puting f_{pm} are necessarily of exponential size (thus, removing the negation gate increases dramatically the circuit size necessary to compute f_{pm}). This also shows that giving an exponential lower bound for a monotone circuit family deciding a language in NP is not enough to show the separation of P and NP (see theorem 6.4.8).

One final observation is that perfect matching is not known to be complete for any natural complexity class.

7.1.2 Primality testing

We present the Rabin-Miller randomized algorithm for primality testing. Although a polytime (deterministic) algorithm for primality is now known (see [MA04]), randomized algorithms[1] are simpler and more efficient, and therefore still used in practice.

Algorithm 7.1.2 (Rabin-Miller)
On input p:
1. If p is even, accept if $p = 2$; otherwise, reject.
2. Select randomly a non-zero a in $\mathbb{Z}_p$.
3. Compute $a^{(p-1)} \pmod p$ and reject if $\neq 1$.
4. Let $(p-1) = st$ where s is odd and $t = 2^h$.
5. Compute the sequence $a^{s\cdot 2^0}, a^{s\cdot 2^1}, a^{s\cdot 2^2}, \dots, a^{s\cdot 2^h} \pmod p$.
6. If some element of this sequence is not 1,
find the last element that is not 1,
and reject if that element is not -1.
7. Accept.

We say that a is a *witness* (of compositness) for p if the algorithm rejects on a.

Theorem 7.1.3 *If p is a prime then the Rabin-Miller algorithm accepts it; if p is composite, then the algorithm rejects it with probability $\geq \frac{1}{2}$.*

Proof: We show first that if p is prime, no witness exists, and so no branch of the algorithm rejects. If a were a stage 3 witness, $a^{(p-1)} \neq 1 \pmod p$ then Fermat's little theorem would imply that p is composite. If a were a stage 6 witness, some b exists in $\mathbb{Z}_p$, where $b \neq \pm 1 \pmod p$ and $b^2 = 1$

[1] In fact it was the randomized test for primality that stirred interest in randomized computation in the late 1970's. Historically, the first randomized algorithm for primality was given by [SS77]; a nice exposition of this algorithm can be found in [Pap94, §11.1].

(mod p). Therefore, $(b^2-1)=0 \pmod p$. Factoring, we obtain that

$$(b-1)(b+1)=0 \pmod p$$

which implies that p divides $(b-1)(b+1)$. But because $b \neq \pm 1 \pmod p$, both $(b-1)$ and $(b+1)$ are strictly between 0 and p. But that contradicts that $p|(b-1)(b+1)$, because p is a prime, so to divide the RHS it has to be a factor of the RHS, but both numbers are smaller than it.

We now show that if p is an odd composite number and a non-zero a is selected randomly in $\mathbb{Z}_p$, then $\Pr[a \text{ is a witness}] \geq \frac{1}{2}$.

For every nonwitness, the sequence computed in stage 5 is either all 1s or contains a -1 at some position, followed by 1s. So, for example, 1 is a nonwitness of the first kind and -1 is a nonwitness of the second kind because s is odd and $(-1)^{s\cdot 2^0}=-1 \pmod p$ and $(-1)^{s\cdot 2^1}=1 \pmod p$.

Among all nonwitnesses of the second kind, find a nonwitness for which the -1 appears in the largest position in the sequence. Let x be such a nonwitness and let j be the position of -1 in its sequence, where the positions are numbered starting at 0. Hence $x^{s\cdot 2^j}=-1 \pmod p$ (and $x^{s\cdot 2^{j+1}}=1 \pmod p$).

Because p is composite, either p is the power of a prime or we can write p as the product of q and r, two numbers that are co-prime. This yields two cases.

