The fundamental theorem of arithmetic for metric measures spaces

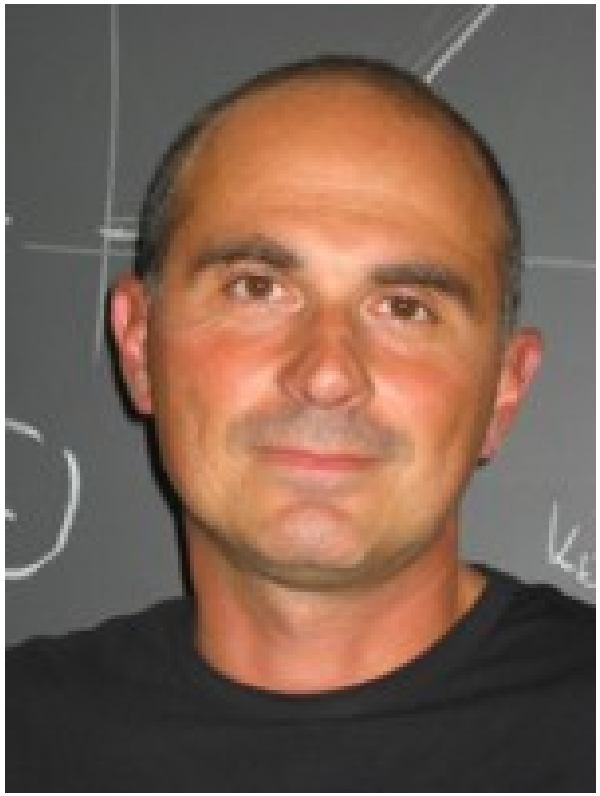
Steven N. Evans

Department of Mathematics & Department of Statistics
Group in Computational and Genomic Biology
Group in Computational Science and Engineering
University of California at Berkeley

September, 2014

Collaborator

Ilya Molchanov
Bern



Cartesian product

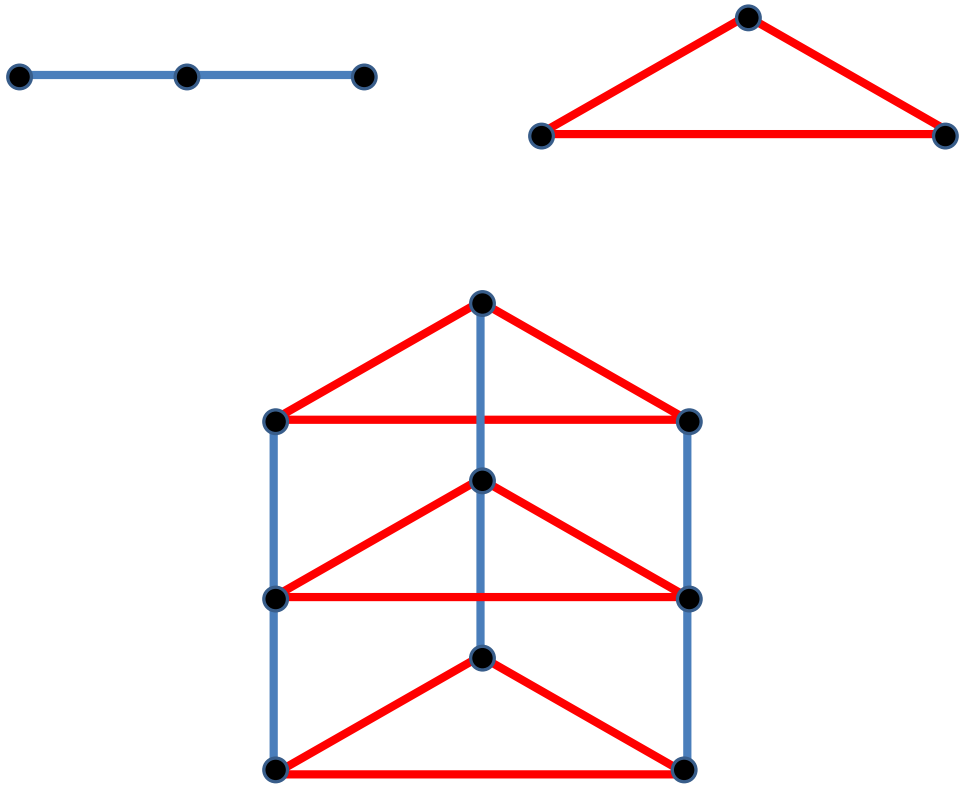


Figure: The Cartesian product of two graphs.

