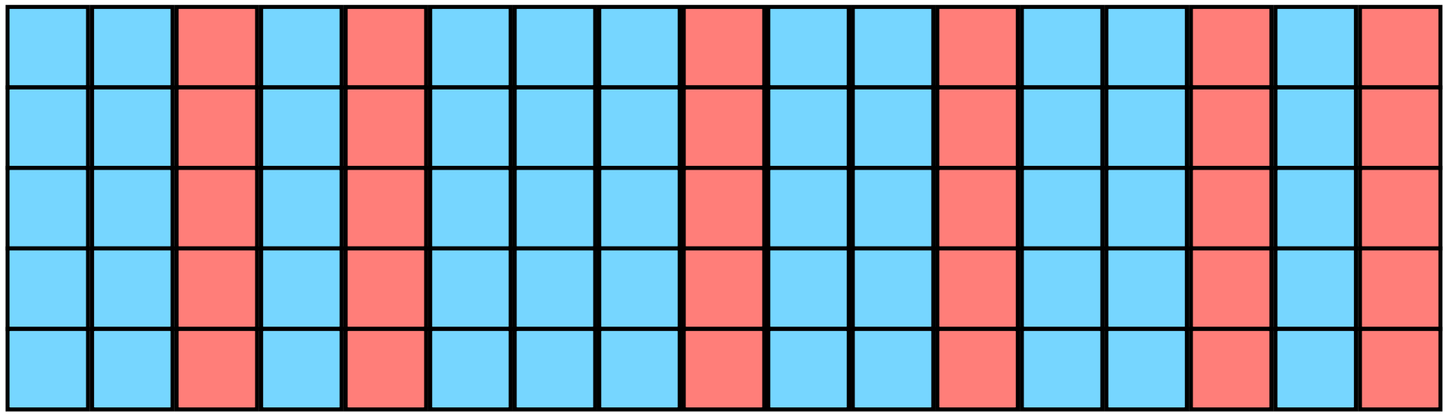
(Improved) Decoding of Interleaved RS-Codes



Amin Shokrollahi

Joint work with A. Brown and L. Minder

EPFL

Cirencester, December 2005

Synopsis

1. RS-Codes

2. The Welch-Berlekamp Decoder

3. RS-Codes over Large Alphabets

4. Generalized WB-Decoding: the BKY-algorithm

5. New Analysis

6. Algorithmic Issues

7. AG-Codes

8. Final Remarks

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.

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

Unique Decoding Problem

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

Cirencester, December 2005

Unique Decoding Problem

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

Transmission

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

Cirencester, December 2005

Unique Decoding Problem

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

Cirencester, December 2005

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

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: $\#E =: e \leq \dfrac{n-k}{2}$

Unique Decoding Problem

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

Transmission

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

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

Promise: $\#E =: e \leq \dfrac{n-k}{2}$

Decoding problem: Find f.

The Error Locator

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

Error locator: $h(x) := \prod_{i \in E} (x - x_i)$

Zeros of error locator yield the error locations

Finding the error locator reveals *f*:

We know the values of *f* at the *n*-*e* correct positions. Since *n*-*e* > *k*-1, interpolation yields *f*.

How do we find the error locator?

$$\forall\, i\colon h(x_i)(f(x_i) - y_i) = 0.$$

The Welch-Berlekamp Decoder

$$h(x)f(x) - yh(x)|_{(x_i,y_i)} = 0$$

$h(x) \in \mathbb{F}_q[x]_{<\frac{n+k}{2}}$ $\quad$ $yh(x) \in \mathbb{F}_q[x]_{\leq\frac{n-k}{2}}$

Theorem: Any pair $(g, h) \in \mathbb{F}_q[x]_{<\frac{n+k}{2}} \times \mathbb{F}_q[x]_{\leq\frac{n-k}{2}} \setminus \{(0, 0)\}$ such that

$$g(x) - yh(x)|_{(x_i,y_i)} = 0$$

for i=1,...,n, satisfies $f = \frac{g}{h}$

First Proof

Theorem: Any pair $(g, h) \in \mathbb{F}_q[x]_{<\frac{n+k}{2}} \times \mathbb{F}_q[x]_{\leq\frac{n-k}{2}} \setminus \{(0,0)\}$ such that

$$g(x) - yh(x)|_{(x_i,y_i)} = 0$$

for i=1,...,n, satisfies $f = \dfrac{g}{h}$

$$F(x) := g(x) - f(x)h(x) \in \mathbb{F}_q[x]_{<\frac{n+k}{2}}$$

$$F(x_i) = 0 \text{ if } y_i = f(x_i)$$

$$F(x) \text{ has at least } \frac{n+k}{2} \text{ roots.}$$

$$F(x) = 0$$

First Proof

Theorem: Any pair $(g, h) \in \mathbb{F}_q[x]_{<\frac{n+k}{2}} \times \mathbb{F}_q[x]_{\leq\frac{n-k}{2}} \setminus \{(0,0)\}$ such that

$$g(x) - yh(x)|_{(x_i,y_i)} = 0$$

for i=1,...,n, satisfies $f = \dfrac{g}{h}$

$$F(x) := g(x) - f(x)h(x) \in \mathbb{F}_q[x]_{<\frac{n+k}{2}}$$

$$F(x_i) = 0 \text{ if } y_i = f(x_i)$$

$$F(x) \text{ has at least } \frac{n+k}{2} \text{ roots.}$$

$$F(x) = 0$$

First Proof

Theorem: Any pair $(g, h) \in \mathbb{F}_q[x]_{<\frac{n+k}{2}} \times \mathbb{F}_q[x]_{\leq\frac{n-k}{2}} \setminus \{(0,0)\}$ such that

$$g(x) - yh(x)|_{(x_i,y_i)} = 0$$

for i=1,...,n, satisfies $f = \dfrac{g}{h}$

$$F(x) := g(x) - f(x)h(x) \in \mathbb{F}_q[x]_{<\frac{n+k}{2}}$$

$$F(x_i) = 0 \text{ if } y_i = f(x_i)$$

$$F(x) \text{ has at least } \frac{n+k}{2} \text{ roots.}$$

$$F(x) = 0$$

First Proof

Theorem: Any pair $(g, h) \in \mathbb{F}_q[x]_{<\frac{n+k}{2}} \times \mathbb{F}_q[x]_{\leq\frac{n-k}{2}} \setminus \{(0,0)\}$ such that

$$g(x) - yh(x)|_{(x_i,y_i)} = 0$$

for i=1,...,n, satisfies $f = \dfrac{g}{h}$

$$F(x) := g(x) - f(x)h(x) \in \mathbb{F}_q[x]_{<\frac{n+k}{2}}$$

$$F(x_i) = 0 \text{ if } y_i = f(x_i)$$

$$F(x) \text{ has at least } \frac{n+k}{2} \text{ roots.}$$

$$F(x) = 0$$

First Proof

Theorem: Any pair $(g, h) \in \mathbb{F}_q[x]_{<\frac{n+k}{2}} \times \mathbb{F}_q[x]_{\leq\frac{n-k}{2}} \setminus \{(0,0)\}$ such that

$$g(x) - yh(x)|_{(x_i,y_i)} = 0$$

for i=1,...,n, satisfies $f = \dfrac{g}{h}$

$$F(x) := g(x) - f(x)h(x) \in \mathbb{F}_q[x]_{<\frac{n+k}{2}}$$

$$F(x_i) = 0 \text{ if } y_i = f(x_i)$$

$$F(x) \text{ has at least } \frac{n+k}{2} \text{ roots.}$$

$$F(x) = 0$$

Second Proof (Essentially the Same)

Theorem: Any pair $(g, h) \in \mathbb{F}_q[x]_{<\frac{n+k}{2}} \times \mathbb{F}_q[x]_{\leq\frac{n-k}{2}} \setminus \{(0,0)\}$ such that

$$g(x) - yh(x)|_{(x_i, y_i)} = 0$$

for i=1,...,n, satisfies $f = \dfrac{g}{h}$

Assume that the zero codeword was sent, and that 1,...,e are the error positions.

$$\begin{array}{l} \left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} e \\ \left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} n-e \geq \frac{n+k}{2} \end{array} \left(\begin{array}{cccc|cccc} 1 & x_1 & \cdots & x_1^{d-1} & y_1 & y_1x_1 & \cdots & y_1x_1^{\ell} \\ 1 & x_2 & \cdots & x_2^{d-1} & y_2 & y_2x_2 & \cdots & y_2x_2^{\ell} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_e & \cdots & x_e^{d-1} & y_e & y_ex_e & \cdots & y_ex_e^{\ell} \\ \hline 1 & x_{e+1} & \cdots & x_{e+1}^{d-1} & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \cdots & x_n^{d-1} & 0 & 0 & \cdots & 0 \end{array}\right) \cdot \begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{d-1} \\ \hline h_0 \\ h_1 \\ \vdots \\ h_{\ell} \end{pmatrix} = 0 \qquad \begin{array}{l} \ell = \frac{n-k}{2} \\ d = \frac{n+k}{2} \end{array}$$

Second Proof (Essentially the Same)

Theorem: Any pair $(g, h) \in \mathbb{F}_q[x]_{<\frac{n+k}{2}} \times \mathbb{F}_q[x]_{\leq\frac{n-k}{2}} \setminus \{(0,0)\}$ such that

$$g(x) - yh(x)|_{(x_i, y_i)} = 0$$

for i=1,...,n, satisfies $f = \dfrac{g}{h}$

Assume that the zero codeword was sent, and that 1,...,e are the error positions.

$$\begin{pmatrix}
1 & x_1 & \cdots & x_1^{d-1} & y_1 & y_1x_1 & \cdots & y_1x_1^{\ell} \\
1 & x_2 & \cdots & x_2^{d-1} & y_2 & y_2x_2 & \cdots & y_2x_2^{\ell} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & x_e & \cdots & x_e^{d-1} & y_e & y_ex_e & \cdots & y_ex_e^{\ell} \\
1 & x_{e+1} & \cdots & x_{e+1}^{d-1} & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
1 & x_n & \cdots & x_n^{d-1} & 0 & 0 & \cdots & 0
\end{pmatrix}
\cdot
\begin{pmatrix}
g_0 \\ g_1 \\ \vdots \\ g_{d-1} \\ h_0 \\ h_1 \\ \vdots \\ h_{\ell}
\end{pmatrix}
= 0$$

(e rows; $n - e \geq \frac{n+k}{2}$ rows)

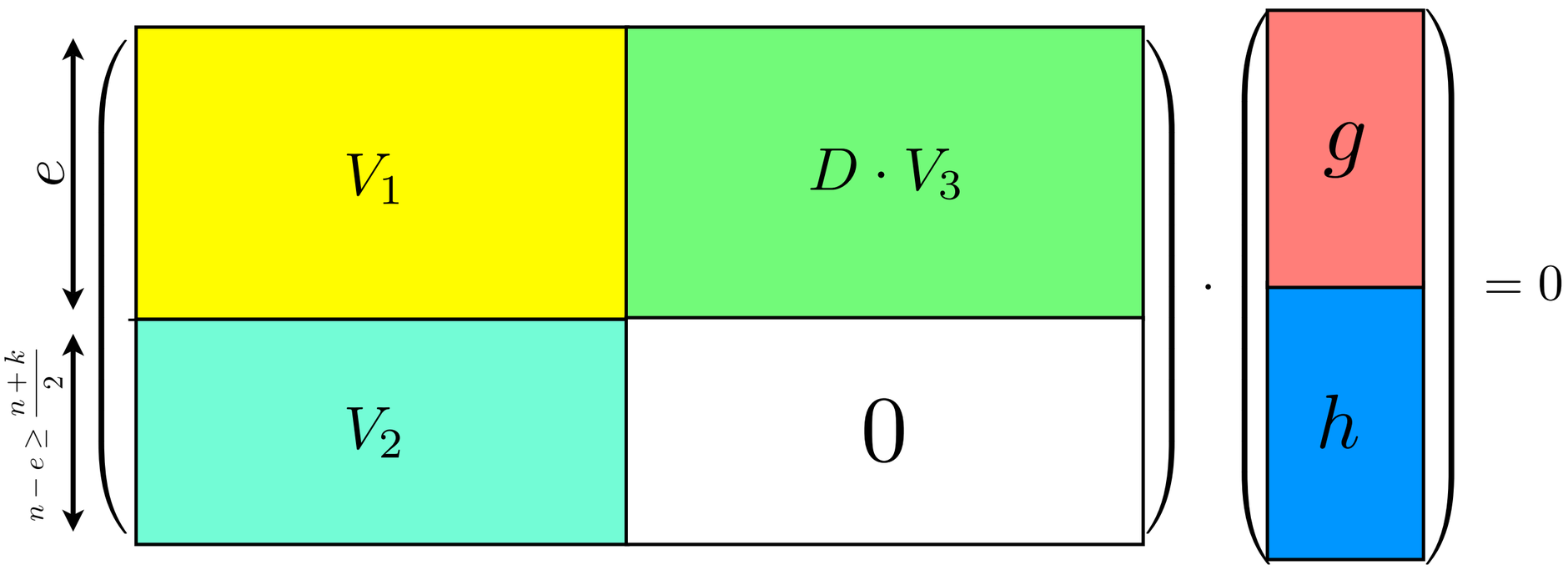
Second Proof (Essentially the Same)

