On the Expressibility of Stochastic Switching Circuits

Hongchao Zhou
Department of Electrical Engineering
California Institute of Technology
Pasadena, CA 91125, USA
hzhou@caltech.edu

Jehoshua Bruck
Department of Electrical Engineering
California Institute of Technology
Pasadena, CA 91125, USA
bruck@caltech.edu

***Abstract*— Stochastic switching circuits are relay circuits that consist of stochastic switches (that we call pswitches). We study the expressive power of these circuits; in particular, we address the following basic question: given an arbitrary integer q, and a pswitch set $\{\frac{1}{q}, \frac{2}{q}, ..., \frac{q-1}{q}\}$, can we realize any rational probability with denominator q^n (for arbitrary n) by a simple series-parallel stochastic switching circuit? In this paper, we generalized previous results and prove that when q is a multiple of 2 or 3 the answer is positive. We also show that when q is a prime number the answer is negative. In addition, we propose a greedy algorithm to realize desired reachable probabilities, and thousands of experiments show that this algorithm can achieve almost optimal size. Finally, we prove that any desired probability can be approximated well by a linear size circuit.**

I. Introduction

Claude Shannon, in his Master's thesis [1], provided the foundation of modern digital circuit design by demonstrating that Boolean algebra can be used to synthesize and simplify switching relay circuits. By replacing deterministic switches with probabilistic switches (pswitches), a new concept called stochastic switching circuit was proposed in [2]. The study of stochastic switching circuits may enhance our understanding of natural systems and help incorporate randomness in engineering system design [3].

A stochastic switching circuit with two terminals can be constructed by composing pswitches, where each pswitch is closed with some probability. The set of possible pswitch closure probabilities from which a circuit is constructed will be referred to as the pswitch set S. We use $P(C)$ to denote the probability that the two terminals of a circuit C are connected, called as the probability of C. Some probability x can be realized iff there exists a circuit C such that $x = P(C)$.

Similarly to resistor circuits [4], connecting a single terminal of a switching circuit C_1 (with probability p_1) to one terminal of C_2 (with probability p_2) places them in series, such that the probability of the resulting circuit is $p_1 \cdot p_2$. Connecting both terminals of two switching circuits C_1 and C_2 places them in parallel, such that the probability of the resulting circuit is $1 - (1 - p_1)(1 - p_2) = p_1 + p_2 - p_1p_2$. In this paper, we focus on simple series-parallel (ssp) switching circuits. An ssp circuit is either: (1) a single pswitch, or (2) a ssp circuit with an additional pswitch added in series or parallel.

Shannon proved that every Boolean function can be realized by a switching relay circuit. It is natural for us to ask: if we replace deterministic switches with pswitches closed with probability $p \in \{\frac{1}{q}, \frac{2}{q}, ..., \frac{q-1}{q}\}$ where $q \in N$, can we realize all rational $\frac{a}{q^n}$ $(0 < a < q^n)$ with a bounded number of pswitches. Also, how many pswitches are sufficient? Wilhelm and Bruck [2] proved that if $q = 2$ or $q = 3$, all rational $\frac{a}{q^n}$ with $0 < a < q^n$ can be realized with at most n pswitches, which is optimal. They also showed that if $q = 4$, all rational $\frac{a}{q^n}$ with $0 < a < q^n$ can be realized with at most $2n - 1$ pswitches. In this paper, we generalize these results as follows:

- If q is an even number, all rational $\frac{a}{q^n}$ with $0 < a < q^n$ can be realized with at most $\lceil \log_2 q \rceil (n-1)+1$ pswitches.
- If q is a multiple of 3, all rational $\frac{a}{q^n}$ with $0 < a < q^n$ can be realized with at most $\lceil \log_3 q \rceil (n-1)+1$ pswitches.

However, given a pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, ..., \frac{q-1}{q}\}$ with q not a multiple of 2 or 3, then not all $\frac{a}{q^n}$ with $0 < a < q^n$ can be realized, even with an unlimited number of pswitches. In this paper, we will show that if q is a prime number greater than 3, there exists at least one rational $\frac{a}{q^n}$ with $0 < a < q^n$ that cannot be realized with ssp circuits. Experiments show that this conclusion is true when extending q to multiples of 2 or 3.

In order to realize desired probabilities with as a few as possible pswitches, Greedy Backward Algorithm (GBA) is proposed with the following characteristics: (1) Given a pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, ..., \frac{q-1}{q}\}$ with q a multiple of 2 or 3, all $\frac{a}{q^n}$ with $0 < a < q^n$ can be realized with GBA. (2) Statistically, the size of the circuits realized by GBA is close to optimal size, where we say one circuit is optimal if and only if the corresponding probability cannot be realized with less pswitches.

In the case that q is a prime number greater than 3, or in the case that the desired probability is not rational (such as $\frac{\sqrt{2}}{2}$), it is possible that the desired probability cannot be realized. However, can we use an ssp circuit to get a good approximation of the desired probability? The answer is yes and is given by:

- If q is an integer greater than one, for all desired probability p $(0 < p < 1)$, there exists a circuit C with at most $2n - 1$ pswitches such that $|P(C) - p| \leq \frac{1}{2q^n}$.

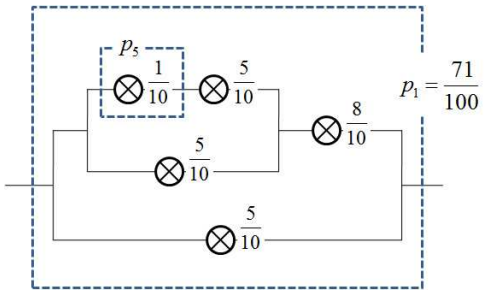


Fig. 1. This circuit realizes $\frac{71}{100}$ for a given pswitch set $S = \{\frac{1}{10}, \frac{2}{10}, ..., \frac{9}{10}\}$, using Algorithm 1.

