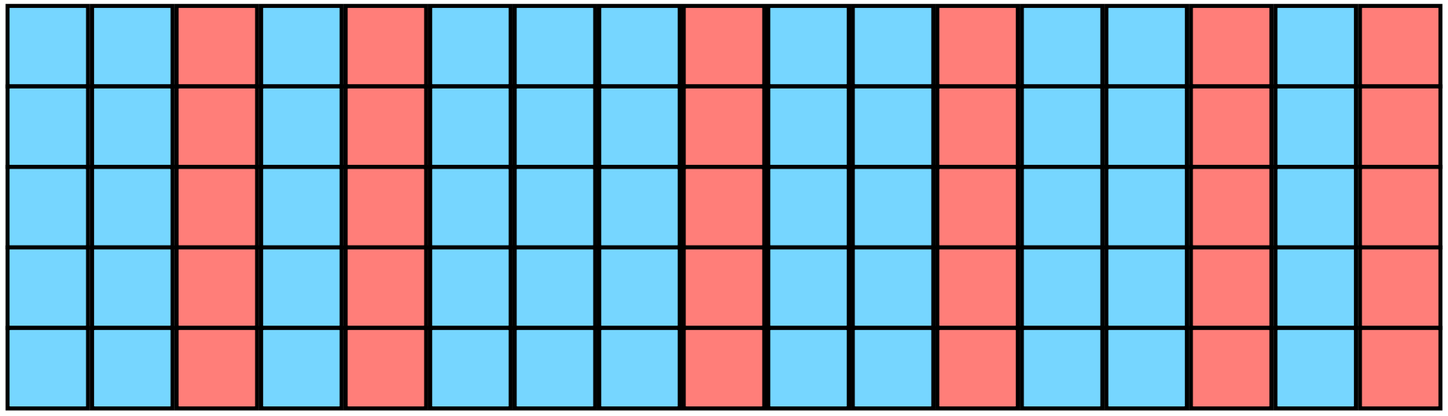
(Improved) Decoding of Interleaved RS- and AG-Codes



Amin Shokrollahi

Joint work with A. Brown and L. Minder

EPFL

Diamantina, August 2006

RS-Codes

$x_1, \ldots, x_n \in \mathbb{F}_q$ pairwise distinct

$\mathbb{F}_q[x]_{<k}$ space of polynomials of degree $<k, k \leq n$

$$\begin{array}{rcl} \varphi\colon \mathbb{F}_q[x]_{<k} & \longrightarrow & \mathbb{F}_q^n \\ f & \longmapsto & (f(x_1), \ldots, f(x_n)) \end{array}$$

$\mathrm{Im}(\varphi)$ is called a RS-code $\mathcal{C}$

A nonzero polynomial of degree $<k$ over a field has at most k-1 roots over the field.

$$\ker(\varphi) = \{f \mid f(x_1) = \cdots = f(x_n) = 0\} = 0.$$

$$0 \neq f \in \mathbb{F}_q[x]_{<k} \Rightarrow \#\{i \mid f(x_i) = 0\} < k \Rightarrow \text{Minimum distance of } \mathcal{C} \geq n-k+1.$$

RS-Codes

$x_1, \ldots, x_n \in \mathbb{F}_q$ pairwise distinct

$\mathbb{F}_q[x]_{<k}$ space of polynomials of degree $<k, k \leq n$

$$\begin{array}{rcl} \varphi\colon \mathbb{F}_q[x]_{<k} & \longrightarrow & \mathbb{F}_q^n \\ f & \longmapsto & (f(x_1), \ldots, f(x_n)) \end{array}$$

$\mathrm{Im}(\varphi)$ is called a RS-code $\mathcal{C}$

A nonzero polynomial of degree $<k$ over a field has at most k-1 roots over the field.

$$\ker(\varphi) = \{f \mid f(x_1) = \cdots = f(x_n) = 0\} = 0.$$

$$0 \neq f \in \mathbb{F}_q[x]_{<k} \Rightarrow \#\{i \mid f(x_i) = 0\} < k \Rightarrow \text{Minimum distance of } \mathcal{C} \geq n-k+1.$$

RS-Codes

$x_1, \ldots, x_n \in \mathbb{F}_q$ pairwise distinct

$\mathbb{F}_q[x]_{<k}$ space of polynomials of degree $<k, k \leq n$

$$\begin{array}{rcl} \varphi\colon \mathbb{F}_q[x]_{<k} & \longrightarrow & \mathbb{F}_q^n \\ f & \longmapsto & (f(x_1), \ldots, f(x_n)) \end{array}$$

$\mathrm{Im}(\varphi)$ is called a RS-code $\mathcal{C}$

A nonzero polynomial of degree $<k$ over a field has at most k-1 roots over the field.

$$\ker(\varphi) = \{f \mid f(x_1) = \cdots = f(x_n) = 0\} = 0.$$

$$0 \neq f \in \mathbb{F}_q[x]_{<k} \Rightarrow \#\{i \mid f(x_i) = 0\} < k \Rightarrow \text{Minimum distance of } \mathcal{C} \geq n-k+1.$$

RS-Codes

$x_1, \ldots, x_n \in \mathbb{F}_q$ pairwise distinct

$\mathbb{F}_q[x]_{<k}$ space of polynomials of degree $<k, k \leq n$

$$\begin{array}{rcl} \varphi\colon \mathbb{F}_q[x]_{<k} & \longrightarrow & \mathbb{F}_q^n \\ f & \longmapsto & (f(x_1), \ldots, f(x_n)) \end{array}$$

$\mathrm{Im}(\varphi)$ is called a RS-code $\mathcal{C}$

A nonzero polynomial of degree $<k$ over a field has at most k-1 roots over the field.

$$\mathcal{C} \text{ is } [n, k, n-k+1]_q - \text{code}$$

Decoding Problem

$$(\quad f(x_1) \quad , \ldots , \quad f(x_n) \quad)$$

Diamantina, August 2006

Decoding Problem

$$\begin{pmatrix} f(x_1) & , \ldots , & f(x_n) \end{pmatrix}$$

Transmission

$$\begin{pmatrix} y_1 & , \ldots , & y_n \end{pmatrix}$$

Diamantina, August 2006

Decoding Problem

$$\underset{\text{Known}}{(\quad y_1 \quad ,\ldots,\quad y_n \quad)} \xleftarrow{\text{Transmission}} \underset{\text{Unknown}}{(\quad f(x_1) \quad ,\ldots,\quad f(x_n) \quad)}$$

Diamantina, August 2006

Decoding Problem

$$\underset{\text{Known}}{(\quad y_1 \quad ,\ldots,\quad y_n \quad)} \xleftarrow{\text{Transmission}} \underset{\text{Unknown}}{(\quad f(x_1) \quad ,\ldots,\quad f(x_n) \quad)}$$

Error positions $E := \{i \mid y_i \neq f(x_i)\}$

Unique Decoding Problem

$$\underset{\text{Known}}{(\quad y_1 \quad ,\ldots,\quad y_n \quad)} \xleftarrow{\text{Transmission}} \underset{\text{Unknown}}{(\quad f(x_1) \quad ,\ldots,\quad f(x_n) \quad)}$$

Error positions $E := \{i \mid y_i \neq f(x_i)\}$

Promise: $\#E =: e \leq t$ for some t.

Decoding Problem

$$\underbrace{(\quad f(x_1) \quad ,\ldots, \quad f(x_n) \quad)}_{\text{Unknown}}$$

Transmission

$$\underbrace{(\quad y_1 \quad ,\ldots, \quad y_n \quad)}_{\text{Known}}$$

Error positions $E := \{i \mid y_i \neq f(x_i)\}$

Promise: $\#E =: e \leq t$ for some t.

Decoding problem: find f.

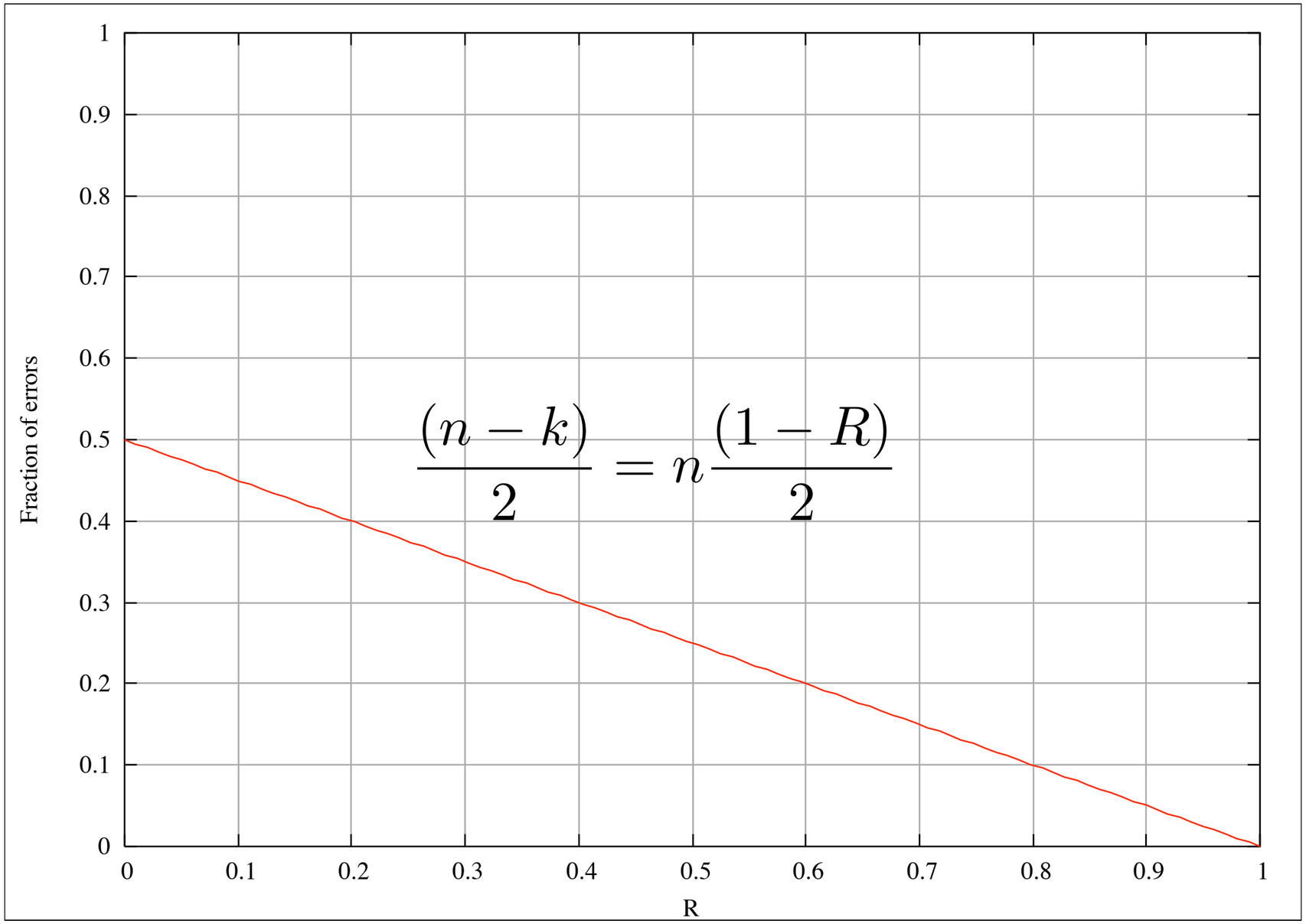
How Many Errors Can We Correct?

