Prime-Residue-Class of Uniform Charges on the Integers

Michael Spece · Joseph B. Kadane

Received: date / Accepted: date

Abstract There is a probability charge on the power set of the integers that gives probability $1/p$ to every residue class modulo a prime $p$. There exists such a charge that gives probability $w$ to the set of prime numbers iff $w \in [0, 1/2]$. Similarly, there is such a charge that gives probability $x$ to a residue class modulo $c$, where $c$ is composite, iff $x \in [0, 1/y]$, where $y$ is the largest prime factor of $c$.

Keywords probability charge · finite additivity · uniform distribution · residue class · prime numbers

Mathematics Subject Classification (2010) MSC 60A05

We thank David Donoho for posing the question of whether $PR = R$. The Department of Defense (DoD) supported the first author through the National Defense Science & Engineering Graduate Fellowship (NDSEG) Program.

M. Spece
Department of Statistics & Data Science and
Machine Learning Department
Carnegie Mellon University
Pittsburgh, PA 15213
Tel.: 412-268-2717
Fax: 412-268-7828
E-mail: spec@cmu.edu

J.B. Kadane
Department of Statistics & Data Science
Carnegie Mellon University
Pittsburgh, PA 15213
Tel.: 412-268-8726
Fax: 412-268-7828
E-mail: kadane@stat.cmu.edu
1 Distributions uniform on the integers

A probability charge\(^1\) uniform on the integers assigns 0 to each integer, but that of 1 to \(\mathbb{Z}\), precluding countable additivity. Every finite set has probability 0, and each cofinite set 1, leaving undetermined jointly infinite-cofinite sets.

Suppose \(C\) is a collection of subsets from \(\Omega\) (here \(\mathbb{Z}\)) such that \(\Omega \in C\). Let \(\mu\) be a non-negative function on \(C\) such that \(\mu(\Omega) = 1\). Theorem 1 of [1] gives a necessary and sufficient condition that \(\mu\) can be extended to a finitely additive probability on the power set of \(\Omega\). Applying this result, they show the special case in which \(C\) is the class of sets that have natural\(^2\) densities\(^3\) admits such an extension, where \(\mu\) is taken to assign a set its natural density, when that exists.

[2] study three classes of finitely additive probabilities: The class \(L\) extending limit relative frequency, the class \(S\) of shift\(^4\) invariant\(^5\) functions \(\mu\), and the class \(R\) assigning probability \(1/m\) to each residue class mod \(m\) for all positive integers \(m\). They show that

\[ L \subset S \subset R \]

where each of the inclusions above are strict.

[4] study the class \(WT\) of weakly thinable probabilities and show it is strictly less inclusive than \(L\).

Each of the previously studied classes\(^6\) has an intuitive interpretation of uniformity that goes beyond assigning each integer 0. The inclusions indicate that these various notions of uniformity are strictly nested, with \(R\) comprising the weakest notion.

2 The Prime Residue Class

One may consider a potentially weaker notion of uniformity than that of \(R\) by specifying the probability of each residue class mod \(m\) for \(m\) in a strict subset of \(\mathbb{Z}\). The primes are a natural choice for this subset. Therefore, consider the class \(PR\) of finitely additive probabilities on the integers that give probability \(1/m\) to each residue class mod \(m\) where \(m\) is a prime number. Since this condition is weaker than that defining the class \(R\), we must have

\[ WT \subset L \subset S \subset R \subseteq PR \]

Given that every integer has a prime factorization, \(R = PR\) is conceivable. To the contrary, we show that \(R \subset PR\).

Since \(PR\) is the least demanding of these classes, it is important to establish at the outset that each member of \(PR\) is uniform on the integers. That is accomplished with the following easy result. First, a notation for sets of “natural” numbers:

**Definition 1 (Natural Numbers)** Denote the nonnegative integers by \(\mathbb{Z}^+\) and the positive ones by \(\mathbb{Z}^{>0}\).

Also, let \(\mathbb{N}_p\) denote the primes, \(\mathbb{Z}\) integers, \(\mathbb{Q}\) rationals, and \(\mathbb{R}\) reals.

---

1 Also known as a finitely additive probability or additive distribution, but these terms conflate with terminology for standard probability.
2 Also, “asymptotic” and “arithmetic”.
3 Also known as limit (or limiting) relative frequencies.
4 Also, “translation”.
5 Equivalently, thinable with respect to (i) affine transformations; or (ii) \(2 \times\) or (iii) general-scale invariance. See Theorem 1.11 of [3].
6 There are others, for example those based on “thinning out” sets in [3].
Proposition 1 (Uniformity) Under PR, each integer has probability 0.

Proof Let \( z \in \mathbb{Z} \) and \( \varepsilon > 0 \) be given, and let \( m \) be a prime greater than \( 1/\varepsilon \). Now \( z \equiv j \mod m \) for some \( j, 0 \leq j \leq m - 1 \). Then

\[
P\{z\} \leq P\{j \mod m\} = 1/m < \varepsilon.
\]

Hence, \( P\{z\} = 0 \) for all \( z \in \mathbb{Z} \).

The remainder of this paper is organized as follows: Section 3 gives general upper bounds on the probability of sets. Sections 4 and 5 respectively apply these results to \( \mathbb{N}_p \) and residue classes, proving the claims thereon. Section 6 concludes.

3 Suprema of Probabilities

For every class of uniform distributions and every subset \( S \) of the space measured under these distributions, the probability range of \( S \) is a closed interval (Theorem 2 of [1]). Restricting to the class PR and the set \( \mathbb{N}_p \) of prime numbers, a greatest lower bound of 0, quoted below for future reference, is immediate from the inclusion \( L \subset PR \).

Proposition 2 (Greatest Lower Bound for Primes)

\[
\inf_{\mu \in PR} \mu(\mathbb{N}_p) = 0.
\]

Thus, to prove the probability of the prime numbers can be any value in the interval \( [0, 1/2] \), it suffices to show the least upper bound of the probability of the primes is \( 1/2 \).

At the heart of affording measure to a set is the following theorem about general sets.

Theorem 1 (Probability Range) Suppose \( \mathcal{C} \) is a subset of the power-set \( 2^\Omega \), that \( \Omega \in \mathcal{C} \), and finally that \( \mu_0 \) is a function on \( \mathcal{C} \) that can be extended to a finitely additive probability on \( 2^\Omega \). Let \( \mathcal{M} \) be the family of such extensions. Then for every \( S \in 2^\Omega \),

\[
\sup_{\mu \in \mathcal{M}} \mu(S) = \inf \left\{ \frac{1}{h} \left( \sum_{i=1}^{a} \mu_0(A_i) - \sum_{j=1}^{b} \mu_0(B_j) \right) \right\},
\]

(Id1)

in which the \( \inf \) is taken over \( h \in \mathbb{Z}^+; a, b \in \mathbb{Z}^+; A_i, B_j \in \mathcal{C} \) such that

\[
\sum_{i=1}^{a} I_{A_i} - \sum_{j=1}^{b} I_{B_j} \geq h I_S.
\]

(Ct2)

Proof The proof is that of Theorem 2 in [1].

Remark (Notation):

- \( S \) typically denotes a set whose probability is of interest.
- The prefix of a number is an abbreviation. For example, Ct2 is short for Constraint 2, and is referred to as Constraint Ct2 in prose. “A” stands for approximation, the meaning of which is to be interpreted liberally.
Definition 2 (Relations) For all sets A and B, define \( A \setminus B := \{ a \in A : a \notin B \} \) and, when + is defined on \( A \times B \), \( A + B := \{ a + b : a \in A, b \in B \} \).

The elements of a residue class are shifts or, less descriptively, representatives. For all \( A \subseteq \mathbb{Z} \) and \( m \in \mathbb{Z}^{>0} \), \( \mod m := \bigcup_{a \in A} a \mod m \).

For all \( a, b \in \mathbb{Z}^{>0} \), \( a \mid b \) denotes that a divides b. For every pair of \( \mathbb{R} \)-valued functions \( f \) and \( g \) with common domain \( X \), \( f \leq g \) is to be understood in the domination or Pareto sense, that is for all \( x \in X \), \( f(x) \leq g(x) \).