Theorem: Any pair $(g, h) \in \mathbb{F}_q[x]_{<\frac{n+k}{2}} \times \mathbb{F}_q[x]_{\leq\frac{n-k}{2}} \setminus \{(0,0)\}$ such that

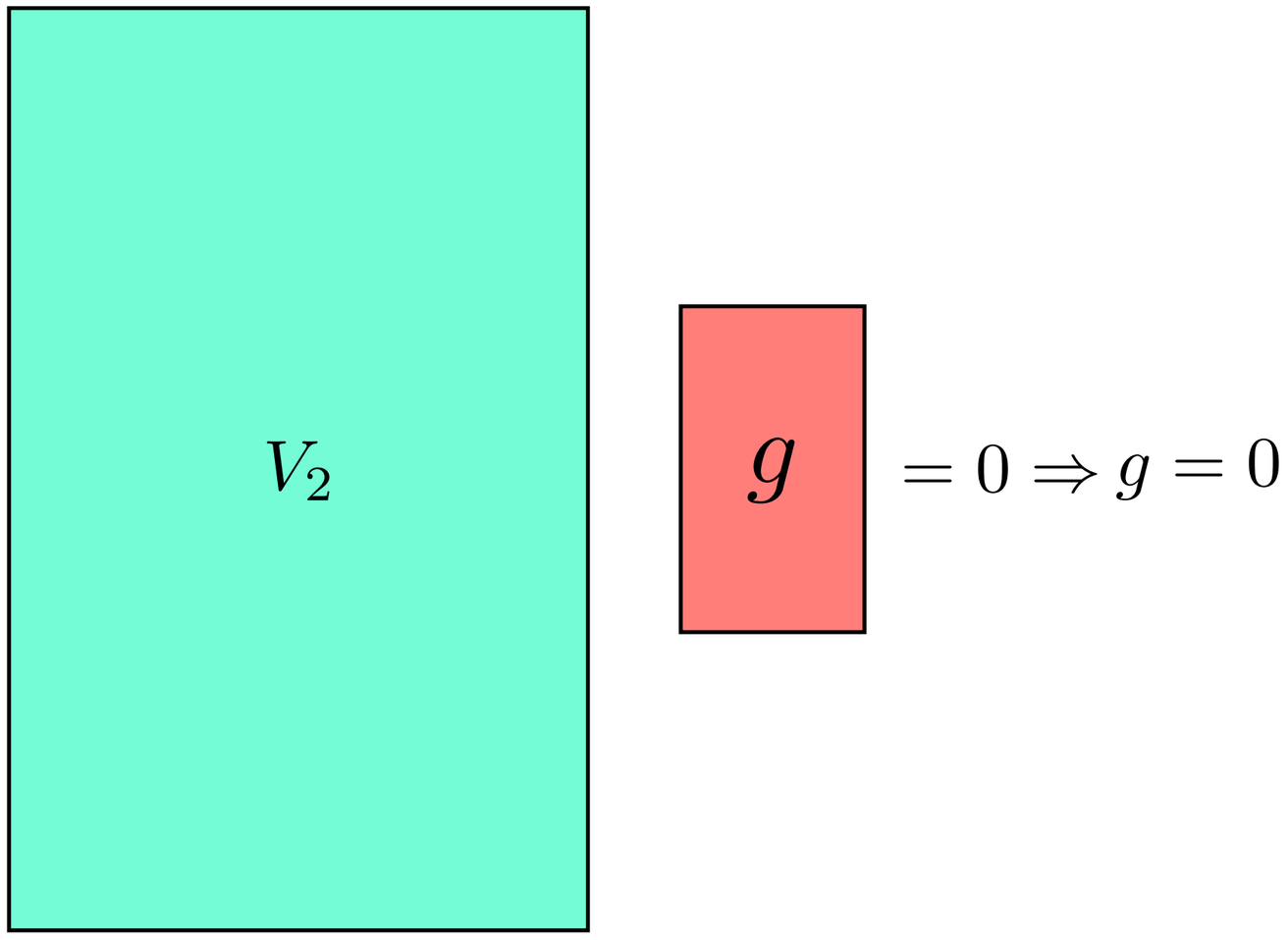
$$g(x) - yh(x)|_{(x_i,y_i)} = 0$$

for i=1,...,n, satisfies $f = \frac{g}{h}$

Assume that the zero codeword was sent, and that 1,...,e are the error positions.



Second Proof (Essentially the Same)



V_2 is Vandermonde, so columns are independent.

Decoding More Errors?

Need other techniques to decode more errors.

If number of errors is larger than $(n\text{-}k)/2$, then the error vector is not necessarily unique.

We could do either (a) list-decoding, or (b) probabilistic decoding.

How many errors can we possible expect to decode?

No more than $(n\text{-}k)$

Decoding More Errors?

List-decoding algorithms of Sudan, and Guruswami-Sudan can decode up to a

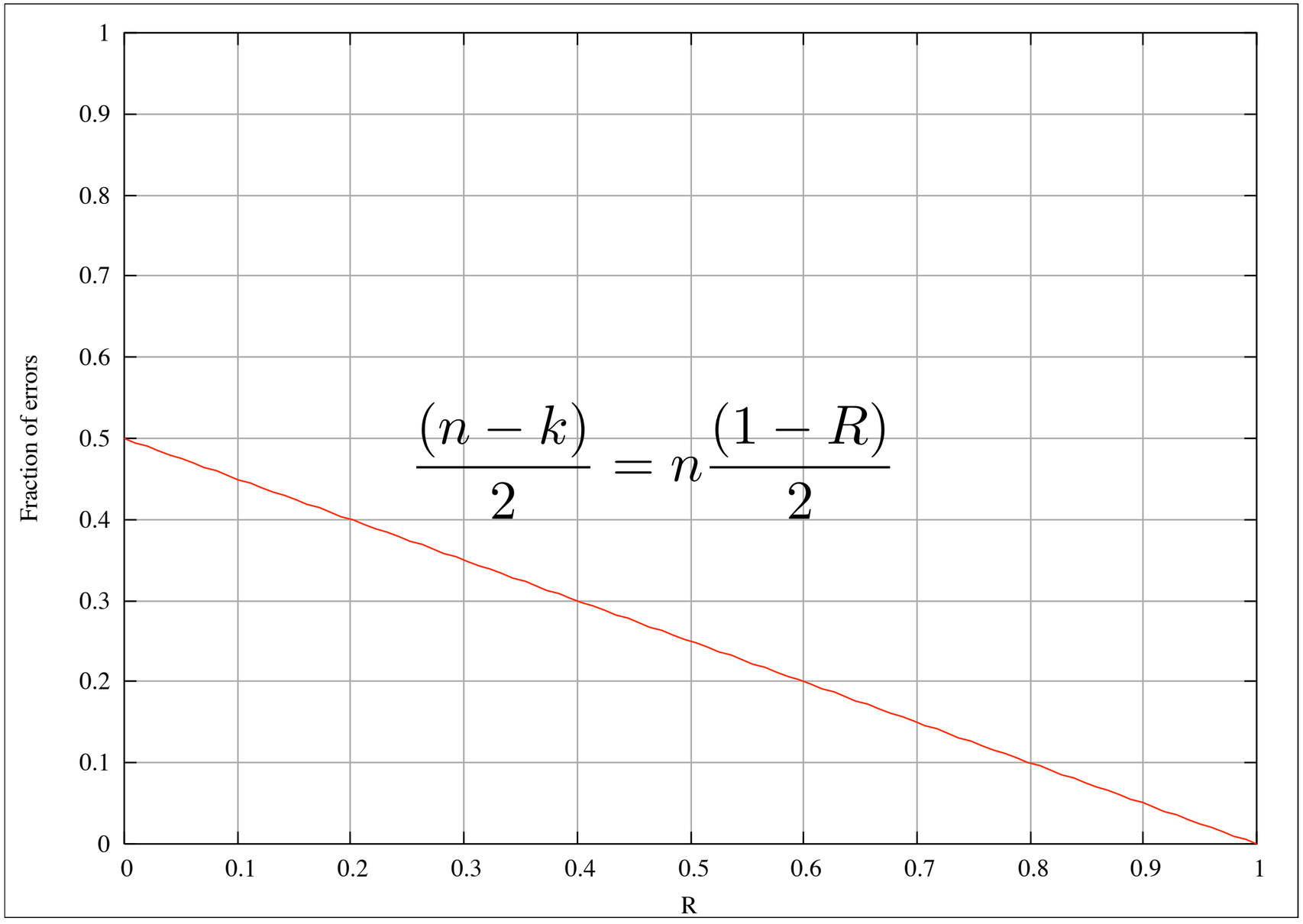
$$1 - \sqrt{k/n}$$

fraction of errors, and produce a short list of possible codewords.

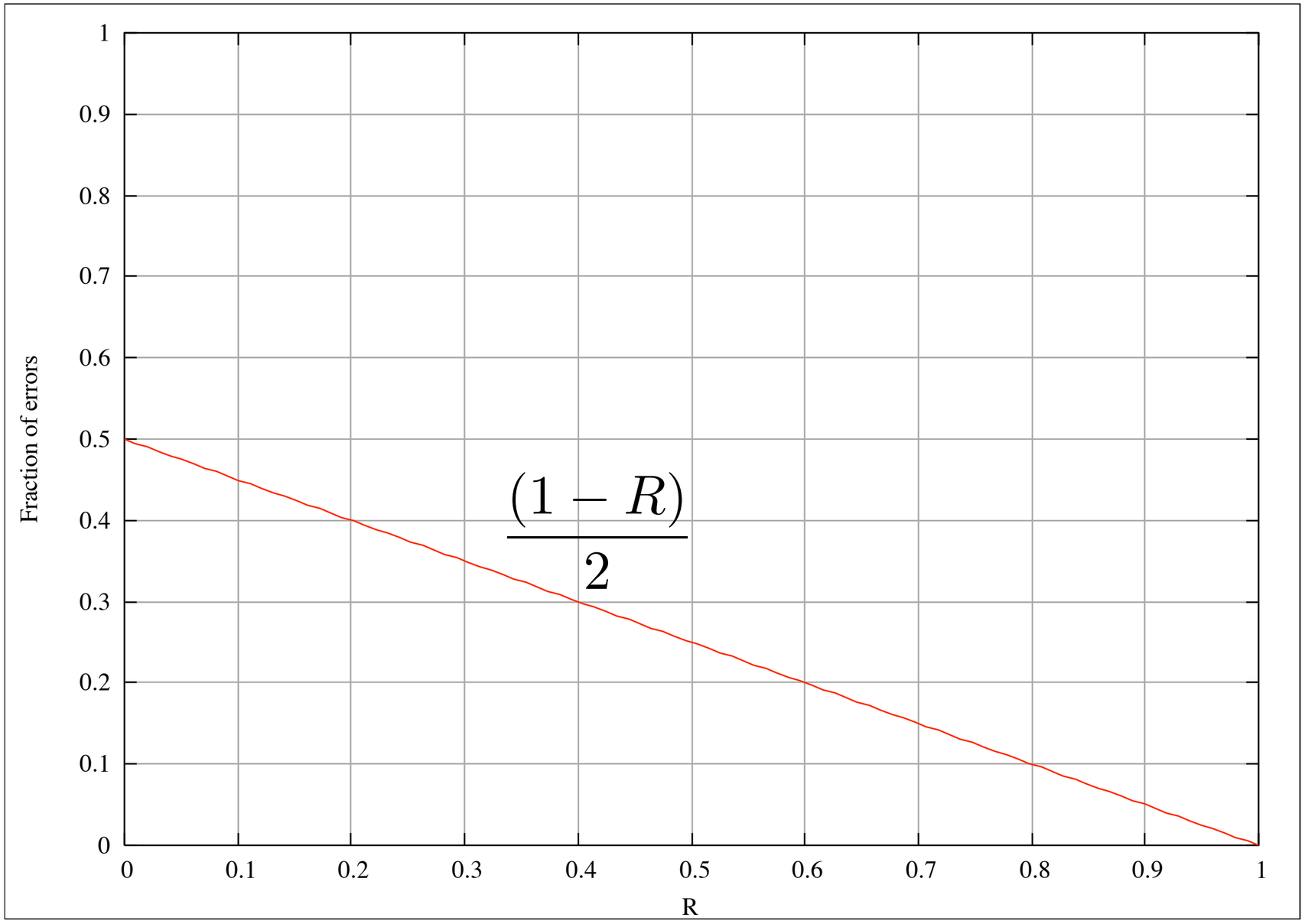
What about more errors?