Cartesian product

- Formally, the Cartesian product $G \square H$ of two graphs G and H with vertex sets $V(G)$ and $V(H)$ and edge sets $E(G)$ and $E(H)$ is the graph with vertex set $V(G \square H) := V(G) \times V(H)$ and edge set

$$E(G \square H) := \{((g', h), (g'', h)) : (g', g'') \in E(G),\ h \in V(H)\} \cup \{((g, h'), (g, h'')) : g \in V(G),\ (h', h'') \in E(H)\}.$$

- This operation is commutative and associative with the trivial graph as identity element if we treat isomorphic graphs as being equal.

Cartesian product

- A nontrivial graph is irreducible if it is not the Cartesian product of two nontrivial graphs.
- Sabidussi (1960) showed that any finite graph is a Cartesian product of irreducible graphs and the factorization is unique up to order.
- Factoring graphs and, more generally, embedding them in Cartesian products is widely studied in computer science following Graham and Winkler (1984, 1985).

Shortest path metric

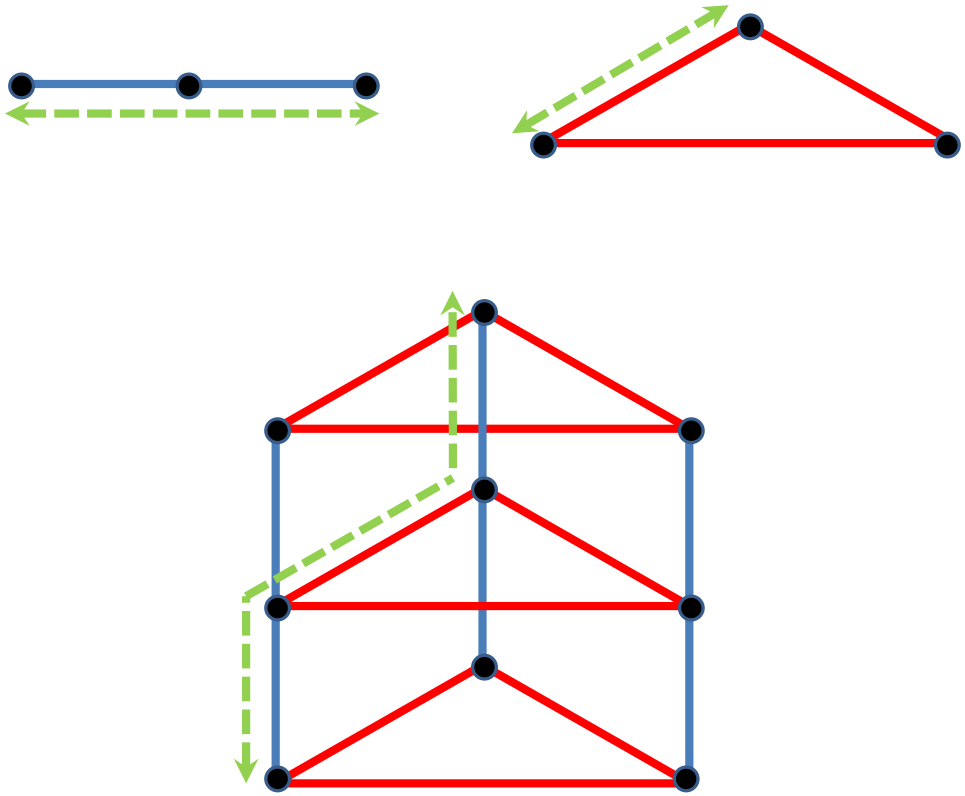


Figure: A shortest path between two points in the Cartesian product of two graphs.

Shortest path metric

- If two connected finite graphs G and H are equipped with the shortest path metrics r_G and r_H, then the shortest path metric on the Cartesian product is given by $r_{G\times H} = r_G \oplus r_H$, where

$$(r_G \oplus r_H)((g', h'), (g'', h'')) := r_G(g', g'') + r_H(h', h''),$$
$$(g', h'), (g'', h'') \in G \times H.$$

- What happens if we extend this binary operation to more general metric spaces?

