What is a bijective proof?

A circuit complexity approach

Greg Kuperberg

UC Davis

June 29, 2024

In (languid) preparation

The ideas of this talk

- A combinatorial set $X \subset (\mathbb{Z}/2)^m$ is one with a membership predicate $p : (\mathbb{Z}/2)^m \to \{\text{yes}, \text{no}\}$, computed by a polynomial-sized circuit P.
- An efficient bijection $f : X \to Y$ is one where f and $g = f^{-1}$ have polynomial-sized circuits F and G, which yield a reversible circuit R.
- An efficient circuit homotopy $P \sim P'$ between two circuits for the same $p : (\mathbb{Z}/2)^m \to \{\text{yes}, \text{no}\}$ is a polynomial sequence of local moves that turn P into P'.
- A bijective proof that $|X| = |Y|$ is an efficient bijection $f : X \to Y$ and an efficient homotopy $P_X \sim P_Y \circ R$.

...versus other people's good ideas

Our circuit-based definitions are meant as one draft version of a rigorous definition of a bijective proof, and as its own topic inspired by bijective proofs.

Feldman and Propp, "Producing new bijections from old" and Conway and Doyle, "Division by three" both consider canonical bijections and the axiom of choice. Theirs is very interesting work in combinatorial set theory, but a canonical bijection need not be efficient, nor vice versa.

Garsia and Milne, "A Rogers–Ramanujan bijection" has within it a canonical bijection for enumerative subtraction. It is not efficient, and I suspect that an efficient bijection does not always exist.

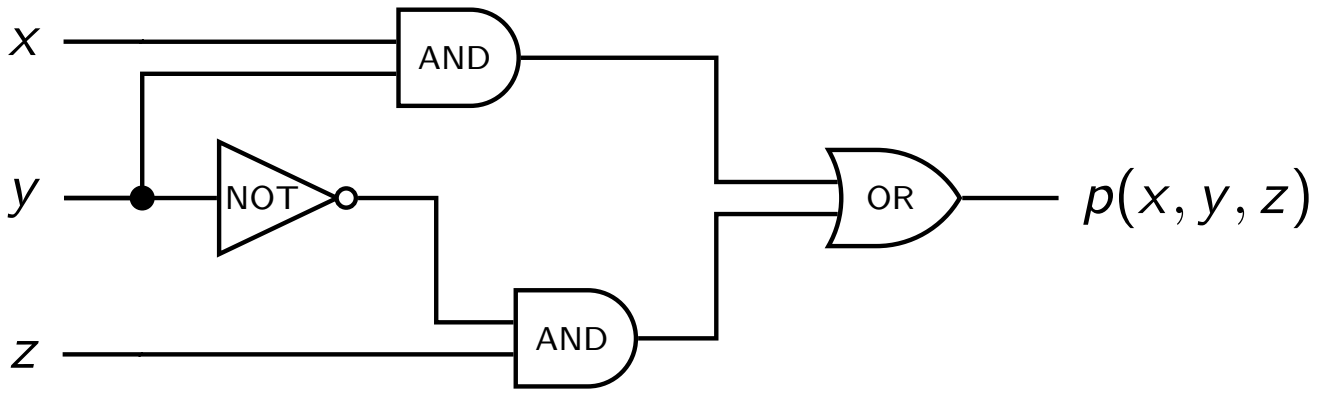
Defining combinatorial objects

Many combinatorial objects can be described by poly(n) bits of data, where n is an integer parameter. We can also often check the validity of examples with a predicate $p \in \mathsf{P}$, deterministic polynomial time. ("We know one when we see one".)

Objects that fit this scheme: subsets of $[n]$, graphs on n vertices, simplicial complexes with n simplices, $n \times n$ alternating-sign matrices, permutations, Young tableaux, spanning trees, perfect matchings, triangulations of a convex polygon, polyomino tilings, etc.

Objects that might not fit this scheme: infinite graphs, functions $f : (\mathbb{Z}/2)^n \to \mathbb{Z}/2$, knot diagrams up to Reidemeister moves.

Everything is a Boolean circuit



Theorem Boolean circuits are universal templates for combinatorial objects; bit strings that satisfy them are the examples.

An algorithm $p \in \mathsf{P}$ to test membership in $X \subseteq (\mathbb{Z}/2)^{\mathrm{poly}(n)}$ yields a poly(n)-sized Boolean circuit P. We can make the circuit the object specification. (*E.g.*, we can equate "$n \times n$ ASMs" with "a circuit to check whether the input is an $n \times n$ ASM".)