Berlekamp, Welch-Berlekamp: $\frac{t}{n} = \frac{1-R}{2}$

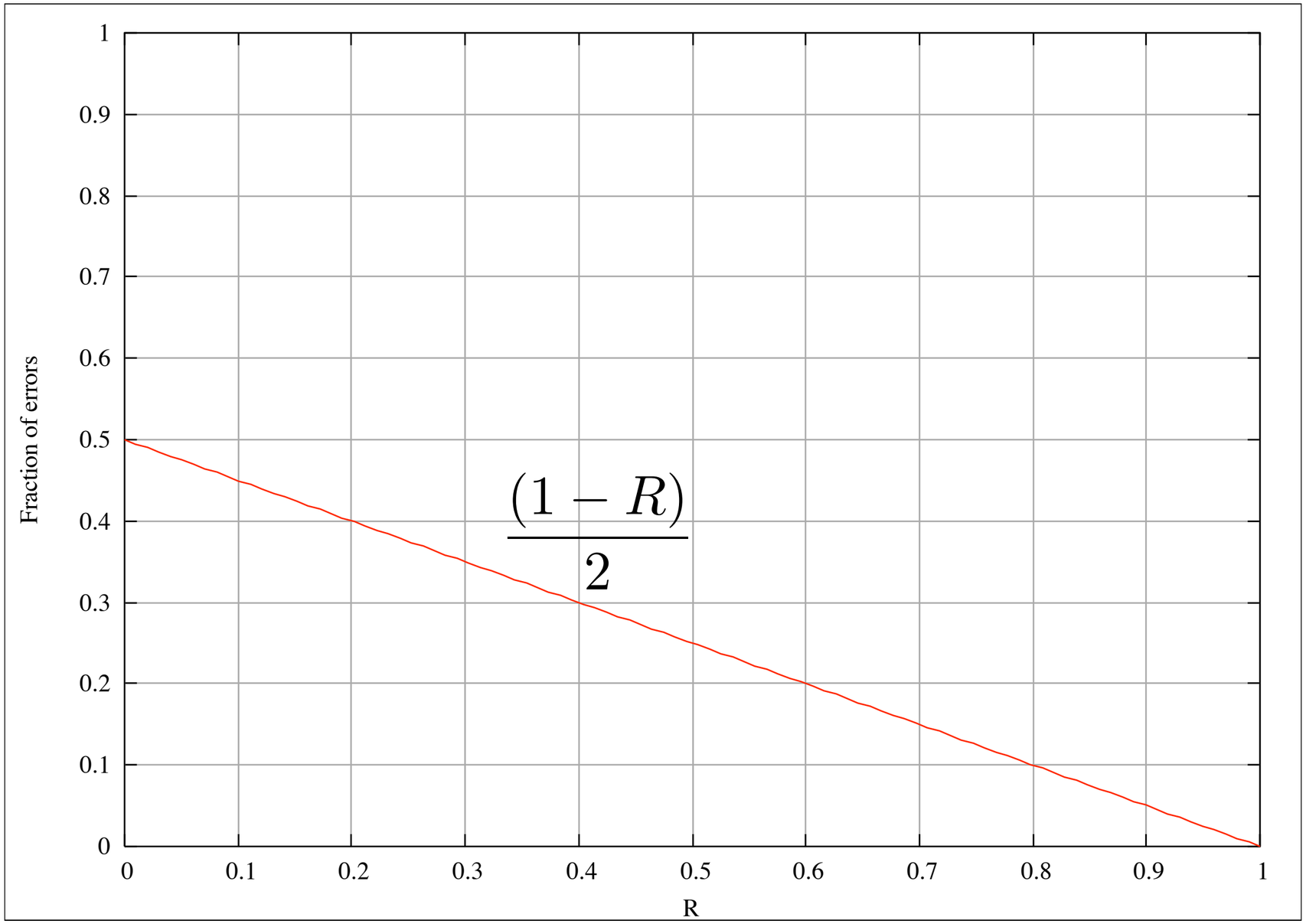
Sudan, Guruswami-Sudan (list-decoding): $\frac{t}{n} = 1 - \sqrt{R}$

What is the ultimate bound? $\frac{t}{n} = 1 - R$

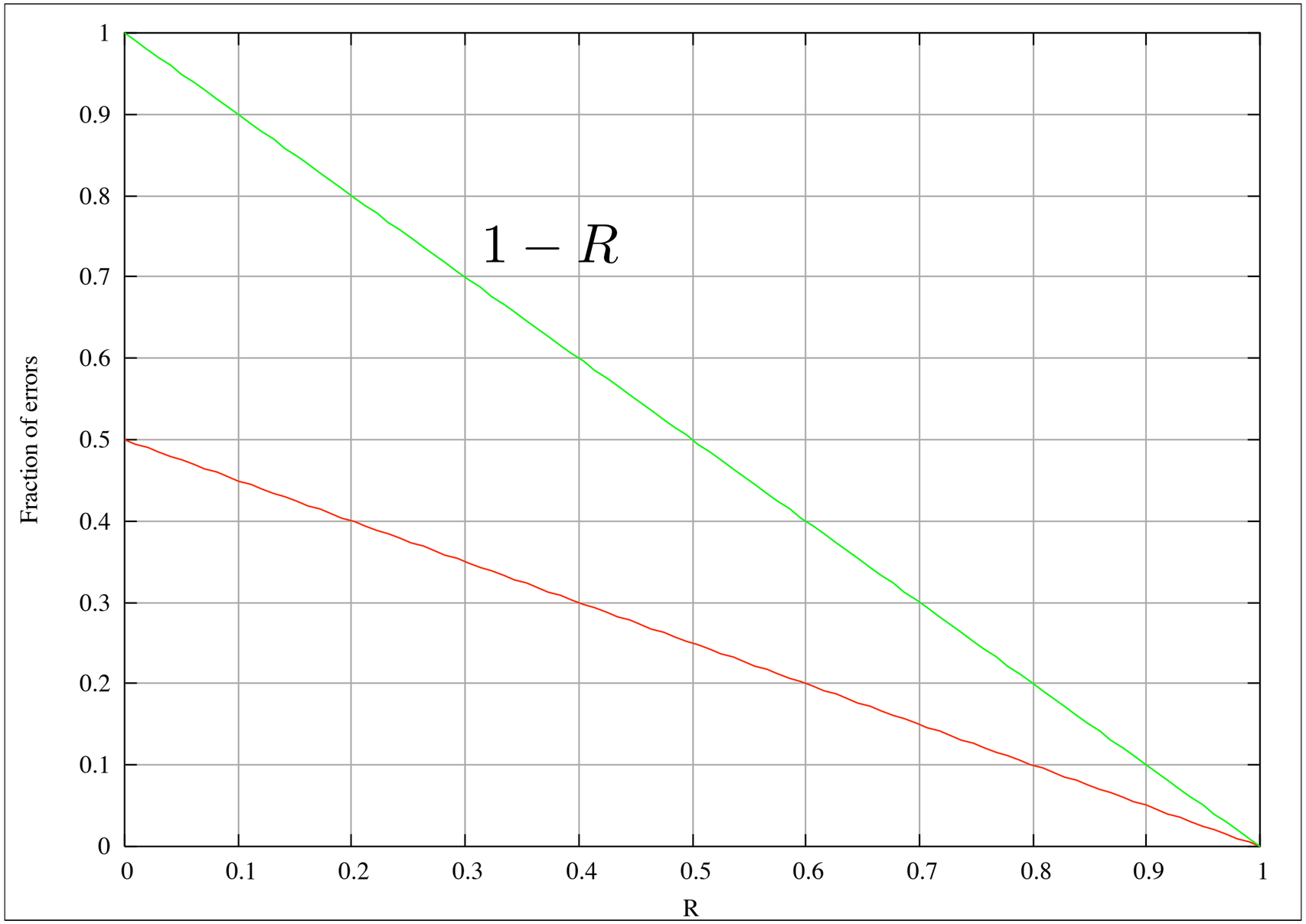
Decoding Errors



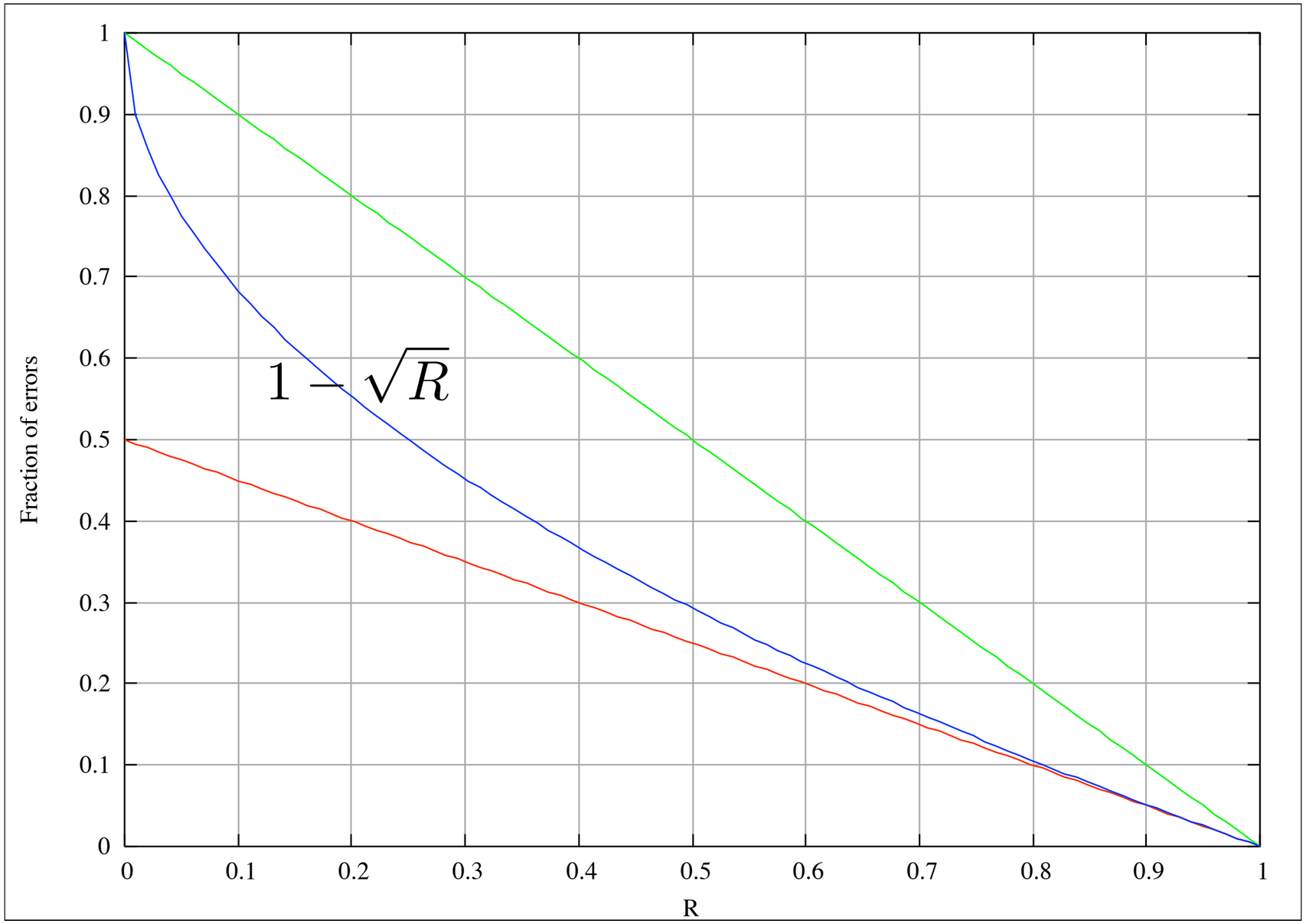
Decoding Errors



Decoding Errors



Decoding Errors



Decoding More Errors?

