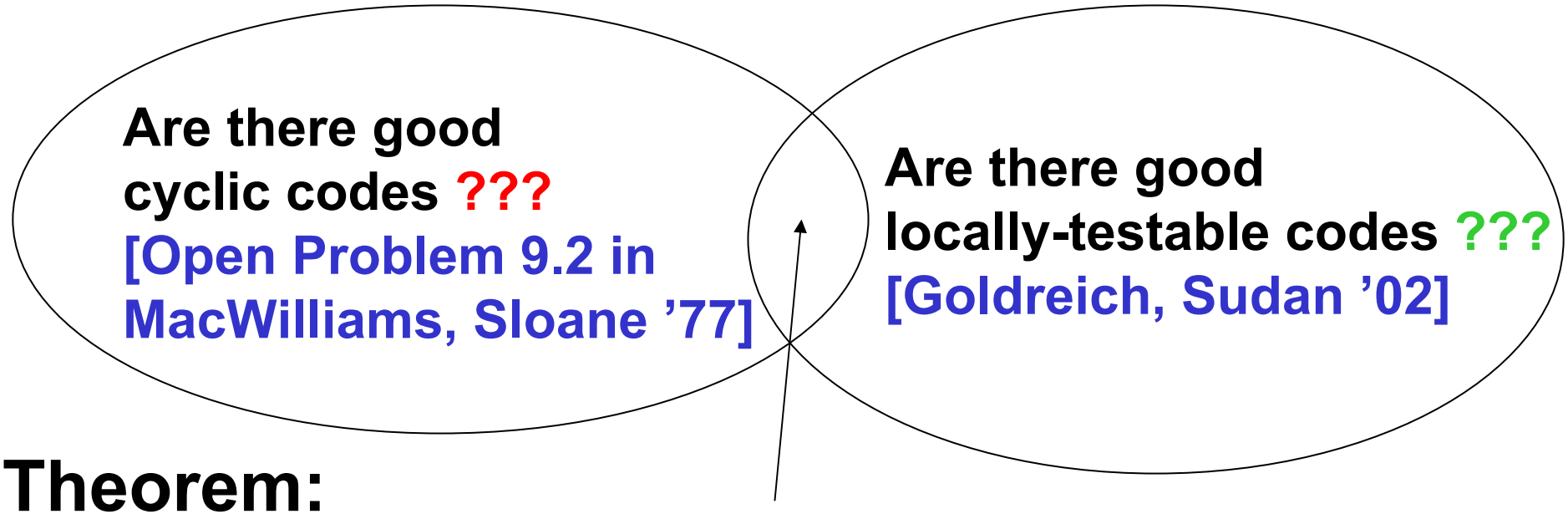
Locally testable cyclic codes

László Babai, Amir Shpilka, Daniel Štefankovič



Theorem:

There are no good families of locally-testable cyclic codes over $\mathbb{F}_q$.

This talk $q = 2$

Linear codes – basic parameters

code C = linear subspace of $\mathbb{F}_q^n$

alphabet size q

block size n

dimension = information length k

minimum weight = distance d

A good family of codes

$n \to \infty$

$k = \Omega(n)$ linear information (const rate)

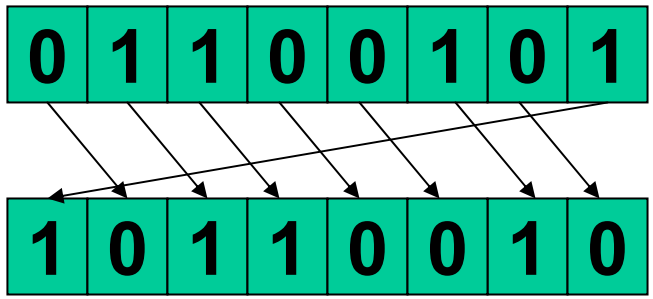
$d = \Omega(n)$ linear distance ($\Omega(n)$ errors corrected)

existence [Shannon'48].

explicit [Justesen'72].

Cyclic codes [Prange'57]

$$(a_0,\ldots,a_{n-1}) \in C \quad \leftrightarrow \quad (a_{n-1},a_0,a_1,\ldots,,a_{n-2}) \in C$$



Why cyclic codes?

- Hardware – shift registers
- Classical codes – BCH, Reed-Solomon
- Theory – principal ideal rings

[MacWilliams,Sloane'77] "Cyclic codes are the most studied of all codes since they are easy to encode and include the important family of BCH codes."

Are there good cyclic codes?

