A note on the Hansen-Mullen conjecture for self-reciprocal irreducible polynomials

Theodoulos Garefalakis, Giorgos Kapetanakis[1,*]

Department of Mathematics and Applied Mathematics, University of Crete, Voutes Campus, 70013, Heraklion, Greece

Abstract

In this note, we complete the work in [*Finite Fields Appl.*, 18(4):832–841, 2012] by using computer calculations to prove that for odd q, there exists a monic self-reciprocal irreducible polynomial of degree $2n$ over $\mathbb{F}_q$, with any of its first (hence any of its last) $\lfloor n/2 \rfloor$ coefficients arbitrarily prescribed, with a couple of genuine exceptions.

Keywords: Self-reciprocal polynomials, Hansen-Mullen conjecture
2010 MSC: 12E05, 12E10, 11T06

Let $\mathbb{F}_q$ denote the finite field of q elements. The famous Hansen-Mullen [6] conjecture states that there exists a monic irreducible polynomial of degree n over $\mathbb{F}_q$ with its k-th coefficient prescribed to a, unless $k = a = 0$ or q even, $n = 2$, $k = 1$, and $a = 0$. Hansen and Mullen proved their conjecture for $k = 1$. Wan [7] proved that the conjecture holds, for $q > 19$ or $n \geq 36$ and Ham and Mullen [5] proved the remaining cases with the help of computers. Those cases have also been settled theoretically by Cohen and Prešern [2, 3].

In [4], the existence of self-reciprocal irreducible monic polynomials with prescribed coeffecients, over $\mathbb{F}_q$ for odd q, was considered. It was shown that if

$$q^{\frac{n-k-1}{2}} \geq \frac{16}{5}k(k+5) + \frac{1}{2},$$

then there exists a monic self-reciprcal irreducible polynomial of degree $2n$ over $\mathbb{F}_q$ with its k-th coefficient arbitrarily prescribed. As a corollary of this, it was also shown that if $k \leq n/2$, then there exists a monic self-reciprcal irreducible polynomial of degree $2n$ over $\mathbb{F}_q$ with its k-th coefficient arbitrarily prescribed, unless (q, n) is one of the 271 pairs of possible exceptions, see [4, Table 1], all lying within the range $q < 839$ and $n < 27$.

*Corresponding author
Email addresses: theo@math.uoc.gr (Theodoulos Garefalakis), gkapet@math.uoc.gr (Giorgos Kapetanakis)
[1]Tel: (+30) 2810 393771, Fax: (+30) 2810 393881

For the purposes of this note, a program was written in SAGE, which searched the remaining cases one-by-one. The SAGE file of this program is available at `http://www.math.uoc.gr/~gkapet/hm/hm-source.sws` and its results are available at `http://www.math.uoc.gr/~gkapet/hm/hm-results.txt`. These calculations combined with the results of [4] imply the following theorem.

Theorem 1. *Let q be an odd prime power and $\mathbb{F}_q$ the finite field of q elements. There exists a self-reciprocal irreducible monic polynomial over $\mathbb{F}_q$, of degree $2n$, with its k-th coefficient prescribed to $a \in \mathbb{F}_q$, unless*

1. $q = 3$, $n = 3$, $k = 1$ *and* $a = 0$ *or*
2. $q = 3$, $n = 4$, $k = 2$ *and* $a = 0$.

REMARK. As the computer results indicate, the two exceptions described above are genuine.

Acknowledgement

This work was funded by the University of Crete's research grant No. 3744.

References

[1] S. D. Cohen. Primitive elements and polynomials with arbitrary trace. *Discrete Math.*, 83(1):1–7, 1990.

[2] S. D. Cohen and M. Prešern. Primitive polynomials with prescribed second coefficient. *Glasgow Math. J.*, 48:281–307, 2006.

[3] S. D. Cohen and M. Prešern. The Hansen-Mullen primitivity conjecture: completion of proof. In *Number theory and polynomials*, volume 352 of *LMS Lecture notes*, pages 89–120. Cambridge University Press, Cambridge, 2008.

[4] T. Garefalakis and G. Kapetanakis. On the Hansen-Mullen conjecture for self-reciprocal irreducible polynomials. *Finite Fields Appl.*, 18(4):832–841, 2012.

[5] K. H. Ham and G. L. Mullen. Distribution of irreducible polynomials of small degrees over finite fields. *Math. Comp.*, 67(221):337–341, 1998.

[6] T. Hansen and G. L. Mullen. Primitive polynomials over finite fields. *Math. Comp.*, 59(200):639–643, 1992.

[7] D. Wan. Generators and irreducible polynomials over finite fields. *Math. Comp.*, 66(219):1195–1212, 1997.