Decoding Reed-Muller codes with the Guruswami-Sudan's algorithm

Daniel Augot,
INRIA, Project-Team CODES

Mikhail Stepanov
St Petersburg State University of Aerospace Instrumentation

Outline

- The Guruswami-Sudan list decoding algorithm of Reed-Solomon codes;
- Multivariate evaluation codes: Reed-Solomon product codes and Reed-Muller codes
- The algorithm for Reed-Muller codes;
- The analysis of Pellikaan and Wu (2004);
- Our analysis;
- The algorithm for Reed-Solomon product codes;
- Reed-Muller codes as "univariate" codes; application (Pellikaan-Wu 2004).

Reed-Solomon codes as Evaluation codes

Let $S = \{x_1, \ldots, x_n\} \subset \mathbb{F}_q$ be a set of n distinct points in $\mathbb{F}_q$.

Let ev be the following *evaluation map*:

$$\begin{array}{rccl} \mathrm{ev}: & \mathbb{F}_q[X] & \to & \mathbb{F}_q^n \\ & f & \mapsto & \mathrm{ev}(f) = (f(x_1), \ldots, f(x_n)) \end{array}$$

and

$$L = \{f \in \mathbb{F}_q[X] \mid \deg f \leq k\}.$$

Then the *Reed-Solomon* code and dimension $k+1$ is

$$C_1 = \mathrm{ev}(L).$$

Hamming distance

Let $x, y \in \mathbb{F}_q^n$, then he *Hamming distance* is

$$d(x, y) = |\{i \in \{1, n\} \mid x_i \neq y_i\}|$$

Then the Reed-Solomon code C_1 is a q-ary code of *length* n, *dimension* $k + 1$ and *minimum distance* $n - k$.

By commodity, we also denote, for $f \in \mathbb{F}_q[X]$, and $(y_1, \ldots, y_n) \in \mathbb{F}_q^n$:

$$d(f, y) = |\{i \in \{1, n\} \mid f(x_i) \neq y_i\}|$$

The decoding problem

Let $S = \{x_1, \ldots, x_n\}$, and C_1 be given, and $y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$ be the received word. We have the following problems:

Unique Decoding $t = \lfloor \frac{d-1}{2} \rfloor$ is given, and one has to find the *at most unique* f such that $d(f, y) < t$. Berlekamp-Welch86.

List Decoding t, *larger than* $= \lfloor \frac{d-1}{2} \rfloor$, is given, one has to find *all* the codewords at distance less than t of y.

In the case of Reed-Solomon codes, this amounts to find all the $f \in \mathbb{F}_q[X]$, $\deg f \leq k$, such that

$$\mu = |\{i \mid f(x_i) = y_i\}|$$

is greater than or equal to $n - t$. Or equivalently $d(f, y) \leq t$.

The Guruswami-Sudan algorithm

input $X = \{x_1, \ldots, x_n\} \subset \mathbb{F}_q$, $k, \mu = n - t \in \mathbb{N}$, $y = (y_1, \ldots, y_n)$
the received word.

auxiliary parameters a degree d et s an order of multiplicity.

interpolation find a polynomial $Q(X, Z) \in \mathbb{F}_q[X, Z]$ such that

1. $Q(X, Z) \neq 0$,
2. $\mathrm{wdeg}_{1,k-1} Q(X, Z) \leq d$,
3. $\mathrm{mult}(Q; (x_i, y_i)) = s$, $i \in \{1, n\}$.

factorization Compute $List = \{f = f(X) \mid Q(X, f) = 0\}$.

verification return all $f \in List$ such that $\deg f \leq k$, et $d(f, y) < t$.

multiplicity and weighted degree

Let $Q = Q(X_1, \ldots, X_m) = Q_0 + Q_1 + \cdots + Q_d$ be given, where Q_i is homogeneous of degree i.

- The *multiplicity* of Q at the point $(0, \ldots, 0)$ is the smallest i such that $Q_i \neq 0$.
- The *multiplicity* of Q at the point $(x_1, \ldots, x_m)$ is the multiplicity at $(0, \ldots, 0)$ of the polynomial $Q(X_1 + x_1, \ldots, X_m + x_m)$.
- let $u_1, \ldots, u_m$ be given, the *weighted degree*, $\mathrm{wdeg}_{u_1,\ldots,u_m}$, of the monomial $X_1^{i_1} \cdots X_m^{i_m}$ is $u_1 i_1 + \cdots u_m i_m$.
- The *weighted degree* of Q is the largest weighted degree of its monomials.

