Vectorial bent functions

Alexander Pott

March 18, 2015

Motivation: $p = 2$, n even

Let

$$f : \mathbb{F}_2^n = \mathbb{F}_{2^n} \to \mathbb{F}_2$$

be bent!

- Highly nonlinear: Cryptography.
- Interesting constructions (spreads).
- Finite Fields.
- Covering radius of 1st-order Reed-Muller codes.

Motivation: p odd, vectorial version

Let

$$f : \mathbb{F}_p^n = \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$$

be planar!

- Semifields.
- MUBs.
- Finite Fields.
- MRD codes, Gabidulin codes.

Beautiful objects have symmetries ...

- Are all objects beautiful?
  - Planes of prime order
- Are most objects beautiful?
  - Semifields in odd characteristic.
  - APN functions.
- We are sure that most objects are ugly, but we do not know them, yet.
  - Semifields in even characteristic (KANTOR 2006)
  - bent functions: we do not know.

Oscar S. Rothaus 1976

Rothaus, Oscar S.

MR Author ID:	226290
Earliest Indexed Publication:	1958
Total Publications:	41
Total Citations:	401

⊞ Published as: Rothaus, O. ...

View Publications
Refine Search
Co-Authors
Collaboration Distance
Mathematics Genealogy Project
Citations

Co-authors (by number of collaborations)

Boen, J. R. Davies, Edward Brian Gerstenhaber, Murray Gross, Leonard Thompson, John Griggs

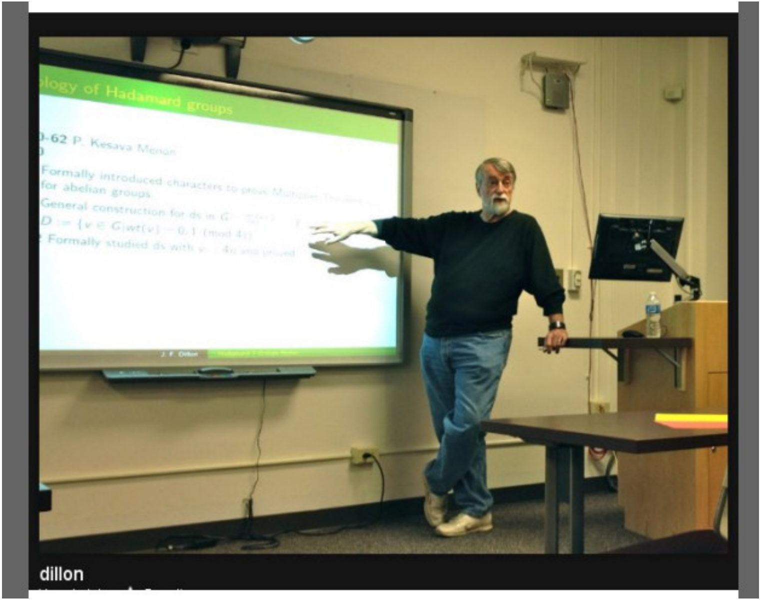
Publications (by number in area)

Combinatorics Convex and discrete geometry Functional analysis Functions of a complex variable Global analysis, analysis on manifolds Group theory and generalizations Information and communication, circuits Linear and multilinear algebra; matrix theory Manifolds and cell complexes Nonassociative rings and algebras Operator theory Optics, electromagnetic theory Ordinary differential equations Several complex variables and analytic spaces Topological groups, Lie groups

Publications (by number of citations)

Combinatorics Convex and discrete geometry Functional analysis Global analysis, analysis on manifolds Group theory and generalizations Information and communication, circuits Linear and multilinear algebra; matrix theory Manifolds and cell complexes Nonassociative rings and algebras Operator theory Ordinary differential equations Several complex variables and analytic spaces Topological groups, Lie groups

John F. Dillon 1974



Outline

- Survey some constructions.
- Walsh transform.
- normality.
- regularity.
- extendability.

Definition of bent

A function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ is called bent if

$$f(x + a) - f(x) = b$$

has 2^{n-1} solutions for all $a \neq 0$ and any b.

Example

$f(x_1, x_2, x_3, x_4) = x_1 x_2 + x_3 x_4$: Compute

$$f \begin{pmatrix} x_1 + a_1 \\ x_2 + a_2 \\ x_3 + a_3 \\ x_4 + a_4 \end{pmatrix} - f \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = x_1 a_2 + x_2 a_1 + x_3 a_4 + x_4 a_3 + a_1 a_2 + a_3 a_4$$

is linear.

