








Improved Lower Bounds for Permutation Arrays Using Permutation Rational Functions

Sergey Beresg , Brian Malouf , Linda Morales , Thomas Stanley ,
and I. Hal Sudborough 

Department of Computer Science, University of Texas at Dallas,
Box 830688, Richardson, TX 75083, USA
hal@utdallas.edu

Abstract. We consider rational functions of the form $V(x)/U(x)$, where both $V(x)$ and $U(x)$ are relatively prime 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 [11]. 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 give a formula for $N_{4,4}(q)$. We conjecture that these are 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 $d \in \{5, 7, 9\}$.

Keywords: Hamming distance · Permutation array · Rational functions · Permutation polynomials

1 Introduction

Permutation arrays (PAs) with large Hamming distance have been the subject of many recent papers with applications in the design of error correcting codes. New lower bounds for the size of such permutation arrays are given, for example [1–7, 12, 14, 15, 19, 20, 22].

Let X be a set of n symbols, and let π and σ be permutations over X . The Hamming distance between π and σ , denoted by $hd(\pi, \sigma)$, is the number

S. Beresg—Research of the first author is supported in part by NSF award CCF-1718994.

© Springer Nature Switzerland AG 2021

J. C. Bajard and A. Topuzođlu (Eds.): WAIFI 2020, LNCS 12542, pp. 234–252, 2021.

https://doi.org/10.1007/978-3-030-68869-1_14

of positions $x \in X$ such that $\pi(x) \neq \sigma(x)$. Define the Hamming distance of a PA A , by $hd(A) = \min\{hd(\pi, \sigma) \mid \pi, \sigma \in A, \pi \neq \sigma\}$. Let $M(n, D)$ denote the maximum number of permutations in any PA A on n symbols with Hamming distance D .

Let \mathbb{F}_q denote the finite field with $q = p^m$ elements, where p is prime and $m \geq 1$. The prime p is called the *characteristic* of the field. A polynomial $V(x)$ over \mathbb{F}_q is a *permutation polynomial (PP)* if it permutes the elements of \mathbb{F}_q . Permutation polynomials have been studied for many decades, for example [2, 8–10, 13, 16, 17, 21].

In this paper, we focus on permutation rational functions (*PRFs*), defined as follows:

Definition 1. Let $V(x)$ and $U(x)$ be polynomials over \mathbb{F}_q , such that $\gcd(V(x), U(x)) = 1$. 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 $\mathcal{P}^1(\mathbb{F}_q)$, then it is called a **permutation rational function (PRF)**.

Yang *et al.* [23] used *PRFs* to compute, for example, an improved lower bound for $M(19, 14)$. Ferraguti and Micheli [11] enumerated all *PRFs* of degree 3.

Let $a \in \mathbb{F}_q$ and $a' \in \mathbb{F}_q \setminus \{0\}$. We use these conventions to evaluate expressions involving ∞ :

$$a/\infty = 0, \quad a'/0 = \infty. \tag{1}$$

Let $\mathcal{W}(x) = \frac{V(x)}{U(x)}$ be a *PRF*, where $V(x)$ has degree v , $U(x)$ has degree u , and their high order coefficients are a_v and b_u , respectively. We use Eq. 1 to evaluate $\mathcal{W}(x)$ at ∞ :

$$\mathcal{W}(\infty) = \mathcal{W}(1/x) \text{ when } x = 0. \tag{2}$$

Specifically, Eq. 2 implies that

$$\mathcal{W}(\infty) = \begin{cases} \infty, & \text{when } v > u \\ 0, & \text{when } v < u \\ a_v/b_v, & \text{when } v = u. \end{cases} \tag{3}$$

Observe that when $v > u$, *PRFs* over $\mathcal{P}^1(\mathbb{F}_q)$ can be viewed as permutations of \mathbb{F}_q by eliminating ∞ from the domain.

Example. Let $V(x) = x^3 + x$ and $U(x) = x^2 + 5$ be polynomials over \mathbb{F}_7 , where our computations are based on the primitive polynomial $x + 4$. Observe that $V(0) = 0, V(1) = 3, V(2) = 3, V(3) = 2, V(4) = 6, V(5) = 6, V(6) = 5$ and $U(0) = 5, U(1) = 6, U(2) = 4, U(3) = 1, U(4) = 6, U(5) = 4, U(6) = 1$. Let $\mathcal{W}(x)$ be the rational function defined by $\mathcal{W}(x) = V(x)/U(x) = (x^3+x)/(x^2+5)$. Then

$$\mathcal{W}(x) = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & \infty \\ 0 & \frac{3}{5} & \frac{3}{4} & \frac{2}{1} & \frac{6}{6} & \frac{6}{4} & \frac{5}{1} & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & \infty \\ 0 & 4 & 6 & 2 & 1 & 3 & 5 & \infty \end{pmatrix}.$$

Clearly $\mathcal{W}(x)$ is a permutation of the elements of $\mathcal{P}^1(\mathbb{F}_7)$. Hence $\mathcal{W}(x)$ is a *PRF*. Observe also that when $\mathcal{W}(x)$ is restricted to \mathbb{F}_7 , the result is a permutation of the elements of \mathbb{F}_7 . Also observe that $\mathcal{W}(1/x)$ is a *PRF*:

$$\mathcal{W}(1/x) = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & \infty \\ \infty & 4 & 5 & 3 & 1 & 2 & 6 & 0 \end{pmatrix}$$

In general, many of the same concepts and techniques discussed for polynomials over finite fields apply to *PRFs*. Let $N_d(q)$ be the number of PPs of degree d over \mathbb{F}_q [17]. We generalize this notion by defining $N_{v,u}(q)$ for *PRFs*.

Definition 2. $N_{v,u}(q)$ is the number of *PRFs* $V(x)/U(x)$, where $V(x)$ has degree v , and $U(x)$ has degree u .

Note that $N_d(q)$ is the same as $N_{d,0}(q)$. Note also that $N_{u,v}(q) = N_{v,u}(q)$, because $\frac{V(x)}{U(x)}$ is a *PRF* if and only if $\frac{U(x)}{V(x)}$ is also a *PRF*. That is, if (a_0, a_1, \dots, a_q) is a permutation of $P^1(\mathbb{F}_q)$, then $(a_0^{-1}, a_1^{-1}, \dots, a_q^{-1})$ is also a permutation of $P^1(\mathbb{F}_q)$.

We compute values of $N_{v,u}(q)$, for many values of v , u and q , and use the computed values to give significantly improved lower bounds for $M(q, D)$ and $M(q+1, D)$. We show that the Hamming distance between permutations defined by *PRFs*, $\frac{V(x)}{U(x)}$ and $\frac{R(x)}{S(x)}$, where $V(x)$ is of degree v , $U(x)$ is of degree u , $R(x)$ is of degree r , and $S(x)$ is of degree s , is at least $q - \max\{v + s, u + r\}$. In this paper we focus on *PRFs* with numerators of degree v and denominators of degree either v or $v - 1$; however, $N_{v,u}(q)$ is computed also for other pairs of v, u for the sake of computing $M(q, D)$.

Definition 3. Define $\mathcal{T}_d(q) = \sum_{v,u} N_{v,u}(q)$, for all $v, u \leq (d + 1)/2$.

We obtain improved lower bounds for $M(q, q - d)$ and $M(q + 1, q - d)$ by showing that $M(q + 1, q - d) \geq \mathcal{T}_d(q)$. In addition, by computation, we show that:

$$\begin{aligned} N_{4,3}(q) &= (q + 1)q^2(q - 1)^2/3, \quad q \leq 307, \\ N_{5,4}(q) &> (q + 1)q^3(q - 1)^2/2, \quad q \leq 97, \text{ and} \\ N_{4,4}(q) &= (q + 1)q^2(q - 1)^3/3, \text{ for odd } q \leq 307. \end{aligned}$$

Based on our experimental evidence, we conjecture that these formulas are valid for all prime powers q . We have also computed $N_{3,2}(q)$ and $N_{3,3}(q)$, not included in the above list as Ferraguti *et al.* [11], described all *PRFs* of degree 3. However, we do use the results for degree 3 *PRFs* to give improved lower bounds for $M(q, q - d)$ and $M(q + 1, q - d)$ for $d \in \{5, 7, 9\}$.

