Alltop Functions

Joanne L. Hall
Asha Rao, Stephen M. Gagola III

57th Meeting of the Australian Mathematical Society
October 2013

Outline

Planar functions

Outline

Planar functions

Alltop functions

Outline

Planar functions

Alltop functions

Applications

Outline

Planar functions

Alltop functions

Applications

Open problems

Outline

Planar functions

Alltop functions

Applications

Open problems

Planar functions

A function on a feild $\mathbb{F}$ is called a planar function if for every $a \in \mathbb{F}$ with $a \neq 0$, the function $\Delta_{f,a} : x \mapsto f(x+a) - f(x)$ is a permutation of $\mathbb{F}$.

Also called

- perfect nonlinear functions,
- differentially 1-uniform functions.

x	$f(x) = x^2$	$\Delta_{f,1} = (x+1)^2 - x^2$	$\Delta_{f,2} = (x+2)^2 - x^2$
0	0	1	1
1	1	0	2
2	1	2	0

x^2 is a planar function on $\mathbb{F}_3$.

Applications of Planar functions

- Geometry
  - Contruct affine Plane
- Cryptographic Protocols
  - Bent function
  - Perfect Nonlinear Functions
- Mutually Unbiased Bases
- CDMA signal sets
- Hadamard Matrices

Known Planar Functions

- x^2
- x^{p^k+1} on $\mathbb{F}_{p^r}$ such that $r/gcd(r,k)$ is odd. [Dembowski & Ostrom, 1968]
- $$x^2 + j\frac{(x - x^{p^r})^2}{(\beta - \beta^{p^r})^2} - \beta^2\frac{(x - x^{p^r})^2}{(\beta - \beta^{p^r})^2}$$
  on $\mathbb{F}_{p^{2r}}$ where j is a non-square and beta is non-zero. [Dickson, 1906, Bundunghyn & Helleseth 2008]
- $$x^{p^r+1} + \omega(\beta x^{p^s+1} + \beta^{p^r} x^{(p^s+1)p^r})$$
  on $\mathbb{F}_{p^{2r}}$ where $\omega^{p^r} = -\omega$, there is no $a \in \mathbb{F}^*_{p^{2r}}$ such that $a^{p^r} = -a$ and $a^{p^s} = -a$ and β^{p^r-1} is not contained in the subgroup of order $p^r + 1/gcd(p^r+1, p^s+1)$. [Bierbrauer, 2009]
- $\ldots$

More known planar functions

- $x^{10} \pm x^6 - x^2$ on $\mathbb{F}_{3^r}$. [Coulter & Mathews, 1997]
- $x^2 + x^{90}$ on $\mathbb{F}_{3^5}$. [Weng, 2007]
- $x^{(3^k+1)/2}$ on $\mathbb{F}_{3^r}$ where k is odd and $gcd(k, r) = 1$. [Coulter & Mathews,1997]
- $x^2 + x^{2p^r} + x^{p^k+1} - x^{(p^k+1)p^r}$ on $\mathbb{F}_{p^{2r}}$ such that $2r/gcd(2r, k)$ is odd. [Gagola & Hall, 2013]
- ...

Outline

Planar functions

Alltop functions

Applications

Open problems

Alltop functions

Definition

A function on a feild $\mathbb{F}$ is called an Alltop function if for every $a \in \mathbb{F}$ with $a \neq 0$, the function $\Delta_{f,a} : x \mapsto f(x+a) - f(x)$ is a planar function of $\mathbb{F}$.

Also called planar difference function.

Known Alltop functions

- x^3. [Alltop 1980]

A new family of Alltop functions

Lemma [Hall, Rao & Donovan 2012]

If $A(x)$ is an Alltop function on $\mathbb{F}_{p^{2r}}$, then $p \geq 5$.

Theorem [Hall, Rao & Gagola 2013]

Let $A(x) = x^{p^r+2}$ on $\mathbb{F}_{p^{2r}}$. If $p \geq 5$, and 3 does not divide $(p^r + 1)$ then $A(x)$ is an Alltop function.