Digression: Ulam's problem

- Ulam constructed a metric on the Cartesian product of two metric spaces (Y, r_Y) and (Z, r_Z) via $((y', z'), (y'', z'')) \mapsto \sqrt{r_Y(y', y'')^2 + r_Z(z', z'')^2}$ and asked: Is it possible that there could be two non-isometric metric spaces U and V such that the metrics spaces $U \times U$ and $V \times V$ are isometric?
- An example of two such spaces was given by Fournier (1971).
- Such an example is not possible if U and V are compact subsets of Euclidean space – Gruber (1971) & Moszyńska (1990).

Digression: Cancellativity

- Ulam's problem is closely related to the question of cancellativity for this binary operation: If $Y \times Z'$ and $Y \times Z''$ are isometric, then are Z' and Z'' isometric?
- Cancellativity does not hold in general; for example, $\ell^2(\mathbb{N}) \times \ell^2(\mathbb{N})$ and $\ell^2(\mathbb{N})$ are isometric, but $\ell^2(\mathbb{N})$ and the trivial metric space are not isometric.
- Cancellativity does not even hold for arbitrary subsets of $\mathbb{R}$ – Herburt (1994).
- There are compact Hausdorff topological spaces K with the property that if L' and L'' are two compact Hausdorff spaces such that $K \times L'$ and $K \times L''$ are homeomorphic, then L' and L'' are homeomorphic – Behrends and Pelant (1995).

Back to "our" binary operation

- Recall that we combine two metric spaces (Y, r_Y) and (Z, r_Z) into the metric space $(Y \times Z, r_Y \oplus r_Z)$.
- If a compact metric space is isometric to a product of finitely many compact irreducible metric spaces, then this factorization is unique up to the order of the factors – Tardif (1992).
- Proof uses results on median algebras, Chebyshev sets, gated spaces from Isbell (1980), Helíková (1983), Dress & Scharlau (1987).
- There are certainly compact metric spaces that are not isometric to a finite product of finitely many irreducible compact metric spaces.
- Are there (unique) factorizations using some sort of infinite product? What does this mean?
- The study of this binary operation seems to be generally rather difficult.

Metric measure spaces

- A metric measure space is just a complete separable metric space (X, r_X) equipped with a probability measure μ_X that has full support.
- Two such spaces are equivalent if they are isometric as metric spaces via an isometry that maps the probability measure on the first space to the probability measure on the second.
- Denote by $\mathbb{M}$ the set of such equivalence classes.
- We do not distinguish between an equivalence class $\mathcal{X} \in \mathbb{M}$ and a representative triple (X, r_X, μ_X).

When are two metric measures spaces equivalent?

- Gromov and Vershik showed that a metric measure space (X, r_X, μ_X) is uniquely determined by the probability distribution of the infinite random matrix of distances

$$(d(\xi_i, \xi_j))_{(i,j)\in\mathbb{N}\times\mathbb{N}},$$

  where $(\xi_k)_{k\in\mathbb{N}}$ is an i.i.d. sample of points in X with common probability distribution μ_X.
- This concise condition for equivalence makes metric measure spaces considerably easier to study than complete separable metric spaces *per se*.

A binary operation

- Given two elements $\mathcal{Y} = (Y, r_Y, \mu_Y)$ and $\mathcal{Z} = (Z, r_Z, \mu_Z)$ of $\mathbb{M}$, let $\mathcal{Y} \boxplus \mathcal{Z}$ be $\mathcal{X} = (X, r_X, \mu_X) \in \mathbb{M}$, where
  - $X := Y \times Z$,
  - $r_X := r_Y \oplus r_Z$, where $(r_Y \oplus r_Z)((y', z'), (y'', z'')) = r_Y(y', y'') + r_Z(z', z'')$ for $(y', z'), (y'', z'') \in Y \times Z$),
  - $\mu_X := \mu_Y \otimes \mu_Z$.
- This binary operation is associative and commutative.
- The isometry class of metric measure spaces $\mathcal{E}$ that each consist of a single point with the only possible metric and probability measure on them is the identity element.
- Thus $(\mathbb{M}, \boxplus)$ is a commutative semigroup with an identity (i.e. a monoid).

