New construction APN quadratic functions

Zahid Mounir*

20 juillet 2011

*Université de Paris 8

Résumé

Le but de cet exposé est de détailler l'article de Mr Carlet. Au passage je ferais un rappel sur quelques résultats intéressants en théorie des corps finis, puis je donnerais des preuves (nouvelles) de quelques résultats connus, ensuite je généraliserais la construction d'une famille de fonction APN. La référence du résultat précédera ce dernier, en cas d'absence de référence, la preuve sera de l'auteur.

1 Corps finies

Certains résultats ne seront pas prouvés nous renvoyons le lecteur curieux à [1]. Certains résultats ne requièrent pas la finitude du corps, nous renvoyons le lecteur à cette référence [2], dans la suite $\mathbf{K}$ désigne un corps commutatif quelconque pas forcément fini.

Proposition 1.1. *[2] Étant donné un corps* $\mathbf{K}$.$P \in \mathbf{K}[X]$. *Le polynôme* P *n'a pas de facteur carrés si et seulement si* $\gcd(P, P') = 1$

Proposition 1.2. *[2]* $\mathbf{K}$ *corps,* $n \in \mathbb{N}_{>1}$, $s \in \mathbb{N}^*$, *dans* $\mathbf{K}[X]$ *on a :*

$$\gcd(X^s - 1, X^n - 1) = X^{\gcd(s,n)} - 1$$

Corollaire 1.1. *[2]* $\mathbf{K}$ *corps ,* $n \in \mathbb{N}_{>1}$, $s \in \mathbb{N}^*$ *:*

$$X^s - 1 | X^n - 1 \Leftrightarrow s | n \text{ dans } \mathbb{N}^*$$

Proposition 1.3. *[1]* $\mathbb{F}$ *un corps fini t.q* $\#\mathbb{F} = q$ alors $\forall x \in \mathbb{F}$

$$x^q = x. \tag{1}$$

et inversement les solution de l'equation (1) sont exactement les éléments de $\mathbb{F}$ *.*

Corollaire 1.2. *[1]* p *un nombre premier* $s, n \in \mathbb{N}^*$. *alors :*

$$\mathbb{F}_{p^s} \bigcap \mathbb{F}_{p^n} = \mathbb{F}_{p^{\gcd(s,n)}}$$

Corollaire 1.3. $\mathbb{F}_{2^n}$ *un corps fini* $\forall \beta \in \mathbb{F}_{2^n}$ $\forall a \in \mathbb{N}$ *:*

$$\beta^{2^a} = \beta^{2^{a \bmod n}}$$

Démonstration. Par division euclidienne de a par n, $\exists (q, r) \in \mathbb{N}^2$ tel que : $a = qn + r \quad$ avec $0 \leq r < n$. Donc $n | nq \Rightarrow \mathbb{F}_{2^n} \subset \mathbb{F}_{2^{nq}} \Rightarrow \forall \beta \in \mathbb{F}_{2^n}$, $\beta^{2^{qn}} = \beta$
on conclut avec : $\beta^{2^a} = \beta^{2^{qn+r}} = (\beta^{2^{qn}})^{2^r} = \beta^{2^r} = \beta^{2^{a \bmod n}}$

□

Corollaire 1.4. *Soit* n *un entier pair non nul.*

(i) $\forall x \in \mathbf{F}_{2^n}$, $x^{2^{\frac{n}{2}}+1} \in \mathbf{F}_{2^{n/2}}$

(ii) *Si* $n/2$ *impair, alors* $\mathbb{F}_{2^{n/2}} \cap \mathbb{F}_{2^2} = \mathbb{F}_2$.

Démonstration.

(i) Il suffit d'appliquer le corollaire 1.2.

(ii) En effet $\left(x^{2^{\frac{n}{2}}+1}\right)^{2^{\frac{n}{2}}} = x^{2^n + 2^{\frac{n}{2}}} = x^{2^{\frac{n}{2}}+1}$

□

Proposition 1.4. *[2] p premier, $n \in \mathbb{N}^*$ et $q = p^n$. Les $\mathbb{F}_p$-sous espaces vectorielles de $\mathbb{F}_q$ sont au nombre de :*

$$\sum_{s=0}^{n} \frac{(p^n-1)(p^{n-1}-1)\dots(p^{n-s+1}-1)}{(p^s-1)(p^{s-1}-1)\dots(p-1)}$$

Démonstration. Pour $s \in \{1,\dots,n\}$, dénombrons les $\mathbb{F}_p$-sous espaces vectorielles de dimension s de $\mathbb{F}_q$.

- Le premier vecteur étant choisi non nul : $p^n - 1$ possibilités.
- Le second vecteur,non colinéaire au premiers : $p^n - p$ possibilités.
- Le troisième vecteur non lié aux deux premiers : $p^n - p^2$ possibilités.
- ...
- Le s-ième vecteur non lié aux précédents : $p^n - p^{s-1}$ possibilités.

Il y'a donc $(p^n-1)(p^n-p)\dots(p^n-p^{s-1})$ systèmes libres à s éléments. Le même raisonnement montre qu'un $\mathbb{F}_p$-sous espace vectorielle de dimension s de $\mathbb{F}_q$ admet : $(p^s-1)(p^s-p)\dots(p^s-p^{s-1})$ bases. Le nombre de $\mathbb{F}_p$-espace vectorielle de dimension de dim s est donc :

$$\frac{(p^n-1)(p^n-p)\dots(p^n-p^{s-1})}{(p^s-1)(p^s-p)\dots(p^s-p^{s-1}} = \frac{(p^n-1)(p^{n-1}-1)\dots(p^{n-s+1}-1)}{(p^s-1)(p^{s-1}-1)\dots(p-1)}$$

□

1.1 Critère d'irréductibilité

Proposition 1.5. *[2] Soit $P \in \mathbf{K}[X]$* tel que *$D^\circ(P) \leq 3$.*
P est irréductible sur $\mathbf{K}$ si et seulement si P n'a pas de racine dans $\mathbf{K}$

Proposition 1.6. *[2] Soit $P \in \mathbf{K}[\mathbf{X}]$ avec $D^\circ(P) = n$.*
P est irréductible si et seulement si P n'a pas de racines dans toutes extension $\mathbf{L}/\mathbf{K}$ tel que : $[\mathbf{L} : \mathbf{K}] \leq n/2$.

Démonstration.

Condition nécéssaire. P irréductible sur $\mathbf{K}$. Soit $\alpha \in \mathbf{L}$, racine de P alors $\mathbf{K}(\alpha)$ est un corps de rupture de P.
Donc $[\mathbf{K}(\alpha) : \mathbf{K}] = n \Rightarrow [\mathbf{L} : \mathbf{K}] \geq n > n/2$.

