Rose-Hulman Undergraduate Mathematics Journal

Volume 17
Issue 2

Article 2

Sums of Reciprocals of Irreducible Polynomials over Finite Fields

Spencer Nelson
St. Lawrence University

Rose-
Hulman
Undergraduate
Mathematics
Journal

Sums of Reciprocals of Irreducible Polynomials over Finite Fields

Spencer M. Nelson[a]

Volume 17, No. 2, Fall 2016

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
mathjournal@rose-hulman.edu
scholar.rose-hulman.edu/rhumj

[a]St. Lawrence University

Rose-Hulman Undergraduate Mathematics Journal
Volume 17, No. 2, Fall 2016

Sums of Reciprocals of Irreducible Polynomials over Finite Fields

Spencer Nelson

Abstract. We will revisit a theorem first proved by L. Carlitz in 1935 in which he provided an intriguing formula for sums involving the reciprocals of all monic polynomials of a given degree over a finite field of a specified order. Expanding on this result, we will consider the equally curious case where instead of adding reciprocals all monic polynomials of a given degree, we only consider adding reciprocals of those that are irreducible.

Acknowledgements: The author is appreciative for all of Dr. Sam Vandervelde's guidance and assistance throughout the process of working on this problem.

1 Introduction

Let $q = p^r$ for some prime p and positive integer r, and let $\mathbb{F}_q$ denote the finite field with q elements. Recall that not only are all finite fields of prime power order, but there exists a unique finite field of order p^r for every prime p and positive integer r (up to isomorphism). Additionally, let $\mathbb{F}_q[x]$ denote the ring of polynomials over $\mathbb{F}_q$ and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ denote the set of nonzero elements in $\mathbb{F}_q$.

In 1935, L. Carlitz proved that for $1 \leq k \leq q$,

$$\sum_{f \in \mathcal{P}_q^n} \frac{1}{f^k} = \frac{1}{\left[\prod_{i=1}^{n} \left(x - x^{q^i}\right)\right]^k}, \tag{1}$$

where $\mathcal{P}_q^n$ denotes the set of all monic polynomials of degree n over $\mathbb{F}_q$ [1]. This result was then reproved by Hicks et al. in 2012 using a simpler induction-based argument [2]. The expression above is peculiar by itself but becomes even more enticing when working through specific examples. We invite the reader to compute this sum by hand for a few relatively small cases in order to appreciate the surprising amount of cancellation that occurs in the numerator of this expression. It is worth mentioning that Carlitz arrived at a closed formula for $\sum_{f \in \mathcal{P}_q^n} \frac{1}{f^k}$ for all values of n and k, but the expression becomes increasingly more complicated when $k > q$.

Hicks et.al. [2] point out that the integers and $\mathbb{F}_q[x]$ bear many similarities such as unique factorization into irreducible elements. In the integers, of course, the irreducible elements are the prime numbers, whose history is both rich and extensive. Since the irreducible polynomials in $\mathbb{F}_q[x]$ are the analogue to the prime numbers in $\mathbb{Z}$, it seemed like a natural question to consider (1) but restricted only to the subset of polynomials that are irreducible. From here on, we will let $\mathcal{I}_q^n$ denote the set of all monic irreducible polynomials of degree n over the finite field with q elements and we will also let $h_{n,q}(x)$ denote the product of all monic irreducible polynomials of degree n over $\mathbb{F}_q$.

If $n = 1$, we have that $\mathcal{P}_q^n = \mathcal{I}_q^n$ since all linear polynomials are also irreducible. So we will begin by considering the case $n = 2$. All monic irreducible polynomials of certain degrees over certain finite fields can be found as an appendix in the text of Lidl and Niederreiter [3], which we relied on to carry out calculation of these sums. To begin, observe that

$$\begin{aligned}
\sum_{f \in \mathcal{I}_3^2} \frac{1}{f} &= \frac{1}{x^2+1} + \frac{1}{x^2+x+2} + \frac{1}{x^2+2x+2} \\
&= \frac{[(x^2+x+2)(x^2+2x+2)] + [(x^2+1)(x^2+2x+2)] + [(x^2+1)(x^2+x+2)]}{h_{2,3}(x)} \\
&= \frac{(x^4+1) + (x^4+2x^3+2x+2) + (x^4+x^3+x+2)}{h_{2,3}(x)} \\
&= \frac{2}{h_{2,3}(x)} \\
&= -\frac{1}{h_{2,3}(x)}.
\end{aligned}$$

As the order of the field increases, the cardinality of $\mathcal{I}_q^2$ increases. Additionally, the algebra involved becomes cumbersome to carry out by hand. To remedy this, we utilized the polynomial module in Python, which is part of the Numpy scientific computing package. We will omit the explicit calculation of this sum over $\mathbb{F}_5$ but the curious reader may verify that we have

$$\sum_{f\in\mathcal{I}_5^2}\frac{1}{f}=\frac{4x^{10}+2x^6+4x^2}{h_{2,5}(x)}=-\frac{(x^5-x)^2}{h_{2,5}(x)}.$$

Further, the sum over $\mathbb{F}_7$ is

$$\sum_{f\in\mathcal{I}_7^2}\frac{1}{f}=\frac{6x^{28}+4x^{22}+x^{16}+4x^{10}+6x^4}{h_{2,7}(x)}=-\frac{(x^7-x)^4}{h_{2,7}(x)}.$$