The Guruswami-Sudan algorithm

input $X = \{x_1, \ldots, x_n\} \subset \mathbb{F}_q$, $k, \mu = n - t \in \mathbb{N}$, $y = (y_1, \ldots, y_n)$
the received word.

auxiliary parameters a degree d et s an order of multiplicity.

interpolation find a polynomial $Q(X, Z) \in \mathbb{F}_q[X, Z]$ such that

1. $Q(X, Z) \neq 0$,
2. $\mathrm{wdeg}_{1,k-1} Q(X, Z) \leq d$,
3. $\mathrm{mult}(Q; (x_i, y_i)) = s$, $i \in \{1, n\}$.

factorization Compute $List = \{f = f(X) \mid Q(X, f) = 0\}$.

verification return all $f \in List$ such that $\deg f \leq k$, et $d(f, y) < t$.

Guruswami-Sudan algorithm, polynomiality

input $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$, $k, \mu \in \mathbb{N}$, $y = (y_1, \ldots, y_n)$ the received word.

auxiliary parameters a degree d et s an order of multiplicity.

interpolation find a polynomial $Q(X, Z) \in \mathbb{F}_q[X, Z]$ such that...

$\Longrightarrow$ Linear algebra problem, polynomial time (in n and s).

factorization Compute $List = \{f = f(X) \mid Q(X, f) = 0\}$.

$\Longrightarrow$ polynomial time (Lenstra85, Kaltofen85, Grigoriev86)

verification return all $f \in List$ such that $\deg f \leq k$, et $d(f, y) < t$.

We will say that the algorithm runs in polynomial time.

Multiplicity transport

We present a general Lemma, which will be useful for generalizations.

LEMMA – let $Q(X_1, \ldots, X_m, Z)$ be such that

$$\mathrm{mult}(Q; (x_{i_1}, \ldots, x_{i_m}, y_{i_1,\ldots,i_m})) \geq s$$

Let f be such that $f(x_{i_1}, \ldots, x_{i_m}) = y_{i_1,\ldots,i_m}$, then, if Q_f denotes $Q(X_1, \ldots, X_m, f)$:

$$\mathrm{mult}(Q_f, (x_{i_1}, \ldots, x_{i_m})) \geq s.$$

Analysis (I)

1. Consider the polynomial $Q(X, f)$, then, for each i such that

$$f(x_i) = y_i,$$

we have $\mathrm{mult}(Q(X, f), x_i) \geq s$. Thus if

$$|\{i, f(x_i) = y_i\}| = \mu, \qquad (*)$$

the sum of multiplicities of $Q(X, f)$ is at least μs.

2. The condition $\mathrm{wdeg}_{1,k} Q(X, Z) \leq d$ implies $\deg Q \leq d$.
3. Thus if $d < \mu s$, all polynomials f such that $(*)$ holds satisfy

$$Q(X, f) = 0.$$

(more zeros, counted with multiplicities, than its degree)

Analysis (II)

The second logical step is to ensure that the polynomial Q always exists. The conditions on the polynomial Q are

1. $Q(X, Z) \neq 0$,
2. $\mathrm{wdeg}_{1,k-1} Q(X, Z) \leq d$, (*)
3. $\mathrm{mult}(Q; (x_i, y_i)) = s,\ i \in \{1, n\}$. (**)

Since (**) is a linear system of equations, a sufficient condition is to have more unknowns than equations. The number of unknowns is induced by (*). This gives

$$\frac{d(d+2)}{2(k-1)} > n\binom{s+1}{2}.$$

Analysis (III)

Working out the two conditions

$$\frac{d(d+2)}{2(k-1)} > n\binom{s+1}{2}.$$

and

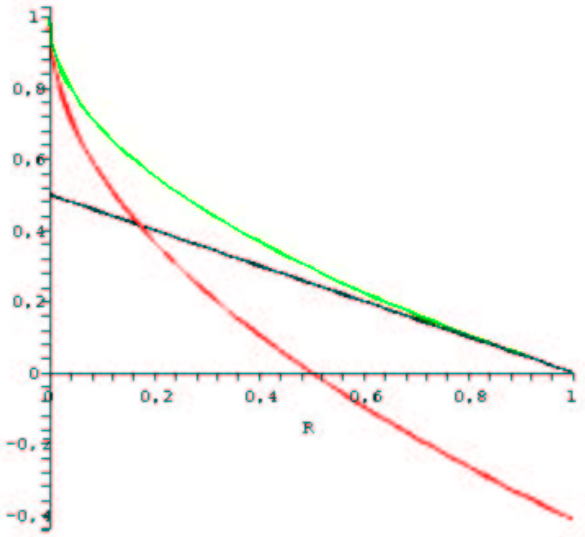
$$d \leq \mu s,$$

with $\mu = n - t$, gives

$$t \leq n\left(1 - \sqrt{\frac{k}{n}(1+\frac{1}{s})}\right) \underset{s \to +\infty}{\longrightarrow} \quad \tau \leq 1 - \sqrt{R},$$

with $\tau = t/n$ and $R = k/n$. (Kötter and Vardy derivation)