Our paper is organized as follows. In Sect. 2 we discuss Hamming distance properties of *PRFs*, and give proofs of our new lower bounds for $M(q, q - d)$ and $M(q + 1, q - d)$. In Sect. 3 we consider various forms of normalization that are useful for speeding up the search for *PRFs*. In Sect. 4 we discuss functions that map *PRFs* into *PRFs* that are also useful for speeding up our computations. In Sect. 5 we give formulas and compute values for $N_{4,3}(q)$, $N_{4,4}(q)$, and $N_{5,4}(q)$. The formulas are verified computationally and conjectured to be valid for all prime powers q . In Tables 3 and 5, we list new results, derived from *PRFs*, for $M(q, D)$, for various q and D . Table 3 shows new results for $M(q, q - 5)$ and $M(q, q - 7)$, for $16 \leq q \leq 149$. Table 4 shows new results for $N_{5,4}(q)$ and values obtained by our formula given in Conjecture 2 (our 5/4 conjecture). Table 5

shows new results for $M(q, q - 9)$, for $13 \leq q \leq 97$. Tables 6 and 7 give new results for $M(q + 1, q - 5)$ and $M(q + 1, q - 7)$, respectively. We have improved lower bounds for $M(q, D)$ for several other values of q and D , but they are not included here due to space restrictions.

Notation. We use the following notation throughout this paper. \mathbb{F}_q is a finite field where $q = p^m$ for some $m \geq 1$. We use the convention that t denotes a generator of the group of non-zero elements of \mathbb{F}_q . Using this notation, the elements of \mathbb{F}_q are $0, t^0 = 1, t^1 = 2, \dots, t^{q-2} = q - 1$. Lidl and Niederreiter [18] give this as one way to represent the elements of a finite field. Another representation lists the elements of \mathbb{F}_{p^m} by degree m polynomials with coefficients from \mathbb{F}_p . *PRFs* can easily be converted from one notation to the other. As a primitive polynomial is needed to do the appropriate arithmetic, we give explicit primitive polynomials for our computations and results. For notational clarity, we let V, U, R and S denote polynomials of degree v, u, r and s , with coefficients a_i, b_i, c_i and d_i respectively, That is, $V(x) = \sum_{i=0}^v a_i x^i, U(x) = \sum_{i=0}^u b_i x^i, R(x) = \sum_{i=0}^r c_i x^i,$ and $S(x) = \sum_{i=0}^s d_i x^i,$ Lastly, we let $\mathcal{W}, \mathcal{Y},$ and \mathcal{Z} denote *PRFs*. So if $\mathcal{W}(x) = \frac{V(x)}{U(x)},$ then $\mathcal{W}(x) = \sum_{i=0}^v a_i x^i / \sum_{i=0}^u b_i x^i.$

2 Hamming Distance of *PRFs*

Recall that by Definition 1, $\gcd(V(x), U(x)) = 1$ for any *PRF*. This property is implicit in our counting arguments for *PRFs*. For example, see Corollary 5 and Corollary 7.

We now discuss properties of *PRFs* that are useful for improving lower bounds for $M(q, D)$ and $M(q + 1, D)$. Some similar ideas were given in [23]. For the proofs in this section, we consider the *PRFs* $\mathcal{W}(x) = \frac{V(x)}{U(x)}$ and $\mathcal{Y}(x) = \frac{R(x)}{S(x)}$ that permute the elements of $\mathcal{P}^1(\mathbb{F}_q)$ such that $V(x)S(x) - U(x)R(x)$ is not a constant. For this discussion, the degrees of the *PRFs* need not be the same.

Theorem 4. *Let $v + s \leq d$ and $u + r \leq d,$ for some $d.$ Let π and σ be the permutations of $\mathcal{P}^1(\mathbb{F}_q)$ generated by $\mathcal{W}(x)$ and $\mathcal{Y}(x)$ respectively. Then $hd(\pi, \sigma) \geq q - d.$*

Proof. We consider the values of the *PRFs* for elements of $\mathbb{F}_q,$ and simultaneously note that $\frac{V(\infty)}{U(\infty)}$ and $\frac{R(\infty)}{S(\infty)}$ may be the same. Assume that for some $a \in \mathbb{F}_q, \frac{V(a)}{U(a)} = \frac{R(a)}{S(a)}.$ Then $V(a)S(a) = U(a)R(a),$ so $V(a)S(a) - U(a)R(a) = 0.$ Observe that $V(x)S(x)$ and $U(x)R(x)$ are polynomials of degree $v + s \leq d$ and $u + r \leq d,$ respectively. Hence, $V(x)S(x) - U(x)R(x)$ is a polynomial of degree at most d and has at most d roots. That is, there are at most d values $a \in \mathbb{F}_q$ such that $V(a)S(a) - U(a)R(a) = 0.$ Note also that if $\frac{V(a)}{U(a)} = \frac{R(a)}{S(a)} = \infty,$ then $U(a) = S(a) = 0.$ So, $V(a)S(a) - U(a)R(a) = 0,$ and a is a root. This means that $\frac{V(a)}{U(a)} = \frac{R(a)}{S(a)}$ for at most d values $a \in \mathbb{F}_q.$ By including the values of the *PRFs* at $\infty,$ there may be $d + 1$ agreements. Thus, there are at least $q + 1 - (d + 1) = q - d$ disagreements. Hence, $hd(\pi, \sigma) \geq q - d.$ □

It follows also that the permutations corresponding to different *PRFs* are different, because the permutations have non-trivial Hamming distance.

Corollary 5. $M(q + 1, q - d) \geq \mathcal{T}_d(q)$.

Proof. Let $v, u, r, s \leq (d + 1)/2$, and consider any pair of distinct *PRFs* $\mathcal{W}(x) = \frac{V(x)}{U(x)}$ and $\mathcal{Y}(x) = \frac{R(x)}{S(x)}$. Observe that, by Eq. 3, $\mathcal{W}(\infty) = \frac{a_v}{b_u} \in \mathbb{F}_q \setminus \{0\}$ if and only if $v = u$, and $\mathcal{Y}(\infty) = \frac{c_r}{d_s} \in \mathbb{F}_q \setminus \{0\}$ if and only if $r = s$.

Case 1. $v = u = r = s$.

For Case 1, observe that $\mathcal{W}(\infty) = \mathcal{Y}(\infty)$ if and only if the ratios of the high order coefficients in the numerator and denominator are the same in $\mathcal{W}(x)$ and $\mathcal{Y}(x)$. That is, $\mathcal{W}(\infty) = \mathcal{Y}(\infty)$ if and only if $a_v/b_u = c_r/d_s$. Call this property (=). Observe that the coefficients of the high order terms in the polynomials $V(x)S(x)$ and $U(x)R(x)$ are $a_v d_s x^{v+s}$ and $b_u c_r x^{u+r}$, respectively, where $v + s = u + r$. So the high order term of the polynomial $V(x)S(x) - U(x)R(x)$ is $(a_v d_s - b_u c_r)x^{v+s}$. If (=) is true, then the polynomial $V(x)S(x) - U(x)R(x)$ is of degree at most d , not $d + 1$, since the high order terms, if they are of the same degree, disappear through subtraction. It follows that, if $\mathcal{W}(x)$ and $\mathcal{Y}(x)$ have the same value at ∞ , then there are at most d agreements when $x \in \mathbb{F}_q$, hence, at most $d + 1$ agreements counting the agreement at infinity. On the other hand, if (=) is not true, then the polynomial $V(x)S(x) - U(x)R(x)$ is of degree at most at $d + 1$, so it too has at most $d + 1$ agreements. Either way, the permutations defined by these *PRFs* have Hamming distance at least $q + 1 - (d + 1) = q - d$.

Case 2. $v = u$ and $r > s$.

It follows that $\mathcal{W}(\infty) \in F_q \setminus \{0\}$ and $\mathcal{Y}(\infty) = \infty$, so $\mathcal{W}(\infty) \neq \mathcal{Y}(\infty)$. Furthermore, $V(x)S(x) - U(x)R(x)$ is of degree at most $d + 1$, so it has at most $d + 1$ roots. That is, there are at most $d + 1$ values $a \in F_q$ such that $\mathcal{W}(a) = \mathcal{Y}(a)$. Consequently, there are at least $q + 1 - (d + 1) = q - d$ positions b where $\mathcal{W}(b) \neq \mathcal{Y}(b)$. So, the permutations defined by these *PRFs* have Hamming distance at least $q - d$.