Collectively, these results led to the following conjecture:

$$\sum_{f\in\mathcal{I}_q^2}\frac{1}{f}=-\frac{(x^q-x)^{q-3}}{h_{2,q}(x)}. \tag{2}$$

In Section 2, we prove that the formula in (2) is indeed true. We will also provide a closed form formula for the sum of the reciprocals of all monic irreducible cubic polynomials. Once we have this information, we will also be able to determine the sum of the reciprocals of all monic reducible polynomials of degree 2 and 3 by using (1). So for future use, we will let $\mathcal{R}_q^n$ denote the set of monic reducible polynomials of degree n over $\mathbb{F}_q$. We will then conclude in Section 3 by discussing some ideas for future study and some of the difficulties we encountered attempting to find a closed form formula for the sum of the reciprocals of monic irreducible quartic polynomials.

2 Sums of Reciprocals of Irreducible Polynomials

Before proving the formula proposed in (2) and a formula for the sum of the reciprocals of all monic irreducible cubic polynomials, we need to take note of a few facts that our proof will rely on. The first of these is a particular fact about polynomials over finite fields that appears as Theorem 3.20 in the text of Lidl and Niederreiter [3].

Theorem 1. *The product of all monic irreducible polynomials over $\mathbb{F}_q$ of degree dividing n is equal to $x^{q^n}-x$. That is,*

$$\prod_{d|n}h_{d,q}(x)=x^{q^n}-x.$$

The next fact that is a lemma that will provide the foundation for our proof strategy.

Lemma 2. *Let f and g be nonzero polynomials over $\mathbb{F}_q$ each having degree less than or equal to n for some positive integer n. If $f(t) = g(t)$ for $n+1$ distinct values of $t \in \mathbb{F}_q$, then $f = g$.*

Proof. Suppose that $t_i \in \mathbb{F}_q$, where $i \in \mathbb{Z}$ and $1 \leq i \leq n+1$, are distinct values at which f and g agree. Since $\deg f \leq n$ and $\deg g \leq n$, it follows that $\deg(f-g) \leq n$. If we let $t_i \in \mathbb{F}_q$ be some value for which f and g agree, then we have that $f(t_i) = g(t_i)$ which implies that $f(t_i) - g(t_i) = 0$ and further that t_i is a root of $f - g$. Since t_i was arbitrary, t_i is a root of $f - g$ for all $1 \leq i \leq n+1$ and $(x - t_i)$ is a factor of $f - g$. However this implies that $f - g$ must have degree at least $n+1$, but we know that $\deg(f-g) \leq n$. Hence it must be the case that $f - g = 0$ and further that $f = g$. □

The following lemma is known as Wilson's Theorem when performing arithmetic in $\mathbb{F}_p$. We will expand this idea to $\mathbb{F}_q$ and utilize it later on to perform cancellations to our advantage.

Lemma 3. *In a finite field $\mathbb{F}_q$, the product of all $\alpha \in \mathbb{F}_q^*$ is equal to -1. That is* $\displaystyle\prod_{\alpha \in \mathbb{F}_q^*} \alpha = -1$.

Proof. To start, consider the polynomial $f(x) = x^2 - 1$ over $\mathbb{F}_q$, whose roots are ± 1. Since a polynomial of degree n over a field can have at most n roots, we know that ± 1 are the only elements of $\mathbb{F}_q$ satisfying $x^2 - 1 = 0$, or equivalently $x^2 = 1$. Hence ± 1 are the only elements of $\mathbb{F}_q$ that are self-inverses.

Upon multiplying every element of $\mathbb{F}_q^*$, we may pair each element of $\mathbb{F}_q^*$ with its inverse so they combine to give 1 since multiplication is commutative in $\mathbb{F}_q^*$. After pairing each element with its inverse, -1 is the only term that remains that is not equal to 1 because it is the only self-inverse element of $\mathbb{F}_q^*$. Hence the overall product is -1. □

With all of the requisite mathematics in place, we now provide a proof of equation (2).

Theorem 4. *Let $\mathcal{I}_q^2$ denote the set of monic irreducible quadratic polynomials over $\mathbb{F}_q$ for $q \geq 3$. Then,*

$$\sum_{f \in \mathcal{I}_q^2} \frac{1}{f} = -\frac{(x^q - x)^{q-3}}{h_{2,q}(x)}. \tag{2}$$

Proof. We will begin by first determining the cardinality of $\mathcal{I}_q^2$. We know that $\mathbb{F}_{q^2}$ is the splitting field extension for all $f \in \mathcal{I}_q^2$. Further, for all $\sigma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, of which there are $q^2 - q$ such elements, we know that there is some $f_\sigma \in \mathcal{I}_q^2$ that is the minimal polynomial of σ over $\mathbb{F}_q$. However f_σ is the minimal polynomial for σ^q, the conjugate of σ, as well. Hence the cardinality of $\mathcal{I}_q^2$ is $\frac{1}{2}(q^2 - q)$. For the sake of convenience, let $k = |\mathcal{I}_q^2|$ and enumerate the polynomials of $\mathcal{I}_q^2$ as $f_1, f_2, \ldots, f_k$.