The remainder of this paper is organized as follows. In Section II, we discuss the case that q is a multiple of 2 or 3. Section III proves that if q is prime number larger than 3, there exists a rational $\frac{a}{q^n}$ that cannot be realized with ssp circuits. Experiments show that it is true for all q not a multiple of 2 or 3. Then, Greedy Backward Algorithm is proposed to realize desired probabilities with good performance, as descried in Section IV. Finally, we show that an approximate rational with small enough error can be realized with a bounded number of pswitches, in Section V.

II. q IS A MULTIPLE OF 2 OR 3

In this section, we first consider the case that q is an even number for a given pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, ..., \frac{q-1}{q}\}$. We will show that using the following backward algorithm for even q, all rational $\frac{a}{q^n}$ $(0 < a < q^n)$ can be realized with a bounded number of pswitches.

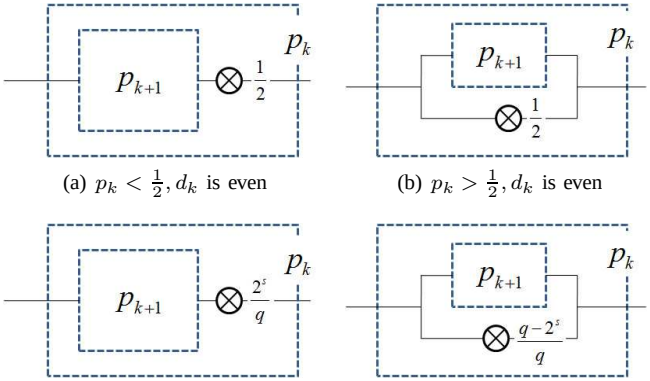
The basic idea of the backward algorithm is to build the circuit last-pswitch first. If we want to realize a rational p_1, we can find another rational p_2 such that if p_2 can be realized, then p_1 can be realized by adding a single pswitch x to p_2 in series or parallel. So, we can insert the pswitch x as the last pswitch and try to realize p_2 instead of p_1. We continue this process recursively until for some m the rational p_m can be realized with a single pswitch. Then, the circuit realizing p_1 is constructed. The detailed algorithm to construct a circuit C to realize $p_1 = \frac{a}{q^n}$ for an even q is described in Algorithm 1. See Fig. 1 as an example.

Theorem 1. *Given a pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, ...\frac{q-1}{q}\}$, if q is even, then Algorithm 1 realizes any rational $\frac{a}{q^n}$ such that $0 < a < q^n$ with at most $\lceil \log_2 q \rceil (n-1) + 1$ pswitches.*

Proof: Since q is even, it can be written as $2^c t$ with odd t. In the following proof, we will show that there exists a stage m such that $p_m \in S$, i.e. p_m can be realized with a single pswitch. We have three steps to prove this:

(1) Step 1: Let $l = \max(s+1, n)$, then for each stage k, the probability p_k can be written as $\frac{a_k}{q^l}$.

This can be proved by induction. When $k = 1$, we have $p_1 = \frac{a}{q^n} = \frac{a_1}{q^l}$, so the statement is true. Assume $p_k = \frac{a_k}{q^l}$ with $0 \le p_k \le 1$. Then, p_{k+1} can be written as $\frac{a_{k+1}}{q^l}$ with $0 < p_{k+1} \le 1$, which can be proved case by case, see Fig. 2. Here we do not prove this for detail.



(a) $p_k < \frac{1}{2}, d_k$ is even (b) $p_k > \frac{1}{2}, d_k$ is even

(c) $p_k < \frac{1}{2}, d_k$ is odd (d) $p_k > \frac{1}{2}, d_k$ is odd

Fig. 2. The way to find p_{k+1} from p_k when q is an even number, where $s = \lfloor \log_2 q \rfloor$.

(2) Step 2: in this step, we write all p_k as $\frac{a_k}{q^l}$, and investigate how a_k varies with k. We show that a_{k+1} and a_k have the following relations:

(a) If $a_k = b_k 2^x t^y$ with $0 \le x < c(l-1), 0 \le y \le (l-1)$ and b_k is odd, then a_{k+1} can be written as $a_{k+1} = b_{k+1} 2^{x+\delta x} t^y$ with $\delta x \ge 1$ and b_{k+1} is odd.

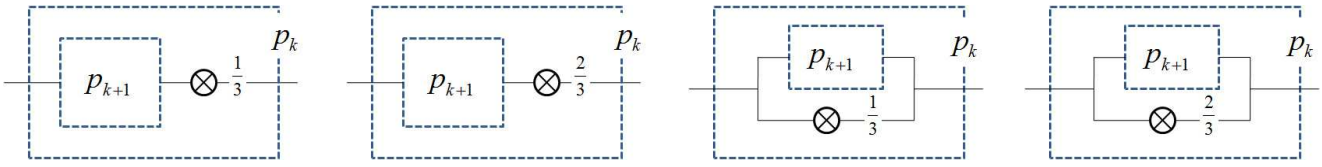
When $a_k = b_k 2^x t^y$ with $0 \le x < c(l-1), 0 \le y \le (l-1)$ and b_k is odd, we have $a_k \mod 2^{c(l-1)} \neq 0$, so d_k is even.

If $p_k < \frac{1}{2}$ (see Fig. 2(a)), we have

$$p_{k+1} = 2p_k = \frac{2a_k}{q^l} = \frac{a_{k+1}}{q^l}$$

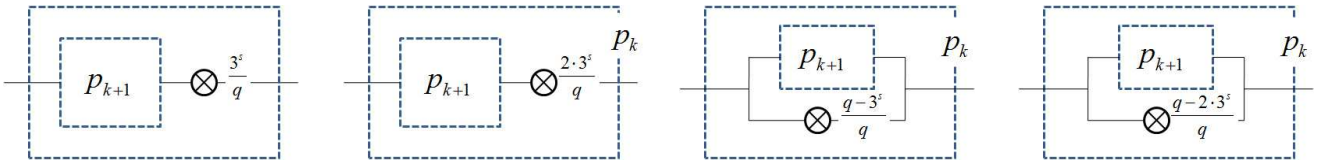
Algorithm 1 Backward algorithm to realize p_1 for an even q