Plot



— : $(1-R)/2$,

— :$1-\sqrt{2R}$,

— : $1-\sqrt{R}$,

Let $S = \{x_1, \ldots, x_n\} \subseteq F_q$ be given, we construct $S^m \subseteq \mathbb{F}_q^m$.

We define

$$\begin{array}{rccl} \mathrm{ev}^m : & F_q[X_1, \ldots, X_m] & \to & (F_q)^{n^m} \\ & f(X_1, \ldots, X_m) & \mapsto & (f(x_{i_1}, \ldots, x_{i_m}))_{(x_{i_1} \ldots, x_{i_m}) \in S^m} \end{array}$$

Then we need to define a space L of polynomials.

Two generalizations

1. $L = \{f(X_1, \ldots, X_m),\ \deg f(X_1, \ldots, X_m) \leq r\}$, which corresponds to the Reed-Muller code of order r with m variables:

   $$C = \mathrm{RM}_q(r, m),$$

   which has dimension $\binom{m+r}{r}$, minimum distance $(n-r)n^{m-1}$.

2. $L = \{f(X_1, \ldots, X_m),\ \deg_{X_i} f(X_1, \ldots, X_m) \leq k, i \in \{1, m\}\}$, which corresponds to the m times product code of the Reed-Solomon code C_1:

   $$C_m = C_1 \otimes \cdots \otimes C_1$$

   which has dimension $(k+1)^m$, minimum distance $(n-k)^m$.

Both codes have length n^m.

The decoding problem

Let $S = \{x_1, \ldots, x_n\}$, and $m \in \mathbb{N}$, be given and $y = (y_{i_1,\ldots,i_m}) \in \mathbb{F}_q^{n^m}$ be the received word.

We want to correct t errors,i.e. to find $f = f(X_1, \ldots, X_m)$ such that:

$$|\{(i_1, \ldots, i_m) \mid f(x_{i_1}, \ldots, x_{i_m}) = y_{i_1,\ldots,i_m}\}| \geq n^m - t = \mu$$

such that (Reed-Muller case)

$$\deg f \leq r$$

or (product of Reed-Solomon case)

$$\deg_{X_i} f \leq k, \quad i \in \{1, m\}.$$

Case of the Reed-Muller codes

input $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$, $k, \mu \in \mathbb{N}$, $y = (y_{i_1,\ldots,i_n})$ the received word.

auxiliary parameters a degree d et s an order of multiplicity.

interpolation find a polynomial $Q(X_1, \ldots, X_m, Z)$ such that

1. $Q(X_1, \ldots, X_m, Z) \neq 0$,
2. $\mathrm{wdeg}_{1,\ldots,1,r} Q(X_1, \ldots, X_m, Z) \leq d$,
3. $\mathrm{mult}(Q; (x_{i_1}, \ldots, x_{i_m}, y_{i_1,\ldots,i_m})) = s$, $(i_1 \ldots, i_m) \in \{1, n\}^m$.

factorization Compute

$$List = \{f = f(X_1, \ldots, X_m) \mid Q(X_1, \ldots, X_m, f) = 0\}.$$

verification return all $f \in L$ such that $\deg f \leq r$, et $d(f, y) < t$.

Properties of Q_f

Let $Q_f = Q(X_1, \ldots, X_m, f)$, then

1. $\deg Q_f \leq d$.
2. for each point such that

$$f(x_{i_1}, \ldots, x_{i_m}) = y_{i_1,\ldots,i_m}$$

then

$$\mathrm{mult}(Q_f; (x_{i_1,\ldots,x_{i_m}})) \geq s$$

3. Thus, if $d(f, y) < t = n^m - \mu$ then the sum of multiplicities of Q_f over S^m is more than or equal to $s\mu$.

More zeros than its degree ?

This will translate into a statement "more points in the Δ-set than allowed". First we count the number of zeros, with multiplicities.