Now if we expand our sum we have

$$\sum_{f \in \mathcal{I}_q^2} \frac{1}{f} = \frac{1}{f_1} + \frac{1}{f_2} + \cdots + \frac{1}{f_k},$$

which we may simplify by obtaining $h_{2,q}(x)$ as a common denominator

$$\sum_{f\in\mathcal{I}_q^2}\frac{1}{f}=\frac{(f_2\cdot f_3\cdots f_k)+(f_1\cdot f_3\cdots f_k)+\cdots+(f_1\cdot f_2\cdots f_{k-1})}{h_{2,q}(x)}. \tag{3}$$

Examining the numerator of (3), we see that each individual term is the product of $k-1$ quadratics from $\mathcal{I}_q^2$. Then it follows that the degree of the numerator in (3) is less than or equal to $2(k-1)=q^2-q-2$. Also from (2), the degree of the numerator of our desired result is equal to $q(q-3)=q^2-3q$. Since the denominators of (2) and (3) are equal, showing that their numerators are equal establishes the theorem. Since the degree of the numerators in (3) and (2) are less than q^2-q-1, showing that the numerators of these two expressions agree for all q^2-q elements of $\mathbb{F}_{q^2}\setminus\mathbb{F}_q$ implies that they are equal by lemma 2 and completes the proof.

Let $\beta_1,\beta_2,\ldots,\beta_{2k}$ be the elements of $\mathbb{F}_{q^2}\setminus\mathbb{F}_q$ and enumerate them so that β_2 is the conjugate of β_1, that is, $\beta_2=\beta_1^q$. We know that the minimal polynomial of β_1 is some polynomial contained in $\mathcal{I}_q^2$; so without loss of generality, let it be $f_1\in\mathcal{I}_q^2$. When evaluating the numerator of (3) at β_1, every term containing f_1 will be equal to 0 since β_1 is a root of f_1. Hence the entire numerator evaluated at β_1 is equal to $f_2(\beta_1)\cdot f_3(\beta_1)\cdots f_k(\beta_1)$. Now since the elements of $\mathbb{F}_{q^2}\setminus\mathbb{F}_q$ are precisely the roots of the polynomials of $\mathcal{I}_q^2$, we may write $h_{2,q}(x)$ as

$$h_{2,q}(x)=\prod_{\beta\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q}(x-\beta)=(x-\beta_1)(x-\beta_2)\cdots(x-\beta_{2k}) \tag{4}$$

Further, since all monic linear polynomials over $\mathbb{F}_q$ are irreducible, we have that

$$\prod_{\alpha\in\mathbb{F}_q}(x-\alpha)=x^q-x$$

by Theorem 1. If we let $\alpha_1,\ldots,\alpha_{q-1}$ denote the nonzero elements of $\mathbb{F}_q$, we arrive at another formulation of $h_{2,q}(x)$ given by

$$h_{2,q}(x)=\frac{[(x-\beta_1)(x-\beta_2)\cdots(x-\beta_{2k})]\cdot[(x)(x-\alpha_1)\cdots(x-\alpha_{q-1})]}{x^q-x}, \tag{5}$$

which is obtained by multiplying (4) by $(x^q-x)/(x^q-x)$ and deliberately leaving x^q-x as the product of all monic linear polynomials over $\mathbb{F}_q$ in the numerator. Since β_1 and β_2 are the roots of $f_1(x)$, we have $f_1(x)=(x-\beta_1)(x-\beta_2)$ and also that $h_{2,q}(x)=f_1(x)\cdots f_2(x)\cdots f_k(x)$. Now using the formulation of $h_{2,q}(x)$ from (5), we derive

$$\begin{aligned}
f_2(x)\cdot f_3(x)\cdots f_k(x) &= \frac{h_{2,q}(x)}{f_1(x)}\\
&= \frac{[(x-\beta_1)(x-\beta_2)\cdots(x-\beta_{2k})]\cdot[(x)(x-\alpha_1)\cdots(x-\alpha_{q-1})]}{(x^q-x)\cdot(x-\beta_1)(x-\beta_2)}\\
&= \frac{[(x-\beta_3)\cdots(x-\beta_{2k})]\cdot[(x)\cdots(x-\alpha_{q-1})]}{x^q-x}.
\end{aligned}$$

Evaluating $f_2(x) \cdot f_3(x) \cdots f_k(x)$ at β_1 gives

$$f_2(\beta_1) \cdot f_3(\beta_1) \cdots f_k(\beta_1) = \frac{[(\beta_1 - \beta_3) \cdots (\beta_1 - \beta_{2k})] \cdot [(\beta_1) \cdots (\beta_1 - \alpha_{q-1})]}{\beta_1^q - \beta_1}.$$

which we may then multiply by $(\beta_1 - \beta_2)/(\beta_1 - \beta_2)$ to obtain

$$f_2(\beta_1) \cdot f_3(\beta_1) \cdots f_k(\beta_1) = \frac{(\beta_1 - \beta_3) \cdots (\beta_1 - \beta_{2k}) \cdot (\beta_1) \cdots (\beta_1 - \alpha_{q-1})(\beta_1 - \beta_2)}{(\beta_1^q - \beta_1)(\beta_1 - \beta_2)}. \quad (6)$$

