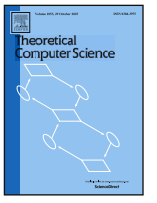
Theoretical Computer Science 1082 (2026) 116158

Contents lists available at ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs



On injective multivariate polynomials over rational numbers

Mika Hirvensalo

Department of Mathematics and Statistics, University of Turku, Turku, FI-20014, Finland

ARTICLE INFO

Editor: Dr. Lila Kari

Keywords:
Injective functions
Multivariate polynomials
Probabilistic automata

ABSTRACT

Let $\mathbb{P}$ be the set of prime numbers. We show that for each finite set $\Pi \subseteq \mathbb{P} \setminus \{2\}$, there exists a subring $\Lambda_\Pi \subseteq \mathbb{Q}$ and an injective polynomial function $P : \Lambda_\Pi \times \Lambda_\Pi \to \Lambda_\Pi$.

1. Background

Notation $\mathbb{N}_0$ stands for the set $\{0, 1, 2, 3 \ldots\}$ and $|A|$ means the cardinality of a set A. For any finite set A, it is clear that $|A \times A| = |A|^2$, hence no bijection $A \times A \to A$ exists unless $|A| = 0$ or $|A| = 1$. Infinite sets, however, are different since a bijection $\mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ can be found by walking through the 2-dimensional diagram as shown in Fig. 1.

Fig. 1 gives in fact more than the mere existence of a bijection. It is an easy excercise to derive the famous *Cantor pairing*

$$C : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0,\ C(x, y) = \frac{1}{2}(x + y + 1)(x + y) + y, \tag{1}$$

which gives the bijection in a form of two-variate polynomial of degree two: $C(0,0) = 0$, $C(1,0) = 1$, $C(0,1) = 2$, $C(2,0) = 3$, $C(1,1) = 4$ etc.

An explicit bijection $A \times A \to A$ can be given also for a strictly greater set cardinality than that of $\aleph_0$. Set $A = \{a, b\}^\omega$ consisting of infinite sequences over alphabet $\{a, b\}$ has cardinality $2^{\aleph_0}$ and is uncountable by Cantor's famous digonalization argument. Nevertheless, there is a simple constructive bijection $f : A \times A \to A$ simply described by interleaving:

$$f(x_1x_2x_3 \ldots, y_1y_2y_3 \ldots) = x_1y_1x_2y_2x_3y_3 \ldots$$

For infinite sets of cardinality higher than $2^{\aleph_0}$, no explicit bijection $A \times A \to A$ is known to the author. It is anyway known that the existence of such bijection for any infinite set A is equivalent to the Axiom of Choice, as shown by A. Tarski [1]. Interestingly, Jan Mycielski mentions [2] that when Tarski submitted this result to *Comptes rendus de l'Académie des Sciences* the paper was rejected: Fréchet wrote that an implication between two well known propositions is not a new result, Lebesgue wrote that an implication between two false propositions is of no interest, and Tarski never tried to publish in the *Comptes rendus* anymore.

2. Motivation

In [3] it was shown that it is undecidable whether a finite quantum automaton (see e.g., [14], [4], [15]) produces a fixed acceptance probability in a unique manner. The construction involved mostly only rational numbers, but the last stage combining various quantum automata into a bigger one involved irrational numbers linearly independent over $\mathbb{Q}$.

E-mail address: mikhirve@utu.fi

https://doi.org/10.1016/j.tcs.2026.116158
Received 17 September 2024; Received in revised form 21 October 2025; Accepted 3 July 2026
Available online 6 July 2026