Let $I(q,m) = \langle X_i^q - X_i; i \in \{1,m\}\rangle$, it is the ideal of all polynomials which vanishes over $\mathbb{F}_q^m$.

Let $I(q,s,m) = I(q,m)^s$, it the ideal of all polynomials which vanishes over $\mathbb{F}_q^m$, with multiplicity $\geq s$.

LEMMA – Let $Q_f \in \mathbb{F}_q[X_1,\ldots,X_m]$, and let μ be the number of points (in $\mathbb{F}_q^m$) where Q_f has multiplicity s then

$$|\Delta\left(I(q,s,m) + \langle Q_f\rangle\right)| \geq \binom{m+s-1}{s-1}\mu$$

Proof (sketch)

Let $\mathcal{M}_{i_1,\ldots,i_m} = \langle X - x_{i_1}, \ldots, X_m - x_{i_m} \rangle$. One uses that:

$$R/\left\langle I(q,s,m) + < Q_f > \right\rangle \approx \bigoplus_{i_1,\ldots,i_m} R/\left\langle \mathcal{M}^s_{i_1,\ldots,i_m} + < Q_f > \right\rangle.$$

If $\mathrm{mult}(Q_f; (x_{i_1}, \ldots, x_{i_m})) \geq s$ then $Q_f \in \mathcal{M}^s_{i_1,\ldots,i_m}$. In that case

$$\dim R/\left\langle \mathcal{M}^s_{i_1,\ldots,i_m} + < Q_f > \right\rangle = \dim R/\left\langle \mathcal{M}^s_{i_1,\ldots,i_m} \right\rangle = \binom{m+s-1}{s-1}$$

Thus a total of

$$\mu \binom{m+s-1}{s-1}$$

(one for each point such that $\mathrm{mult}(Q_f; (x_{i_1}, \ldots, x_{i_m})) \geq s$)

Upper bound on the Δ-set ($n = q$)

LEMMA – let $f \in R$, such that $\deg f \leq d$. Let $w = \lfloor d/q \rfloor$, then

$$\Delta\left(I(q,s,m)+ < f >\right) \leq$$

$$\binom{m+s-1}{m} q^m + (d - qw)\binom{m+s-w-2}{m-1} q^{m-1} - \binom{m+s-w-1}{m} q^m$$

PROOF – 3 pages...

It can be rewritten as

$$\Delta\left(I(q,s,m)+ < f >\right) \leq q^m \left(\binom{m+s-1}{m} - \binom{m+s-w-2}{m} \right).$$

More zeros than allowed

Choose s and d such that (more zeros than allowed)

$$q^m \left(\binom{m+s-1}{m} - \binom{m+s-w-2}{m} \right) < \binom{m+s-1}{m} \mu$$

with $w = \lfloor d/q \rfloor$.

Rewrite:

$$\mu > q^m \left(1 - \frac{\binom{m+s-w-2}{m}}{\binom{m+s-1}{m}} \right).$$

After computations...

$$\mu > q^m \left(1 - \left(1 - \frac{w}{s} \right)^m \right)$$

More unknowns than equations

The number of equations is (number of monomials in $m+1$ variables of degree less than $s-1$)

$$N_{eq} = \binom{m+s}{s-1} n^m$$

N_Q, the number of terms of $Q(X_1, \ldots, X_m, X)$ follows from

$$\mathrm{wdeg}_{1,\ldots,1,r}\, Q(X_1, \ldots, X_m, Z) \leq d,$$

which implies that $Q = \sum_j Q_j(X_1, \ldots, X_m) Z^j$, with $\deg Q_j \leq d - jr$:

$$N_Q = \sum_j \binom{d - jr + m}{m}$$

Number of terms

$$N_Q = \sum_{j=0}^{d/r} \binom{d-rj+m}{m} \geq \sum_{j=0}^{d/r} \frac{(d-rj)^m}{m!}$$

$$\geq \int_0^{\frac{d}{r}} \frac{(d-rx)^m}{m!} dx = \frac{d^{m+1}}{r(m+1)!}$$

Thus $N_Q > N_{eq}$ gives

$$d > q \cdot \sqrt[m+1]{\frac{r}{q} s(s+1)\cdots(s+m)}.$$

Two conditions

If

$$d > q \cdot \sqrt[m+1]{\frac{r}{q} s(s+1)\cdots(s+m)}$$

the polynomial Q *always exists*, and if

$$\mu > q^m \left(1 - \left(1 - \frac{w}{s}\right)^m\right)$$

with $w = \lfloor d/q \rfloor$. then, all $f = f(X_1, \ldots, X_m)$ such that

$$\deg f \leq r$$

and

$$d(f, y) < t = n^m - \mu$$

will satisfy $Q(X_1, \ldots, X_m, f) = 0$.