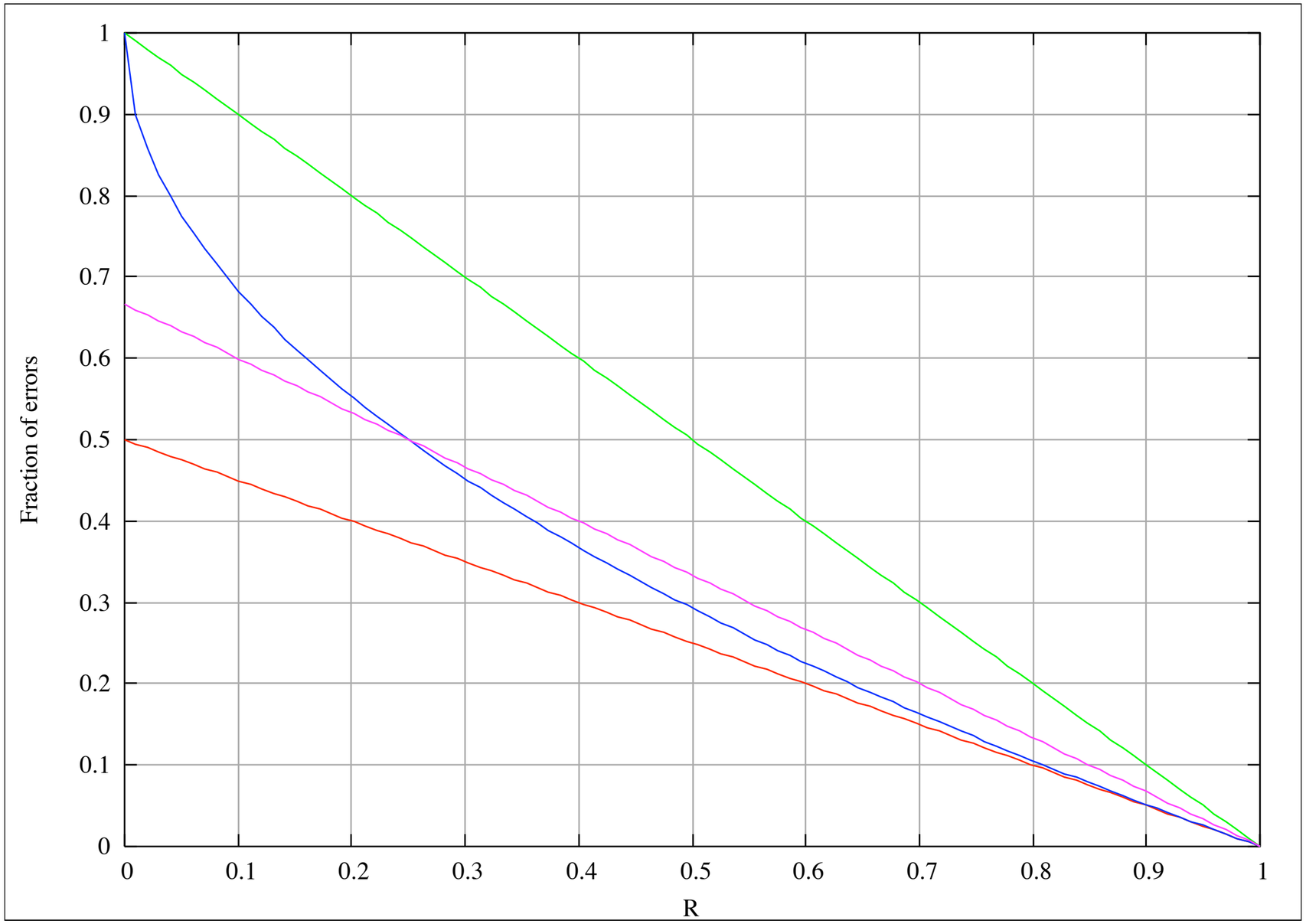
We will introduce probabilistic algorithms parameterized by a parameter m.

Algorithms will be able to correct (roughly) up to

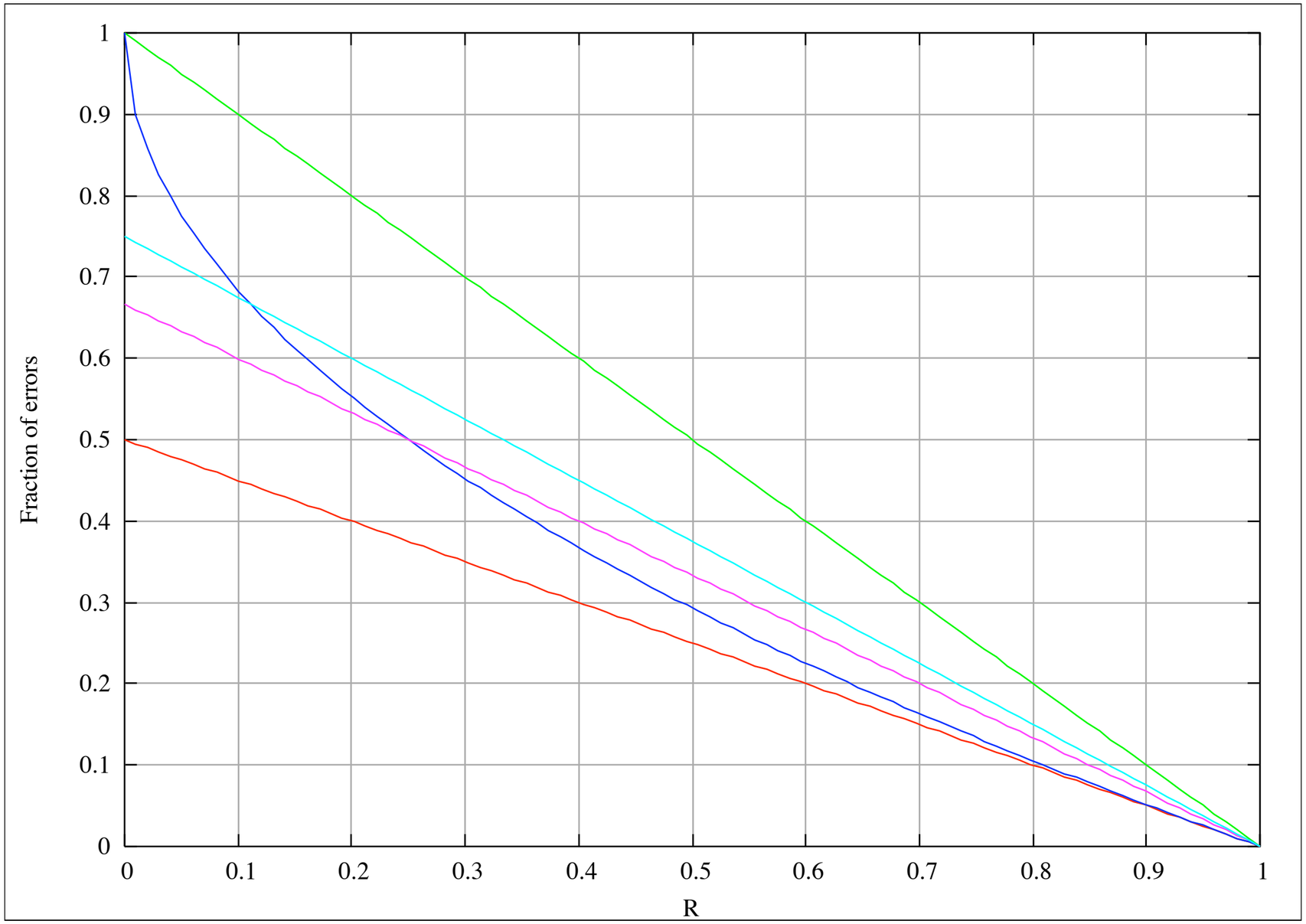
$$\frac{t}{n} = \frac{m}{m+1}(1-R)$$

The probabilistic model and main parts of the algorithm are due to Bleichenbacher, Kiyaias, and Yung (BKY).

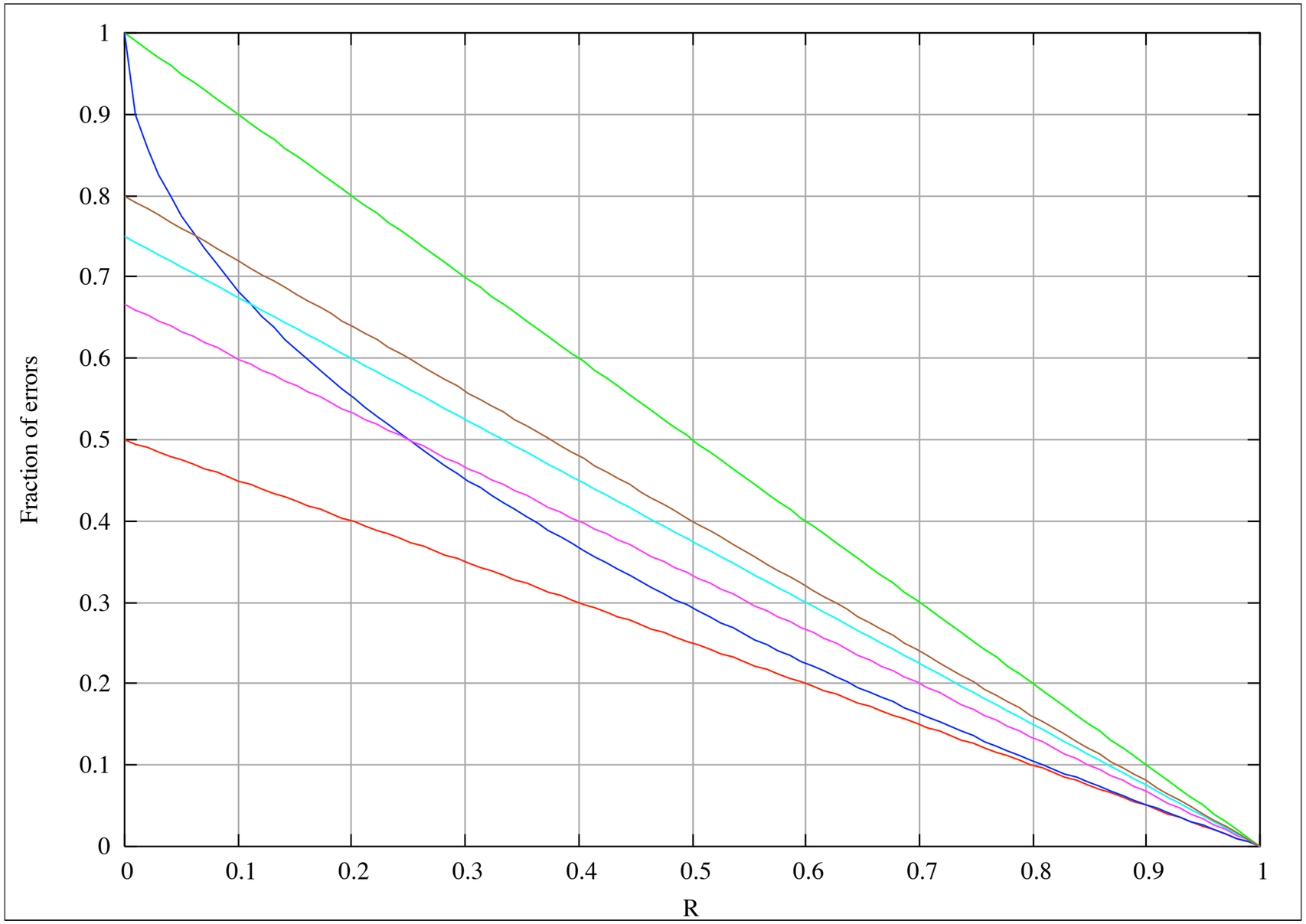
Decoding More Errors?



