

SCHMIDT, Bernhard

Associate Professor

Division of Mathematical Sciences
School of Physical & Mathematical Sciences
MS (Mathematics) Giessen
PhD (Mathematics) Augsburg



*Major Research Interest: Finite Geometries;
Computational Algebraic Number Theory*

Email: bernhard@ntu.edu.sg

<http://www.ntu.edu.sg/home/bernhard/>

Tel: (65) 6790 3740

Combinatorial theory and algebraic methods

I am working on the existence theory of finite combinatorial structures (sequences, finite geometries, codes) with “nice” algebraic properties. To obtain constructions or nonexistence proofs, any useful methods are welcome, but the main tools I use come from Algebra and Number Theory. This approach is often combined with heavy computer searches. Some examples of results obtained in this way are described below.

Hadamard matrices and Barker sequences

An *Hadamard matrix of order n* is an n by n matrix H with entries -1 and 1 such that any two rows of H are orthogonal. A matrix is called *circulant* if any row of the matrix can be obtained from the first row by a cyclic shift. The *Hadamard Conjecture* states that a Hadamard matrix of order n exists whenever n is divisible by 4 . The Hadamard Conjecture goes back to Paley (1933), but is still wide open despite of half a century of intensive research. The *Circulant Hadamard Matrix Conjecture* states that there is no circulant Hadamard matrix of order greater than 4 . This conjecture is especially interesting because of its connection to Signal Processing and Information Theory. A *Barker sequence* is a binary sequence all of whose nontrivial aperiodic autocorrelation coefficients are -1 , 0 , or 1 . It is conjectured that there is no Barker sequence of length >13 .

Some of my results on these problems:

- For any set S of primes there are at most finitely many numbers of the form

$$\prod_{p \in S} p^{e(p)}, e(p) \in \mathbb{Z}^+$$

which are orders of circulant Hadamard matrices or length of Barker sequences.

- There is no circulant Hadamard matrix of order n with $4 < n < 548,964,900$

- There is no Barker sequence of length L with $13 < L < 10^{22}$

Selected Publications

1. Proof of the prime power conjecture for projective planes of order n with abelian collineation groups of order n^2 . A. Blokhuis, D. Jungnickel, B. Schmidt, Proc. Amer. Math. Soc. 130 , 1473-1476 (2002)
2. Asymptotic nonexistence of difference sets in dihedral groups. K.H. Leung , B. Schmidt, J. Combin. Theory Ser. A 99 , 261-280 (2002)
3. Constructions of Relative Difference Sets with Classical Parameters and Circulant Weighing Matrices. K.H. Leung, S.L. Ma, B. Schmidt, J. Combin. Theory Ser. A 99 , 111-127 (2002)
4. Nonexistence of abelian difference sets: Lander's conjecture for prime power orders. K.H. Leung, S.L. Ma, B. Schmidt, Trans. Amer. Math. Soc. 356 , 4343-4358 (2004)
5. The Field Descent Method. K.H. Leung, B. Schmidt, Des. Codes Cryptogr. 36 , 171-188 (2005)

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \end{pmatrix}$$

An Hadamard matrix