Now we note that every nonzero element of $\mathbb{F}_{q^2}$ appears in the numerator of (6), which, by lemma 3, implies that

$$f_2(\beta_1) \cdot f_3(\beta_1) \cdots f_k(\beta_1) = -\frac{1}{(\beta_1^q - \beta_1)(\beta_1 - \beta_2)} = \frac{1}{(\beta_1^q - \beta_1)^2}.$$

However, the numerator of our desired result is $-(x^q - x)^{q-3}$, which is equal to $-(\beta_1^q - \beta_1)^{q-3}$ when evaluated at β_1. Therefore we must show that these two quantities are equal, that is,

$$\frac{1}{(\beta_1^q - \beta_1)^2} = -(\beta_1^q - \beta_1)^{q-3},$$

or equivalently that $-(\beta_1^q - \beta_1)^{q-1} = 1$. Now note that

$$\begin{aligned} -(\beta_1^q - \beta_1)^{q-1} &= -\frac{(\beta_1^q - \beta_1)^q}{\beta_1^q - \beta_1} \\ &= -\frac{\beta_1^{q^2} - \beta_1^q}{\beta_1^q - \beta_1} \\ &= -\frac{\beta_1 - \beta_1^q}{\beta_1^q - \beta_1} \\ &= 1. \end{aligned}$$

Hence the numerator in (2) and (3) agree for all $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ since β_1 was arbitrary. Hence, by lemma 2, we have that

$$\sum_{f \in \mathcal{I}_q^2} \frac{1}{f} = -\frac{(x^q - x)^{q-3}}{h_{2,q}(x)}.$$

□

Since we have closed form expressions for both the sum of reciprocals of monic irreducible quadratic polynomials as well as all monic polynomials due to Carliz, it is a routine algebraic exercise to determine the sum of reciprocals of all reducible quadratic polynomials over $\mathbb{F}_q$. We certainly have

$$\sum_{f \in \mathcal{R}_q^2} \frac{1}{f} = \sum_{f \in \mathcal{P}_q^2} \frac{1}{f} - \sum_{f \in \mathcal{I}_q^2} \frac{1}{f}.$$

Then using Carlitz's formulation for the sum of reciprocals of all monic polynomials coupled with our formulation for the sum of reciprocals of monic irreducible quadratics, we have

$$\sum_{f\in\mathcal{R}_q^2}\frac{1}{f}=\frac{1}{\prod_{i=1}^{2}(x-x^{q^i})}-\left[-\frac{(x^q-x)^{q-3}}{h_{2,q}(x)}\right].$$

By Theorem 1, we have that

$$x^{q^2}-x=\prod_{d|2}h_{d,q}(x)=h_{1,q}(x)\cdot h_{2,q}(x),$$

and since $h_{1,q}(x)=x^q-x$, it follows that

$$h_{2,q}(x)=\frac{x^{q^2}-x}{x^q-x}.$$

Therefore,

$$\begin{aligned}\frac{1}{\prod_{i=1}^{2}(x-x^{q^i})}-\left[-\frac{(x^q-x)^{q-3}}{h_{2,q}(x)}\right] &= \frac{1}{(x-x^q)(x-x^{q^2})}+\frac{(x^q-x)^{q-2}}{x^{q^2}-x}\\ &= \frac{1}{(x^{q^2}-x)(x^q-x)}+\frac{(x^q-x)^{q-1}}{(x^{q^2}-x)(x^q-x)}\\ &= \frac{1+(x^q-x)^{q-1}}{(x^{q^2}-x)(x^q-x)}.\end{aligned}$$

If we then multiply this expression by $(x^q-x)/(x^q-x)$, we obtain

$$\begin{aligned}\sum_{f\in\mathcal{R}_q^2}\frac{1}{f} &= \frac{(x^q-x)+(x^q-x)^q}{(x^{q^2}-x)(x^q-x)^2}\\ &= \frac{x^q-x+x^{q^2}-x^q}{(x^{q^2}-x)(x^q-x)^2}\\ &= \frac{x^{q^2}-x}{(x^{q^2}-x)(x^q-x)^2}\\ &= \frac{1}{(x^q-x)^2}.\end{aligned}$$

Having determined the sum of the reciprocals of monic irreducible quadratics, it is a natural next step to consider the sum of reciprocals of monic irreducible cubics. Rather than computing the sum $\sum_{f\in\mathcal{I}_q^3}\frac{1}{f}$ for a number of specific cases and then conjecturing a formula, we proceeded with the proof as in Theorem 4 until the calculations simplified to what we believed the sum was equal to. We then went about proving that our conjecture was indeed correct.

Theorem 5. *Let $\mathcal{I}_q^3$ denote the set of monic irreducible cubic polynomials over $\mathbb{F}_q$ for $q \geq 4$. Then,*

$$\sum_{f \in \mathcal{I}_q^3} \frac{1}{f} = \frac{[h_{2,q}(x)]^3 \cdot (x^{q^2} - x)^{q-4}}{h_{3,q}(x)}. \tag{7}$$

Proof. We will again begin by determining the cardinality of $\mathcal{I}_q^3$. We know that $\mathbb{F}_{q^3}$ is the splitting field extension for all $f \in \mathcal{I}_q^3$. Additionally, for all $\sigma \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$, of which there are $q^3 - q$ such elements, we know that there is some $f_\sigma \in \mathcal{I}_q^3$ that is the minimal polynomial of σ over $\mathbb{F}_q$. However f_σ is the minimal polynomial for σ^q and σ^{q^2}, the conjugates of σ, as well. Hence the cardinality of $\mathcal{I}_q^3$ is $\frac{1}{3}(q^3 - q)$; so let $k = |\mathcal{I}_q^3|$ and enumerate the polynomials of $\mathcal{I}_q^3$ as $f_1, f_2, \ldots, f_k$.

