

### použitie vyžaduje

- dostatok svedkov
- efektívny prístup k svedkom

pomer kandidátov a svedkov je konštanta

### princíp použitia

- náhodný výber kandidáta plus overenie, či je alebo nie je svedkom
- ak je v množine kandidátov dostatočne veľa svedkov, je pravdepodobnosť toho, že vybratý kandidát je svedok, dostatočná

### aplikovanie

- testovanie prvočíselnosti
- generovanie náhodných prvočísel

malá Fermátová veta

$p \in PRIM$ ,  $a \in Z_p^* = \{d \in Z_p | gcd(a, p) = 1\}$ . Potom  $a^{(p-1)} \pmod p \equiv 1$

veta o čínskych zvyškoch, I. verzia

Nech  $m = m_1 \times \dots \times m_k$ ,  $k \in N - \{0\}$ ,  $gcd(m_i, m_j) = 1$  pre  $i \neq j$ . Potom  
 $r_1 \in Z_{m_1}, \dots, r_k \in Z_{m_k} \rightsquigarrow \exists ! r \in Z_m : r \equiv r_i \pmod{m_i}$

veta o čínskych zvyškoch, II. verzia

Nech  $n = p \times q$ ,  $gcd(p, q) = 1$ . Nech  $\odot_{p,q}, \oplus_{p,q}$  sú operácie nad  $Z_p \times Z_q$ .

$$(a_1, a_2) \oplus_{p,q} (b_1, b_2) = ((a_1 \oplus_{p,q} b_1) \pmod p, (a_2 \oplus_{p,q} b_2) \pmod q)$$

$$(a_1, a_2) \odot_{p,q} (b_1, b_2) = ((a_1 \odot_{p,q} b_1) \pmod p, (a_2 \odot_{p,q} b_2) \pmod q)$$

Potom  $(Z_n, \oplus \pmod p, \odot \pmod q)$  a  $(Z_p \times Z_q, \oplus_{p,q}, \odot_{p,q})$  sú izomorfné.

Lagrange

Pre každú podgrupu  $(H, \circ)$  konečnej grupy  $(A, \circ)$  platí

$$|A| = Index_H(A) \cdot |H| \rightsquigarrow H \circ b = \{h \circ b | h \in H\}$$
$$Index_H(A) = |\{H \circ b | b \in H\}|$$

## svedok pre zložené číslo

- [1.] prvok  $a$  je svedkom pre zložené číslo, ak poskytuje efektívne overenie tohto faktu
- [2.] ľahko rozlíšime, či kandidát je svedok alebo nie
- [3.] množina kandidátov obsahuje dostatočne veľa svedkov

naivný prístup prvočíslo je číslo deliteľné iba jednotkou a samým sebou

deliteľ  $n \notin PRIM \Leftrightarrow a$  delí  $n$  !  $n = p \cdot q$ ,  $p, q$  prvočísla...

$a$  je svedok pre  $n \notin PRIM \Leftrightarrow a^{\frac{n-1}{2}} \bmod n \neq 1$  // malá Fermátová  
výpočet  $a^{p-1} \bmod p$  je založený na iterovanom umocňovaní

$$a^2 \bmod p = a \cdot a \bmod p$$

$$a^{2^k} \bmod p = [(a^{2^{k-1}} \bmod p) \cdot (a^{2^{k-1}} \bmod p)] \bmod p$$

$$\text{nech } b = \sum_{i=1}^k b_i 2^{i-1}; \text{ potom } a^b = a^{b_1 2^0} \cdot a^{b_2 2^1} \cdot \dots \cdot a^{b_k 2^{k-1}}$$

$$a^b \bmod p \rightsquigarrow a_i = a^{2^{i-1}} \bmod p, \prod_{i=1, b_i=1}^k a_i \bmod p$$

zložitosť  $O(\log n)$  násobení nad  $Z_p \rightsquigarrow O((\log n)^3)$  bitových operácií

Carmichaelove čísla:

$\forall a \in \{1, \dots, n-1\}$  platí  $a^{(n-1)} \bmod n = 1$ , ale  $n$  je prvočíslo

veta Nech  $p > 2$  je nepárne. Potom

$$p \text{ je prvočíslo} \Leftrightarrow a^{\frac{(p-1)}{2}} \pmod{p} \in \{1, p-1\} \quad \forall a \in \mathbb{Z}_p - \{0\}$$

veta Pre každé  $n, n \equiv 3 \pmod{4}$ , platí

ak  $n$  je prvočíslo, potom  $a^{(n-1)/2} \pmod{n} \in \{1, n-1\} \quad \forall a \in \{1, \dots, n-1\}$

ak  $n$  je zložené, potom  $a^{(n-1)/2} \pmod{n} \notin \{1, n-1\}$  pre aspoň polovicu prvkov  $a \in \{1, \dots, n-1\}$



