Skew Reed Mueller Codes

Felix Ulmer
joint work with Willi Geiselmann

IRMAR, UMR 6625, Université de Rennes 1

Lens, june 2017

Reed-Solomon over $\mathbb{F}_q$

An $\mathbb{F}_q$-linear code of length n is a k-dimensional subspace of $(\mathbb{F}_q)^n$

Encoding :

$$\begin{array}{rcl} (\mathbb{F}_q)^k & \to & (\mathbb{F}_q)^n \\ (b_0, \ldots, b_{k-1}) & \mapsto & (c_0, \ldots, \ldots, c_{n-1}) \end{array}$$

Reed-Solomon Codes : Pick $\alpha_0, \ldots, \alpha_{n-1}$ in $\mathbb{F}_q$

$$\begin{array}{rcl} (\mathbb{F}_q)^k & \to & (\mathbb{F}_q)^n \\ f = \sum_{i=0}^{k-1} b_i X^i & \mapsto & (f(\alpha_0), f(\alpha 1) \ldots, f(\alpha_{n-1})) \end{array}$$

singleton bound, systematic incoding, decoding via interpolation

Reed-Solomon over $\mathbb{F}_q$

An $\mathbb{F}_q$-linear code of length n is a k-dimensional subspace of $(\mathbb{F}_q)^n$

Encoding :

$$\begin{array}{rcl} (\mathbb{F}_q)^k & \to & (\mathbb{F}_q)^n \\ (b_0, \ldots, b_{k-1}) & \mapsto & (c_0, \ldots, \ldots, c_{n-1}) \end{array}$$

Reed-Solomon Codes : Pick $\alpha_0, \ldots, \alpha_{n-1}$ in $\mathbb{F}_q$

$$\begin{array}{rcl} (\mathbb{F}_q)^k & \to & (\mathbb{F}_q)^n \\ f = \sum_{i=0}^{k-1} b_i X^i & \mapsto & (f(\alpha_0), f(\alpha 1) \ldots, f(\alpha_{n-1})) \end{array}$$

singleton bound, systematic incoding, decoding via interpolation

Reed-Solomon over $\mathbb{F}_q$

An $\mathbb{F}_q$-linear code of length n is a k-dimensional subspace of $(\mathbb{F}_q)^n$

Encoding :

$$\begin{array}{rcl} (\mathbb{F}_q)^k & \to & (\mathbb{F}_q)^n \\ (b_0, \ldots, b_{k-1}) & \mapsto & (c_0, \ldots, \ldots, c_{n-1}) \end{array}$$

Reed-Solomon Codes : Pick $\alpha_0, \ldots, \alpha_{n-1}$ in $\mathbb{F}_q$

$$\begin{array}{rcl} (\mathbb{F}_q)^k & \to & (\mathbb{F}_q)^n \\ f = \sum_{i=0}^{k-1} b_i X^i & \mapsto & (f(\alpha_0), f(\alpha 1) \ldots, f(\alpha_{n-1})) \end{array}$$

singleton bound, systematic incoding, decoding via interpolation

Reed Mueller Codes over $\mathbb{F}_q$

Pick n-points $(\alpha_{0,1}, \ldots, \alpha_{0,m}), \ldots, (\alpha_{n-1,0}, \ldots, \alpha_{n-1,m})$ in $(\mathbb{F}_q)^m$

$$(\mathbb{F}_q)^k \quad \rightarrow \quad (\mathbb{F}_q)^n$$

$$\sum_{i_1+\cdots,i_m<d} b_{i_1,\ldots,i_m} X^{i_1} \cdots X^{i_m}$$

$$\mapsto (f((\alpha_{0,1}, \ldots, \alpha_{0,m})), \ldots, f(\alpha_{n-1,1}, \ldots, \alpha_{n-1,m}))$$