Case 3. $v = u$ and $r < s$.

This is similar to Case 2. The difference is that $\mathcal{Y}(\infty) = 0$.

Case 4. $v < u$ and $r > s$.

This is similar to Case 2. The difference is that $\mathcal{W}(\infty) = 0$.

Case 5. $v < u$ and $r < s$.

It follows that $\mathcal{W}(\infty) = \mathcal{Y}(\infty) = 0$. Since, $V(x)S(x) - U(x)R(x)$ is of degree at most d , it has at most d roots. Hence, there are at most d values $a \in F_q$ such that $\mathcal{W}(a) = \mathcal{Y}(a)$, and counting the agreement at infinity, the result is a total of $d + 1$ agreements. That is, at least $q + 1 - (d + 1) = q - d$ positions b where $\mathcal{W}(b) \neq \mathcal{Y}(b)$. So, the permutations defined by these *PRFs* have Hamming distance at least $q - d$. □

Definition 6. Define $\mathcal{S}_d(q) = N_{t,t}(q)/(q - 1) + \sum_{v,u} N_{v,u}(q)$, where $t = (d - 3)/2$, and in the sum, v and u are evaluated as

$$v, u = \begin{cases} v \leq (d + 1)/2, u \leq (d - 1)/2 & \text{when } v > u, \\ v \leq (d - 1)/2, u \leq (d - 3)/2 & \text{when } v < u, \\ u, v \leq (d - 5)/2 & \text{when } v = u. \end{cases}$$

Corollary 7. $M(q, q - d) \geq \mathcal{S}_d(q)$.

Proof. Consider the PRRFs $\mathcal{W}(x) = \frac{V(x)}{U(x)}$ and $\mathcal{Y}(x) = \frac{R(x)}{S(x)}$. Observe that by the definition of $\mathcal{S}_d(q)$, the largest values for v and s are $(d + 1)/2$ and $(d - 1)/2$, respectively, and similarly for u and r . Let $v, r \leq (d + 1)/2$ and $u, s \leq (d - 1)/2$. It follows that $V(x)S(x) - U(x)R(x)$ is of degree $\leq d$. As seen in the proof of Theorem 4, this means that permutations defined by $\mathcal{W}(x)$ and $\mathcal{Y}(x)$ have at most d agreements.

As we want to consider permutations on \mathbb{F}_q (not $\mathcal{P}^1(\mathbb{F}_q)$) we need to eliminate occurrences of the symbol ∞ in the permutations corresponding to $\mathcal{W}(x)$ and $Y(x)$ using an operation called *contraction* [1]. If $\mathcal{W}(\infty) = \infty$, then we can simply eliminate the symbol ∞ in the corresponding permutation, which of course makes no new agreements. If $\mathcal{W}(\infty) = a$, with $a \in \mathbb{F}_q$, then we exchange the symbol ∞ wherever it occurs in the permutation with a . This moves the symbol ∞ to the last position in the permutation, so it can be eliminated. One, or at most two, new agreements could be created, the latter situation arising when $v = u$. Consequently, if $\mathcal{W}(\infty) \neq \infty$ (so an exchange with ∞ is required), stronger conditions are needed to ensure that there are a total of at most d agreements. The terms in the sum $\mathcal{S}_d(q)$ are calculated to ensure that the Hamming distance between permutations (after all needed contractions are performed) is at least $q - d$.

We do a proof by cases based on the values of v, u, r, s and t .

Case 1. $v = u = t = (d - 3)/2$.

Suppose that $U(x)$ and $V(x)$ are monic polynomials. Then the related permutations always end with the same symbol, namely 1. Contraction applied to the permutation associated with $\mathcal{W}(x)$ creates at most one new agreement with any other permutation that already has the symbol 1 in the exchanged position. The number of such permutations produced by PRRFs with $U(x)$ and $V(x)$ both monic and both of degree t is $N_{t,t}(q)/(q - 1)$.

Case 2. v and u have their maximum values, and $r = s \leq (d - 5)/2$.

It follows that the polynomial $V(x)S(x) - U(x)R(x)$ has degree at most $d - 2$. Then permutations defined by $\mathcal{W}(x)$ and $\mathcal{Y}(x)$ have at most $d - 2$ agreements. Since contraction creates at most 2 new agreements, it follows that there are at most d agreements. Therefore, the permutations have Hamming distance at least $q - d$.

Case 3. $r \leq v \leq (d + 1)/2$ and $s \leq u \leq (d - 1)/2, v > u$ and $r > s$.

It follows that the polynomial $V(x)S(x) - U(x)R(x)$ has degree at most d , so permutations defined by $\mathcal{W}(x)$ and $\mathcal{Y}(x)$ have at most d agreements. Note that

$\mathcal{W}(\infty) = \infty$ and $\mathcal{Y}(\infty) = \infty$. Hence the permutations defined by $\mathcal{W}(x)$ and $\mathcal{Y}(x)$ make no new agreements through contraction, *i.e.*, the ∞ simply disappears in each permutation. Therefore, the permutations have Hamming distance at least $q - d$.

Case 4. $u < v \leq (d + 1)/2$, and $r < s \leq (d - 3)/2$.

It follows that the polynomial $V(x)S(x) - U(x)R(x)$ has degree $\leq d - 1$, so permutations defined by $\mathcal{W}(x)$ and $\mathcal{Y}(x)$ have at most $d - 1$ agreements. Since $\mathcal{W}(\infty) = \infty$ and $\mathcal{Y}(\infty) = 0$, at most one new agreement is created through contraction. Therefore, the total number of agreements is d , and the permutations have Hamming distance at least $q - d$.

Case 5. $v < u \leq (d - 3)/2$ and $r < s \leq (d - 3)/2$.

It follows that the polynomial $V(x)S(x) - U(x)R(x)$ has degree at most $d - 4$, so permutations defined by $\mathcal{W}(x)$ and $\mathcal{Y}(x)$ have at most $d - 4$ agreements. Contraction of these permutations makes at most 2 new agreements. Therefore, the permutations have Hamming distance at least $q - d$.

Hence the Hamming distance between permutations defined by $\mathcal{W}(x)$ and $\mathcal{Y}(x)$, with the stated numerator/denominator degree bounds given in the sum in the definition of $\mathcal{S}_d(q)$, is at most $q - d$. It follows that total number of permutations on q symbols with pairwise Hamming distance $q - d$ is at least as large as $\mathcal{S}_d(q)$. □

Examples. (Note: Some of the terms in the sums are not shown because they are zero. Also, some terms are written as $2N_{u,v}$ to denote $N_{u,v} + N_{v,u}$ when applicable).

- (a) $M(q, q - 5) : \mathcal{S}_5(q) = N_{3,2}(q) + N_{3,0}(q) + N_{2,0}(q) + N_{1,1}(q)/(q - 1) + 2N_{1,0}(q)$.
- (b) $M(q, q - 7) : \mathcal{S}_7(q) = N_{4,3}(q) + N_{3,2}(q) + N_{4,0}(q) + N_{3,0}(q) + 2N_{2,0}(q) + N_{2,2}(q)/(q - 1) + N_{1,1}(q) + 2N_{1,0}(q)$.
- (c) $M(q, q - 9) : \mathcal{S}_9(q) = N_{5,4}(q) + N_{5,3}(q) + N_{5,0}(q) + N_{4,3}(q) + N_{4,0}(q) + N_{3,3}(q)/(q - 1) + 2N_{3,2}(q) + 2N_{3,0}(q) + N_{2,2}(q) + 2N_{2,0}(q) + N_{1,1}(q) + 2N_{1,0}(q)$.

3 Normalization of PRFs

The goal of normalization is to enable a more efficient search for *PRFs*. That is, normalization indicates that certain coefficients can be fixed at a specified value and a search algorithm need not try all possibilities. Normalization has been discussed previously in the context of PPs [2, 17, 21]. Equivalence relations based on normalization [2] allow partitioning of PPs of degree d in \mathbb{F}_q into equivalence classes, each represented by a *normalized permutation polynomial (nPP)*.

We use normalization to map *PRFs* to normalized *PRFs (nPRFs)*. Normalization operations [18], listed in Table 1, are essentially the same for PPs and *PRFs*. We point out a few subtleties that arise due to the presence of a denominator in *PRFs*. Let $a, b, c, r, y, z \in \mathbb{F}_q$. Multiplying a *PRF* $\mathcal{W}(x) = \frac{V(x)}{U(x)}$ by a nonzero constant a is equivalent to multiplying by $a = y/z$, for $y, z \neq 0$. Addition of a constant b to the variable is accomplished by replacing x by $x + b$

Table 1. Normalization operations for PPs and *PRFs* in \mathbb{F}_q .