**$n \equiv 3 \pmod{4}, a^{(n-1)/2} \pmod{n} \notin \{1, n-1\} \Rightarrow a$  potvrdzuje  $n \notin \text{PRIM}$**

veta Nech  $p > 2$  je nepárne. Potom

$$p \text{ je prvočíslo} \Leftrightarrow a^{\frac{(p-1)}{2}} \pmod{p} \in \{1, p-1\} \quad \forall a \in Z_p - \{0\}$$

$$p = 2p' + 1 \quad \Rightarrow$$

$$\text{MF} \quad \rightsquigarrow \left. \begin{array}{l} a^{p-1} \equiv 1 \pmod{p} \forall a \in Z_p - \{0\} \\ a^{p-1} = a^{2p'} = (a^{p'} - 1)(a^{p'} + 1) + 1 \end{array} \right\} (a^{p'} - 1)(a^{p'} + 1) \equiv 0 \pmod{p}$$

$$a^{\frac{(p-1)}{2}} \pmod{p} \in \{1, p-1\}$$

$$a^{\frac{(p-1)}{2}} \in \{1, p-1\} \forall a \in Z_p - \{0\}; \text{ nech by } p = ab \quad \Leftarrow$$

$$\left. \begin{array}{l} a^{\frac{p-1}{2}} \pmod{p} \in \{1, p-1\} \\ b^{\frac{p-1}{2}} \pmod{p} \in \{1, p-1\} \end{array} \right\} (ab)^{\frac{p-1}{2}} \pmod{p} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \pmod{p} \in \{1, -1\}$$

$$ab = p \rightsquigarrow 0 = p \pmod{p} = p^{\frac{p-1}{2}} \pmod{p} = (ab)^{\frac{p-1}{2}} \pmod{p} \in \{1, -1\}$$

□

**veta** Pre každé  $n, n \equiv 3 \pmod{4}$ , platí

- a. ak  $n$  je **prvočíslo**, potom  $a^{(n-1)/2} \pmod n \in \{1, n-1\} \quad \forall a \in \{1, \dots, n-1\}$
- b. ak  $n$  je **zložené**, potom  $a^{(n-1)/2} \pmod n \notin \{1, n-1\}$  pre aspoň polovicu prvkov  $a \in \underbrace{\{1, \dots, n-1\}}_{A(n-1)}$

**b.** zložené  $n, n \equiv 3 \pmod{4}$

$\hookrightarrow$  rozklad  $A(n-1)$  na **Wit** a **Euler**

$$\text{Wit} = \{a \in A(n-1) \mid a^{(n-1)/2} \pmod n \notin \{1, n-1\}\}$$

$$\text{Euler} = \{a \in A(n-1) \mid a^{(n-1)/2} \pmod n \in \{1, n-1\}\}$$

$\hookrightarrow$  injektívne zobrazenie  $h_b : \text{Euler} \rightsquigarrow \text{Wit}$   
 $b \in \text{Wit}, b^{-1}$  existuje  $h_b(a) = ab \pmod n$

$$a \in \text{Euler}, h_b(a) = ab \pmod n$$

$$(a \cdot b)^{(n-1)/2} \pmod n = (a^{(n-1)/2} \pmod n) \cdot (b^{(n-1)/2} \pmod n) = \pm b^{(n-1)/2} \pmod n$$

$$b \in \text{Wit}, b^{(n-1)/2} \pmod n \notin \{1, n-1\} \rightsquigarrow h_b(a) \in \text{Wit}$$

$$a_1, a_2 \in \text{Euler}, \mathbf{a_1} \neq \mathbf{a_2} \wedge \mathbf{h_b(a_1)} = \mathbf{h_b(a_2)}, \text{ resp. } a_1 b \equiv a_2 b \pmod n.$$

$$\mathbf{a_1} \equiv a_1 b b^{-1} \pmod n \equiv a_2 b b^{-1} \pmod n = \mathbf{a_2} \quad \square$$

$b \in \text{Wit}$ ,  $\mathbf{b}^{-1}$  existuje

$n$  je zložené,  $n = pq$ ,  $\gcd(p, q) = 1$

//  $n = p^i$  ?

