J. Combin. Theory Ser. A 145 (2017) 340–363

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Merit factors of polynomials derived from difference sets ☆

Christian Günther, Kai-Uwe Schmidt

Department of Mathematics, Paderborn University, Warburger Str. 100, 33098 Paderborn, Germany

ARTICLE INFO

Article history:
Received 20 April 2015
Available online 3 September 2016

Keywords:
Difference set
Binary sequence
Merit factor
Asymptotic
Character sum
Aperiodic autocorrelation

ABSTRACT

The problem of constructing polynomials with all coefficients 1 or -1 and large merit factor (equivalently with small L^4 norm on the unit circle) arises naturally in complex analysis, condensed matter physics, and digital communications engineering. Most known constructions arise (sometimes in a subtle way) from difference sets, in particular from Paley and Singer difference sets. We consider the asymptotic merit factor of polynomials constructed from other difference sets, providing the first essentially new examples since 1991. In particular we prove a general theorem on the asymptotic merit factor of polynomials arising from cyclotomy, which includes results on Hall and Paley difference sets as special cases. In addition, we establish the asymptotic merit factor of polynomials derived from Gordon–Mills–Welch difference sets and Sidelnikov almost difference sets, proving two recent conjectures.

1. Introduction

The problem of constructing polynomials having all coefficients in the set $\{-1, 1\}$ (frequently called *Littlewood polynomials*) with small L^α norm on the complex unit circle

☆ The authors are supported by German Research Foundation (DFG).
E-mail addresses: chriguen@math.upb.de (C. Günther), kus@math.upb.de (K.-U. Schmidt).

http://dx.doi.org/10.1016/j.jcta.2016.08.006

arises naturally in complex analysis [27,28,6,12], condensed matter physics [3], and the design of sequences for communications devices [13,2].

Recall that, for $1 \le \alpha < \infty$, the L^α norm on the unit circle of a polynomial $f \in \mathbb{C}[z]$ is

$$\|f\|_\alpha = \left(\frac{1}{2\pi} \int_0^{2\pi} \left| f(e^{i\phi}) \right|^\alpha d\phi \right)^{1/\alpha}.$$

The L^4 norm has received particular attention because it is easier to calculate than most other L^α norms. Specifically, the L^4 norm of $f \in \mathbb{C}[z]$ is exactly the sum of the squared magnitudes of the coefficients of $f(z)\overline{f(z^{-1})}$. It is customary (see [6], for example) to measure the smallness of the L^4 norm of a polynomial f by its *merit factor* $F(f)$, defined by

$$F(f) = \frac{\|f\|_2^4}{\|f\|_4^4 - \|f\|_2^4},$$

provided that the denominator is nonzero. Note that, if f is a Littlewood polynomial of degree $n-1$, then $\|f\|_2 = \sqrt{n}$ and so a large merit factor means that the L^4 norm is small.

We note that Golay's original equivalent definition [13] of the merit factor involves the aperiodic autocorrelations (which are precisely the coefficients of $f(z)\overline{f(z^{-1})}$) of the sequence formed by the coefficients of f.

In spite of substantial progress on the merit factor problem in the last fifty years (see [19,17,7] for surveys and [20] for a brief review of more recent work), modulo generalisations and variations, only three nontrivial families of Littlewood polynomials are known, for which we can compute the asymptotic merit factor. These are: Rudin–Shapiro polynomials and polynomials whose coefficients are derived either from multiplicative or additive characters of finite fields. As shown by Littlewood [28], Rudin–Shapiro polynomials are constructed recursively in such a way that their merit factor satisfies a simple recurrence, which gives an asymptotic value of 3. The largest asymptotic merit factors that have been obtained from the other two families equal cubic algebraic numbers $6.342061\ldots$ and $3.342065\ldots$, respectively [21,20] (see Corollary 2.4 and Theorem 2.1 in this paper for precise statements).

The latter two families of polynomials are closely related to classical difference sets, namely Paley and Singer difference sets. Recall that a *difference set* with parameters (n, k, λ) is a k-subset D of a finite group G of order n such that the $k(k-1)$ nonzero differences of elements in D hit every nonzero element of G exactly λ times (so that $k(k-1) = \lambda(n-1)$). We are interested in the case that the group G is cyclic. In this case, we fix a generator θ of G and associate with a subset D of G the Littlewood polynomial

$$f_{r,t}(z) = \sum_{j=0}^{t-1} \mathbb{1}_D(\theta^{j+r}) z^j, \tag{1}$$