ulm university universität uulm

Single-Trial Adaptive Decoding of Concatenated Codes

Vladimir R. Sidorenko, Christian Senger, Martin Bossert
(TAIT, Ulm University)
Victor V. Zyablov (IITP, Russian Academy of Sciences)

11th International Workshop on Algebraic and Combinatorial Coding Theory, 16.06.-22.06.2008, Pamporovo, Bulgaria

Motivation/History

- Since their invention by Forney in 1966, serially concatenated codes are frequently used in applications.
- Reason: Easily decodable component codes might be chosen resulting in low overall decoding complexity.
- However, decoding up to half the minimum concatenated code distance is non-trivial. Multiple decoding trials are required.
- Several approaches to optimize single-trial decoding by [Zyablov, 1973], [Kovalev, 1986], (some refinements in [Weber and Abdel-Ghaffar, 2003]), [Sorger, 1993] and [Kötter, 1993].
- All previous approaches assume outer BMD decoding

Motivation/History

- Since their invention by Forney in 1966, serially concatenated codes are frequently used in applications.
- Reason: Easily decodable component codes might be chosen resulting in low overall decoding complexity.
- However, decoding up to half the minimum concatenated code distance is non-trivial. Multiple decoding trials are required.
- Several approaches to optimize single-trial decoding by [Zyablov, 1973], [Kovalev, 1986], (some refinements in [Weber and Abdel-Ghaffar, 2003]), [Sorger, 1993] and [Kötter, 1993].
- All previous approaches assume outer BMD decoding – we derive a single-trial algorithm for outer BD decoding!

Encoding of Concatenated Codes

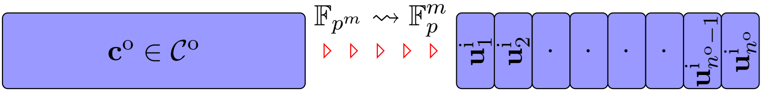
Codeword of outer code
$\mathcal{C}^{\mathrm{o}}(\mathbb{F}_{p^m}; n^{\mathrm{o}}, k^{\mathrm{o}}, d^{\mathrm{o}})$

$\mathbf{c}^{\mathrm{o}} \in \mathcal{C}^{\mathrm{o}}$

Encoding of Concatenated Codes

Codeword of outer code $\mathcal{C}^{\mathrm{o}}(\mathbb{F}_{p^m}; n^{\mathrm{o}}, k^{\mathrm{o}}, d^{\mathrm{o}})$

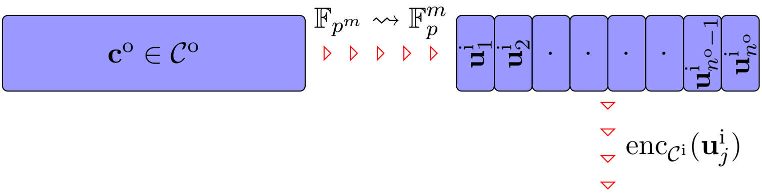
Map symbols from $\mathbb{F}_{p^m}$ to column vectors from $\mathbb{F}_p^m$



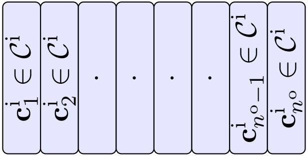
Encoding of Concatenated Codes

Codeword of outer code
$\mathcal{C}^{\mathrm{o}}(\mathbb{F}_{p^m}; n^{\mathrm{o}}, k^{\mathrm{o}}, d^{\mathrm{o}})$

Map symbols from $\mathbb{F}_{p^m}$ to column vectors from $\mathbb{F}_p^m$



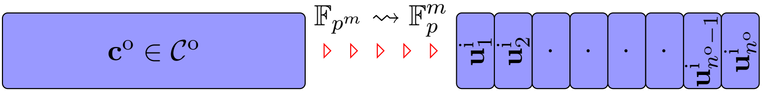
Encode columns with encoder of inner code $\mathcal{C}^{\mathrm{i}}(\mathbb{F}_p; n^{\mathrm{i}}, k^{\mathrm{i}} = m, d^{\mathrm{i}})$

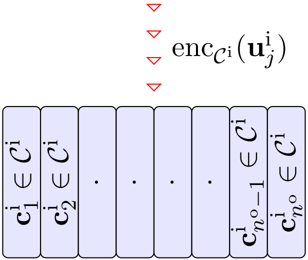


Encoding of Concatenated Codes

Codeword of outer code $\mathcal{C}^{\mathrm{o}}(\mathbb{F}_{p^m}; n^{\mathrm{o}}, k^{\mathrm{o}}, d^{\mathrm{o}})$