$\Leftrightarrow (\mathbf{a} \bmod \mathbf{p}, \mathbf{a} \bmod \mathbf{q})$  jednoznačne reprezentuje  $\mathbf{a} \in \{1, \dots, n - 1\}$

reprezentácii čísel z Euler –  $a^{(n-1)/2} \bmod pq \in \{1, n - 1\}$

ak  $a^{(n-1)/2} = kpq + 1$ , potom  $a^{(n-1)/2} \bmod p \equiv a^{(n-1)/2} \bmod q \equiv 1$ ;

$$a^{(n-1)/2} \rightsquigarrow (1, 1)$$

ak  $a^{(n-1)/2} = kpq + n - 1$ , potom

$$a^{(n-1)/2} \bmod p = (n - 1) \bmod p = (pq - 1) \bmod p = p - 1$$

$$a^{(n-1)/2} \bmod q = (n - 1) \bmod q = (pq - 1) \bmod q = q - 1$$

$$a^{(n-1)/2} \rightsquigarrow (p - 1, q - 1)$$

$b \in \text{Wit} \rightsquigarrow (1, q - 1)$ :

$$(\mathbf{b}^{(n-1)/2} \bmod \mathbf{p}, \mathbf{b}^{(n-1)/2} \bmod \mathbf{q}) = (1^{(n-1)/2} \bmod p, (-1)^{(n-1)/2} \bmod q) = (1, -1)$$

$b \notin \text{Euler}$ , preto  $b \in \text{Wit}$ .

Inverzný prvok k  $b$  je  $b$ :

$$\mathbf{b} \cdot \mathbf{b} = (1, q - 1) \odot (1, q - 1) = (1 \bmod p, (q - 1)(q - 1) \bmod q) = (\mathbf{1}, \mathbf{1})$$

□

(\*)  $a \in \{1, \dots, n-1\}$  je svedok, že nepárne  $n \notin \text{PRIM}$ , ak // chceme odstrániť  $n \equiv 3 \pmod{4}$

- $\gcd(a, n) > 1$  alebo
- $\gcd(a, n) = 1$  a  $a^{(n-1)/2} \pmod{n} \notin \{1, -1\}$

Euclid(a,b)  
if  $b = 0$  then return(a)  
else return(Euclid(b, a mod b))

$O((\log a + b)^3)$

fakt  $n$  zložené, nie Carmichaelovo  $\Rightarrow$  aspoň polovica zo  $Z_n - \{0\}$  potvrdzuje  $n \notin \text{PRIM}$  podľa podmienky (\*)

(\*) Nech  $p > 2$  je prvočíslo s  $\gcd(a, p) = 1$ . Legendrov symbol pre  $a$  a  $p$  je

$$\mathbf{Leg} \left[ \frac{\mathbf{a}}{\mathbf{p}} \right] \begin{cases} 1, & a \text{ je kvadratický zvyšok modulo } p \\ -1, & a \text{ je kvadratický nezvyšok modulo } p \end{cases}$$

fakt Prvočíslo  $p$  s  $\gcd(a, p) = 1 \Rightarrow \mathbf{Leg} \left[ \frac{\mathbf{a}}{\mathbf{p}} \right] = \mathbf{a}^{(p-1)/2} \pmod{p}$

(\*) Nech  $n = p_1^{k_1} p_2^{k_2} \dots p_\ell^{k_\ell}$  je faktorizácia nepárneho  $n \geq 3$ , pričom  $k_j$  sú kladné. Ak  $\gcd(a, n) = 1$ , potom Jacobiho symbol pre  $a, n$  je // faktorizáciu nepoznáme

$$\mathbf{Jac} \left[ \frac{\mathbf{a}}{\mathbf{n}} \right] = \prod_{i=1}^{\ell} \left( \mathbf{Leg} \left[ \frac{\mathbf{a}}{p_i} \right] \right)^{k_i} = \prod_{i=1}^{\ell} \left( a^{(p_i-1)/2} \pmod{p_i} \right)^{k_i}$$

fakt  $a, n$  splňajúce (\*)  $\Rightarrow \mathbf{Jac} \left[ \frac{\mathbf{a}}{\mathbf{n}} \right] \in \{-1, 1\}$

lema Pre nepárne  $n \geq 3$ ,  $a, b$  :