Trivial necessary condition/Trivial construction

If $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is bent, then n has to be even:

$$\mathbf{H} = ((-1)^{f(x-y)})_{x,y \in \mathbb{F}_2^n}$$

which satisfies

$$\mathbf{H}^2 = 2^n \cdot \mathbf{I}.$$

Theorem (quadratic bent)

If $\mathbf{A} + \mathbf{A}^T$ is regular, then

$$x \mapsto x^T \cdot \mathbf{A} \cdot x$$

is bent.

Extension I

p odd: A function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is called bent if

$$f(x+a) - f(x) = b$$

has p^{n-1} solutions for $a \neq 0$ and any b.

Example

- As before.
- $\mathrm{Trace}(x^2)$ on $\mathbb{F}_{p^n}$ for any n, also n odd:

$$\mathrm{Trace}((x+a)^2 - x^2) = \mathrm{Trace}(2xa + a^2)$$

Extension II: Vectorial bent

Consider Trace(x^2) without Trace:

Example

$F(x) = x^2$ on $\mathbb{F}_{p^n}$ with p odd satisfies

$$F(x + a) - F(x) = b$$

has exactly one solution for all $a \neq 0$ and all b.

Using "projections" $\varphi : \mathbb{F}_p^n \to \mathbb{F}_p^m$, we find functions $f = \varphi \circ F : \mathbb{F}_p^n \to \mathbb{F}_p^m$ such that

$$f(x + a) - f(x) = b$$

has p^{n-m} solutions for all $a \neq 0$ and all b

Extension II: Vectorial bent

A function $f : \mathbb{F}_p^n \to \mathbb{F}_p^m$ is vectorial bent if

$$f(x + a) - f(x) = b$$

has p^{n-m} solutions for all $a \neq 0$ and all b.

$m = n$ planar: projective planes, connection with semifields.

Extension III

Do we have vectorial bent functions $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$?

Example ($n = 2m$)

$$\begin{array}{rccc} f: & \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} & \to & \mathbb{F}_{2^m} \\ & (x, y) & \mapsto & x \cdot y \end{array}$$

Theorem (NYBERG 1993; SCHMIDT 1995)

If $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is vectorial bent, then n is even and $m \leq n/2$.

Conclusion

The necessary conditions for the existence of vectorial bent functions $f : \mathbb{F}_p^n \to \mathbb{F}_p^m$ are also sufficient:

- $p = 2$: n even and $m \leq n/2$
- p odd: $m \leq n$.

What else can we do?

Generalizing the differential properties

- Other groups: JEDWAB, DAVIS, SCHMIDT, LEUNG, MA, P. '90.
- $p = 2$ and $n = m$: Modified planar functions (ZHOU 2013, HORADAM 2007).
- $\mathbb{Z}_4$ bent (many authors '90).

The Walsh transform: the Boolean case

Given a function $f : \mathbb{F}_p^n \to \mathbb{F}_p$, then $\mathcal{F} : \mathbb{F}_p^n \to \mathbb{C}$ such that

$$\mathcal{F}(a) = \sum_{x \in \mathbb{F}_p^n} \zeta_p^{f(x)+\langle a,x \rangle}$$

is the Walsh transform of f (where ζ_p complex p-th root of unity).

Theorem

f is bent if and only if

$$|\mathcal{F}(a)| = p^{n/2}.$$

for all a.

The Walsh transform: the vectorial case

Given a function $f : \mathbb{F}_p^n \to \mathbb{F}_p^m$, then $\mathcal{F} : \mathbb{F}_p^{n+m} \to \mathbb{C}$ such that

$$\mathcal{F}(a, b) = \sum_{x \in \mathbb{F}_p^n} \zeta_p^{\langle b, f(x) \rangle + \langle a, x \rangle}$$

is the Walsh transform of f.

Theorem

f is vectorial bent if and only if

$$|\mathcal{F}(a, b)| = p^{n/2}.$$

for all a, b, $b \neq 0$

If $p = 2$:

$$2^{n-1} - \frac{1}{2} \max |\mathcal{F}(a, b)|$$

is called the non-linearity of f.

Generalizing the non-linearity properties

Goal: minimize $\max |\mathcal{F}(a,b)|$, achieved for vectorial bent functions.