Lemma 1 (Concise Rewrite) Let \( \mathcal{C} \) be a collection of sets and \( \mathcal{F} := \ell^0 (\mathbb{Q}^\mathcal{C}) \). For all \( h \in \mathbb{Z}^{>0} ; a, b \in \mathbb{Z}^+ ; A_i, B_j \in \mathcal{C} \), there exists a unique \( f \in \mathcal{F} \) such that, for all \( g \in \mathbb{R}^\mathcal{C} \),

\[
\frac{1}{h} \left( \sum_{i=1}^{a} g(A_i) - \sum_{j=1}^{b} g(B_j) \right) = \sum_{C \in \mathcal{C}} f(C)g(C). \tag{Id3}
\]

Conversely, if \( f \in \mathcal{F} \) and \( g \in \mathbb{R}^\mathcal{C} \), then there exists \( h \in \mathbb{Z}^{>0} ; a, b \in \mathbb{Z}^+ ; A_i, B_j \in \mathcal{C} \) such that Identity (Id3) holds.

Proof Suppose \( h \in \mathbb{Z}^{>0} ; a, b \in \mathbb{Z}^+ ; A_i, B_j \in \mathcal{C} \).

Uniqueness follows from the flexibility in choosing \( g \); for all \( C \in \mathcal{C} \),

\[
f(C) = \frac{1}{h} \left( \sum_{i=1}^{a} I_{A_i=C} - \sum_{j=1}^{b} I_{B_j=C} \right). \tag{Id4}
\]

The question becomes whether, for all \( g \),

\[
\sum_{C \in \mathcal{C}} \left( \sum_{i=1}^{a} I_{A_i=C} - \sum_{j=1}^{b} I_{B_j=C} \right) g(C) = \left( \sum_{i=1}^{a} g(A_i) - \sum_{j=1}^{b} g(B_j) \right),
\]

for which the following system (if true) suffices

\[
\sum_{C \in \mathcal{C}} \sum_{i=1}^{a} I_{A_i=C} g(C) = \sum_{i=1}^{a} g(A_i)
\]

\[
\sum_{C \in \mathcal{C}} \sum_{j=1}^{b} I_{B_j=C} g(C) = \sum_{j=1}^{b} g(B_j).
\]

But indeed

\[
\sum_{i=1}^{a} g(A_i) = \sum_{i=1}^{a} \sum_{C \in \mathcal{C}} I_{A_i=C} g(C) = \sum_{C \in \mathcal{C}} \sum_{i=1}^{a} I_{A_i=C} g(C)
\]

\[
\sum_{j=1}^{b} g(B_j) = \sum_{j=1}^{b} \sum_{C \in \mathcal{C}} I_{B_j=C} g(C) = \sum_{C \in \mathcal{C}} \sum_{j=1}^{b} I_{B_j=C} g(C).
\]
and symmetrically for $\sum_{j=1}^{k} g(B_j)$.

Turning to the converse, invert Identity Id4. Since therein only $A_i$ and $B_j$ that equal $C$ count, $\text{card}(i : A_i = C)$ and $\text{card}(j : B_j = C)$ can be set without regard to $a$, $b$, $(A_i)_{i: A_i \neq C}$, or $(B_j)_{j: A_j \neq C}$. Set $h$ to a common denominator of $\{ f(C) : C \in \mathcal{C} \}$ so that $hf(C)$ is always an integer. Set $\text{card}(i : A_i = C) := hf(C)I_{f(C) > 0}$ and $\text{card}(j : B_j = C) := hf(C)I_{f(C) < 0}$.

Rewriting the sums appearing in Theorem 1 according to Lemma 1, one obtains the following theorem restatement.

**Theorem 2 (Concise Form of Theorem 1)** Suppose $\mathcal{C} \subseteq 2^\Omega$, that $\Omega \in \mathcal{C}$, and finally that $\mu_0$ is a function on $\mathcal{C}$ that can be extended to a finitely additive probability on $2^\Omega$. Let $\mathcal{M}$ be the family of such extensions. Then for every $S \in 2^\Omega$,

$$\sup_{\mu \in \mathcal{M}} \mu(S) = \inf_{\alpha \in \mathcal{P}(\mathcal{C})} \sum_{C \in \mathcal{C}} \alpha(C)\mu_0(C),$$

(Id5)

in which $\alpha$ is additionally subject to

$$\sum_{C \in \mathcal{C}} \alpha(C)I_C \geq I_S.$$  

(Ct6)

**Proof** Applying Lemma 1 simultaneously to $\mu_0, I \in \mathbb{R}^{\mathcal{C}}$ in Identity Id1 and Constraint Ct2, respectively, yields the desired form of the objective function in the right-hand side of Identity Id5 and in Constraint Ct6. The converse in Lemma 1 ensures the constraint set has not expanded.

Remark: In contrast to Theorem 1, each $C \in \mathcal{C}$ appears in at most one term in each of the sums appearing on the right (resp. left) hand side of Identity Id5 and Constraint Ct6; thereof, also, $I_S$ has no coefficient. Both of these simplifications, especially the first, make bookkeeping easier when applying the theorem to PR.

**Definition 4 (Subsets of Primes)** Let $p_i$ be the $i$th largest prime ($i \in \mathbb{Z}^+0$), $p_0 := 1$, and $\{1, \ldots, p_i\}$ or $\{1 : p_i\}$ the set of positive integers less than $p_i + 1$.

For all $N \in \mathbb{Z}^+$, let $N!_p := \prod_{i=1}^{N} p_i$ and, for all $j \in \times_{i=1}^{N} \{1, \ldots, p_i\}$, $s(j)$ the shift of $\cap_{i=1}^{N} j_i \bmod p_i$ in $\{1, \ldots, N!_p\}$ (which exists and is unique by the Chinese Remainder Theorem). Note $s$ depends on $N$ implicitly.

**Definition 5 ( )** Let $\ell_Q := \ell^0(\mathbb{Q}^{\mathbb{Z}^+} \times \mathbb{Z}^{-\mathbb{N}})$. For all $(\alpha_{i,j})_{i,j} \in \ell_Q$, let $\alpha_i$ denote the vector $\alpha_{i,1}, \alpha_{i,2}, \ldots$. More generally, a dot is used as the placeholder for a function argument.

Theorem 2— with $\mathcal{M} := PR$, $\mathcal{C}$ the collection of prime residue classes, and $\mu_0(\cdot \bmod p_i) \equiv \frac{1}{p_i}$ for all $i \in \mathbb{Z}^+$—gives

$$\sup_{\mu \in \mathcal{M}} \mu(S) = \inf_{\alpha \in \ell_Q} f(\alpha),$$

(Id7)

in which $f(\alpha) := \sum_{i=0}^{\infty} \sum_{j=1}^{p_i} \frac{\alpha_{i,j}}{p_i}$ and $\alpha$ is additionally subject to

$$G(\alpha) \geq I_S,$$

(Ct8)

where $G(\alpha) := \sum_{i=0}^{\infty} \sum_{j=1}^{p_i} \alpha_{i,j} I_{j \bmod p_i}$.

The following proposition provides a convenient avenue through which to make explicit the dependence of $\alpha \in \ell_Q$ (as appears in Identity Id7) on only a finite number of components.
Proposition 3 (Continuity) Suppose $(S1)$ $f : A \to \mathbb{R}$ and $(S2)$ $\bigcup_{n=1}^{\infty} A_n = A$. Then
\[
\lim_{N \to \infty} \inf_{\alpha \in \bigcup_{n=1}^{N} A_n} f(\alpha) = \inf_{\alpha \in A} f(\alpha). \tag{Id9}
\]

Proof inf$_{\alpha \in \bigcup_{n=1}^{N} A_n} f(\alpha)$ over the weakening constraint $\alpha \in \bigcup_{n=1}^{N} A_n$ is monotonic over $N$. Hence, the left-hand side of Identity Id9 is well defined.

Because, for all $N \in \mathbb{Z}^>0$, $\bigcup_{n=1}^{N} A_n \subseteq A$;
\[
\lim_{N \to \infty} \inf_{\alpha \in \bigcup_{n=1}^{N} A_n} f(\alpha) \geq \inf_{\alpha \in A} f(\alpha), \tag{A10}
\]
so it suffices to prove the reverse inequality of Approximation A10.