Result

And we get ($q = n$):

$$t < q^m \left(1 - \sqrt[m+1]{\frac{r}{q}(1+\frac{1}{s})\cdots(1+\frac{m}{s})}\right)^m \underset{s\to+\infty}{\longrightarrow} n^m \left(1 - \sqrt[m+1]{\frac{r}{q}}\right)^m$$

Note that $m = 1$ gives the decoding radius of the Guruswami-Sudan decoding algorithm.

A stronger lemma

LEMMA – Let $Q_f = Q_f(X_1, \ldots, X_m)$ of total degree d, and $S = \{x_1, \ldots, x_n\}$, then the sum of multiplicities of Q_f over S^m is less than or equal to

$$dn^{m-1}$$

PROOF: by induction.

Generalization of Schwartz-Zippel Lemma (1980), with multiplicities.

Analysis (III)

Thus if

$$s\mu > dn^{m-1}, \quad (*)$$

then $Q(X_1, \ldots, X_m, f) = 0$.

The second condition, to ensure $Q(X_1, \ldots, X_m, Z)$ always exists is

$$N_Q > N_{eq}.$$

The analysis for the existence of the polynomial Q is the same as previously (same number of equations, same number of unknowns):

$$d > q \cdot \sqrt[m+1]{\frac{r}{q} s(s+1)\cdots(s+m)}$$

Thus

$$s\mu > dn^{m-1},$$

give

$$t \leq n^m(1 - \sqrt[m+1]{\frac{r}{n}(1+\frac{1}{s})\cdots(1+\frac{m}{s})}) \quad \overrightarrow{s \to +\infty} \quad n^m\left(1 - \sqrt[m+1]{\frac{r}{n}}\right),$$

to be compared with

$$n^m\left(1 - \sqrt[m+1]{\frac{r}{n}}\right)^m.$$

Case of products of Reed-Solomon codes

input $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$, $k, \mu \in \mathbb{N}$, $y = (y_{i_1,\ldots,i_n})$ the received word.

auxiliary parameters a degree k' et s an order of multiplicity.

interpolation find a polynomial $Q(X_1, \ldots, X_m, Z)$ such that

1. $Q(X_1, \ldots, X_m, Z) \neq 0$,
2. Q has no term $q_{i_1,\ldots,i_m,j}$ such that at least one index i_l satisfies $i_l + kj > k'$;
3. $\mathrm{mult}(Q; (x_{i_1}, \ldots, x_{i_m}, y_{i_1,\ldots,i_m})) = s$, $(i_1 \ldots, i_m) \in \{1, n\}^m$.

factorization Compute $List = \{f \mid Q(X_1, \ldots, X_m, f) = 0\}$.

verification return all $f \in List$ such that $\deg_{X_i} f \leq k$, $i \in \{1, m\}$, and $d(f, y) < t$.

One can check that the condition

2. Q has no term $q_{i_1,\ldots,i_m,j}$ if at least one index i_l satisfies $i_l + kj > k'$

gives: $Q_f = Q(X_1, \ldots, X_m, f)$ satisfies $\deg_{X_i} Q_f \leq k', \quad i \in \{1, m\}$.

And the sum of multiplicities of Q_f over S^m is at least

$$s\mu$$

if $t = n^m - \mu$.

Analysis (II)

Since Q_f has degree $\leq k'$ in each variable, and Q_f has at least $s\mu$ zeros (counted with multiplicities) then ???

LEMMA – Let $u = u(X_1, \ldots, X_m)$ of degree less than or equal to k' in each variable, and $S = \{x_1, \ldots, x_n\}$, then the sum of multiplicities of u over S^m is less than or equal to

$$mk'n^{m-1}.$$

(Kind of Schwartz-Zippel Lemma).

Thus the first condition to ensure $Q_f = 0$ is

$$s\mu > mk'n^{m-1}.$$

Analysis (II)

Second condition, for existence of the Q polynomial is $N_Q > N_{eq}$, with

$$\begin{aligned} N_Q &= \sum_{i=0}^{\lfloor k'/k \rfloor} (k' - ik)^m \\ &\geq \int_0^{k'/k} (k' - xk)^m dx \\ &= \frac{k'^{m+1}}{(m+1)k} \end{aligned}$$

and

$$N_{eq} = \frac{\binom{m+s}{s-1}^m}{n} .$$

Result

Working out

$$\frac{k'^{m+1}}{(m+1)k} > \frac{s\dots(s+m)}{(m+1)!}n^m$$

and

$$s\mu > mk'n^{m-1},$$

with $t = n^m - \mu$, gives

$$t = n^m - \mu \leq n^m \left(1 - \sqrt[m+1]{\frac{m^{m+1}}{m!} \cdot \frac{k}{n} \cdot (1+\frac{1}{s}) \cdots (1+\frac{m}{s})}\right)$$

$$\overrightarrow{s \to +\infty} \quad n^m \left(1 - \sqrt[m+1]{\frac{m^{m+1}}{m!} \cdot \frac{k}{n}}\right)$$

Univariate approach

. . . or the discrete charm of finite fields (following Pellikaan-Wu2004).

Reed-Muller codes as cyclic codes

Let $S = \mathbb{F}_q$, consider $\mathrm{RM}_q(r, m)$, rearranging the order of the elements, and deleting the position corresponding to $(0, \ldots, 0)$.

We get a code of length $N^* = q^n - 1$, and minimum distance $d - 1$, where d can be computed explicitly from the parameters q, m, r.

PROPOSITION – The q-ary code $\mathrm{RM}_q^*(r, m)$ is the *subfield subcode* of the BCH code, over $\mathbb{F}_{q^m}$, whose generator polynomial is

$$\mathrm{lcm}(Z - \alpha, \ldots, Z - \alpha^i, \ldots, Z - \alpha^{d-2}),$$

where α is a primitive n-th root of unity. That is to say:

$$\mathrm{RM}_q(r, m) = \mathrm{BCH}_{q^m}(d - 1) \cap \mathbb{F}_q^{N^*}$$

[Kasami-Lin-Peterson68]

The BCH code as an evaluation Reed-Solomon code

Let $X = \{1, \alpha, \alpha^2, \ldots, \alpha^{N^*-1}\}$, in that order, with the corresponding evaluation map.

$$\begin{array}{rccl} \mathrm{ev}: & \mathbb{F}_q[X] & \to & \mathbb{F}_q^{N^*} \\ & f & \mapsto & \mathrm{ev}(f) = (f(1), f(\alpha) \ldots, f(\alpha^{N^*-1})). \end{array}$$

Let $p = \mathrm{ev}(f) = (p_0, \ldots, p_{N^*-1})$, to be considered as a polynomial:

$$p(X) = p_0 + p_1 X + \cdots + p_{N-1} X^{N^*-1}.$$

Then, if $\deg f \leq N^* - d + 1$, then (property of the Fourier transform)

$$p(\alpha^i) = 0, \quad i \in \{1, d-2\},$$

i.e $p \in \mathrm{BCH}_{q^m}$ of designed distance $d - 1$.

So:

$$\mathrm{RM}_q(r,m)^* = \mathrm{BCH}_{q^m}(d-1) \cap \mathbb{F}_q^{N^*} = \mathrm{RS}_{N^*-d+2}(X) \cap \mathbb{F}_q^{N^*}$$

with $X = \{1, \alpha, \alpha^2, \ldots, \alpha^{N^*-1}\}$, Thus, extending the codes:

$$\mathrm{RM}_q(r,m) = \mathrm{RS}_{N^*-d+2}(X \cup \{0\}) \cap \mathbb{F}_q^{N}.$$

i.e. the Reed-Muller code can be seen as "univariate" evaluation code.

The result

Thus the algorithm is:

decode with respect the Generalized Reed-Solomon, of parameters $[N, N-d+1, d]_{q^m}$, with the Guruswami-Sudan algorithm,

check if the corresponding words are in the subfield subcode.

One gets (for $r < q$:

$$t < N\left(1 - \sqrt{\frac{r}{q}}\right),$$

compare with $N\left(1 - \sqrt[m+1]{\frac{r}{q}}\right)$.

Conclusion

- Various "multivariate" interpolation based decoding algorithm have been shown
- It is essential to have a statement "more zeros than allowed".
- Depending on the strength of the corresponding lemma, one get different results.
- From coding theory, one can interpret multivariate evaluation codes as univariate codes (over finite fields).
- One can use the Guruswami-Sudan algorithm to get a much better performance.
- Disappointing to get a bad performance with ad hoc theorems.