Now if we expand our sum we have

$$\sum_{f \in \mathcal{I}_q^3} \frac{1}{f} = \frac{1}{f_1} + \frac{1}{f_2} + \cdots + \frac{1}{f_k},$$

which we may simplify by obtaining $h_{3,q}(x)$ as a common denominator

$$\sum_{f \in \mathcal{I}_q^3} \frac{1}{f} = \frac{(f_2 \cdot f_3 \cdots f_k) + (f_1 \cdot f_3 \cdots f_k) + \cdots + (f_1 \cdot f_2 \cdots f_{k-1})}{h_{3,q}(x)}. \tag{8}$$

Since each individual term appearing in the numerator of (8) is the product of $k-1$ cubic polynomials, the degree of the numerator in (8) is less than or equal to $3(k-1) = q^3 - q - 3$. Recall from Theorem 4 that $|\mathcal{I}_q^2| = \frac{1}{2}(q^2 - q)$, which implies that the degree of the numerator of (7) is equal to $q^3 - q^2 - 3q$. Since the degree of the numerator of (7) and the degree of the numerator of (8) are both less than $q^3 - q - 1$, showing that they agree for all $q^3 - q$ elements of $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$ implies they are equal by lemma 2 and completes the proof.

So let $\beta_1, \beta_2, \ldots, \beta_{3k}$ be the elements of $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and enumerate them in such a way that β_2 and β_3 are the conjugates of β_1, that is, $\beta_2 = \beta_1^q$ and $\beta_3 = \beta_1^{q^2}$. We know that the minimal polynomial of β_1 is some polynomial contained in $\mathcal{I}_q^3$. Then, without loss of generality, let it be $f_1 \in \mathcal{I}_q^3$. Upon evaluating the numerator of (8) at β_1, every term containing f_1 will be equal to 0 since β_1 is a root of f_1. Hence the entire numerator evaluated at β_1 is equal to $f_2(\beta_1) \cdot f_3(\beta_1) \cdots f_k(\beta_1)$. Since the elements of $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$ are precisely the roots of the polynomials of $\mathcal{I}_q^3$, we may write $h_{3,q}(x) = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_{3k})$. Further, since $f_1(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3)$, we have that

$$\begin{aligned} f_2(x) \cdot f_3(x) \cdots f_k(x) &= \frac{h_{3,q}(x)}{f_1(x)} \\ &= \frac{(x - \beta_1)(x - \beta_2)(x - \beta_3) \cdots (x - \beta_{3k})}{(x - \beta_1)(x - \beta_2)(x - \beta_3)} \\ &= (x - \beta_4)(x - \beta_5) \cdots (x - \beta_{3k}). \end{aligned}$$

Now if we let $\alpha_1, \ldots, \alpha_{q-1}$ denote the nonzero elements of $\mathbb{F}_q$, we know that

$$x^q - x = (x)(x-\alpha_1)\cdots(x-\alpha_{q-1})$$

by Theorem 1. Therefore we have that

$$f_2(x)\cdot f_3(x)\cdots f_k(x) = \frac{(x-\beta_4)(x-\beta_5)\cdots(x-\beta_{3k})(x)(x-\alpha_1)\cdots(x-\alpha_{q-1})}{x^q - x},$$

which is obtained by multiplying $(x-\beta_4)(x-\beta_5)\cdots(x-\beta_{3k})$ by $(x^q-x)/(x^q-x)$ and deliberately writing $x^q - x$ as $(x)(x-\alpha_1)\cdots(x-\alpha_{q-1})$ in the numerator. Hence, the numerator of (8) when evaluated at β_1 is

$$f_2(\beta_1)\cdot f_3(\beta_1)\cdots f_k(\beta_1) = \frac{(\beta_1-\beta_4)\cdots(\beta_1-\beta_{3k})(\beta_1)\cdots(\beta_1-\alpha_{q-1})}{\beta_1^q - \beta_1}. \tag{9}$$

We may then multiply (9) by

$$\frac{(\beta_1-\beta_2)(\beta_1-\beta_3)}{(\beta_1-\beta_2)(\beta_1-\beta_3)}$$

to obtain

$$\frac{(\beta_1-\beta_4)(\beta_1-\beta_5)\cdots(\beta_1-\beta_{3k})(\beta_1)(\beta_1-\alpha_1)\cdots(\beta_1-\alpha_{q-1})(\beta_1-\beta_2)(\beta_1-\beta_3)}{(\beta_1^q-\beta_1)(\beta_1-\beta_2)(\beta_1-\beta_3)}. \tag{10}$$

Since every nonzero element of $\mathbb{F}_{q^3}$ appears in the numerator (10), the entire numerator of (10) is equal to -1 by lemma 3 and so we have

$$f_2(\beta_1)\cdot f_3(\beta_2)\cdots f_k(\beta_1) = -\frac{1}{(\beta_1^q-\beta_1)(\beta_1-\beta_2)(\beta_1-\beta_3)} = -\frac{1}{(\beta_1^q-\beta_1)^2(\beta_1^{q^2}-\beta_1)}. \tag{11}$$

