Pancakes and crooked graphs

van Dam, E.R.

Published in:
Dima Fon-Der-Flaass

Document version:
Peer reviewed version

Publication date:
2012

Pancakes and crooked graphs*

Edwin R. van Dam
Tilburg University, Dept. Econometrics & O.R.
PO Box 90153, 5000 LE Tilburg, The Netherlands
email: Edwin.vanDam@uvt.nl

Abstract

We give a very brief account of the work of Dima Fon-Der-Flaass on pancakes and distance-regular graphs.

Pancakes

Thinking back of Dima, I have only positive memories. Working with Dima was fun! Having him as a visitor was even more fun. I remember very well that on one of his visits to Tilburg, he invited me over for lunch at the hotel. No ordinary lunch, no: he baked delicious pancakes in his hotel room. That is Dima as I will remember and miss him. Dima's recipe for the pancakes: keep your feet on the ground, be creative and surprising.

Distance-regular graphs

A distance-regular graph with intersection array $\{b_0, b_1, ..., b_{d-1}; c_1, ..., c_d\}$ is a connected graph with diameter d such that for every vertex x and vertex y at distance i from x, the number of neighbours of y at distance $i-1$ from x equals c_i, and the number of neighbours of y at distance $i+1$ from x equals b_i, for all i. Such a graph is regular with valency b_0 (for more basic information on distance-regular graphs, see [3]).

Crooked graphs

De Caen, Mathon, and Moorhouse [7] constructed distance-regular graphs with intersection array $\{2^{2t}-1, 2^{2t}-2, 1; 1, 2, 2^{2t}-1\}$. Such graphs are antipodal covers of the complete graph. The graphs are easily defined as follows. Let $GF(2^{2t-1}) \times GF(2) \times GF(2^{2t-1})$ be the vertex set. Two vertices (a, i, α) and (b, j, β) are adjacent precisely if

$$\alpha + \beta = a^2b + ab^2 + (i + j)(a^3 + b^3).$$

Actually, the graphs are defined in somewhat greater generality; and they are related to the Preparata codes; see [7] for details. The construction also allows for taking quotients. In this way distance-regular graphs with intersection arrays $\{2^{2t}-1, 2^{2t}-2^i, 1; 1, 2^i, 2^{2t}-1\}$

*In memory of Dima Fon-Der-Flaass. Presented at the International Conference on Algebraic and Geometric Combinatorics, Gyeongju, Korea, July 13, 2010. The author thanks Misha Klin for useful comments.

for $i = 1, ..., 2t$ arise. Prior to this construction, no distance-regular graphs with these intersection arrays were known for $i < t$.

Together with Bending [1], Dima very creatively introduced the concept of crooked functions to generalize this construction. Let V be an n-dimensional vector space over $GF(2)$. A function $Q : V \to V$ is called crooked if it satisfies the following three properties:

$Q(0) = 0$;
$Q(x) + Q(y) + Q(z) + Q(x + y + z) \neq 0$ for any three distinct x, y, z;
$Q(x) + Q(y) + Q(z) + Q(x + a) + Q(y + a) + Q(z + a) \neq 0$ if $a \neq 0$ (x, y, z arbitrary).

A crooked function Q is a bijection such that $H_a(Q) := \{Q(x) + Q(x + a) : x \in V\}$ is the complement of a hyperplane for every $a \neq 0$. These sets $H_a(Q)$ are all distinct, so every complement of a hyperplane appears among them exactly once.

Given a crooked function Q, a distance-regular 'crooked' graph with the same intersection array as the above one can be defined. Now the vertex set is $V \times GF(2) \times V$, and two vertices (a, i, α) and (b, j, β) are adjacent precisely if

$$\alpha + \beta = Q(a + b) + (i + j + 1)(Q(a) + Q(b)).$$

The crooked function that gives the graphs of De Caen, Mathon, and Moorhouse is given by $Q(x) = x^3$ on $V = GF(2^n)$ for odd n (and more generally $Q(x) = x^{2^e+1}$ with $\gcd(e, n) = 1$).

Crooked functions form a special class of almost bent functions, which in turn form a special class of almost perfect nonlinear functions. Recently, a lot of new quadratic almost perfect nonlinear functions have been discovered. For odd n, each such function is almost bent. If in addition the function is bijective and maps 0 to 0, then it is also crooked (cf. [9, p. 92]). A new family of crooked functions was thus constructed by Budaghyan, Carlet, and Leander [4, Prop. 1]. See also [2], but beware that a less strict definition of crookedness (compared to Dima's definition) is used there.

Dima and I [9] showed that almost bent (and hence crooked) functions can be used also to construct distance regular graphs with the same intersection array as a Kasami distance regular graph [3, Theorem 11.2.1, (13), $q = 2$]. They are defined on vertex set $V \times V$, with two vertices (a, α) and (b, β) being adjacent precisely if

$$\alpha + \beta = Q(a + b).$$

Using crooked functions, we [8] also constructed symmetric five-class association schemes similar to those constructed in [5] from Kasami graphs, and uniformly packed codes with the same parameters as the double error-correcting BCH codes (Kasami codes) and Preparata codes.