$$\gcd(a, n) = \gcd(b, n) = 1$$

$$1. \text{ Jac } \left[ \frac{ab}{n} \right] = \text{Jac } \left[ \frac{a}{n} \right] \cdot \text{Jac } \left[ \frac{b}{n} \right]$$

$$2. \text{ Jac } \left[ \frac{a}{n} \right] = \text{Jac } \left[ \frac{b}{n} \right] \text{ pre } a \equiv b \pmod{n}$$

$$3. \text{ Jac } \left[ \frac{a}{n} \right] = -1^{\frac{(a-1)(n-1)}{2}} \text{Jac } \left[ \frac{n}{a} \right] \text{ pre } n \text{ nepárne}$$

$$4. \text{ Jac } \left[ \frac{1}{n} \right] = 1, \quad \text{Jac } \left[ \frac{n-1}{n} \right] = (-1)^{(n-1)/2}$$

$$5. \text{ Jac } \left[ \frac{2}{n} \right] = \begin{cases} -1, & \text{pre } n \pmod{8} \in \{3, 5\} \\ 1, & \text{pre } n \pmod{8} \in \{1, 7\} \end{cases}$$

Algoritmus

– rekurzívne volanie zníži aspoň jeden z parametrov aspoň na polovicu  $\Rightarrow$  hĺbka rekurzie  $O(\log n)$

– manipulácia s parametrami je  $O(1)$  aritmetických, resp.  $O((\log(a + n))^2)$  bitových operácií

– čas výpočtu  $\text{Jac } \left[ \frac{a}{n} \right]$  je  $O((\log(a + n))^3)$  binárnych operácií.

$$\begin{aligned} (1.) \quad \text{Jac } \left[ \frac{ab}{n} \right] &= \prod_{i=1}^{\ell} \left( (ab)^{(p_i-1)/2} \pmod{p_i} \right)^{k_i} = \\ &= \prod_{i=1}^{\ell} \left( a^{(p_i-1)/2} \pmod{p_i} \right)^{k_i} \left( b^{(p_i-1)/2} \pmod{p_i} \right)^{k_i} = \\ &= \prod_{i=1}^{\ell} \left( a^{(p_i-1)/2} \pmod{p_i} \right)^{k_i} \prod_{i=1}^{\ell} \left( b^{(p_i-1)/2} \pmod{p_i} \right)^{k_i} \\ &= \text{Jac } \left[ \frac{a}{n} \right] \text{Jac } \left[ \frac{b}{n} \right] \end{aligned}$$

$n \geq 3$  nepárne;  $a \in \{1, \dots, n-1\}$  je Jac-svedok pre  $n \notin \text{PRIM}$ , ak

- $\gcd(a, n) \neq 1$ , alebo
- $\gcd(a, n) = 1$  a  $Jac \left[ \frac{a}{n} \right] \neq a^{(n-1)/2} \pmod n$

**veta** Pre každé nepárne  $n \geq 3$  platí

1. ak  $n$  je *prvočíslo*, potom  $Jac \left[ \frac{a}{n} \right] = Leg \left[ \frac{a}{n} \right] = a^{(n-1)/2} \pmod n$  pre všetky  $a \in \{1, 2, \dots, n-1\}$
2. ak  $n$  je *zložené číslo*, potom  $Jac \left[ \frac{a}{n} \right] \neq a^{(n-1)/2} \pmod n$  pre aspoň polovicu z tých  $a \in \{1, 2, \dots, n-1\}$ , pre ktoré  $\gcd(a, n) = 1$

(2.)  $n \geq 3$  nepárne, množina kandidátov  $Z_n - \{0\}$

$$\begin{aligned} \overline{\text{Wit}}_n &= \{a \in Z_n^* \mid Jac \left[ \frac{a}{n} \right] = a^{(n-1)/2} \pmod n\} \\ \text{Wit}_n &= Z_n^* - \overline{\text{Wit}}_n \end{aligned}$$

$$|\overline{\text{Wit}}_n| \leq |Z_n^*|/2 \implies |\{1, 2, \dots, n-1\} - \overline{\text{Wit}}_n| \geq |\overline{\text{Wit}}_n|$$

chceme  $(\overline{\text{Wit}}_n, \odot_{\text{mod}n})$  je vlastná podgrupa  $(Z_n^*, \odot_{\text{mod}n})$

$$\left. \begin{aligned} \text{Jac} \left[ \frac{ab}{n} \right] &= \text{Jac} \left[ \frac{a}{n} \right] \text{Jac} \left[ \frac{b}{n} \right] = \left( a^{\frac{n-1}{2}} \pmod{n} \right) \left( b^{\frac{n-1}{2}} \pmod{n} \right) \\ &= (ab)^{\frac{n-1}{2}} \pmod{n} \end{aligned} \right\} \Rightarrow ab \in \overline{\text{Wit}}_n$$