Iterated skew polynomial rings

$\mathbb{F}_q$ a ring, $\theta \in \mathrm{Aut}(\mathbb{F}_q)$, $\delta : \mathbb{F}_q \to \mathbb{F}_q$ a θ-derivation :

$$\begin{cases} \delta(a+b) &= \delta(a)+\delta(b) \\ \delta(ab) &= \delta(a)b+\theta(a)\delta(b). \end{cases}$$

$$R = \mathbb{F}_q[X;\theta,\delta] = \left\{ a_n X^n + \ldots + a_1 X + a_0 \,|\, a_i \in A \text{ and } n \in \mathbb{N} \right\}.$$

$$X\, a = \theta(a)\, X + \delta(a)$$

$$R_\ell = (\cdots(\mathbb{F}_q[X_1;\theta_1,\delta_1])\ldots)[X_m;\theta_m,\delta_m]$$

In order to generalize Reed Mueller codes to Iterated skew polynomial rings we need the notion of evaluation

Iterated skew polynomial rings

$\mathbb{F}_q$ a ring, $\theta \in \mathrm{Aut}(\mathbb{F}_q)$, $\delta : \mathbb{F}_q \to \mathbb{F}_q$ a θ-derivation :

$$\begin{cases} \delta(a+b) &= \delta(a)+\delta(b) \\ \delta(ab) &= \delta(a)b+\theta(a)\delta(b). \end{cases}$$

$$R = \mathbb{F}_q[X;\theta,\delta] = \{a_n X^n + \ldots + a_1 X + a_0 \mid a_i \in A \text{ and } n \in \mathbb{N}\}.$$

$$X\,a = \theta(a)\,X + \delta(a)$$

$$R_\ell = (\cdots(\mathbb{F}_q[X_1;\theta_1,\delta_1])\ldots)[X_m;\theta_m,\delta_m]$$

In order to generalize Reed Mueller codes to Iterated skew polynomial rings we need the notion of evaluation

Previous results in $\mathbb{F}_q[X;\theta,\delta]$ (one variable)

1. Operator evaluation
   1. Gabidulin (1985) :

      $\varphi : \mathbb{F}_q[X;\theta] \to \mathrm{End}(\mathbb{F}_q),\ f = \sum_{i=0}^{m} a_i X^i \mapsto \sigma_f = \sum_{i=0}^{m} a_i \theta^i$

      for $b \in \mathbb{F}_q$ define $f(b) = \sum_{i=0}^{m} a_i \sigma_f^i(b) = \sum_{i=0}^{m} a_i b^{q^i}$

   2. Boucher, U. (2014) : in $\mathbb{F}_q[X;\theta,\delta]$ with $\delta \neq 0$

      for $b \in \mathbb{F}_q$ define $f(b) = \delta_f(b) = \sum_{i=0}^{m} a_i \delta^i(b)$

2. Remainder eval : Lam-Leroy (1988), Boucher, U. (2014) :

   for $b \in \mathbb{F}_q$ consider $f = q(X-b) + r$ and set $f(b) = r$. (remainder evaluation).

Evaluation points limited by rank of Wronskian/Vandermonde

Previous results in $\mathbb{F}_q[X;\theta,\delta]$ (one variable)

1. Operator evaluation
   1. Gabidulin (1985) :

      $\varphi : \mathbb{F}_q[X;\theta] \to \mathrm{End}(\mathbb{F}_q),\ f = \sum_{i=0}^{m} a_i X^i \mapsto \sigma_f = \sum_{i=0}^{m} a_i \theta^i$

      for $b \in \mathbb{F}_q$ define $f(b) = \sum_{i=0}^{m} a_i \sigma_f^i(b) = \sum_{i=0}^{m} a_i b^{q^i}$

   2. Boucher, U. (2014) : in $\mathbb{F}_q[X;\theta,\delta]$ with $\delta \neq 0$

      for $b \in \mathbb{F}_q$ define $f(b) = \delta_f(b) = \sum_{i=0}^{m} a_i \delta^i(b)$

2. Remainder eval : Lam-Leroy (1988), Boucher, U. (2014) :

   for $b \in \mathbb{F}_q$ consider $f = q(X-b) + r$ and set $f(b) = r$. (remainder evaluation).