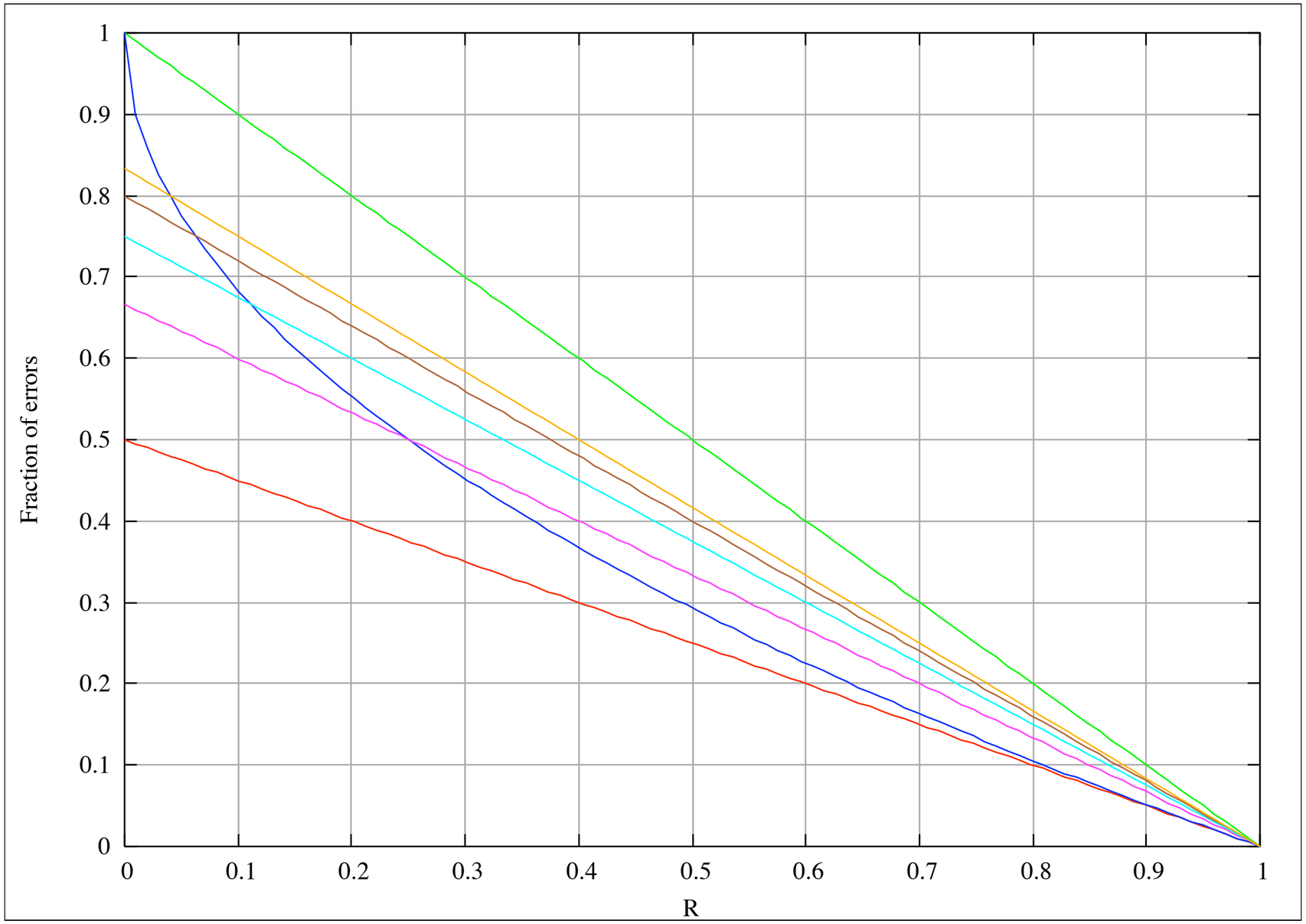
Decoding More Errors?



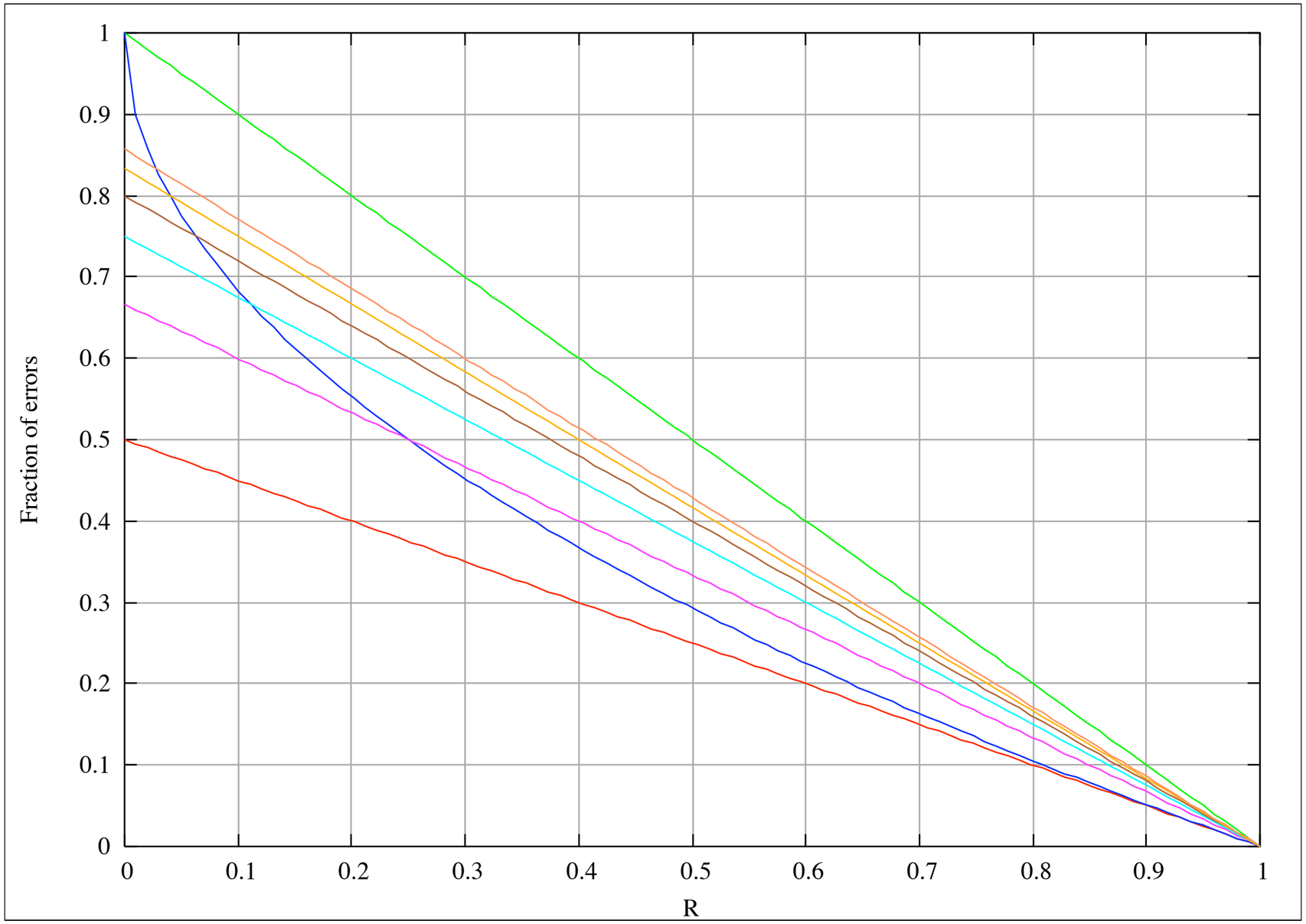
Decoding More Errors?



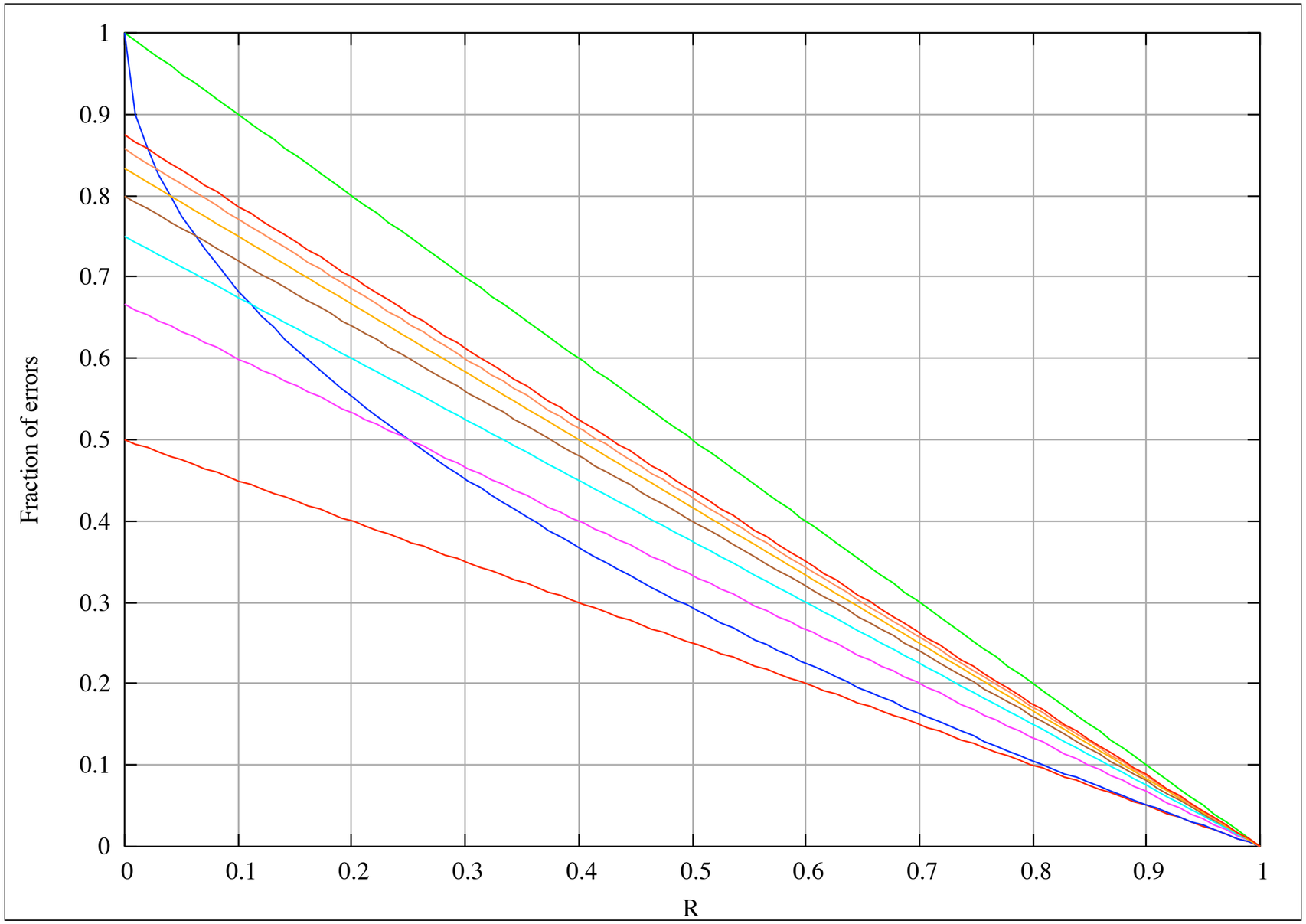
Decoding More Errors?