$k = 1$, start with an empty circuit.
while p_k cannot be realized with a single pswitch. **do**
a) Write p_k as $\frac{b}{q^w}$, let $d_k = \frac{q^{w-1}}{gcd(b, q^{w-1})}$*, where $gcd(x, y)$ is the greatest common divisor between x and y.
b) Insert one pswitch to the circuit (see Fig.2)
i) **if** $p_k < \frac{1}{2}$ and d_k is even
Insert one pswitch $\frac{1}{2}$ in series.
Let $p_{k+1} = 2p_k$.
ii) **if** $p_k > \frac{1}{2}$ and d_k is even
Insert one pswitch $\frac{1}{2}$ in parallel.
Let $p_{k+1} = 2p_k - 1$.
iii) **if** $p_k < \frac{1}{2}$ and d_k is odd.
Insert a pswitch $\frac{2^s}{q}$ in series with $s = \lfloor \log_2 q \rfloor$.
Let $p_{k+1} = \frac{q}{2^s} p_k$.
iv) **if** If $p_k > \frac{1}{2}$ and d_k is odd.
Insert a pswitch $\frac{q-2^s}{q}$ in parallel with $s = \lfloor \log_2 q \rfloor$.
Let $p_{k+1} = \frac{q}{2^s}(p_k - \frac{q-2^s}{q})$.
c) $k = k + 1$
end while
Insert one pswitch p_k to the circuit.
*Note that d_k keeps unchanged if we write p_k as $\frac{bc}{q^w c}$ instead of $\frac{b}{q^w}$.



(a) $p_k \le \frac{1}{3}$ (b) $\frac{1}{3} < p_k \le \frac{2}{3}$, a_k is even (c) $p_k > \frac{2}{3}$ (d) $\frac{1}{3} < p_k \le \frac{2}{3}$,$a_k$ is odd

Fig. 3. The way to find p_{k+1} from p_k when $q \mod 2 \neq 0$, $q \mod 3 = 0$ and $d_k \mod 3 = 0$.



(a) $p_k \le \frac{1}{3}$ (b) $\frac{1}{3} < p_k \le \frac{2}{3}$,$a_k$ is even (c) $p_k > \frac{2}{3}$ (d) $\frac{1}{3} < p_k \le \frac{2}{3}$,$a_k$ is odd

Fig. 4. The way to find p_{k+1} from p_k when $q \mod 2 \neq 0$,$q \mod 3 = 0$ and $d_k \mod 3 \neq 0$, where $s = \lfloor \log_3 q \rfloor$

$$a_{k+1} = 2a_k = 2b_k 2^x t^y = b_k 2^{x+1} t^y$$

So a_{k+1} can be written as $b_{k+1}2^{x+\delta x}t^y$ with $\delta x \ge 1$.

If $p_k > \frac{1}{2}$ (see Fig. 2(b)), we have

$$p_{k+1} = 2p_k - 1 = \frac{2a_k - q^l}{q^l} = \frac{a_{k+1}}{q^l}$$

$$\begin{aligned} a_{k+1} &= 2a_k - q^l = 2b_k 2^x t^y - 2^{cl} t^l \\ &= (b_k - 2^{cl-x-1} t^{l-y}) 2^{x+1} t^y \end{aligned}$$

So a_{k+1} can be written as $b_{k+1}2^{x+\delta x}t^y$ with $\delta x \ge 1$.

(b) If $a_k = b_k 2^x t^y$ with $x \ge c(l-1), 0 \le y < (l-1)$ and b_k is odd, then a_{k+1} can be written as $a_{k+1} = b_{k+1}2^{cl-s+\delta x}t^{y+1}$ with $\delta x \ge 0$ and and b_{k+1} is odd.

When $a_k = b_k 2^x t^y$ with $x \ge c(l-1), 0 \le y < (l-1)$ and b_k is odd, we have $a_k \mod 2^{c(l-1)} = 0$, so d_k is odd.

If $p_k < \frac{1}{2}$ (see Fig. 2(c)), we have

$$p_{k+1} = \frac{q}{2^s} p_k = \frac{\frac{a_k q}{2^s}}{q^l}$$

$$a_{k+1} = b_k 2^{x-s} t^y q = b_k 2^{x-s+c} t^{y+1} = b_k 2^{x-c(l-1)} 2^{cl-s} t^{y+1}$$

So a_{k+1} can be written as $b_{k+1}2^{cl-s+\delta x}t^{y+1}$ with $\delta x \ge 0$.

If $p_k > \frac{1}{2}$ (see Fig. 2(d)), we have

$$p_{k+1} = \frac{q}{2^s}(p_k - \frac{q - 2^s}{q}) = \frac{\frac{q}{2^s}(a_k - q^l + q^{l-1}2^s)}{q^l}$$

$$a_{k+1} = (b_k 2^{x-c(l-1)} - 2^c t^{l-y} + 2^s t^{l-1-y}) 2^{cl-s} t^{y+1}$$

So a_{k+1} can be written as $b_{k+1}2^{cl-s+\delta x}t^{y+1}$ with $\delta x \ge 0$.

3) Using the results from Step 2, we will show that there exists a number m ($m \le \lceil \log_2 q \rceil (n-1)+1$) such that a_m can be written as $b_m 2^x t^y$ with $x \ge c(l-1)$ and $y \ge l-1$, therefore

$$p_m = \frac{a_m}{q^l} = \frac{b_m 2^{x-c(l-1)} t^{y-(l-1)}}{q}$$

can be realized with a single pswitch.

At the beginning, $p_1 = \frac{a}{q^n} = \frac{aq^{l-n}}{q^l} = \frac{a_1}{q^l}$. Then, $a_1 = a2^{c(l-n)}t^{l-n} = b_1 2^{c(l-n)+z}t^{l-n}$ with $z \ge 0$ and odd b_1. Now, we discuss the cases of $t = 1$ and $t > 1$ separately:

(a) If $t = 1$, we have $a_1 = b_1 2^{c(l-n)+z}$ with $z \ge 0$ and odd b_1. According to the first relation between a_{k+1} and a_k in Step 2, there exists a number m where

$$m \le c(l-1) - c(l-n) + 1 = c(n-1) + 1$$

such that $a_m = b_m 2^x$ with $x \ge c(l-1)$ and b_m is odd. Since $c = \lceil \log_2 q \rceil$, we have $m \le \lceil \log_2 q \rceil (n-1) + 1$.