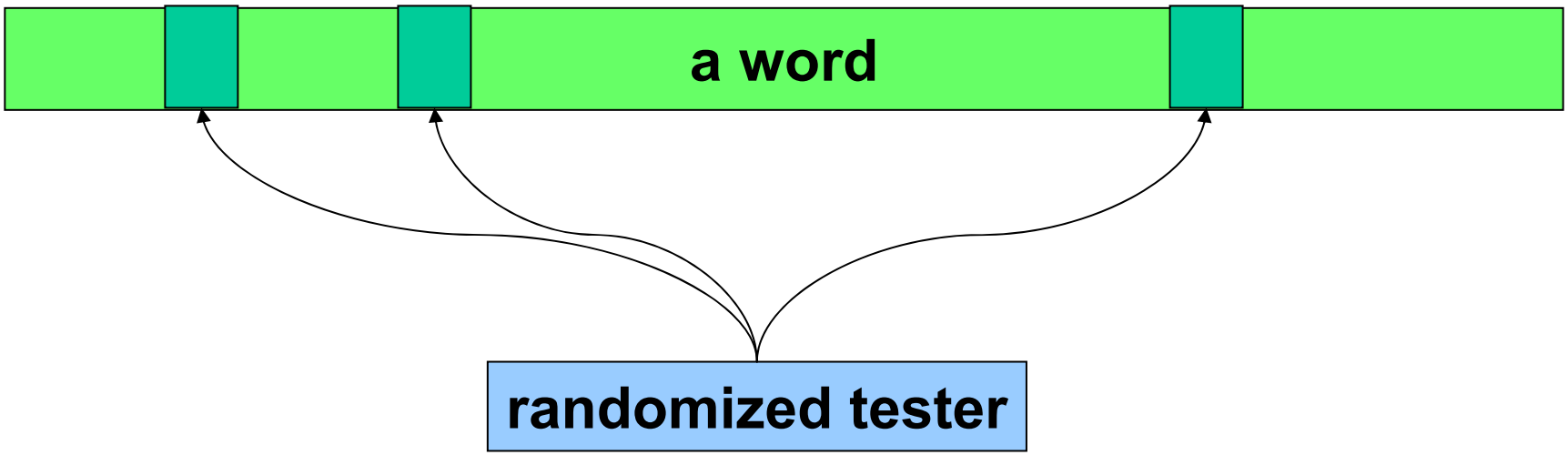
???

[Lin, Weldon '67] BCH codes are not good

[Berman '67] If the largest prime divisor of n is $O(1)$ then the family cannot be good.

[BSS '03] If the largest prime divisor of n is $\leq c\sqrt{\ln n \ln \ln n}$ then the family cannot be good.

Local testability
(context: holographic proofs/PCPs)



check few bits - randomized

codeword	**- surely accepted**
far from all codewords	**- likely rejected**

Holographic proofs/PCPs

[Babai, Fortnow, Lund '91]

polylog bits checked, quasipoly length

[Babai, Fortnow, Levin, Szegedy '91, 20??]

polylog bits checked, nearly linear length

[Arora, Lund, Motwani, Sudan, Szegedy'92]

const bits checked, polynomial length

Locally testable codes

[Friedl, Sudan'95] – local testability formalized

const bits checked, nearly quadratic length

[Goldreich, Sudan'02]

const bits checked, nearly linear length

Clarified PCP ↔ loc. testable codes connection

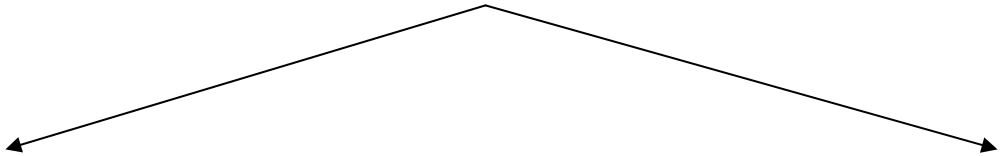
Locally decodable codes

strengthening of local testability

stronger tradeoffs known

[Katz, Trevisan ’00]
[Goldreich, Karloff, Schulman, Trevisan ‘02]
[Deshpande, Jain, Kavitha, Lokam, Radhakrishnan ’02]
[Kerenidis, de Wolf ’03]

Are there good locally testable cyclic codes?



n is smooth

no good cyclic code

[Berman ’67, BSS ‘03]

No local testability assumption needed!

n contains a large prime

no good locally testable cyclic code

Our lower bound proof works against

- **adaptive tester**
- **codeword always accepted**
- **word at distance $\Omega(n)$ rejected with positive probability**