Normalization operation	For PPs $V(x)$	For <i>PRFs</i> $\mathcal{W}(x) = \frac{V(x)}{U(x)}$
Multiplication by a nonzero constant	$aV(x) : a \in \mathbb{F}_q$	$\frac{yV(x)}{zU(x)} : y, z \in \mathbb{F}_q$
Addition to the variable	$V(x + b) : b \in \mathbb{F}_q$	$\frac{V(x+b)}{U(x+b)} : b \in \mathbb{F}_q$
Addition of a constant	$V(x) + c : c \in \mathbb{F}_q$	$\frac{V(x)+cU(x)}{U(x)} : c \in \mathbb{F}_q$
Multiplication of the variable by a constant	$V(rx) : r \in \mathbb{F}_q$	$\frac{V(rx)}{U(rx)} : r \in \mathbb{F}_q$

in both numerator and denominator. Adding a constant c to $\mathcal{W}(x)$ equates to computing $\frac{V(x)}{U(x)} + c = \frac{V(x)+cU(x)}{U(x)}$. Multiplication of the variable by a constant is accomplished by replacing the argument x by rx , for some constant $r \neq 0$. Note that if $\mathcal{W}(x)$ permutes the elements of $\mathcal{P}^1(\mathbb{F}_q)$, then so does $\mathcal{W}(rx)$. That is, if $\mathcal{W}(x)$ is a *PRF*, then $\mathcal{W}(rx)$ is also a *PRF*. In fact, all of the normalization operations in Table 1 map *PRFs* to *PRFs*.

We now discuss the usage of these operations to map *PRFs* to *nPRFs*. In Table 2 we define three types of normalized *PRFs* and list the restrictions on each. The definitions are modeled after the definitions of normalization of PPs which are described in [2]. Note that normalization of *PRFs* fixes four coefficients: a_v and b_u both have the value 1, a_0 is 0, and an additional coefficient, determined by the type of normalization, is zero. In the sections that follow, we prove that almost all *PRFs* can be normalized. As explained earlier, this is useful for an efficient search for *PRFs*. We use the following in our proofs for normalization. Let $a, b, c \in \mathbb{F}_q$, $a \neq 0$, let $x, y \in \mathbb{F}_q \setminus \{0\}$ such that $y/z = a$. Let $\mathcal{Y}(x) = a\mathcal{W}(x + b) + c$. Then

$$\begin{aligned} \mathcal{Y}(x) &= a\mathcal{W}(x + b) + c = \frac{yV(x + b)}{zU(x + b)} + \frac{czU(x + b)}{zU(x + b)} \\ &= \frac{yV(x + b) + czU(x + b)}{zU(x + b)} = \frac{V'(x)}{U'(x)}, \text{ where} \end{aligned}$$

$$\begin{aligned} V'(x) &= yV(x + b) + cU'(x) \\ &= (ya_v(x + b)^v + ya_{v-1}(x + b)^{v-1} + \dots + ya_1(x + b) + ya_0) \\ &\quad + (czb_u(x + b)^u + czb_{u-1}(x + b)^{u-1} + \dots + czb_1(x + b) + czb_0), \end{aligned} \tag{4}$$

and

$$U'(x) = zU(x + b) = zb_u(x + b)^u + zb_{u-1}(x + b)^{u-1} + \dots + zb_0. \tag{5}$$

3.1 C-Normalization

As seen in Table 2, c-normalization applies to *PRFs* when the field characteristic p does not divide the degree of the denominator. We use *nPRFs* to define an equivalence relation on *PRFs* as follows:

Table 2. Types of normalization for *PRFs* $\mathcal{W}(x) = \frac{V(x)}{U(x)}$, where $V(x) = \sum_{i=0}^v a_i x^i$ and $U(x) = \sum_{i=0}^u b_i x^i$, with field characteristic p . The degrees of $V(x)$ and $U(x)$ are v and u , respectively.

Normalization type	Degree restriction	<i>nPRF</i> properties
<i>c-normalization</i>	$p \nmid u$ $v > u$	$V(x)$ and $U(x)$ are monic, $V(0) = 0$, and $b_{u-1} = 0$
<i>m-normalization</i>	$p \mid u$ and $p > 2$ $v > u$	$V(x)$ and $U(x)$ are monic, $V(0) = 0$, and in $U(x)$, either $b_{u-1} = 0$ or $b_{u-2} = 0$
<i>b-normalization</i>	$p \mid u$ and $p = 2$ $v > u$	$V(x)$ and $U(x)$ are monic, $V(0) = 0$, and if $2^i \leq u \leq 2^{i+1} - 3$ for some i , then either $b_r = 0$ or $b_{r-1} = 0$, where $r = 2^i - 1$

Definition 8. Let $\mathcal{W}(x) = \frac{V(x)}{U(x)}$ and $\mathcal{Y}(x) = \frac{R(x)}{S(x)}$ be *PRFs*. We say that $\mathcal{W}(x)$ and $\mathcal{Y}(x)$ are related by \mathcal{R}_c if there is a sequence of the first three normalization operations in Table 1 that converts $\mathcal{W}(x)$ into $\mathcal{Y}(x)$.

It is easily seen that \mathcal{R}_c is an equivalence relation on *PRFs*. That is, observe that each of the three operations has an inverse. For example, the inverse of multiplying by a is multiplying by the inverse of a . So, $\mathcal{W}(x)$ is related to itself by the empty sequence of operations. If $\mathcal{W}(x)$ and $\mathcal{Y}(x)$ are \mathcal{R}_c related, then there is some sequence that transforms $\mathcal{W}(x)$ into $\mathcal{Y}(x)$. A sequence formed by taking the inverse of each operation in backwards order transforms $\mathcal{Y}(x)$ into $\mathcal{W}(x)$. So, $\mathcal{Y}(x)$ and $\mathcal{W}(x)$ are also \mathcal{R}_c related. That is, \mathcal{R}_c is symmetric. Finally, if there is a sequence of operations that transforms $\mathcal{W}(x)$ into $\mathcal{Y}(x)$ and a sequence that transforms $\mathcal{Y}(x)$ into $\frac{P(x)}{Q(x)}$, then a concatenation of these sequences transforms $\mathcal{W}(x)$ into $\frac{P(x)}{Q(x)}$. So, \mathcal{R}_c is transitive.

The equivalence class under the relation \mathcal{R}_c containing $\mathcal{W}(x)$, denoted by $[\mathcal{W}]$, is the set

$$\begin{aligned}
 [\mathcal{W}] &= \{a\mathcal{W}(x + b) + c \mid a, b, c \in \mathbb{F}_q \text{ and } a \neq 0\} \\
 &= \left\{a \frac{V(x + b)}{U(x + b)} + c \mid a, b, c \in \mathbb{F}_q \text{ and } a \neq 0\right\}.
 \end{aligned}$$

We show that $[\mathcal{W}]$ contains exactly $q^2(q - 1)$ *PRFs*. Theorem 9 below is nearly identical to one proved (for PPs) in [2].

Theorem 9 [2]. Let $\mathcal{W}(x) = \frac{V(x)}{U(x)}$ be a *PRF* with $v > u$. Then there is a unique triple (a, b, c) such that $\mathcal{Y}(x) = a\mathcal{W}(x + b) + c = \frac{V'(x)}{U'(x)}$ is *c-normalized*.

Lemma 10. All $q^2(q - 1)$ *PRFs* in $[\mathcal{W}]$ are different.