Evaluation points limited by rank of Wronskian/Vandermonde

Previous results in $\mathbb{F}_q[X;\theta,\delta]$ (one variable)

1. Operator evaluation
   1. Gabidulin (1985) :

      $\varphi : \mathbb{F}_q[X;\theta] \to \mathrm{End}(\mathbb{F}_q),\ f = \sum_{i=0}^{m} a_i X^i \mapsto \sigma_f = \sum_{i=0}^{m} a_i \theta^i$

      for $b \in \mathbb{F}_q$ define $f(b) = \sum_{i=0}^{m} a_i \sigma_f^i(b) = \sum_{i=0}^{m} a_i b^{q^i}$

   2. Boucher, U. (2014) : in $\mathbb{F}_q[X;\theta,\delta]$ with $\delta \neq 0$

      for $b \in \mathbb{F}_q$ define $f(b) = \delta_f(b) = \sum_{i=0}^{m} a_i \delta^i(b)$
2. Remainder eval : Lam-Leroy (1988), Boucher, U. (2014) :

   for $b \in \mathbb{F}_q$ consider $f = q(X-b) + r$ and set $f(b) = r$. (remainder evaluation).

Evaluation points limited by rank of Wronskian/Vandermonde

Previous results in $\mathbb{F}_q[X;\theta,\delta]$ (one variable)

1. Operator evaluation
   1. Gabidulin (1985) :

      $\varphi : \mathbb{F}_q[X;\theta] \to \mathrm{End}(\mathbb{F}_q),\ f = \sum_{i=0}^{m} a_i X^i \mapsto \sigma_f = \sum_{i=0}^{m} a_i \theta^i$

      for $b \in \mathbb{F}_q$ define $f(b) = \sum_{i=0}^{m} a_i \sigma_f^i(b) = \sum_{i=0}^{m} a_i b^{q^i}$

   2. Boucher, U. (2014) : in $\mathbb{F}_q[X;\theta,\delta]$ with $\delta \neq 0$

      for $b \in \mathbb{F}_q$ define $f(b) = \delta_f(b) = \sum_{i=0}^{m} a_i \delta^i(b)$
2. Remainder eval : Lam-Leroy (1988), Boucher, U. (2014) :

   for $b \in \mathbb{F}_q$ consider $f = q(X-b) + r$ and set $f(b) = r$. (remainder evaluation).

Evaluation points limited by rank of Wronskian/Vandermonde

Lemma

(Zippel 1979) For a non zero $f \in \mathbb{F}_q[X_1, \ldots, X_m]$, *where* $\deg_{X_i}(f) \leq d_i$, *we have* $Pr_{\alpha \in (\mathbb{F}_q)^m}[f(\alpha) \neq 0] \leq \frac{\prod_{i=1}^{m}(q - d_i)}{q^m}$.

Example : $\mathbb{F}_9 = \mathbb{F}_3[\omega]$, $\theta_1 : x \mapsto x^3$, $R = [X_1; \theta_1]$

$X_1^2 + 1$	$\{\omega, \omega^3, \omega^5, \omega^7\}$
$X_1^3 + 2X_1^2 + X_1 + 2$	$\{1, \omega, \omega^3, \omega^5, \omega^7\}$
$X_1^4 + 2$	$\{1, 2, \omega, \omega^2, \omega^3, \omega^5, \omega^6, \omega^7\}$

Lemma

(Zippel 1979) For a non zero $f \in \mathbb{F}_q[X_1, \ldots, X_m]$, *where* $\deg_{X_i}(f) \leq d_i$, *we have* $Pr_{\alpha \in (\mathbb{F}_q)^m}[f(\alpha) \neq 0] \leq \frac{\prod_{i=1}^{m}(q - d_i)}{q^m}$.