Map symbols from $\mathbb{F}_{p^m}$ to column vectors from $\mathbb{F}_p^m$





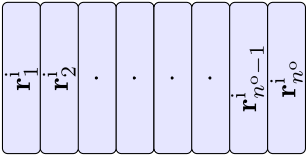
Encode columns with encoder of inner code $\mathcal{C}^{\mathrm{i}}(\mathbb{F}_p; n^{\mathrm{i}}, k^{\mathrm{i}} = m, d^{\mathrm{i}})$

Result of this procedure: $n^{\mathrm{i}} \times n^{\mathrm{o}}$ matrix $\boldsymbol{C}$ over $\mathbb{F}_p$

$$\Longrightarrow \boldsymbol{C} \in \mathcal{C}(\mathbb{F}_p;\ n = n^{\mathrm{o}} n^{\mathrm{i}},\ k = m k^{\mathrm{o}},\ d = d^{\mathrm{o}} d^{\mathrm{i}})$$

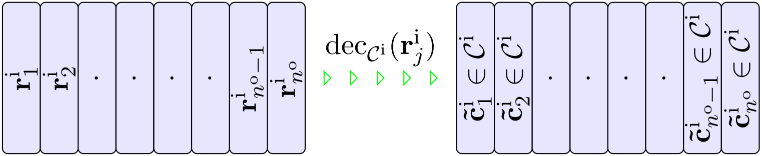
Classical Decoding of Concatenated Codes

Received word $\boldsymbol{R} = \boldsymbol{C} + \boldsymbol{E}$



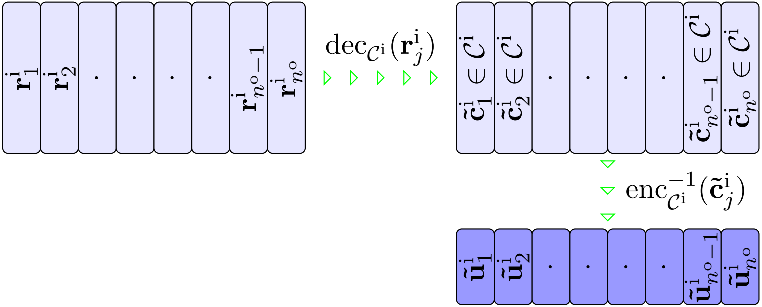
Classical Decoding of Concatenated Codes

Received word $\boldsymbol{R} = \boldsymbol{C} + \boldsymbol{E}$



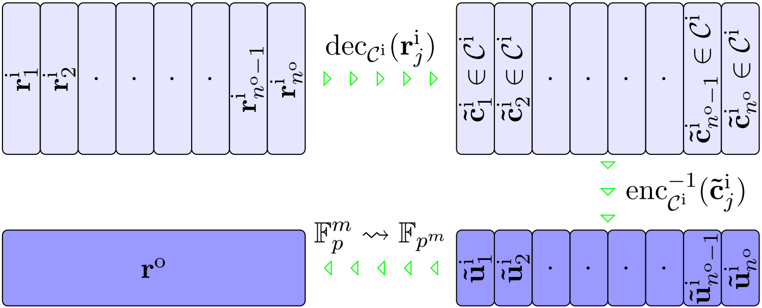
Classical Decoding of Concatenated Codes

Received word $\boldsymbol{R} = \boldsymbol{C} + \boldsymbol{E}$



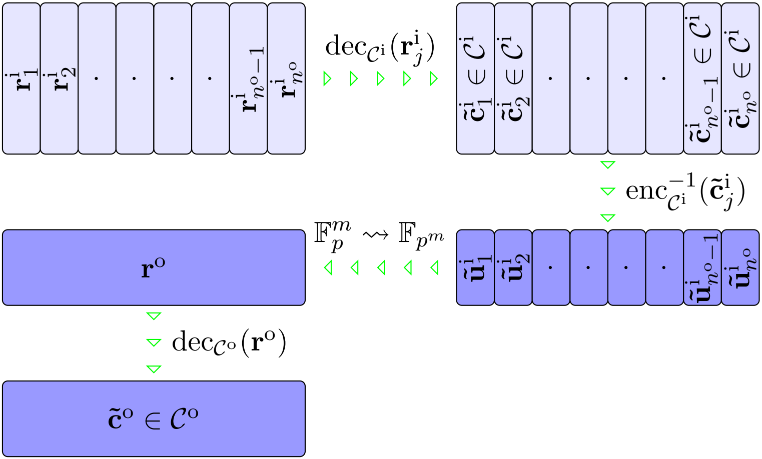
Classical Decoding of Concatenated Codes