Proof. Let $\mathcal{Y}(x) \in [\mathcal{W}]$ be a *PRF* that is not normalized, and let $\mathcal{W}(x)$ be the *nPRF* that represents $[\mathcal{W}]$. That is, let $\mathcal{Y}(x) = a\mathcal{W}(x + b) + c$. We compute the

triple (a', b', c') such that $\mathcal{Y}'(x) = a'\mathcal{Y}(x + b') + c'$ is normalized as follows.

$$\begin{aligned} \mathcal{Y}'(x) &= a'\mathcal{Y}(x + b') + c' = a'(a\mathcal{W}(x + b) + b') + c + c' \\ &= a'a\mathcal{W}(x + (b + b')) + a'c + c' = \mathcal{W}(x), \end{aligned}$$

where the last equality is achieved by letting $a' = a^{-1}$, $b' = -b$, and $c' = -(a'c)$. By Theorem 9, the triple (a', b', c') is unique for normalizing the specific *PRF* $\mathcal{Y}(x)$. By the uniqueness properties of inverses in a field, a , b and c are unique as well. Thus each triple in the set $\{(a, b, c) \mid a, b, c \in \mathbb{F}_q \text{ and } a \neq 0\}$ is unique. Since there are $q^2(q - 1)$ such triples, the claim follows. \square

Note that Theorem 9 implies that each equivalence class of \mathcal{R}_c contains one and only one *nPRF*. By Lemma 10, each equivalence class contains exactly $q^2(q - 1)$ members (including the representative *nPRF*). Equivalence classes by definition are disjoint, so, if the number of *nPRFs* is k , there are $kq^2(q - 1)$ *PRFs*. Note that *c*-normalization indicates that we can fix four coefficients, namely the first coefficient of both $V(x)$ and $U(x)$, the second coefficient of $U(x)$, and the last coefficient of $V(x)$. There are, in general, q possible values for each coefficient. Furthermore, $V(x)$ and $U(x)$ are of degrees v and u , respectively, so there are $v + u + 2$ coefficients altogether. This means a naive search program (which exhaustively tries all combinations of coefficients) needs to examine q^{u+v+2} rational functions. Normalization allows the number to be reduced to q^{u+v-2} .

3.2 M-Normalization

As seen in Table 2, *m*-normalization is used when $p \mid u$ and $p \neq 2$. See Eqs. 4 and 5 for the definitions of $V'(x)$ and $U'(x)$.

Theorem 11. *Let $v, u \in \mathbb{F}_{p^m}$, where $v > u$ and $p \mid u$ and $p \neq 2$. Any *PRF* $\mathcal{W}(x) = \frac{V(x)}{U(x)}$ can be transformed to an *m*-normalized *PRF* $\mathcal{Y}(x) = \frac{V'(x)}{U'(x)}$ by the normalization operations.*

Proof. For *m*-normalization, we need to show that

- (A) either the coefficient of x^{u-1} , or the coefficient of x^{u-2} in $U'(x)$ is zero,
- (B) $U'(x)$ is monic,
- (C) $V'(x)$ is monic, and
- (D) $V'(0)$, the constant term of $V'(x)$, is zero.

To show that (A) holds, we must show that either $zb_{u-1} = 0$ or $zb_{u-2} = 0$.

Case 1. $b_{u-1} = 0$. So, $zb_{u-1} = 0$.

Case 2. $b_{u-1} \neq 0$. Consider zb_{u-2} in $U'(x)$. Since u is a multiple of p , the expansion of $(x + b)^u$ will derive nonzero coefficients only for terms whose degrees are multiples of p . Since $p > 2$, this means that $p \nmid (u - 2)$, so $(x + b)^u$ will have a coefficient of 0 for the degree $u - 2$ term. Hence b_{u-2} is calculated solely by the expansion of $(x + b)^{u-1}$ and $(x + b)^{u-2}$.

The expansion of $(x+b)^{u-1}$ will produce a term of degree $u-2$ with coefficient $zb_{u-1}b'$ where $b' = \sum_1^{u-1} b$. The expansion of $(x+b)^{u-2}$ will produce a term of degree $u-2$ with coefficient zb_{u-2} . Therefore the coefficient of x^{u-2} in $U'(x)$ is $zb_{u-1}b' + zb_{u-2} = z(b_{u-1}b' + b_{u-2})$, which is zero if $b_{u-1}b' + b_{u-2} = 0$. Since $b_{u-1} \neq 0$, and $u-1$ is not a multiple of p , we can choose b such that b' is the additive inverse of b_{u-2}/b_{u-1} , making the coefficient of x^{u-2} in $U'(x)$ equal to zero.

It follows that, in $U'(x)$, either $b_{u-1} = 0$ or $b_{u-2} = 0$, so (A) holds.

To show that (B) holds, observe that the degree u term of $U'(x)$ has the coefficient zb_u . If we choose z to be the multiplicative inverse of b_u , then $U'(x)$ will be monic. To show that (C) holds, observe that every term in $U'(x)$ has smaller degree than v . Hence none of them affect the coefficient of degree v term in $V'(x)$. This means that the coefficient of x^v term of $V'(x)$ is ya_v . Since $a_v \neq 0$, we choose $y = a_v^{-1}$, making $V'(x)$ monic. To show that (D) holds, observe that the coefficient of x^0 in $V'(x)$ is $y \sum_{j=0}^v a_j b^j + cz \sum_{j=0}^u b_j b^j$. We choose c to be $(-y \sum_{j=0}^v a_j b^j) / (z \sum_{j=0}^u b_j b^j)$, making the coefficient of x^0 in $V'(x)$ equal to zero.

It follows that $\mathcal{Y}(x)$ is m-normalized. □

3.3 B-Normalization

In this section, we consider the remaining case, namely, $p \mid u$ and $p = 2$, and show that *b-normalization* can be achieved except when $u = 2^i - 2$, for some $i \geq 2$.

We begin with a brief description of the Gap Lemma for polynomials (Lemma 12 below), and its application for normalization of polynomials (Lemma 13 below). Both were proven in [2]. We use these lemmas in the proof of Theorem 14 which describes b-normalization for *PRFs*.

We say that the integer interval $[r, s]$ has a $[t, w]$ gap, if for all $d \in [r, s]$, the expansion of $(x+b)^d$, does not include any nonzero x^e monomials, where $e \in [t, w]$.

Lemma 12 [Gap Lemma [2]]. *For all $i > 1$, the expansion of $(x+b)^d$, for $d \in [2^i, 2^{i+1} - 3]$, has a $[2^i - 2, 2^i - 1]$ gap.*

Lemma 13 [2]. *Let $i > 1$, $m > 2$ and let $d \in [2^i, 2^{i+1} - 3]$ be even. For any PP $P(x)$ over \mathbb{F}_{2^m} , there is a constant b in \mathbb{F}_{2^m} such that in the PP $P(x+b)$, either the x^{2^i-1} term or the x^{2^i-2} term is zero.*

For example, let $d = 2^3$, and let $P(x) = a_8x^8 + a_7x^7 + a_6x^6 + \dots + a_1x + a_0$. Adding b to the argument gives:

$$\begin{aligned} P(x+b) &= a_8(x+b)^8 + a_7(x+b)^7 + a_6(x+b)^6 + \dots + a_1x + a_0 \\ &= a_8(x^8 + b^8) + a_7(x^7 + bx^6 + b^2x^5 + \dots) + a_6(x^6 + b^2x^4 + \dots) + \dots \\ &= a_8x^8 + a_8b^8 + (a_7x^7 + a_7bx^6 + \dots) + (a_6x^6 + a_6b^2x^4 + \dots) + \dots \end{aligned}$$

We want to solve for the value of b that makes the coefficient of the x^6 term of $P(x + b)$ zero. So $a_7bx^6 + a_6x^6 = 0$ is satisfied by $b = -a_7/a_6$.

We now use Lemma 13 in our proof that certain *PRFs* can be b -normalized.

Theorem 14. Any *PRF* $\frac{V(x)}{U(x)}$ in \mathbb{F}_{2^m} with $v > u, m > 2$, and $2 \mid u$, can be transformed to a b -normalized *PRF* $\frac{V'(x)}{U'(x)}$ by the normalization operations, except when $u = 2^i - 2$, for some $i \geq 2$.