◇

chceme existenciu prvku  $a \in Z_n - \overline{\text{Wit}}_n$

$$n = \underbrace{p_1^{i_1}}_q \underbrace{p_2^{i_2} \dots p_k^{i_k}}_m, \geq 1$$

$g$  – generátor cyklickej grupy  $(Z_q^*, \odot_{\text{mod}q})$ . Potom

$$\left. \begin{aligned} a &\equiv g \pmod{q} \\ a &\equiv 1 \pmod{m} \end{aligned} \right\} \mathbf{a} \stackrel{\text{def}}{=} (\mathbf{g}, \mathbf{1}) \in \mathbf{Z}_q \times \mathbf{Z}_m \quad // \text{ resp } g \text{ ak } m = 1$$

$\gcd(a, n) = 1 \Leftrightarrow$  žiadne z prvočísel  $p_1, \dots, p_k$  nedelí  $a$  // chceme  $a \in Z_n^*$

– ak  $p_1$  delí  $a$ :  $a = 0 \pmod{p_1}$  plus  $g \equiv a \pmod{p_1} \Rightarrow$  SPOR:  $g$  je generátor

– ak  $p_r$  delí  $a$   $\left. \begin{array}{l} a = p_r b \\ a = mx + 1 \end{array} \right\} p_r b = mx + 1 = p_r \left(\frac{m}{p_r}\right) x + 1$   
 $\hookrightarrow$  SPOR:  $p_r$  delí 1, pričom  $p_r > 1$

$i_1 = 1, n = p_1 m, \gcd(p_1, m) = 1$  // chceme  $a \notin \overline{\text{Wit}}_n$

$$\begin{aligned} \text{Jac} \left[ \frac{a}{n} \right] &= \text{Jac} \left[ \frac{a}{p_1} \right] \prod_{j=2}^k \left( \text{Jac} \left[ \frac{a}{p_j} \right] \right)^{i_j} \\ a \equiv 1 \pmod{m} &\stackrel{=}{=} \text{Jac} \left[ \frac{a}{p_1} \right] \prod_{j=2}^k \left( \text{Jac} \left[ \frac{1}{p_j} \right] \right)^{i_j} \quad // (\cdot) = 1 \\ &= \text{Jac} \left[ \frac{a}{p_1} \right] = \text{Jac} \left[ \frac{g}{p_1} \right] = \text{Leg} \left[ \frac{g}{p_1} \right] \quad // a = (g, 1) \\ &= -1 \quad // \text{generátor nemôže byť kvadratický zvyšok} \end{aligned}$$

$$\mathbf{a}^{(n-1)/2} \pmod{\mathbf{m}} = (a \pmod{m})^{(n-1)/2} \pmod{m} = 1^{(n-1)/2} \pmod{m} = \mathbf{1}$$

$$a^{(n-1)/2} \pmod{n} = 1 \text{ a } \boxed{-1 = \text{Jac} \left[ \frac{a}{n} \right] \neq \mathbf{a}^{(n-1)/2} \pmod{\mathbf{n}} \text{ pre } i_1 = 1}$$

$i_1 \geq 2$

Nech  $a \in \overline{\text{Wit}}_n$

$\Rightarrow a^{(n-1)/2} \pmod{n} = \text{Jac} \left[ \frac{a}{n} \right] \in \{1, -1\} \Rightarrow a^{(n-1)} \equiv 1 \pmod{n}$

// chceme  $a \notin \overline{\text{Wit}}$

$$g \equiv a \pmod{q}, \quad n = p_1^{i_1} m = qm$$

$$1 = a^{n-1} \pmod{n} = a^{n-1} \pmod{q} = (a \pmod{q})^{n-1} \pmod{q} = g^{n-1} \pmod{q}$$

$g$  je generátor cyklickej grupy, jeho rád  $|Z_q^*|$  delí  $n - 1$

$Z_q^* = \{x \in Z_q \mid p_1 \text{ nedelí } x\}$ .