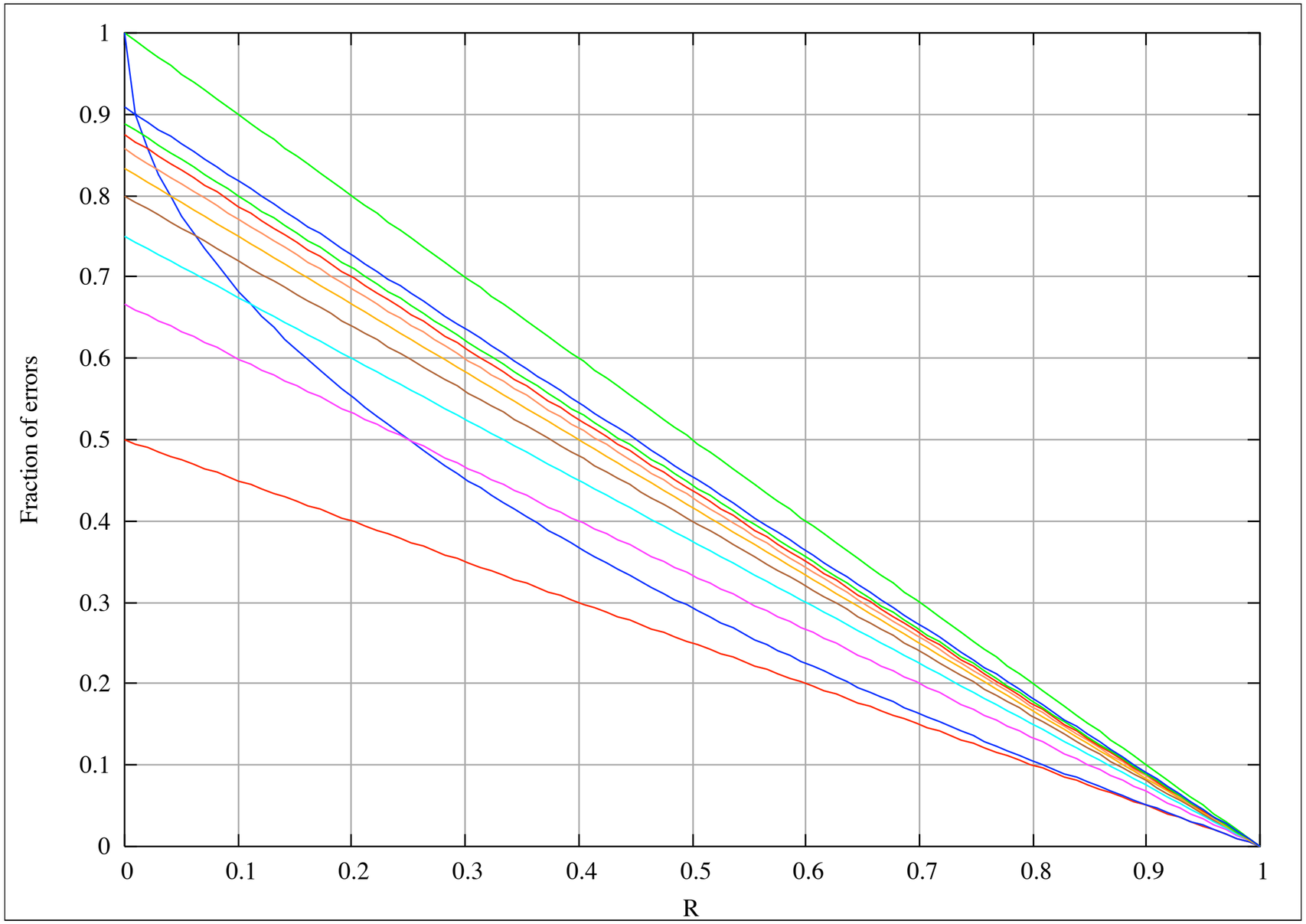
Decoding More Errors?



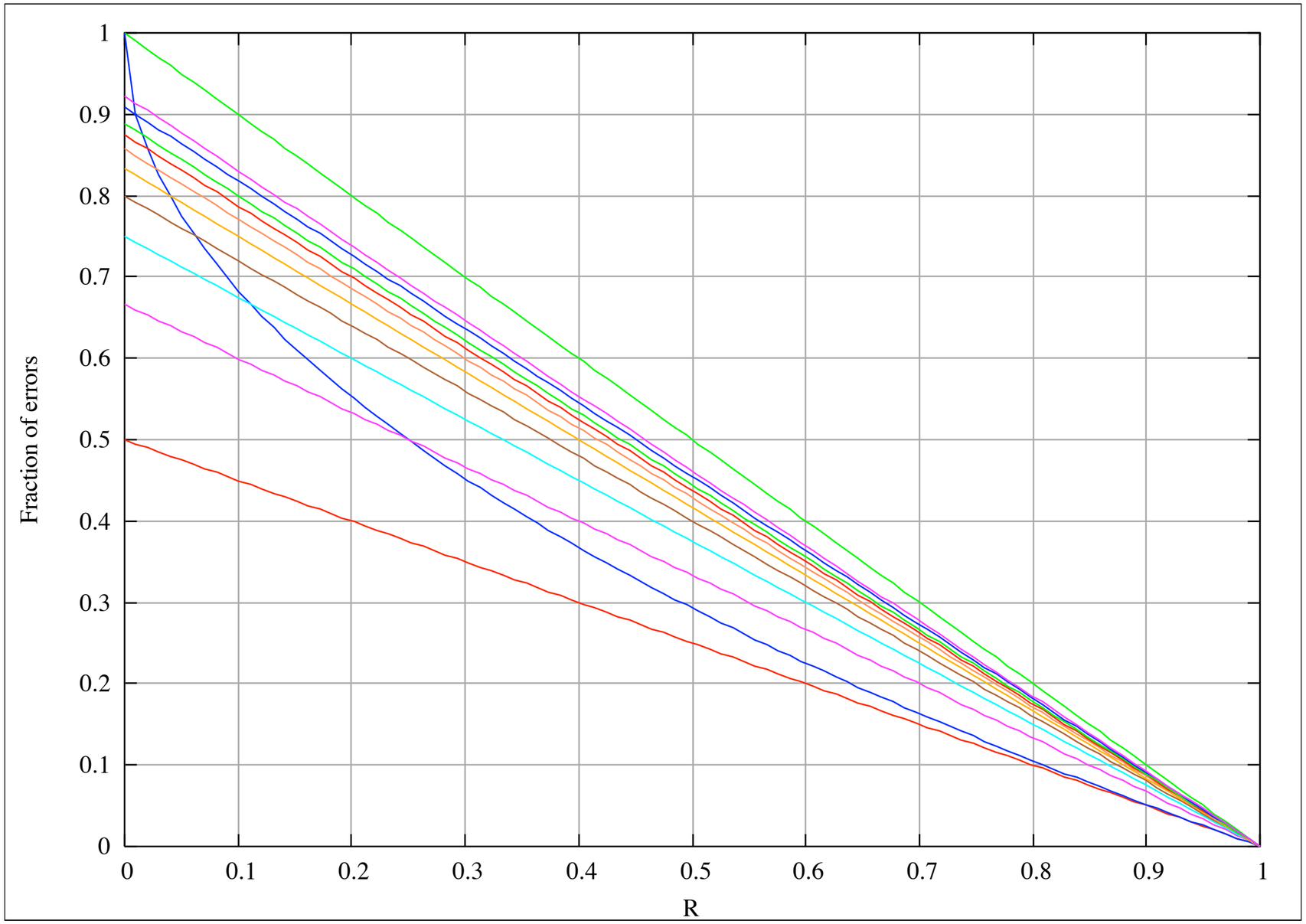
Decoding More Errors?



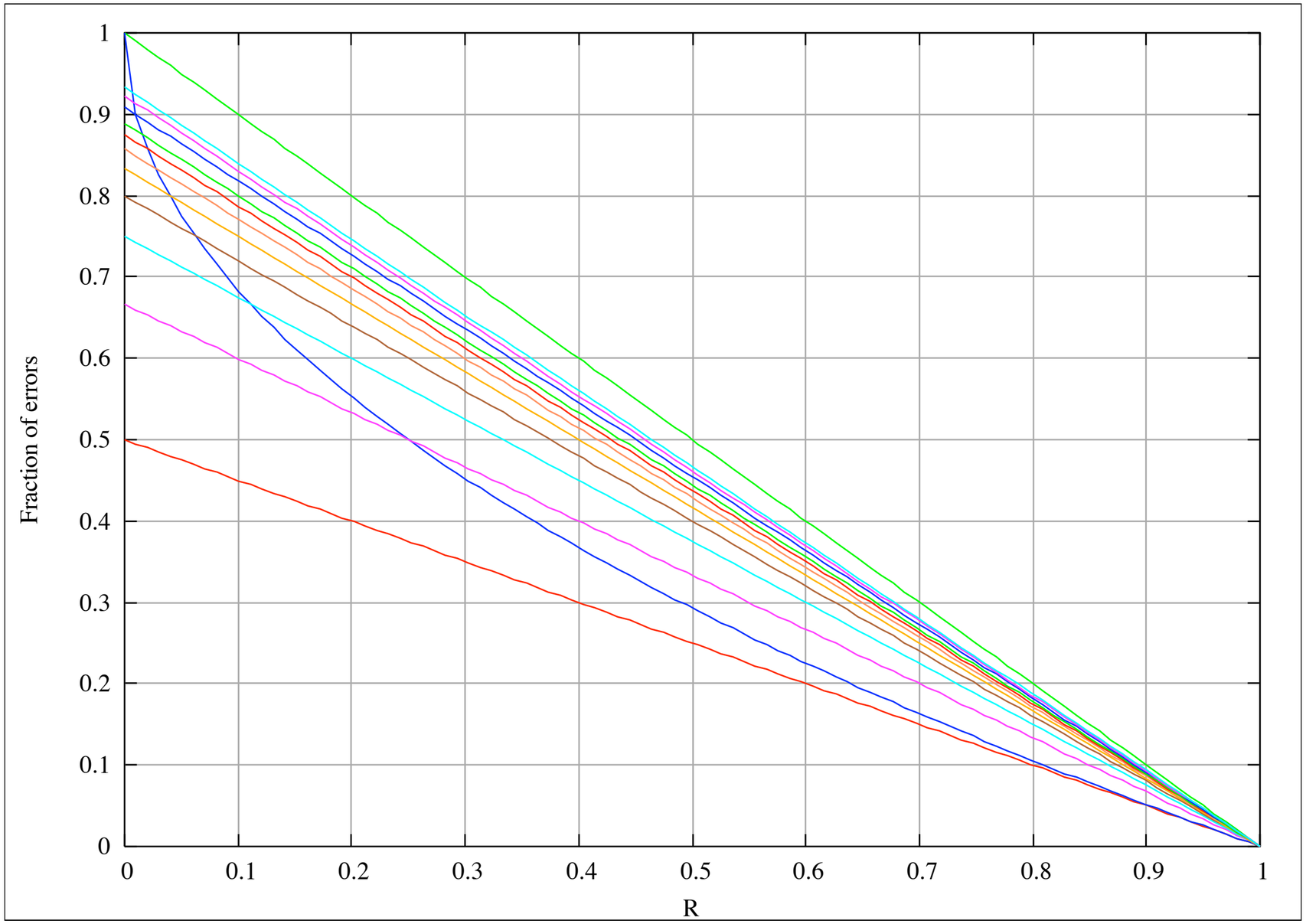
Decoding More Errors?