Example : $\mathbb{F}_9 = \mathbb{F}_3[\omega]$, $\theta_1 : x \mapsto x^3$, $R = [X_1; \theta_1]$

$X_1^2 + 1$	$\{\omega, \omega^3, \omega^5, \omega^7\}$
$X_1^3 + 2X_1^2 + X_1 + 2$	$\{1, \omega, \omega^3, \omega^5, \omega^7\}$
$X_1^4 + 2$	$\{1, 2, \omega, \omega^2, \omega^3, \omega^5, \omega^6, \omega^7\}$

Generalization of commutative evaluation

1. The evaluation of $f \in \mathbb{F}_q[X_1, \ldots, X_m]$ at $(a_1, \ldots, a_m)$ is a representative of f modulo the ideal $(X_1 - a_1, \ldots, X_m - a_m)$.
2. $(X_1 - a_1, \ldots, X_m - a_m)$ is a Gröbner basis for lex order and $f(a_1, \ldots, a_m)$ is the remainder of the "division" of f by $\{X_1 - a_1, \ldots, X_m - a_m\}$.

We need :

1. Rings $R_m = (\ldots(\mathbb{F}_q[X_1; \theta_1, \delta_1])\ldots[X_m; \theta_m, \delta_m])$.
2. Evaluation ideals $I = (X_1 - a_1, \ldots, X_m - a_m) \subset R_m$.
3. Gröbner basis for $I \subset R_m$.

$(X_1 - a_1, \ldots, X_m - a_m) = R_m \quad \rightsquigarrow$ always zero evaluation

Generalization of commutative evaluation

1. The evaluation of $f \in \mathbb{F}_q[X_1, \ldots, X_m]$ at $(a_1, \ldots, a_m)$ is a representative of f modulo the ideal $(X_1 - a_1, \ldots, X_m - a_m)$.
2. $(X_1 - a_1, \ldots, X_m - a_m)$ is a Gröbner basis for lex order and $f(a_1, \ldots, a_m)$ is the remainder of the "division" of f by $\{X_1 - a_1, \ldots, X_m - a_m\}$.

We need :

1. Rings $R_m = (\ldots(\mathbb{F}_q[X_1; \theta_1, \delta_1])\ldots[X_m; \theta_m, \delta_m])$.
2. Evaluation ideals $I = (X_1 - a_1, \ldots, X_m - a_m) \subset R_m$.
3. Gröbner basis for $I \subset R_m$.

$(X_1 - a_1, \ldots, X_m - a_m) = R_m \quad \rightsquigarrow$ always zero evaluation

Generalization of commutative evaluation

1. The evaluation of $f \in \mathbb{F}_q[X_1, \ldots, X_m]$ at $(a_1, \ldots, a_m)$ is a representative of f modulo the ideal $(X_1 - a_1, \ldots, X_m - a_m)$.
2. $(X_1 - a_1, \ldots, X_m - a_m)$ is a Gröbner basis for lex order and $f(a_1, \ldots, a_m)$ is the remainder of the "division" of f by $\{X_1 - a_1, \ldots, X_m - a_m\}$.

We need :

1. Rings $R_m = (\ldots(\mathbb{F}_q[X_1; \theta_1, \delta_1])\ldots[X_m; \theta_m, \delta_m])$.
2. Evaluation ideals $I = (X_1 - a_1, \ldots, X_m - a_m) \subset R_m$.
3. Gröbner basis for $I \subset R_m$.

$(X_1 - a_1, \ldots, X_m - a_m) = R_m \quad \rightsquigarrow$ always zero evaluation

D. Jordan (1995) : $\beta \in \mathbb{F}_q^*$, $\gamma \in \mathbb{F}_q$, $d_1 \in \mathbb{F}_q$ and $\theta_1 \in \mathrm{Aut}(\mathbb{F}_q)$.