Condition suffisante. Par Contraposition. Si P n'est pas irréductible, il existe $(Q, R) \in \mathbf{K}[\mathbf{X}]^2$. tel que : $P = QR$ et $1 \leq D^\circ(R), D^\circ(Q) < n$, sans perte de généralité on peut supposer que : $D^\circ(Q) \leq \frac{n}{2}$. Soit f un facteur irréductible de Q, et $\mathbf{L} = \mathbf{K}(\alpha)$ un corps de rupture de f alors $\alpha \in \mathbf{L}$ est une racine de $P(X)$ et $[\mathbf{L} : \mathbf{K}] = D^\circ(f) \leq \frac{n}{2}$.

□

Proposition 1.7. *[2] Soit $P \in \mathbf{K}[\mathbf{X}]$ irréductible, $D^\circ(P) = n$ et $\mathbf{L}/\mathbf{K}$ extension de degré m de $\mathbf{K}$ avec $\gcd(m, n) = 1$ alors P est irréductible dans $\mathbf{L}[\mathbf{X}]$.*

Démonstration. Supposons P est réductible dans $\mathbf{L}[\mathbf{X}]$, soit f un facteur irréductible de P dans $\mathbf{L}[\mathbf{X}]$ alors $0 < D^\circ(f) < n$. Soit $M = \mathbf{L}(\alpha)$ un corps de rupture de f.
P étant irréductible dans $\mathbf{K}[\mathbf{X}]$, donc $\mathbf{K}(\alpha)$ corps de rupture de P sur $\mathbf{K}$. Alors $[\mathbf{K}(\alpha) : \mathbf{K}] = n$, donc $[\mathbf{M} : \mathbf{K}] = [\mathbf{M} : \mathbf{K}(\alpha)][\mathbf{K}(\alpha) : \mathbf{K}]$ est divisible par n. Or $[\mathbf{M} : \mathbf{K}] = [\mathbf{M} : \mathbf{L}].[\mathbf{L} : \mathbf{K}] = D^\circ(f) \times m$. Comme $\gcd(m, n) = 1$, il vient n divise $D^\circ(f)$, contradiction. □

Remarque : La proposition 1.7, peut être déduite de la proposition qui va suivre, si nous avons éviter, c'est pour insister sur son caractère générique.

Proposition 1.8. *[1] Soit $P \in \mathbb{F}_q[X]$ irréductible de degré n et soit $k \in \mathbb{N}^*$, alors P se factorise en d polynômes irréductibles sur $\mathbb{F}_{q^k}[X]$ de degré n/d avec $d = \gcd(n,k)$*

1.2 Trace sur un corps

Définition 1.1. *Soient $\mathbf{K} = \mathbb{F}_q$ et $\mathbf{F} = \mathbb{F}_{q^m}$. Pour tout $\alpha \in \mathbf{F}$, la trace $\boldsymbol{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha)$ de α sur $\mathbf{K}$ est définie par :*

$$\boldsymbol{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha) = \alpha + \alpha^q + \ldots + \alpha^{q^{m-1}}$$

Si $\mathbf{K}$ est un corps premier la trace est dite absolue et on la note seulement $\boldsymbol{Tr}_{\mathbf{F}}$.

La trace a des propriétés intéressantes que nous énoncerons sous forme d'un théorème :

Théorème 1.1. *[1] Soient $\mathbf{F} = \mathbb{F}_{q^m}$ et $\mathbf{K} = \mathbb{F}_q$ alors :*

(i) $\boldsymbol{Tr}_{\mathbf{F}/\mathbf{K}}$ *est une forme $\mathbf{K}$-linéaire non nulle surjective.*

(ii) *Pour tout $a \in \mathbf{K}$, $\boldsymbol{Tr}_{\mathbf{F}/\mathbf{K}}(a) = ma$.*

(iii) *Pour tout $\alpha \in \mathbf{F}$, $\boldsymbol{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha^q) = \boldsymbol{Tr}_{\mathbf{F}/\mathbf{K}}(\alpha)$ (La trace est stable par le **Frobenius**).*

Proposition 1.9 (Transitivité de la trace)**.** *[1]*
Soient $\mathbf{K}$ un corps fini, $\mathbf{F}$ une extension finie de $\mathbf{K}$ et $\mathbf{E}$ une extension finie de $\mathbf{F}$. Alors

$$\boldsymbol{Tr}_{\mathbf{E}/\mathbf{K}} = \boldsymbol{Tr}_{\mathbf{F}/\mathbf{K}} o\, \boldsymbol{Tr}_{\mathbf{E}/\mathbf{F}}$$

Corollaire 1.5. *Soit n un entier pair non nul. Alors :*

1. $\forall x \in \mathbb{F}_{2^{n/2}}$, $\boldsymbol{Tr}_{\mathbb{F}_{2^n}}(x) = 0$. (*i.e* $\mathbb{F}_{2^{n/2}} \subset \mathcal{K}\mathrm{er}(\boldsymbol{Tr}_{\mathbb{F}_{2^n}})$)
2. *Il existe $\omega \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^{n/2}}$ tel que $\boldsymbol{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}(\omega) = 1$*

Démonstration.

1. Par définition : Pour tout $x \in \mathbb{F}_{2^n}$, $\mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}(x) = x + x^{2^{\frac{n}{2}}}$ et donc $\mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}$ est nulle sur $\mathbb{F}_{2^{n/2}}$ on conclut avec $\mathbf{Tr}_{\mathbb{F}_{2^n}} = \mathbf{Tr}_{\mathbb{F}_{2^{n/2}}} o \mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}$(cf. proposition 1.9)
2. $\mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}$ est une forme $\mathbb{F}_{2^{n/2}}$-linéaire non nulle.Donc,il existe $x_0 \in \mathbb{F}_{2^n}$ tel que $\mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}(x_0) \neq 0$. Il suffit de choisir $\omega = \frac{x_0}{\mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}(x_0)}$ est conclure par la $\mathbb{F}_{2^{n/2}}$ -linéarité de la $\mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}$.

□

Remarque : le point (2) peut-être directement prouvé on utilisant la surjectivité de la trace, seulement je voulais donner une construction effective.