Generalizations are only of interest if $p = 2$.

- n odd, $m = 1$: Covering radius problem for Reed-Muller code PATTERSON, WIEDEMANN 1983; MYKKELTVEIT ($n = 7$) 1980; KAVUT, YÜCEL ($n = 9$) 2010.
- $n = m$ odd: almost bent functions.
- n odd $m < n$?
- n even and $m > n/2$?

It seems that we miss something ...

There are MANY bent functions, but only very few of them can be described by a theorem! Not much is known about equivalence classes:

n	No. of bent functions
$n = 4$	896
$n = 6$	$5,425,430,528$
$n = 8$	$99,270,589,265,934,370,305,785,861,242,880$

LANGEVIN, LEANDER 2009 ($n = 8$), PRENEEL 1993 ($n = 6$)
Only a few of the $n = 8$ examples are explained by a theorem.

Equivalence

$f, g : \mathbb{F}_p^n \to \mathbb{F}_p^m$ are equivalent if the graphs

$$G_f := \{(x, f(x)) \ : \ x \in \mathbb{F}_p^n\} \subseteq \mathbb{F}_p^{n+m}$$

and

$$G_g := \{(x, g(x)) \ : \ x \in \mathbb{F}_p^n\} \subseteq \mathbb{F}_p^{n+m}$$

are in the same orbit of $\mathrm{AGL}(n + m, p)$.

One may also use isomorphism of corresponding designs.

The Maiorana-McFarland construction

$F : \mathbb{F}_{p^m}^2 \to \mathbb{F}_{p^m}$ such that

$$F\begin{pmatrix} x \\ y \end{pmatrix} = x \cdot \pi(y) + \rho(y)$$

is bent if π is a permutation and $\rho : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ arbitrary:

$$(x + a) \cdot \pi(y + b) + \rho(y + b) - x \cdot \pi(y) - \rho(y)$$

$$= x(\pi(y + b) - \pi(y)) +$$

terms depending on y.

The spread construction

Decompose $V = \mathbb{F}_p^{2m}$ into $p^m + 1$ subspaces which meet pairwise in $\{0\}$, call them U_∞ and U_v, $v \in \mathbb{F}_{p^m}$ (spread).

Let π be a permutation on $\mathbb{F}_p^m$. Then $F : \mathbb{F}_p^{2m} \to \mathbb{F}_p^m$ such that

$$F(x) = \begin{cases} v_0 & \text{if } x \in U_\infty \\ \pi(v) & \text{if } x \in U_v \setminus \{0\} \end{cases}$$

is vectorial bent.

For bent functions $\mathbb{F}_p^{2m} \to \mathbb{F}_p^2$, partial spreads are sufficient!

Niho construction

Consider

$$U_v := \{(x, v \cdot x) \ : \ x \in \mathbb{F}_{2^m}\}$$

and

$$U_\infty := \{(0, x) \ : \ x \in \mathbb{F}_{2^m}\}$$

Let $\pi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be a permutation such that $\pi(x) + a \cdot x$ is $2 - 1$ mapping for all $a \neq 0$. Then

$$F(x) = \begin{cases} 0 & \text{if } x \in U_\infty \\ \pi(v) \cdot x & \text{if } x \in U_v \setminus \{0\}. \end{cases}$$

is bent.

Connection to geometry

$\pi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is a permutation such that $\pi(x) + a \cdot x$ is $2 - 1$ mapping for all $a \neq 0$ means π is an o-polynomial (hyperoval!)

DILLON 1974; CARLET, MESNAGER; BUDAGHYAN, HELLESETH, KHOLOSHA '10

Çeşmelioğlu, Meidl, P. 2015

Theorem
A "mix" of linear and constant functions on the spread is impossible.

Theorem
Only works for $p = 2$.

Theorem
There are also other spreads that can be used, but the corresponding (known) bent functions are Maiorana-McFarland.

Question
Is it possible to use other functions on the spread? Cyclotomy?

Normal bent functions

All the constructions above ($p = 2$) are normal: There is a subspace of dimension $n/2$ on which f is affine.

Theorem (CANTEAUT, DAUM, DOBBERTIN, LEANDER 2006)

$Trace(a \cdot x^{57})$ is non-normal bent on $\mathbb{F}_{2^{14}}$ when $a \in \mathbb{F}_4 \setminus \mathbb{F}_2$ (plus recursion).