Efficient bijections

Given $X \subseteq (\mathbb{Z}/2)^m$ and $Y \subseteq (\mathbb{Z}/2)^k$ with $m, k = \text{poly}(n)$ and $|X| = |Y|$, we want an efficient bijection. Precisely, we want to express

$$f : X \to Y \qquad g = f^{-1} : Y \to X$$

with $\text{poly}(n)$ circuits

$$F, G : (\mathbb{Z}/2)^\ell \to (\mathbb{Z}/2)^\ell,$$

whence we write $X \cong_{\mathsf{e}} Y$. Given the predicate circuits

$$P, Q : (\mathbb{Z}/2)^m \to \{\text{yes}, \text{no}\}$$

for X and Y, $Q \circ F \sim P$ is an alternate predicate for X and $P \circ G \sim Q$ is an alternate predicate for Y. Note: Such an alternate predicate is the same function, but a different circuit.

Reversible circuits

A reversible circuit is a circuit whose gates are permutations of $(\mathbb{Z}/2)^k$ rather than Boolean functions. The NOT and Toffoli gates,

$$N(a) = a + 1 \qquad T(a, b, c) = (a, b, c + ab),$$

are universal. We can expand any circuit F for a function f into a reversible circuit E_F with the aid of ancilla bits, initially all 0. For example,

$$A(a, b) = ab \qquad \text{becomes} \qquad T(a, b, 0) = (a, b, ab).$$

The output of such an E has three parts,

$$E_F(\vec{x}, \vec{0}, \vec{0}) = (\vec{x}, s(\vec{x}), f(\vec{x})),$$

where $s(\vec{x})$ is scratch work. This can be improved.

Clean reversible circuits

Theorem

1. A function $f : X \to Y$ with a circuit F yields a reversible circuit R_F such that $|R_F| = \text{poly}(|F|)$ and

$$R_F(\vec{x}, \vec{0}, \vec{0}) = (\vec{x}, \vec{0}, f(\vec{x})).$$

2. If $f : X \to Y$ and $g : Y \to X$ are inverses with circuits F and G, then they yield a reversible circuit $R_{F,G}$ such that $|R_{F,G}| = \text{poly}(|F|, |G|)$ and

$$R_{F,G}(\vec{x}, \vec{0}, \vec{0}) = (\vec{0}, \vec{0}, f(\vec{x})) \qquad R^{-1}_{F,G}(\vec{0}, \vec{0}, \vec{y}) = (g(\vec{y}), \vec{0}, \vec{0})$$

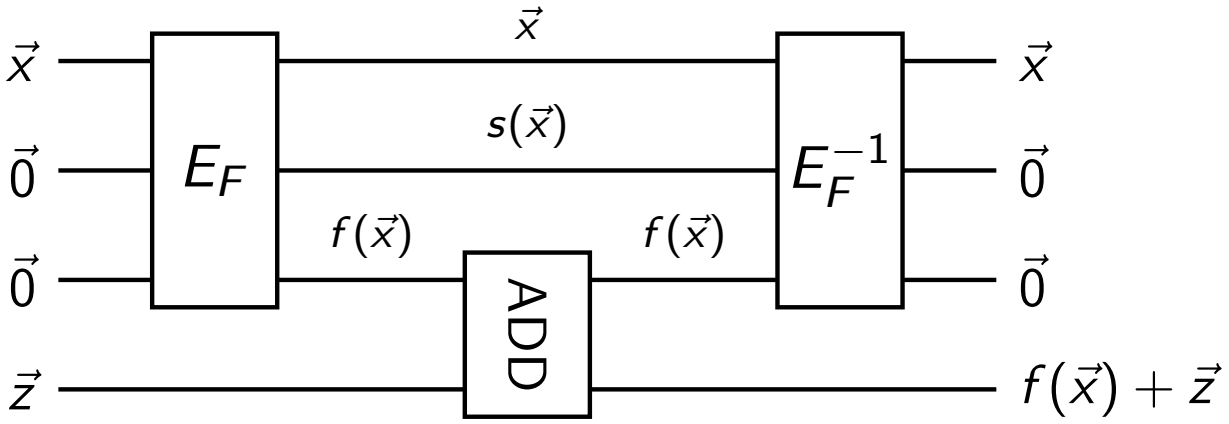
when $\vec{x} \in X$ and $\vec{y} \in Y$.