By completeness of the real numbers, there exists $(\alpha_n)_{n=1}^{\infty} \in A^{\infty}$ such that
\[
\lim_{n \to \infty} f(\alpha_n) = \inf_{\alpha \in A} f(\alpha). \tag{Id11}
\]

By Supposition (S2), there exists a subsequence $(N_k)_{k=1}^{\infty}$ of $(N)_{N=1}^{\infty}$ such that, for all $k \in \mathbb{Z}^>0$, $\alpha_k \in \bigcup_{n=1}^{N_k} A_n$. Then
\[
\lim_{N \to \infty} \inf_{\alpha \in \bigcup_{n=1}^{N} A_n} f(\alpha) = \lim_{k \to \infty} \inf_{\alpha \in \bigcup_{n=1}^{N_k} A_n} f(\alpha). \tag{Id12}
\]

Because, for all $k \in \mathbb{Z}^>0$, inf$_{\alpha \in \bigcup_{n=1}^{N_k} A_n} f(\alpha) \leq f(\alpha_k)$; the right-hand side of Identity Id12 is upper bounded by
\[
\lim_{k \to \infty} f(\alpha_k). \tag{A13}
\]

Combining Identity Id11 and Approximation A13, the reverse of Approximation A10 holds.

The theorem following relies on the notion of multi-sets.

Definition 6 (Multi-sets) Multi-set is an extension of set, endowing each of its elements with a multiplicity in $\mathbb{Z}^>0 \cup \{\infty\}$. Every set can be viewed as a multi-set each of whose elements has multiplicity 1. $\mathcal{J}$, or an embellishment thereof, denotes a multi-set.

The cardinality of a multi-set is the sum of its elements’ multiplicities. Multi-set and set cardinalities coincide on countable sets.

Multi-set intersection also extends that for set. Intersections of multi-sets are taken to preserve the highest multiplicity of an element appearing in any of the multi-sets (excluding a multiplicity of zero).

Multi-set inclusion similarly takes multiplicity into consideration: $\mathcal{J}_0 \subseteq \mathcal{J}$ if $\mathcal{J}_0 \cap \mathcal{J}$ does not increase the multiplicity of any element. However, multi-set inclusion in a set is only meant to indicate the elements of that multi-set are in that set.

Definition 7 (Coordinates) Given, either implicitly by its use or explicitly by its declaration, an $N \in \mathbb{Z}^{>0} \cup \{\infty\}$, let $\mathcal{N} := \begin{cases} \{1, \cdots, N\} & N < \infty \\ \mathbb{Z}^{>0} & N = \infty. \end{cases}$

For all $n \in \mathcal{N}$, finite-cardinality multi-sets $A \subseteq \times_{n \in \mathcal{N}} \{1, \cdots, p_n\}$, $a \in A$, $i \in \mathbb{Z}^{>0}$, and $b \in \{1, \cdots, p_i\}$,
- $a_n$ is the $n$ (of $N$)th coordinate of $a$.
Prime-Residue-Class of Uniform Charges

– \( \text{proj}(A) \) (projection) is the set of \( n \)th coordinates from \( A \), endowing each coordinate value with a multiplicity equal to the cardinality of \( \text{proj}_n^{-1}(a) \cap A \),\(^7\) in which the inverse image is taken with respect to regarding \( \times_{n \in A} \{1, \cdots, p_n\} \) as the domain of \( \text{proj}_n \).

– \( \text{card}_n(A) := \text{card}(\text{proj}_n(A)) \)
– \( a \rightarrow := (a_1, \cdots, a_{i-1}, a_{i+1}, \cdots, a_N) \)
– \( (a_i, b) := (a_1, \cdots, a_{i-1}, b, a_{i+1}, \cdots, a_N) \).

Similarly, for all sets \( A, B \in \times_{n=1}^N \{1, \cdots, p_n\} \) and \( i \in \{1, \cdots, N\} \), \( A_{-i} \times B_i := \{(a_{-i}, b_i) : a \in A, b \in B\} \).

**Theorem 3 (Probability Range over \( PR \))** For every \( S \subseteq \mathbb{Z} \),

\[
\sup_{\mu \in PR} \mu(S) \geq \lim_{N \to \infty} \max_{\mathcal{J}} \frac{\text{card}(\mathcal{J} \cap \mathcal{S}^{-1}(S \mod N!)_p)}{N!_p},
\]

in which

(C1) For all \( N \in \mathbb{Z}^+ \), the \( \mathcal{J} \) of

\[
\max_{\mathcal{J}} \frac{\text{card}(\mathcal{J} \cap \mathcal{S}^{-1}(S \mod N!)_p)}{N!_p}
\]

within the right-hand side of Approximation A14 varies over multi-sets such that (i) \( \mathcal{J} \subseteq \times_{i=1}^N \{1, \cdots, p_i\} \) and (ii) for all \( n \in \mathcal{N} \), \( \text{proj}_n(\mathcal{J}) = \{1^{N/p_i}, \cdots, p_n^{N/p_i}\} \); in which superscripts denote the multiplicity of elements in the multi-set with non-positive subscripts signifying the absence of that element.

**Proof** Invoking Proposition 3, with \( A_n := \{\alpha \in \ell_Q : |\alpha|_0 \leq n\} \), the right-hand side of Identity Id7

\[
\sup_{\mu \in PR} \mu(S)
\]

becomes

\[
\lim_{N \to \infty} \inf_{\alpha \in \ell_Q : |\alpha|_0 \leq N} \sum_{i=0}^N \sum_{j=1}^{p_i} \frac{\alpha_{i,j}}{p_i} = \lim_{N \to \infty} \inf_{\alpha \in \ell_Q} \sum_{i=0}^N \sum_{j=1}^{p_i} \frac{\alpha_{i,j}}{p_i},
\]

(Id16) in which, for all \( N \in \mathbb{Z}^+ \), the \( \alpha \) of

\[
\inf_{\alpha \in \ell_Q} \sum_{i=0}^N \sum_{j=1}^{p_i} \frac{\alpha_{i,j}}{p_i}
\]

within the right-hand side of Identity Id16 is additionally subject to

\[
\sum_{i=0}^N \sum_{j=1}^{p_i} \alpha_{i,j}j \mod p_i \geq IS.
\]

(Ct18) By the Chinese Remainder Theorem, every \( z \in \mathbb{Z} \) corresponds to a

\[
j_z \in \times_{i=0}^N \{1, \cdots, p_i\}
\]

\(^7\) That \( A \) is finite-cardinality ensures the endowed multiplicities are finite.
such that $z \mod N!_p = s(j, z, 0) \mod N!_p$. ($j$ as defined is a branch of $s^{-1}$.) Moreover, $z$ is in no other residue classes than $s(j, k) \mod p_k$ for all positive integers $k \leq N$. Therefore, the left-hand side of Constraint Ct18 evaluated at $z$ is $\sum_{i=0}^{N} \alpha_{i,j,i}$ and Constraint Ct18 can be re-written as

$$\sum_{(j_0, j) \in \times_{i=0}^{N-1} \{1, \ldots, p_i\}} \left( \sum_{i=0}^{N} \alpha_{i,j,i} \right) I_{s(j) \mod N!_p} \geq I_{S}(z).$$

(Ct19)

Constraint Ct19 can be decomposed point-by-point as the set of constraints

$$\left\{ \sum_{(j_0, j) \in \times_{i=0}^{N-1} \{1, \ldots, p_i\}} I_{s(j) \mod N!_p} (z) \sum_{i=0}^{N} \alpha_{i,j,i} \geq I_{S}(z) \right\}_{z \in \mathbb{Z}}.$$  

(Ct20)

Breaking the left and right-hand sides of the inequalities Ct20 into cases of which modular class representative and which value in the indicator range are picked out by $z$, respectively:

$$\left\{ \sum_{i=0}^{N} \alpha_{i,j,i} : z \in s(j) \mod N!_p \right\}_{(j_0, j) \in \times_{i=0}^{N-1} \{1, \ldots, p_i\}} \geq \left\{ \begin{array}{ll} 0 & z \in \mathbb{Z} \setminus S \\ 1 & z \in S \end{array} \right\}$$  

Combine conditions

$$\left\{ \sum_{i=0}^{N} \alpha_{i,j,i} \geq \begin{cases} 0 & z \in \mathbb{Z} \setminus S \cap s(j) \mod N!_p \\ 1 & z \in S \cap s(j) \mod N!_p \neq \emptyset \end{cases} \right\}_{(j_0, j) \in \times_{i=0}^{N-1} \{1, \ldots, p_i\}}$$  

Combine inequalities

$$\sum_{i=0}^{N} \alpha_{i,j,i} \geq \begin{cases} 1 & (j, j) : s(j) \in S \mod N!_p \\ 0 & \text{otherwise} \end{cases}$$  

Condition on $j$

$$\sum_{i=0}^{N} \alpha_{i,j,i} \geq \begin{cases} 1 & j \in \{1\} \times s^{-1}(S \mod N!_p) \\ 0 & \text{otherwise} \end{cases}$$  

Definition of $s^{-1}$.  