Possible, under a probabilistic model. Algorithm is due to Bleichenbacher, Kiyaias, and Yung (BKY).

Decoding More Errors?

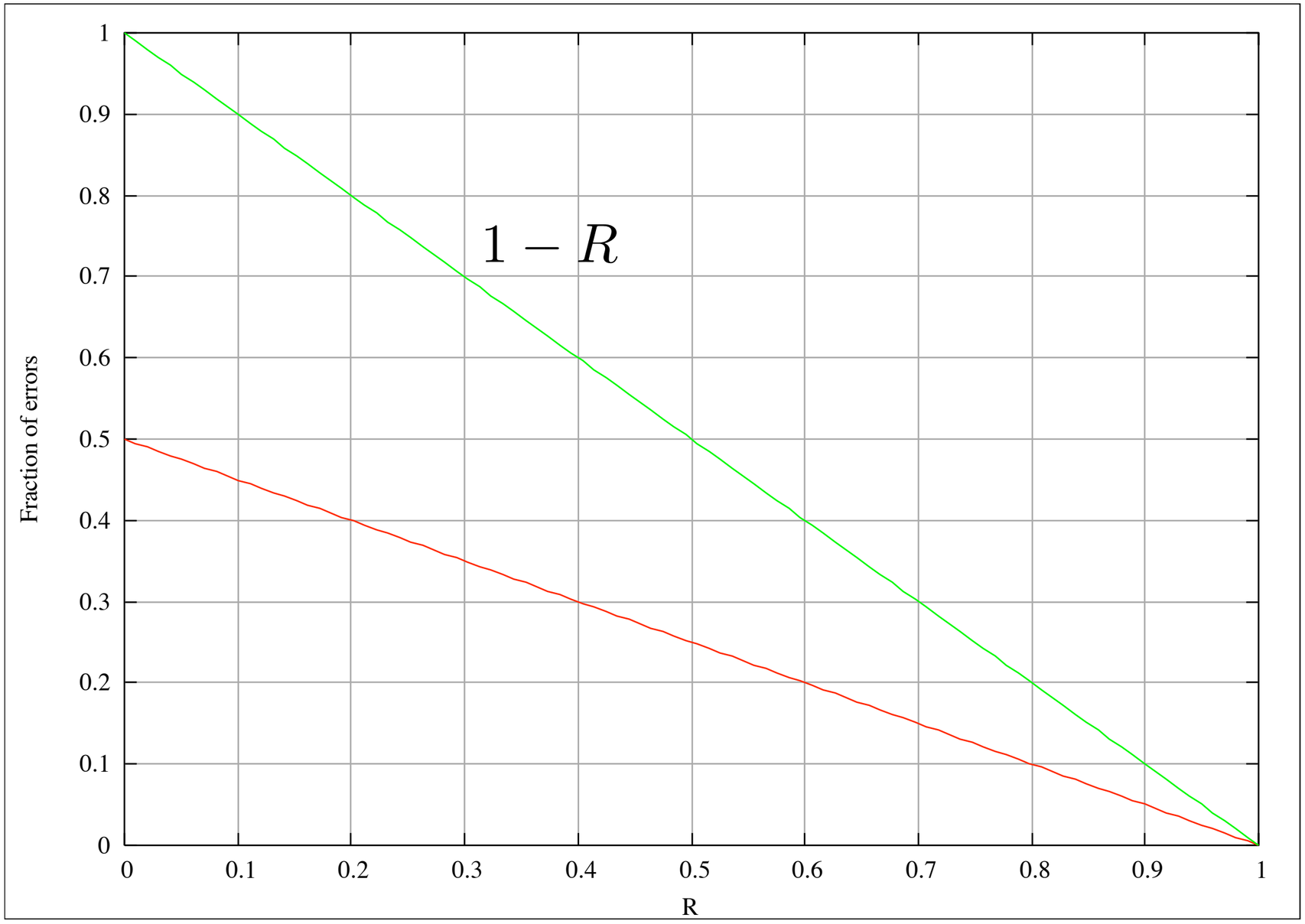


Decoding More Errors?



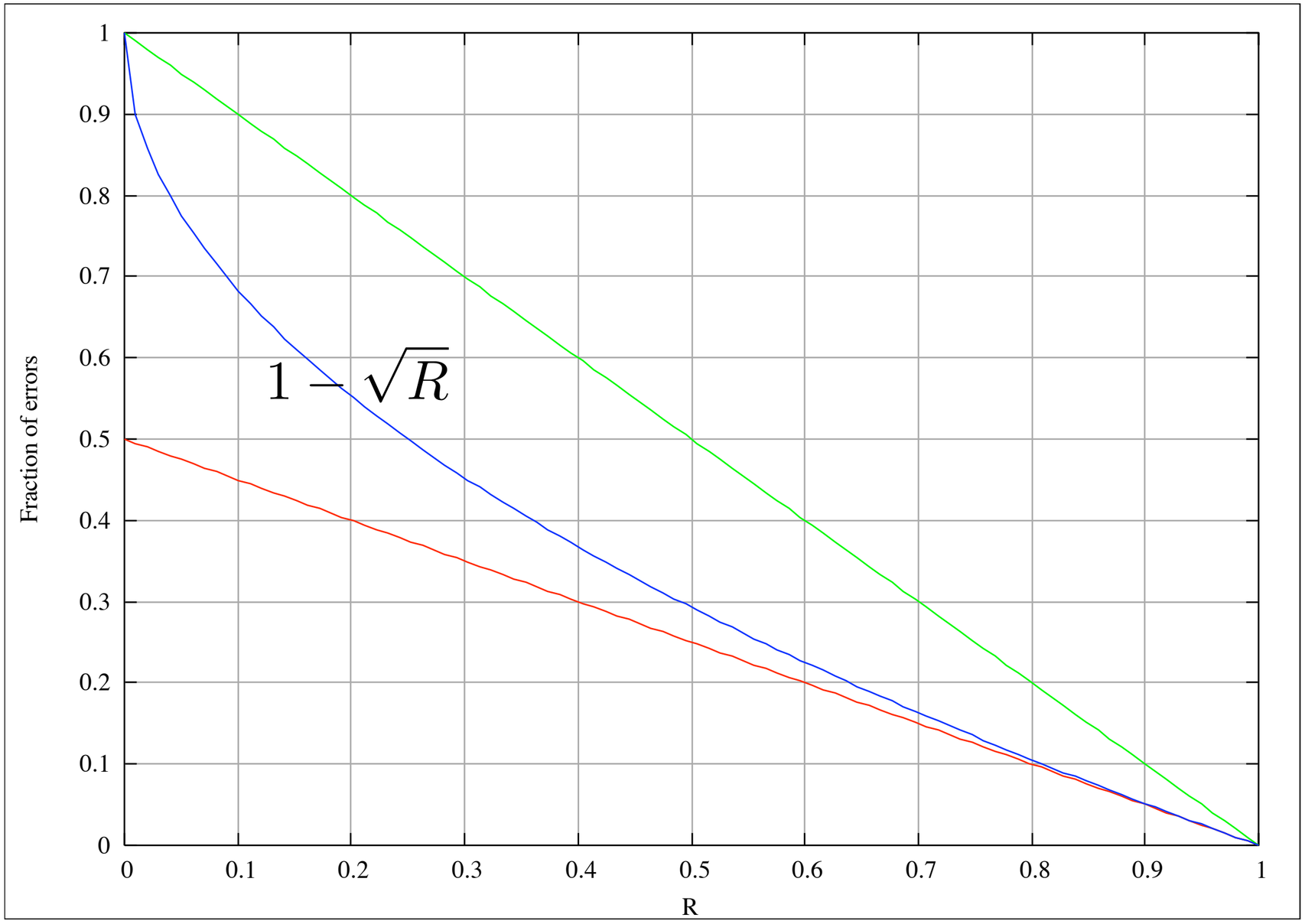
Cirencester, December 2005

Decoding More Errors?



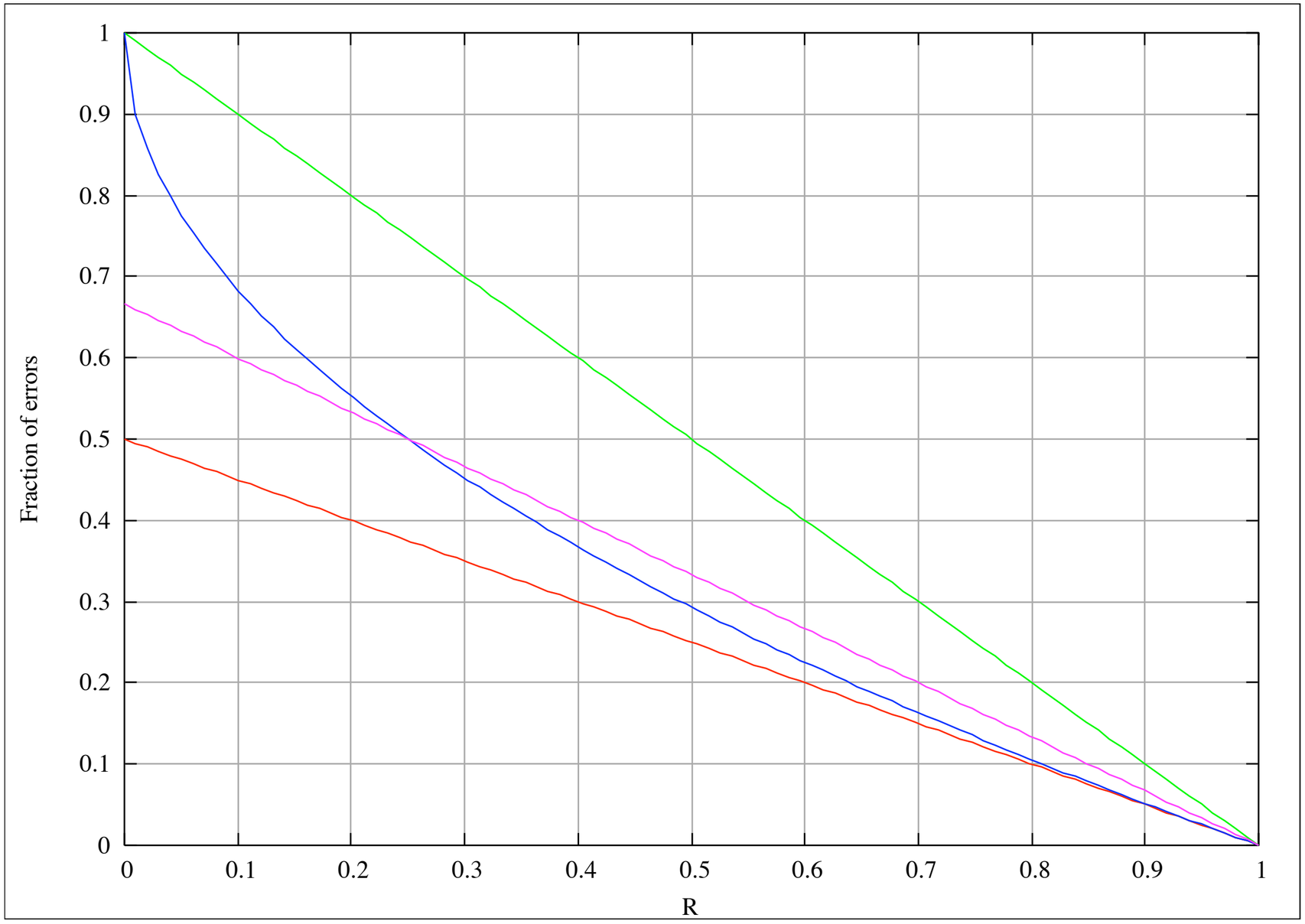
Cirencester, December 2005

Decoding More Errors?