1. $\theta_1 \in \mathrm{Aut}(\mathbb{F}_q)$ and $\delta_1 : x \mapsto d_1 x - \theta_1(x) d_1$ (inner derivation)

$$\boxed{R_1 = \mathbb{F}_q[X_1; \theta_1, \delta_1], \text{ where } \forall a \in \mathbb{F}_q,\ X_1 a = \theta_1(a) X_1 + \delta_1(a)}$$

2. Extend to $\widetilde{\theta_1} \in \mathrm{Aut}(R_1)$ by $\widetilde{\theta_1}(X_1) = \beta^{-1} X_1$. $\theta_2 = \widetilde{\theta_1}^{-1}$. Then $\delta_2(\mathbb{F}_q) = 0$ and $\delta_2(X_1) = \gamma - \beta\theta_1(\gamma) \in \mathbb{F}_q$

$$\boxed{R_2 = R_1[X_2; \theta_2, \delta_2] = \mathbb{F}_q[X_1; \theta_1, \delta_1][X_2; \theta_2, \delta_2]}$$

$$R_2 = \{\sum a_{i,j} X_1^i X_2^j \mid a_{i,j} \in \mathbb{F}_q\}.$$

Example : $\mathbb{F}_9[X_1; \theta_1, \delta_1][X_2; \theta_2, \delta_2]$, $\mathbb{F}_9$-algebra generated by X_1, X_2

$\mathbb{F}_9 = \mathbb{F}_3[\omega]$, $\theta_1 : x \mapsto x^3$, $d_1 = \omega \ \rightsquigarrow \delta_1 : x \mapsto \omega x - \theta_1(x)\omega$.

$$\rightsquigarrow \quad \forall a \in \mathbb{F}_9,\ X_1 a = a^3 X_1 + \omega a - a^3 \omega = \theta_1(a) X_1 + \delta_1(a)$$

$\beta = \omega^2 \ \rightsquigarrow \ \theta_2 : X_1 \mapsto \omega^2 X_1$ $\gamma = \omega \ \rightsquigarrow \delta_2 : X_1 \mapsto \omega^5$

$$\rightsquigarrow \quad \forall a \in \mathbb{F}_9,\ X_2 a = a^3 X_2 \quad \text{and} \quad X_2 X_1 = \omega^2 X_1 X_2 + \omega^5$$

D. Jordan (1995) : $\beta \in \mathbb{F}_q^*$, $\gamma \in \mathbb{F}_q$, $d_1 \in \mathbb{F}_q$ and $\theta_1 \in \mathrm{Aut}(\mathbb{F}_q)$.

1. $\theta_1 \in \mathrm{Aut}(\mathbb{F}_q)$ and $\delta_1 : x \mapsto d_1 x - \theta_1(x) d_1$ (inner derivation)

$$\boxed{R_1 = \mathbb{F}_q[X_1; \theta_1, \delta_1], \text{ where } \forall a \in \mathbb{F}_q,\ X_1 a = \theta_1(a) X_1 + \delta_1(a)}$$

2. Extend to $\widetilde{\theta_1} \in \mathrm{Aut}(R_1)$ by $\widetilde{\theta_1}(X_1) = \beta^{-1} X_1$. $\theta_2 = \widetilde{\theta_1}^{-1}$. Then $\delta_2(\mathbb{F}_q) = 0$ and $\delta_2(X_1) = \gamma - \beta\theta_1(\gamma) \in \mathbb{F}_q$

$$\boxed{R_2 = R_1[X_2; \theta_2, \delta_2] = \mathbb{F}_q[X_1; \theta_1, \delta_1][X_2; \theta_2, \delta_2]}$$

$$R_2 = \{\sum a_{i,j} X_1^i X_2^j \mid a_{i,j} \in \mathbb{F}_q\}.$$

Example : $\mathbb{F}_9[X_1; \theta_1, \delta_1][X_2; \theta_2, \delta_2]$, $\mathbb{F}_9$-algebra generated by X_1, X_2
$\mathbb{F}_9 = \mathbb{F}_3[\omega]$, $\theta_1 : x \mapsto x^3$, $d_1 = \omega \ \rightsquigarrow \delta_1 : x \mapsto \omega x - \theta_1(x)\omega$.

