LANG-TROTTER AND THE ORDER OF THE CUBICS

REBECCA BILBRO, KEVIN JAMES, AND ERIC MANLEY

1. Introduction

Let E be an elliptic curve and E_p be the elliptic curve over $\mathbb{F}_p$ obtained by reduction of E modulo some prime p. If $a_p(E)$ is the trace of $E/\mathbb{F}_p$ then $\#E(\mathbb{F}_p) = p + 1 - a_p(E)$ and $|a_p(E)| \leq 2\sqrt{p}$.

2. The Lang-Trotter Conjecture

In 1976, Lang and Trotter [5] conjectured that if an elliptic curve E does not have complex multiplication and

$$\pi(x) = \#\{p < x \colon E/\mathbb{F}_p \text{ is singular}\}$$

then

$$\pi(x) \sim c\sqrt{x}/\log x \text{ as } x \to \infty$$

where $c > 0$ is a constant depending the Galois representation associated with E. They used the probabilistic model to describe their conjectural constant c.

3. Background and Survey

- The L-T conjecture is based on heuristics relating to the Sato-Tate [8] distribution of primes.
- Serre [7] proved that

$$\#\{p < x \colon E/\mathbb{F}_p \text{ is singular}\} \ll x/(\log x)^{5/4-\epsilon}$$

- If $c = 0$, there are finitely many primes such that $a_p(E) = r$. Elkies [3] proved that this cannot happen if $r = 0$. If $r \neq 0$ there can only be finitely many p's such that $a_p(E) = r$.
- Fouvry and Murty [4] obtained average estimates for c when $r = 0$.
- David and Pappalardi [2] generalized F&M's results for any $r \in \mathbb{Z}$

Date: blah.

- Thus, the L-T conjecture has been shown to be true in an average sense. However, based on some recent computations (see "Frobenius Distributions and Galois Representations-Numerical Evidence" by Kevin James and V. Kumar Murty) and additional averaging theorems, there remains some doubt as to whether the conjecture holds for all curves.

4. What was (is) missing?

Our goal is not to disprove the L-T Conjecture but to diminish the gaps in the evidence produced thus far. We would like either to find more evidence in support of Lang and Trotter's conjecture or to generate some strong computational evidence against LT. We can look at many curves modulo many primes which makes computation especially useful in this problem.

5. Methods

5.1. **Naïve Method.** The order of E over $\mathbb{F}_p$ can be computed by finding

$$\#E(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} \left(\left(\frac{x^3 + ax + b}{p} \right) + 1 \right)$$

$$= 1 + p + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p} \right)$$

This computation has running time $O(p \log p)$. Running this algorithm for all primes less than n takes $O(n^2)$ operations.

5.2. **Schoof's Algorithm.** In his paper, Schoof [6] introduces division polynomials. Using the relation $Y^2 = X^3 + AX + B$ and the division polynomials, he demonstrates how to find explicit formulas for computation on l-torsion points. He uses these formulas and the Chinese Remainder Theorem to compute the trace t of the Frobenius endomorphism mod l. He then shows how to determine values of a_p with t. Gjøsteen (See "Schoof's Algorithm" by Kristian Gjøsteen) nicely summarizes Schoof's Algorithm as follows[1] :

1. Start with $n = 1$ and $l_0 = 2$.
2. Find the smallest prime l_n greater than l_{n-1} and different from p.
3. Compute $t_n \equiv t \pmod{l_n}$

[1]Please note that the summary is taken directly from Gjøsteen.

4. If $\prod_{i=1}^{n} l_i < 4\sqrt{q}$, increment n and return to step 2.
5. Solve the system of congruences $t \equiv t_i \pmod{l_i}$ for $1 \leq i \leq n$ to find t, and hence $\#E(K) = q + 1 - t$.

5.3. **Mestre-Shanks Method.** Shanks provides an algorithm for finding discrete logarithms called the baby-steps, giant-steps algorithm [1][chapter 5.3.1]. Using this idea and a theorem of Hasse's, Mestre discovered an algorithm for finding the order of elliptic curves over finite fields that has running time $O(p^{1/4} \log p)$. The treatment of this algorithm follows [1][chapter 7].