Now note that

$$\frac{\beta_1^{q^3}-\beta_1^q}{\beta_1^q-\beta_1} = -1,$$

which we may substitute for -1 in (11) to obtain

$$\begin{aligned} f_2(\beta_1)\cdot f_3(\beta_2)\cdots f_k(\beta_1) &= \frac{\beta_1^{q^3}-\beta_1^q}{(\beta_1^q-\beta_1)^3(\beta_1^{q^2}-\beta_1)} \\ &= \frac{(\beta_1^{q^2}-\beta_1)^q}{(\beta_1^q-\beta_1)^3(\beta_1^{q^2}-\beta_1)} \\ &= \left(\frac{\beta_1^{q^2}-\beta_1}{\beta_1^q-\beta_1}\right)^3 \cdot (\beta_1^{q^2}-\beta_1)^{q-4}. \end{aligned}$$

By Theorem 1 we have that $h_{2,q}(x) = \dfrac{x^{q^2} - x}{x^q - x}$ and so $h_{2,q}(\beta_1) = \dfrac{\beta_1^{q^2} - \beta_1}{\beta_1^q - \beta_1}$, which implies that

$$f_2(\beta_1) \cdot f_3(\beta_2) \cdots f_k(\beta_1) = \left(\frac{\beta_1^{q^2} - \beta_1}{\beta_1^q - \beta_1} \right)^3 \cdot (\beta_1^{q^2} - \beta_1)^{q-4} = [h_{2,q}(\beta_1)]^3 \cdot (\beta_1^{q^2} - \beta_1)^{q-4}.$$

However this is precisely the same as the numerator of (7) evaluated at β_1. Since β_1 was arbitrary, the numerator of (7) and (8) agree for all $q^3 - q$ elements of $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$. Then by lemma 2 we have

$$\sum_{f \in \mathcal{I}_q^3} \frac{1}{f} = \frac{[h_{2,q}(x)]^3 \cdot (x^{q^2} - x)^{q-4}}{h_{3,q}(x)}.$$

□

Just as before, we can use Carlitz's formulation along with our findings to determine the sum of the reciprocals of all reducible monic cubic polynomials over $\mathbb{F}_q$. So then we have that

$$\sum_{f \in \mathcal{R}_q^3} \frac{1}{f} = \sum_{f \in \mathcal{P}_q^3} \frac{1}{f} - \sum_{f \in \mathcal{I}_q^3} \frac{1}{f} = \frac{1}{\prod_{i=1}^3 (x - x^{q^i})} - \frac{[h_{2,q}(x)]^3 \cdot (x^{q^2} - x)^{q-4}}{h_{3,q}(x)}. \tag{12}$$

Further, we have

$$x^{q^3} - x = \prod_{d|3} h_{d,q}(x) = h_{1,q}(x) \cdot h_{3,q}(x)$$

by Theorem 1 and since $h_{1,q}(x) = x^q - x$, we have that $h_{3,q}(x) = \dfrac{x^{q^3} - x}{x^q - x}$. Replacing $h_{3,q}(x)$ with $\dfrac{x^{q^3} - x}{x^q - x}$ in (12) yields

$$\frac{1}{(x - x^q)(x - x^{q^2})(x - x^{q^3})} - \frac{[h_{2,q}(x)]^3 \cdot (x^q - x) \cdot (x^{q^2} - x)^{q-4}}{x^{q^3} - x},$$

which simplifies to

$$-\frac{1 + [h_{2,q}(x)]^3 \cdot (x^q - x)^2 \cdot (x^{q^2} - x)^{q-3}}{(x^{q^3} - x)(x^{q^2} - x)(x^q - x)}.$$

Now if we replace $h_{2,q}(x)$ with $\dfrac{x^{q^2}-x}{x^q-x}$ and multiply by $(x^q-x)/(x^q-x)$, we obtain

$$\begin{aligned}\sum_{f\in\mathcal{R}_q^3}\frac{1}{f} &= -\frac{1+\left(\frac{x^{q^2}-x}{x^q-x}\right)^3\cdot(x^q-x)^2\cdot(x^{q^2}-x)^{q-3}}{(x^{q^3}-x)(x^{q^2}-x)(x^q-x)}\cdot\frac{x^q-x}{x^q-x}\\ &= -\frac{(x^q-x)+(x^{q^2}-x)^q}{(x^{q^3}-x)(x^{q^2}-x)(x^q-x)^2}\\ &= -\frac{x^q-x+x^{q^3}-x^q}{(x^{q^3}-x)(x^{q^2}-x)(x^q-x)^2}\\ &= -\frac{1}{(x^{q^2}-x)(x^q-x)^2}.\end{aligned}$$

3 Concluding Remarks

There are a number of directions that we could inquire further about for this particular topic. In Carlitz's original paper, he deduced a closed form expression for the sum of the reciprocals of all monic polynomials raised to some integer power. For future studies, it would be worth exploring expressions such as $\sum_{f\in\mathcal{I}_q^n}\frac{1}{f^k}$.