(b) If $t > 1$, according to the first relation in step 2, there exists a number m_1

$$m_1 \le c(l-1) - c(l-n) + 1 = c(n-1) + 1$$

such that $a_{m_1} = b_{m_1} 2^x t^{l-n}$ with $x \ge c(l-1)$ and b_{m_1} odd. According to the second relation, we know that a_{m_1+1} can be written as $b_{m_1+1}2^x t^{l-n+1}$ with $x \ge cl - s$ and b_{m_1+1} odd.

We continue the process above until the numerator a_m can be written as $b_m 2^x t^{l-1}$ with $x \ge c(l-1)$ for some m. And we have

$$m \le m_1 + (s - c + 1)(n-1) = (s+1)(n-1) + 1$$

Since $t \neq 1$ and t is odd, we have $\frac{q}{2} < 2^s < q$, so $s + 1 = \lceil \log_2 q \rceil$.

Based on the discussion above, we know that in both of the cases there exists a number m (where $m \le \lceil \log_2 q \rceil (n-1)+1$), such that p_m can be realized with a single pswitch. Therefore, there are at most $\lceil \log_2 q \rceil (n-1) + 1$ pswitches in the circuit constructed by Algorithm 1 for arbitrary probability $\frac{a}{q^n}$. ■

If q is a multiple of 3, the backward algorithm to realize $p_1 = \frac{a}{q^n}$ is described in Algorithm 2. Using a similar method to prove Theorem 1, we get the following results:

Theorem 2. *Given a pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, \ldots \frac{q-1}{q}\}$, if q is a multiple of 3, then Algorithm 2 realizes any rational $\frac{a}{q^n}$ such that $0 < a < q^n$ with at most $\lceil \log_3 q \rceil (n-1) + 1$ pswitches.*

We also can prove the following theorem:

Theorem 3. *Given a pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, ...\frac{q-1}{q}\}$, if q is multiple of 6 ($q \mod 6 = 0$), all rational $\frac{a}{q^n}$ with $0 < a < q^n$ can be realized with at most N pswitches, where*

$$N \leq \begin{cases} (2s)(n-1)+1 & (\text{if } 6^s = q) \\ (2s+1)(n-1)+1 & (\text{if } \frac{q}{2} \leq 6^s < q) \\ (2s+2)(n-1)+1 & (\text{if } \frac{q}{3} \leq 6^s < \frac{q}{2}) \\ (2s+3)(n-1)+1 & (\text{if } \frac{q}{6} < 6^s \leq \frac{q}{3}) \end{cases}$$

III. q IS NOT MULTIPLE OF 2 OR 3

In the above section, we proved that if q is a multiple of 2 or 3, all rational $\frac{a}{q^n}$ can be realized with a bounded number of pswitches. Is this true if q is an arbitrary number greater than 2?

Theorem 4. *Given a pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, ..., \frac{q-1}{q}\}$, if a rational $\frac{a}{q^n}$, with q a prime number, cannot be realized with n pswitches, then it cannot be realized with any number of pswitches.*

Proof: We will prove this by contradiction. Assume that there exists some rational $\{\frac{a_i}{q^{k_i}}\}$ with $i = 1, 2, 3, ...$, where $\frac{a_i}{q^{k_i}}$ cannot be realized with k_i pswitches but can be realized at least with l_i (where $l_i > k_i$) pswitches. Let $l = \min_i l_i$, so there exists one rational $\frac{a}{q^n}$ (where $n < l$) which can be realized with at least l pswitches. As a result, in the following proof we will get another rational $\frac{c}{q^{l-2}}$ which cannot be realized with $l-2$ pswitches but can be realized with $l-1$ pswitches. This contradicts the assumption that l is minimal.

Let C^l denote a circuit that realizes $\frac{a}{q^n}$ with l pswitches. Assume the circuit formed by the first $l-1$ pswitches is C^{l-1} with probability $\frac{b}{q^{l-1}}$, and the last pswitch of C^l is $\frac{u}{q}$ $(0 < u < q)$.

If the last pswitch is added in series, we can get

$$\frac{b}{q^{l-1}} \frac{u}{q} = \frac{a}{q^n}$$

Algorithm 2 Backward algorithm to realize p_1 when q is a multiple of 3

$k = 1$, start with an empty circuit.
while p_k cannot be realized with a single pswitch. **do**
a) Write p_k as $\frac{b}{q^w}$, let $d_k = \frac{q^{w-1}}{gcd(b, q^{w-1})}$, where $gcd(x, y)$ is the greatest common divisor between x and y.
b) Insert one pswitch to the circuit:
i) **if** d_k is a multiple of 3:
Insert one pswitch to the circuit as shown in Fig. 3. Calculate p_{k+1}.
ii) **if** d_k is not a multiple of 3:
Insert one pswitch to the circuit as shown in Fig. 4. Calculate p_{k+1}.
c) $k = k + 1$
end while
Insert one pswitch p_k to the circuit.

Therefore $bu = aq^{l-n}$, bu is a multiple of q. Since q is a prime number, either b or u is a multiple of q. But we know that u cannot divide q due to $0 < u < q$. So we can conclude that b is a multiple of q.

If the last pswitch is added in parallel, we can get

$$\frac{b}{q^{l-1}} + \frac{u}{q} - \frac{b}{q^{l-1}} \frac{u}{q} = \frac{a}{q^n}$$

Therefore $b(q-u) = aq^{l-n} - uq^{l-1}$. Similar as above, we can conclude that b is a multiple of q.

