ROOTS OF POLYNOMIALS AND THE DERANGEMENT PROBLEM

LIOR BARY-SOROKER AND OFIR GORODETSKY

Abstract. We present a new killing-a-fly-with-a-sledgehammer proof of one of the oldest results in probability which says that the probability that a random permutation on n elements has no fixed points tends to e^{-1} as n tends to infinity. Our proof stems from the connection between permutations and polynomials over finite fields and is based on an independence argument, which is trivial in the polynomial world.

1. Introduction.

The derangement problem, first studied by Pierre Rémond de Montmort in 1708, asks what is the probability P_n that a random permutation on n letters has no fixed points. A simple argument using the inclusion-exclusion principle, given by Nicholas Bernoulli in 1713, computes P_n explicitly (namely, $P_n = \sum_{i=0}^{n} \frac{(-1)^i}{i!}$) and, in particular,

$$\lim_{n\to\infty} P_n = e^{-1}. \tag{1}$$

If $X_k = \{\sigma(k) \neq k\}$ is the event that k is not a fixed point, then $P_n = \mathbb{P}(X_1 \cap \cdots \cap X_n)$. Since $\mathbb{P}(X_k) = 1 - \frac{1}{n}$, one gets that $\prod_k \mathbb{P}(X_k) = (1-\frac{1}{n})^n \to e^{-1}$. However, this argument does not imply (1) since the events X_k are not independent.

Our goal is to give a new proof of (1) based on an independence argument of polynomials over finite fields. This approach may be considered natural for finite field theorists due to the ancient connection between polynomials, permutations, and integers which goes back at least to Gauss's exact formula; see (9) below. For further reading on recent progress see the survey papers [2, 3, 5].

We approximate P_n by the probability $P_{n,q}$ that a random uniform monic polynomial of degree n over a finite field $\mathbb{F}_q$ with q elements has no root in $\mathbb{F}_q$ (here q is a prime power): If $n \geq q$, then the events $\tilde{X}_\alpha = \{f(\alpha) \neq 0\}$, $\alpha \in \mathbb{F}_q$ are independent and $\mathbb{P}(\tilde{X}_\alpha) = 1 - q^{-1}$. (This is straightforward from Lagrange interpolation or from the Chinese remainder theorem; see Section 2.) Thus,

$$P_{n,q} = \mathbb{P}\Big(\bigcap_{\alpha\in\mathbb{F}_q} \tilde{X}_\alpha\Big) = \prod_{\alpha\in\mathbb{F}_q} \mathbb{P}(\tilde{X}_\alpha) = (1-q^{-1})^q \to e^{-1}, \quad (n \geq q \to \infty). \tag{2}$$

A special case of a theorem of Arratia, Barbour, and Tavaré [1, Cor. 5.6] says that

$$|P_n - P_{n,q}| = O\Big(\frac{1}{q}\Big); \tag{3}$$

see Section 4 for a simplified proof of (3). Substitute $q = 2^{\lfloor \log_2 n \rfloor}$ in (3) and take $n \to \infty$ to get by (2) that

$$\lim_{n\to\infty} P_n = \lim_{n\to\infty} P_{n,q} = e^{-1},$$

as needed. □

2. Independence argument.

Assume $n \geq q$. By Lagrange interpolation, for any subset S of $\mathbb{F}_q$ and any choice of $(c_\alpha)_{\alpha\in S}$ with $c_\alpha \in \mathbb{F}_q$, there exists a unique polynomial $g(X)$ of degree less than $\#S$ such that $g(\alpha) = c_\alpha$ for all $\alpha \in S$. Thus the monic polynomials of degree n passing through $(\alpha, c_\alpha)_{\alpha\in S}$ have the form

$$f(X) = g(X) + h(X) \prod_{\alpha\in S} (X - \alpha),$$

where h is monic and $\deg h = n - \#S$ and there are $q^{n-\#S}$ of them. (This parametrization also follows from the Chinese remainder theorem.) Thus

$$\mathbb{P}\Big(\bigcap_{\alpha\in S} \tilde{X}_\alpha \Big) = \sum_{c_\alpha\neq 0} \mathbb{P}(f(\alpha) = c_\alpha,\ \alpha \in S) = \sum_{c_\alpha\neq 0} \frac{q^{n-\#S}}{q^n} = \Big(\frac{q-1}{q}\Big)^{\#S},$$

which proves independence. Here the sum runs over all tuples of $(c_\alpha)_{\alpha\in S}$ of nonzero elements in $\mathbb{F}_q$. □

3. Probability measures on the space of partitions.

Consider the space Ω of all n-tuples $\mathbf{a} = (a_1, a_2, \dots, a_n)$ of nonnegative integers such that $\sum ia_i = n$. We define two probability measures on Ω, one coming from permutations and the other from polynomials over a finite field and compare them.