$$\rightsquigarrow \quad \forall a \in \mathbb{F}_9,\ X_1 a = a^3 X_1 + \omega a - a^3 \omega = \theta_1(a) X_1 + \delta_1(a)$$

$\beta = \omega^2 \ \rightsquigarrow \ \theta_2 : X_1 \mapsto \omega^2 X_1$ $\gamma = \omega \ \rightsquigarrow \delta_2 : X_1 \mapsto \omega^5$

$$\rightsquigarrow \quad \forall a \in \mathbb{F}_9,\ X_2 a = a^3 X_2 \quad \text{and} \quad X_2 X_1 = \omega^2 X_1 X_2 + \omega^5$$

$\mathbb{F}_9[X_1;\theta_1,\delta_1][X_2;\theta_2,\delta_2] \rightsquigarrow 81$ evaluation points
i.e. evaluation ideals $(X_1 - a_1, X_2 - a_2) \subset R_2$.

Example 1 : $\theta_1, d_1 = \omega, \beta = \omega^2, \gamma = \omega$

$I = (x2 + w, x1) \subset R_2$ is a maximal ideal

$I = (X_2+w, X_1) \subset R_2 : \ \omega^2 X_1(X_2+\omega) - X_2X_1 = \omega^{-5}X_1 + \omega^{-5} \ \Rightarrow \ 1 \in I$

$[24, 3, 20]_9$	polynomials of degre ≤ 1
$[24, 6, 8]_9$	polynomials of degre ≤ 2
$[24, 10, 4]_9$	polynomials of degre ≤ 3
$[24, 12, 3]_9$	polynomials of degre ≤ 4

Example 2 : $\theta_1, d_1 = 1, \beta = 1, \gamma = 1$

$[33, 3, 24]_9$	polynomials of degre ≤ 1
$[33, 6, 16]_9$	polynomials of degre ≤ 2
$[33, 10, 8]_9$	polynomials of degre ≤ 3
$[33, 14, 1]_9$	polynomials of degre ≤ 4

Example 2 : $\theta_1, d_1 = w, \beta = 1, \gamma = 1$

$[15, 3, 6]_9$	polynomials of degre ≤ 1
$[15, 6, 3]_9$	polynomials of degre ≤ 2
$[15, 9, 2]_9$	polynomials of degre ≤ 3
$[15, 11, 1]_9$	polynomials of degre ≤ 4

Example 2 : $\theta_1, d_1 = 1, \beta = \omega, \gamma = 1$

$[8, 3, 4]_9$	polynomials of degre ≤ 1
$[8, 6, 2]_9$	polynomials of degre ≤ 2
$[8, 8, 1]_9$	polynomials of degre ≤ 3

Example 2 : $\theta_1, d_1 = 1, \beta = \omega^2, \gamma = 1$

$[6, 3, 3]_9$	polynomials of degre ≤ 1
$[6, 5, 2]_9$	polynomials of degre ≤ 2
$[6, 6, 1]_9$	polynomials of degre ≤ 3

Codes over rings

$A = \mathbb{F}_2[y]/(y^3)$ a ring of order 8

commutative polynomial $y^2 X_1 X_2 \in A[X_1, X_2]$ has 48 zeros in A^2

Lemma

(Zippel 1979) For a non zero $f \in \mathbb{F}_q[X_1, \ldots, X_m]$, *where* $\deg_{X_i}(f) \leq d_i$, *we have* $Pr_{\alpha \in (\mathbb{F}_q)^m}[f(\alpha) \neq 0] \leq \frac{\prod_{i=1}^{m}(q - d_i)}{q^m}$.

$\rightsquigarrow$ 15