So in both of the cases, b is a multiple of q. i.e. b can be written as cq. Let's consider the rational $\frac{c}{q^{l-2}} = \frac{b}{q^{l-1}}$. It can be realized by the circuit C^{l-1} with $l-1$ pswitches. Now, assume it can realized with $l-2$ pswitches. Then, $\frac{a}{q^n}$ can be realized by adding one more pswitch. This contradicts our assumption that $\frac{a}{q^n}$ can be realized with at least l pswitches. So we have that $\frac{c}{q^{l-2}}$ cannot be realized with $l-2$ pswitches but can be realized with $l-1$ pswitches. However, this contradicts the assumption that l is minimal. ■

Theorem 5. *For a prime number $q > 3$, there exists an integer a (where $0 < a < q^n$) such that $\frac{a}{q^n}$ cannot be realized with any number of pswitches for $n \geq 2$.*

Proof: In [2], the following result is given: No pswitch set containing all $\frac{a}{q}$, $0 < a < q$, for any $q > 3$, can realize all $P_r(C) = \frac{b}{q^2}$ $(0 < b < q^2)$ with at most 2 pswitches. The conclusion follows from this result and Theorem 4. ■

Now, we know that if q is a multiple of 2 or 3, given pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, ..., \frac{q-1}{q}\}$, all rational $\frac{a}{q^n}$ $(0 < a < q^n)$ can be realized with a bounded number of pswitches. But if q is a prime number greater than 3, there is at least one rational $\frac{a}{q^n}$ $(0 < a < q^n)$ cannot be realized. It is natural to ask that what will happen if q is neither a multiple of 2 or 3, nor a prime number greater than 3? For example, $q = 5 \times 7$.

We have simulated the cases that q is less than 10000. The simulation results show that if q is not a multiple of 2 or 3, there is at least one rational $\frac{a}{q^2}$ with $0 < a < q^2$ that cannot be realized using a limited number of pswitches closed with probability in $\{\frac{1}{q}, \frac{2}{q}, ..., \frac{q-1}{q}\}$. Therefore, we have the following conjecture:

Conjecture 1. *Given a pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, ...\frac{q-1}{q}\}$, all rational $\frac{a}{q^n}$ with $0 < a < q^n$ can be realized with a limited number of pswitches if and only if q is a multiple of 2 or 3.*

This conjecture is not easily proved. Now, we only show an example that q is neither a multiple of 2 or 3, nor a prime number. In this example there exists a rational $\frac{a}{q^2}$ that cannot be realized.

Example 1. *Given a pswitch set $S = \{\frac{1}{25}, \frac{2}{25}, ..., \frac{24}{25}\}$, the rational $\frac{155}{25^2}$ cannot be realized.*

Proof: Assume $\frac{155}{25^2}$ can be realized by adding one pswitch $\frac{x}{25}$ $(0 < x < 25)$ to a circuit closed with probability $\frac{y}{25^n}$, where $0 < y < 25^n$ and y cannot be divided by 25.

If the single pswitch is added in series, we have

$$\frac{y}{25^n}\frac{x}{25} = \frac{155}{25^2}$$

So

$$xy = 25^{n-1}155$$

Since y cannot by divided by 25, the only possible value of n is 1. Furthermore, since $0 < x < 25$, we can get $(x, y) = (1, 155)$ or $(x, y) = (5, 31)$, which conflicts with the condition that $0 < y < 25^n = 25$.

If the single pswitch is added in parallel, we have

$$\frac{y}{25^n} + \frac{x}{25} - \frac{xy}{25^{n+1}} = \frac{155}{25^2}$$

So

$$25y + 25^n x - xy = 25^{n-1}155$$

If $n \geq 2$, $xy = 25y + 25^n x - 25^{n-1}155$ can be divided by 25. Since neither x nor y can be divided by 25, so x can be written as $5x'$ and y can be written $5y'$, therefore, we can get

$$x'y' = 5y' + 25^{n-1} - 25^{n-2}155$$

We can conclude that $x'y'$ can divided by 5, so either x or y can be divided by 25, which conflicts with our assumptions. Therefore the only possible value of n is 1. In this case, we have

$$xy = 25y + 25x - 155$$

It tells us that either x or y can be divided by 5. Without losing the generality, we assume x can be divided by 5, so the possible values of x are $\{5, 10, 15, 20\}$. Since $y > 0$, we have $25x < 155$, so the only possible value of x is 5. Then the corresponding value of y is 1.5, which is not an integer. ■

IV. Greedy Backward Algorithm

In the two sections above, we discuss whether all rational $\frac{a}{q^n}$ with $0 < a < q^n$ can be realized for a given pswitch set $\{\frac{1}{q}, \frac{2}{q}, ..., \frac{q-1}{q}\}$. In this section, we try to find an algorithm to realize the desired probabilities using as a few as possible pswitches.

In backward algorithm above, if we want to realize a rational p_1, we can find another rational p_2 such that if p_2 can be realized, then p_1 can be realized by adding a single pswitch x to p_2 in series or parallel. So, we can insert the pswitch x as the last pswitch and try to realize p_2 instead of p_1. Now, x is chosen from $\{\frac{1}{q}, \frac{2}{q}, ..., \frac{q-1}{q}\}$ and can be inserted in series or in parallel, so there are totally $2(q-1)$ choices to insert this single pswitch, and $2(q-1)$ possible values for p_2:

$$\begin{aligned} F &= \{p | p \cdot x = p_1, x \in \{1, 2, ..., q-1\}\} \\ &\bigcup \{p | p + x - px = p_1, x \in \{1, 2, ..., q-1\}\} \end{aligned}$$

For each rational $p \in F$ that possibly can be realized should satisfy the following conditions:

(a) $0 < p < 1$, due to the property of probability.

(b) p can be written as $\frac{a}{q^n}$ with some integer n and $0 < a < q^n$, since only the rational with denominator q^n can be realized using the pswitches in $\{\frac{1}{q}, \frac{2}{q}, ..., \frac{q-1}{q}\}$.