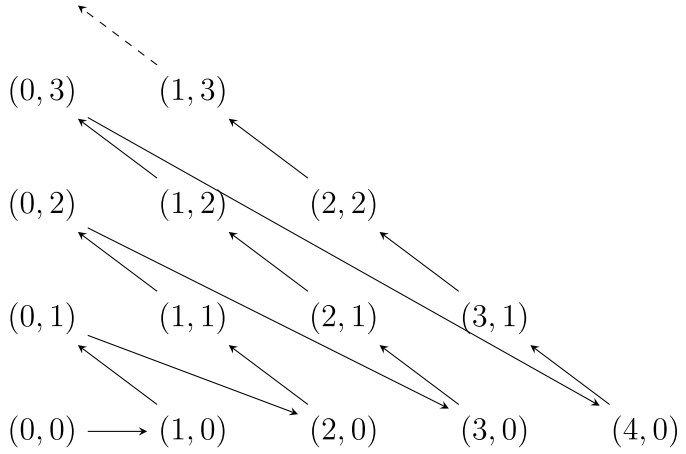


Fig. 1. A path visiting all points in $\mathbb{N}_0 \times \mathbb{N}_0$ exactly once demonstrates the existence of a bijection $\mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$.

The authors wondered whether it is possible to avoid irrational numbers in the construction, and it was clear that one way of doing so is to introduce an injective multivariate polynomial P: $\mathbb{Q}^n \to \mathbb{Q}$. As explained in the sequel, such a polynomial is quite difficult to find, but in [5], the authors resolved the problem by introducing a polynomial which was proven to be injective on a subset of $\mathbb{Q}^n$ large enough for the purposes of [5].

It is clear that for any set A, an injection $f : A \times A \to A$ can be extended to injection $f : A^n \to A$ recursively, and that if f is a polynomial, then the recursive extension to higher cartesian power is a polynomial, as well.

From this on, we separate the motivation and target, and just concentrate on finding a polynomial injection $P : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$. Set $\mathbb{Q}$ has cardinality $\aleph_0$, and there exists an explicit bijection $\mathbb{Q} \to \mathbb{N}$, hence we know that bijection $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ exists independently of the Axiom of Choice.

3. Previous considerations

Independently of the aforesaid, it turns out that the existence of a polynomial bijection (let alone injection) $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ is not a straightforward issue at all. From Section 1 we recall that the Cantor pairing (1) defines a polynomial injection $\mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$, and it may be worth studying it in order to get some hints about potential bijection $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$.

It has been known for more than 100 years that that no degree 2 polynomial bijections $\mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ different from $C(x, y)$ or $C(y, x)$ exist [6], and a simpler proof was given only recently [7]. In [8], it was shown that no degree > 2 polynomial bijection $\mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ exists.

Based on the above, the Cantor pairing function is very unique. Unfortunately, it is not our desired injection $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$, as the counterexample

$$C(\frac{11}{25}, \frac{2}{25}) = \frac{297}{625} = C(\frac{9}{25}, \frac{3}{25}),$$

shows, and it is not too difficult to find infinitely many counterexamples. Bijection $\mathbb{Q} \to \mathbb{N}$ does not help here, either, as no such bijection is polynomial. The reason for this is simply that for any continuous function such as a polynomial, the images get arbitrarily close to each other, if the preimages do. But natural numbers are alway at least distance one apart from each other.

The question about the existence of polynomial injections $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ however has a generally accepted solution among number-theorists: it is believed that they can be found almost everywhere.

Cornelissen [9] wrote about the conversation between famous number-theoretists Harvery Friedman and Don Zagier. According to Cornelissen, Friedman asked Zagier whether a polynomial injection $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ exists. According to the story, Zagier had replied something like "almost all complex enough polynomials will do, for example $x^7 + 3y^7$ is most likely a desired injection". However, to point out even a single polynomial injection with an unconditional proof has appeared very problematic.

Cornelissen [9] showed that from the 4-term version of the abc-conjecture it follows that $f(x, y) = x^n + 3y^n$ defines an injection $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ if (odd) n is large enough. Unfortunately, status of even the 3-term version of the abc-conjecture [10,11] is still open.

Recall that a field $\mathbb{K}$ is called *perfect*, if every irreducible polynomial over $\mathbb{K}$ has distinct roots, and that especially every field of characteristic 0 is perfect. A field of characteristic $p > 0$ is *imperfect*, if there is an element which is not a pth power – a transcendental extension of a finite field serves as an example of an imperfect field. It is interesting to notice the following:

Remark 1. For any imperfect field $\mathbb{K}$ of characteristic p and $\gamma \in \mathbb{K} \setminus \mathbb{K}^p$,

$$f(x, y) = x^p + \gamma y^p$$

is trivially an injection $\mathbb{K} \times \mathbb{K} \to \mathbb{K}$.