Proposition 1.10. *Soient n un entier pair non nul, $q = 2^{n/2}$ et $c \in \mathbb{F}_{2^n}$ vérifiant : $c^{q+1} = 1$ alors $(\frac{1}{c^{2^{n-1}}})^q = \frac{c}{c^{2^{n-1}}}$ de plus on a :*

$$\forall \omega \in \mathbb{F}_{2^n} \quad \frac{\omega + c\omega^q}{c^{2^{n-1}}} \in \mathbb{F}_{2^{n/2}}.$$

Démonstration. $c^{q+1} = 1 \Leftrightarrow c = \frac{1}{c^q} \Rightarrow$

$$\begin{aligned}\left(\frac{1}{c^{2^{n-1}}}\right)^q &= c^{2^{n-1}} \\ &= c^{2^n - 2^{n-1}} \\ &= \frac{c^{2^n}}{c^{2^{n-1}}} \\ &= \frac{c}{c^{2^{n-1}}}\end{aligned}$$

Soit $\omega \in \mathbb{F}_{2^n}$.

$$\frac{\omega + c\omega^q}{c^{2^{n-1}}} = \frac{w}{c^{2^{n-1}}} + \omega^q \frac{c}{c^{2^{n-1}}} = \frac{\omega}{c^{2^{n-1}}} + \left(\frac{\omega}{c^{2^{n-1}}}\right)^q = \mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}\left(\frac{\omega}{c^{2^{n-1}}}\right) \in \mathbb{F}_{2^{n/2}}$$

□

1.3 Permutation particulière sur un corps fini

Lemme 1.3.1. *Soit $G =< x >$ un groupe cyclique d'ordre n. Alors $\forall d,\ d \mid n$ dans $\mathbb{N}^*$ il existe un unique sous groupe d'ordre d de G. Il est engendré par x^k, $k = \frac{n}{d}$*

Proposition 1.11. *Soient $\mathbf{F}_q$ un corps fini, $i \in \mathbb{N}^*$.*

(i) *X^i permute $\mathbf{F}_q$ si et seulement si* $\gcd(i, q-1) = 1$.

(ii) *Le nombre de i^e puissance non nulle dans $\mathbf{F}_q$ (i.e $\#{\mathbb{F}^*_q}^i$) est* $(q-1)/\gcd(i, q-1)$.

Démonstration. Remarquons d'abord que 0 est la seule solution de l'équation $X^i = 0$.
Considérons le morphisme de groupe $\mathfrak{F}_\mathfrak{i} : x \in {\mathbb{F}_q}^* \to x^i \in {\mathbb{F}^*}_q$. Calculons son noyau :

$$\mathcal{K}\mathrm{er}(\mathfrak{F}_\mathfrak{i}) = \{\, x \in {\mathbb{F}_q}^* \mid x^i = 1 \,\}$$

On a $x \in \mathcal{K}\mathrm{er}(\mathfrak{F}_\mathfrak{i}) \Rightarrow \ \mathrm{ord}(x) \mid i \Rightarrow \mathrm{ord}(x) \mid d$, ou $d = \gcd(i, q-1) \Rightarrow x \in \mathcal{K}\mathrm{er}(\mathfrak{F}_d)$ l'inverse est évidente. Donc :

$$\mathcal{K}\mathrm{er}(\mathfrak{F}_\mathfrak{i}) = \mathcal{K}\mathrm{er}(\mathfrak{F}_d) \text{ avec } d = gcd(i, q-1).$$

Le polynôme $P(x) = X^d - 1$ n'a que des racines simples. (Voir Proposition 1.1). Étant un polynôme de degré d, P a donc d racine distinct. $d \mid (q-1)$ implique $X^d - 1 \mid X^{(q-1)} - 1$. Donc tous les racines de P sont dans ${\mathbb{F}_q}^*$.
Ceci entraîne $\#\mathcal{K}\mathrm{er}(\mathfrak{F}_d) = d$.
$\mathfrak{F}_\mathfrak{i}$ est un isomorphisme si et seulement si $d = 1$, c-à-d $\gcd(i, q-1) = 1$.

D'après le 1er théorème d'isomorphisme

$${\mathbb{F}_q}^*/\mathcal{K}\mathrm{er}(\mathfrak{F}_\mathfrak{i}) \cong \mathcal{I}m(\mathfrak{F}_\mathfrak{i})$$

or $\mathcal{I}m(\mathfrak{F}_\mathfrak{i})$:= les i^e puissances non nulles dans $\mathbf{F}_q$, ce qui conclut la preuve. □

Remarque :

1. $\mathcal{I}m(\mathfrak{F}_\mathfrak{i}) = \mathcal{I}m(\mathfrak{F}_d)$; c-à-d les i^e puissances non nulles dans $\mathbf{F}_q$ sont exactement les d^e puissances non nulles dans $\mathbf{F}_q$.
2. $\forall (x, y) \in {\mathbf{F}_q}^2 \quad x^i = y^i \Leftrightarrow x^d = y^d$ (Découle de $\mathcal{K}\mathrm{er}(\mathfrak{F}_\mathfrak{i}) = \mathcal{K}\mathrm{er}(\mathfrak{F}_d)$).

3. Soit α un générateur de ${\mathbb{F}_q}^*$
   $\mathcal{K}\text{er}(\mathfrak{F}_d)$ est un sous-groupe de ${\mathbb{F}_q}^*$ d'ordre d, il est donc engendré par $\xi = \alpha^{(q-1)/d}$ (cf. lemme 1.3.1).
$$\mathcal{K}\text{er}(\mathfrak{F}_d) = \left\{\xi^k; k = 0, \ldots, d-1\right\}$$

4. Définissons une relation d'équivalence sur ${\mathbb{F}_q}^*$ par :
   $\forall (x,y) \in {\mathbb{F}_q}^{*2}, \quad x\mathfrak{R}y$ sietseulementsi $y \in x\mathcal{K}\text{er}(\mathfrak{F}_\text{i})$
   C'est bien une relation d'équivalence et : $\forall x \in {\mathbb{F}_q}^* \quad \mathcal{C}l(x) = x\mathcal{K}\text{er}(\mathfrak{F}_d) = \left\{x\xi^k; k = 0, \ldots, d-1\right\}$.
   Les classes forment une partition de l'ensemble en question :

$$ {\mathbb{F}_q}^* = \bigcup_{x \in \mathcal{I}} \mathcal{C}l(x) \quad \text{avec } \#\mathcal{I} = \frac{q-1}{d} \text{ et } \#\mathcal{C}l(x) = d.$$

1.4 $\mathbb{F}_{2^n}$ versus $\mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$

Certaines fonctions sont définies sur $\mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$, on aimerait bien expliciter leur représentation univariée et pour cela il faut les définir sur $\mathbb{F}_{2^n}$, nous allons voir comment :

Soit $\omega \in \mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}$. $(1, \omega)$ est une base du $\mathbb{F}_{2^{n/2}}$-espace vectorielle $\mathbb{F}_{2^n}$. Pour tout $X \in \mathbb{F}_{2^n}$, il existe un unique couple (x, y) dans $\mathbb{F}_{2^{n/2}}$ tel que

$$X = x + \omega y \tag{2}$$

($i.e\ \mathbb{F}_{2^n} = \mathbb{F}_{2^{n/2}} \oplus \omega\mathbb{F}_{2^{n/2}}$).