Therefore, the feasible set of p_2 can be written as

$$S_f = \{p | p \in F, 0 < p < 1, pq^n \text{is an integer for some n}\}$$

Now, we want to select one element in S_f as the value of p_2. However, which element in S_f is the "best" choice for p_2? In another word, which element in S_f can be realized with as a few as possible pswitches? In a special case that if there is an element which can be written as $\frac{u}{q}$, the question becomes trivial since this element $\frac{u}{q}$ must be the "best" choice for p_2, due to it can be realized with only one pswitch. But in other cases, it is not easy to say that one element is absolutely better than another one. Here, we have an intuition: one element $\frac{a}{q^2}$ with a cannot be divided by q is easier to be realized than another element $\frac{b}{q^{10}}$ with b cannot be divided by q. That is if one element is "closer" to single pswitches, it will be easier to be realized. Based on this intuition, we define the following function to measure the "distance" between one element $\frac{a}{q^n}$ and single pswitch set $\{\frac{1}{q}, \frac{2}{q}, ..., \frac{q-1}{q}\}$:

$$d(\frac{a}{q^n}) = d(\frac{a}{q^n}, S) = \frac{q^{n-1}}{gcd(a, q^{n-1})}$$

where $gcd(a, q^{n-1})$ is the greatest common divisor between a and q^{n-1} as described before. The element "closest" to the single pswitches in the feasible set is chosen as the value of p_2. We continue this process recursively until for some m the rational p_m can be realized with a single pswitch. Then, the circuit realizing p_1 is constructed. Since we always choose the "best" value locally in each step, we call this algorithm as Greedy Backward Algorithm (GBA), which is described in Algorithm 3. An instance is given in Fig. 5. The realization of this algorithm can be found in [5].

For GBA, we have the following properties:

Theorem 6. *Given a pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, ...\frac{q-1}{q}\}$, if q is a multiple of 2 or 3, then GBA realizes any rational $\frac{a}{q^n}$ such that $0 < a < q^n$.*

Proof: We only prove that the theorem is true for the case of even q. There are two things that we need to prove: (1) For each p_k, there always exists a rational p in the feasible set S_f such that $d(p) < d(p_k)$, therefore $d(p_{k+1}) = \min_{x \in S_f} d(x) \leq$

Algorithm 3 Greedy Backward Algorithm to realize p_1

$k = 1$, start with an empty circuit.
while p_k cannot be realized with a single pswitch. **do**
a) Calculate the feasible set S_f for p_{k+1}.
b) Let $p_{k+1} = \arg\min_{p \in S_f} d(p)$.
d) IF $d(p_{k+1}) \geq d(p_k)$
p_1 cannot be realized using GBA. Return.
d) Insert a pswitch x corresponding to p_{k+1}, such that $p_{k+1}x = p_k$ or $p_{k+1} + x - xp_{k+1} = p_k$.
e) $k = k + 1$
end while
Insert one pswitch p_k to the circuit.

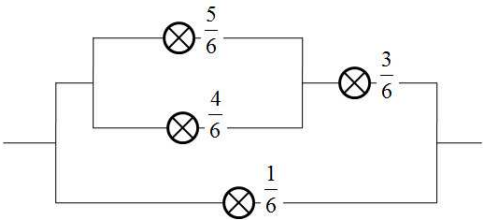


Fig. 5. Given a pswitch set $\{\frac{1}{6}, \frac{2}{6}, ..., \frac{5}{6}\}$, the rational $\frac{121}{6^4}$ is realized using GBA.

$d(p) < d(p_k)$. (2) For each p_k, there are only a limited number of possible values for $d(p_k)$.

In order to prove (1), we only need to find a way to get p from p_k. Fortunately, Algorithm 1 provides us such a way, see Fig. 2. For example, when $p_k > \frac{1}{2}$ and $d(p_k)$ is even, we have $p = 2p_k - 1$. Assume $p_k = \frac{a}{q^n}$ and let $c = gcd(a, q^{n-1})$, then we can write $q^{n-1} = h_1 c$ and $a = h_2 c$ such that h_1 and h_2 are relatively prime. Therefore $d(p_k) = h_1$ is even.

Furthermore, we can get

$$\begin{aligned} d(p) &= \frac{q^{n-1}}{gcd(2a - q^n, q^{n-1})} = \frac{h_1 c}{gcd(2h_2 c - q h_1 c, h_1 c)} \\ &= \frac{h_1}{gcd(2h_2, h_1)} = \frac{h_1}{2} < h_1 \end{aligned}$$

Similarly, we can also prove that (1) is true for other cases.

For (2), we know that the prime factors of $d(p_k)$ must also be prime factors of q. Since $d(p_k)$ is decreasing with k, we can know that $d(p_k) < d(p_1) = const$. Therefore, the possible number of values of $d(p_k)$ is bounded by $(\log_2 d(p_1) + 1)^l$, where l is the number of prime factors of q.

Based on (1) and (2), there must be a number m such that $d(p_m) = 1$. Therefore p_m can be realized with one single pswitch. ■

The theorem above tells us that all rational $\frac{a}{q^n}$ with $0 < a < q^n$ can be realized using GBA method if q is a multiple of 2 or 3. Surprisingly, a lot of experiments show that when q is a multiple of 2 or 3, GBA can realize most of desired probabilities with almost optimal size. Here, we say that a desired probability is realized with optimal size if it cannot be realized with less pswitches. In Fig. 6, for each value $q \in [2, 3, 4, 6, 8, 9, 10]$, we enumerate all rationals with the same optimal size n, then we use GBA to realize these rationals and account the average number of used pswitches . It is shown that GBA can work well to realize desired probabilities. In Fig. 7, q is chosen as 6, it shows that as the optimal size increases, the average pswitch number used in GBA also increases. And their difference is approximately proportional to the optimal size.

V. Error-tolerant circuits

If a desired probability can never be realized using the pswitch set $S = \{\frac{1}{q}, \frac{2}{q}, ...\frac{q-1}{q}\}$, for example the desired probability is not a rational, can we construct a circuit to realize an approximate probability? And how many pswitches are enough for us to achieve a required accuracy?

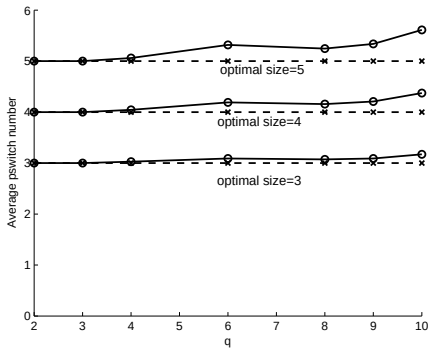


Fig. 6. For each q, the average number of pswtiches used in GBA to realize all the rationals with the same optimal size 3 or 4 or 5.

