A Nonmeasurable Set from Coin Flips

Author(s): Alexander E. Holroyd and Terry Soo

Source: *The American Mathematical Monthly*, Dec., 2009, Vol. 116, No. 10 (Dec., 2009), pp. 926-928

Published by: Taylor & Francis, Ltd. on behalf of the Mathematical Association of America

Stable URL: https://www.jstor.org/stable/40391252

2. I. N. Herstein, *Topics in Algebra*, 2nd ed., John Wiley, Hoboken, NJ, 1975.
3. A. Jackson, Supporting a national treasure, *Notices Amer. Math. Soc.* **50** (2003) 1221.
4. J. Miller, Nadine Kowalsky: In memoriam, *AWM Newsletter* **26** (1996) 4.

IDA Center for Communications Research, 805 Bunn Drive, Princeton, NJ 08540
beals@idaccr.org

A Nonmeasurable Set from Coin Flips

Alexander E. Holroyd and Terry Soo

To motivate the elaborate machinery of measure theory, it is desirable to show that in some natural space Ω one cannot define a measure on *all* subsets of Ω, if the measure is to satisfy certain natural properties. The usual example is given by the Vitali set, obtained by choosing one representative from each equivalence class of $\mathbb{R}$ induced by the relation $x \sim y$ if and only if $x - y \in \mathbb{Q}$. The resulting set is not measurable with respect to any translation-invariant measure on $\mathbb{R}$ that gives nonzero, finite measure to the unit interval [**8**]. In particular, the resulting set is not Lebesgue measurable. The construction above uses the axiom of choice. Indeed, the Solovay theorem [**7**] states that in the absence of the axiom of choice, there is a model of Zermelo-Frankel set theory where all the subsets of $\mathbb{R}$ are Lebesgue measurable.

In this note we give a variant proof of the existence of a nonmeasurable set (in a slightly different space). We will use the axiom of choice in the guise of the well-ordering principle (see the later discussion for more information). Other examples of nonmeasurable sets may be found for example in [**1**] and [**5**, Ch. 5].

We will produce a nonmeasurable set in the space $\Omega := \{0, 1\}^{\mathbb{Z}}$. Translation-invariance plays a key role in the Vitali proof. Here shift-invariance will play a similar role. The **shift** $T : \mathbb{Z} \to \mathbb{Z}$ on integers is defined via $Tx := x + 1$, and the shift $\tau : \Omega \to \Omega$ on elements $\omega \in \Omega$ is defined via $(\tau\omega)(x) := \omega(x - 1)$. We write $\tau A := \{\tau\omega : \omega \in A\}$ for $A \subseteq \Omega$.

Theorem 1. *Let $\mathcal{F}$ be a σ-algebra on Ω that contains all singletons and is closed under the shift (that is, $A \in \mathcal{F}$ implies $\tau A \in \mathcal{F}$). If there exists a measure μ on $\mathcal{F}$ that is shift-invariant (that is, $\mu = \mu \circ \tau$) and satisfies $\mu(\Omega) \in (0, \infty)$, and $\mu(\{\omega\}) = 0$ for all $\omega \in \Omega$, then $\mathcal{F}$ does not contain all subsets of Ω.*

The conditions on $\mathcal{F}$ and μ in Theorem 1 are indeed satisfied by measures that arise naturally. A central example is the probability space $(\Omega, \mathcal{G}, \mathbb{P})$ for a sequence of independent fair coin flips indexed by $\mathbb{Z}$, which is defined as follows. Let $\mathcal{A}$ be the algebra of all sets of the form $\{\omega \in \Omega : \omega(k) = a_k, \text{ for all } k \in K\}$, where $K \subset \mathbb{Z}$ is any finite subset of the integers and $a \in \{0, 1\}^K$ is any finite binary string. The measure $\mathbb{P}$ restricted to $\mathcal{A}$ is given by $\mathbb{P}\big(\{\omega \in \Omega : \omega(k) = a_k, \text{ for all } k \in K\}\big) = 2^{-|K|}$, where $|K|$ denotes the cardinality of K. Thus $\mathbb{P}(\Omega) = 1$, and $\mathbb{P} = \mathbb{P} \circ \tau$ on $\mathcal{A}$. The Carathéodory extension theorem [**6**, Ch. 12, Theorem 8] gives a unique extension $\mathbb{P}$ to $\mathcal{G} := \sigma(\mathcal{A})$ (the σ-algebra generated by A) satisfying $\mathbb{P} = \mathbb{P} \circ \tau$. In addition, the continuity of measure implies $\mathbb{P}(\{\omega\}) = 0$ for all $\omega \in \Omega$. Hence Theorem 1 implies that $\mathcal{G}$ does not

doi:10.4169/000298909X477041

contain all subsets of Ω. Of course, the same holds for any extension $(\Omega, \mathcal{G}', \mathbb{P}')$ of $(\Omega, \mathcal{G}, \mathbb{P})$ for which $\mathbb{P}'$ is shift-invariant (such as the completion under $\mathbb{P}$).

To prove Theorem 1 we will define a nonmeasurable function. We are interested in functions from Ω to $\mathbb{Z}$ that are defined everywhere except on some set of measure zero. Therefore, for convenience, introduce an additional element $\Delta \notin \mathbb{Z}$. Consider a function $X : \Omega \to \mathbb{Z} \cup \{\Delta\}$. We call X **almost-everywhere defined** if $X^{-1}\{\Delta\}$ is countable, which implies that $\mu(X^{-1}\{\Delta\}) = 0$, for any measure μ satisfying the conditions of Theorem 1. A function X is **measurable** with respect to $\mathcal{F}$ if $X^{-1}\{x\} \in \mathcal{F}$ for all $x \in \mathbb{Z}$. We call X **shift-equivariant** if

$$X(\tau\omega) = T(X(\omega)) \quad \text{for all } \omega \in \Omega$$

(where $T(\Delta) := \Delta$). (We may think of a shift-equivariant X as an "origin-independent" rule for choosing an element from the sequence ω.) Shift-equivariant functions of random processes are important in many settings, including percolation theory (for example in [**2**]) and coding theory (for example in [**3, 4**]).