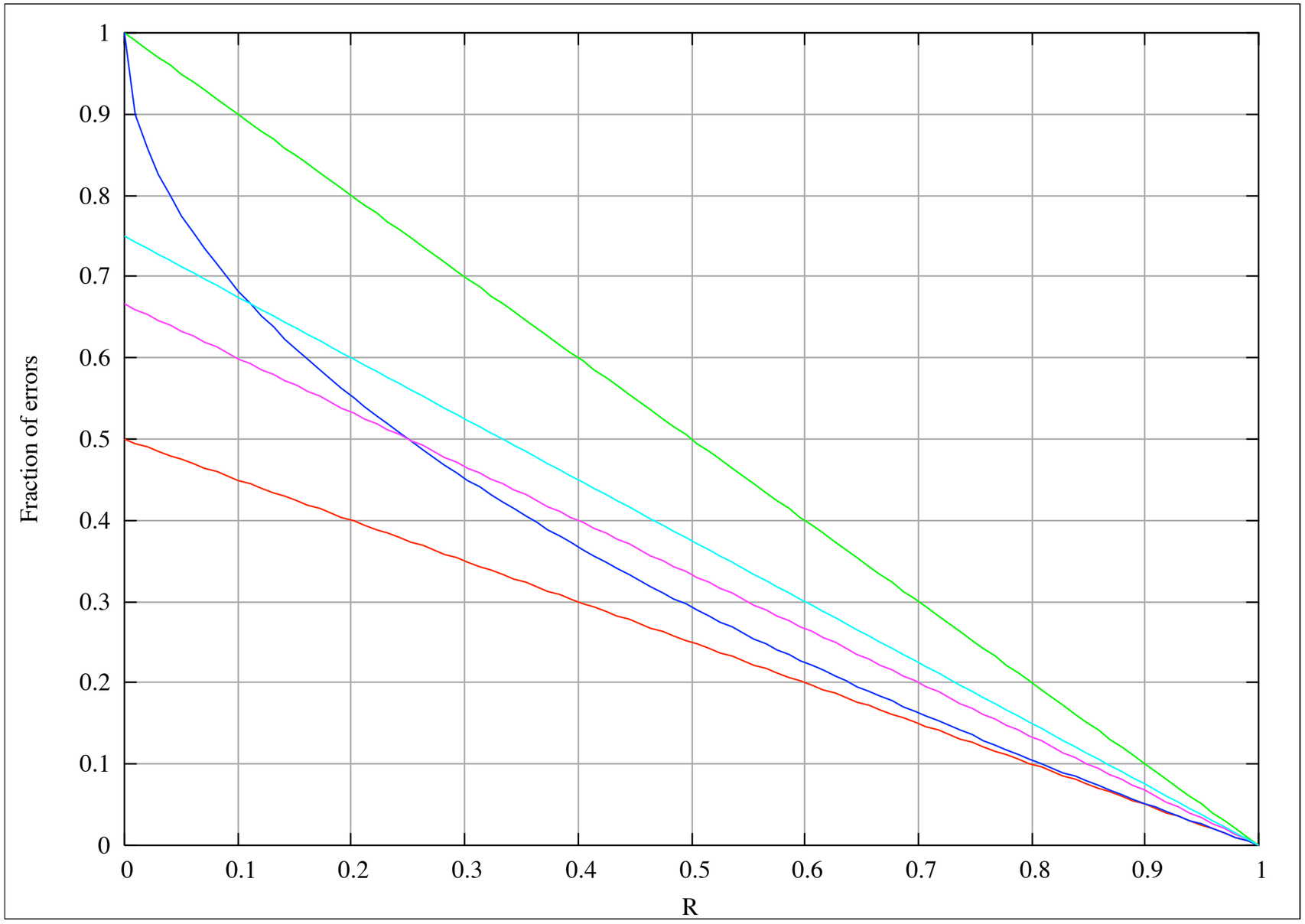


Cirencester, December 2005

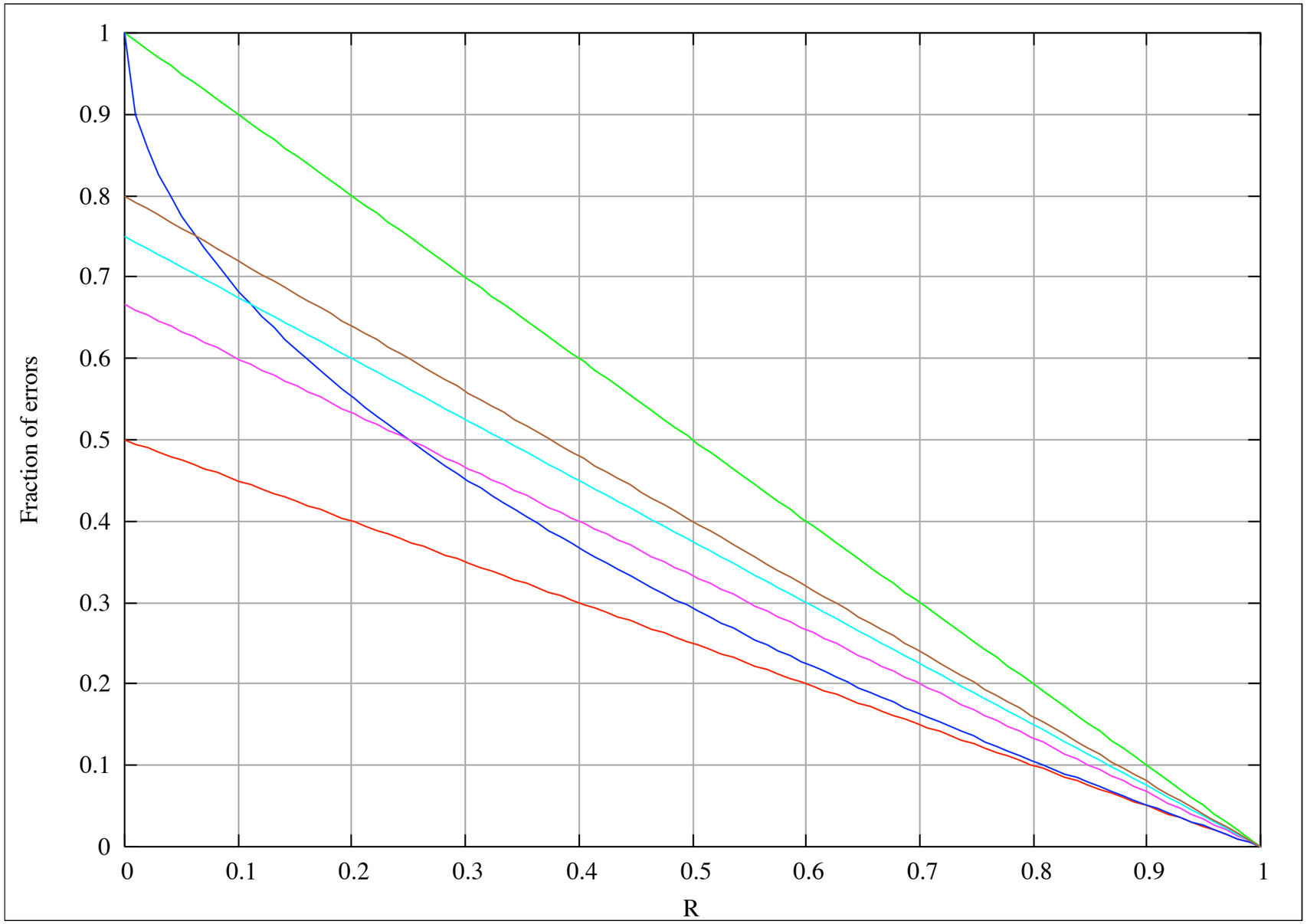
Decoding More Errors?



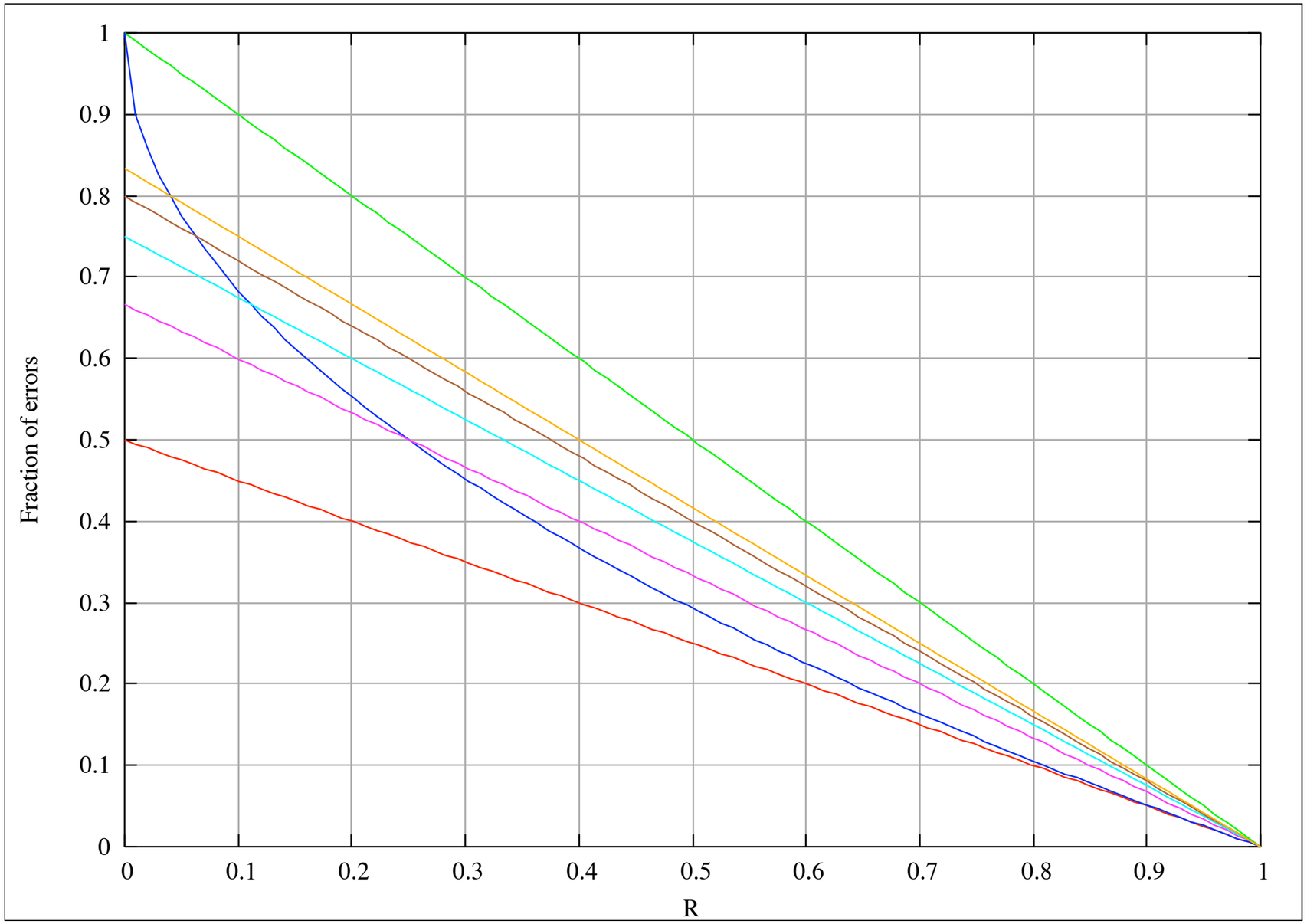
Decoding More Errors?



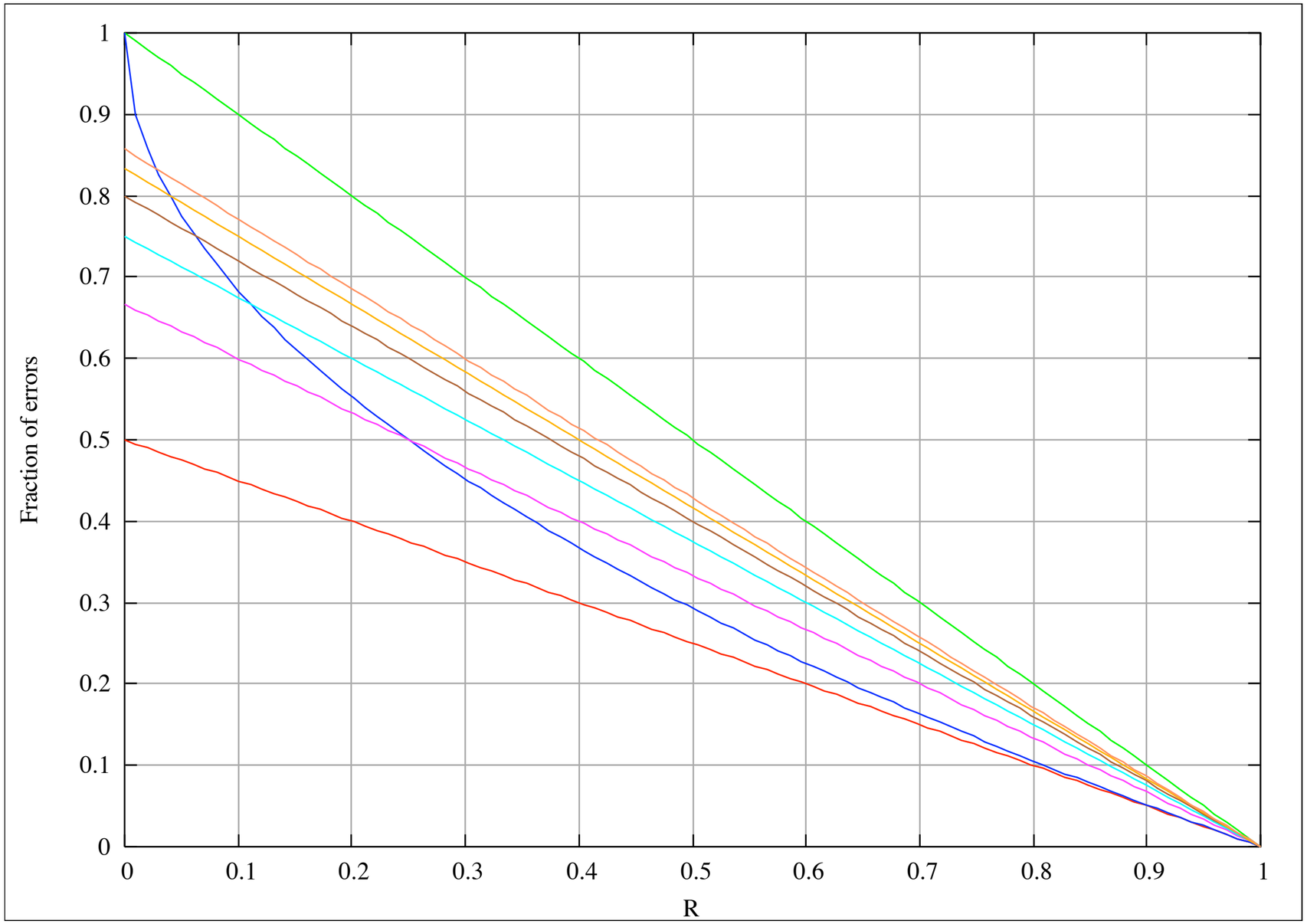
Decoding More Errors?