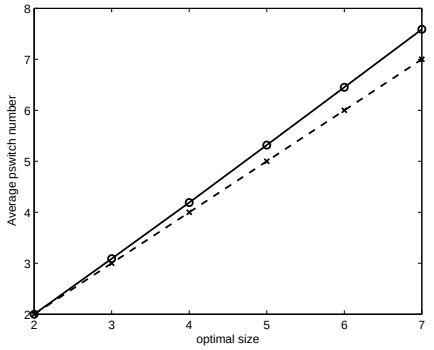
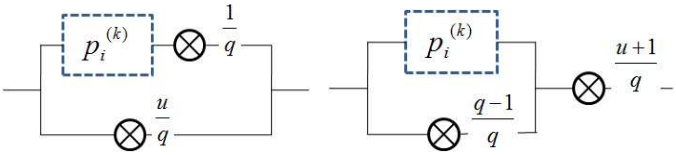


Fig. 7. For $q = 6$, the average number of pswtiches used in GBA to realize all the rationals with the same optimal size in $2, 3, 4, 5, 6, 7$.



(a) Case I (b) Case II

Fig. 8. Operate the rationals in F_k in two ways, where $u = 0, 1, ..., q-1$

Theorem 7. *Given a pswitch set $S = \{\frac{1}{q}, \frac{2}{q}...\frac{q-1}{q}\}$, for any desired probability p_d, there exists a rational probability p_a such that $|p_a - p_d| \leq \frac{1}{2q^n}$ and p_a can be realized with at most $2n-1$ pswitches.*

Proof: Assume F_n is the set of rationals that can be realized with at most $2n-1$ pswitches. It can be written as

$$F_n = \{p_1^{(n)}, p_2^{(n)}, p_3^{(n)} ... p_{m_n}^{(n)}\}$$

where m_n is the number of rationals that can be realized, and $p_1^{(n)} = 0 < p_2^{(n)} < ... < p_{m_n}^{(n)} = 1$. We can prove this theorem by induction. For $n = 1$, the statement is true. Assume for any probability $p_d^{(k)}$, there exists a rational $p_a^{(k)} \in F_k$ such that $|p_a^{(k)} - p_d^{(k)}| \leq \frac{1}{2q^k}$. Then, we want to prove that for any probability $p_d^{(k+1)}$, there exists a rational $p_a^{(k+1)} \in F_{k+1}$ such that $|p_a^{(k+1)} - p_d^{(k+1)}| \leq \frac{1}{2q^{k+1}}$.

(1) If $p_d^{(k+1)} \in [\frac{u}{q}, \frac{u}{q} + \frac{1}{q} - \frac{u}{q^2}]$ for some $u \in \{0, 1, ..., q-1\}$.

Let

$$p_d^{(k)} = \frac{p_d^{(k+1)} - \frac{u}{q}}{\frac{1}{q} - \frac{u}{q^2}}$$

Since $\frac{u}{q} \le p_d^{(k+1)} \le \frac{u}{q} + \frac{1}{q} - \frac{u}{q^2}$, we have $0 \le p_d^{(k)} \le 1$. For $p_d^{(k)}$, according to our assumption, there exists a rational $p_a^{(k)} \in F_k$ such that $|p_a^{(k)} - p_d^{(k)}| \le \frac{1}{2q^k}$.

Now, we can get $p_a^{(k+1)}$ from $p_a^{(k)}$ by adding a $\frac{1}{q}$ pswitch in series and a $\frac{u}{q}$ pswitch in parallel (see Fig. 8(a)). Note if $u = 0$, then we do not add the pswitch. Since $p_a^{(k)}$ can be realized with at most $2k-1$ pswitches, $p_a^{(k+1)}$ can be realized with at most $2(k+1)-1$ pswitches. Therefore, $p_a^{(k+1)} \in F_{k+1}$. $p_a^{(k)}$ and $p_a^{(k+1)}$ have the following relation:

$$p_a^{(k)} = \frac{p_a^{(k+1)} - \frac{u}{q}}{\frac{1}{q} - \frac{u}{q^2}}$$

$$|p_a^{(k)} - p_d^{(k)}| = |\frac{p_a^{(k+1)} - \frac{u}{q}}{\frac{1}{q} - \frac{u}{q^2}} - \frac{p_d^{(k+1)} - \frac{u}{q}}{\frac{1}{q} - \frac{u}{q^2}}| \le \frac{1}{2q^k}$$

which can be simplified as

$$|p_a^{(k+1)} - p_d^{(k+1)}| \le \frac{1}{2q^k}(\frac{1}{q} - \frac{u}{q^2}) \le \frac{1}{2q^{k+1}}$$

(2) If $p_d^{(k+1)} \in [\frac{u}{q} + \frac{1}{q} - \frac{u}{q^2}, \frac{u+1}{q}]$ for some $u \in \{0, 1, ..., q-1\}$. Let

$$p_d^{(k)} = (p_d^{(k+1)} \frac{q}{u+1} - \frac{q-1}{q})q$$

Since $\frac{u}{q} + \frac{1}{q} - \frac{u}{q^2} \le p_d^{(k+1)} \le \frac{u+1}{q}$, we have $\frac{1}{u+1} \le p_d^{(k)} \le 1$. For $p_d^{(k)}$, according to our assumption, there exists a rational $p_a^{(k)} \in F_k$ such that $|p_a^{(k)} - p_d^{(k)}| \le \frac{1}{2q^k}$.