Warning: Part 2 assumes that f has an inverse $g = f^{-1}$, so this result must be used carefully in bijective proofs.

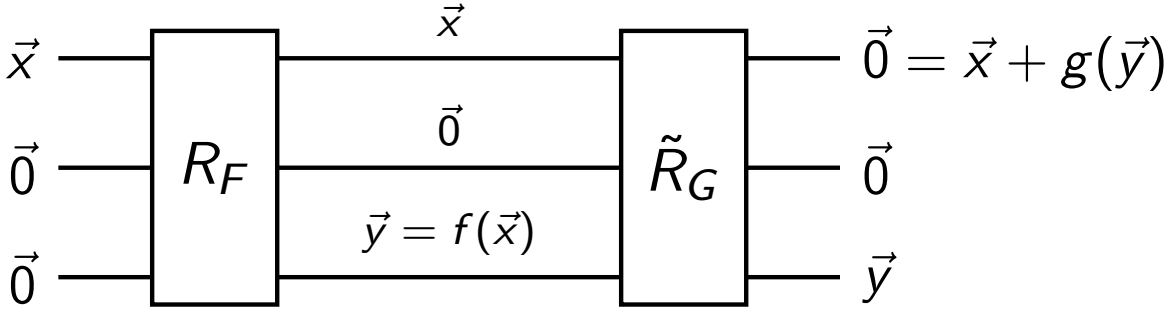
Uncomputation

The construction of R_F and $R_{F,G}$ uses uncomputation:

$R_F =$



$R_{F,G} =$



Circuit homotopy

The category set_2 of functions $f : (\mathbb{Z}/2)^m \to (\mathbb{Z}/2)^k$ is finitely presented (as a tensor category) by Boolean operators and Boolean laws. We choose some finite presentation.

Definition A circuit homotopy H between two Boolean circuits $F \sim G : (\mathbb{Z}/2)^m \to (\mathbb{Z}/2)^k$ is a sequence

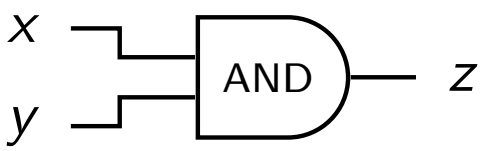
$$F = H_0, H_1, H_2, \ldots, H_\ell = G$$

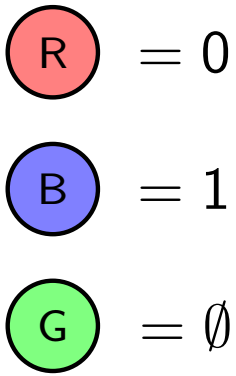
given by relations in set_2 that change F to G. If $\ell = \mathrm{poly}(n)$ for a parameter n, then H is an efficient homotopy, or $F \sim_{\mathsf{e}} G$.

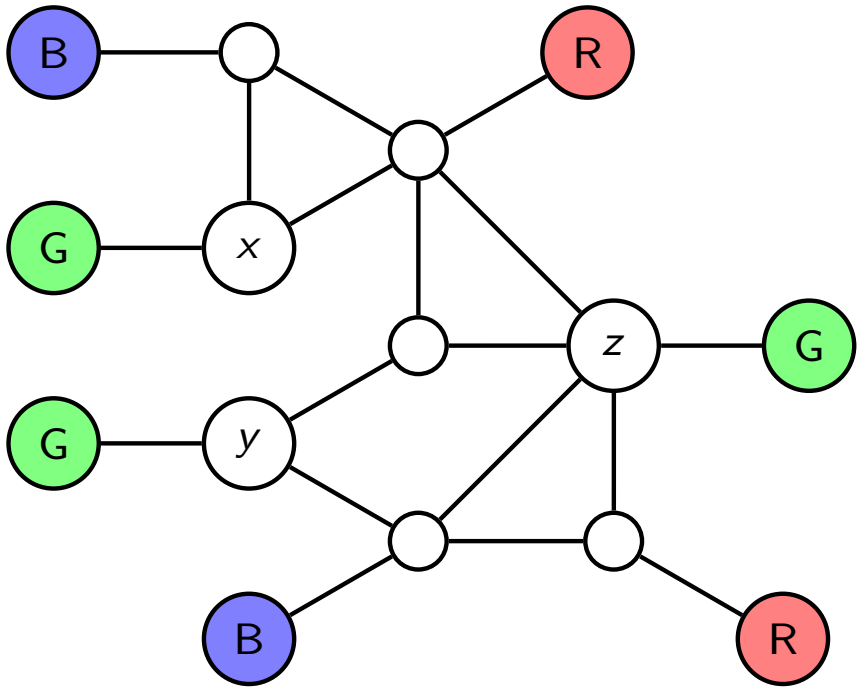
$F = G$ (as functions) iff $F \sim G$ (as circuits). We take a homotopy to be a "reasonable" proof of equality when it is efficient, $F \sim_e G$.