Received word $\boldsymbol{R} = \boldsymbol{C} + \boldsymbol{E}$



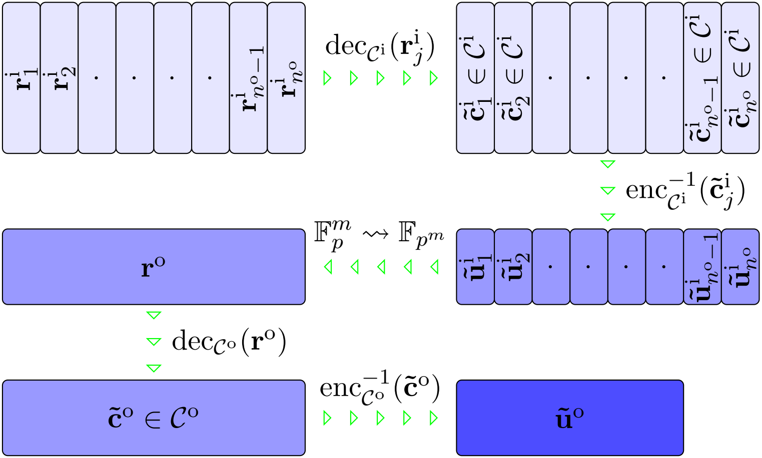
Classical Decoding of Concatenated Codes

Received word $\boldsymbol{R} = \boldsymbol{C} + \boldsymbol{E}$



Classical Decoding of Concatenated Codes

Received word $\boldsymbol{R} = \boldsymbol{C} + \boldsymbol{E}$



Decoding result

Decoding Radius of Classical Decoding

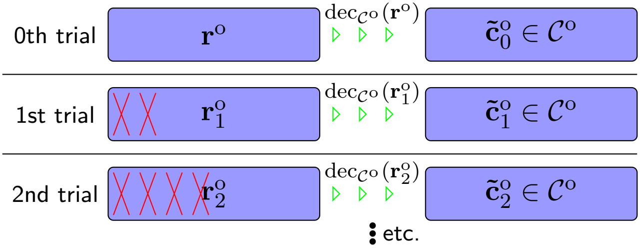
Classical decoding as described above guarantees to decode

$$e < \frac{d^{\mathrm{o}} d^{\mathrm{i}}}{4}$$

channel errors [Forney, 1966].

Multi-Trial Error/Erasure Decoding of Conc. Codes

- Input for the outer decoder is $\mathbf{r}^{\mathrm{o}} = (r_1^{\mathrm{o}}, \dots, r_{n^{\mathrm{o}}}^{\mathrm{o}})$.
- For each symbol r_j^{o} inner decoding implicitly yields the *un*reliability measure $\Delta_j := \mathrm{d_H}(\mathbf{r}_j^{\mathrm{i}}, \tilde{\mathbf{c}}_j^{\mathrm{i}})$. W.l.o.g. $\Delta_j \geq \Delta_{j+1}$.
- Decoding in $d^{\mathrm{o}}/2$ trials with increasing number of erased (X) most unreliable received symbols:



- Result: List of at most $d^{\mathrm{o}}/2$ codeword candidates.
- Selection among the list possible by known criterion.

Decoding Radius of Multi-Trial Decoding

- Multi-trial error/erasure decoding as described above guarantees to decode
$$e < \frac{d^{\mathrm{o}} d^{\mathrm{i}}}{2}$$
channel errors.
- In literature, procedure is called Generalized Minimum Distance (GMD) decoding [Forney, 1966].

Single-Trial Approaches

- [Zyablov, 1973] proposes single-trial decoding by fixing a static threshold T for erasing received symbols, i.e. r_j^{o} is erased if $\Delta_j > T$. The decoding radius is

$$e < \frac{d^{\mathrm{o}} d^{\mathrm{i}}}{3}.$$

  Threshold T is chosen independently of $\boldsymbol{\Delta}$.
- [Kovalev, 1986] takes the unreliabilities $\boldsymbol{\Delta}$ into consideration (adaptive decoding). Bounds for the decoding radius give

$$e < \rho \approx \frac{3 d^{\mathrm{o}} d^{\mathrm{i}}}{8}.$$

- Aforementionend approaches assume outer BMD decoding. Our task: Derive an adaptive single-trial decoder assuming outer BD decoding!