The most obvious avenue to examine would be to determine the sum, not involving any powers, for $\mathcal{I}_q^n$ where $n\geq 4$. Having had determined $\sum_{f\in\mathcal{I}_q^3}\frac{1}{f}$ by working as if we knew what the correct answer was, we believed we could repeat the same process for $\mathcal{I}_q^4$. So, we began by determining the cardinality of $\mathcal{I}_q^4$. First, we know that $\mathbb{F}_{q^4}$ is the splitting field extension for all $f\in\mathcal{I}_q^4$. Additionally, every $\sigma\in\mathbb{F}_{q^4}\setminus\mathbb{F}_{q^2}$ has a minimal polynomial contained in $\mathcal{I}_q^4$ and since $|\mathbb{F}_{q^4}\setminus\mathbb{F}_{q^2}|=q^4-q^2$ and the minimal polynomial for σ is also the minimal polynomial for the conjugates of σ, we have that $|\mathcal{I}_q^4|=\frac{1}{4}(q^4-q^2)$; so let k denote $|\mathcal{I}_q^4|$ from here on and enumerate the polynomials of $\mathcal{I}_q^4$ as $f_1,f_2,\ldots,f_k$.

We then expand the sum and obtain $h_{4,q}(x)$ as a common denominator; so we have

$$\sum_{f\in\mathcal{I}_q^4}\frac{1}{f}=\frac{(f_2\cdot f_3\cdots f_k)+(f_1\cdot f_3\cdots f_k)+\cdots+(f_1\cdot f_2\cdots f_{k-1})}{h_{4,q}(x)}. \tag{13}$$

Now since every term in the numerator of (13) is the product of $k-1$ quartics, we know that the degree of the numerator is less than or equal to $4(k-1)=q^4-q^2-4$. Now let $\beta_1,\beta_2,\ldots,\beta_{4k}$ be the elements of $\mathbb{F}_{q^4}\setminus\mathbb{F}_{q^2}$ and enumerate them in such a way that β_2, β_3, and β_4 are the conjugates of β_1, that is $\beta_2=\beta_1^q$, $\beta_3=\beta_1^{q^2}$, $\beta_4=\beta_1^{q^3}$. Now we know that the minimal polynomial of β_1 is some polynomial in $\mathcal{I}_q^4$; so, without loss of generality, let it be $f_1\in\mathcal{I}_q^4$. Now if we evaluate the numerator of (13) at β_1, then every term containing f_1 is equal to 0 since β_1 is a root of f_1; so we have that the entire numerator is equal to $f_2(\beta_1)\cdot f_3(\beta_1)\cdots f_k(\beta_1)$ when evaluated at β_1.

Since the elements of $\mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}$ are precisely the roots of the polynomials belonging to $\mathcal{I}_q^4$ and $h_{4,q}(x) = f_1(x) \cdot f_2(x) \cdots f_k(x)$, we have

$$h_{4,q}(x) = \prod_{\beta \in \mathbb{F}_{q^4} \setminus \mathbb{F}_{q^2}} (x - \beta).$$

Since $h_{4,q}(x) = f_1(x) \cdot f_2(x) \cdots f_k(x)$ and $f_1(x) = (x-\beta_1)(x-\beta_2)(x-\beta_3)(x-\beta_4)$, we have

$$\begin{aligned} f_2(x) \cdot f_3(x) \cdots f_k(x) &= \frac{h_{4,q}(x)}{f_1(x)} \\ &= \frac{(x-\beta_1)(x-\beta_2)(x-\beta_3)(x-\beta_4)\cdots(x-\beta_{4k})}{(x-\beta_1)(x-\beta_2)(x-\beta_3)(x-\beta_4)} \\ &= (x-\beta_5)(x-\beta_6)\cdots(x-\beta_{4k}). \end{aligned}$$

Now recall that $h_{1,q}(x) = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha)$ and $h_{2,q}(x) = \prod_{\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q} (x - \alpha)$ from earlier. Since $x^{q^2} - x = h_{1,q}(x) \cdot h_{2,q}(x)$ by Theorem 1, we have that

$$x^{q^2} - x = h_{1,q}(x) \cdot h_{2,q}(x) = \left(\prod_{\alpha \in \mathbb{F}_q} (x - \alpha) \right) \cdot \left(\prod_{\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q} (x - \alpha) \right) = \prod_{\alpha \in \mathbb{F}_{q^2}} (x - \alpha).$$

So if we let $\alpha_1, \alpha_2, \ldots, \alpha_{q^2-1}$ denote the nonzero elements of $\mathbb{F}_{q^2}$, we have

$$f_2(x) \cdot f_3(x) \cdots f_k(x) = \frac{(x-\beta_5)(x-\beta_6)\cdots(x-\beta_{4k})(x)(x-\alpha_1)\cdots(x-\alpha_{q^2-1})}{x^{q^2} - x},$$

which is obtained by multiplying $(x-\beta_5)(x-\beta_6)\cdots(x-\beta_{4k})$ by $(x^{q^2} - x)/(x^{q^2} - x)$ and deliberately leaving $x^{q^2} - x$ as $(x)(x-\alpha_1)\cdots(x-\alpha_{q^2-1})$ in the numerator. Further we may multiply this expression by

$$\frac{(x-\beta_2)(x-\beta_3)(x-\beta_4)}{(x-\beta_2)(x-\beta_3)(x-\beta_4)}$$

so that we have

$$f_2(x) \cdot f_3(x) \cdots f_k(x) = \frac{(x-\beta_5)\cdots(x-\beta_{4k})(x)(x-\alpha_1)\cdots(x-\alpha_{q^2-1})(x-\beta_2)(x-\beta_3)(x-\beta_4)}{(x^{q^2} - x)(x-\beta_2)(x-\beta_3)(x-\beta_4)}. \tag{14}$$