To paraphrase T.W. Körner

"The ease with which we proved [the central limit] explains why Fourier analysis plays a rôle in probability theory that in other branches of mathematics is played by thought."

Semicharacters

- A semicharacter is a map $\chi : \mathbb{M} \to [0,1]$ such that $\chi(\mathcal{Y} \boxplus \mathcal{Z}) = \chi(\mathcal{Y})\chi(\mathcal{Z})$ for all $\mathcal{Y}, \mathcal{Z} \in \mathbb{M}$.
- Denote by $\mathbb{A}$ the family of arrays of the form $A = (a_{ij})_{1 \leqslant i < j \leqslant n} \in \mathbb{R}_+^{\binom{n}{2}}$ for $n \in \mathbb{N}$.
- For each $A \in \mathbb{A}$ define a semicharacter χ_A by

$$\chi_A((X, r_X, \mu_X)) := \int_{X^n} \exp\left(- \sum_{1 \leqslant i < j \leqslant n} a_{ij} r_X(x_i, x_j) \right) \mu_X^{\otimes n}(dx).$$

- Two elements $\mathcal{X}, \mathcal{Y} \in \mathbb{M}$ are equal if and only if $\chi_A(\mathcal{X}) = \chi_A(\mathcal{Y})$ for all $A \in \mathbb{A}$.

Putting a metric on $\mathbb{M}$

- Equip $\mathbb{M}$ with the Gromov-Prohorov metric of Greven, Pfaffelhuber & Winter (2009). Two elements of $\mathbb{M}$ are close if their random distance matrices are close in distribution.
- The space $(\mathbb{M}, d_{\mathrm{GPr}})$ is complete and separable.
- $d_{\mathrm{GPr}}(\mathcal{X}_1 \boxplus \mathcal{X}_2, \mathcal{Y}_1 \boxplus \mathcal{Y}_2) \leqslant d_{\mathrm{GPr}}(\mathcal{X}_1, \mathcal{Y}_1) + d_{\mathrm{GPr}}(\mathcal{X}_2, \mathcal{Y}_2)$ and so $(\mathcal{X}, \mathcal{Y}) \mapsto \mathcal{X} \boxplus \mathcal{Y}$ is continuous.
- $\lim_{n\to\infty} \mathcal{X}_n = \mathcal{X}$ if and only if $\lim_{n\to\infty} \chi_A(\mathcal{X}_n) = \chi_A(\mathcal{X})$ for all $A \in \mathbb{A}$.

Putting a partial order on $\mathbb{M}$

- Define a partial order $\preccurlyeq$ on $\mathbb{M}$ by declaring that $\mathcal{Y} \preccurlyeq \mathcal{Z}$ if $\mathcal{Z} = \mathcal{Y} \boxplus \mathcal{X}$ for some $\mathcal{X} \in \mathbb{M}$.
- For any $\mathcal{Z} \in \mathbb{M}$, the set $\{\mathcal{Y} \in \mathbb{M} : \mathcal{Y} \preccurlyeq \mathcal{Z}\}$ is compact.

Cancellativity

- The commutative semigroup $(\mathbb{M}, \boxplus)$ is cancellative; that is, if $\mathcal{X}, \mathcal{Y}, \mathcal{Z}', \mathcal{Z}'' \in \mathbb{M}$ satisfy

$$\mathcal{X} = \mathcal{Y} \boxplus \mathcal{Z}'$$

and

$$\mathcal{X} = \mathcal{Y} \boxplus \mathcal{Z}'',$$

then

$$\mathcal{Z}' = \mathcal{Z}''.$$

Measuring the size of a metric measure space

- Put $D_A(\mathcal{X}) := -\log \chi_A(\mathcal{X})$ and

$$D(\mathcal{X}) := D_1(\mathcal{X}) = -\log \chi_1(\mathcal{X}) = -\log \int_{X^2} \exp\left(-r_X(x_1, x_2)\right) \mu_X^{\otimes 2}(dx).$$

- Put

$$R(\mathcal{X}) := \int_{X^2} \left(r_X(x_1, x_2) \wedge 1\right) \mu_X^{\otimes 2}(dx).$$

- For suitable constants, $aD(\mathcal{X}) \leqslant D_A(\mathcal{X}) \leqslant bD(\mathcal{X})$.
- $\frac{1}{4} R(\mathcal{X}) \leqslant d_{\mathrm{GPr}}(\mathcal{X}, \mathcal{E}) \leqslant \sqrt{R(\mathcal{X})}$.
- For suitable constants, $\alpha(D(\mathcal{X}) \wedge 1) \leqslant R(\mathcal{X}) \leqslant \beta(D(\mathcal{X}) \wedge 1)$.