Derivation of a Single-Trial Adaptive Decoder

- Assume an outer BD decoder with error/erasure tradeoff parameter $1 < \lambda \leq 2$. Outer decoding fails if

$$\lambda\varepsilon + \tau > d^{\mathrm{o}} - 1.$$

- For given number τ of erasures (☓), outer decoding fails if

$$\varepsilon(\tau) \geq \left\lfloor \frac{d^{\mathrm{o}} - \tau - 1}{\lambda} \right\rfloor + 1.$$

- For given unreliabilities $\boldsymbol{\Delta} := (\Delta_1, \ldots, \Delta_{n^{\mathrm{o}}})$, $\Delta_j \geq \Delta_{j+1}$, the minimum number of channel errors to obtain $\varepsilon(\tau)$ errors is

$$\begin{aligned} e_\tau(\boldsymbol{\Delta}) &:= \sum_{j=1}^{\tau} \Delta_j + \sum_{j=\tau+1}^{\tau+\varepsilon(\tau)} (d^{\mathrm{i}} - \Delta_j) + \sum_{j=\tau+\varepsilon(\tau)+1}^{n^{\mathrm{o}}} \Delta_j \\ &= \sum_{j=1}^{n^{\mathrm{o}}} \Delta_j + \sum_{j=\tau+1}^{\tau-\varepsilon(\tau)} (d^{\mathrm{i}} - 2\Delta_j). \end{aligned}$$

Single-Trial Outer Error/Erasure Decoding

Input. Received vector $\mathbf{r}^{\mathrm{o}}$, ordered unreliabilities $\mathbf{\Delta}$ from inner decoder. d^{i}, d^{o} and parameter $1 < \lambda \leq 2$.

Step 1. Find $\tau^* = \underset{\tau \in \{0,\ldots,d^{\mathrm{o}}-1\}}{\arg\max} \sum_{j=\tau+1}^{\tau+\varepsilon(\tau)} (d^{\mathrm{i}} - 2\Delta_j)$.

Step 2. Decode $\mathbf{r}^{\mathrm{o}}$ with erased most unreliable (first) τ^* positions by error/erasure decoder for $\mathcal{C}^{\mathrm{o}}$ with error/erasure tradeoff parameter λ.

Output. Either a codeword of $\mathcal{C}^{\mathrm{o}}$ or decoding failure.

Decoding Radius of Single-Trial Decoder

- General decoding radius of the single-trial decoder by assuming the "worst" unreliability vector $\boldsymbol{\Delta}$ and choosing the "best" number of erasures τ, i.e.

$$\rho(\lambda) := \min_{\boldsymbol{\Delta}} \max_{\tau} e_\tau(\boldsymbol{\Delta}).$$

- Next step: Derive bounds on $\rho(\lambda)$!

Simplified Formula for the General Decoding Radius

- Transform *un*reliabilities $\boldsymbol{\Delta}$ into normalized reliabilities $\boldsymbol{h}$ by $h_j := (d^{\mathrm{i}} - 2\Delta_j)/d^{\mathrm{i}}$. It holds: $0 \leq h_1 \leq \cdots \leq h_{n^{\mathrm{o}}} \leq 1$.
- Decoding radius for fixed $\boldsymbol{h}$ and τ:

$$e_\tau(\boldsymbol{h}) := d^{\mathrm{i}} \left(\frac{1}{2} \sum_{j=1}^{n^{\mathrm{o}}} (1 - h_j) + \sum_{j=\tau+1}^{\tau+\varepsilon(\tau)} h_j \right).$$

- General decoding radius:

$$\rho(\lambda) = \min_{\boldsymbol{h}} \max_{\tau} e_\tau(\boldsymbol{h}).$$

- Observe that selection of τ does not depend on $h_{d^{\mathrm{o}}+1}, \ldots, h_{n^{\mathrm{o}}}$. Simplification:

$$\rho(\lambda) = d^{\mathrm{i}} \left(\frac{d^{\mathrm{o}}}{2} - \max_{\boldsymbol{h}} \min_{\tau} \left(\frac{1}{2} \sum_{j=1}^{d^{\mathrm{o}}} h_j - \sum_{j=\tau+1}^{\tau+\varepsilon(\tau)} h_j \right) \right)$$

Bounds for the Error Correcting Radius (1)