TRADEOFF: If L bits tested then either

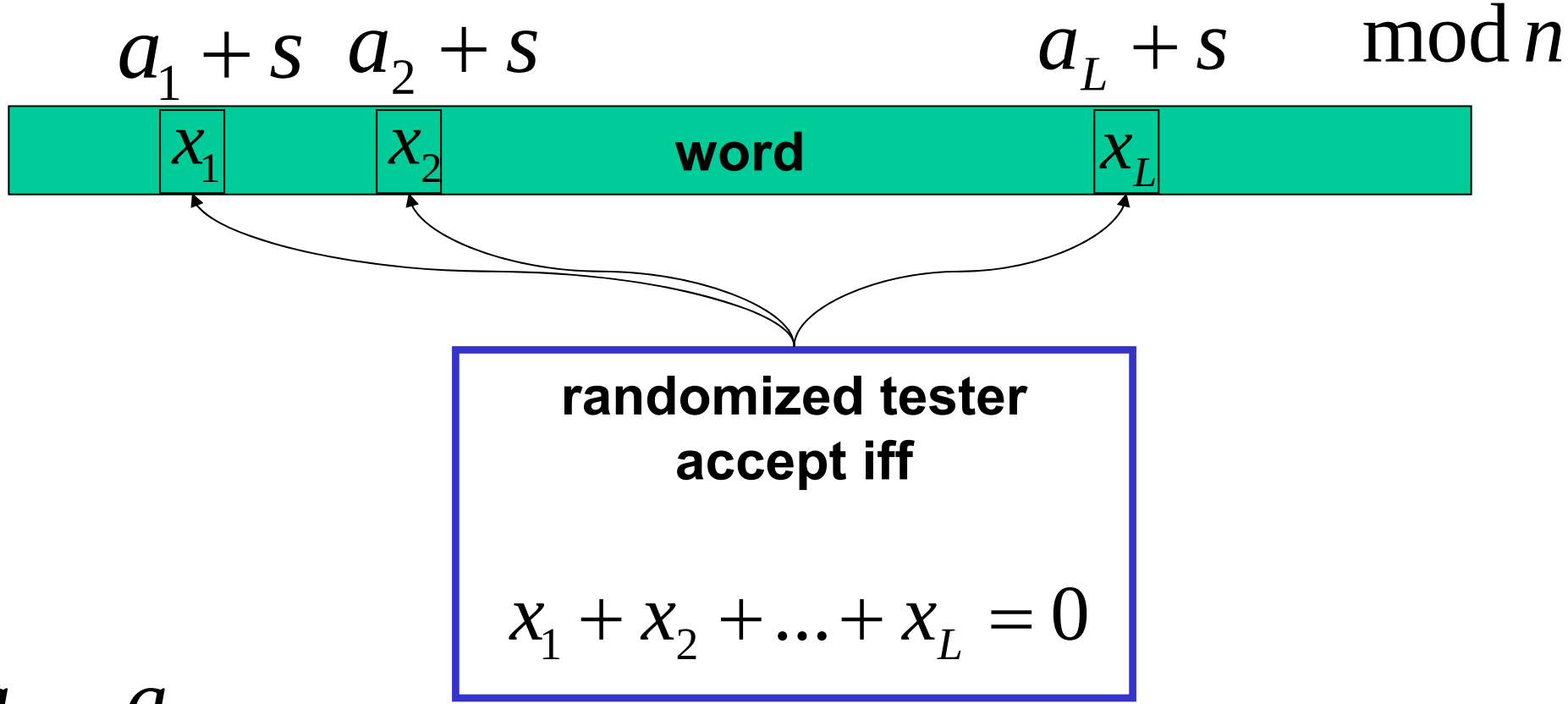
information length $k \leq \dfrac{n}{(\log n)^{1/2L}}$

or

distance $d \leq \dfrac{n}{(\log n)^{1/2}}$

Idea of proof – illustrated

CASE: n prime + cyclic pattern tester



$a_1, \ldots a_L$ **fixed**

s **uniformly random from** $\{0, \ldots, n-1\}$

Method of proof: Diophantine approximation

Dirichlet's Theorem

(simultaneous Diophantine approximation)

