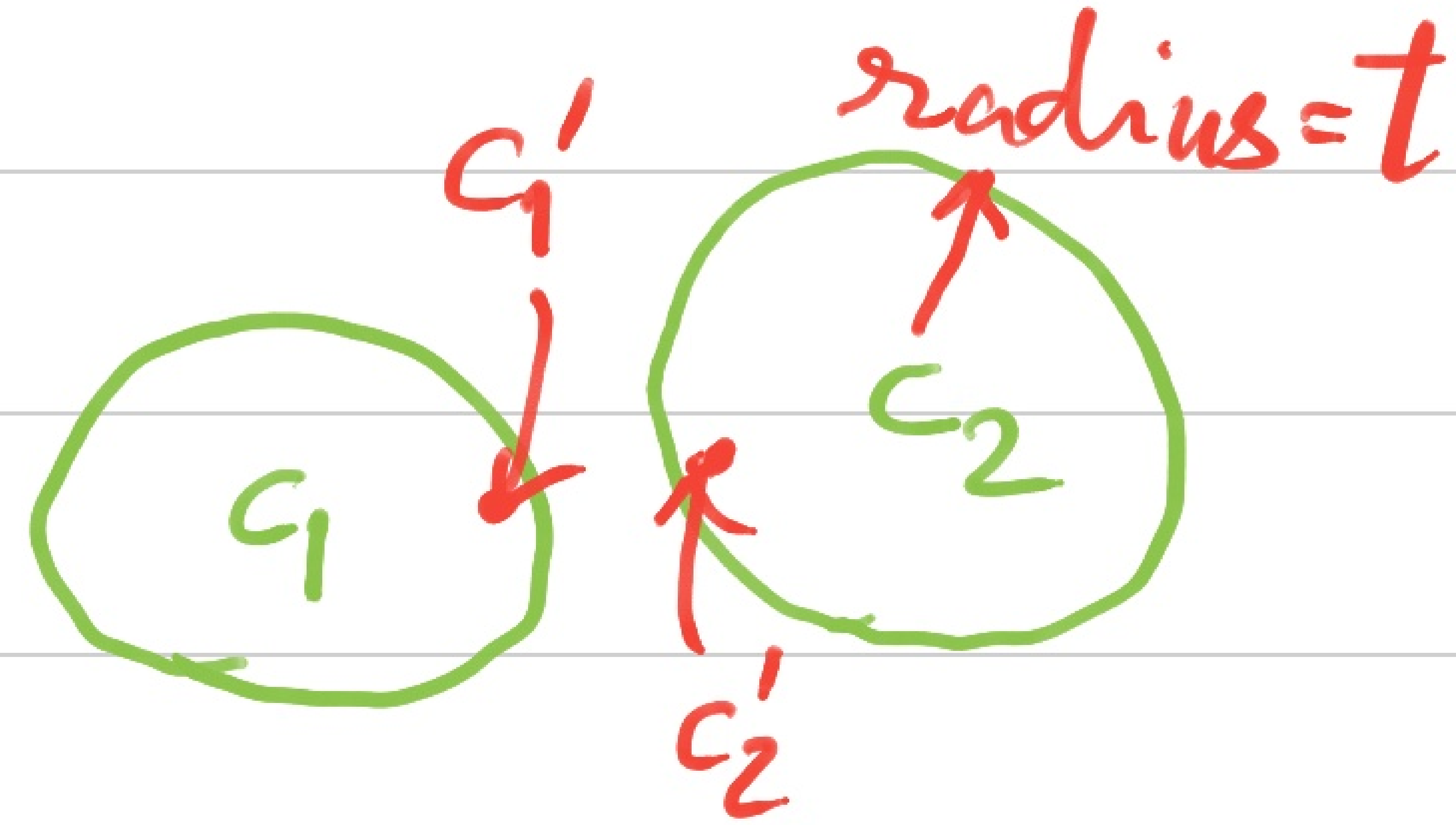
Distance

- $(2t+1)$ is called distance of the (RS) code.
- It is the minimum Hamming distance between any two distinct codewords.



▷ Distance $= \Delta \Rightarrow$ error-tolerance (of any code) is $< \Delta/2$.

- With error-bound $t \geq N/2$, there are many messages corresponding to a corrupted codeword.

- Could we find the list of messages?

- (Madhu Sudan, 1995) found an efficient way to list decode (RS code).