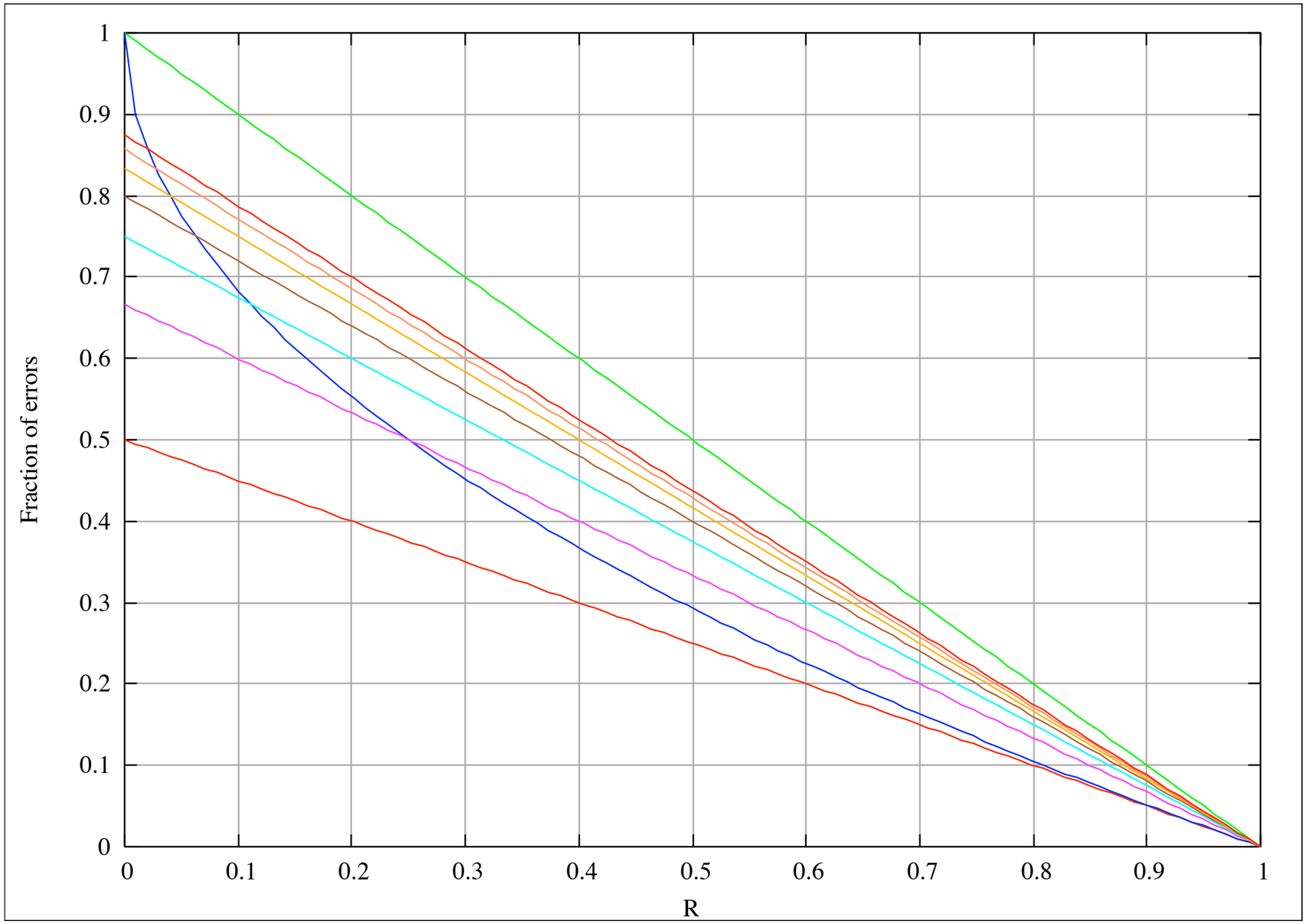
Decoding More Errors?



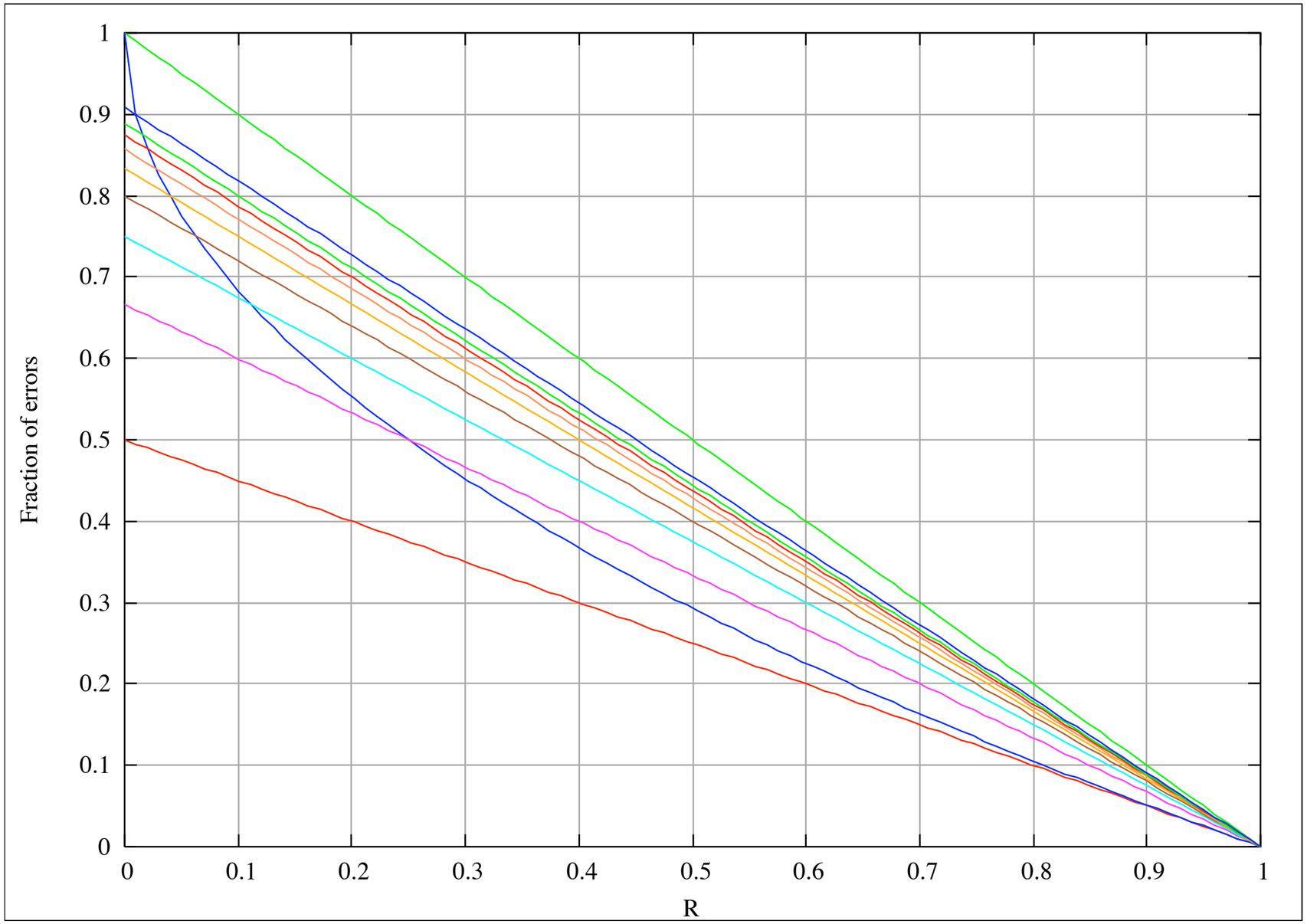
Decoding More Errors?



Decoding More Errors?

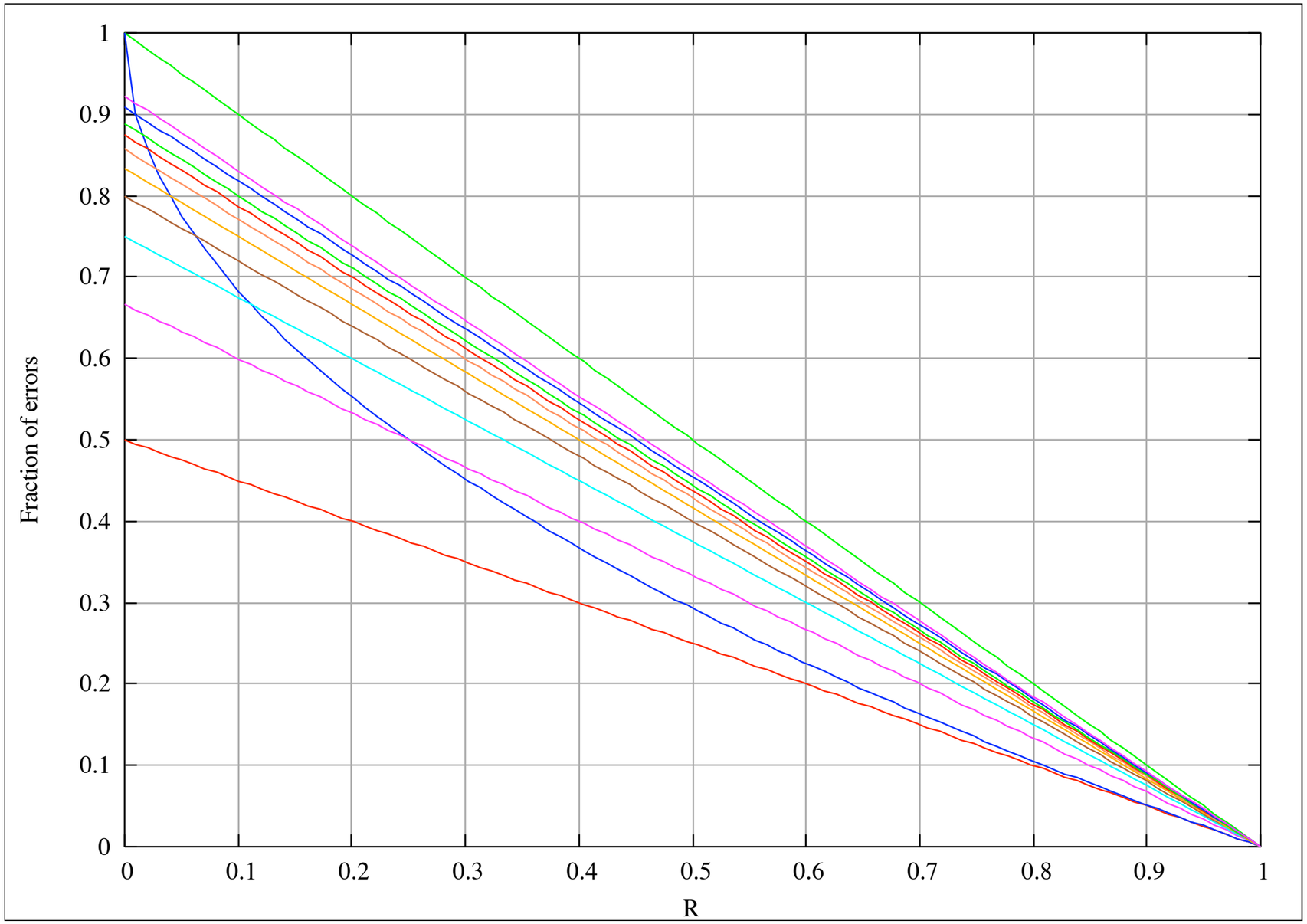


Decoding More Errors?