For any integer T**, reals** $\alpha_1, \ldots, \alpha_L$

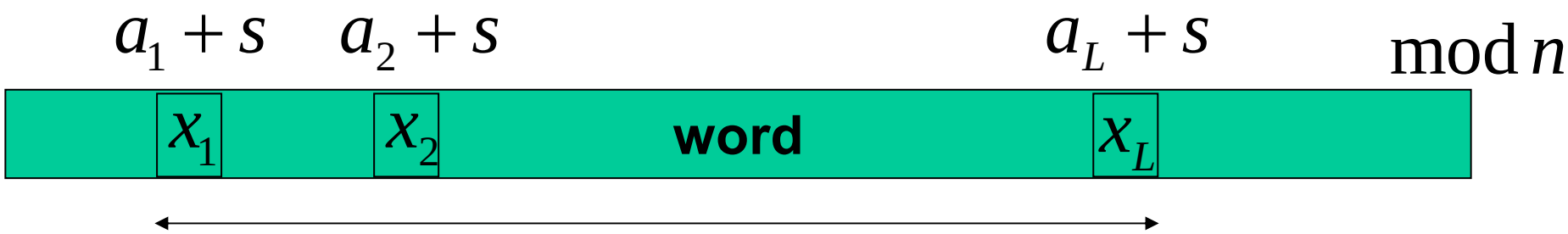
it is possible to simultaneously approximate $\alpha_1, \ldots, \alpha_L$

by rationals $\frac{b_1}{t}, \ldots, \frac{b_L}{t} \quad 0 < t \leq T$

with error bounded by $\frac{1}{tT^{1/L}}$ **:**

$$(\forall i) \quad \left| \alpha_i - \frac{b_i}{t} \right| \leq \frac{1}{tT^{1/L}}$$

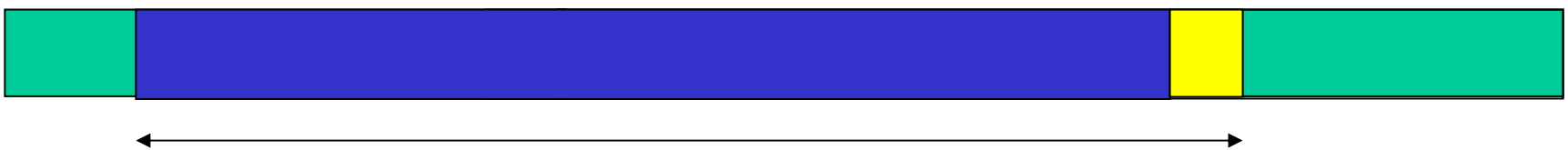
n prime + cyclic pattern tester



"spread" of the tester:

shortest arc which includes an instance of the pattern

determines the codeword



"spread"

dimension $\leq$ spread-1

The trick:

We shrink the spread to $o(n)$ without changing the dimension.

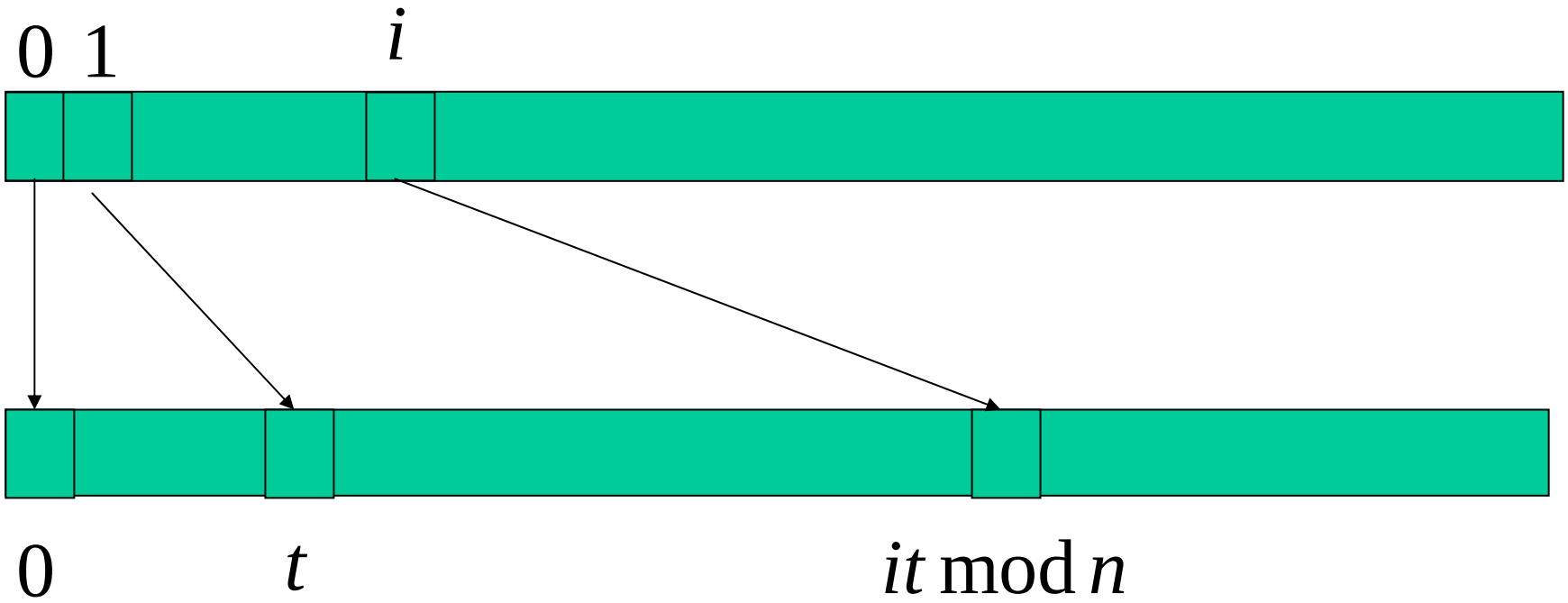
Corollary:

dimension $d = o(n)$

code not good **Q.E.D.**

Q: How to shrink the spread?

A: Stretch the code $\bmod n$ **.**



Stretch factor t $\quad \gcd(t, n) = 1$

New code: cyclic, same dimension

We can even use our old tester! Instead of querying positions

$a_1 + s, \ldots, a_L + s \bmod n$, **query positions** $t(a_1 + s), \ldots, t(a_L + s) \bmod n$

Lemma:

If n is prime then there exists a stretch factor which reduces the spread to

$$2n^{1-1/L}$$

Proof: apply Dirichlet's Theorem to approximating with denominator $\leq n-1$

$$\frac{a_1}{n},\ldots,\frac{a_L}{n}$$

The stretch factor will be the common denominator.

Algebraic machinery for cyclic codes

$$(a_0,\ldots,a_{n-1}) \mapsto f(x) = a_0 + \ldots + a_{n-1}x^{n-1}$$
$$\in \mathbb{F}_2^n \qquad\qquad \in \mathbb{F}_2[x]$$

cyclicity $\longrightarrow \mod(x^n - 1)$

$h(x)$ **: check polynomial of cyclic code** C

$$h(x) \mid x^n - 1$$

$$f(x) \in C \Leftrightarrow (x^n - 1) \mid f(x)h(x)$$

Information length $k = \deg h(x)$

We need to understand divisors of degree $\Omega(n)$ of $x^n - 1$ over $\mathbb{F}_2$.

Factoring $x^n - 1$ over $\mathbb{Z}$

$$x^n - 1 = \prod_{s|n} \Phi_s(x)$$

$\Phi_s(x)$ **cyclotomic polynomial of order s**

$$\Phi_1(x) = x - 1$$
$$\Phi_2(x) = x + 1$$
$$\Phi_3(x) = x^2 + x + 1$$
$$\Phi_4(x) = x^2 + 1$$
$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$
$$\Phi_6(x) = x^2 - x + 1$$
$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$
$$\Phi_8(x) = x^4 + 1$$
$$\Phi_9(x) = x^6 + x^3 + 1$$
$$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$$
$$\Phi_{11}(x) = x^{10} + x^9 + \ldots + x + 1$$
$$\Phi_{12}(x) = x^4 - x^2 + 1$$

$$\Phi_{mp^r}(x) = \Phi_{mp}(x^{p^{r-1}})$$

very sparse,
weight independent of r

$\Phi_s(x)$ **irreducible over** $\mathbb{Z}$
but not over $\mathbb{F}_2$ **(ignore for now)**

If n is smooth (all prime divisors small)

then

$\exists$ **large** r **, small** p**, such that** $p^r \mid n$

We use the sparsity of $\Phi_{mp^r}(x)$
to show

$$\exists \text{ sparse } f(x) \quad \text{s.t.} \quad (x^n - 1) \mid f(x)h(x)$$

small weight — **codeword**

So, code not good. **Q.E.D?**

$\Phi_s(x)$ **irreducible over** $\mathbb{Z}$

but not over $\mathbb{F}_2$ **(don't ignore)**

$$\Phi_{mp^r}(x) = \Phi_{mp}(x^{p^{r-1}})$$

very sparse, weight independent of r

even the $\mathbb{F}_2$ **irreducible factors exhibit similar pattern of sparsity**

So, code not good. **Q.E.D!**

("some" technical details omitted :-)

Are there good cyclic codes?

$n := 2^p - 1$ **Mersenne prime**

Factors of Φ_n **in** $\mathbb{F}_2[x]$ **have degree** p

Conjecture:

Random cyclic code with Mersenne prime block length is good.