$$|Z_q^*| = |Z_q| - \underbrace{\frac{|Z_q|}{p_1}}_{\text{deliteľné } p_1} = p_1^{i_1} - p_1^{i_1-1} = p_1(p_1^{i_1-1} - p_1^{i_1-2})$$

$$\left. \begin{array}{l} p_1 \text{ delí } |Z_q^*|, \quad |Z_q^*| \text{ delí } n - 1 \\ p_1 \text{ delí } n = p_1^{i_1} m \end{array} \right\} \implies p_1 \text{ delí } n, n - 1$$

SPOR  $\square$

## Solovay-Strassen

//vstupom je nepárne  $n \geq 3$

vygeneruj náhodne  $a \in \{1, 2, \dots, n - 1\}$

vypočítaj  $\gcd(a, n)$

$O((\log n)^3)$

if  $\gcd(a, n) \neq 1$  then return( $n \notin \text{PRIM}$ )

$J \leftarrow \text{Jac} \left[ \frac{a}{n} \right]; A \leftarrow a^{(n-1)/2} \pmod n$

$O((\log n)^3)$

if  $J = A$

then return( $n \in \text{PRIM}$ )

else return( $n \notin \text{PRIM}$ )

generovanie prvočísla:  $\text{PrimGen}(\ell, k)$  vstupom je dĺžka prvočísla  $\ell$  a počet opakovaní testov  $k$

$2\ell^2$  pokusov:

– náhodná postupnosť  $a_1, a_2, \dots, a_{\ell-2}$  bitov

–  $n \leftarrow 2^{\ell-1} + \sum_{i=1}^{\ell-2} a_i 2^i + 1$

–  $k$  nezávislých testov Solovay-Strassen

čas  $O(k \cdot \ell^2 \cdot \ell^3)$

nevygeneroval prvočíslo, resp. číslo, o ktorom by dokázal, že je zložené

$$\begin{aligned} \Pr[\text{náhodné } n \text{ dĺžky } \ell \text{ JE prvočíslo}] &\geq \frac{1}{\ln n} > \frac{1}{2\ell} \\ \Leftrightarrow \Pr[\text{NIE JE prvočíslo}] &\leq \left(1 - \frac{1}{2\ell}\right) \end{aligned}$$

$$\Pr[\ell \text{ krát Solovay-Strassen dokáže, že zložené } n \notin \text{PRIM}] = w_\ell \geq 1 - 1/2^\ell$$

$$\text{Prob}[\text{PrimGen}(\ell, \ell) = \text{"nenašiel"}] < \left(\left(1 - \frac{1}{2\ell}\right) w_\ell\right)^{2\ell^2} < \left(1 - \frac{1}{2\ell}\right)^{2\ell^2} < e^{-\ell}$$

vygenerované "prvočíslo" je zložené

$p_i$  pravdepodobnosť toho, že v  $i$ -tom behu,  $i \in 1, \dots, 2\ell^2$ , dáme na výstup ako prvočíslo číslo, ktoré je v skutočnosti zložené.

$$\begin{aligned}
 - p_1 &< \left(1 - \frac{1}{2\ell}\right) \cdot \frac{1}{2^\ell} \\
 - p_i &\leq \left[\left(1 - \frac{1}{2\ell}\right) w_\ell\right]^{i-1} \left(1 - \frac{1}{2\ell}\right) \cdot \frac{1}{2^\ell} = \left(1 - \frac{1}{2\ell}\right)^i w_\ell \frac{1}{2^\ell}
 \end{aligned}$$

$$\begin{aligned}
 Pr[chyba(\ell, \ell)] &\leq p_1 + \sum_{j=2}^{2\ell^2} p_j \leq \left(1 - \frac{1}{2\ell}\right) \cdot \frac{1}{2^\ell} + \sum_{j=2}^{2\ell^2} \left(1 - \frac{1}{2\ell}\right)^j w_\ell^{j-1} \frac{1}{2^\ell} \leq \\
 &\leq \left(1 - \frac{1}{2\ell}\right) \cdot \frac{1}{2^\ell} \left[ \sum_{j=1}^{2\ell^2-1} \left(1 - \frac{1}{2\ell}\right)^j w_\ell^{j-1} + 1 \right] \\
 &\leq \left(1 - \frac{1}{2\ell}\right) \cdot \frac{1}{2^\ell} \left[ \sum_{j=1}^{2\ell^2-1} \underbrace{\left(1 - \frac{1}{2\ell}\right)^j}_{<2} + 1 \right] \\
 &< \left(1 - \frac{1}{2\ell}\right) \cdot \frac{1}{2^\ell} 2\ell^2 \leq \frac{\ell^2}{2^{\ell-1}}
 \end{aligned}$$