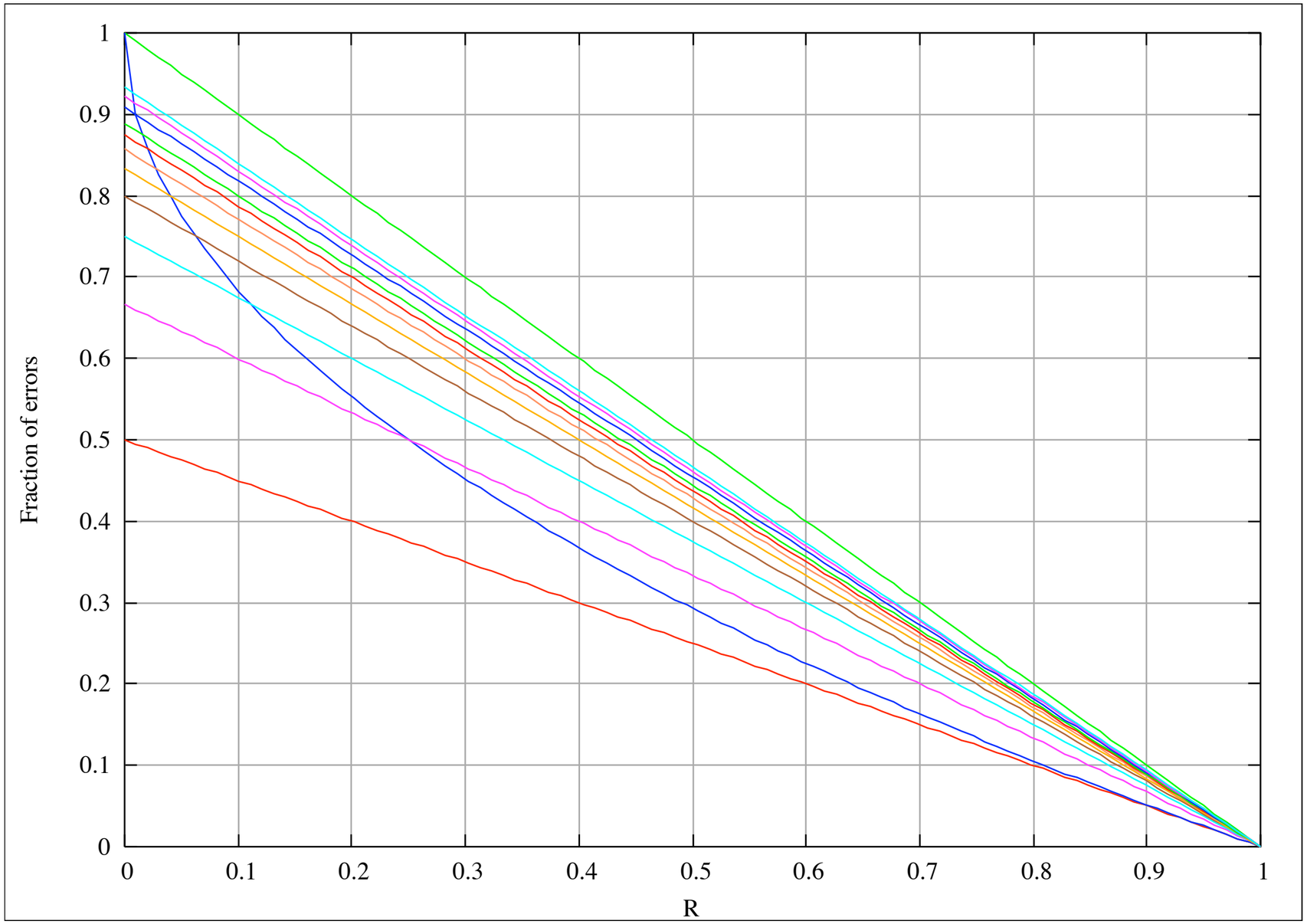


Cirencester, December 2005

Decoding More Errors?

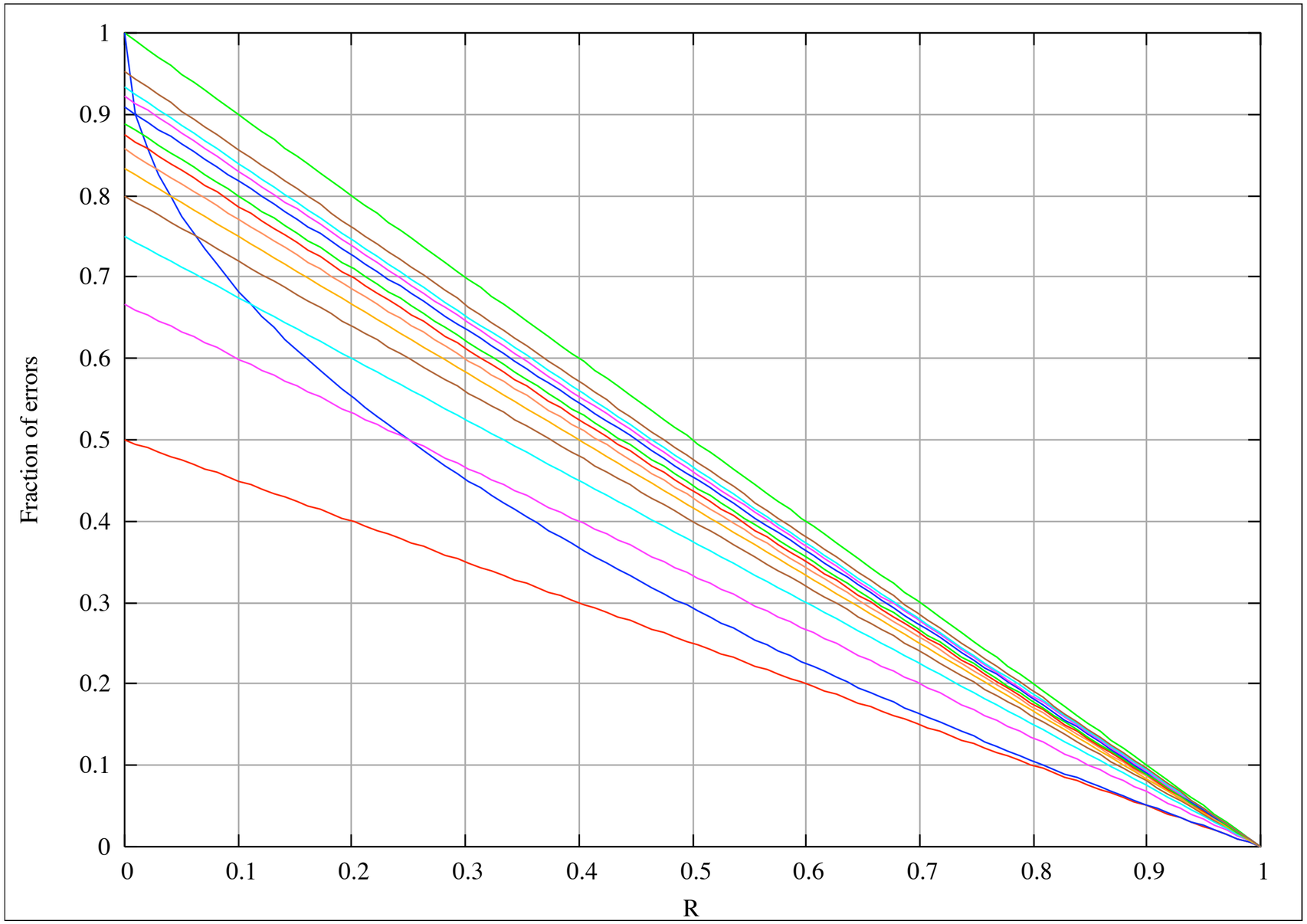


Decoding More Errors?

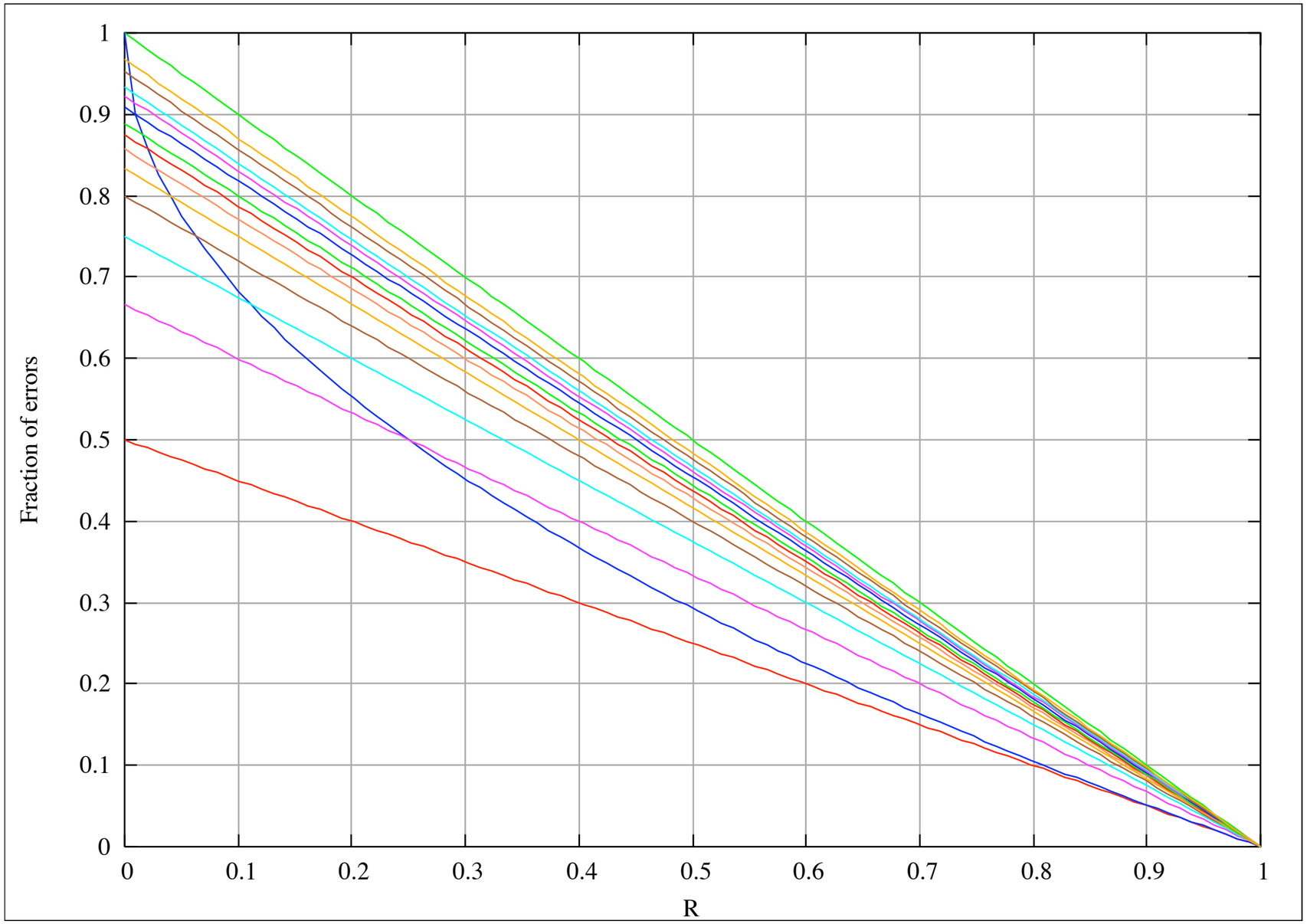


Cirencester, December 2005

Decoding More Errors?



Decoding More Errors?