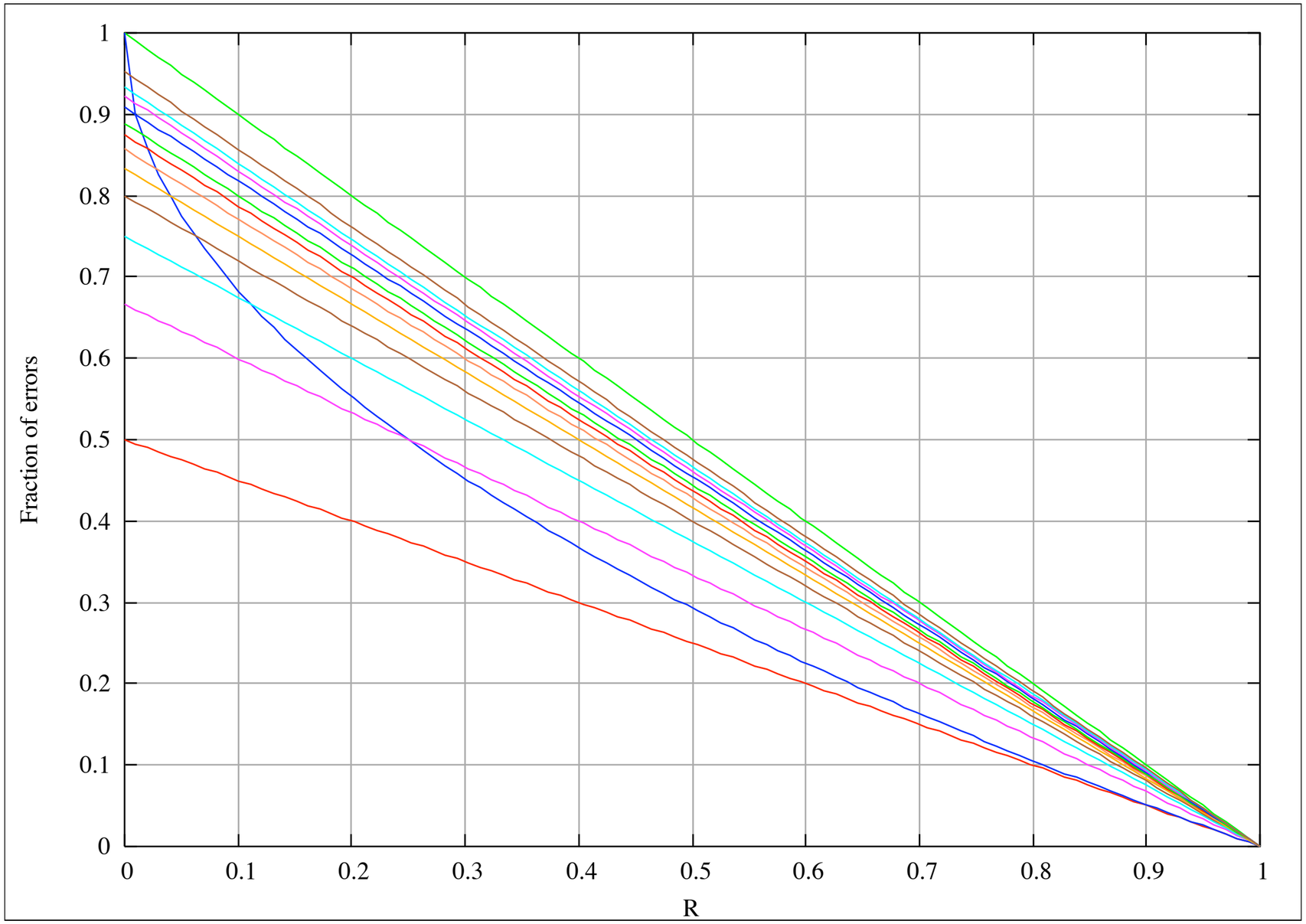
Decoding More Errors?



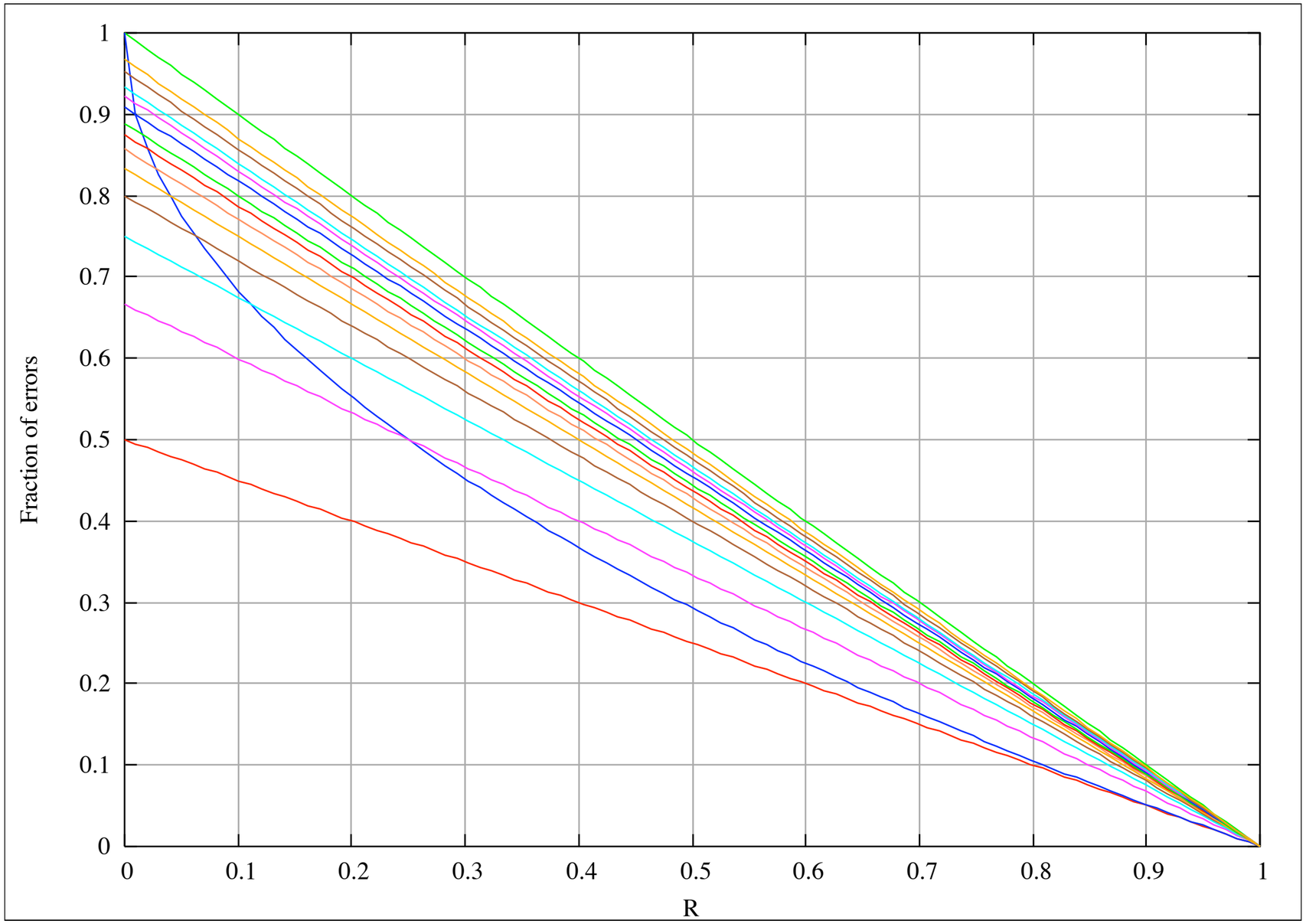
Decoding More Errors?



Decoding More Errors?



Decoding More Errors?



RS-Codes over Large Alphabets

$x_1, \ldots, x_n \in \mathbb{F}_q$ pairwise distinct, $m \geq 1$

$$\begin{array}{rcl} \varphi_m \colon \mathbb{F}_{q^m}[x]_{<k} & \longrightarrow & \mathbb{F}_{q^m}^n \\ f & \longmapsto & (f(x_1), \ldots, f(x_n)) \end{array}$$

Diamantina, August 2006

RS-Codes over Large Alphabets

$x_1, \ldots, x_n \in \mathbb{F}_q$ pairwise distinct, $m \geq 1$

$$\begin{array}{rcl} \varphi_m : \mathbb{F}_{q^m}[x]_{<k} & \longrightarrow & \mathbb{F}_{q^m}^n \\ f & \longmapsto & (f(x_1), \ldots, f(x_n)) \end{array}$$

$$\mathbb{F}_{q^m}[x]_{<k} \simeq \left(\mathbb{F}_q[x]_{<k}\right)^m$$

$$\mathbb{F}_{q^m}[x]_{<k} \ni f \leftrightarrow (f_1, \ldots, f_m) \in \left(\mathbb{F}_q[x]_{<k}\right)^m$$

RS-Codes over Large Alphabets

$x_1, \ldots, x_n \in \mathbb{F}_q$ pairwise distinct, $m \geq 1$

$$\begin{array}{rcl} \varphi_m \colon \mathbb{F}_{q^m}[x]_{<k} & \longrightarrow & \mathbb{F}_{q^m}^n \\ f & \longmapsto & (f(x_1), \ldots, f(x_n)) \end{array}$$

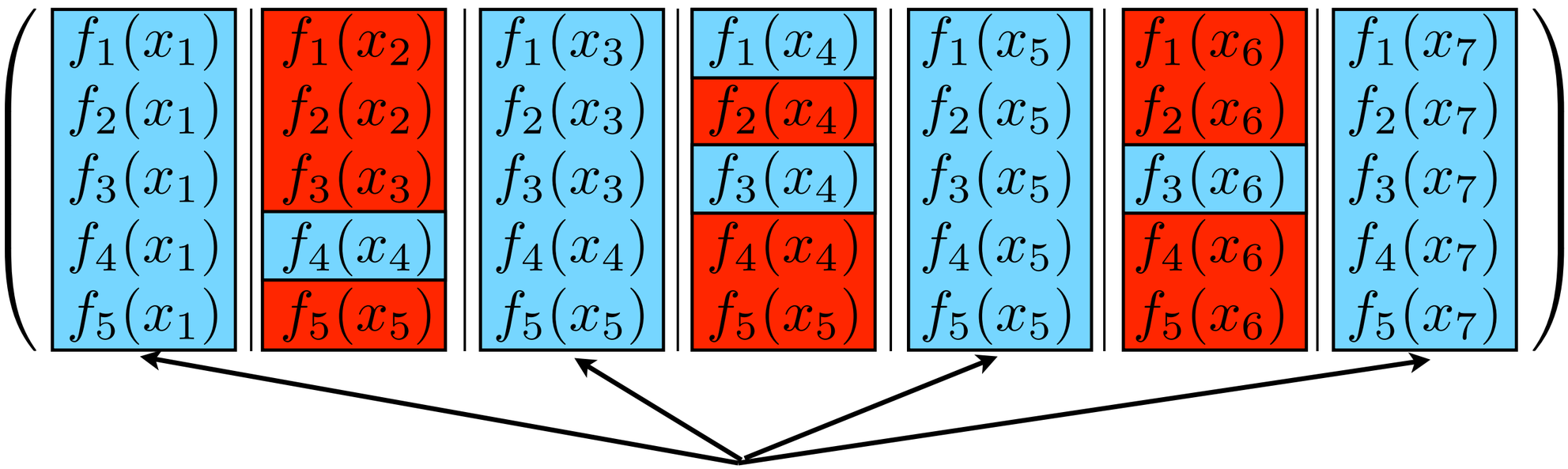
$$\mathbb{F}_{q^m}[x]_{<k} \simeq \left(\mathbb{F}_q[x]_{<k}\right)^m$$

$$\mathbb{F}_{q^m}[x]_{<k} \ni f \leftrightarrow (f_1, \ldots, f_m) \in \left(\mathbb{F}_q[x]_{<k}\right)^m$$

$$\left(\begin{array}{c|c|c|c} f_1(x_1) & f_1(x_2) & \cdots & f_1(x_n) \\ f_2(x_1) & f_2(x_2) & \cdots & f_2(x_n) \\ \vdots & \vdots & \ddots & \vdots \\ f_m(x_1) & f_m(x_2) & \cdots & f_m(x_n) \end{array}\right)$$