However, $\mathbb{Q}$ is not an imperfect field, and hence the construction of the above remark does not work. Bjorn Poonen [12] took an important step by proving the following theorem:

Theorem 1. *Assume that there is a homogenous polynomial $F(x, y)$ over rationals so that the rational points in the projective surface X defined as $F(x, y) = F(z, w)$ are not Zariski dense in X. Then there exists a polynomial injection $f : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$.*

Combining this with the following conjecture, we can have a strong opinion about the existence of the required injection.

Conjecture 1 (Bombieri-Lang)**.** *If X is a smooth projective irreducible algebraic surface over rationals of general type. Then the set of rational points of X is not Zariski dense in X [12].*

Remark 2. "General type" in the above definition refers to the Kodaira dimension. It suffices that $F(x, y)$ is separable, homogenous, and of degree at least 5 [12]. Hence if Conjecture 1 holds, there certainly are desired polynomial injections $f : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ almost everywhere.

It is also worth noticing that in [13] H. Pasten very showed how to construct injective bivariate polynomials on elliptic curves over an arbitrary number field.

4. Explicit restricted construction

If anything can be learned from the previous section, it is that a polynomial injection $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ quite likely exists, but unconditional existence proof, let alone an example of such injection appears to be beyond current knowledge. Therefore we cannot give any explicit construction but for $A \subset \mathbb{Q} \times \mathbb{Q}$, where A is restricted in many ways, but still useful for purposes such as in [5].

In [5], a construction of a bijectice bivariate polynomial defined on set $\Lambda = \{ \frac{a}{5^k} \mid a, k \in \mathbb{N}_0, a < 5^k \}$ was given. Equipping f with a renormalization factor $\frac{1}{25}$ then provided a polynomial injection $f : \Lambda \times \Lambda \to \Lambda$, of degree 12, which was sufficient for the purposes of [5]. Here we present a generalization of that construction.

Definition 1. For any finite set $\Pi \subset \mathbb{P} \setminus \{2\}$ of odd prime numbers, we define R_Π as a subset of $\mathbb{Q}$ having the property that their denominators in the reduced form are divisible only by primes in Π. More formally:

$$R_\Pi = \{q \in \mathbb{Q} \mid v_p(q) < 0 \implies p \in \Pi\},$$

where v_p stands for the p-adic valuation.

It is easy to see that R_Π is subring of $\mathbb{Q}$. To generalize the notions of [5], we define

$$\Lambda_\Pi = R_\Pi \cap [0, 1]$$

and introduce a polynomial injection $\Lambda_\Pi \times \Lambda_\Pi \to \Lambda_\Pi$. Set Λ_Π may appear restricted in the first sight, but in the context of finite semigroups generated by stochastic matrices over rational numbers, it becomes understandable: The number of matrix elements is finite, hence there are only finitely many primes occurring in the denominators, and as probabilities, all matrix elements are in the interval $[0, 1]$.

Theorem 2. *For each finite nonempty set $\Pi \subset \mathbb{P} \setminus \{2\}$, there exists a bivariate polynomial $p(x, y) \in \mathbb{Q}[x, y]$ so that the induced function $p : \Lambda_\Pi \times \Lambda_\Pi \to \Lambda_\Pi$ is injective.*

Proof. Let N be any number coprime to each $p_i - 1$ and p_i, for each $p_i \in \Pi$. For example, any prime greater than the maximal prime in Π will do, but depending on the set Π, also a smaller value may be chosen. Let also $M = \mathrm{lcm}\{p - 1 \mid p \in \Pi\}$. By definition $N \geq 2$ anyway.