Theorem (Lower Bound)

$$\rho(\lambda) \;\geq\; \underline{\rho}(\lambda) := \frac{d^{\mathrm{i}}}{2}\left(\left\lfloor\frac{d^{\mathrm{o}}-1}{\lambda}\right\rfloor + \left\lfloor\frac{d^{\mathrm{o}}-\left\lfloor\frac{d^{\mathrm{o}}-1}{\lambda}\right\rfloor-2}{\lambda}\right\rfloor + 2\right)$$

Proof (Sketch): For any minimization we have

$$\min_{s\in\mathcal{S}} f(s) \leq \min_{s\in\mathcal{S}'\subseteq\mathcal{S}} f(s) \leq \frac{1}{|\mathcal{S}'|}\sum_{s\in\mathcal{S}'} f(s).$$

From this we get

$$\min_{\tau}\left(\frac{1}{2}\sum_{j=1}^{d^{\mathrm{o}}} h_j - \sum_{j=\tau+1}^{\tau+\varepsilon(\tau)} h_j\right) \leq \frac{1}{2}\sum_{j=\varepsilon(0)+\varepsilon\left(\varepsilon(0)\right)+1}^{d^{\mathrm{o}}} h_j.$$

Bounds for the Error Correcting Radius (2)

Maximizing this term over $\boldsymbol{h}$ by setting all involved h_j to 1 gives

$$\max_{\boldsymbol{h}} \left(\frac{1}{2} \sum_{j=\varepsilon(0)+\varepsilon\left(\varepsilon(0)\right)+1}^{d^{\mathrm{o}}} h_j \right) \leq \frac{1}{2}\left(d^{\mathrm{o}} - \varepsilon(0) - \varepsilon\left(\varepsilon(0)\right) \right).$$

□

Theorem (Upper Bound)

$$\rho(\lambda) \ \leq \ \overline{\rho}(\lambda) := \frac{d^{\mathrm{i}}}{\lambda} \left(d^{\mathrm{o}} - 1 - \frac{1}{2} \left\lfloor \frac{d^{\mathrm{o}} - 1}{\lambda} \right\rfloor \right)$$

Decoding Radius Deduced from the Bounds

- From the bounds we can deduce the decoding radius

$$e < \rho(\lambda) \approx \frac{d^{\mathrm{o}} d^{\mathrm{i}}}{2} \left(1 - \left(\frac{\lambda - 1}{\lambda}\right)^2\right).$$

- For $\lambda = 2$, i.e. outer BMD decoding, our results coincide with [Kovalev, 1986], i.e. $\rho(2) \approx \frac{3 d^{\mathrm{o}} d^{\mathrm{i}}}{8}$.
- In [Schmidt et al., 2006] a BD decoder with parameter $\lambda = \frac{\ell+1}{\ell}$ for Interleaved Reed–Solomon (IRS) codes[1] is presented, where ℓ is the number of interleaved codes.
- Expressed in terms of ℓ the decoding radius is

$$e < \rho(\ell) \approx \frac{d^{\mathrm{o}} d^{\mathrm{i}}}{2} \left(1 - \left(\frac{1}{(1+\ell)^2}\right)\right).$$

[1] IRS codes can be interpreted as punctured RS codes and vice versa [Sidorenko et al., 2008].

Conclusions/Outlook

- Derived single-trial adaptive algorithm for decoding concatenated codes.
- Provided tight bounds for its decoding radius.
- For outer BMD decoding ($\lambda = 2$), decoding radius coincides with [Kovalev, 1986], i.e. $e < \rho(2) \approx \frac{3d^{\mathrm{o}}d^{\mathrm{i}}}{8}$.
- For outer BD decoding, the decoding radius quickly approaches $\frac{d^{\mathrm{o}}d^{\mathrm{i}}}{2}$ for decreasing error/erasure tradeoff parameter λ.
- In special case of outer IRS codes, the radius approaches $\frac{d^{\mathrm{o}}d^{\mathrm{i}}}{2}$ quadratically with number ℓ of interleaved codes.
- Next step: Error exponent analysis, investigate influence of outer BD decoder's error probability.