RS-Codes over Large Alphabets

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

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

RS-Codes over Large Alphabets

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

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

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

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

RS-Codes over Large Alphabets

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

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

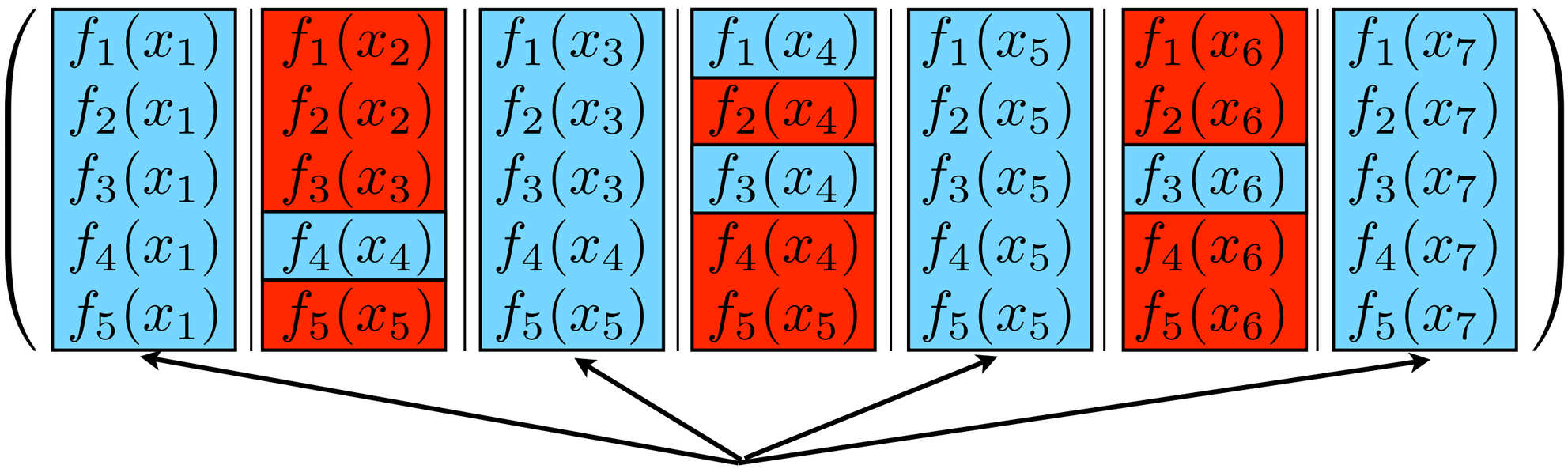
$$\mathbb{F}_{q^m}[x]_{<k} \simeq \left(\mathbb{F}_q[x]_{<k}\right)^m$$

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

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

Interleaved codeword

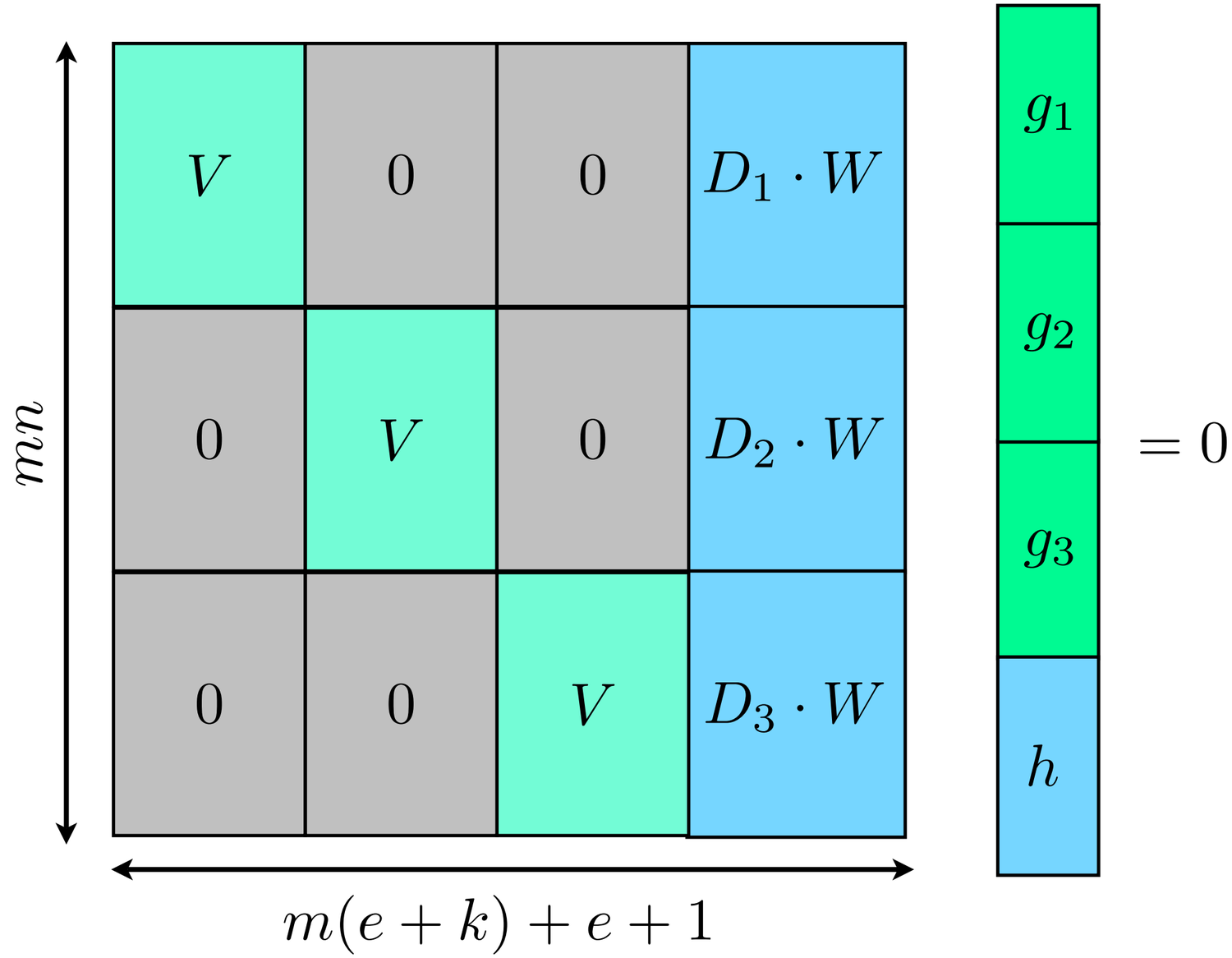
RS-Codes over Large Alphabets



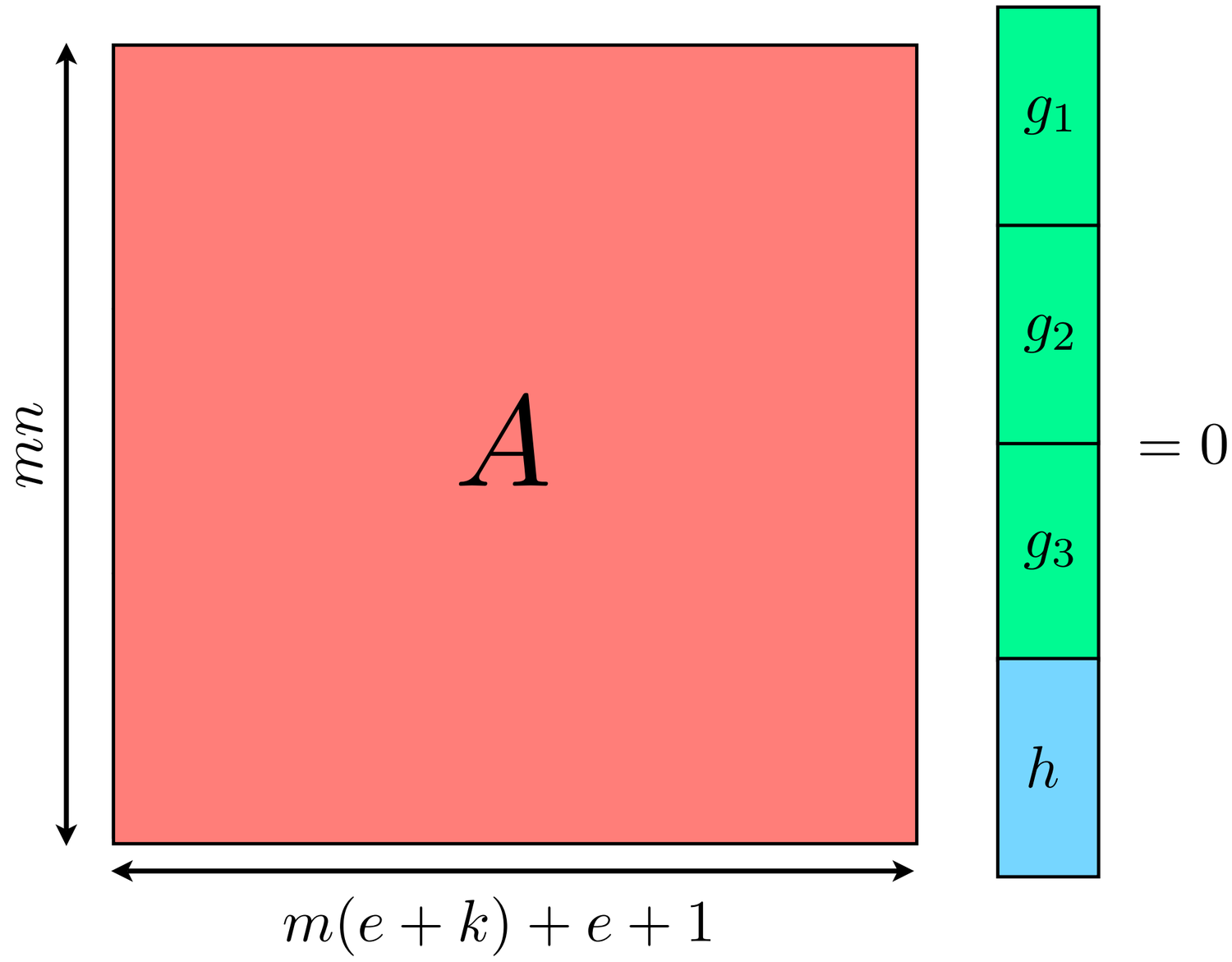
Non-error positions are the same for all the polynomials, so same error locator

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

RS-Codes over Large Alphabets



RS-Codes over Large Alphabets

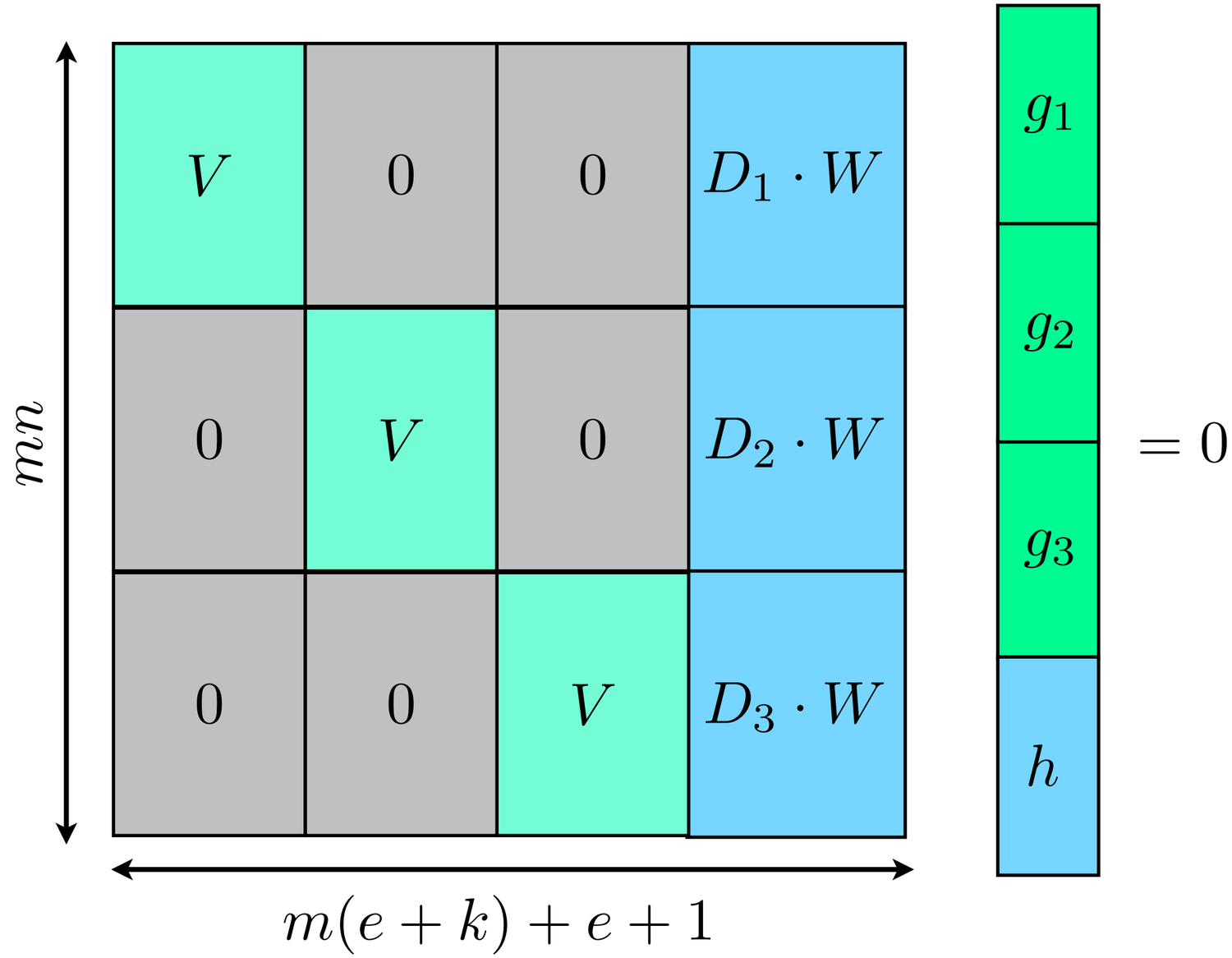


Algorithm

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

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 $f_i = g_i/h$.

