# Notes on **Sha1-Prefix**'s Probabilities

Ștefan Vargyas

**stvar@yahoo.com**

Jul 15, 2019

## 1 The Sha1-Prefix Program

**Sha1-Prefix** is a solution program to the following *SHA1 prefix problem*:

> Given an input UTF-8 string and a *difficulty* number $n \in \mathbb{N}$ with $1 \leq n \leq 9$, do find an UTF-8 string that appended to the input string would produce a SHA1 digest of which hexadecimal representation has its leftmost $n$ digits all equal to $0$.

**Sha1-Prefix** is structured on two tiers:

- `sha1-prefix` — obtained from `sha1-prefix.c` and a few other source files — is the main program tackling the core of the SHA1 prefix problem. It gets the input string (not necessarily UTF-8) from `stdin` or from a named file and the difficulty number as a command line argument. `sha1-prefix` will run until it finds the first suffix string that satisfies the specified prefix condition. It can be told to terminate cleanly the execution when signaled with `SIGHUP` if '`-e|--sighup-exits`' was passed on the invoking command line.

- `sha1-prefix.sh` is a quite involved `bash` shell script that drives the main program's execution. The shell script's main use case is that of running `sha1-prefix` in series controlled by time outs.

Bellow we will present simple theoretical arguments that founds the approach taken. Under reasonably acceptable assumptions, we show that running `sha-prefix` in series increases **Sha1-Prefix**'s probability of success producing required outcome.

## 2 Mathematical Evaluations

The basic theoretical assumption we're considering hereafter is that successive runs of `sha1-prefix` by `sha1-prefix.sh` are to be modeled as Bernoulli trials **[1]** with constant or, by case, non-constant probability of success.

**1 Fact.** *If the random variable $X$ follows the binomial distribution with parameters $n \in \mathbb{N}^*$ and $0 \leq p \leq 1$, then the probability of getting* at least one success *in $n$ trials is given by $1 - (1 - p)^n$.*

*Proof.* As per **[2]**, the probability of exactly $k$ successes in $n$ trials is given by:

$$\Pr(X = k) = \binom{n}{k} p^k (1-p)^{n-k}$$

Then follows easily that:

$$\begin{aligned}
\Pr(X \geq 1) &= 1 - \Pr(X < 1) \\
&= 1 - \Pr(X = 0) \\
&= 1 - \binom{n}{0} p^0 (1-p)^{n-0} \\
&= 1 - (1-p)^n
\end{aligned}$$

□

**2 Fact.** *If $0 < p < 1$, for $B_n \stackrel{\text{def}}{=} 1 - (1-p)^n$, it holds true that $p < B_n < B_{n+1}$, for all $n \in \mathbb{N}^*$.*

*Proof.* We have that:

$$\begin{aligned}
0 < p < 1 &\implies 0 < 1 - p < 1 \\
&\implies (1-p)^{n-1} < 1 \\
&\implies (1-p)^n < 1 - p \\
&\implies p < B_n
\end{aligned}$$

Moreover:

$$\begin{aligned}
0 < p < 1 &\implies 0 < 1 - p < 1 \\
&\implies (1-p)^{n+1} < (1-p)^n \\
&\implies B_n < B_{n+1}
\end{aligned}$$

□

**3 Fact.** *If the random variable $X$ follows the Poisson's binomial distribution with parameters $n \in \mathbb{N}^*$ and $0 \leq p_i \leq 1$, for $1 \leq i \leq n$, then the probability of getting* at least one success *in $n$ trials is given by $1 - \prod_{i=1}^{n}(1 - p_i)$.*

*Proof.* As per **[3]**, the probability of exactly $0$ successes in $n$ trials is given by:

$$\Pr(X = 0) = \prod_{i=1}^{n}(1 - p_i)$$

Then:

$$\begin{aligned}
\Pr(X \geq 1) &= 1 - \Pr(X < 1) \\
&= 1 - \Pr(X = 0) \\
&= 1 - \prod_{i=1}^{n}(1 - p_i)
\end{aligned}$$

□

**4 Fact.** *If* $0 < p_i < 1$ *for all* $i \in \mathbb{N}$, $1 \leq i \leq n$, *for* $P_n \stackrel{\text{def}}{=} 1 - \prod_{i=1}^{n}(1 - p_i)$, *it holds true that* $p_i < P_n < P_{n+1}$, *for all* $i \in \mathbb{N}$, $1 \leq i \leq n$, *and* $n \in \mathbb{N}^*$.

*Proof.* For arbitrary but fixed $i \in \mathbb{N}$, $1 \leq i \leq n$, we have that:

$$
\begin{aligned}
0 < p_i < 1 &\implies 0 < 1 - p_i < 1 \\
&\implies \prod_{k=1}^{n}(1 - p_k) < 1 - p_i \\
&\implies p_i < P_n
\end{aligned}
$$

Moreover:

$$
\begin{aligned}
0 < p_i < 1 &\implies 0 < 1 - p_i < 1 \\
&\implies \prod_{k=1}^{n+1}(1 - p_k) = \left(\prod_{k=1}^{n}(1 - p_k)\right) \cdot (1 - p_{n+1}) < \prod_{k=1}^{n}(1 - p_k) \\
&\implies P_n < P_{n+1}
\end{aligned}
$$

□

# References


**[1]** Bernoulli Trial

https://en.wikipedia.org/wiki/Bernoulli_trial

**[2]** Binomial Distribution

https://en.wikipedia.org/wiki/Binomial_distribution

**[3]** Poisson Binomial Distribution

https://en.wikipedia.org/wiki/Poisson_binomial_distribution



Copyright © 2019 **Ştefan Vargyas**

This file is part of **Sha1-Prefix**.

**Sha1-Prefix** is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

**Sha1-Prefix** is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with **Sha1-Prefix**. If not, see http://www.gnu.org/licenses/.