Convergence of sums

- Suppose that $(\mathcal{X}_n)_{n\in\mathbb{N}}$ is a sequence such that $\lim_{n\to\infty} \mathcal{X}_0 \boxplus \cdots \boxplus \mathcal{X}_n = \mathcal{Y}$ for some $\mathcal{Y} \in \mathbb{M}$. If $(\mathcal{X}'_n)_{n\in\mathbb{N}}$ is a sequence that is obtained by re-ordering the sequence $(\mathcal{X}_n)_{n\in\mathbb{N}}$, then $\lim_{n\to\infty} \mathcal{X}'_0 \boxplus \cdots \boxplus \mathcal{X}'_n = \mathcal{Y}$ also.
- The limit $\lim_{n\to\infty} \mathcal{X}_0 \boxplus \cdots \boxplus \mathcal{X}_n$ exists if and only if $\sum_n D(\mathcal{X}_n) < \infty$ (equivalently, $\sum_n R(\mathcal{X}_n) < \infty$).
- So, we can make sense of $\boxplus_{s\in S} \mathcal{X}_s$ for any family $(\mathcal{X})_{s\in S}$ without specifying the "order of summation".

Irreducible elements

- An element $\mathcal{X} \in \mathbb{M}$ is irreducible if $\mathcal{X} \neq \mathcal{E}$ and $\mathcal{Y} \leqslant \mathcal{X}$ for $\mathcal{Y} \in \mathbb{M}$ implies that $\mathcal{Y}$ is either $\mathcal{E}$ or $\mathcal{X}$.
- It is not clear *a priori* that there are irreducible elements. For example, the semigroup $\mathbb{R}_+$ with the usual addition operation no irreducible elements in the analogous sense.
- If $\mathcal{X} \in \mathbb{M} \backslash \{\mathcal{E}\}$, then there is an irreducible element $\mathcal{Y} \in \mathbb{M}$ with $\mathcal{Y} \leqslant \mathcal{X}$ – this seems to be not at all obvious.
- Also, the irreducible elements are a dense G_δ subset of $\mathbb{M}$.

Prime elements

- An element $\mathcal{X} \in \mathbb{M}$ is prime if $\mathcal{X} \neq \mathcal{E}$ and $\mathcal{X} \leqslant \mathcal{Y} \boxplus \mathcal{Z}$ for $\mathcal{Y}, \mathcal{Z} \in \mathbb{M}$ implies that $\mathcal{X} \leqslant \mathcal{Y}$ or $\mathcal{X} \leqslant \mathcal{Z}$.
- Prime elements are clearly irreducible, but the converse is not *a priori* true. There are commutative, cancellative semigroups where the analogue of the converse is false.
- All irreducible elements of $\mathbb{M}$ are prime.
- The analogous result for the integers is the key to proving the fundamental theorem of arithmetic and the usual proof uses Euclid's algorithm.

Prime factorization – the "fundamental theorem of arithmetic"

- Given any $\mathcal{X} \in \mathbb{M} \backslash \{\mathcal{E}\}$, there is either a finite sequence $(\mathcal{X}_n)_{n=0}^N$ or an infinite sequence $(\mathcal{X}_n)_{n=0}^\infty$ of irreducible elements of $\mathbb{M}$ such that $\mathcal{X} = \mathcal{X}_0 \boxplus \cdots \boxplus \mathcal{X}_N$ in the first case and $\mathcal{X} = \lim_{n\to\infty} \mathcal{X}_0 \boxplus \cdots \boxplus \mathcal{X}_n$ in the second.
- The sequence is unique up to the order of its terms.
- Each irreducible element appears a finite number of times, so the representation is specified by the irreducible elements that appear and their finite multiplicities.
- It follows that $(\mathbb{M}, \preccurlyeq)$ is a distributive lattice: there is an analogue of the greatest common divisor (meet) and the least common multiple (join).