(Ct21)

Expression 17 is, dividing out repetitions,

$$\inf_{\alpha \in \times_{j \in \times_{i=0}^{N-1} \{1, \ldots, p_i\}}} \frac{1}{\prod_{k \neq i} p_k} \sum_{i=0}^{N} \frac{1}{p_i} \sum_{j \in \times_{i=0}^{N-1} \{1, \ldots, p_i\}} \alpha_{i,j,i}.$$  

(22)

due to there being $\prod_{k \neq i} p_k$ repetitions of each $\{1, \ldots, p_i\}$ in the $i$th component of $\times_{i=0}^{N} \{1, \ldots, p_i\}$.

Factoring out (the constant) $\frac{1}{N!_p}$ from Expression 22 obtains

$$\inf_{\alpha \in \times_{j \in \times_{i=0}^{N-1} \{1, \ldots, p_i\}}} \frac{1}{N!_p} \sum_{j \in \times_{i=0}^{N-1} \{1, \ldots, p_i\}} \sum_{i=0}^{N} \alpha_{i,j,i}.$$  

(23)

The indices of $\alpha$ being summed over in

$$\sum_{j \in \times_{i=0}^{N-1} \{1, \ldots, p_i\}} \sum_{i=0}^{N} \alpha_{i,j,i}.$$  

(24)
of Expression 23 forms a multi-set of pairs

\[
\begin{cases}
0 & j > p_i \\
\left(\frac{N!_p}{p_i} \right) & j \in \{1, \ldots, p_i\}
\end{cases}
\]

whose multiplicities depend on the second coordinate \(j\). (Because \(p_i\) divides \(N!_p\), the multiplicities are non-negative integers, and thus valid.)

For every \(J\) obeying Condition (C1), the indices of \(\alpha\) being summed over in

\[
\sum_{j \in \{1\} \times J} N!_p \sum_{i=0}^{N} \alpha_{i,j_i}
\]

forms the multi-set 25 as well. Therefore, sums 24 and 26 must have the same multi-sets of terms and so, themselves being the sums of precisely the terms thereof, must be equal:

\[
\sum_{j \in \times_{i=0}^{N} \{1, \ldots, p_i\}} \sum_{i=1}^{N} \alpha_{i,j_i} = \sum_{j \in \{1\} \times J} \sum_{i=0}^{N} \alpha_{i,j_i}
\]

(25)

By Identity Id27, Expression 23, and in turn Expressions 22 and 17, are equal to

\[
\inf_{\alpha \in \times_{i=0}^{N} Q_{p_i}} \frac{1}{N!_p} \sum_{j \in \{1\} \times J} \sum_{i=0}^{N} \alpha_{i,j_i}
\]

for every \(J\) obeying (C1).

Sums 26 can be split up as

\[
\sum_{j \in \{1\} \times \mathcal{J} \cap \alpha^{-1}(S \mod N!_p)} \sum_{i=0}^{N} \alpha_{i,j_i} + \sum_{j \in \{1\} \times \mathcal{J} \setminus \alpha^{-1}(S \mod N!_p)} \sum_{i=0}^{N} \alpha_{i,j_i}
\]

(29)

Imposing Constraint Ct21 on Expression 29 yields a lower bound, that of

\[
\sum_{j \in \{1\} \times \mathcal{J} \cap \alpha^{-1}(S \mod N!_p)} 1 + \sum_{j \in \{1\} \times \mathcal{J} \setminus \alpha^{-1}(S \mod N!_p)} 0
\]

\[
= \text{card} \left( \mathcal{J} \cap \alpha^{-1}(S \mod N!_p) \right)
\]

(A30)

in which the equality leading to A30 is by the definition of cardinality (6).

Combining Expression 29 and Approximation A30, Expression 17 is bounded below by

\[
\max_{\mathcal{J}} \inf_{\alpha \in \times_{i=0}^{N} Q_{p_i}} \frac{\text{card} \left( \mathcal{J} \cap \alpha^{-1}(S \mod N!_p) \right)}{N!_p} = \max_{\mathcal{J}} \frac{\text{card} \left( \mathcal{J} \cap \alpha^{-1}(S \mod N!_p) \right)}{N!_p},
\]

(A31)

in which, for all \(N \in \mathbb{Z}_{>0}\), \(\mathcal{J}\) obeys Condition (C1). (The left-hand side of Approximation A31 does not depend on \(\alpha\), so can be dropped to obtain the right-hand side.)

Taking \(N \to \infty\) in Approximation A31 and Expression 17, while equating the latter limit to the left-hand side of Identity Id7, yields Approximation A14.
Remark: The \( \mathcal{J} \) of Condition (C1) is in some sense a re-arrangement of the components of \( x_{i=1}^{N} \{1, \cdots, p_n\} \).

Remark: The requirement \( \text{proj}_n(\mathcal{J}) = \{1^{N_1/p_n}, \cdots, P_n^{N_p/p_n} \} \) of Condition (C1) can be weakened to

\[
\text{proj}_n(\mathcal{J}) \subseteq \{1^{N_1/p_n}, \cdots, P_n^{N_p/p_n} \}.
\]

Moreover, the maximum in Approximation A14 is attained by some \( \mathcal{J} \) for which \( \text{proj}_n(\mathcal{J}) \subseteq \text{proj}_n(\mathcal{J}) \cap \text{proj}_n (s^{-1}(S \bmod N_1)) \) (where the intersection obeys Definition 6).

The following proposition further concerns the projections of a multi-set (which appear in the constraint set specified in Condition (C1)).

**Proposition 4 (Exchange Preserving)** \( \text{proj}_n(\mathcal{J}) \)

\[ \text{Let } N \in \mathbb{Z}^{>0} \cup \{\infty\}, \mathcal{J} \subseteq x_{n \in \mathcal{N}} \{1, \cdots, p_n\}, \text{a multi-set with at least two elements, say } j, k, \text{ and } n_{\in \mathcal{N}}. \text{Let } \mathcal{J}' := \mathcal{J} \setminus \{j, k\} \cup \{j', k'\}; \text{ where } 1. j' := (j_{-n}, k_{n}), 2. k' := (k_{-n}, j_{n}), 3. \text{decrements multiplicities as follows: for all objects } a \text{ and } b, c \in \mathbb{Z}, \{a^b, \cdots\} \cup \{a^c, \cdots\} = \{a^{b+c}, \cdots\}, \text{ and 4. increments them as follows: for all objects } a \text{ and } b, c \in \mathbb{Z}^+, \{a^b, \cdots\} \cup \{a^c, \cdots\} = \{a^{b+c}, \cdots\}. \text{ Then, for all } n \in \mathcal{N}, \text{proj}_n(\mathcal{J}) = \text{proj}_n(\mathcal{J}) \Rightarrow \text{proj}_n(\mathcal{J}') = \text{proj}_n(\mathcal{J}). \]

**Proof** \( j, k \in \mathcal{J} \) implies subtracting (or adding) \( \{j, k\} \) has the reverse effect on \( \text{proj}_n \) of the resultant multi-set, for all \( n \in \mathcal{N} \), as adding \( \{j', k'\} \) (or subtracting, respectively).