We will show that the polynomial

$$p(x, y) = (x^M + y^M)^N + y^M \tag{2}$$

up to constant coefficient defines the desired injection. For this purpose, we select arbitrary four numbers in set Λ_Π. By the definition of Λ_Π, we can present those numbers as $\frac{a}{P}$, $\frac{b}{P}$, $\frac{c}{P}$, and $\frac{d}{P}$, where P is a product of primes in set Π, and $\{a, b, c, d\} \subset \mathbb{N}_0 \cap [0, P]$. Without loss of generality, we will also assume for each $p \in \Pi$, at least one of the numbers a, b, c and d is not divisible by p, meaning that the choice of P is minimal.

To prove the injectivity, we show that the assumption

$$p(\frac{a}{P}, \frac{b}{P}) = p(\frac{c}{P}, \frac{d}{P}) \tag{3}$$

impies $a = c$ and $b = d$. For brevity, we denote $\alpha = (\frac{a}{P})^M$, $\beta = (\frac{b}{P})^M$, $\gamma = (\frac{c}{P})^M$, and $\delta = (\frac{d}{P})^M$. Moreover, let $S_1 = \alpha + \beta$ and $S_2 = \gamma + \delta$.

Using (2) and these notations, (3) becomes

$$S_1^N + \beta = S_2^N + \delta \tag{4}$$

If $S_1 = S_2$, then $\beta = \delta$, and $\alpha = \gamma$, and as each of numbers P, a, b, c, and d is nonnegative, it follows that $a = c$ and $b = d$.

We can therefore assume that $S_1 \neq S_2$, and without loss of generality, that $S_1 > S_2$. Assume first that $\Delta = S_1 - S_2 \geq 1$. Then by (4) and binomial theorem we have

$$\delta - \beta = (S_2 + \Delta)^N - S_2^N = \sum_{i=0}^{N} \binom{N}{i} S_2^{N-i} \Delta^i - S_2^N$$

$$\geq \sum_{i=0}^{N} \binom{N}{i} S_2^{N-i} - S_2^N = \sum_{i=1}^{N} \binom{N}{i} S^{N-i} > \binom{N}{N-1} S_2 \geq S_2.$$

Thus

$$\delta - \beta > S_2 = \gamma + \delta,$$

which implies $-\beta > \gamma$, which is a contradiction, as $\beta, \gamma \geq 0$.

We can therefore assume that $\Delta < 1$ which can be rewritten as

$$\begin{aligned} &\left| \left(\frac{a}{P}\right)^M + \left(\frac{b}{P}\right)^M - \left(\left(\frac{c}{P}\right)^M + \left(\frac{d}{P}\right)^M \right) \right| < 1 \\ \Rightarrow &\left| a^M + b^M - (c^M + d^M) \right| < P^M. \end{aligned} \tag{5}$$

If now (3) holds, then

$$\begin{aligned} &\left(\left(\frac{a}{P}\right)^M + \left(\frac{b}{P}\right)^M \right)^N + \left(\frac{b}{P}\right)^M = \left(\left(\frac{c}{P}\right)^M + \left(\frac{d}{P}\right)^M \right)^N + \left(\frac{d}{P}\right)^M \\ \Leftrightarrow &(a^M + b^M)^N + b^M P^{M(N-1)} = (c^M + d^M)^N + d^M P^{M(N-1)}, \end{aligned} \tag{6}$$

hence

$$(a^M + b^M)^N \equiv (c^M + d^M)^N \pmod{P^{M(N-1)}},$$

and since $N \geq 2$, we have also

$$(a^M + b^M)^N \equiv (c^M + d^M)^N \pmod{P^M}. \tag{7}$$

Consider now any prime p dividing P. Recall that then $p \in \Pi$ and that M was chosen so that $p - 1 \mid M$. Fermat's litle theorem therefore implies that each of a^M, b^M, c^M or d^M is congruent to 0 or 1 $\pmod{p}$. On the other hand, P was chosen so that at least one of a, b, c, and d is not divisible by p. Without loss of generality, we can assume that $a^M \equiv 1 \pmod{p}$, so $a^M + b^M$ is either $\equiv 1$ or $\equiv 2 \pmod{p}$. If both c and d are divisible by p, we have a contradiction with (7). Hence also $c^M + d^M$ is congruent to 1 or 2 $\pmod{p}$.