Nonlinear functions and accomplices

Crooked functions, almost bent, and almost perfect nonlinear functions have, in some sense, an extremely high degree of nonlinearity. These type of functions play an important role in cryptography. In [9], Dima and I described several characterizations of the mentioned classes of nonlinear functions. We also gave an overview of constructions of all kinds of combinatorial objects from these functions, such as semi-biplanes, difference sets, distance regular graphs, symmetric association schemes, and uniformly packed codes. We even came up with a further generalization of the crooked graphs using 'accomplices' of almost bent functions (not surprisingly, a crooked function is an accomplice of itself).

Prolific constructions

With De Caen [6], Dima obtained yet another generalization of the above mentioned distance-regular graphs, by using Latin squares. This initiated the prolific construction by Dima [13] of distance-regular n-covers of complete graphs K_{n^2} by using affine planes of order n. Dima realized that, in general, his method produces many (potentially) non-isomorphic such graphs; at least $2^{\frac{1}{2}n^3 \log n(1+o(1))}$ to be more precise. Computational results by Degraer and Coolsaet [10] confirm this. Muzychuk [14] later extended Dima's prolific ideas further.

Nonexistence and the Fon-Der-Flaass graph?

There are quite some feasibility conditions known on possible intersection arrays of distance-regular graphs. Still, there are many intersection arrays for which it is undecided whether there can be distance-regular graphs with such an array. The monograph by Brouwer, Cohen, and Neumaier [3] contains a list of intersection arrays passing the known (in 1989 to the authors) conditions. Dima contributed by eliminating two possibilities from that list: $\{5, 4, 3; 1, 1, 2\}$ [11] and $\{5, 4, 3, 3; 1, 1, 1, 2\}$ [12].

One of the smaller — still 'open' — intersection arrays is $\{7, 6, 6; 1, 1, 2\}$. Deciding whether a distance-regular graph with this intersection array exists is an intriguing open problem that would have been an ideal one to work on with Dima. In fact, I wouldn't be surprised if he at least played a bit with this problem. So if someone wants to solve it: keep your feet on the ground, be creative and surprising. If such a graph exists, I would call it the Fon-Der-Flaass graph!

References

[1] T. Bending, D. Fon-Der-Flaass. Crooked functions, bent functions, and distance regular graphs, *Electronic J. Combinatorics* 5 (1998), R34.

[2] J. Bierbrauer. A family of crooked functions, *Des. Codes Cryptography* 50 (2009), 235–241.

[3] A.E. Brouwer, A.M. Cohen, A. Neumaier. *Distance-Regular Graphs*, Springer-Verlag, 1989.

[4] Budaghyan, L., Carlet, C., Leander, G., Two classes of quadratic APN binomials inequivalent to power functions, *IEEE Trans. Inf. Th.* 54 (2008), no. 9, 4218–4229.

[5] D. de Caen, E.R. van Dam. Association schemes related to Kasami codes and Kerdock sets, *Des. Codes Cryptography* 18 (1999), 89–102.

[6] D. de Caen, D. Fon-Der-Flaass. Distance regular covers of complete graphs from Latin squares, *Des. Codes Cryptography* 34 (2005), 149–153.

[7] D. de Caen, R. Mathon, G.E. Moorhouse. A family of antipodal distance-regular graphs related to the classical Preparata codes, *J. Algebraic Combin.* 4 (1995), 317–327.

[8] E.R. van Dam, D. Fon-Der-Flaass. Uniformly packed codes and more distance regular graphs from crooked functions, *J. Algebraic Combin.* 12 (2000), 115–121.

[9] E.R. van Dam, D. Fon-Der-Flaass. Codes, graphs, and schemes from nonlinear functions, *European J. Combin.* 24 (2003), 85–98.

[10] J. Degraer, K. Coolsaet. Classification of three-class association schemes using backtracking with dynamical variable ordering, *Discrete Math.* 300 (2005), 71-81.

[11] D.G. Fon-Der-Flaass. There exists no distance-regular graph with intersection array $(5, 4, 3; 1, 1, 2)$, *European J. Combin.* 14 (1993), 409–412.

[12] D.G. Fon-Der-Flaass. A distance-regular graph with intersection array $(5, 4, 3, 3; 1, 1, 1, 2)$ does not exist, *J. Algebraic Combin.* 2 (1993), 49–56.

[13] D.G. Fon-Der-Flaass. New prolific constructions of strongly regular graphs, *Adv. Geom.* 2 (2002), 301–306.

[14] M. Muzychuk. A generalization of Wallis–Fon-Der-Flaass construction of strongly regular graphs, *J. Algebraic Combin.* 25 (2007), 169–187.