Given the frequency with which \( x_{n \in \mathcal{N}} \{1, \cdots, p_n\} \) occurs, a descriptive notation specific to its elements is given.

**Definition 8 (Paths)** Given any \( N \in \mathbb{Z}^{>0} \cup \{\infty\}, \text{ multi-set } \mathcal{J} \subseteq x_{n \in \mathcal{N}} \{1, \cdots, p_n\}, m \in \mathbb{Z}^{>0}, \text{ and } \]

\[
b^m \in x_{n \in \mathcal{N}} \{1, \cdots, p_n\}.
\]

\( b \) is a path. An illustration of the path \((1, 2) (N = 2)\):

\[
\begin{array}{c}
1 \\
2 \\
1
\end{array}
\]

where each column array of integers corresponds to a set in the product \( x_{n \in \mathcal{N}} \{1, \cdots, p_n\} \).

For every \( j \in \mathbb{Z}^{>0} \) and set \( A \subseteq \{1, \cdots, p_n\} \), \( b \) passes through, in its \( j \)th component, \( A \) iff \( b_j \in A \). In the illustration above, the path shown passes through \( \{1\} \) (both \( \{2\} \) and \( \{1, 2\} \) in the first (second) component, respectively.

Combinatorial arguments are described using the following terminology.

**Definition 9 (Life)** Given any \( N \in \mathbb{Z}^{>0} \cup \{\infty\}, \text{ set } A \subseteq x_{n \in \mathcal{N}} \{1, \cdots, p_n\}, \text{ and multi-set } \mathcal{J} \subseteq x_{n \in \mathcal{N}} \{1, \cdots, p_n\}, \text{a path in } \mathcal{J} \text{ is alive iff it is in } A. \text{ Exchanging components as in Proposition 4 is enlivening iff } j \text{ is dead and } j' \text{ alive or } k \text{ is dead and } k' \text{ is alive; and is (life) preserving iff, for each } i \in \{j, k\} \text{ that is alive, so is } i'. \text{ An enlivening and preserving exchange between an alive path and dead one is a (successful) donation (that leaves both } j', k' \text{ alive).}

**Proposition 5 (Re-Directing Paths)** Fix arbitrary

1. \( i, j \in \mathbb{Z}^{>0} \) (not necessarily distinct),
2. a multi-set \( \mathcal{J} \subseteq x_{n \in \mathbb{Z}^{>0}} \{p_1, \cdots, p_n\} \) of finite cardinality,
3. and, \( \forall k \in \{i, j\}, A_k \subseteq \{1, \cdots, p_k\} \).

Suppose \((C2) \text{ card}(\text{proj}_i(\mathcal{J}) \cap A_i) \leq \text{card}(\text{proj}_i(\mathcal{J}) \cap A_j) \). Then there exists a multiset \( \mathcal{J}' \) such that \((C3) \text{ proj}_n(\mathcal{J}') = \text{proj}_n(\mathcal{J}) \) for all \( n \in \mathcal{N} \) and \((C4)\) for all \( v \in \mathcal{J}' \), \( v_i \in A_i \implies v_j \in A_j \).
Proof Suppose $i = j$. Substituting $j$ into $A_i$ shows $A_i = A_j$, and the conclusion is trivial.

Suppose instead $i \neq j$.

Let $\mathcal{J}_{\text{donor}}$ be the sub-multiset of all paths (and their multiplicities) in $\mathcal{J}$ whose $j$th components pass through $A_j$ but whose $i$th ones do not pass through $A_i$ and $\mathcal{J}_{\text{recipient}}$ the sub-multiset of all paths whose $i$th components pass through $A_i$ but whose $j$th ones do not pass through $A_j$. Then Condition (C4) is equivalent to the condition that all paths of $\mathcal{J}'$ whose $i$th component passes through $A_i$ are alive with respect to $\times_{n \in \mathbb{Z}^\succ 0, \{i,j\}}\{1, \ldots, p_i\} \times A_i \times A_j$. As for $\mathcal{J}$, each path in $\mathcal{J}_{\text{donor}}$ is a potential donor to each path in $\mathcal{J}_{\text{recipient}}$ (with the donations occurring in the $j$th components). Therefore, by Proposition 4, it suffices to show (C5) $\text{card}(\mathcal{J}_{\text{donor}}) \geq \text{card}(\mathcal{J}_{\text{recipient}})$. To invoke Condition (C2), observe

$$\text{card}(\text{proj}_j(\mathcal{J}) \cap A_j) = \text{card}(\mathcal{J}_{\text{recipient}}) + \text{card}\left(\mathcal{J} \cap \times_{n \in \mathbb{Z}^\succ 0, \{i,j\}}\{1, \ldots, p_i\} \times A_i \times A_j\right)$$

$$\text{card}(\text{proj}_j(\mathcal{J}) \cap A_i) = \text{card}(\mathcal{J}_{\text{donor}}) + \text{card}\left(\mathcal{J} \cap \times_{n \in \mathbb{Z}^\succ 0, \{i,j\}}\{1, \ldots, p_i\} \times A_i \times A_j\right),$$

which by plugging into Condition (C2) gives (C5).

\[\square\]

Remark: If $j = 1$, the proposition is trivial.

The point of Proposition 5 is its corollary:

Corollary 1 Fix arbitrary $N \in \mathbb{Z}^\succ 0$, $i, j \in \mathcal{N}$, and $\mathcal{J} \subseteq \times_{n \in \mathcal{N}}\{p_1, \ldots, p_N\}$ such that, for $n \in \{i,j\}$,

$$\text{proj}_n(\mathcal{J}) = \left\{1^{N/p_i}, \ldots, p_n^{N/p_n}\right\}.$$  \hspace{1cm} (Ct32)

Let $A_i$ and $B_j$ be ordinary sets that partition $\{1, \ldots, p_i\}$ and, similarly, $\{A_j, B_j\}$ a partition of $\{1, \ldots, p_j\};$
and suppose $\frac{\text{card}(A_i)}{\text{card}(B_j)} \leq \frac{\text{card}(A_j)}{\text{card}(B_j)}$. Then there exists $\mathcal{J}'$ such that (i) $\text{proj}_n(\mathcal{J}') = \text{proj}_n(\mathcal{J})$ for all $n \in \mathcal{N}$
and (ii) for all $v \in \mathcal{J}'$, $v_i \in A_i \implies v_j \in A_j$.

Proof Let $a_i := \text{card}(A_i)$.

$$\left(\frac{\text{card}(A_i)}{\text{card}(B_j)} \leq \frac{\text{card}(A_j)}{\text{card}(B_j)}\right) \iff \left(\frac{a_i}{\text{card}(\{1, \ldots, p_i\} \setminus A_i)} \leq \frac{\text{card}(A_j)}{\text{card}(\{1, \ldots, p_j\} \setminus A_j)}\right)$$

$$\iff \left(\frac{a_i}{p_i - a_i} \leq \frac{\text{card}(A_j)}{p_j - \text{card}(A_j)}\right)$$

$$\iff (a_ip_j - a_i\text{card}(A_j) \leq p_j\text{card}(A_j) - a_i\text{card}(A_j))$$

$$\iff (p_ja_i \leq p_i\text{card}(A_j)).$$

By Constraint Ct32, $\text{card}(A_j)N/p_j$ paths pass through, in their $j$th components, $A_j$, whereas only $a_iN/p_i \leq \frac{p_i}{p_j}\text{card}(A_j)N/p_j$ paths pass through, in their $i$th components, $A_i$. Thus Proposition 5 can be invoked.

The upshot of Corollary 1 is the following lemma.

Lemma 2 (Intersecting Products) Fix arbitrary $N \in \mathbb{Z}^\succ 0$ and partitions $(A_n, B_n)$ of $\{1, \ldots, p_n\}$ for $n = 1, \ldots, N$. Let $n^* \in \arg \min_{n \in \mathcal{N}} \frac{\text{card}(A_n)}{\text{card}(B_n)}$. Then there exists $\mathcal{J}$ satisfying Condition (C1) for which

$$\text{card}(\mathcal{J} \cap \times_{n \in \mathcal{N}}B_n) = \frac{N/p_{n^*}}{p_{n^*}} \text{card}(B_{n^*}).$$
Proof Start with any \( J \) satisfying Condition (C1), for example \( \times_{i=1}^{N} \{1, \ldots, p_i\} \). By construction of \( n_s \), Corollary 1 can be iteratively applied over all \( n \in \mathcal{N} \) path components, with \( i := n \) and \( j := n_s \).