Proof. See Eqs. 4 and 5 for the definitions of $V'(x)$ and $U'(x)$. Observe first that the degree u term of $U'(x)$ has the coefficient zb_u . Noting that $b_u \neq 0$, we choose $z = b_u^{-1}$, making $U'(x)$ monic. Observe further that every term in $U'(x)$ has smaller degree than v . Hence none of them affect the coefficient of degree v term in $V'(x)$. This means that the coefficient of x^v term of $V'(x)$ is ya_v . Noting that $a_v \neq 0$, we choose $y = a_v^{-1}$, making $V'(x)$ monic. To see that $V'(0) = 0$, observe that the coefficient of x^0 in $V'(x)$ is $y \sum_{j=0}^v a_j b^j + cz \sum_{j=0}^u b_j b^j$. We choose c to be $(-y \sum_{j=0}^v a_j b^j) / (z \sum_{j=0}^u b_j b^j)$, making the coefficient of x^0 in $V'(x)$ equal to zero. Finally, by Lemma 13, there is a b such that in $U'(x)$, the coefficient of either the degree $2^i - 1$ term or degree $2^i - 2$ term equal to 0, except when $u = 2^i - 2$, for some $i \geq 2$. Hence $\frac{V'(x)}{U'(x)}$ is b -normalized. \square

4 Mapping *nPRFs* to *nPRFs*

We are interested in methods to optimize the search for *PRFs*. In [2] we described several operations on permutation polynomials that allow certain coefficients of PPs to be fixed, making the search space smaller. These operations include normalization and the *F-map* and the *G-map*. The *F-map* allows an additional coefficient to be fixed. The *G-map* partitions *nPRFs* into disjoint cycles, and each cycle can be described by a representative *nPRF*. We show that the *F-map* and the *G-map* can be extended to *nPRFs*, allowing again faster searches.

Definition 15. Define the *F-map* on a polynomial $V(x)$ over \mathbb{F}_q [2] by

$$F(V(x)) = t^0 a_v x^v + t^1 a_{v-1} x^{v-1} + \dots + t^{v-1} a_1 x + t^v a_0.$$

Define the *F-map* on a *PRF* $\mathcal{W}(x) = V(x)/U(x)$ over \mathbb{F}_q by

$$F(\mathcal{W}(x)) = \frac{F(V(x))}{F(U(x))} = \frac{t^0 a_v x^v + t^1 a_{v-1} x^{v-1} + \dots + t^{v-1} a_1 x + t^v a_0}{t^0 b_u x^u + t^1 b_{u-1} x^{u-1} + \dots + t^{u-1} b_1 x + t^u b_0}. \tag{6}$$

It is shown in [2] that $F(V(x)) = t^v V(x/t)$. So for a *PRF* $\mathcal{W}(x)$, we have

$$F(\mathcal{W}(x)) = \mathcal{W}'(x) = \frac{t^v V(x/t)}{t^u U(x/t)} = \frac{t^{v-u} V(x/t)}{U(x/t)} = t^{v-u} \mathcal{W}(x/t).$$

Thus, if $\mathcal{W}(x)$ is a *PRF*, then so is $\mathcal{W}'(x) = t^{v-u} \mathcal{W}(x/t)$. That is, if $\mathcal{W}(x)$ permutes the elements of $\mathcal{P}^1(\mathbb{F}_q)$, then so does $\mathcal{W}'(x)$. Consequently, the *F-map*

maps *PRFs* to *PRFs*. In fact, referring to Eq. 6, we see that the *F*-map maps *nPRFs* to *nPRFs*, as the first coefficients of both numerator and denominator map to themselves, and any zero coefficient is mapped to itself.

We use the *F*-map to fix an additional coefficient in a *PRF*, resulting in a total of 5 fixed coefficients for each *nPRF*. For example, consider searching for *nPRFs* of the form $\mathcal{W}(x) = \frac{V(x)}{U(x)}$. By the definition of normalization, $V(x)$ and $U(x)$ are monic, the coefficient of x^0 in $V(x)$ is zero, and one other coefficient in $U(x)$ is zero, as determined by the type of normalization. Using the *F*-map, the coefficient of x^{v-1} in $V(x)$ can also be fixed to either 0 or 1. That is, if the coefficient of x^{v-1} is not zero, then consider the cycle, $V(x), F(V(x)), F^2(V(x)), \dots, F^i(V(x)), \dots$. By the definition of the *F*-map, the coefficient of x^{v-1} in $F^i(V(x))$ is $t^i a_{v-1}$, and for some i , $t^i a_{v-1} = 1$. Thus, if $\frac{V(x)}{U(x)}$ is an *nPRF* and the coefficient of x^{v-1} in $V(x)$ is nonzero and is not equal to 1, then there is also an *nPRF* where the coefficient of x^{v-1} in $V(x)$ is equal to 1. We now discuss the *G*-map [2] and how it can be applied to *PRFs*. The *G*-map raises each coefficient in a polynomial to the p -th power, where p is the field characteristic.

Definition 16. Define the **G-map on polynomials** [2] over \mathbb{F}_q by

$$G(V(x)) = a_v^p x^v + a_{v-1}^p x^{v-1} + \dots + a_1^p x + a_0^p$$

Define the **G-map on PRFs** over \mathbb{F}_q by

$$G(\mathcal{W}(x)) = \frac{G(V(x))}{G(U(x))} = \frac{a_v^p x^v + a_{v-1}^p x^{v-1} + \dots + a_1^p x + a_0^p}{b_u^p x^u + b_{u-1}^p x^{u-1} + \dots + b_1^p x + b_0^p}.$$

It is shown in [2] that, if $V(x)$ is a PP (nPP), then $G(V(x))$ is a PP (nPP), and that $G(V(x^p)) = V(x)^p$. Similarly,

$$G(\mathcal{W}(x^p)) = \frac{G(V(x^p))}{G(U(x^p))} = \frac{V(x)^p}{U(x)^p} = \mathcal{W}(x)^p.$$

Consequently, if $\mathcal{W}(x)$ is a *PRF*, then $G(\mathcal{W}(x))$ is a *PRF*. That is, $(0^p, 1^p, \dots, (q-1)^p, \infty^p)$ is a permutation of $P^1(\mathbb{F}_q)$, and, if $\mathcal{W}(x)$ is a *PRF*, then $\mathcal{W}(x)^p$ is a *PRF*. This follows from the fact that $(x+y)^p = x^p + y^p$, when p is the characteristic of the field.

Iterating the *G*-map gives a cycle based on orbits of elements in \mathbb{F}_q . For example, consider the field \mathbb{F}_{23} , when defined by the primitive polynomial $x^3 + x^2 + 1$, and the *PRF* $W(x) = \frac{x^3 + x^2 + 2x}{x^2 + 4x + 1}$. We have $G(W(x)) = \frac{x^3 + x^2 + 3x}{x^2 + 7x + 1}$, $G^2(W(x)) = \frac{x^3 + x^2 + 5x}{x^2 + 6x + 1}$, $G^3(W(x)) = W(x)$. Consequently, it is not necessary to search separately for cases when the coefficient of x in the numerator is either 3 or 5. It is sufficient to search with the coefficient 2. In general, cycles partition the elements of \mathbb{F}_q into disjoint sets, so for a chosen coefficient, the search can be limited to one value in each set.

5 Results

A basic computational strategy computes $N_{v,u}$ by considering all possible rational functions, $\frac{V(x)}{U(x)}$, where $V(x)$ and $U(x)$ are polynomials of degree v and u , respectively. This entails evaluating q^{u+v+2} different rational functions. We use a more efficient strategy that implements the normalization theorems in Table 1, and the F -map and the G -map described in Sect. 4. This fixes five coefficients, thus requiring at most q^{u+v-3} different rational functions to be evaluated. This computational strategy yields equivalence class representatives, which in turn yield the total number of $PRFs$, as indicated in Sects. 3 and 4. Our results are presented in Tables 3 through 7.

We have found several interesting classes of $PRFs$. Specifically, there are good classes with degree ratios $3/2$, $4/3$, and $5/4$ for $PRFs$ of \mathbb{F}_q , and with degree ratios $3/3$, $4/4$, and $5/5$ for $PRFs$ of $\mathcal{P}^1(\mathbb{F}_q)$. Note that when the degree of the numerator is larger than the degree of the denominator, the permutations of $\mathcal{P}^1(\mathbb{F}_q)$ end with ∞ , and ∞ can just be deleted giving a permutation of \mathbb{F}_q .

Theorem 17 below justifies substantial improvements on lower bounds for $M(q, q - 5)$ and $M(q + 1, q - 5)$, for many prime powers q , as shown in Table 3 and Table 6. As mentioned earlier, Ferraguti *et al.* [11] have recently given a complete characterization of monic degree 3 $PRFs$, which subsumes our results for degree ratios $3/2$ and $3/3$. They gave essentially Theorem 17 based on monic $PRFs$, hence we omit a proof.