Nous allons expliciter x et y en fonction de X. Appliquons $\mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}$ a l'equation (2), on obtient $\mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}(X) = y\mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}(\omega)$ de même d'après (2) : $X\omega^{2^{n/2}} + X^{2^{n/2}}\omega = x(\omega^{2^{n/2}} + \omega)$

c-à-d $x = \dfrac{\mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}\left(X\omega^{2^{n/2}}\right)}{\mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}(\omega)}$

Nous avons le $\mathbb{F}_{2^{n/2}}$-isomorphisme d'espace vectorielle suivant :

$X \in \mathbb{F}_{2^n} \to (x, y) \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$

avec $x = \dfrac{\mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}\left(X\omega^{2^{n/2}}\right)}{\mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}(\omega)}$ et $y = \dfrac{\mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}(X)}{\mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}(\omega)}$

Remarque :

1. D'après le corollaire 1.5 ω peut-être choisi tel que $\mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}(\omega) = 1$ ce qui simplifie considérablement le calcul.
2. Dans le cas ou $n/2$ est impair, on a davantage de simplification, il suffit de choisir ω élément primitif de $\mathbb{F}_4$ on a d'après la corollaire 1.3 : $\omega^{2^{n/2}} = w^2$
3. Rien n'empêche de prendre $\omega = \alpha^{2^{n/2}-1}$ et dans ce cas :$\mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}}(\omega) = \omega + \omega^{-1}$

2 Fonctions Courbes

Nous allons donner quelques résultats intéressants, pour une étude plus approfondie, nous envoyons à [3].

2.1 Transformée de Walsh

La Transformée de **Walsh** d'une fonction booléenne f et la transformée de **Fourier** de sa fonction signe. Son expression est donc :

$$\forall u \in \mathbb{F}_2^n \quad \hat{\chi}_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+u\cdot x} \text{ où } u \cdot x \text{ désigne le produit scalaire dans } \mathbb{F}_2^n$$

Si $\hat{\chi}_f(0) = 0$ alors f est équilibrée.
Si $\forall u \in \mathbb{F}_2^n \ \hat{\chi}_f(u) = \pm 2^{n/2}$ alors f est dite **courbe**.

2.2 Étude d'une fonction booléenne particulière

Dans la suite nous identifions $\mathbb{F}_{2^n}$ a $\mathbb{F}_2^n$ et nous posons $u \cdot x = \mathbf{Tr}_{\mathbb{F}_{2^n}}(xu)$
Étude de la fonction $f(x) = \mathbf{Tr}_{\mathbb{F}_{2^n}}(ax^i)$ avec $a \neq 0$. On peu déjà remarquer que $\gcd(i, 2^n - 1) \neq 1$ sinon f serait équilibrée, une telle fonction n'est jamais courbe.

2.2.1 Cas $a \in \mathbb{F}_{2^n}^{*i}$

Proposition 2.1. *f est courbe si et seulement si $g(x) = \boldsymbol{Tr}_{\mathbb{F}_{2^n}}(x^i)$ est courbe.*

Démonstration. $a \in \mathbb{F}_{2^n}^{*i} \Leftrightarrow \exists b \in \mathbb{F}_{2^n}^* \mid a = b^i$. Soit $\beta \in \mathbb{F}_{2^n}$

$$\begin{aligned}
\hat{\chi}_f(\beta) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{\mathbf{Tr}_{\mathbb{F}_{2^n}}(ax^i)+\mathbf{Tr}_{\mathbb{F}_{2^n}}(\beta x)} \\
&= \sum_{x \in \mathbb{F}_2^n} (-1)^{\mathbf{Tr}_{\mathbb{F}_{2^n}}((bx)^i)+\mathbf{Tr}_{\mathbb{F}_{2^n}}(\beta x)} \\
&= \sum_{x \in \mathbb{F}_2^n} (-1)^{\mathbf{Tr}_{\mathbb{F}_{2^n}}(x^i)+\mathbf{Tr}_{\mathbb{F}_{2^n}}(\frac{\beta}{b} x)} \\
&= \hat{\chi}_g\left(\frac{\beta}{b}\right)
\end{aligned}$$

□

Remarque : L'étude que j'ai menée sur le caractère courbe de g sur $\mathbb{F}_{2^k}$ où $k = 4, \ldots, 22$, a montré que g est courbe uniquement sur $\mathbb{F}_{2^s}$ avec l'exposant $i = (1 + j)15,\ j = 0, \ldots, 15$. Ce qui correspond a un exposant de **Dillon**, étrangement $\mathbb{F}_{2^8}$ c'est le corps où est définit l'**A.E.S**, y'a t-il une causalité ? ?.

2.2.2 Cas $a \notin \mathbb{F}_{2^n}^{*i}$

Dans cette partie nous allons tirer profit de l'étude que nous avons réalisé dans la Proposition 1.11. Les notations sont celles de la-dite Proposition et de la remarque qui l'a suivie avec $q = 2^n$. Soit $\beta \in \mathbb{F}_{2^n}$
$\xi = \alpha^{(2^n-1)/d}$, ou $d = \gcd(2^n - 1, i)$

$$\begin{aligned}
\hat{\chi}_f(\beta\xi) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{\mathbf{Tr}_{\mathbb{F}_{2^n}}(ax^i)+\mathbf{Tr}_{\mathbb{F}_{2^n}}(\beta\xi x)} \\
&= \hat{\chi}_f(\beta). \text{ (car } x \longmapsto x\xi \text{ est une permutation sur } \mathbb{F}_{2^n} \text{)}
\end{aligned}$$

Pour résumer :

$$\boxed{\forall y \in \mathcal{C}l(x) \quad \hat{\chi}_f(x) = \hat{\chi}_f(y)}$$