Let S_n be the symmetric group on n elements. Each $\sigma \in S_n$ has a cycle structure which may be regarded as an element $\mathbf{a}$ in Ω: We set a_i to be the number of orbits of σ of length i. Then $\sum_i ia_i = n$. For example, the trivial element corresponds to $(n, 0, \dots, 0)$, a transposition to $(n-2, 1, 0, \dots, 0)$, an n-cycle to $(0, \dots, 0, 1)$, etc. The uniform measure on S_n then induces a probability measure $\mathbb{P}_{S_n}$ on Ω, which by Cauchy's formula is given by

$$\mathbb{P}_{S_n}(\mathbf{a}) = \prod_{k=1}^{n} \frac{1}{k^{a_k} a_k!}. \tag{4}$$

Let q be a prime power, $\mathbb{F}_q$ the finite field with q elements, $\mathbb{F}_q[X]$ the ring of polynomials with coefficients in $\mathbb{F}_q$, and denote by $\mathcal{M} = \mathcal{M}_{n,q}$ the set of monic polynomials of degree n in $\mathbb{F}_q[X]$. The unique factorization of $f \in \mathcal{M}$ to monic irreducible polynomials,

$$f = P_1 \cdots P_k,$$

defines an element $\mathbf{a}$ of Ω; namely,

$$a_i = \#\{j : \deg P_j = i\}.$$

We emphasize that the counting is with multiplicity. Hence $\sum_i ia_i = \deg f = n$. The uniform measure on $\mathcal{M}$ then induces a probability measure on Ω given by

$$\mathbb{P}_{\mathcal{M}}(\mathbf{a}) = \frac{\prod_{i=1}^{n} \pi_q(i, a_i)}{q^n}, \tag{5}$$

where $\pi_q(i, a_i)$ is the number of ways to choose a_i monic irreducible polynomials of degree i (with repetition). If we denote by $\pi_q(i) = \pi_q(i, 1)$ the number of monic irreducible polynomials of degree i, then $\pi_q(i, a_i) = \binom{\pi_q(i)+a_i-1}{a_i}$. Thus, (5) transforms into

$$\mathbb{P}_{\mathcal{M}}(\mathbf{a}) = \prod_{k=1}^{n} \frac{1}{k^{a_k} a_k!} \cdot \left(\prod_{i=1}^{n} \prod_{j=0}^{a_i-1} \frac{i\pi_q(i) + ij}{q^i} \right). \tag{6}$$

To connect these probability measures with the derangement probabilities discussed in the introduction, we note that if Ω_0 is the event that $a_1 = 0$, then

$$P_n = \mathbb{P}_{S_n}(\Omega_0) \quad \text{and} \quad P_{n,q} = \mathbb{P}_{\mathcal{M}}(\Omega_0). \tag{7}$$

4. Comparison of probability measures.

We prove that the two measures defined above are close in the ℓ^1-norm.

Theorem. *Let n be a positive integer and q a prime power. Then*

$$\|\mathbb{P}_{S_n} - \mathbb{P}_{\mathcal{M}}\|_1 := \sum_{\mathbf{a}\in\Omega} |\mathbb{P}_{S_n}(\mathbf{a}) - \mathbb{P}_{\mathcal{M}}(\mathbf{a})| = O\Big(\frac{1}{q}\Big). \tag{8}$$

The bound (8) immediately implies (3) using (7). Indeed, by the triangle inequality,

$$|P_n - P_{n,q}| \le \sum_{\mathbf{a}\in\Omega_0} |\mathbb{P}_{S_n}(\mathbf{a}) - \mathbb{P}_{\mathcal{M}}(\mathbf{a})| \le \|\mathbb{P}_{S_n} - \mathbb{P}_{\mathcal{M}}\|_1 = O\Big(\frac{1}{q}\Big).$$

The key tool in proving the theorem above is *Gauss's exact formula* for the number of prime polynomials, which may be regarded as comparison of the measures on the event $\{\mathbf{a} = (0,\dots,0,1)\}$. It is given in terms of the Möbius function defined as

$$\mu(n) = \begin{cases} (-1)^r, & n = p_1\cdots p_r, \text{ for distinct prime numbers } p_i \\ 0, & \text{otherwise.} \end{cases}$$

Then Gauss's formula is

$$i\pi_q(i) = q^i + \sum_{1\ne d|i} \mu(d) q^{i/d}. \tag{9}$$

The proof is elementary and easy, but beautiful; see [4, Thm. 2.2]. From (9) one readily derives the useful bounds

$$q^i \ge i\pi_q(i) \ge q^i - 2\cdot q^{\lfloor i/2\rfloor}. \tag{10}$$

Proof of the Theorem. We may assume that $n > 1$ and we put

$$X = \|\mathbb{P}_{\mathcal{M}} - \mathbb{P}_{S_n}\|_1. \tag{11}$$

We write $\mathbb{P}_{\mathcal{M}}(\mathbf{a})$ as

$$\mathbb{P}_{\mathcal{M}}(\mathbf{a}) = p_{\mathbf{a},1} + p_{\mathbf{a},2}, \tag{12}$$

where $p_{\mathbf{a},1}$ and $p_{\mathbf{a},2}$ are the respective contributions from squarefree and non-squarefree polynomials. Apply the triangle inequality to (11) to obtain

$$X \le \mathbb{P}(f \text{ is not squarefree}) + \sum_{\mathbf{a}\in\Omega(n)} |\mathbb{P}_{S_n}(\mathbf{a}) - p_{\mathbf{a},1}|.$$

Here f is sampled uniformly from $\mathcal{M}$. It is well known that $\mathbb{P}(f \text{ is not squarefree}) = \frac{1}{q}$ (see, e.g., [4, Prop. 2.3]); thus it remains to show

$$Y = \sum_{\mathbf{a}\in\Omega(n)} |\mathbb{P}_{S_n}(\mathbf{a}) - p_{\mathbf{a},1}| = O\Big(\frac{1}{q}\Big).$$

We write $Y = Y_1 + Y_2$, according to whether there exists j with $a_j > \pi_q(j)$ or not and show that each Y_i is bounded by $O(1/q)$. To bound Y_1, we recall that a_j corresponds to the number of

irreducible factors, so the pigeonhole principle tells us the corresponding polynomial has a repeated factor, hence does not contribute to $p_{\mathbf{a},1}$, so $p_{\mathbf{a},1}=0$. It then follows by (4) that

$$\begin{aligned} Y_1 &\le \sum_{j=1}^{n} \sum_{\substack{\mathbf{a}\in\Omega(n)\\ a_j>\pi_q(j)}} \mathbb{P}_{S_n}(\mathbf{a}) \\ &= \sum_{j=1}^{n} \sum_{a_j>\pi_q(j)} \frac{1}{j^{a_j}a_j!} \sum_{\substack{\mathbf{b}\in\Omega(n)\\ b_j=a_j}} \prod_{i\neq j} \frac{1}{i^{b_i}b_i!} \le \sum_{j=1}^{n} \sum_{a_j>\pi_q(j)} \frac{1}{j^{a_j}a_j!}, \end{aligned} \tag{13}$$

where $\sum_{\substack{\mathbf{b}\in\Omega(n)\\ b_j=a_j}} \prod_{i\neq j} \frac{1}{i^{b_i}b_i!} \le 1$ as the probability of a permutation on $n-ja_j$ letters not to have an orbit of size j. Since $\frac{1}{j^{a_j+1}(a_j+1)!}\Big/\frac{1}{j^{a_j}a_j!} = \frac{1}{j(a_j+1)} \le \frac{1}{2}$, we may bound the inner sum in the right-hand side of (13) by twice the first summand, so by using the lower bound in (10), we obtain

$$Y_1 \le 2\sum_{j\ge 1} \frac{1}{j^{\pi_q(j)+1}(\pi_q(j)+1)!} \le 2\sum_{j\ge 1} \frac{1}{(\pi_q(j)+1)!} = O\Big(\frac{1}{q}\Big).$$

Now we bound Y_2; i.e., considering only $\mathbf{a}$'s with $a_j \le \pi_q(j)$ for all j. Similar to the derivation of (6); namely, using $\sum ia_i = n$, we have

$$p_{\mathbf{a},1} = \frac{1}{q^n}\prod_{i=1}^{n}\binom{\pi_q(i)}{a_i} = \prod_{k=1}^{n}\frac{1}{k^{a_k}a_k!}\prod_{i=1}^{n}\prod_{j=0}^{a_i-1}\frac{i\pi_q(i)-ij}{q^i}, \tag{14}$$

so

$$Y_2 = \sum_{\substack{\mathbf{a}\in\Omega(n)\\ \forall r: a_r\le\pi_q(r)}} |\mathbb{P}_{S_n}(\mathbf{a}) - p_{\mathbf{a},1}| = \sum_{\substack{\mathbf{a}\in\Omega(n)\\ \forall r: a_r\le\pi_q(r)}} \prod_{k=1}^{n}\frac{1}{k^{a_k}a_k!}\left|1-\prod_{i=1}^{n}\prod_{j=0}^{a_i-1}\frac{i\pi_q(i)-ij}{q^i}\right|. \tag{15}$$

