Dedekind-finite.

**Proof:** Suppose for the sake of contradiction that there exists an injection $f : p(x_1, \cdots, x_m) \to q(x_1, \cdots, x_m)$ and $x_{\alpha_1} \geqslant n_1, \cdots, x_{\alpha_k} \geqslant n_k$. Since $x_{\alpha_1} \geqslant n_1, \cdots, x_{\alpha_k} \geqslant n_k$, create ordered lists of $n_1, \cdots, n_k$ elements from $x_{\alpha_1}, \cdots, x_{\alpha_k}$ respectively, as above.

Since $p(0, \cdots, n_1, \cdots, n_k, \cdots, 0) > q(0, \cdots, n_1, \cdots, n_k, \cdots, 0)$, we have an ordered list of $p(0, \cdots, n_1, \cdots, n_k, \cdots, 0)$ points in $p(x_1, \cdots, x_m)$, and we can map them to the same number of points in $q(x_1, \cdots, x_m)$ via $f$. Using the ordering from $f$, take the first new point in the ordered list and append it to the respective list of points in $x_1, \cdots, x_m$.

Since at each stage we have ordered lists of points in $x_1, \cdots, x_m$ with at least $n_1, \cdots, n_k$ points in $x_{\alpha_1}, \cdots, x_{\alpha_k}$ respectively, we can repeat inductively countably infinitely many times. By the pigeonhole principle, at least one of the $x$'s will end up with a countably infinite ordered sequence of points, so that $x$ is not Dedekind-finite. □

# 4 Possible extensions

The following are unproven conjectures that may be interesting with regards to Dedekind-finite sets and polynomials.

**Lemma 4.1.** Let $A$ be the set of atoms in the basic Fraenkel model, as described in chapter 4 of Jech's *The Axiom of Choice*. There is no injection $f : A^n \to K \times A^{n-1}$ for any $K, n \in \mathbb{N}$.

**Proof:** Suppose for the sake of contradiction that there exists such an injection $f$ in the model. Then it is supported by some finite $E \subset A$. Pick $a_1, \cdots, a_n$ all distinct elements of $A \backslash E$, then $f(a_1, \cdots, a_n) = (j, b_1, \cdots, b_{n-1})$ for some $j \in K$, and $b_1, \cdots, b_{n-1} \in A$. Since $a_1, \cdots, a_n$ are all distinct, at least one of them must be distinct from $b_1, \cdots, b_{n-1}$, say it is $a_i$.

Let $\pi$ be a permutation of $A$ that fixes all the elements of $A$ except for swapping $a_i$ with some $a'$ not in $E$ or $b_1, \cdots, b_{n-1}$. $\pi$ fixes $E$ so it fixes $f$, so we have $f(a_1, \cdots, a', \cdots, a_n) = (j, b_1, \cdots, b_{n-1})$, which contradicts $f$ being an injection. □

All that was required of $K$ in this proof was to be a pure set (or well-orderable, and thus in bijection with an ordinal/pure set). This suggests that the theorem may be generalizable to polynomials with well-orderable coefficients. It may also be interesting to look at polynomials with Dedekind-finite coefficients and exponents.

This proof can also be adapted to the second Fraenkel model by specifying that all the $a$'s are from different pairs and none are paired with elements in $E$, then swapping $a_i$ not paired with any $b$. It can also be adapted to the Mostowski model by choosing a permutation that fixes every element of $A$ outside of the interval that $a_i$ is in (where the interval endpoints are the $b$'s and the elements of $E$) but does not fix $a_i$. This suggests that perhaps the theorem can be generalized to all Dedekind-finite sets.

**Conjecture.** Suppose $f(x, y), g(x, y)$ are distinct polynomials and $x, y$ are Dedekind-finite. There exist $k, n \in \mathbb{N}$ such that either $f(x, y) < g(x, y)$ for all $y > kx^n$ or $g(x, y) < f(x, y)$ for all $y > kx^n$.

**Partial proof:** We can assume without loss of generality that $f, g$ have no overlapping terms and all non-negative coefficients, because otherwise we can cancel terms.

Case 1: $f, g$ both have $n$ as the highest power of $x$ and $m$ as the highest power of $y$. It is unclear what conditions on $x$ and $y$ would ensure that $f > g$ or $g > f$.

Case 2: Without loss of generality, $f$ has a higher power of $y$ than $g$. I claim that if $y > x^k$ where $k$ is the largest power of $x$ in $g$ and $y$ is sufficiently large, then $f(x, y) > g(x, y)$.

Let $g'$ be $g$ but with every power of $x$ replaced with $x^k$ and let $f'$ be $f$ but with every power of $x$ replaced with 1. Then $g'$ is of the form $p(y)x^k$ where $p(y)$ is some polynomial in $y$ with degree less than the highest power of $y$ in $f$. Also $f'$ is of the form $q(y)$, a polynomial in $y$ with degree equal to the highest power of $y$ in $f$.

Note that $g < g'$ because since $x \geqslant 1$, replacing lower powers of $x$ with $x^k$ only increases the polynomial value, and $f' < f$ because replacing higher powers of $x$ with 1 only decreases the polynomial value. Then if $y > x^k$, $g' < f'$, so $g < g' < f' < f$.

While the general case of polynomials in multiple variables may not yield any interesting results (for instance, there is no useful criterion to determine when Dedekind-finite sets $x \geqslant y$ without any restriction on $x$ and $y$), this may give another criterion to tell when one polynomial is greater than another.

Almost all of the proofs given so far do not depend on the model of Zermelo-Fraenkel set theory used to generate infinite Dedekind-finite sets, which leads one to wonder if there are describable differences in arithmetic in different models' Dedekind-finite sets. If there are, is there some set in say, the Mostowski model with the same arithmetic properties as the set of atoms in the basic Fraenkel model, and so on?

These proofs also all deal with ways that infinite Dedekind-finite sets are more similar to finite sets than Dedekind-infinite sets arithmetically, but it is not clear exactly how similar they are, or which differences between infinite Dedekind-finite sets and finite sets can be detected with polynomials.

Since binomial coefficients can be expressed as polynomials with rational coefficients, one may also wonder if we can characterize binomial coefficients with regards to Dedekind-finite sets similarly.

# 5 References

T. J. Jech; *The Axiom of Choice*; North Holland Publishing Company: Amsterdam, 1973.