Theorem 17. *For all q ,*

$$\begin{aligned} N_{3,2}(q) &= q^2(q - 1)^2/2, \\ N_{3,3}(q) &= q^2(q - 1)^2(q + 1)/2, && \text{if } q \equiv 2 \pmod{3}, \\ N_{3,3}(q) &= q^2(q - 1)^3/2, && \text{if } q \equiv 1 \pmod{3}, \\ N_{3,3}(q) &= (q^4 - q^3 + q^2 - q)/2, && \text{if } q \equiv 0 \pmod{3}. \end{aligned}$$

For degree ratios $4/3$, $4/4$, and $5/4$, the number of $nPRFs$ is also predictable. Formulas for the number of $PRFs$ for ratios $4/3$, $4/4$, and $5/4$ are given in Conjectures 1, 2 and Theorem 18 below. Experimentally, we have verified that $N_{4,3}(q)$ is exactly $(q + 1)q^2(q - 1)^2/3$, for all $q \leq 307$. Again, this justifies substantial improvements on previous lower bounds for $M(q, q - 7)$ for many prime powers q , as shown in Table 3.

Table 3. Lower bounds for $M(q, q - 5)$ and $M(q, q - 7)$ using $\mathcal{S}_5(q)$ and $\mathcal{S}_7(q)$, respectively. Improved bounds are shown in bold. (* see [23]).

q	$M(q, q - 5) \geq$	Previous	$M(q, q - 7) \geq$	Previous
16	29,792	40,320	381,120	1,377,360
17	42,466	83,504	490,960	1,240,320
19	59,546	65,322*	845,766	1,221,624
23	141,220	291,456	2,201,100	10,200,960
25	181,850	192,000	3,316,800	867,000
27	248,562	522,288	4,866,966	1,280,448
29	355,656	58,968	6,971,020	42,033,992
31	435,240	58,968	9,687,810	3,056,919
32	496,000	1,388,800	11,691,712	3,420,416
37	891,108	1,824,480	23,411,232	3,648,348
41	1,416,960	68,880	39,135,320	1,720,944
43	1,636,236	3,341,100	49,547,610	413,280
47	2,445,232	4,879,634	77,330,416	9,655,492
49	2,773,008	117,600	95,081,952	9,433,872
53	3,952,104	7,887,928	140,812,308	15,632,032
59	6,067,206	407,218	240,463,940	12,319,200
61	6,708,780	226,920	283,767,120	13,622,520
64	8,144,640	5,773,824	360,991,078	13,622,032
67	9,790,308	19,854,780	453,303,642	39,705,138
71	12,718,230	357,840	605,882,760	12,355,419
73	13,828,536	28,014,480	695,631,600	56,023,704
79	19,003,608	492,960	1,032,017,922	38,950,002
81	21,280,320	571,704	1,169,529,840	42,787,440
83	23,746,134	47,858,238	1,321,303,228	48,423,136
89	31,390,656	1,401,920	1,872,278,760	63,439,192
97	43,384,604	87,625,920	2,876,904,792	88,529,184
101	52,045,300	1,030,200	3,520,385,300	104,060,300
103	55,209,030	111,458,154	3,881,578,278	222,926,814
107	65,556,760	129,854,358	4,696,631,464	260,934,052
109	69,313,536	1,294,920	5,150,579,616	141,158,052
113	80,112,480	161,604,464	6,166,737,248	163,047,248
121	105,444,240	1,771,440	8,679,213,840	212,601,840
125	122,093,500	123,935,000	10,212,593,500	125,472,500
127	128,064,006	258,112,260	11,053,461,510	258,112,260
128	132,161,280	90,903,592	11,495,251,584	95,861,632
131	145,044,510	2,247,960	12,905,964,110	294,409,790
137	173,612,976	349,704,008	16,142,578,480	701,979,232
139	184,012,926	370,634,604	17,354,972,046	741,250,026
149	243,189,456	6,593,548	24,557,724,656	496,170,000

Conjecture 1. (4/3 - conjecture) For all q , $N_{4,3}(q) = (q + 1)q^2(q - 1)^2/3$.

Conjecture 2. (5/4 - conjecture) $N_{5,4}(q) > (q + 1)q^3(q - 1)^2/2$.

The 5/4-conjecture is true for all $q \leq 97$. $N_{5,4}(q)$ for $q \leq 97$ is shown in Table 4. This justifies substantial improvements on previous lower bounds on $M(q, q - 9)$, which are shown in Table 5. We can show the following.

Table 4. Computed results for $N_{5,4}(q)$ and 5/4-conjectured lower bound.

q	$N_{5,4}(q)$	$(q + 1)q^3(q - 1)^2/2$	q	$N_{5,4}(q)$	$(q + 1)q^3(q - 1)^2/2$
17	16,189,440	11,319,552	53	11,074,291,488	10,869,212,016
19	24,503,958	22,223,160	59	21,084,006,242	20,726,848,680
23	74,762,512	70,665,936	61	25,753,041,000	25,331,079,600
25	125,820,000	117,000,000	64	34,351,091,712	33,814,609,920
27	193,179,168	86,279,912	67	45,315,700,848	44,544,203,352
29	297,858,652	286,814,640	71	64,037,083,250	63,135,500,400
31	444,126,150	428,990,400	73	75,638,717,568	74,616,572,736
32	553,107,456	519,585,792	79	121,523,765,922	119,985,971,040
37	1,280,989,728	1,247,279,472	81	141,192,720,000	139,450,118,400
41	2,373,572,000	2,315,745,600	83	163,422,731,808	161,477,223,096
43	3,157,263,648	3,085,507,656	89	248,458,577,312	245,667,597,120
47	5,384,729,088	5,272,547,232	97	416,397,477,888	412,148,524,032
49	6,917,645,952	6,776,582,400			

Table 5. Lower bounds for $M(q, q - 9)$ using $S_9(q)$. Improved bounds are shown in bold. Previous values are obtained by permutation polynomials, except where indicated: (a, b) = Mathieu group M_{24} and contraction [3], (a, d) = Mathieu group M_{24} and $M(n + 1, d) \geq M(n, d)$, (c) coset search [5].

n	$M(q, q - 9) \geq$	Previous	q	$M(q, n - 9) \geq$	Previous
13	4,926,480	60,635,520 ^(c)	49	6,877,311,504	20,497,680
16	12,629,280	70,804,800 ^(c)	53	11,025,653,600	23,373,636
17	12,342,272	75,176,640 ^(c)	59	20,979,628,398	35,941,256
19	23,218,380	12,421,152	61	25,628,242,320	13,622,520
23	73,414,022	244,823,040 ^(a,b)	64	34,192,366,054	332,236,800
25	121,108,200	244,823,040 ^(a,d)	67	45,036,911,436	39,705,686
27	191,914,893	28,928,802	71	63,766,789,800	605,529,877
29	294,515,648	42,033,992	73	75,367,839,096	56,023,418
31	439,831,410	22,084,310	79	121,056,446,004	38,930,002
32	533,338,880	32,759,808	81	140,641,174,881	3,100,641,122
37	1,274,288,436	3,648,348	83	162,892,864,290	94,909,620
41	2,357,705,000	22,392,560	89	247,603,307,248	125,475,872
43	3,141,656,196	10,125,360	97	415,199,758,776	88,529,184
47	5,359,530,978	42,883,412			

Table 6. Lower bounds for $M(q + 1, q - 5)$ using $\mathcal{T}_5(q)$.

$q + 1$	$M(q + 1, q - 5) \geq$	Previous	$q + 1$	$M(q + 1, q - 5) \geq$	Previous
14	172,536	380,160	50	138,415,200	2,768,309
17	497,730	187,600	54	213,115,968	7,890,428
18	753,984	83,504	60	363,621,720	821,240
20	1,176,480	177,840	62	415,490,520	13,622,520
24	3,363,888	291,456	65	528,877,440	5,515,776
26	4,695,600	218,418	68	665,139,552	19,854,780
28	788,346	522,288	72	914,996,880	28,014,480
30	10,620,960	170,520	74	1,022,533,776	28,014,480
32	13,868,160	1,388,810	80	1,519,302,720	38,930,002
33	17,320,320	1,388,810	82	64,314,000	21,001,679
38	33,760,872	1,824,800	84	1,993,531,848	47,458,238
42	59,374,560	1,419,680	90	2,823,749,280	125,475,872
44	71,835,456	1,632,624	98	4,249,866,432	87,625,920
48	117,163,104	4,879,634			

Table 7. Lower bounds for $M(q + 1, q - 7)$ using $\mathcal{T}_7(q)$.