If follows (since $p > 2$) that $\gcd(p, a^M + b^M) = \gcd(p, c^M + d^M) = 1$, and as this is true for each $p \mid P$, we can conclude that $\gcd(P^M, a^M + b^M) = \gcd(P^M, c^M + d^M) = 1$.

As P is a product of primes in Π, $P^M = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$, for some $a_i \in \mathbb{N}$, we have $\varphi(P^M) = p_1^{a_1 - 1} \dots p_n^{a_n - 1}(p_1 - 1) \dots (p_n - 1)$, where φ stands for the Euler totient function. Recall that N was chosen so that $(\varphi(P^M), N) = 1$ and hence there exists a multiplicative inverse N_1 of N modulo P^N, and raising to the power N_1, (7) implies

$$a^M + b^M \equiv c^M + d^M \pmod{P^M}. \tag{8}$$

Together with (5) and (8) we have

$$a^M + b^M = c^M + d^M,$$

which implies $S_1 = S_2$, a contradiction.

Note that by definition, the set Λ_Π is restriced in interval $[0, 1]$, but the value of $p(x, y)$ could be bounded by

$$\left| (x^M + y^M)^N + x^M \right| \leq (1 + 1)^N + 1 = 2^N + 1.$$

However, we can select any product P_1 of elements in Π so that $P_1 > 2^N + 1$, and an injection $\Lambda_\Pi \times \Lambda_\Pi \to \Lambda_\Pi$ can hence be obtained simply by introducing a renormalization factor $\frac{1}{P_1}$ to p. □

CRediT authorship contribution statement

Mika Hirvensalo: Writing – review & editing, Writing – original draft, Investigation, Formal analysis.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] A. Tarski, Sur quelques theorems qui equivalent a l'axiome du choix, Fundam. Math. 5 (1924) 147–154.
[2] J. Mycielski, A system of axioms of set theory for the rationalists, Not. Am. Math. Soc. 53 (2) (2006) 209–213.
[3] P. Bell, M. Hirvensalo, Acceptance ambiguity for quantum automata, in: P. Rossmanith, P. Heggernes, J.-P. Katoen (Eds.), Proceedings of MFCS 2019, Vol. 138, Leibniz International Proceedings in Informatics, 2019.
[4] M. Hirvensalo, Various aspects of finite quantum automata, Lecture Notes in Computer Science, 5257 Proceedings of DLT 2008, 2008, pp. 21–33.
[5] P.C. Bell, M. Hirvensalo, On injectivity of quantum finite automata, J. Comput. Syst. Sci. 122 (2021) 19–33.
[6] R. Fueter, G. Pólya, Rationale abzählung der gitterpunkte, Vierteljschr. Naturforsch. Ges. Zürich 68 (1923) 380–386.
[7] M.A. Vsemirnov, Two elementary proofs of the Fueter–Pólya theorem on pairing polynomials, St Petersburg Math. J. 13 (5) (2002) 705–715.

[8] P.W. Adriaans, (https://arxiv.org/abs/1809.09871).
[9] G. Cornelissen, Stockage diophantien et hypothèse abc généralisée, Comptes Rendus Acad. Sci. Paris Sér. I Math. 328 (1) (1999) 3–8.
[10] D.W. Masser, Open problems, in: W.W.L. Chen (Ed.), Proceedings of the Symposium on Analytic Number Theory, London Imperial College, 1985.
[11] J. Oesterlé, Nouvelles approches du "théorème" de fermat, Astérisque Exp. No. 694 (1988) 161–162.
[12] B. Poonen, Multivariable polynomial injections on rational numbers, 2009. https://arxiv.org/abs/0902.3961.
[13] H. Pasten, Bivariate polynomial injections and elliptic curves, 2018. https://arxiv.org/abs/1811.02416.
[14] M. Hirvensalo, Quantum Computing, Springer, 2004.
[15] M. Hirvensalo, Quantum automata with open time evolution, Int. J. Nat. Comput. Res. 1 (2010) 70–85.