No nonconstant nondecreasing continuous functions

- If $\Phi : \mathbb{R}_+ \to \mathbb{M}$ is a continuous function such that $\Phi(0) = \mathcal{E}$ and

$$\Phi(s) \leqslant \Phi(t), \quad 0 \leqslant s \leqslant t < \infty,$$

  then $\Phi \equiv \mathcal{E}$.
- If $\Phi : \mathbb{R}_+ \to \mathbb{M}$ is a function such that $\Phi(0) = \mathcal{E}$ and

$$\Phi(s+t) = \Phi(s) \boxplus \Phi(t), \quad 0 \leqslant s, t < \infty,$$

  then $\Phi \equiv \mathcal{E}$.

Infinitely divisible random elements – Lévy-Hiňcin-Itô

- A random element $\mathbf{Y}$ of $\mathbb{M}$ is infinitely divisible if for each positive integer n there are i.i.d. random elements $\mathbf{Y}_{n1}, \ldots, \mathbf{Y}_{nn}$ such that $\mathbf{Y}$ has the same distribution as $\mathbf{Y}_{n1} \boxplus \cdots \boxplus \mathbf{Y}_{nn}$.
- An infinitely divisible random element $\mathcal{Y}$ has the same distribution as

$$\boxplus \{\mathcal{X} : (t, \mathcal{X}) \in \Pi\},$$

where Π is a Poisson point process on $[0,1] \times (\mathbb{M} \backslash \{\mathcal{E}\})$ with intensity of the form $\lambda \otimes \nu$, where λ is Lebesgue measure and and ν is a σ-finite measure on $\mathbb{M} \backslash \{\mathcal{E}\}$ such that

$$\int D(\mathcal{X}) \wedge 1 \, \nu(d\mathcal{X}) < \infty.$$

- Conversely, any such measure ν corresponds to an infinitely divisible random element in this way.
- Constants are not infinitely divisible and there is no analogue of the Gaussian distribution.

Scaling

- Given $\mathcal{X} \in \mathbb{M}$ and $a > 0$, set $a\mathcal{X} := (X, ar_X, \mu_X) \in \mathbb{M}$.
- This scaling operation operation is continuous and satisfies

$$a(\mathcal{X} \boxplus \mathcal{Y}) = (a\mathcal{X}) \boxplus (a\mathcal{Y}).$$

- If

$$(a\mathcal{X}) \boxplus (b\mathcal{X}) = c\mathcal{X}$$

for some $\mathcal{X} \in \mathbb{M}$ and $a, b, c > 0$, then $\mathcal{X} = \mathcal{E}$, so the second distributivity law certainly does not hold.

Stable random elements – "LePage" representations

- A $\mathbb{M}$-valued random element $\mathbf{Y}$ is stable with index $\alpha > 0$ if for any $a, b > 0$ the random element

$$(a+b)^{\frac{1}{\alpha}} \mathbf{Y}$$

has the same distribution as

$$a^{\frac{1}{\alpha}} \mathbf{Y}' \boxplus b^{\frac{1}{\alpha}} \mathbf{Y}''.$$

- A stable random element is necessarily infinitely divisible.
- The index must satisfy $0 < \alpha < 1$.
- An α-stable random element has the same distribution as

$$\bigboxplus_{n \in \mathbb{N}} \Gamma_n^{-\frac{1}{\alpha}} \mathbf{Z}_n,$$

where $(\Gamma_n)_{n \in \mathbb{N}}$ is the sequence of successive arrivals of a homogeneous unit intensity Poisson point process on $\mathbb{R}_+$ and $(\mathbf{Z}_n)_{n \in \mathbb{N}}$ is a sequence of i.i.d. random elements of $\mathbb{M}$.

Future directions

- Cancellativity allows us to embed the semigroup $\mathbb{M}$ into a group – analogous to passing from $\mathbb{N}$ to $\mathbb{Z}$.
- Are there analogues of objects such as Gaussian random variables in this world?
- Rieffel has shown that one can obtain a "quantum" analogue of the space of compact metric spaces equipped with the Gromov–Hausdorff distance by considering C^*-algebras with properties that generalize those of the algebra of Lipschitz functions on a compact metric space. Is there a similar "quantization" for metric measure spaces? Ongoing work with Benson Au.