ICM 1998, Berlin, Aug. 18–27

Abstracts of Plenary and Invited Lectures

Section:

13. Combinatorics

1991 MS Classification: 05, 11, 14, 94

Niederreiter, Harald, Austrian Academy of Sciences, Austria

Nets, (t, s)-sequences, and algebraic curves over finite fields with many rational points

Nets and (t, s)-sequences are finite point sets, respectively infinite sequences, satisfying strong uniformity properties with regard to their distribution in the s-dimensional unit cube $I^s = [0, 1]^s$. The general theory of these combinatorial objects was first developed by the speaker [2], and they have attracted a lot of interest in recent years because of their applications to difficult problems of scientific computing, such as high-dimensional numerical integration. For a given dimension $s \geq 1$ and integers $b \geq 2$ and $0 \leq t \leq m$, a (t, m, s)-*net in base* b is a point set P consisting of b^m points in I^s such that every subinterval J of I^s of the form $J = \prod_{i=1}^{s}[a_i b^{-d_i}, (a_i + 1)b^{-d_i})$ with integers $d_i \geq 0$ and $0 \leq a_i < b^{d_i}$ for $1 \leq i \leq s$ and with $\mathrm{Vol}(J) = b^{t-m}$ contains exactly b^t points of P. Furthermore, a sequence $\mathbf{x}_0, \mathbf{x}_1, \ldots$ of points in I^s is a (t, s)-*sequence in base* b if for all integers $k \geq 0$ and $m > t$, the point set consisting of the $\mathbf{x}_n$ with $kb^m \leq n < (k+1)b^m$ is a (t, m, s)-net in base b.

It was realized early on (see [2], [3]) that (t, m, s)-nets are closely linked with classical combinatorial objects such as MOLS and orthogonal arrays. In fact, there is a combinatorial equivalence between (t, m, s)-nets and certain generalized orthogonal arrays. This implies combinatorial obstructions to the existence of (t, m, s)-nets and (t, s)-sequences and leads to the lower bounds in the recent tables [1] for the quality parameter t.

Powerful methods of constructing (t, m, s)-nets and (t, s)-sequences can be based on algebraic geometry, and the currently best results are achieved by using algebraic curves over finite fields with many rational points (see [4], [5]). For a prime power q and an integer $g \geq 0$, let $N_q(g)$ be the maximum number of $\mathbf{F}_q$-rational points that a smooth, projective, absolutely irreducible algebraic curve over $\mathbf{F}_q$ of genus g can have. Then it has been shown, for instance, that for every q and every dimension $s \geq 1$ there exists a $(V_q(s), s)$-sequence in base q, where $V_q(s) = \min\{g \geq 0 : N_q(g) \geq s + 1\}$.

In view of this connection, the speaker and C. P. Xing have embarked on a systematic search for algebraic curves over $\mathbf{F}_q$ with many rational points, in order to obtain good lower bounds for $N_q(g)$; upper bounds can be derived by a known technique from Weil's explicit formula for the number of rational points in terms of the zeta function of an algebraic curve over $\mathbf{F}_q$. This research has led to new principles for the construction of algebraic curves over

$\mathbf{F}_q$ with many rational points, among them methods based on Hilbert class fields and Drinfeld modules of rank 1. The full paper will contain an up-to-date table of lower and upper bounds on $N_q(g)$ for $q = 2, 3, 4, 5, 8, 9, 16, 27$ and all $g \leq 50$.
Related work of the speaker and C. P. Xing [6] used algebraic curves over $\mathbf{F}_q$ with many rational points, or equivalently global function fields over $\mathbf{F}_q$ with many rational places, to produce an improvement on the classical Gilbert-Varshamov bound for the existence of good linear codes over $\mathbf{F}_q$ in the case where q is a sufficiently large composite nonsquare. This extends the well-known result in [7] for squares q.

References

[1] A. T. Clayman, K. M. Lawrence, G. L. Mullen, H. Niederreiter, and N. J. A. Sloane, Updated tables of parameters of (t, m, s)-nets, *J. Combinatorial Designs*, to appear.

[2] H. Niederreiter, Point sets and sequences with small discrepancy, *Monatsh. Math.* **104**, 273–337 (1987).

[3] H. Niederreiter, Orthogonal arrays and other combinatorial aspects in the theory of uniform point distributions in unit cubes, *Discrete Math.* **106/107**, 361–367 (1992).

[4] H. Niederreiter and C. P. Xing, Low-discrepancy sequences and global function fields with many rational places, *Finite Fields Appl.* **2**, 241–273 (1996).

[5] H. Niederreiter and C. P. Xing, Quasirandom points and global function fields, *Finite Fields and Applications* (S. Cohen and H. Niederreiter, eds.), pp. 269–296, Cambridge Univ. Press, Cambridge, 1996.

[6] H. Niederreiter and C. P. Xing, Towers of global function fields with asymptotically many rational places and an improvement on the Gilbert-Varshamov bound, *Math. Nachr.* , to appear.

[7] M. A. Tsfasman, S. G. Vlăduţ, and T. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, *Math. Nachr.* **109**, 21–28 (1982).