Then, in the final \( J' \) for all \( n \in \mathcal{N} \), there are \( \frac{N_p}{p_n} \) card(\( B_n \)) paths passing through, in their \( n \)th components, \( B_n \) and, in the \( n_s \)th ones, \( B_{n_s} \). Moreover, every such path cannot pass through, in its \( n \)'th component, some \( A_{n'} \) by construction of \( J' \) (doing so would have to pass through, in the \( n_s \)th component, \( A_{n_s} \), a contradiction). Therefore, all of these paths are in \( \times_{n \in A} B_n \).

The following two corollaries give simpler approximations of Problem P15 than Theorem 3, and are collectively adequate, that is without further use of the theorem, for ascertaining the probability of \( \mathbb{N}_p \) and residue classes.

**Corollary 2 (Product)** Fix an arbitrary \( S \subseteq \mathbb{Z} \). Suppose, for all \( N \in \mathbb{Z}^{\geq 0} \) and \( \mathcal{I}_n \subseteq \mathbb{Z} \) (for all \( n \in \mathbb{Z}^{\geq 0} \)),

\[
S^{-1}(S \bmod N!_p) \supseteq \times_{n \in \mathcal{N}} \mathcal{I}_n. 
\] (A33)

Then

\[
\sup_{\mu \in \mathcal{P}(\mathbb{Z})} \mu(S) \geq \inf_{n \in \mathbb{Z}^{\geq 0}} \frac{\text{card}(\mathcal{I}_n)}{p_n}.
\]

**Proof** Combining Approximation A33 and Approximation A14 yields

\[
\sup_{\mu \in \mathcal{P}(\mathbb{Z})} \mu(S) \geq \lim_{N \to \infty} \max_{J \subseteq \mathcal{I}} \frac{\text{card}(J \cap \times_{n \in \mathcal{N}} \mathcal{I}_n)}{N!_p},
\]

which, by Lemma 2, is lower bounded by

\[
\lim_{N \to \infty} \min_{n \in \mathcal{N}} \frac{N!_n}{p_n} \frac{\text{card}(\mathcal{I}_n)}{N!_p} \geq \inf_{n \in \mathbb{Z}^{\geq 0}} \frac{\text{card}(\mathcal{I}_n)}{p_n}.
\]

\( \square \)

In the next corollary, the total number of paths that can be made to pass through \( \mathcal{I}_n \) in their \( n \)th components is once again the basis for bounding Problem P15, albeit this time such a bound cannot be further simplified. That is because \( S^{-1}(S \bmod N!_p) \) may no longer be well approximated by a product as it was in Approximation A33; instead it is approximated by a product \( \times_{n \in \mathcal{N}} \mathcal{I}_n \) minus another one, say \( \times_{n \in \mathcal{N}} \mathcal{K}_n \). Because of this complication, paths must be re-arranged more intricately to realize the maximum in Approximation A14. The ability to re-arrange enough paths to “make up for” the subtraction of \( \times_{n \in \mathcal{N}} \mathcal{K}_n \) depends on the relative sizes of the sets \( \mathcal{I}_n \) and \( \mathcal{K}_n \). (Namely, Approximation A35 below suffices.)

**Corollary 3 (Difference of Products)** Fix an arbitrary \( S \subseteq \mathbb{Z} \) and let for all \( n \in \mathcal{N} \) (recall Definition 7).

1. \( \mathcal{I}_n, \mathcal{K}_n \subseteq \mathbb{Z} \) 
2. \( \mathcal{K}_n := \mathcal{I}_n \setminus \mathcal{K}_n \), 
3. \( I_n := \text{card}(\mathcal{I}_n) \), 
4. \( K_n := \text{card}(\mathcal{K}_n) \), and 
5. \( H_n := \text{card}(\mathcal{H}_n) \).

Further, let \( N := \{k \in \mathcal{N} : \mathcal{K}_k \neq \emptyset\} \) and \( n := \text{card}(N) \); and, for all \( N \in \mathbb{Z}^{\geq 0} \), \( n \in \mathcal{N} \), \( m \in \mathbb{Z}^{\geq 0} \) and \( \{i_1, \ldots, i_m\} \subseteq \mathbb{Z}^{\geq 0} \), let \( N^{-1} := N \setminus \{i_1, \ldots, i_m\} \) and \( \mathcal{N}^{-1} := \mathcal{N} \setminus (\mathcal{N} \cup \{i_1, \ldots, i_m\}) \). Note \( \{i_1, \ldots, i_m, i_m, N^{-1}, \mathcal{N}^{-1}\} \) partitions \( \mathcal{N} \).

Suppose, for all \( N \in \mathbb{Z}^{\geq 0} \),

\[
S^{-1}(S \bmod N!_p) \supseteq \mathcal{I}^N, 
\] (A34)
in which \( \mathcal{J}^N := \times_{n \in \mathcal{N}} \mathcal{J}_n \setminus \times_{n \in \mathcal{N}} \mathcal{K}_n \) and
\[
\sum_{m=0}^{N_s-2} (N_s - 1 - m) \sum_{\{i_1, \ldots, i_m \} \subseteq \mathcal{N}_s} \left[ \prod_{n \in \{i_1, \ldots, i_m \} \setminus \mathcal{K}_n} \prod_{n \in \mathcal{N}_s \setminus \{i_1, \ldots, i_m \}} K_n \prod_{n \in \mathcal{N}_s \setminus \{i_1, \ldots, i_m \}} H_n \prod_{n \in \mathcal{N}_s - i} I_n \right] \geq \prod_{n \in \mathcal{N}_s} K_n. \tag{A35}
\]

Then
\[
\sup_{\mu \in \text{PR}} \mu(S) \geq \lim_{N \to \infty} \frac{\prod_{n \in \mathcal{N}_s} I_n}{N!^p}. \tag{A36}
\]

**Proof** Combining Approximations A34 and A14 yields
\[
\sup_{\mu \in \text{PR}} \mu(S) \geq \lim_{N \to \infty} \frac{\text{card}(\mathcal{J} \cap \mathcal{J}^N)}{N!^p}. \tag{A36}
\]

By definition of \( s^{-1}(A) \), for all \( n \in \mathcal{N} \), \( \mathcal{J}_n \) and \( \mathcal{K}_n \) are subsets of \( \{1, \ldots, p_n\} \). Hence, \( \times_{n \in \mathcal{N}} \{1, \ldots, p_n\} \) contains \( \bigcup_{m \in \{0, \ldots, N_s - 2\}, i_1 < \cdots < i_m} \mathcal{K}_n \times \times_{n \in \mathcal{N}_s \setminus \{i_1, \ldots, i_m\}} \mathcal{H}_n \times \times_{n \in \mathcal{N}_s \setminus \{i_1, \ldots, i_m\}} \mathcal{J}_n \) for any \( m \in \{0, \ldots, N_s - 2\} \) (in which \( \{0, \ldots, N_s - 2\} := \{0\}, i_1 < \cdots < i_m \), and \( n \in \mathcal{N}_s - i \). For example, if \( N = 2 \), \( \mathcal{J}_1 = 1 = \mathcal{K}_1 = \mathcal{H}_2 \), \( \mathcal{J}_2 = \{1, 2\} \), \( \mathcal{K}_2 = \{2\}, \mathcal{H}_1 = \{2\}, \mathcal{N}_s - 2 < 0 \), and \( k = (1, 1) \) is (dead and) can be enlivened by exchanging its second component with the same of \( (1, 2) \in \mathcal{J}_1 \times \mathcal{H}_2 \). In this simple case with no overlapping paths, the live and dead paths can be distinguished by thickness (or, alternatively, color) with thick denoting alive.