Interleaved codeword

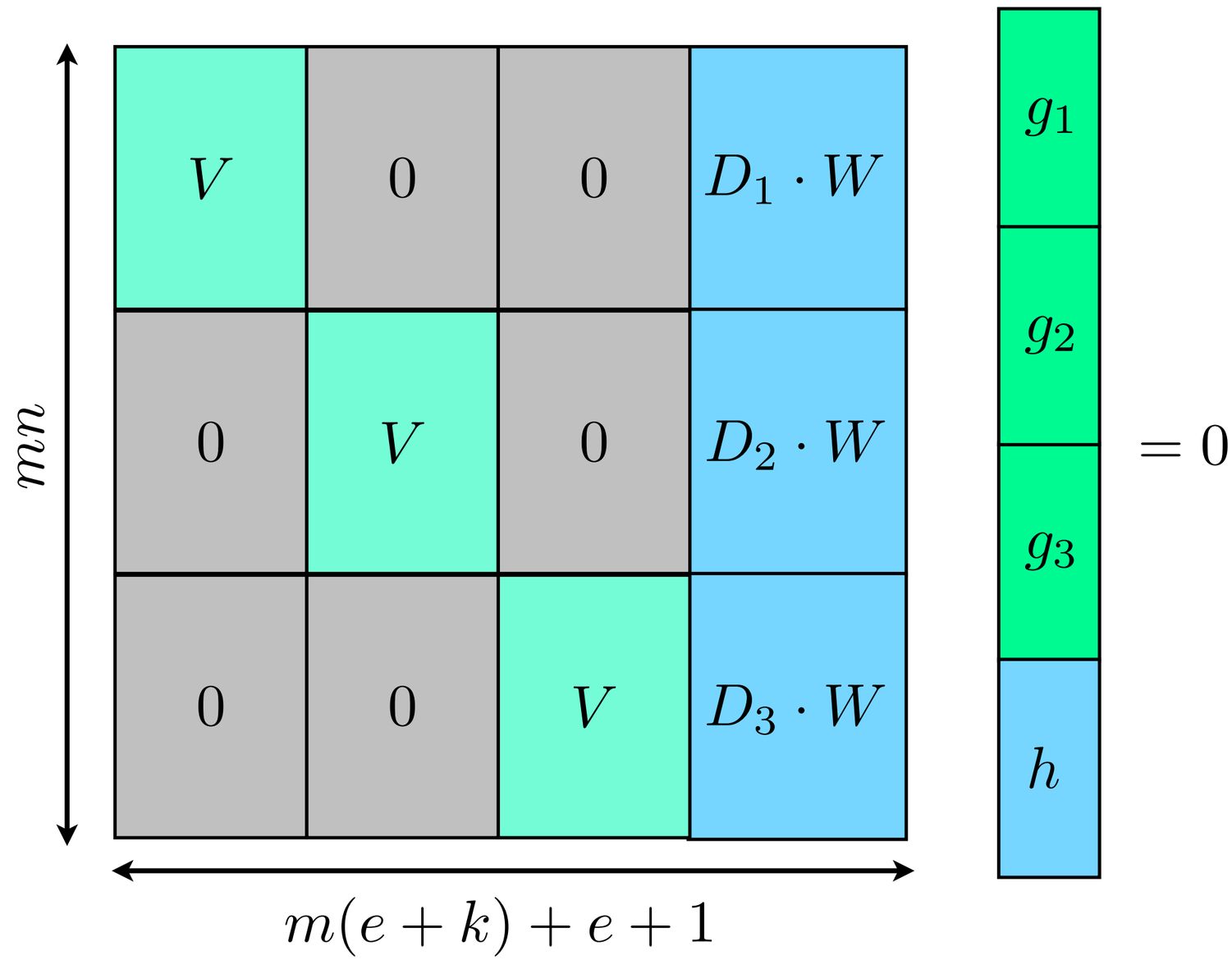
RS-Codes over Large Alphabets



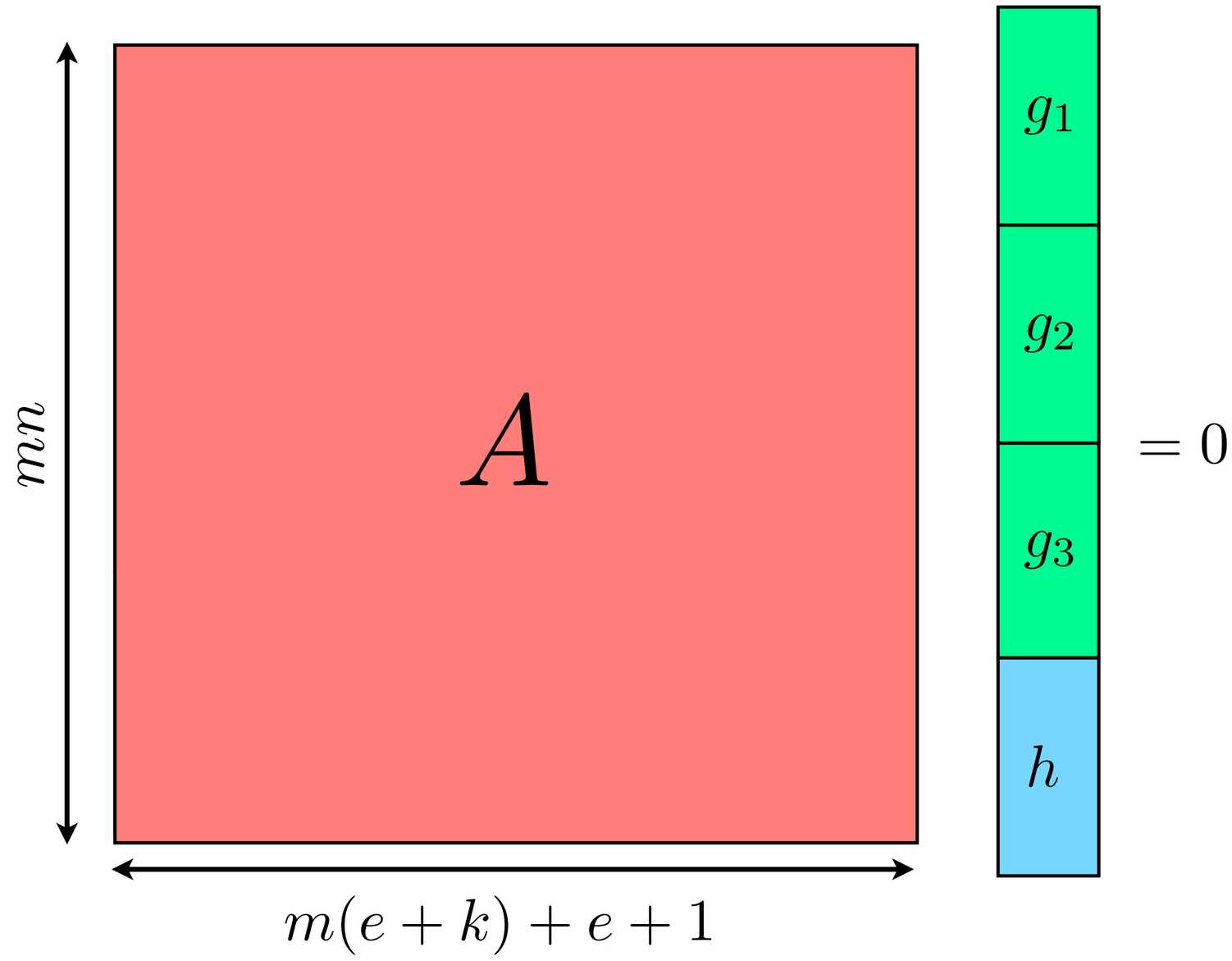
Non-error positions are the same for all the polynomials, so same error locator

$$
\begin{aligned}
g_1(x_i) - y_{i,1}h(x_i) &= 0 \\
g_2(x_i) - y_{i,2}h(x_i) &= 0 \\
g_3(x_i) - y_{i,3}h(x_i) &= 0 \\
g_4(x_i) - y_{i,4}h(x_i) &= 0 \\
g_5(x_i) - y_{i,5}h(x_i) &= 0
\end{aligned}
$$

RS-Codes over Large Alphabets



RS-Codes over Large Alphabets

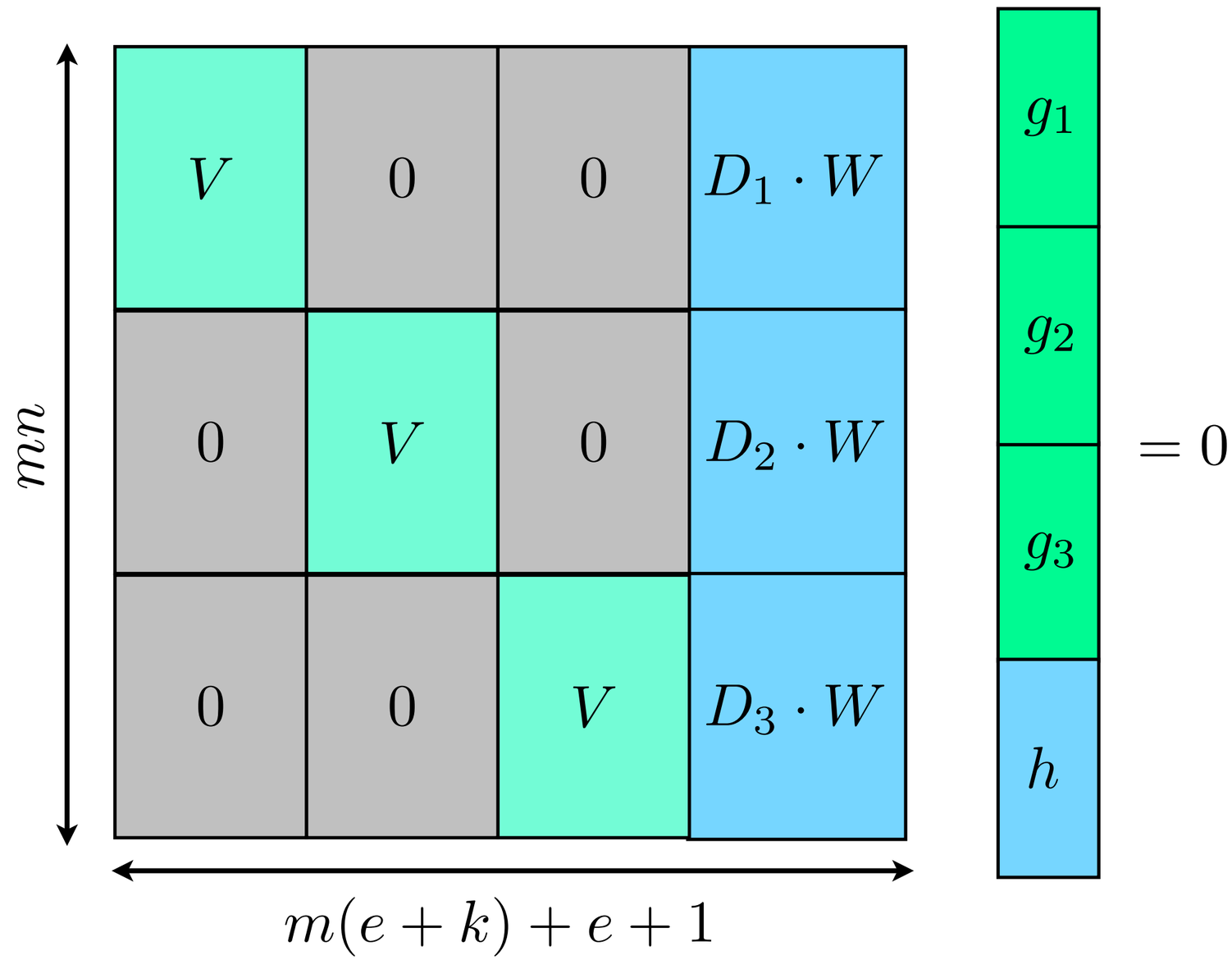


Algorithm

$$A \cdot \begin{pmatrix} g_1 \\ g_2 \\ g_3 \\ h \end{pmatrix} = 0$$

1. Find element $(g_1|g_2|g_3|h)^\top$ in the right kernel of A.
2. If $g_i/h \notin \mathbb{F}_q[x]_{<k}$ for some i, return error.
3. If not, then set $f_i = g_i/h$.