Now, we can get $p_a^{(k+1)}$ from $p_a^{(k)}$ by adding an $\frac{q-1}{q}$ pswitch in parallel and a $\frac{u+1}{q}$ pswitch in series (see Fig. 8(b)). Since $p_a^{(k)}$ can be realized with at most $2k-1$ pswitches, $p_a^{(k+1)}$ can be realized with at most $2(k+1)-1$ pswitches. Therefore, $p_a^{(k+1)} \in F_{k+1}$. $p_a^{(k)}$ and $p_a^{(k+1)}$ have the following relation:

$$p_a^{(k)} = (p_a^{(k+1)} \frac{q}{u+1} - \frac{q-1}{q})q$$

$$|p_a^{(k)} - p_d^{(k)}| = |p_a^{(k+1)} \frac{q^2}{u+1} - p_d^{(k+1)} \frac{q^2}{u+1}| \le \frac{1}{2q^k}$$

which can be simplified as

$$|p_a^{(k+1)} - p_d^{(k+1)}| \le \frac{1}{2q^k} \frac{u+1}{q^2} \le \frac{1}{2q^{k+1}}$$

For all $p_d^{(k+1)} (0 \le p_d^{k+1} \le 1)$, either $p_d^{(k+1)} \in [\frac{u}{q}, \frac{u}{q} + \frac{1}{q} - \frac{u}{q^2}]$ or $p_d^{(k+1)} \in [\frac{u}{q} + \frac{1}{q} - \frac{u}{q^2}, \frac{u+1}{q}]$ for some $u \in \{0, 1, ..., q-1\}$. So we can conclude that if the statement is true for $n = k$, then it is also true for $n = k+1$. Therefore, we can conclude that for any desired probability $p_d (0 \le p_d \le 1)$, there exists a rational $p_d \in F_n$ such that $|p_a - p_d| \le \frac{1}{2q^n}$ ■

Based on this proof, we can use Algorithm 4 to construct a circuit to get a good approximation of the desired probability with error smaller than ϵ. We can conclude that there are at most $2\lceil \log_q \frac{1}{2\epsilon} \rceil - 1$ pswitches in the circuit.

Algorithm 4 Backward algorithm to realize p_1 with error$< \epsilon_1$.

$k = 1$, start with an empty circuit

while $|\frac{i}{q} - p_k| > \epsilon_k$, $\forall i \in \{0, 1, 2...q\}$ **do**

a) **if** $p_k \in [\frac{u}{q}, \frac{u}{q} + \frac{1}{q} - \frac{u}{q^2}]$ for some $u \in \{0, 1, ..., q-1\}$ Insert a $\frac{u}{q}$ pswitch in parallel, and then insert a $\frac{1}{q}$ pswitch in series. (see Fig. 8(a)) Let

$$p_{k+1} = \frac{p_k - \frac{u}{q}}{\frac{1}{q} - \frac{u}{q^2}}, \epsilon_{k+1} = \frac{q^2 \epsilon_k}{q-u}$$

b) **if** $p_k \in [\frac{u}{q} + \frac{1}{q} - \frac{u}{q^2}, \frac{u+1}{q}]$ for some $u \in \{0, 1...q-1\}$ Insert a $\frac{u+1}{q}$ pswitch in series, and then insert a $\frac{q-1}{q}$ pswitch in parallel.(see Fig. 8(b)) Let

$$p_{k+1} = (p_k \frac{q}{u+1} - \frac{q-1}{q})q, \epsilon_{k+1} = \frac{q^2 \epsilon_k}{u+1}$$

c) $k = k + 1$

end while

Let $u = \arg\min_i |\frac{i}{q} - p_k|$ and insert an $\frac{u}{q}$ pswitch to replace p_k.

For the special case of $q = 2$ or $q = 3$, we can also obtain the following theorem:

Theorem 8. *Given a pswitch set $S = \{0, \frac{1}{q}, \frac{2}{q} ... \frac{q-1}{q}\}$ with $q = 2$ or $q = 3$, for any desired probability p_d $(0 \le p_d \le 1)$, there exists a rational p_a $(0 \le p_a \le 1)$ such that $|p_a - p_d| \le \frac{1}{2q^n}$ and p_a can be realized with at most n pswitches.*

Proof: This theorem is a corollary of the following theorem: Given a pswitch set $S = \{0, \frac{1}{q}, \frac{2}{q} ... \frac{q-1}{q}\}$ with $q = 2$ or $q = 3$, all rational $\frac{a}{q^n} (0 < a < q^n)$ can be realized with at most n pswitches. ■

According to this theorem, given a pswitch set $S = \{\frac{1}{2}\}$ or $S = \{\frac{1}{3}, \frac{2}{3}\}$, if we want to realize p_d with error smaller than ϵ, we can construct a circuit closed with probability $p_a = \frac{a}{q^n}$ with $n = \lceil \log_q \frac{1}{2\epsilon} \rceil$ and $|p_d - p_a| < \epsilon$. Using the algorithms in [2], p_a can be realized with at most $\lceil \log_q \frac{1}{2\epsilon} \rceil$ pswitches.

VI. Conclusion

In this paper, we generalized the results in [2] and proved that when q is a multiple of 2 or 3, all rational fractions $\frac{a}{q^n}$ can be realized with pswitches, each closed with a probability in $\{\frac{1}{q}, \frac{2}{q}, ..., \frac{q-1}{q}\}$. However, this property does not hold for other q. In addition, we proposed Greedy Backward Algorithm to realize desired probabilities with good performance. Finally, we proved that any desired probability can be approximated well by a linear size ssp circuit.

There are a number of open problems, for example, how to construct an optimal stochastic switching circuit with an arbitrary pswitch set? If q is neither a prime number nor a multiple of 2 or 3 (like $q = 25$), can we strictly prove that there exists at least one rational $\frac{a}{q^n}$ cannot be realized using a simple series-parallel circuit?

ACKNOWLEDGMENT

The authors would like to thank Dan Wilhelm for discussions and assistance.

REFERENCES

[1] C.E. Shannon. A symbolic analysis of relay and switching circuits. Trans. AIEE, 57:713C723, 1938.

[2] D. Wihelm, J. Bruck. Stochastic switching circuit synthesis. IEEE International Symposium on Information Theory(ISIT), 2008. 1388-1392

[3] B. Fett, J. Bruck, and M.D. Riedel. Synthesizing stochasticity in biochemical systems. In Proceedings of the 44th Annual Conference on Design Automation(DAC), 2007. 640-645

[4] P.A. MacMahon. The combinations of resistances. The Electrician, 28:601C602, 1892. (Reprinted in: Discr. Appl. Math., 54:225- 228, 1994.).

[5] Website: *http://paradise.caltech.edu/˜hzhou/stochastic.html*