Returning to the general case, every such \( k \), could make \( N_s - 1 - m \) donations before another exchange would kill it or there were no more recipients in \( \times_{n \in \mathcal{N}_s} \mathcal{K}_n \), which would only be the case if every path therein had been enlivened. When inequality A35 is satisfied, the latter is possible. Beginning with \( \times_{n \in \mathcal{N}_s} \{1, \ldots, p_n\} \) and exhausting donations yields some \( \mathcal{J} \) satisfying Condition (C1). Because the foregoing procedure begins with \( \text{card}(I^N) \) lives and performs at least \( \prod_{n \in \mathcal{N}_s} K_n \) donations, \( \mathcal{J} \) satisfies
\[
\text{card}(\mathcal{J} \cap \mathcal{J}^N) \geq \prod_{n \in \mathcal{N}_s} \text{card}(\mathcal{J}_n). \tag{A37}
\]

Combining Approximations A37 and A36 concludes.

\( \square \)

### 4 Application to \( N_p \)

For an application of Theorem 3 or one of its corollaries (2 and 3) to a given \( S \), the approximation of \( s^{-1}(S \mod N!^p) \) for all \( N \) is fundamental. The following propositions concern the intersections of residue classes. When there is an infinite number of intersections, there is a simple characterization:

**Proposition 6 (Infinite Intersections)** Suppose 1. \( \mathcal{I} \) is a set, 2. for all \( i \in \mathcal{I} \), \( j_i, m_i \in \mathbb{Z}^{>0} \), and 3. \( \sup_{i \in \mathcal{I}} m_i = \infty \). Then
\[
\cap_{i \in \mathcal{I}} j_i \mod m_i \tag{38}
\]
can have at most one element \( s \), in which case, for all \( i \in \mathcal{I} \),
\[
j_i \mod m_i = s \mod m_i.
\]
Proof: The three suppositions guarantee Set 38 is well defined. The gaps between elements of (38) must be at least $m_i - 1$ for all $i \in \mathcal{I}$, implying the gaps must be arbitrarily close to $\sup_{i \in \mathcal{I}} m_i - 1 = \infty$, by Supposition 3. This excludes the possibility of multiple elements. One element, say $s$, is possible precisely when, for all $i \in \mathcal{I}$, $s \equiv j_i \mod m_i$. But for every given $i, s \equiv j_i \mod m_i$ if $j_i \mod m_i = s \mod m_i$. □

The following proposition examines the nature of individual residue classes within a non-empty intersection thereof.

Proposition 7 (Computation of Shift) Suppose

- $N \in \mathbb{Z}^{>0}$,
- $m_1, \cdots, m_N$ are co-prime,
- $s_1, \cdots, s_N$ are positive integers,
- $k \in \{1, \cdots, N\}$, and
- $m_k$ divides the shifts of $\cap_{i=1}^N s_i \mod m_i$.

Then $s_k \equiv 0 \mod m_k$.

Proof: By the Chinese Remainder Theorem, $\cap_{i=1}^N s_i \mod m_i$ is indeed a residue class.

Suppose the shifts of $\cap_{i=1}^N s_i \mod m_i$ are divisible by $m_k$. Then

$$(0 \mod m_k) \cap (\cap_{i=1}^N s_i \mod m_i) \neq \emptyset.$$ 

In particular, $(0 \mod m_k) \cap (s_k \mod m_k)$ is non-empty. Hence, $s_k \equiv 0 \mod m_k$. □

The point of Proposition 7 is its corollary:

Corollary 4 Suppose $s_1, \cdots, s_N$ are integers and for all $i \in \{1, \cdots, N\}$ $s_i \not\equiv 0 \mod p_i$. Then the shift and modulus of $\cap_{i=1}^N s_i \mod p_i$ are co-prime.

Proof: Suppose, contrarily, that the shift and modulus of $\cap_{i=1}^N s_i \mod p_i$ have a common divisor greater than 1, it is equal to $p_k$ for some $k \in \{1, \cdots, N\}$. Then the previous proposition gives $s_k \equiv 0 \mod p_k$. □

Finally a computation of $s^{-1}$:

Lemma 3 (Primes in the Intersection of Residue Classes) For all $N \in \mathbb{Z}^{>0}$,

$$s^{-1} (\mathbb{N}_p \mod N!_p) \supseteq \times_{n \in \mathcal{N}} \{1, \cdots, p_n - 1\}.$$ 

Proof: If, for all $n \in \mathcal{N}$, $j_n \in \{1, \cdots, p_n - 1\}$, then, by Corollary 4, the shift and modulus of $\cap_{i=1}^N s_i \mod p_i$ are co-prime. Hence, by Dirichlet’s theorem on the distribution of primes in residue classes, $\cap_{i=1}^N s_i \mod p_i \cap \mathbb{N}_p \neq \emptyset$. □

Theorem 4 (Probability Range of Primes) $\mu(\mathbb{N}_p) : \mu \in PR = [0, 1/2]$.

Proof: By Corollary 2, with Approximation A33 given by Lemma 3 and $\mathcal{I}_n := \{1, \cdots, p_n - 1\}$,

$$\sup_{\mu \in PR} \mu(S) \geq \inf_{i \in \mathbb{Z}^{>0}} \frac{\text{card}(\mathcal{I}_i)}{p_i} = \inf_{i \in \mathbb{Z}^{>0}} \frac{p_i - 1}{p_i} = \frac{1}{2},$$

with $i = 1$ attaining the infimum.

$\sup_{\mu \in PR} \mu(S) \leq 1/2$ by virtue of the primes inclusion in the odd numbers union $\{2\}$. Therefore the least upper bound is $1/2$. The greatest lower bound of 0 is the content of Proposition 2. □
5 Application to Residue Classes

Because the primes have zero mass under $R$ ([11]), we know a priori that there must be a residue class on which $PR$ and $R$ can disagree. It turns out the residue classes that have non-singleton bounds under $PR$ are those mod neither 1 nor a prime; that is all residue classes on which $PR$ was not initially defined!

The following two lemmas instantiate Approximations A33 and A34, respectively.

**Lemma 4 (Intersection of Residue Classes)** Let $r, m \in \mathbb{Z}^{>0}$ and $S := r \mod m$ be an arbitrary residue class. For all $n \in \mathbb{Z}^{>0}$, let $\mathcal{S}^S_n := \{1 : p_n\}$ if $p_n$ does not divide $m$ and $r \mod p_n \cap \{1 : p_n\}$ otherwise. For all $N \in \mathbb{Z}^{>0}$,

$$s^{-1}(S) \supseteq \times_{n \in N \cap \mathcal{S}^S_n}$$

**Proof** For all $j \in \times_{n \in N \cap \mathcal{S}^S_n}$,

$$\cap_{n \in N} j_\mod p_n \cap S = \cap_{n \in N : p_n | m} j_\mod p_n \cap \cap_{n \in N : p_n | m} j_\mod p_n \cap S$$

$$= \cap_{n \in N : p_n | m} r \mod p_n \cap \cap_{n \in N : p_n | m} j_\mod p_n \cap S$$

$$= \cap_{n \in N : p_n | m} j_\mod p_n \cap S,$$  \hspace{1cm} (39)

the last equality holds because $r \mod p_n \subseteq S$ for all $p_n$ dividing $m$. By the Chinese Remainder Theorem, set 39 is non-empty. □

**Lemma 5 (Intersecting a Residue Class Union)** Suppose $r, m \in \mathbb{Z}^{>0}$ is such that $m$ is made up of two (not necessarily unique) prime factors $m_1, m_2$. Let $S := \mathbb{Z} \setminus r \mod m$. For all $N \in \mathbb{Z}^{>0}$,

$$s^{-1}(S \mod N! p) \supseteq \times_{n \in N \cap \mathcal{S}^S_n} \{1 : p_n\} \setminus \left[\times_{n \in N \setminus \{i_1, i_2\}} \{1 : p_n\} \times \times_{n \in \{i_1, i_2\}} r \mod p_n\right],$$  \hspace{1cm} (A40)

in which $i_1$ and $i_2$ are such that $p_{i_1} = m_1$ and $p_{i_2} = m_2$.