Case 1. Suppose that $p=q^e$ where q is prime and $e>1$. Let $t=1+q^{e-1}$. From the binomial expansion of t^p we obtain:

$$t^p=(1+q^{e-1})^p=1+pq^{e-1}+\sum_{l=2}^{p}\binom{p}{l}(q^{e-1})^l \tag{7.1}$$

which is congruent to 1 (mod p). Hence t is a stage 3 witness because, if $t^{p-1}=1 \pmod p$, then $t^p=t \pmod p$, which from the observation about (7.1) is not possible. We use this one witness to get many others. If d is a (stage 3) nonwitness, we have $d^{p-1}=1 \pmod p$, but then $dt \pmod p$ is a witness. Moreover, if d_1,d_2 are distinct nonwitnesses, then $d_1t \neq d_2t \pmod p$. Otherwise,

$$d_1=d_1\cdot t\cdot t^{p-1}=d_2\cdot t\cdot t^{p-1}=d_2 \pmod p.$$

Thus the number of (stage 3) witnesses must be at least as large as the number of nonwitnesses.

Case 2. By the CRT there exists $t\in\mathbb{Z}_p$ such that

$$\begin{matrix} t=x \pmod q \\ t=1 \pmod r \end{matrix} \quad\Rightarrow\quad \begin{matrix} t^{s\cdot 2^j}=-1 \pmod q \\ t^{s\cdot 2^j}=1 \pmod r \end{matrix}$$

Hence t is a witness because $t^{s\cdot 2^j} \neq \pm 1 \pmod p$ (see footnote [2]) but $t^{s\cdot 2^{j+1}} = 1 \pmod p$. Now that we have one witness, we can get many more, and show that $dt \pmod p$ is a unique witness for each nonwitness d by making two observations.

First, $d^{s\cdot 2^j} = \pm 1 \pmod p$ and $d^{s\cdot 2^{j+1}} = 1 \pmod p$ owing to the way that j was chosen. Therefore $dt \pmod p$ is a witness because $(dt)^{s\cdot 2^j} \neq \pm 1 \pmod p$ and $(dt)^{s\cdot 2^{j+1}} = 1 \pmod p$.

Second, if d_1 and d_2 are distinct nonwitnesses, $d_1 t \neq d_2 t \pmod p$. The reason is that $t^{s\cdot 2^{j+1}} = 1 \pmod p$. Hence $t \cdot t^{s\cdot 2^{j+1}-1} = 1 \pmod p$. Therefore, if $d_1 t = d_2 t \pmod p$, then

$$d_1 = d_1 t \cdot t^{s\cdot 2^{j+1}-1} = d_2 t \cdot t^{s\cdot 2^{j+1}-1} = d_2 \pmod p$$

Thus in case 2., as well, the number of witnesses must be at least as large as the number of nonwitnesses. □

Note that by running the algorithm k times on independently chosen a, we can make sure that it rejects a composite with probability $\geq (1 - \frac{1}{2^k})$ (it will always accept a prime with probability 1). Thus, for $k = 100$ the probability of error, i.e., of a false positive, is negligable.

Thus we have a Monte Carlo algorithm for composites, and therefore $\textsc{Primes} = \{(n)_b | n \text{ is primes}\} \in$ co-RP. Here $(n)_b$ denotes the binary encoding of the number n; see section 7.2 for a definition of co-RP.

7.1.3 Pattern matching

In this section we design a randomized algorithm for pattern matching. Consider the set of strings over $\{0,1\}$, and let $M : \{0,1\} \longrightarrow M_{2\times 2}(\mathbb{Z})$, that is, M is a map from strings to 2×2 matrices over the integers ($\mathbb{Z}$) defined as follows:

$$M(\varepsilon) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$M(0) = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$
$$M(1) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

[2] To see why $t^{s\cdot 2^j} \neq \pm 1 \pmod p$ observe the following: suppose that $a = -1 \pmod q$ and $a = 1 \pmod r$, where $\gcd(q,r) = 1$. Suppose that $p = qr | (a+1)$, then $q|(a+1)$ and $r|(a+1)$, and since $r|(a-1)$ as well, it follows that $r|[(a+1)-(a-1)]$, so $r|2$, so $r = 2$, so p must be even, which is not possible since we deal with even p's in line 1 of the algorithm.