Math

- finite field / galois field = field with finite number of elements (size / order)
  - size always a prime power, i.e. p^k where p is prime, k is positive integer
  - all finite fields of same size are isomorphic to each other and a field cannot contain distinct subfields of the same order, so we can denote all finite fields of order $q = p^k$ as $GF(q)$
  - examples: $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ for prime p

    $\mathbb{Z}_p[x]/(f)$ for some irreducible polynomial f (quotient ring)

    K is a field $\Leftrightarrow$ $K[x]$ is a principal ideal domain
- concretely here we choose to make finite fields of order 2^b (secret tool for later, we like characteristic 2 fields)

  so we generate $GF(2^b)$ using a degree b polynomial in $\mathbb{Z}_2[x]$.
- define a function $S: m \mapsto 1 + mx + m^2x^2 + m^3x^3 + \dots$ (infinite)

  and a n-ary function $S: M = \{m_1 \dots m_n\} \mapsto S(m_1) + \dots + S(m_n)$

  - $S(a) + S(a) = 0 \quad \forall a \in GF(2^b)$
  - $S(\{m_1, m_2\}) + S(\{m_2, m_3\}) = S(m_1) + S(m_2) + S(m_2) + S(m_3) = S(m_1) + S(m_3)$
  - $S(m)$ is like a geometric series with $r = (1 - mx)$ (not really tho)
  - no convergence, but
    - $(1 - mx) \cdot (S(m)) = 1 = (1 - mx)(1 + mx + m^2x^2 + \dots)$

      $= (1 - mx) + mx(1 - mx) + m^2x^2(1 - mx)$

      $= 1 - \cancel{mx} + \cancel{mx} - \cancel{m^2x^2} + \cancel{m^2x^2} - m^3x^3 + \dots$

    - $(1 - m_1x)(1 - m_2x)S(\{m_1, m_2\}) = (1 - m_2x) + (1 - m_1x)$

      $= \cancel{(1 - m_1x)}(1 - m_2x)\cancel{S(m_1)} + (1 - m_1x)\cancel{(1 - m_2x)}\cancel{S(m_2)}$

    - $(1 - m_1x)(1 - m_2x)(1 - m_3x)S(\{m_1, m_2, m_3\}) = (1 - m_2x)(1 - m_3x) + (1 - m_1x)(1 - m_3x) + (1 - m_1x)(1 - m_2x)$

      $= \cancel{(1 - m_1x)}(1 - m_2x)(1 - m_3x)\cancel{S(m_1)} + (1 - m_1x)\cancel{(1 - m_2x)}(1 - m_3x)\cancel{S(m_2)} + (1 - m_1x)(1 - m_2x)\cancel{(1 - m_3x)}\cancel{S(m_3)}$

$$\boxed{\prod_{m_i \in M}(1 - m_i x) \cdot S(M) = \text{polynomial of degree } n-1}$$

Sketches

- if your set is of size 2^b (fits in b bits) and capacity $= c$, sketch can be stored in bc bits (pinsketch)
- create sketch: given $M = [m_1 \dots m_n] \rightarrow$ (odd) syndromes $[s_0 \dots s_{2n-1}]$
  - choose b based on size of elements
  - apply function: $S(M) = S(m_1) + S(m_2) + \dots + S(m_n)$
    $= n + (m_1 + \dots + m_n)x + \dots + (m_1 + \dots + m_n)x^n$
    $= S_0 + S_1 x + S_2 x^2 + S_3 x^3 + \dots$
  - send $S_1, S_3, S_5 \dots S_{2n-1}$

- Merge: given 2 serialized sketches $S(M_a), S(M_b)$
  n must be the same, b must be the same
  merged $S_i = S_{ai} \oplus S_{bi}$ (only necessary for odd ones!)
- Decode: given syndromes $[S_1 \dots S_{2n-1}]$. also need $S_0 = n \rightarrow$ get $S_0 \dots S_{2n}$
  - since we know all S_i are elements of a finite field with characteristic 2, can always compute the even ones:

$$S(M) = \underbrace{n}_{S_0} + \underbrace{(m_1 + \dots + m_n)}_{S_1}x + \underbrace{(m_1^2 + \dots + m_n^2)}_{S_2}x^2 + \dots + \underbrace{(m_1^{2n} + \dots + m_n^{2n})}_{S_n}x^{2n}$$

$$S_2 = m_1^2 + m_2^2 + \dots + m_n^2 = (m_1 + m_2 + \dots + m_n)^2 = S_1^2$$
$$S_4 = m_1^4 + m_2^4 + \dots + m_n^4 = (m_1 + m_2 + \dots + m_n)^4 = S_2^2$$
$$S_6 = m_1^6 + m_2^6 + \dots + m_n^6 = (m_1 + m_2 + \dots + m_n)^6 = S_3^2$$

now you have all of $S(M) = S_0 + S_1 x + \dots + S_{2n} x^{2n}$

- solve for set: given $S_0 \ldots S_{2n} \to$ items $[m_1, \ldots m_n]$

we know that $(1-m_1x)\cdot \ldots \cdot(1-m_nx)\, S(M) =$ $n-1$ deg polynomial P.

unknown polynomial $L = (1-m_1x)(1-m_2x)(1-m_3x)\cdots(1-m_nx)$

degree n. $= l_0 + l_1x + l_2x^2 + \ldots + l_nx^n$ note $l_0 = 1$ is known

$$P = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_{n-1}x^{n-1} + \underline{0}x^n + \ldots + \underline{0}x^{2n}$$

because P has degree $n-1$

$$\left.\begin{aligned}
a^{n+1} &= S_{n+1}l_0 + S_nl_1 + S_{n-1}l_2 + S_{n-2}l_3 + \ldots + S_1l_n = 0\\
a^{n+2} &= S_{n+2}l_0 + S_{n+1}l_1 + S_nl_2 + S_{n-1}l_3 + \cdots + S_2l_n = 0\\
&\vdots\\
a^{2n} &= S_{2n}l_0 + S_{2n-1}l_1 + S_{2n-2}l_2 + S_{2n-3}l_3 + \cdots + S_nl_n = 0
\end{aligned}\right\}\text{system of } n \text{ linear equations}$$

↳ solve for $l_0 + l_1x + l_2x^2 + \ldots + l_nx^n = (1-m_1x)(1-m_2x)\cdots(1-m_nx)$

now you know $l_0 \ldots l_n$, polynomial degree n, must have $\leq n$ roots.

if n roots $\Rightarrow$ unique roots, can solve for $m_1 \ldots m_n$.

otherwise, you need to try again