If, further, $i_1 = i_2$,

$$s^{-1}(S \mod N! p) \supseteq \times_{n \in N \cap \mathcal{S}^S_n} \{1 : p_n\},$$  \hspace{1cm} (A41)

**Proof** Fix an element $j$ in the right-hand side

$$\left[\times_{n \in N \setminus \{i_1, i_2\}} \{1 : p_n\} \times \times_{n \in \{i_1, i_2\}} r \mod p_n\right]$$  \hspace{1cm} (42)

of Approximation A40. Then, if $i_1 \neq i_2$, for some $i_\in \{i_1, i_2\}$,

$$S_\i := j_\mod p_\i \subseteq S.$$  \hspace{1cm} (43)

In that case,

$$\cap_{n \in N \setminus \{i_1, i_2\}} j_\mod p_n \cap S = \cap_{n \in \{i_1, i_2\}} j_\mod p_n \cap \cap_{n \in N \setminus \{i_1, i_2\}} j_\mod p_n \cap S$$

$$= (S_\i \cap S) \cap \cap_{n \in \{i_1, i_2\}} j_\mod p_n \cap \cap_{n \in N \setminus \{i_1, i_2\}} j_\mod p_n$$

$$= \cap_{n \in \{i_1, i_2\}} j_\mod p_n \cap \cap_{n \in N \setminus \{i_1, i_2\}} j_\mod p_n,$$

the latter equality by Expression 43. In summary,

$$\cap_{n \in N \setminus \{i_1, i_2\}} j_\mod p_n \subseteq S$$  \hspace{1cm} (A44)

By the Chinese Remainder Theorem, the left-hand side of Approximation A44 is non-empty. In particular, $S \mod N! p \cap \cap_{n \in N \setminus \{i_1, i_2\}} j_\mod p_n \neq \emptyset$. Because $j$ was an arbitrary element of set 42, Approximation A40 holds.

If, instead, $r = m_1^2$ and $j$ in the right-hand side of Approximation A41, then Approximation A44 still holds. □
**Theorem 5 (Probability Range of Residue Class)** For every \( r \in \mathbb{Z} \) and \( m \in \mathbb{Z}^{>0} \setminus \{p_0, p_1, \cdots\} \),

\[
\{\mu \left( r \mod m \right) : \mu \in PR\} = \left[0, \frac{1}{\max\{p \in \mathbb{N}_p : p|m\}}\right].
\]

**Proof** With Approximation A33 given by Lemma 4 and \( \mathcal{I}_n := \mathcal{I}_n^S \), by Corollary 2,

\[
\sup_{\mu \in PR} \mu(S) \geq \inf_{n \in \mathbb{Z}^{>0}} \frac{\operatorname{card}(\mathcal{I}_n^S)}{p_n} = \inf_{n \in \mathbb{Z}^{>0}, p_n|m} \frac{1}{p_n} = \frac{1}{\max\{p \in \mathbb{N}_p : p|m\}}.
\]

For \( p_n \) dividing \( m \), \( \mu(S) \) can be no larger than the measure \( \mu \left( r \mod p_n \right) \) of a set containing it, so

\[
\sup_{\mu \in PR} \mu(S) = \frac{1}{\max\{p \in \mathbb{N}_p : p|m\}}.
\]

It remains to show merely

\[
\inf_{\mu \in PR} \mu(S) = 0. \tag{Id45}
\]

It suffices to consider \( m \) with at most two prime factors, as every residue class of a modulus with more prime factors is a subset of some class with two; and thus has probability at most that of the superset. Classes with one prime factor are defined. Therefore, it suffices to consider moduli with exactly two prime factors \( m_1 \) and \( m_2 \).

Since our theory is based on suprema rather than infima, consider the set complement \( S^c \), itself a union of residue classes. Claimed Identity Id45 is equivalent to \( \sup_{\mu \in PR} \mu(S^c) = 1 \), which in turn is equivalent to

\[
\sup_{\mu \in PR} \mu(S^c) \geq 1 \tag{A46}
\]

by definition of finitely additive probability.

If \( m_1 = m_2 \), then by Corollary 2, with Approximation A33 given by Approximation A41 and \( \mathcal{I}_n := \{1, \cdots, p_n\} \),

\[
\sup_{\mu \in PR} \mu(S^c) \geq \inf_{n \in \mathbb{Z}^{>0}} \frac{\operatorname{card}(\{1, \cdots, p_n\})}{p_n} = \inf_{n \in \mathbb{Z}^{>0}} \frac{p_n}{p_n} = 1.
\]

Now consider \( m_1 \neq m_2 \). Fix \( N \in \mathbb{Z}^{>0} \). Let, for all \( n \in N \), \( \mathcal{I}_n := \{1 : p_n\} \) and

\[
\mathcal{K}_n := \left\{ \begin{array}{ll}
\{1 : p_n\} & n \in N \setminus \{i_1, i_2\} \\
 r \mod p_n \setminus \{1 : p_n\} & n \in \{i_1, i_2\}
\end{array} \right.,
\]

in which \( i_1 \) and \( i_2 \) are such that \( p_{i_1} = m_1 \) and \( p_{i_2} = m_2 \). (Compare to the setup of Lemma 5.) Then

\[
\operatorname{card}(\mathcal{K}_n) = \begin{cases}
\operatorname{card}(\mathcal{I}_n) & n \in N \setminus \{i_1, i_2\} \\
1 & n \in \{i_1, i_2\}
\end{cases} \tag{Id47}
\]

and \( N := \{n \in N : \mathcal{I}_n \setminus \mathcal{K}_n \neq \emptyset\} = \{i_1, i_2\} \). Plugging \( N_\ast = \operatorname{card}(\{i_1, i_2\}) = 2 \) into the left-hand side of A35 yields

\[
\sum_{m=0}^0 (2 - 1 - m) \sum_{\{i_1, \cdots, i_m\} \subseteq N \setminus \{i_1, i_2\}} \left[ \prod_{n \in \emptyset} \mathcal{K}_n \prod_{n \in N \setminus N_\ast} \operatorname{card}(\mathcal{I}_n \setminus \mathcal{K}_n) \prod_{n \in N \setminus N_\ast} \operatorname{card}(\mathcal{I}_n) \right] = \prod_{n \in N_\ast} \operatorname{card}(\mathcal{I}_n \setminus \mathcal{K}_n) \prod_{n \in N \setminus N_\ast} \operatorname{card}(\mathcal{I}_n),
\]
matching Identity Id47 and thereby satisfying inequality A35.

Therefore, with Approximation A34 given by (i) Approximation A40 of Lemma 5 and (ii) \( S' \) in place of \( S \), by Corollary 3,

\[
\sup_{\mu \in PR} \mu(S) \geq \lim_{N \to \infty} \frac{\prod_{n \in \mathbb{N}} \text{card}(\mathcal{I}_n)}{N!^p} = \lim_{N \to \infty} \frac{\prod_{n \in \mathbb{N}} p_n}{N!^p} = 1
\]

which, in turn, gives Approximation A46, all that remained to prove. \( \square \)

Remark: The proof of the lower bound in the case \( m = p^2 \) for some prime \( p \) could have appealed to Corollary 2 rather than 3, but the former has more conditions to check.

6 Conclusion

\( PR \) is a distinct family of uniform finitely additive probabilities over \( \mathbb{Z} \). From the strict inclusions

\[
WT \subset L \subset S \subset R \subset PR,
\]

we have shown the last. We have given necessary and sufficient conditions for there to exist a probability charge in \( PR \) assigning \( w \) to \( \mathbb{N}_p \), namely \( w \in [0, 1/2] \). We have also given necessary and sufficient conditions for the existence of a probability charge in \( PR \) assigning \( x \) to a class modulo \( c \), where \( c \) is composite, namely \( x \in [0, 1/y] \), where \( y \) is the largest prime factor of \( c \).

References

1. J.B. Kadane, A. O’Hagan, Using finitely additive probability: Uniform distributions on the natural numbers, Journal of the American Statistical Association 90, 626 (1995)
2. O. Schirokauer, J.B. Kadane, Uniform distributions on the natural numbers, Journal of Theoretical Probability 20(3), 429 (2007)
3. E.K. van Douwen, Finitely additive measures on \( \mathbb{N} \), Topology and its Applications 47(3), 223 (1992)
4. T. Kerkvliet, R. Meester, Uniquely determined uniform probability on the natural numbers, Journal of Theoretical Probability 29(3), 797 (2016)