La transformée de **Walsh** est constante sur les classes,ceci peut conduire à un algorithme plus rapide(?). On peut aussi réécrire la **TW** autrement :

$$\hat{\chi}_f(\beta) = \sum_{x\in\mathbb{F}_2^n} (-1)^{\mathbf{Tr}_{\mathbb{F}_{2^n}}(ax^i)+\mathbf{Tr}_{\mathbb{F}_{2^n}}(\beta x)} \tag{3}$$

$$= 1 + \sum_{x\in\mathbb{F}_{2^n}^*} (-1)^{\mathbf{Tr}_{\mathbb{F}_{2^n}}(ax^i)+\mathbf{Tr}_{\mathbb{F}_{2^n}}(\beta x)} \tag{4}$$

$$= 1 + \sum_{x\in\mathcal{I}} (-1)^{\mathbf{Tr}_{\mathbb{F}_{2^n}}(ax^i)} \sum_{y\in Cl(x)} (-1)^{\mathbf{Tr}_{\mathbb{F}_{2^n}}(\beta y)} \tag{5}$$

$$= 1 + \sum_{x\in\mathcal{I}} (-1)^{\mathbf{Tr}_{\mathbb{F}_{2^n}}(ax^i)} \sum_{k=0}^{d-1} (-1)^{\mathbf{Tr}_{\mathbb{F}_{2^n}}(\beta x\xi^k)} \tag{6}$$

Proposition 2.2. *Si* $f(x) = \boldsymbol{Tr}_{\mathbb{F}_{2^n}}(ax^i)$ *est* ***courbe****, alors :*

$$\hat{\chi}_f(0) = \begin{cases} 2^{n/2}, & ssi\ \gcd(i, 2^{n/2}+1) = 1 \\ -2^{n/2}, & ssi\ \gcd(i, 2^{n/2}-1) = 1 \end{cases}$$

Démonstration. $d = \gcd(i, 2^n - 1) = \gcd(i, 2^{n/2} - 1).\gcd(i, 2^{n/2} + 1)$.
$k = \gcd(i, 2^{n/2} - 1)$ et $l = \gcd(i, 2^{n/2} + 1)$.En posant $\beta = 0$ dans l'égalité (6)

$$\hat{\chi}_f(0) - 1 = kl \sum_{x\in\mathcal{I}} (-1)^{\mathbf{Tr}_{\mathbb{F}_{2^n}}(ax^i)}$$

1er cas : $\hat{\chi}_f(0) = 2^{n/2}$ ceci entraîne $2^{n/2} - 1 = kl \sum_{x\in\mathcal{I}} (-1)^{\mathbf{Tr}_{\mathbb{F}_{2^n}}(ax^i)}$
Alors $l|2^{n/2} - 1$ comme $\gcd(l, 2^{n/2} - 1) = 1$, cela implique $l = 1$

2me cas : $\hat{\chi}_f(0) = -2^{n/2}$ le même raisonnement conduit à $k = 1$.

□

3 Construction d'une classe APN a partir d'une fonction Bent

Définition 3.1. *Une* $(n, n)-$*fonction* F *est dite* ***APN*** *si :*
$\forall a \in \mathbb{F}^*{}_{2^n}, \forall b \in \mathbb{F}_{2^n}$. *L'équation :* $F(x) + F(x + a) = b$ *à au plus* 0 *ou* 2 *solutions .*

Notation :

$$\forall a \in \mathbb{F}^*{}_{2^n}, D_aF(x) = F(x + a) + F(x). \tag{7}$$

Proposition 3.1. *[3]*

(i) B *est courbe* ***si et seulement si*** D_aB *est équilibré.*

(ii) B *quadratique* ***alors*** D_aB *est affine.*

Démonstration. voir livre [3]. □

Remarque : Si B une $(n, n/2)-$courbe quadratique, alors les solutions de $D_aB(x) = b$ avec $(a, b) \in \mathbb{F}^*_{2^n} \times \mathbb{F}_{2^{n/2}}$ est un sous-espaces affine de $\mathbb{F}_{2^n}$ affinement isomorphe a $\mathbb{F}_{2^{n/2}}$. Seulement c'est isomorphisme il n'est pas simple de l'explicité, d'autant plus qu'il depend de a et b. On va voir que dans le cas de la fonction simple de **Mairona Mac Farland** ce n'est pas le cas. L' auteur de l'article [4] a exploité cette idée, pour construire une classe de fonction APN.

Posons : $B(x) = X^{2^{n/2}+1}$ et soit G une $(n, n/2)-$fonction.
Et définissons $F : x \in \mathbb{F}_{2^n} \to (B(x), G(x)) \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$.
Probleme : Donner une condition nécessaire et suffisante portant sur G pour que F soit **APN**.
F APN ssi $\forall a \in \mathbb{F}^*_{2^n}, \forall (c, d) \in \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}}$ $D_aF(X) = (c, d)$ à au plus 0 ou deux solutions dans $\mathbb{F}_{2^n}$.

$$\begin{cases} B(X) + B(X + a) & = c \\ G(X) + G(X + a) & = d \end{cases} \tag{8}$$

or $D_aB(X) = \mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}(a^{2^{n/2}}X) + a^{2^{n/2}+1}$ et donc :
$D_aB(X) = c \Leftrightarrow \mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}(a^{2^{n/2}}X)+a^{2^{n/2}+1} = c \Leftrightarrow \mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}(X) = 1+\frac{c}{a^{2^{n/2}+1}}$ chgement de variable $X \to aX$
Soit $b \in \mathbb{F}_{2^n}$ tel que $\mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}(b) = 1 + \frac{c}{a^{2^{n/2}+1}}$ Voir la surjéctivité de la trace et donc :
$D_aB(X) = c \Leftrightarrow \mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}(X+b) = 0 \Leftrightarrow \mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}(X) = 0$ changement de variable $X \to X + b \Leftrightarrow$
$X \in \mathbb{F}_{2^{n/2}}$
L'îsomorphisme affine est $\varphi : X \in \mathbb{F}_{2^{n/2}} \xrightarrow{\sim} aX + b \in (D_aB)^{-1}(c)$ avec $\mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}(b) = 1 + \frac{c}{a^{2^{n/2}+1}}$
En reportant dans l'equation (8)
F APN ssi

$$\forall a \in \mathbb{F}^*_{2^n}, \forall b \in \mathbb{F}_{2^n}, \forall d \in \mathbb{F}_{2^{n/2}}. G(aX + b) + G(aX + b + a) = d \tag{9}$$

à au plus 0 ou deux solutions sur $\mathbb{F}_{2^{n/2}}$.
On a le théorème suivant :

Théorème 3.1. *Soit $B(x) = X^{2^{n/2}+1}$ et soit G une $(n, n/2)-$fonction, $L : \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}} \to \mathbb{F}_{2^n}$ un isomorphisme linéaire et $F : X \in \mathbb{F}_{2^n} \to L(B(x), G(x)) \in \mathbb{F}_{2^n}$ alors F est APN si et seulement si*

$$\forall a \in \mathbb{F}^*_{2^n}, \forall b \in \mathbb{F}_{2^n}, \forall d \in \mathbb{F}_{2^{n/2}}\ G(aX + b) + G(aX + b + a) = d \tag{10}$$

à 0 ou 2 solutions au plus dans $\mathbb{F}_{2^{n/2}}$.