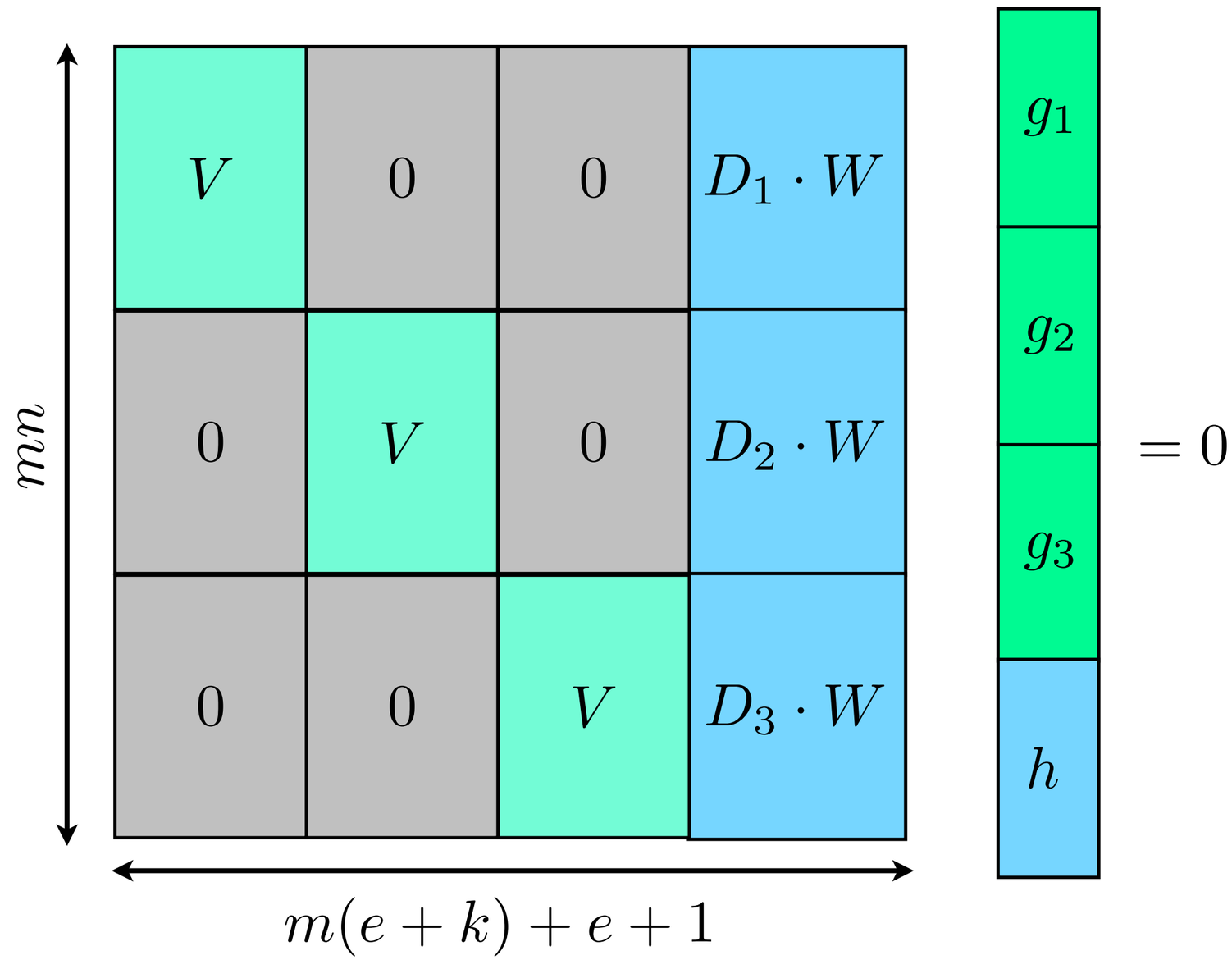
RS-Codes over Large Alphabets



Right kernel is one-dimensional $\Rightarrow$

$$m(e+k)+e+1 = n+1 \Rightarrow \boxed{e = \frac{m}{m+1}(n-k)}$$

Problem



Uniqueness is not guaranteed!

BKY Model

1. Choose $e \leq \frac{m}{m+1}(n-k)$ positions.
2. For each of these positions at least one of the components is in error.
3. The error value is uniformly distributed in $\mathbb{F}_q$.

$$\left(\begin{array}{c|c|c|c|c|c|c} f_1(x_1) & f_1(x_2) & f_1(x_3) & f_1(x_4) & f_1(x_5) & f_1(x_6) & f_1(x_7) \\ f_2(x_1) & f_2(x_2) & f_2(x_3) & f_2(x_4) & f_2(x_5) & f_2(x_6) & f_2(x_7) \\ f_3(x_1) & f_3(x_3) & f_3(x_3) & f_3(x_4) & f_3(x_5) & f_3(x_6) & f_3(x_7) \\ f_4(x_1) & f_4(x_4) & f_4(x_4) & f_4(x_4) & f_4(x_5) & f_4(x_6) & f_4(x_7) \\ f_5(x_1) & f_5(x_5) & f_5(x_5) & f_5(x_5) & f_5(x_5) & f_5(x_6) & f_5(x_7) \end{array}\right)$$

What is the probability of decoding error?

BKY Model

Bleichenbacher et al.: If $e = \frac{m}{m+1}(n-k)$, then the probability of decoding error is $O(n/q)$.

Brown et al.: If $e = \frac{m}{m+1}(n-k)$, then the probability of decoding error is $O(1/q)$.

This talk: Roughly, if $e = \frac{m}{m+1}(n-k) - \epsilon n$, then the error probability of the decoder is $O(q^{-m\epsilon n})$.

BKY Model

Suppose that

$$e \leq \frac{\beta m}{\beta m + 1}(n-k) - \frac{c}{\beta m + 1},$$

for some $c > 0$, and where $\beta = \frac{\ln(q^m - 1)}{\ln(q^m)}$. Then we have:

(1) If $e + t < n - k$, then the error probability of the decoder is zero.

(2) In general the error probability of the decoder is at most $\frac{q}{q-1} \cdot q^{-c}$.

BKY Model

Suppose that

$$e \leq \frac{\beta m}{\beta m + 1}(n-k) - \frac{c}{\beta m + 1},$$

for some $c > 0$, and where $\beta = \frac{\ln(q^m - 1)}{\ln(q^m)}$. Then we have:

(1) If $e + t < n - k$, then the error probability of the decoder is zero.

(2) In general the error probability of the decoder is at most $\frac{q}{q-1} \cdot q^{-c}$.

$$\beta \simeq 1$$

BKY Model

Suppose that

$$e \leq \frac{\beta m}{\beta m + 1}(n-k) - \frac{c}{\beta m + 1},$$

for some $c > 0$, and where $\beta = \frac{\ln(q^m - 1)}{\ln(q^m)}$. Then we have:

(1) If $e + t < n - k$, then the error probability of the decoder is zero.

(2) In general the error probability of the decoder is at most $\frac{q}{q-1} \cdot q^{-c}$.

$$\beta \simeq 1$$

$$\text{Roughly: } e \leq \frac{m}{m+1}(n-k) - \epsilon n \Rightarrow \text{Error probability } \simeq q^{-m\epsilon n}$$

Method of Proof

$$A \cdot \begin{pmatrix} g_1 \\ g_2 \\ g_3 \\ h \end{pmatrix} = 0$$

1. Find element $(g_1|g_2|g_3|h)^\top$ in the right kernel of A.
2. If $g_i/h \notin \mathbb{F}_q[x]_{<k}$ for some i, return error.
3. If not, then set $f_i = g_i/h$.

Method of Proof

$$A \cdot \begin{pmatrix} g_1 \\ g_2 \\ g_3 \\ h \end{pmatrix} = 0$$

Need to show that right kernel of A is one-dimensional, w.h.p.

Calculate expectation of size of right kernel, and apply Markov.

Complexity

$$A \cdot \begin{pmatrix} g_1 \\ g_2 \\ g_3 \\ h \end{pmatrix} = 0$$

$$O((mn)^3 \log^2(q))$$

Complexity

$$A \cdot \begin{pmatrix} g_1 \\ g_2 \\ g_3 \\ h \end{pmatrix} = 0$$

$$O((mn)^3 \log^2(q))$$

$$O((mn)^2 \log^2(q))$$

Diamantina, August 2006

Complexity

$$A \cdot \begin{pmatrix} g_1 \\ g_2 \\ g_3 \\ h \end{pmatrix} = 0$$

$$O((mn)^3 \log^2(q))$$

$$O((mn)^2 \log^2(q))$$

$$O((mn) \log^2(mn) \log^2(q))?$$

AG-Codes

For a variety of reasons, we are interested in constructing codes for which q and m are fixed, but the length goes to infinity.

Not possible for RS-codes: the length of the code is no more than q+1.

AG-codes offer a solution! They are constructed by

(a) Realizing the RS-codes are related to the projective line, and
(b) replacing the projective line with an algebraic curve.

The algorithm described has to be properly generalized to AG-codes, and the new algorithm has to be analyzed in this setting.

AG-Codes

In this case the upper bound on the number of correctable errors is

$$\frac{\beta m}{\beta m + 1}(n - k) - 2g$$

where g is the genus of the curve. The probabilistic statements remain with respect to this bound.

Open Questions

1. Can we get better error-correction capability with exponential error bounds and same or better running times?

2. Is it possible to improve the running time of the algorithms to

$$O(mn^{1+\epsilon}\log^{1+\epsilon}(q))?$$

Diamantina, August 2006

Open Questions

1. Can we get better error-correction capability with exponential error bounds and same or better running times?

2. Is it possible to improve the running time of the algorithms to

$$O(mn^{1+\epsilon}\log^{1+\epsilon}(q))?$$

3. Is it possible to make the algorithms "practical?"

Open Questions

1. Can we get better error-correction capability with exponential error bounds and same or better running times?

2. Is it possible to improve the running time of the algorithms to

$$O(mn^{1+\epsilon}\log^{1+\epsilon}(q))?$$

3. Is it possible to make the algorithms "practical?"

4. Are there other applications of "Interleaved codes?"

~~Open~~ Questions

Thank you.

Diamantina, August 2006