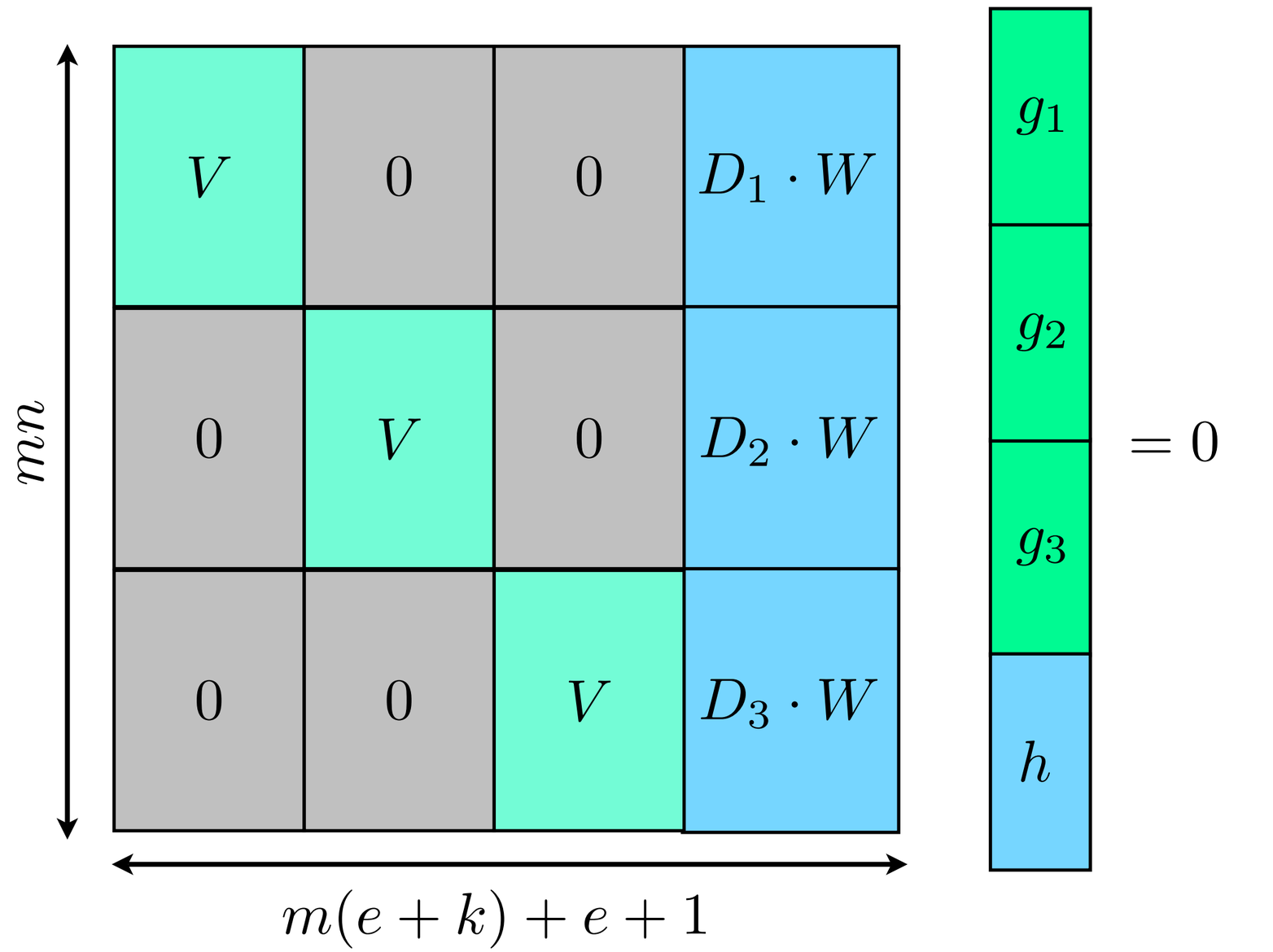
RS-Codes over Large Alphabets



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 $O(q^{-m\epsilon n})$.

Comparison to Other Methods

Hashing: every symbol has $q^{1-\delta}$ symbols; error probability is $O(n/q^{\delta})$.

Comparison to Other Methods

Hashing: every symbol has $q^{1-\delta}$ symbols; error probability is $O(n/q^{\delta})$.

Coppersmith and Sudan: Different algorithm, error probability is $O(q^{O(m)}/n)$.

Comparison to Other Methods

Hashing: every symbol has $q^{1-\delta}$ symbols; error probability is $O(n/q^{\delta})$.

Coppersmith and Sudan: Different algorithm, error probability is $O(q^{O(m)}/n)$.

Hashing and error-correction: slightly worse rate with same error probability as in our case.

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 $f_i = g_i/h$.

Assumptions

(a) The error positions are $1, 2, \ldots, e$.

(b) The functions $f_1, \ldots, f_m$ sent over the channel are all zero.

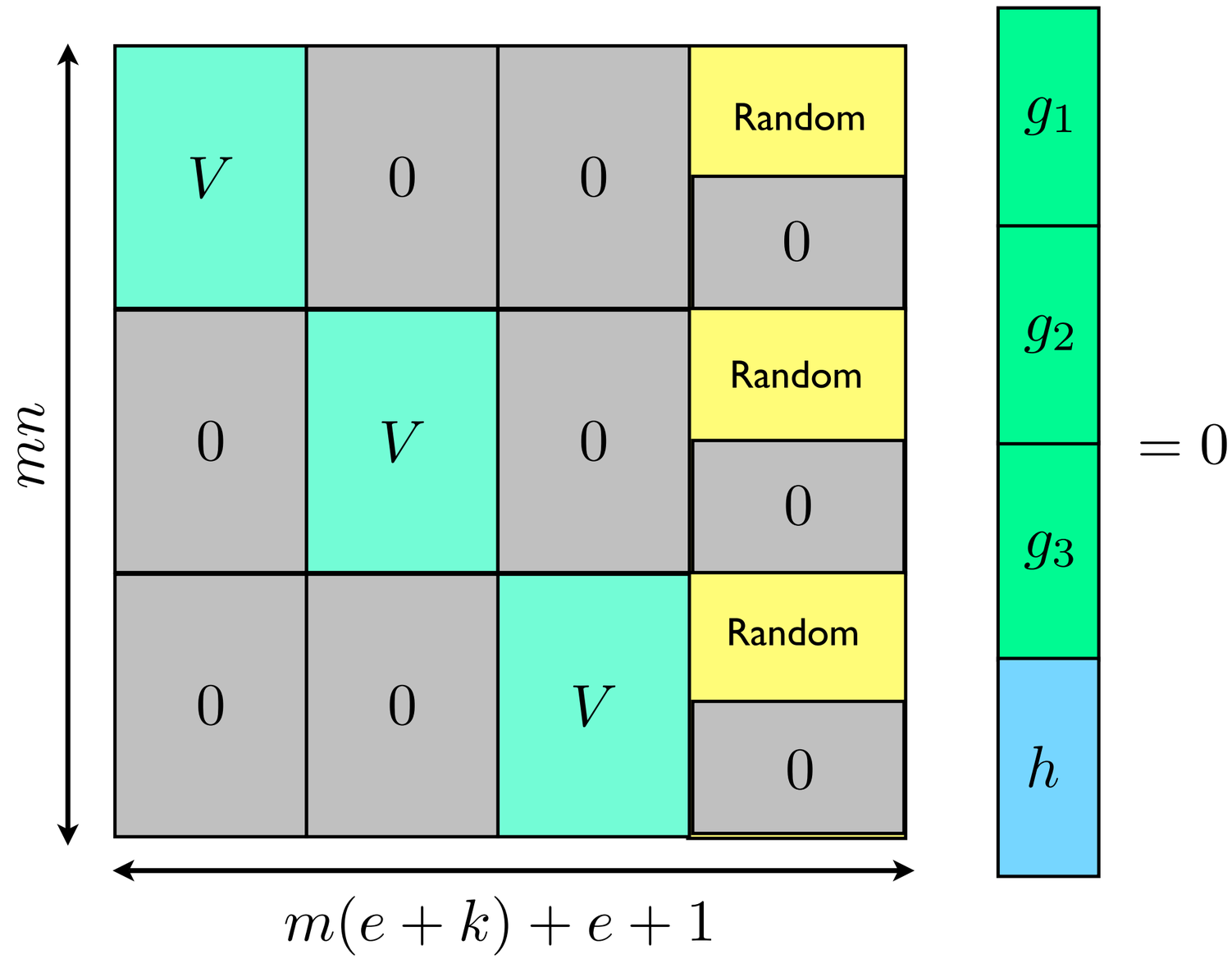
Assumption (a) amounts to re-ordering and is trivial.

Assumption (b) follows from linearity:
Error probability is independent of the choice of the word sent.

Assumptions

$$
\underbrace{\begin{pmatrix}
V & 0 & 0 & D_1 \cdot W \\
0 & V & 0 & D_2 \cdot W \\
0 & 0 & V & D_3 \cdot W
\end{pmatrix}}_{m(e+k)+e+1}
\underbrace{\begin{pmatrix} g_1 \\ g_2 \\ g_3 \\ h \end{pmatrix}}_{uu}
= 0
$$

Assumptions



Error Event

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

Error Event

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

There exists $(g_1|g_2|g_3|h)$ in the right kernel of A such that $g_j \neq 0$ for some j.

Method of Proof

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

Given $v = (g_1|g_2|g_3|h)$, with some $g_j \neq 0$, calculate $\Pr[v \in \ker(A)]$

Method of Proof

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

Given $v = (g_1|g_2|g_3|h)$, with some $g_j \neq 0$, calculate $\Pr[v \in \ker(A)]$

Use Markov's inequality

Method of Proof

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

Given $v = (g_1|g_2|g_3|h)$, with some $g_j \neq 0$, calculate $\Pr[v \in \ker(A)]$

Method of Proof

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

Given $v = (g_1|g_2|g_3|h)$, with some $g_j \neq 0$, calculate $\Pr[v \in \ker(A)]$

Hard part

Complexity

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

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

Complexity

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

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

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

Complexity

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

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

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

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

An Example

Want to transmit an MP3 file (4MB) over a packet-based network to a receiver, and every packet is 1024 bytes.

Due to low level of physical layer error-correction, we expect that at most 33% of the packets are corrupted.

Want to be able to recover the file with high probability using packet level error correction.

An Example

$$q = 2^{16} \qquad \Rightarrow \quad \beta \simeq 1$$

$$m = 512$$

An Example

$$q = 2^{16} \qquad \Rightarrow \quad \beta \simeq 1$$

$$m = 512$$

$$k = 4000$$

$$n = 6010$$

$$e \leq \frac{n}{3} = \frac{512}{513}(n-k) - 2.75$$

An Example

$$q = 2^{16} \qquad \Rightarrow \quad \beta \simeq 1$$
$$m = 512$$

$$k = 4000 \qquad e \leq \frac{n}{3} = \frac{512}{513}(n-k) - 2.75$$
$$n = 6010$$

$$\text{Error probability} \leq q^{-2.75m} < 10^{-6000}$$

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.

Refer to the paper to see how this is done!

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.

Summary

1. Provided a slight modification of the algorithm of Bleichenbacher et al.

Cirencester, December 2005

Summary

1. Provided a slight modification of the algorithm of Bleichenbacher et al.

2. Provided a new analysis which guarantees exponentially small error probabilities.

Cirencester, December 2005

Summary

1. Provided a slight modification of the algorithm of Bleichenbacher et al.

2. Provided a new analysis which guarantees exponentially small error probabilities.

3. Provided generalizations to AG-codes.

Cirencester, December 2005

Open Questions

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

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

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

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

Cirencester, December 2005

~~Open~~ Questions

Thank you.

Cirencester, December 2005