Circuit homotopy = urban renewal

Since circuit homotopy is given by local replacement, it is the same concept as urban renewal. We can also locally replace Boolean circuits by other combinatorics, *e.g.*, 3-coloring completion of graphs:







Efficient homotopy = bijective proof

Definition Let $X \cong_{\mathsf{e}} Y$ be efficiently bijective combinatorial sets. *I.e.*, $X, Y \subseteq (\mathbb{Z}/2)^{\ell}$ with predicates P and Q, and there is a bijection $f : X \to Y$ with an efficient reversible circuit R. Then a bijective proof in the circuit complexity sense is an efficient homotopy $P \sim_{\mathsf{e}} Q \circ R$, whence we write $X \cong_{\mathsf{eh}} Y$.

Theorem If $X \cong_{\mathsf{eh}} Y$, then $Y \cong_{\mathsf{eh}} X$.

Proof. If R is reversible, then $R \circ R^{-1} \sim_{e} I$, because the gates cancel locally in pairs. □

Note: Whether $X \cong_{\mathsf{eh}} Y$ depends on their predicates P and Q.

Numbers and formulas

Given $N \geq 0$ with at most $m = \text{poly}(n)$ digits, we define the standard counting set

$$[N] \stackrel{\text{def}}{=} \{0, 1, \ldots, N-1\} \hookrightarrow (\mathbb{Z}/2)^m$$

with the computed predicate $\vec{x} <_? N$, where $\vec{x}$ is read as a non-negative integer. An efficient homotopy $X \cong_{\text{eh}} [N]$ is then a bijective proof that $|X| = N$.

Any formula for N with a $\text{poly}(n)$ circuit C yields an equivalent predicate, because an incremental evaluation of C is a circuit homotopy. WLOG, N is given by a list of digits. Consequently every integer equality $f(n) = g(n)$ with $f, g \in \mathsf{P}$ has a bijective proof. Our model works too well for this.

Bags of coins

We generalize $[N]$ to bags of coins

$$[N_0, N_1, \ldots, N_{\ell-1}] \stackrel{\text{def}}{=} N_0 \amalg N_1 \amalg \cdots \amalg N_{\ell-1}$$

with $\ell = \text{poly}(n)$. *I.e.*, the bag of coins is the set of ordered pairs $(i, \vec{x})$ with $i <_? \ell$ and $\vec{x} <_? N_i$.

Lemma $[N]$ is equivalent to its minimal bag of binary coins:

$$N = \sum_{i \in I} 2^i \quad \Longrightarrow \quad [N] \cong_{\text{eh}} \coprod_{i \in I} [2^i].$$

Lemma We can merge two identical coins:

$$[2^i] \amalg [2^i] \cong_{\text{eh}} [2^{i+1}].$$

Addition and multiplication have efficient homotopies

Theorem Given $A, B > 0$ with poly(n) digits,

$$[A] \amalg [B] \cong_{\text{eh}} [A + B] \qquad [A] \times [B] \cong_{\text{eh}} [AB].$$