Lemme 3.0.1.

(i) $\forall a, b \in \mathbb{F}_{2^r}, (aX + b)^{2^k+2^j} + (aX + a + b)^{2^k+2^j} = a^{2^k+2^j}(X^{2^k} + X^{2^j} + 1) + b^{2^k}a^{2^i} + b^{2^i}a^{2^k}$

(ii) *Soient i et r premiers entre eux, c élément de $\mathbb{F}_{2^r}$, alors l'équation : $X^{2^i} + X + c = 0$ à 0 ou 2 solutions au plus dans $\mathbb{F}_{2^r}$*

Démonstration. Le point (i) est calculatoire, le point (ii) découle du fait que, $X \to X^{2^i+1}$ est APN (**Gold**). □

3.0.3 Familles de fonctions connues

Je commencerais par trois lemmes que j'ai jugé fort utile.

Lemme 3.0.2. *Pour tout entier i*

(i) $2^i + 1$ *est divisible par* 3 *ssi i est impair.*

(ii) $2^i - 1$ *est divisible par* 3 *ssi* i *est pair.*

Démonstration. Tout entier i peut s'écrire : $i = 2k + \epsilon$ avec $(k, \epsilon) \in \mathbb{N} \times \{0, 1\}$

(i) $2^i + 1 = 2^{2k+\epsilon} + 1 = 4^k 2^\epsilon + 1 \equiv (2^\epsilon + 1) \mod 3$
donc $2^i + 1 \equiv 0 \mod 3$ ssi $\epsilon = 1$

(ii) $2^i - 1 = 2^{2k+\epsilon} - 1 = 4^k 2^\epsilon - 1 \equiv (2^\epsilon - 1) \mod 3$
donc $2^i - 1 \equiv 0 \mod 3$ ssi $\epsilon = 0$

□

Lemme 3.0.3. *Soient* n *un entier pair et* i *un entier vérifiant* $\gcd(i, n/2) = 1$ *alors*

$$\gcd(2^i + 1, 2^{n/2} + 1) = \begin{cases} 1, & \textit{ssi } i \textit{ pair} \\ 1, & \textit{ssi } i \textit{ impair et } n/2 \textit{ pair} \\ 3, & \textit{ssi } i \textit{ impair et } n/2 \textit{ impair} \end{cases}$$

Démonstration. On a d'un coté $\gcd(2^{2i} - 1, 2^n - 1) = \gcd(2^i + 1, 2^n - 1).\gcd(2^i - 1, 2^n - 1) = \gcd(2^i + 1, 2^{n/2} - 1)\gcd(2^i + 1, 2^{n/2} + 1)(2^{\gcd(i,n)} - 1)$.
de l'autre $\gcd(2^{2i} - 1, 2^n - 1) = 2^{2.\gcd(i,n/2)} - 1 = 3$. Soit

$$\boxed{3 = \gcd(2^i + 1, 2^{n/2} - 1)\gcd(2^i + 1, 2^{n/2} + 1)(2^{\gcd(i,n)} - 1)}$$

on conclut on traitons selon la parité de i et on utilisant le lemme 3.0.2. □

Lemme 3.0.4. *Soit* $q = 2^{n/2}$*, les solutions de l'équation*

$$X^{q+1} + 1 = 0 \tag{11}$$

sont exactement les éléments de $\mathbb{F}_{2^n}^{*(q-1)}$

Démonstration. En effet, soit $x \in \mathbb{F}_{2^n}^{*(q-1)}$, donc il existe $y \in \mathbb{F}_{2^n}^*$ vérifiant $x = y^{q-1}$, soit $x^{q+1} = y^{q^2-1} = 1$ donc x est solution de l'équation 11. Or d'après la proposition 1.11, $\#\mathbb{F}_{2^n}^{*(q-1)} = q + 1$. D'un autre coté les solutions de l'équation (11) sont simples voir proposition 1.1, ils sont au nombre de $q + 1$, vue que son degré est $q + 1$. Ce qui achève la preuve. □

Dorénavant et dans toutes la suite, nous prendrons pas en compte, les termes de $\mathbb{F}_{2^{n/2}}$ indépendants de X qui apparaissent dans $G(aX + b') + G(aX + b' + a)$, puisqu'on peut toujours les affectés à d dans l'égalité (10).

Corollaire 3.1. *La fonction* $F(X) = X^{2^{2i}+2^i} + bX^{q+1} + cX^{q(2^{2i}+2^i)}$ *où* $\gcd(i, n/2) = 1$, $q = 2^{n/2}$, $(c, b) \in {\mathbb{F}_{2^n}}^2$, *tel que :* $c^{q+1} = 1$, $c \notin \left\{\lambda^{(2^i+1)(q-1)},\ \lambda \in \mathbb{F}_{2^n}\right\}$ *et* $cb^q + b \neq 0$ *est* ***APN***

Démonstration. Nous allons commencer par quelques remarques simples :

(i) $c \notin \mathbb{F}_{2^{n/2}}$
En effet : Si $c \in \mathbb{F}_{2^{n/2}}$ alors $c^{q+1} = c^2 = 1 \Rightarrow c = 1 \Rightarrow c \in \left\{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^n}\right\}$, contradiction.

(ii) $\frac{b}{c^{2^{(n-1)}}} \notin \mathbb{F}_{2^{n/2}}$
En effet, sinon : $\left(\frac{b}{c^{2^{(n-1)}}}\right)^q = \frac{b}{c^{2^{(n-1)}}}$ or $\left(\frac{1}{c^{2^{(n-1)}}}\right)^q = \frac{c}{c^{2^{(n-1)}}}$ (cf. proposition 1.10)
$\Leftrightarrow b^q \frac{c}{c^{2^{(n-1)}}} = \frac{b}{c^{2^{(n-1)}}} \Leftrightarrow cb^q + b = 0$, contradiction.
et donc $(1, \frac{b}{c^{2^{(n-1)}}})$ forme une base de $\mathbb{F}_{2^n}$ sur $\mathbb{F}_{2^{n/2}}$.

(iii) F est APN si et seulement si $\frac{F}{c^{2^{(n-1)}}}$ est APN (evident).