Question

Are most bent functions non-normal, and we know only the nice examples?

Theorem (Çeşmelioğlu, Meidl, P. 2014)

If p is odd and n even, one class of quadratic bent functions on $\mathbb{F}_{p^n}$ are not normal (elliptic quadrics).

(weak) regularity (only for p odd interesting)

All the constructions of bent functions f presented so far are regular:

$$\mathcal{F}(v) \in \{\Gamma \cdot \zeta_p^i\}$$

where Γ is independent from v.
$\Gamma \neq p^{n/2}$: weakly regular.

Question

Are most bent functions not (weakly) regular?

Some sporadic examples are known (Tan, Yang, Zhang 2010, Helleseth, Kholosha 2010) as well as only one generic construction method (Çeşmelioğlu, McGuire, Meidl 2012) and a recursive construction.

Theorem (Çeşmelioğlu, Meidl, P. 2013)

If n is even and f weakly regular, then f is not normal.

Extendability

A bent function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is extendable if there is a vectorial bent $F : \mathbb{F}_p^n \to \mathbb{F}_p^2$ such that

$$F(x) = \begin{pmatrix} f(x) \\ g(x) \end{pmatrix}$$

If $p = 2$, all constructions (perhaps with the exception of partial spreads) are extendable. If p is odd and $n = 2$, there are non-extendable bent functions.

Question

Are most bent functions not extendable?

Some computational results: $q = 3$, $n = 4$

Özbudak computed quadratic bent functions $f : \mathbb{F}_3^4 \to \mathbb{F}_3^m$.
quadratic: $f(x+a) - f(x) - f(a) + f(0)$ is linear!

	inequivalent quadratic bent
$m = 1$	2
$m = 2$	7
$m = 3$	14
$m = 4$	2

- All quadratic bent functions with $m = 2$ are extendable.
- Only 5 with $m = 3$ are extendable.
- Only one of the $m = 3$ examples can be extended to both $m = 4$ examples.
- Four of the $m = 3$ examples extend to the non-Desarguesian commutative semifield ($x^4 + x^{10} - x^{36}$).

Extendability of quadratic bent functions

If $p = 2$, quadratic bent functions are

$$x \mapsto x^T \cdot \mathbf{A} \cdot x$$

where $\mathbf{A} + \mathbf{A}^T$ is invertible, without loss of generality

$$\mathbf{A} = \begin{pmatrix} \mathbf{U} & 0 & \dots & 0 \\ 0 & \mathbf{U} & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \dots & \dots & \mathbf{U} \end{pmatrix}$$

where $\mathbf{U} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

The number of quadratic bent functions and the number of inequivalent functions is known.

The 2-dimensional case

- How many (say N) quadratic bent functions $f : \mathbb{F}_2^n \to \mathbb{F}_2^2$ without linear terms?
- How many inequivalent ones?

Theorem (P., Schmidt, Zhou 2014/15)

Let $n = 2m$ be even and let X be the set of $n \times n$ alternating matrices over $\mathbb{F}_2$. Then

$$N = \frac{v}{2^m} \sum_{i=0}^{m} (-1)^i \, 2^{i(i-1)} \begin{bmatrix} m \\ i \end{bmatrix} \prod_{k=1}^{m-i} (2^{2k-1} - 1)^2,$$

where

$$v = 2^{m(m-1)} \prod_{k=1}^{m} (2^{2k-1} - 1)$$

is the number of nonsingular matrices in X.

Classification results for quadratic bent functions

$$f : \mathbb{F}_p^n \to \mathbb{F}_p^m, \qquad p \text{ prime}$$

- $p = 2, m = 1$: Only one example.
- p odd, n even, $m = 1$: Two examples
- p odd, n odd, $m = 1$: One example
- p odd, $n = m = 2$: One example
- p odd, $n = 3, m = 3$: Two examples (Menichetti 1977)
- p odd, $n = 3, m = 2$: One example (Özbudak, P. 2014)

Conclusion

- Survey of known constructions of (vectorial) bent functions.
- Apparently, we know only a few bent functions.
- Most bent functions are perhaps non-normal ($p = 2$), but all constructions are normal, similarly non-regular-
- Most bent functions are perhaps not extendable, but almost all constructions are extendable.
- Number of quadratic vectorial bent functions?