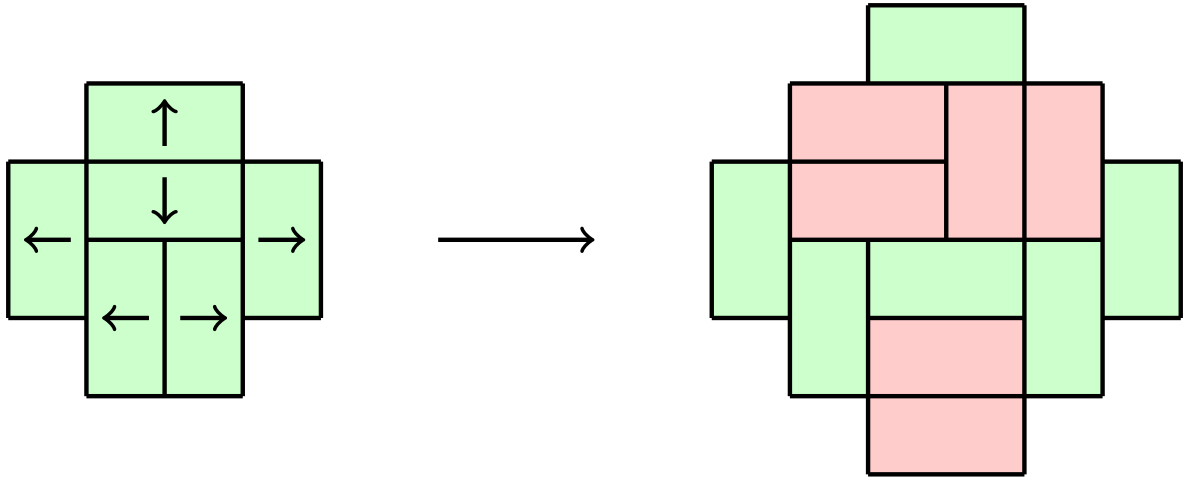
Proof. Expand $[A]$ and $[B]$ into minimal bags of coins, then use the lemmas on the previous slide. □

This result yields efficient homotopies for many basic facts in combinatorics: That $|S_n| = n!$ (using multiplication), that $|P_k([n])| = \binom{n}{k}$ (using the Pascal recurrence), etc.

It also yields a structural fact: If $[N]_a$ is the model of N with $\vec{x} <_? N$ computed in base a, then $[N]_a \cong_{\text{eh}} [N]_b$ for any a and b.

Domino shuffling

Domino shuffling is commonly recognized as a bijective proof that there are $2^{n(n+1)/2}$ domino tilings of an Aztec diamond of order n.



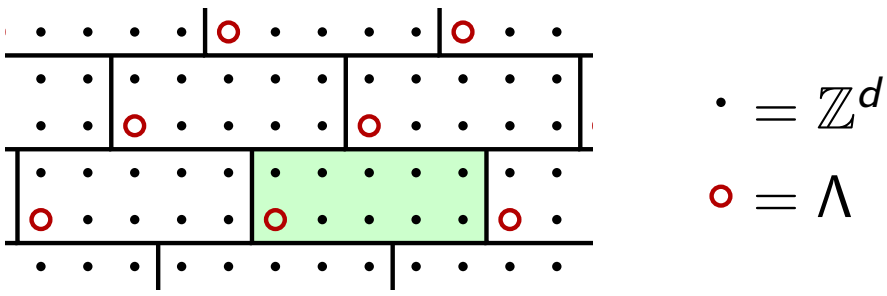
Theorem (I think) $\mathrm{AD}(n) \cong_{\mathsf{eh}} [2^{n(n+1)/2}]$ via domino shuffling.

Integer cokernels

An integer matrix $M \in \mathrm{M}(d, \mathbb{Z})$ has a (column) Hermite normal form H, which is a triangular matrix the same lattice image:

$$\Lambda \stackrel{\text{def}}{=} \operatorname{im} M = \operatorname{im} H \subseteq \mathbb{Z}^d.$$

We can compute H from M in P (Kannan-Bachem). If $\det M = \pm \det H \neq 0$, then Λ is cofinite and H yields a Λ-periodic tiling of $\mathbb{Z}^d$ by rectangular bricks:



The brick anchored at $\vec{0}$ is a combinatorial model for coker M with a predicate in P. Since it is a brick, coker $M \cong_{\text{eh}} [|\det M|]$.

Cokernel bijections

Theorem

1. If $M \in \mathrm{M}(d, \mathbb{Z})$ is nonsingular and S is its Smith normal form, then $\operatorname{coker} M \cong_{\mathrm{e}} \operatorname{coker} S$ via the induced isomorphism of cokernels.

2. If X is the set of spanning trees of a connected graph G and M is a Kirchhoff matrix for G, then $X \cong_{\mathrm{e}} \operatorname{coker} M$.

3. If $X \neq \emptyset$ is the set of perfect matchings of a planar bipartite graph G and M is a Kasteleyn-Percus matrix for G, then $X \cong_{\mathrm{e}} \operatorname{coker} M$.

Conjecture In all three cases, "$\cong_{\mathrm{e}}$" can be made "$\cong_{\mathrm{eh}}$".