$q + 1$	$M(q + 1, q - 7) \geq$	Previous	$q + 1$	$M(q + 1, q - 7) \geq$	Previous
14	1,762,488	10,834,560	30	208,424,160	14,326,150
17	6,087,810	6,617,760	32	309,087,360	22,887,424
18	8,744,256	12,421,152	33	375,214,080	14,076,480
20	16,771,680	10,745,640	38	887,754,024	6,529,464
24	52,522,800	244,823,040	42	1,640,859,360	10,125,360
26	85,815,600	9,313,200	44	2,176,677,888	3,341,100
28	129,574,458	10,511,196	48	3,706,982,496	143,116,896

Theorem 18. For any $v > 1$, $N_{v,v}(q) = (q - 1) \sum_{u < v} N_{v,u}(q)$.

We use the $N_{4,4}(q)$ results to obtain improved lower bounds for $M(q + 1, q - 7)$ as shown in Table 7.

Examples of overall results:

(a) $\mathcal{S}_5(23) = N_{3,2}(23) + N_{3,0}(23) + N_{1,1}(23)/22 + 2N_{1,0}(23) = 140,688$. So, $M(23, 18) \geq 140,688$.

(b) $\mathcal{S}_7(23) = N_{4,3}(23) + N_{3,2}(23) + N_{3,0}(23) + N_{2,2}(23)/22 + 2N_{2,0}(23) + N_{1,1}(23) + 2N_{1,0}(23) = 2,201,100$, since $N_{4,3}(23) = 2,048,288$, $N_{3,2}(23) = 128,018$, $N_{3,0}(23) = 11,638$, $N_{1,1}(23) = 12,144$, and $N_{1,0}(23) = 506$. So, $M(23, 16) \geq 2,201,100$.

(c) $N_{5,5}(19) = 446,802,480$. This yields $M(20, 10) \geq N_{5,5}(19) + 2N_{5,4}(19) + 2N_{5,0}(19) + N_{4,4}(19) + 2N_{4,3}(19) + N_{3,3}(19) + 2N_{3,2}(19) + N_{1,1}(19) + 2N_{1,0}(19) = 508,177,876$.

(d) $N_{5,5}(23) = 1,650,664,092$. This yields $M(24,14) \geq N_{5,5}(23) + 2N_{5,4}(23) + 2N_{5,0}(23) + N_{4,4}(23) + 2N_{4,3}(23) + N_{3,3}(23) + 2N_{3,2}(23) + 2N_{3,0}(23) + N_{1,1}(23) + 2N_{1,0}(23) = 1,845,054,112$.

6 Conclusions, Acknowledgments, and Future Work

We have substantially improved many lower bounds for $M(n, D)$. We conjecture that many of our bounds represent formulas that are true for all powers of a prime q . We wish to thank Dr. Carlos Arreche in the Department of Mathematical Sciences at the University of Texas at Dallas for many helpful discussions.

References

1. Berge, S., Levy, A., Sudborough, I.H.: Constructing permutation arrays from groups. *Des. Codes Crypt.* **86**(5), 1095–1111 (2017). <https://doi.org/10.1007/s10623-017-0381-1>
2. Berge, S., Malouf, B., Morales, L., Stanley, T., Sudborough, I.H., Wong, A.: Equivalence relations for computing permutation polynomials. arXiv e-prints [arXiv:1911.12823](https://arxiv.org/abs/1911.12823) (2019)
3. Berge, S., Miller, Z., Mojica, L.G., Morales, L., Sudborough, I.H.: New lower bounds for permutation arrays using contraction. *Des. Codes Crypt.* **87**(9), 2105–2128 (2019). <https://doi.org/10.1007/s10623-019-00607-y>
4. Berge, S., Mojica, L.G., Morales, L., Sudborough, H.: Constructing permutation arrays using partition and extension. *Des. Codes Crypt.* **88**(2), 311–339 (2019). <https://doi.org/10.1007/s10623-019-00684-z>
5. Berge, S., Morales, L., Sudborough, I.H.: Extending permutation arrays: improving MOLs bounds. *Des. Codes Crypt.* **83**(3), 661–683 (2016). <https://doi.org/10.1007/s10623-016-0263-y>
6. Chu, W., Colbourn, C.J., Dukes, P.: Constructions for permutation codes in powerline communications. *Des. Codes Crypt.* **32**(1–3), 51–64 (2004). <https://doi.org/10.1023/b:desi.0000029212.52214.71>
7. Colbourn, C., Kløve, T., Ling, A.C.: Permutation arrays for powerline communication and mutually orthogonal latin squares. *IEEE Trans. Inf. Theory* **50**(6), 1289–1291 (2004). <https://doi.org/10.1109/tit.2004.828150>
8. Fan, X.: A classification of permutation polynomials of degree 7 over finite fields. *Finite Fields Appl.* **59**, 1–21 (2019). <https://doi.org/10.1016/j.ffa.2019.05.001>
9. Fan, X.: Permutation polynomials of degree 8 over finite fields of characteristic 2. *Finite Fields Their Appl.* **64**, 101662 (2020). <https://doi.org/10.1016/j.ffa.2020.101662>
10. Fan, X.: Permutation polynomials of degree 8 over finite fields of odd characteristic. *Bull. Aust. Math. Soc.* **101**(1), 40–55 (2020). <https://doi.org/10.1017/S0004972719000674>
11. Ferraguti, A., Micheli, G.: Full classification of permutation rational functions and complete rational functions of degree three over finite fields. *Des. Codes Crypt.* **88**(5), 867–886 (2020). <https://doi.org/10.1007/s10623-020-00715-0>
12. Gao, F., Yang, Y., Ge, G.: An improvement on the Gilbert-Varshamov bound for permutation codes. *IEEE Trans. Inf. Theory* **59**(5), 3059–3063 (2013). <https://doi.org/10.1109/tit.2013.2237945>

13. Hou, X.: Permutation polynomials over finite fields - a survey of recent advances. *Finite Fields Appl.* **32**, 82–119 (2015). <https://doi.org/10.1016/j.ffa.2014.10.001>
14. Janiszczak, I., Lempken, W., Östergård, P.R.J., Staszewski, R.: Permutation codes invariant under isometries. *Des. Codes Crypt.* **75**(3), 497–507 (2014). <https://doi.org/10.1007/s10623-014-9930-z>
15. Janiszczak, I., Staszewski, R.: Isometry invariant permutation codes and mutually orthogonal latin squares. *J. Combin. Des.* **27**(9), 541–551 (2019). <https://doi.org/10.1002/jcd.21661>
16. Li, J., Chandler, D.B., Xiang, Q.: Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2. *Finite Fields Appl.* **16**, 406–419 (2010). <https://doi.org/10.1016/j.ffa.2010.07.001>
17. Lidl, R., Mullen, G.L.: When does a polynomial over a finite field permute the elements of the fields? II. *Am. Math. Monthly* **100**(1), 71–74 (1993). <https://doi.org/10.1080/00029890.1993.11990369>
18. Lidl, R., Niederreiter, H.: *Introduction to Finite Fields and Their Applications*. Cambridge University Press, Cambridge (1994). <https://doi.org/10.1017/cbo9781139172769>. Revised edn.
19. Micheli, G., Neri, A.: New lower bounds for permutation codes using linear block codes. *IEEE Trans. Inf. Theory* **66**(7), 4019–4025 (2020). <https://doi.org/10.1109/tit.2019.2957354>
20. Pavlidou, N., Vinck, A.H., Yazdani, J., Honary, B.: Power line communications: state of the art and future trends. *IEEE Commun. Mag.* **41**(4), 34–40 (2003). <https://doi.org/10.1109/mcom.2003.1193972>
21. Shallue, C.J., Wanless, I.M.: Permutation polynomials and orthomorphism polynomials of degree six. *Finite Fields Appl.* **20**, 84–92 (2013). <https://doi.org/10.1016/j.ffa.2012.12.003>
22. Wang, X., Zhang, Y., Yang, Y., Ge, G.: New bounds of permutation codes under Hamming metric and Kendall’s τ -metric. *Des. Codes Crypt.* **85**(3), 533–545 (2016). <https://doi.org/10.1007/s10623-016-0321-5>
23. Yang, L., Chen, K., Yuan, L.: New constructions of permutation arrays. arXiv e-prints (2006). <https://arxiv.org/pdf/0801.3987.pdf>