Upper Bound for the Error Correcting Radius (1)

Theorem (Upper Bound)

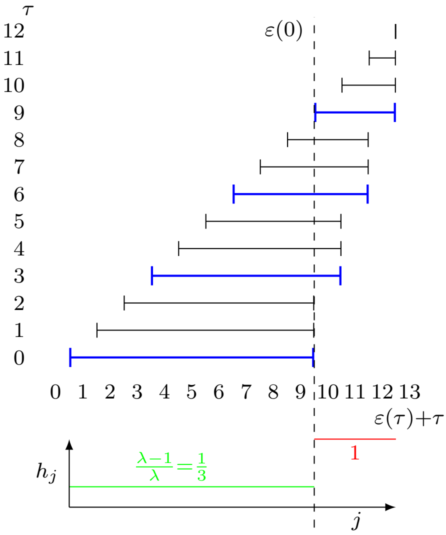
$$\rho(\lambda) \;\leq\; \overline{\rho}(\lambda) := \frac{d^{\mathrm{i}}}{\lambda}\left(d^{\mathrm{o}} - 1 - \frac{1}{2}\left\lfloor \frac{d^{\mathrm{o}}-1}{\lambda} \right\rfloor\right)$$

Proof (Sketch): Derive a lower bound on

$$\max_{\boldsymbol{h}} \min_{\tau} \left(\frac{1}{2}\sum_{j=1}^{d^{\mathrm{o}}} h_j - \sum_{j=\tau+1}^{\tau+\varepsilon(\tau)} h_j\right),$$

this means to maximize the second sum $\sum_{j=\tau+1}^{\tau+\varepsilon(\tau)} h_j$.

Upper Bound for the Error Correcting Radius (2)



Consider example on the left, $\lambda = 3/2,\ d^{\mathrm{o}} = 13,\ \varepsilon(0) = 9$.

Choose $\boldsymbol{h}$ s. t. $\sum_{j=\tau+1}^{\tau+\varepsilon(\tau)} h_j$ is constant for all decisive τ.

$$h_j = \begin{cases} \frac{\lambda-1}{\lambda} & j = 1, \ldots, \varepsilon(0) \\ 1 & j = \varepsilon(0)+1, \ldots, d^{\mathrm{o}} \end{cases}$$

Then: $\sum_{j=\tau+1}^{\tau+\varepsilon(\tau)} h_j = \varepsilon(0) - \frac{\varepsilon(0)}{\lambda}$.

Inserting proves the Theorem. $\square$

Tightness of the Bounds

Corollary (Conformity of the Bounds)

If

$$\lambda = \frac{\ell + 1}{\ell}, \ \ell \in \mathbb{N} \setminus \{0\}$$

and

$$d^{\mathrm{o}} = s(\ell + 1)^2 + \ell + 2, \ s \in \mathbb{N},$$

then

$$\underline{\rho}(\lambda) = \rho(\lambda) = \overline{\rho}(\lambda).$$

Bibliography

[Forney, 1966] Forney, G. D. (1966).
Concatenated Codes.
M.I.T. Press, Cambridge, MA, USA.

[Kötter, 1993] Kötter, R. (1993).
Fast generalized minimum-distance decoding of Algebraic–Geometry and Reed–Solomon codes.
IEEE Trans. Inform. Theory, IT-42(3):721–737.

[Kovalev, 1986] Kovalev, S. I. (1986).
Two classes of minimum generalized distance decoding algorithms.
Problems of Information Transmission, 22(3):186–192.
Translated from Russian, original in Problemy Peredachi Informatsii, pp. 35–42.

[Schmidt et al., 2006] Schmidt, G., Sidorenko, V. R., and Bossert, M. (2006).
Collaborative decoding of interleaved Reed–Solomon codes and concatenated code designs.
Preprint, available online at ArXiv, `arXiv:cs.IT/0610074`.

[Sidorenko et al., 2008] Sidorenko, V. R., Schmidt, G., and Bossert, M. (2008).
Decoding punctured Reed–Solomon codes up to the Singleton Bound.
In *Proc. International ITG Conference on Source and Channel Coding*, Ulm, Germany.

[Sorger, 1993] Sorger, U. K. (1993).
A new Reed–Solomon code decoding algorithm based on Newton's interpolation.
IEEE Trans. Inform. Theory, IT-39(2):358–365.

[Weber and Abdel-Ghaffar, 2003] Weber, J. H. and Abdel-Ghaffar, K. A. S. (2003).
Reduced GMD decoding.
IEEE Trans. Inform. Theory, IT-49(4):1013–1027.

[Zyablov, 1973] Zyablov, V. V. (1973).
Optimization of concatenated decoding algorithms.
Problems of Information Transmission, 9(1):19–24.
Translated from Russian, original in Problemy Peredachi Informatsii, pp. 26–32.