Lemma 2. *If $X : \Omega \to \mathbb{Z} \cup \{\Delta\}$ is an almost-everywhere defined, shift-equivariant function then X is not measurable with respect to any $\mathcal{F}$ satisfying the conditions of Theorem 1.*

Lemma 3. *There exists an almost-everywhere defined, shift-equivariant function X : $\Omega \to \mathbb{Z} \cup \{\Delta\}$.*

Theorem 1 is an immediate consequence of the preceding two facts.

Proof of Theorem 1. Let $(\Omega, \mathcal{F}, \mu)$ be a measure space satisfying the conditions of Theorem 1. Using Lemma 3, let X be an almost-everywhere defined shift-equivariant function. By Lemma 2, X is not $\mathcal{F}$-measurable. Therefore there exists $z \in \mathbb{Z}$ such that $X^{-1}\{z\} \notin \mathcal{F}$. ■

Proof of Lemma 2. Towards a contradiction, let X be a measurable function on $(\Omega, \mathcal{F}, \mu)$ satisfying the conditions of Lemma 2. Since X is shift-equivariant we have for each $x \in \mathbb{Z}$,

$$\mu(X^{-1}\{x\}) = \mu\big(\tau^{-x}X^{-1}\{x\}\big) = \mu(X^{-1}\{0\}).$$

Hence

$$\mu(X^{-1}\mathbb{Z}) = \mu\Big(\bigcup_{x\in\mathbb{Z}} X^{-1}\{x\}\Big) = \sum_{x\in\mathbb{Z}} \mu(X^{-1}\{0\}) = 0 \text{ or } \infty,$$

which contradicts the facts that $\mu(X^{-1}\{\Delta\}) = 0$ and $\mu(\Omega) \in (0, \infty)$. ■

Let us recall some facts about well-ordering. A total order $\preceq$ on a set W is a **well order** if every nonempty subset of W has a least element. The well-ordering principle states that every set has a well order. It is a classical result of Zermelo [**9**] that the well-ordering principle is equivalent to the axiom of choice.

Proof of Lemma 3. Say $\omega \in \Omega$ is **periodic** if $\tau^x\omega = \omega$ for some $x \in \mathbb{Z} \setminus \{0\}$. If ω is not periodic then $(\tau^x\omega)_{x\in\mathbb{Z}}$ are all distinct. Using the well-ordering principle, fix a well order $\preceq$ of Ω and define the function

$$X(\omega) := \begin{cases} \Delta & \text{if } \omega \text{ is periodic;} \\ \text{the unique } x \text{ minimizing } \tau^{-x}\omega \text{ under } \preceq & \text{otherwise.} \end{cases}$$

(We may think of $\tau^{-x}\omega$ as ω viewed from location x, in which case X is the location from which ω appears least.) Clearly, X is shift-equivariant. It is almost-everywhere defined since Ω contains only countably many periodic elements. ■

ACKNOWLEDGMENTS. Alexander E. Holroyd is funded in part by an NSERC (Canada) Discovery Grant. Terry Soo is funded in part by an NSERC PGS D and a UBC Graduate fellowship.

REFERENCES

1. D. Blackwell and P. Diaconis, A non-measurable tail set, in *Statistics, Probability and Game Theory*, IMS Lecture Notes-Monograph Series, vol. 30, Institute of Mathematical Statistics, Hayward, CA, 1996, 1–5.
2. R. M. Burton and M. Keane, Density and uniqueness in percolation, *Comm. Math. Phys.* **121** (1989) 501–505. doi:10.1007/BF01217735
3. M. Keane and M. Smorodinsky, A class of finitary codes, *Israel J. Math.* **26** (1977) 352–371. doi:10.1007/BF03007652
4. ———, Bernoulli schemes of the same entropy are finitarily isomorphic, *Ann. of Math. (2)* **109** (1979) 397–406. doi:10.2307/1971117
5. J. C. Oxtoby, *Measure and Category*, 2nd ed., Graduate Texts in Mathematics, vol. 2, Springer-Verlag, New York, 1980.
6. H. L. Royden, *Real Analysis*, 3rd ed., Macmillan, New York, 1988.
7. R. M. Solovay, A model of set-theory in which every set of reals is Lebesgue measurable, *Ann. of Math. (2)* **92** (1970) 1–56. doi:10.2307/1970696
8. G. Vitali, Sul problema della misura dei gruppi di punti di una retta, Gamberini and Parmeggiani, Bologna, 1905.
9. E. Zermelo, Beweis, daß jede Menge wohlgeordnet werden kann, *Math. Ann.* **59** (1904) 514–516. doi:10.1007/BF01445300

Department of Mathematics, University of British Columbia, 121–1984 Mathematics Rd, Vancouver, BC V6T 1Z2, Canada
holroyd@math.ubc.ca; tsoo@math.ubc.ca

A Note on Euler's Factoring Problem

John Brillhart

1. THE INITIAL PROBLEM. In 1640 Fermat communicated the following result to Mersenne [**5**, p. 67]: A prime of the form $4n + 1$ can be expressed as a sum of two squares in just one way.

About a century later, Euler became interested in the following immediate consequence of this result: An odd integer N that can be expressed as a sum of two squares in two different ways is composite. (That N has the form $4n + 1$ is clear from reducing the sum of two squares mod 4). The factoring problem associated with this

doi:10.4169/000298909X477050