List decoding RS code

- Consider $(d_0, \ldots, d_{k-1}) \xrightarrow{RS} (c_0, \ldots, c_{n-1}) \xrightarrow{\text{channel}}$ ($\geq T$ are correct)

$c_0 = P(e_0)$, $c_{n-1} = P(e_{n-1})$

$P := \sum_{i<k} d_i x^i$

$\mapsto (c_0', \ldots, c_{n-1}')$ ← Bob receives

- Consider a bivariate "error locator" polynomial $Q(x,y)$ of degree $D_x := \deg_x Q$ & $D_y := \deg_y Q$

(1) s.t. $Q(e_j, c_j') = 0$, $\forall j \in [0 \ldots n-1]$.

[If $(1+D_x)\cdot(1+D_y) \geq n$ then such a $Q \neq 0$ exists. It can be computed by linear algebra.]

- Consider $R := Q(x, P(x))$. It has $\deg \leq D_x + (k-1)D_y$.
- We know: $R(e_j) = 0$ for T-many $j \in [0 \ldots n-1]$.
[by (1)]

$\triangleright$ $T > D_x + (k-1)D_y \geq \deg R \Rightarrow R = 0 \Rightarrow (y-P) \mid Q$.

Lemma: If $n < (1+D_x)(1+D_y)$ & $D_x + (k-1)D_y < T$, then any curve Q fitting $\{(e_j, c_j') \mid j \in [0..n-1]\}$ has $y - P(x)$ as a factor.

The List Decoding algorithm:

1) Fix $D_x = \sqrt{nk}$, $D_y = \sqrt{n/k}$ & $T = 2\sqrt{nk}$.
2) Compute Q : $Q(e_j, c_j') = 0$, $\forall\, 0 \le j \le n-1$.

3) Factor $Q(x,y)$ & collect its factors of the form $y - f(x)$ with $\deg f < k$. [#f's $\le D_y \le \sqrt{n/k}$.]
4) Output the list of $\{f$ as above$\}$.

- eg. setting: For $n = k\lg^2 k$, we only need $2k\lg k$ correct values.

  [Note $2k\lg k / n \to 0$!]

▷ This list-decoding algorithm is in randomized poly-time.

It works up to $(n - 2\sqrt{nk})$ many bit errors!

- In decoding RS codes we require two new algebraic algorithms:

1) construction of a finite field (eg. $\mathbb{F}_{2^b}$).
2) factoring a bivariate polynomial.

Constructing $\mathbb{F}_q$ ($q = p^b$ given in binary)

- Basically, we want to construct an irreducible polynomial over $\mathbb{F}_p$ of $\deg = b$.

- We'll show that a random choice works!

- Let $\underline{\pi(\ell)}$ be the # irreducibles in $\mathbb{F}_p[x]$ of degree ℓ.
- Recall that $x^{p^\ell} - x$ has, as factors, <u>all</u> irreducibles of $\deg = k \mid \ell$.

$$\triangleright \quad p^\ell = \sum_{k \mid \ell} \pi(k) \cdot k \quad \text{--- (R)}$$

<u>Theorem:</u> $\forall \ell \geq 1$, $\frac{1}{2\ell} \leq \pi(\ell)/p^\ell \leq 1/\ell$ &

[analog of Prime Number Theorem] $\pi(\ell) = p^\ell/\ell + O(p^{\ell/2}/\ell)$.

- Proof: · From eqn. (R): $\ell \cdot \pi(\ell) = p^\ell - \sum_{\substack{k \mid \ell \\ k<\ell}} k \cdot \pi(k)$

$\Rightarrow$ D $\quad k \cdot \pi(k) \leq p^k$.

$\Rightarrow$ D $\quad \ell \cdot \pi(\ell) \geq p^\ell - \sum_{\substack{k \mid \ell \\ k<\ell}} p^k \geq p^\ell - \sum_{k=1}^{\ell/2} p^k$

$$\geq p^\ell - \frac{p}{p-1} \cdot (p^{\ell/2} - 1) \qquad \text{---} \; (1)$$

$\Rightarrow \quad \ell \cdot \pi(\ell) = p^\ell + O(p^{\ell/2})$.

- Moreover, by eqn. (1), $\ell \cdot \pi(\ell) \geq p^\ell - \frac{p^\ell}{2} = p^\ell/2$.

$(\forall\, p \geq 2,\ \ell \geq 1)$ $\square$

- Thus, we pick a <u>random</u> degree-b polynomial in $\mathbb{F}_p[X]$; it is irreducible with probability $\geqslant 1/2b$.

- On repeating $(2b)$-times ; prob. $\geqslant 1-\left(1-\frac{1}{2b}\right)^{2b}$

$$> 1/2.$$