Evaluating (14) at β_1 gives

$$f_2(\beta_1) \cdot f_3(\beta_1) \cdots f_k(\beta_1) = \frac{(\beta_1-\beta_5)\cdots(\beta_1-\beta_{4k})(\beta_1)\cdots(\beta_1-\alpha_{q^2-1})(\beta_1-\beta_2)(\beta_1-\beta_3)(\beta_1-\beta_4)}{(\beta_1^{q^2} - \beta_1)(\beta_1-\beta_2)(\beta_1-\beta_3)(\beta_1-\beta_4)}. \tag{15}$$

Now since every nonzero element of $\mathbb{F}_{q^4}$ appears in the numerator of (15), by lemma 3, we have that

$$f_2(\beta_1) \cdot f_3(\beta_1) \cdots f_k(\beta_1) = -\frac{1}{(\beta_1^{q^2} - \beta_1)(\beta_1-\beta_2)(\beta_1-\beta_3)(\beta_1-\beta_4)}.$$

We may now simplify this expression so that we have

$$\begin{aligned} f_2(\beta_1)\cdot f_3(\beta_1)\cdots f_k(\beta_1) &= -\frac{1}{(\beta_1^{q^2}-\beta_1)(\beta_1-\beta_2)(\beta_1-\beta_3)(\beta_1-\beta_4)} \\ &= \frac{1}{(\beta_1^q-\beta_1)(\beta_1^{q^2}-\beta_1)^2(\beta_1^{q^3}-\beta_1)}. \end{aligned}$$

Now note that

$$-1 = \frac{\beta_1^{q^4}-\beta_1^q}{\beta_1^q-\beta_1},$$

and so we have

$$\begin{aligned} f_2(\beta_1)\cdot f_3(\beta_1)\cdots f_k(\beta_1) &= \frac{1}{(\beta_1^q-\beta_1)(\beta_1^{q^2}-\beta_1)^2(\beta_1^{q^3}-\beta_1)} \\ &= -\frac{\beta_1^{q^4}-\beta_1^q}{(\beta_1^q-\beta_1)^2(\beta_1^{q^2}-\beta_1)^2(\beta_1^{q^3}-\beta_1)} \\ &= -\frac{(\beta_1^{q^3}-\beta_1)^q}{(\beta_1^q-\beta_1)^2(\beta_1^{q^2}-\beta_1)^2(\beta_1^{q^3}-\beta_1)} \\ &= -\left(\frac{\beta_1^{q^3}-\beta_1}{\beta_1^q-\beta_1}\right)^2\cdot\frac{(\beta_1^{q^3}-\beta_1)^{q-3}}{(\beta_1^{q^2}-\beta_1)^2}. \end{aligned}$$

Since $h_{3,q}(x) = \dfrac{x^{q^3}-x}{x^q-x}$ by Theorem 1, we have

$$f_2(\beta_1)\cdot f_3(\beta_1)\cdots f_k(\beta_1) = -\left(\frac{\beta_1^{q^3}-\beta_1}{\beta_1^q-\beta_1}\right)^2\cdot\frac{(\beta_1^{q^3}-\beta_1)^{q-3}}{(\beta_1^{q^2}-\beta_1)^2} = -[h_{3,q}(\beta_1)]^2\cdot\frac{(\beta_1^{q^3}-\beta_1)^{q-3}}{(\beta_1^{q^2}-\beta_1)^2}.$$

Now at this point, we may express $(\beta_1^{q^3}-\beta_1)^{q-3}$ as $[h_{1,q}(\beta_1)\cdot h_{3,q}(\beta_1)]^{q-3}$ and $(\beta_1^{q^2}-\beta_1)^2$ as $[h_{1,q}(\beta_1)\cdot h_{2,q}(\beta_1)]^2$ using Theorem 1 and while we can cancel the two $h_{1,q}(\beta_1)$ terms that appear in the denominator, we cannot cancel the two $h_{2,q}(\beta_1)$ terms in any obvious manner. In all attempts to reduce this expression further, we were unable to cancel $[h_{2,q}(\beta_1)]^2$ while still keeping the degree of the polynomial small enough to invoke lemma 2. This same problem arises for $\mathcal{I}_q^n$ where $n \geq 4$ since we only introduce more conjugate terms in the denominator. For future studies, it may be necessary to rely on our old technique of computing the sum for a number of specific cases and then conjecturing a formula or to adopt an entirely new proof strategy all together.

References

[1] L. Carlitz, On certain functions connected with polynomials in a Galois field, *Duke Math. J.* **1** (1935) 139 – 158.

[2] K. Hicks, X. Hou, G. Mullen, Sums of Reciprocals of Polynomials over Finite Fields, *The American Math. Monthly J.* **119** (2012) 313 – 317.

[3] R. Lidl, H. Niederreiter, Finite Fields, *Encyclo. Math. Appl.*, 20, Cambridge University Press, Cambridge, 1983.