Sans perte de généralité nous pouvons identifier F à $\frac{F}{c^{2^{(n-1)}}}$ et donc
$F = \frac{X^{2^{2i}+2^i}}{c^{2^{(n-1)}}} + \frac{b}{c^{2^{(n-1)}}} X^{q+1} + \frac{c}{c^{2^{(n-1)}}} X^{q(2^{2i}+2^i)} = \mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}} \left(\frac{X^{2^{2i}+2^i}}{c^{2^{(n-1)}}} \right) + \frac{b}{c^{2^{(n-1)}}} X^{q+1}$

Posons $L(u,v) = u + v\frac{b}{c^{2^{(n-1)}}}$ c'est bien un isomorphisme, et $G(X) = \mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}} \left(\frac{X^{2^{2i}+2^i}}{c^{2^{(n-1)}}} \right)$.
Montrons que G vérifie l'équation (10).

$$\begin{aligned} G(aX+b') + G(aX+a+b') &= \mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}} \left(\frac{a^{2^{2i}+2^i}}{c^{2^{(n-1)}}} (X^{2^{2i}} + X^{2^i} + 1) \right) \\ &= (X^{2^{2i}} + X^{2^i} + 1) \mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}} \left(\frac{a^{2^{2i}+2^i}}{c^{2^{(n-1)}}} \right) \\ &= (X^{2^i} + X + 1)^{2^i} \mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}} \left(\frac{a^{2^{2i}+2^i}}{c^{2^{(n-1)}}} \right) \\ &= d \end{aligned}$$

Or $x \to x^{2^i}$ est une permutation sur $\mathbb{F}_{2^{n/2}}$, d'après le lemme 3.0.1, et le théorème 3.1, F est APN si et seulement si $\forall a \in \mathbb{F}^*{}_{2^n} \quad \mathbf{Tr}_{\mathbb{F}_{\mathbf{2^n}}/\mathbb{F}_{\mathbf{2^{n/2}}}} \left(\frac{a^{2^{2i}+2^i}}{c^{2^{(n-1)}}} \right) = 0$ n'a pas de solution.
Supposons que c'est le cas, ceci équivaut à

$$\begin{aligned} \frac{a^{2^{2i}+2^i}}{c^{2^{(n-1)}}} &= \frac{a^{q(2^{2i}+2^i)}}{c^{q2^{(n-1)}}} \\ &= \frac{c}{c^{2^{(n-1)}}} a^{q(2^{2i}+2^i)} \quad \text{(cf. proposition 1.10)} \end{aligned}$$

Ceci implique $c = a^{-(q-1)(2^{2i}+2^i)} = a^{-(q-1)2^i(2^i+1)} \in \mathbb{F}_{2^n}^{(q-1)2^i(2^i+1)}$
Comme $x \to x^{2^i}$ est une permutation, ce qui entraîne $c \in \mathbb{F}_{2^n}^{(q-1)(2^i+1)}$ contradiction, ce qui achève la preuve. □

Remarque :

(i) Les lemmes que j'ai donné 3.0.2, 3.0.4 et surtout 3.0.3, sont très puissantes, ils trouveront leur application dans ce qui va suivre, mais peuvent être appliqués en dehors de l'article.

(ii) L'étude faite à la sous-section 1.3, montre que $\mathbb{F}_{2^n}^{(q-1)(2^i+1)} = \mathbb{F}_{2^n}^{\gcd((q-1)(2^i+1),2^n-1)} = \mathbb{F}_{2^n}^{(q-1)\gcd(2^i+1,q+1)}$
On utilisant le lemme 3.0.3, on a :

$$\mathbb{F}_{2^n}^{(q-1)(2^i+1)} = \begin{cases} \mathbb{F}_{2^n}^{(q-1)}, & \text{ssi } i \text{ pair} \\ \mathbb{F}_{2^n}^{(q-1)}, & \text{ssi } i \text{ impair et } n/2 \text{ pair} \\ \mathbb{F}_{2^n}^{3(q-1)}, & \text{ssi } i \text{ impair et } n/2 \text{ impair} \end{cases}$$

(iii) Le corollaire 3.1, n'est pas tout à fait correcte, car ils y'a des cas où les hypotheses ne seront jamais satisfaites, et ça c'est très important quand on implémente, de chercher la où on peut trouver. En effet le lemme 3.0.4, supprime les deux cas : i pair et i impair avec $n/2$ pair, nous allons donné une version corrigée est optimale de ce résultat.

Corollaire 3.2 (version optimale)**.** *Soient $q = 2^{n/2}$, i et $n/2$ impairs, vérifiant* $\gcd(i, n/2) = 1$.
Alors :
La fonction $F(X) = X^{2^{2i}+2^i} + bX^{q+1} + cX^{q(2^{2i}+2^i)}$ *où* $c, b \in \mathbb{F}_{2^n}$, *tel que :* $c^{q+1} = 1$, $c \notin \mathbb{F}_{2^n}^{*3(q-1)}$, *et* $cb^q + b \neq 0$ *est* ***APN***

Corollaire 3.3. *Soient $q = 2^{n/2}$, s et $n/2$ impairs, vérifiant* $\gcd(s, n/2) = 1$, $b \in \mathbb{F}_{2^n}$ *non cube, et* $c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^{n/2}}$, $r_i \in \mathbb{F}_{2^{n/2}}$. *Alors la fonction F définit par :*
$F(X) = bX^{2^s+1} + b^q X^{q(2^s+1)} + cX^{q+1} + \sum_{i=1}^{n/2-1} r_i X^{2^i(q+1)}$ *est APN.*

Démonstration. On a l'isomorphisme suivant $L(u, v) = cu + \sum_{i=1}^{n/2-1} r_i u^{2^i} + v$ (cf :c $\in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^{n/2}}$)
et donc $G(X) = bX^{2^s+1} + b^q X^{q(2^s+1)} = \mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}\left(bX^{2^s+1}\right)$
Montrons que G vérifie l'équation (10)

$$\begin{aligned} G(aX + b') + G(aX + a + b') &= \mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}\left(ba^{2^s+1}(X^{2^s} + X + 1)\right) \\ &= (X^{2^s} + X + 1)\mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}\left(ba^{2^s+1}\right) \\ &= d \end{aligned}$$

