Improved Lower Bounds for Permutation Arrays Using Permutation Rational Functions

Sergey Bereg∗ Brian Malouf∗ Linda Morales∗ Thomas Stanley∗ I. Hal Sudborough∗

June 12, 2020

Abstract

We consider rational functions of the form $V(x)/U(x)$, where both $V(x)$ and $U(x)$ are polynomials over the finite field $\mathbb{F}_q$. Polynomials that permute the elements of a field, called permutation polynomials (PPs), have been the subject of research for decades. Let $\mathcal{P}^1(\mathbb{F}_q)$ denote $\mathbb{F}_q \cup \{\infty\}$. If the rational function, $V(x)/U(x)$, permutes the elements of $\mathcal{P}^1(\mathbb{F}_q)$, it is called a permutation rational function (PRF). Let $N_d(q)$ denote the number of PPs of degree $d$ over $\mathbb{F}_q$, and let $N_{v,u}(q)$ denote the number of PRFs with a numerator of degree $v$ and a denominator of degree $u$. It follows that $N_{d,0}(q) = N_d(q)$, so PRFs are a generalization of PPs. The number of monic degree 3 PRFs is known [1]. We develop efficient computational techniques for $N_{v,u}(q)$, and use them to show $N_{4,3}(q) = (q + 1)q^2(q - 1)^2/3$, for all prime powers $q \leq 307$, $N_{5,4}(q) = (q + 1)q^3(q - 1)^2/2$, for all prime powers $q \leq 97$, and $N_{4,4}(p) = (p + 1)p^2(p - 1)^3/3$, for all primes $p \leq 47$. We conjecture that these formulas are, in fact, true for all prime powers $q$. Let $M(n, D)$ denote the maximum number of permutations on $n$ symbols with pairwise Hamming distance $D$. Computing improved lower bounds for $M(n, D)$ is the subject of much current research with applications in error correcting codes. Using PRFs, we obtain significantly improved lower bounds on $M(q, q - d)$ and $M(q + 1, q - d)$, for $d \in \{5, 7, 9\}$.

References

[1] A. Ferraguti and G. Micheli. Full classification of permutation rational functions and complete rational functions of degree 3. Designs, Codes, and Cryptography, 23, January 2020.

∗Department of Computer Science, University of Texas at Dallas, Box 830688, Richardson, TX 75083 USA. Research of the first author is supported in part by NSF award CCF-1718994.