Outline

Planar functions

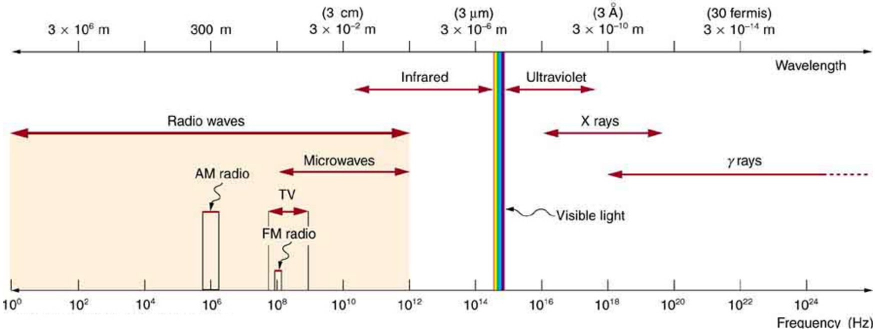
Alltop functions

Applications

Open problems

The electromagnetic spectrum

A finite and valuable resource



Source: openstax college, creative commons

Signal Sets

Theorem [Hall, Rao & Gagola, 2013]

Let $A(x)$ be a Alltop function on $\mathbb{F}_q$. Let

$$c_{ab} = \frac{1}{\sqrt{q}} \left(\omega_p^{tr(A(x+a)+b(x+a))} \right)_{x \in \mathbb{F}_q}$$

Let $C_\Pi = \{c_{ab} : a, b \in \mathbb{F}_q\} \cup E$. Then C_Π is a $(q^2 + q, q)$ signal set with $I_{\max} = \frac{1}{\sqrt{q}}$.

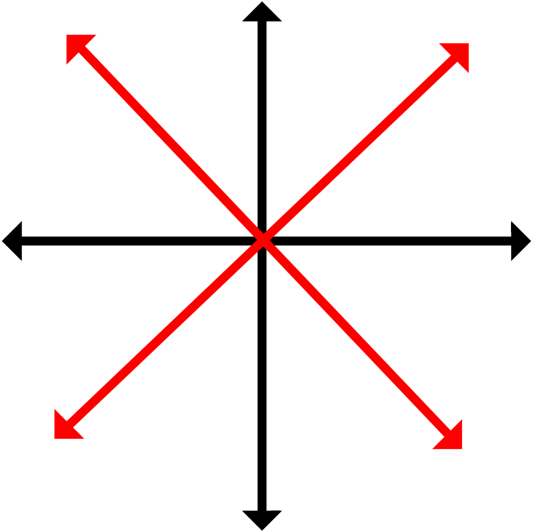
- Optimal with respect to Maximum bound on auto and cross correlation.
- Optimal with respect to RMS bound on auto and cross correlation.

Already known for $A(x) = x^3$. [Alltop, 1980]

Using an Alltop function on field with q elements, we can find as set of $q^2 + q$ signals with minimal interference.

These signal sets with $A(x) = x^3$ have been used in radar applications [Ender, 2010].

Measuring photons



Mutually unbiased bases in $\mathbb{R}^2$

Mutually Unbiased Bases

Theorem [Hall, Rao & Gagola, 2013]

Let $\mathbb{F}_q$ be a field of odd characteristic p. Let $A(x)$ be a Alltop function on $\mathbb{F}_q$. Let $V_a := \{\vec{v}_{ab} : b \in \mathbb{F}_q\}$ be the set of vectors

$$\vec{v}_{ab} = \frac{1}{\sqrt{q}} \left(\omega_p^{tr(A(x+a)+b(x+a))} \right)_{x \in \mathbb{F}_q}$$

with $a, b \in \mathbb{F}_q$. The standard basis E along with the sets V_a, $a \in \mathbb{F}_q$, form a complete set of $q+1$ MUBs in $\mathbb{C}^q$.

Using an Alltop function on field with q elements, a complete set of mutually unbiased can be constructed.

Already known for $A(x) = x^3$. [Klappeneker and Röttler, 2003]

Outline

Planar functions

Alltop functions

Applications

Open problems

Open Problems

Algebra

- Find new planar functions
- Find new Alltop functions

Geometry

- What geometric structure do Alltop functions produce?

Telecommunications

- Physical Implementation

Quantum physics

- Physical Implementation

Potential Applications

- Cryptography
- Coding Theory

- Joanne L. Hall, Asha Rao, Stephen M.Gagola III,
  A family of Alltop functions that are EA-inequivalent to the cubic function
  IEEE Transactions in Communications.
  To appear.
- Joanne L. Hall, Asha Rao, Diane Donovan,
  Planar difference functions,
  IEEE International Symposium on Information Theory,
  Boston 2012. pp 1082-1086.