D'après le lemme 3.0.1, et le théorème 3.1, F est APN si et seulement si $\forall a \in \mathbb{F}^*_{2^n}$ $\mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}\left(ba^{2^s+1}\right) = 0$ n'a pas de solutions. C'est le cas, sinon : $ba^{2^s+1} \in \mathbb{F}_{2^{n/2}}$ comme $\mathbb{F}_{2^n}^{(2^s+1)} = \mathbb{F}_{2^n}^{\gcd(2^s+1, 2^n-1)} = \mathbb{F}_{2^n}^3$
et que les élément de $\mathbb{F}_{2^{n/2}}$ sont tous des cubes, ceci conduit à b est un cube, contradiction.
Donc F est APN. □

Corollaire 3.4. *Soient* $\gcd(i, n/2) = 1$, $c \in \mathbb{F}_{2^n}$, $s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^{n/2}}$, $q = 2^{n/2}$
$F(X) = X(X^{2^i} + X^q + cX^{2^i q}) + X^{2^i}(c^q X^q + sX^{q2^i}) + X^{(2^i+1)q}$.
où : $X^{2^i+1} + cX^{2^i} + c^q X + 1$ *est irréductible sur* $\mathbb{F}_{2^n}$. *Alors F est APN.*

Démonstration.

$$\begin{aligned} F(X) &= X^{2^i+1} + X^{q+1} + cX^{2^i q+1} + c^q X^{q+2^i} + sX^{2^i(q+1)} + X^{(2^i+1)q}. \\ &= X^{q+1} + sX^{2^i(q+1)} + X^{2^i+1} + cX^{2^i q+1} + c^q X^{q+2^i} + X^{(2^i+1)q} \\ &= L(B(X), G(X)) \end{aligned}$$

où : $L(u, v) = u + su^{2^i} + v$ est un isomorphisme; $G(X) = \mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}\left(X^{2^i+1} + cX^{2^i q+1}\right)$
Montrons que G vérifie l'équation (10)

$$\begin{aligned} G(aX + b') + G(aX + a + b') &= \mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}\left(a^{2^i+1}(X^{2^i} + X + 1) + ca^{2^i q+1}(X^{2^i q} + X + 1)\right) \quad (\text{ comme } X \in \mathbb{F}_{2^{n/2}}) \\ &= (X^{2^i} + X + 1)\mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}\left(a^{2^i+1} + ca^{2^i q+1}\right) \\ &= d. \end{aligned}$$

Supposons que $\mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}\left(a^{2^i+1} + ca^{2^i q+1}\right) = 0$ a une solution dans $\mathbb{F}_{2^{n/2}}$, ceci équivaut a :
$a^{2^i+1} + ca^{2^i q+1} = a^{q(2^i+1)} + c^q a^{2^i+q}$, en divisant par a^{2^i+1}, et en notant :
$P(X) = X^{2^i+1} + cX^{2^i} + c^q X + 1$, ceci donne $P(a^{q-1}) = 0$, contradiction. □

On voit que le théorème 3.1, permet de construire une multitude de fonction APN, moi même j'en donne deux, assez générales.

posons $G(X) = \mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}\left(X^{2^i+1} + cX^{2^iq+1} + tX^{2^i+q}\right)$ et trouvons les conditions nécéssaire et suffisante pour que ca conduit a une fonction APN.

$$\begin{aligned} G(aX+b') + G(aX+a+b') &= \mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}\left(a^{2^i+1}(X^{2^i}+X+1) + ca^{2^iq+1}(X^{2^iq}+X+1) + ta^{q+2^i}(X^{2^i}+X+1)\right) \\ &= (X^{2^i}+X+1)\mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}\left(a^{2^i+1} + ca^{2^iq+1} + ta^{q+2^i}\right) \\ &= d. \end{aligned}$$

Supposons que $\mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}\left(a^{2^i+1} + ca^{2^iq+1} + ta^{q+2^i}\right) = 0$ a une solution dans $\mathbb{F}_{2^n}$. Ceci équivaut a :
$P(a^{q-1}) = 0$ où $P(X) = X^{2^i+1} + (t^q+c)X^{2^i} + (c^q+t)X + 1$, il suffit de choisir P irréductible sur $\mathbb{F}_{2^n}$

Corollaire 3.5. *Soient $q = 2^{n/2}$, i tel que $\gcd(i, n/2) = 1$, $B(X) = X^{q+1}$.*
$G(X) = \boldsymbol{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}\left(X^{2^i+1} + cX^{2^iq+1} + tX^{2^i+q}\right)$, et $L : \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}} \to \mathbb{F}_{2^n}$ un isomorphisme quelconque.
*Alors $F = L(B, G)$ est **APN** si et seulement si $P(X) = X^{2^i+1} + (t^q+c)X^{2^i} + (c^q+t)X + 1$ n'a pas de racines dans $\mathbb{F}_{2^n}$.*

Corollaire 3.6. *Soient $n/2$ impair, et i, j vérifiant $(j-i)$ impairs et $\gcd(j-i, n/2) = 1$, c élément de $\mathbb{F}_{2^n}^{*(q-1)} \setminus \mathbb{F}_{2^n}^{*3(q-1)}$, $B(X) = X^{q+1}$. $G(X) = \boldsymbol{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}\left(\frac{X^{2^j+2^i}}{c^{2^n-1}}\right)$, et $L : \mathbb{F}_{2^{n/2}} \times \mathbb{F}_{2^{n/2}} \to \mathbb{F}_{2^n}$ un isomorphisme quelconque. Alors*
*$F = L(B, G)$ est **APN**.*

Démonstration. Vérifiant que G satisfait l'équation (10).

$$\begin{aligned} G(aX+b') + G(aX+a+b') &= \mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}\left(\frac{a^{2^j+2^i}}{c^{2^n-1}}(X^{2^j}+X^{2^i}+1)\right) \\ &= (X^{2^{j-i}}+X+1)^{2^i}\mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}\left(\frac{a^{2^j+2^i}}{c^{2^n-1}}\right) \\ &= d \end{aligned}$$

Les mêmes arguments utiliser jusqu'ici, montre que F est APN ssi $\mathbf{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^{n/2}}}\left(\frac{a^{2^j+2^i}}{c^{2^n-1}}\right) = 0$ n'a pas de solutions pour tout a dans $\mathbb{F}^*{}_{2^n}$. Supposons que c'est le cas alors $c \in \mathbb{F}_{2^n}^{*(q-1)(2^j+2^i)}$ soit d'apres le lemme 3.0.3, $c \in \mathbb{F}_{2^n}^{*3(q-1)}$ contradiction, donc F est APN.

□

Références

[1] R.Lidl,H.Niederreiter ,*Finite Fields.*

[2] Y. Gozard,*Theorie de Galois.*

[3] C.Carlet,*Boolean Functions for Cryptography and Error Correcting Codes.*

[4] C.Carlet,*Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions*