A note on the generalisation of the Guruswami-Sudan list decoding algorithm to Reed-Muller codes

Daniel Augot[1] and Michael Stepanov[2]

[1] INRIA Paris-Rocquencourt, Project-Team Secret Daniel.Augot@inria.fr
[2] St. Petersburg State University of Aerospace Instrumentation
mstepanov@gmail.com

Summary. We revisit the generalisation of the Guruswami-Sudan list decoding algorithm to Reed-Muller codes. Although the generalisation is straightforward, the analysis is more difficult than in the Reed-Solomon case. A previous analysis has been done by Pellikaan and Wu, relying on the theory of Gröbner bases [2, 3]. We give a stronger form of the well-known Schwartz-Zippel Lemma [5, 4], taking multiplicities into account. Using this Lemma, we get an improved decoding radius.

1 Definitions and Notation

We consider $S = \{x_1, \ldots, x_n\}$ a set of n distinct elements of $\mathbb{F}_q$. Let N, r be integers greater than or equal to one, we consider the evaluation map, defined on $\mathbb{F}_q[X_1, \ldots, X_n]$:

$$\mathrm{ev}^N : f(X_1, \ldots, X_N) \mapsto (f(x_{i_1}, \ldots, x_{i_N}))_{(x_{i_1} \ldots, x_{i_N}) \in S^N}$$

We fix the following space of polynomials: $L = \{f(X_1, \ldots, X_N),\ \deg f \leq r\}$. Then the code $\mathrm{ev}^N(L)$ is the Reed-Muller code of order r with N variables.

We say that a polynomial $Q(X_1, \ldots, X_N)$ has multiplicity s at the point $(0, \ldots, 0)$ if it does not contain any monomial of degree strictly less than s. We say that a polynomial $Q(X_1, \ldots, X_N)$ has multiplicity s at $(x_{i_1}, \ldots, x_{i_N})$ if the polynomial $Q(X_1 + x_{i_1}, \ldots, X_N + x_{i_N})$ has multiplicity s at $(0, \ldots, 0)$. The weighted degree $\mathrm{wdeg}_{a_1, \ldots, a_N}$ of a monomial $X_1^{i_1} \cdots X_N^{i_N}$ is $a_1 i_1 + \cdots + a_N i_N$. The weighted degree of a polynomial is the maximum weighted degree of its monomials.

2 The algorithm

The algorithm is as follows. Let τ be the number of errors that will be corrected. The received word is a N -dimensional array $y = (y_{i_1, \ldots, i_N})_{(i_1, \ldots, i_N) \in \{1, \ldots, n\}^N}$.

input $(x_1, \ldots, x_n) \in \mathbb{F}_q^n$, $r, \tau \in \mathbb{N}$, $y = (y_{i_1,\ldots,i_N})$ the received word; auxiliary parameters: a degree d and s an order of multiplicity.

interpolation find a polynomial $Q = Q(X_1, \ldots, X_N, Z)$ such that
1. $Q(X_1, \ldots, X_N, Z) \neq 0$,
2. $\mathrm{wdeg}_{1,\ldots,1,r} Q(X_1, \ldots, X_N, Z) \leq d$,
3. $\mathrm{mult}(Q; (x_{i_1}, \ldots, x_{i_N}, y_{i_1,\ldots,i_N})) = s$, $(i_1 \ldots, i_N) \in \{1, \ldots, n\}^N$.

factorisation Compute $L = \{f = f(X_1, \ldots, X_N) \mid Q(X_1, \ldots, X_N, f) = 0\}$.

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

The analysis of this family of interpolation based decoding algorithms is in two steps. First we must find conditions such that the polynomial $Q(X_1, \ldots, X_N, Z)$ always exists, and secondly analyze the conditions under which $Q(X_1, \ldots, X_N, f) = 0$. For the existence of the polynomial Q, we will require that the number of unknowns is greater than the number of equations. Each condition $\mathrm{mult}(Q; (x_{i_1}, \ldots, x_{i_N}, y_{i_1,\ldots,i_N})) = s$ implies $\binom{s+N}{N+1}$ linear equations on Q. On the other hand, the number of unknowns in the Q polynomial is roughly $\frac{d^{N+1}}{(N+1)!r}$, and a condition for the existence of Q is

$$\frac{d^{N+1}}{(N+1)!r} > \binom{s+N}{N+1} n^N,$$

Let Q_f be the polynomial $Q(X_1, \ldots, X_m, f)$. We note that, since the condition $\mathrm{wdeg}_{1,\ldots,1,r} Q(X_1, \ldots, X_N, Z) \leq d$ holds, we have that $\deg Q_f \leq d$. We need a Theorem to conclude that the polynomial $\deg Q(X_1, \ldots, X_N, f)$ has "more zeros than allowed". In the univariate case, it is enough to state the a polynomial can not have more zeros than its degree. In the multivariate case, things are harder. Pellikaan and Wu have overcome this difficulty by relying on the theory of Gröbner bases and footprints. They eventually get the following relative decoding radius:

$$\frac{\tau}{n^N} \leq \left(1 - \sqrt[N+1]{\frac{r}{n}}\right)^N. \tag{1}$$

3 The analysis

Lemma 1. *Let $Q(X_1, \ldots, X_N)$ be of total degree less than d. Let $x_1, \ldots, x_n$ be n distinct points in $\mathbb{F}_q$. The sum of multiplicities of $Q(X_1, \ldots, X_N)$ over the n^N points $(x_{i_1}, \ldots, x_{i_N}) \in \mathbb{F}_q^N$ is less than or equal to dn^{N-1}.*

Proof. By induction. The statement is true for $N = 1$. Let us consider the set I of points $x_{i_1}, \ldots, x_{i_l}$, such that $Q(X_1, \ldots, X_{N-1}, x_{i_j})$ is identically zero, $j = 1, \ldots, l$. Also let I' be $\{1, \ldots, n\} \backslash I$. Then, for $x_{i_j} \notin I$, let Q_{i_j} be the polynomial $Q(X_1, \ldots, X_{N-1}, x_{i_j})$. Then the number of zeros, counted with multiplicities of Q_{i_j}, over the points whose last coordinates is x_{i_j} is by induction bounded by dn^{N-2}. Now, for $x_{i_j} \in I$, we can write

$$Q(X_1,\dots,X_N) = (X_n - x_{i_j})^{t_{i_j}} \tilde{Q}_{i_j}(X_1,\dots,X_N)$$

for some $t_{i_j} > 0$, and where $\tilde{Q}_{i_j}(X_1,\dots,X_N)$ is such that $\tilde{Q}_{i_j}(X_1,\dots,X_{N-1},x_{i_j})$ is not identically zero. The degree of $\tilde{Q}_{i_j}(X_1,\dots,X_N)$ is $d - t_{i_j}$. Now the number of multiplicities of $\tilde{Q}_{i_j}(X_1,\dots,X_N)$ over the points whose last coordinate is x_{i_j} is bounded by $(d-t_{i_j})n^{N-2}$, using the induction hypothesis. Let Σ be the sum of multiplicities. Let S_{i_j} be the set of points whose last coordinates is x_{i_j}. Then

$$\begin{aligned}
\Sigma &= \sum_{x_{i_j}\in I'} \sum_{p\in S_{i_j}} \mathrm{mult}(Q,p) + \sum_{x_{i_j}\in I} \sum_{p\in S_{i_j}} \mathrm{mult}(Q,p) \\
&\le |I'|dn^{N-2} + \sum_{x_{i_j}\in I} \sum_{p\in S_{i_j}} \Big(t_{i_j} + \mathrm{mult}(\tilde{Q}_{i_j},p) \Big) \\
&\le |I'|dn^{N-2} + \sum_{x_{i_j}\in I} \big(t_{i_j} n^{N-2} + (d-t_{i_j})n^{N-2} \big) \\
&\le |I'|dn^{N-2} + |I|dn^{N-2} = dn^{N-1}.
\end{aligned}$$

To ensure that the polynomial Q_f is identically zero, we must have that Q_f has more than dn^{N-1} zeros counted with multiplicities. If $s(n^N - \tau) > dn^{N-1}$, Q_f is identically zero. Working out the formulas leads to:

$$\tau \le n^N - \sqrt[N+1]{rn^N(1+\frac{1}{s})\dots(1+\frac{N}{s})} \le n^N \left(1 - \sqrt[N+1]{\frac{r}{n}}\right). \qquad (2)$$

This compares favourably to the Pellikaan-Wu radius. In conclusion, we note that, over the binary field, the Reed-Muller codes can be considered as subfield subcodes of classical Reed-Solomon codes [1], and one can get a better decoding radius, using the univariate Guruswami-Sudan algorithm.

References

1. T. Kasami, Shu Lin, and W. Peterson. New generalizations of the Reed-Muller codes–I: Primitive codes. *IEEE Transactions on Information Theory*, 14(2):189–199, 1968.
2. Ruud Pellikaan and Xin-Wen Wu. List decoding of q-ary Reed-Muller codes. preprint available form authors, 2004.
3. Ruud Pellikaan and Xin-Wen Wu. List decoding of q-ary Reed-Muller codes. *IEEE Transactions on Information Theory*, 50(4):679–682, 2004.
4. J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, October 1980.
5. Richard Zippel. Probabilistic algorithms for sparse polynomials. In Edward W. Ng, editor, *Symbolic and Algebraic Computation: EUROSM '79*, volume 72 of *Lecture Notes in Computer Science*, pages 216–226. Springer, 1979.