Some computational complexity classes

- P is the set of decision (or function) problems computable in deterministic polynomial time.
- NP is P with the aid of an omniscient prover, who provides a certificate to lobby the verifier to output "yes".
- coNP is NP with "yes" and "no" switched, *i.e.*, with a disprover.
- Σ_nP is the model of debates between a prover and a disprover with n half-rounds, and with a referee in P.
- PH, the polynomial hierarchy, is the union of all Σ_nP.
- #P is the number of accepted certificates, the patron class of enumerative combinatorics.
- $C_=$P asks when two problems in #P have the same value.

Quantifiers for complexity classes

If C is a decision complexity class, then it can be rigorously modified with $\exists$ and $\forall$ as class operators. Formally, if $d \in \mathsf{C}$, then

$$e(\vec{x}) = \exists_? \vec{y} : d(\vec{x}, \vec{y}) \in \exists \cdot \mathsf{C} \qquad a(\vec{x}) = \forall_? \vec{y} : d(\vec{x}, \vec{y}) \in \forall \cdot \mathsf{C},$$

where in both cases $|\vec{x}| = |\vec{y}| = \mathrm{poly}(n)$. For example,

$$\mathsf{NP} = \exists \cdot \mathsf{P} \qquad \mathsf{coNP} = \forall \cdot \mathsf{P} \qquad \Sigma_4\mathsf{P} = \exists \cdot \forall \cdot \exists \cdot \forall \cdot \mathsf{P}.$$

Theorem (Tarui, 1991) $\mathsf{PH} \subseteq \exists \cdot \mathsf{C}_=\mathsf{P}$.

This important result contrasts with the conjecture that $\Sigma_n\mathsf{P}$ grows as n increases, *i.e.*, that PH does not collapse. Assuming so, $\mathsf{C}_=\mathsf{P} \not\subseteq \mathsf{PH}$.

A conditional non-existence result

If every efficient bijection had an efficient homotopy,

$$X \cong_{\mathsf{e}} Y \quad \Longrightarrow \quad X \cong_{\mathsf{eh}} Y,$$

then it would be so when $X = Y = \emptyset$. This would imply that coNP $\subseteq$ NP, which would imply that PH collapses to NP.

E.g., a bijection between "n-digit primes that end in 6" and "n-digit counterexamples to Fermat's last theorem" does not by itself shed any light on Fermat's last theorem.

Another conditional non-existence result

If combinatorial sets X and Y with $|X| = |Y|$ always had an efficient bijection,

$$X \cong Y \quad \Longrightarrow \quad X \cong_{\mathsf{e}} Y,$$

then it would imply that $\mathsf{C}_{=}\mathsf{P} \subseteq \Sigma_2\mathsf{P}$, because a prover can offer an efficient bijection and a disprover can critique it. By Tarui's theorem, PH would collapse to $\Sigma_3\mathsf{P}$.

When a bijection is a one-way street

Computer scientists also conjecture that there are bijections $f : X \to Y$ such that $f \in \mathsf{P}$ while $f^{-1} \notin \mathsf{P}$. Such an f is called a one-way permutation.

For example, if P is a large prime and $r \in \mathbb{Z}/P$ is a primitive root, then the exponentiation map $f : \mathbb{Z}/(P-1) \to (\mathbb{Z}/P)^\times$ given by $f(x) = r^x$ is thought to be a one-way permutation. (Albeit that $f^{-1} \in \mathsf{BQP}$ in this case.)

Note that the (forward) composition $f \circ g$ of two one-way permutations f and g is often again conjectured to be a one-way permutation.

Conflicting one-way streets

We have a lot of freedom to make two one-way permutations:

$$X \xrightarrow{f} Y \xleftarrow{g} Z$$

For example, if $P \lessapprox Q \lessapprox N$ with P and Q prime, then we can initially make f and g as:

$$\mathbb{Z}/(P-1) \xrightarrow{f(x)=r^x} (\mathbb{Z}/P)^\times \hookrightarrow [N] \hookleftarrow (\mathbb{Z}/Q)^\times \xleftarrow{g(z)=s^z} \mathbb{Z}/(Q-1)$$

We can define $Y \subseteq [\min(P,Q)] \setminus \{0\}$ by a chaotic predicate $p \in \mathsf{P}$, then define X and Z by the predicates $p \circ f$ and $p \circ g$. This yields a bijection $h = g^{-1} \circ f$ between X and Y and a proof that $|X| = |Y|$. But there might be no semi-efficient bijection and $|X|$ is probably intractable too.