By the upper bound in (10) and the assumption $j<a_i\le\pi_q(i)$, we have $0\le\frac{i\pi_q(i)-ij}{q^i}\le 1$. So we may use the Bernoulli-type inequality

$$0 \le 1-\prod_{k=1}^{m}(1-x_k) \le \sum_{k=1}^{m} x_k \tag{16}$$

with $\{x_k\}_k = \{1-\frac{i\pi_q(i)-ij}{q^i}\}_{i,j}$ to obtain

$$Y_2 \le \sum_{\substack{\mathbf{a}\in\Omega(n)\\ \forall j: a_j\le\pi_q(j)}} \prod_{k=1}^{n}\frac{1}{k^{a_k}a_k!}\sum_{i=1}^{n}\sum_{j=0}^{a_i-1}(1-\frac{i\pi_q(i)-ij}{q^i}). \tag{17}$$

From the lower bound in (10), we conclude that

$$\sum_{j=0}^{a_i-1}(1-\frac{i\pi_q(i)-ij}{q^i}) \le 2a_iq^{-\lceil\frac{i}{2}\rceil} + \frac{i}{q^i}\frac{a_i(a_i-1)}{2} \le 4a_i^2iq^{-\lceil\frac{i}{2}\rceil}. \tag{18}$$

Plugging (18) in (17) yields

$$\begin{aligned} Y_2 &\le 4 \sum_{\mathbf{a}\in\Omega(n)} \prod_{k=1}^{n} \frac{1}{k^{a_k} a_k!} \sum_{i=1}^{n} a_i^2 i q^{-\lceil \frac{i}{2} \rceil} \\ &= 4 \sum_{i=1}^{n} \sum_{0\le a\le n} \sum_{\substack{\mathbf{b}\in\Omega(n) \\ b_i=a}} \prod_{\substack{k=1 \\ k\neq i}}^{n} \frac{1}{k^{b_k} b_k!} \frac{1}{i^a a!} a^2 i q^{-\lceil \frac{i}{2} \rceil} \\ &\le 4 \sum_{i=1}^{n} \sum_{0\le a\le n} \frac{a^2 i q^{-\lceil \frac{i}{2} \rceil}}{i^a a!}, \end{aligned}$$

where as before $\sum_{\substack{\mathbf{b}\in\Omega(n) \\ b_i=a}} \prod_{\substack{k=1 \\ k\neq i}}^{n} \frac{1}{k^{b_k} b_k!} \le 1$. Thus,

$$Y_2 \le 4 \sum_{i\ge 1} i q^{-\lceil \frac{i}{2} \rceil} \sum_{a\ge 0} \frac{a^2}{a!} = O\Big(\frac{1}{q}\Big),$$

as needed to finish the proof. □

Acknowledgments.

The authors are partially supported by a grant of the Israel Science Foundation.

References

[1] Arratia, R., Barbour, A. D., Tavaré, S. (1993). On random polynomials over finite fields. *Math. Proc. Cambridge Philos. Soc.* 114, no. 2, 347–368. DOI: doi.org/10.1017/S0305004100071620

[2] Bary-Soroker, L. (2016). Prime Polynomials in Function Fields. *Snapshots of modern mathematics*, MFO, No. 10/2016. DOI: doi.org/10.14760/SNAP-2016-010-EN

[3] Keating, J. P., Rudnick, Z., Wooley, T. D. (2015). Number fields and function fields: coalescences, contrasts and emerging applications. *Philos. Trans. Roy. Soc. A* 373, no. 2040, 20140315, 4 pp. DOI: doi.org/10.1098/rsta.2014.0315

[4] Rosen, M. (2002). *Number Theory in Function Fields*. New York, NY: Springer-Verlag.

[5] Rudnick, Z. (2014). Some problems in analytic number theory for polynomials over a finite field. In: Jang, S. Y., Kim, Y. R., Lee, D. W., Yie, I., eds. *Proceedings of the ICM, Seoul 2014, Volume II*. Seoul, Korea: KYUNG MOON, pp. 443–460.

School of Mathematical Sciences, Tel Aviv University, Ramat Aviv, Tel Aviv 6997801, Israel
Email address: barylior@post.tau.ac.il

School of Mathematical Sciences, Tel Aviv University, Ramat Aviv, Tel Aviv 6997801, Israel
Email address: ofir.goro@gmail.com