Theorem 5.1 (Hasse)**.**

$$-a_p = \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p} \right) < |2\sqrt{p}|$$

That is,

$$p + 1 - 2\sqrt{p} < \#E(\mathbb{F}_p) < p + 1 + 2\sqrt{p}.$$

So, if $u - v$ or $u + v < |2\sqrt{p}|$ and the relation

$$[p + 1 + u]P = \pm[v]P.$$

is satisfied for some point P, then $[p + 1 + u \mp v]P = \mathcal{O}$. Since $p + 1 + u \mp v$ is a multiple of the order of P and one of them is in Hasse's interval, it could be the order of the curve itself. In fact, if u and v are unique, then whichever of $p+1+u\mp v$ is in the target interval is guaranteed to be the curve order.

So let $b = \lceil p^{1/4}\sqrt{2} \rceil$. If $k < 2\sqrt{p}$, the k can be written as $k = i + jb$ where $i \in [0, b-1]$ and $j \in [0, b]$. Now, construct the following two lists:

$$\{[p + 1 + i]P : i \in [0, b-1]\},$$

$$\{[jb]P : j \in [0, b]\}.$$

Then, elements in the intersection of these lists are candidates for the curve order. If the intersection has exactly one element, then it is the curve order. If the intersection has more than one element, another point may be chosen. However, if the curve has only points of small order, this may not always work. Mestre provides a theorem which fixes this problem.

Lemma 5.2. *Let E_D be the quadratic twist of E by D. If $p \nmid D$, then*

$$a_p(E) = \left(\frac{D}{p}\right) a_p(E_D).$$

Proof. If $E : y^2 = x^3 + ax + b$, then $E_D : y^2 = D^3(x^3 + ax + b)$. Also,

$$\left(\frac{x^3 + ax + b}{p}\right) = \left(\frac{D}{p}\right)\left(\frac{D^3(x^3 + ax + b)}{p}\right).$$

Therefore,

$$a_p(E) = \left(\frac{D}{p}\right) a_p(E_D).$$

□

Theorem 5.3 (Mestre)**.** *If $p > 229$, at least one of E and E_D has a point P with the property that the only integer $m \in (p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$ with $[m]P = O$ is the actual order of the curve.*

Also, the number of such points exceeds $cp/log(log(p))$ for some positive constant c that is independent of p and the elliptic curve. So, the points satisfying the theorem are fairly common. Thus, if a point on E fails to yield the order of the curve, then the method can be repeated for E_D. Then the order of the curve can be determined from the order of its twist. Eventually, this process will find the correct curve order.

Creation of the lists has running time $O(p^{1/4})$. Finding the intersection of the lists has running time $O(p^{1/4} \log p)$. Thus, the algorithm has $O(p^{1/4} \log p)$ running time. Running the algorithm for all primes less than n takes $O(n^{5/4})$.

5.4. **Quadratic Twists.** Computationally verifying the L-T conjecture can be time consuming due to the complexity of the algorithms for calculating a_p. For this reason, it is desirable *to state a number of results which will allow the avoidance of unnecessary computation*.

Lemma 5.4. *If E has an m torsion point, then $a_p(E) \equiv p + 1 \pmod{m}$.*

Theorem 5.5. *Suppose E satisfies the L-T Conjecture. If E has an m torsion point and $\left(\frac{D}{p}\right)$ is determined by a congruence modulo m, then E_D also satisfies the L-T Conjecture.*

Proof. Let r be some fixed integer. Consider the sets $A = \{p : a_p(E) = r\}$, $B = \{p : a_p(E) = -r\}$, and $H = \{p : a_p(E_D) = r\}$.

Let $A_0 = \{p : a_p(E) = r \text{ and } \left(\frac{D}{p}\right) = 1\}$ and $B_0 = \{p : a_p(E) = -r \text{ and } \left(\frac{D}{p}\right) = -1\}$. By lemma 5.2, $H = A_0 \cup B_0$.

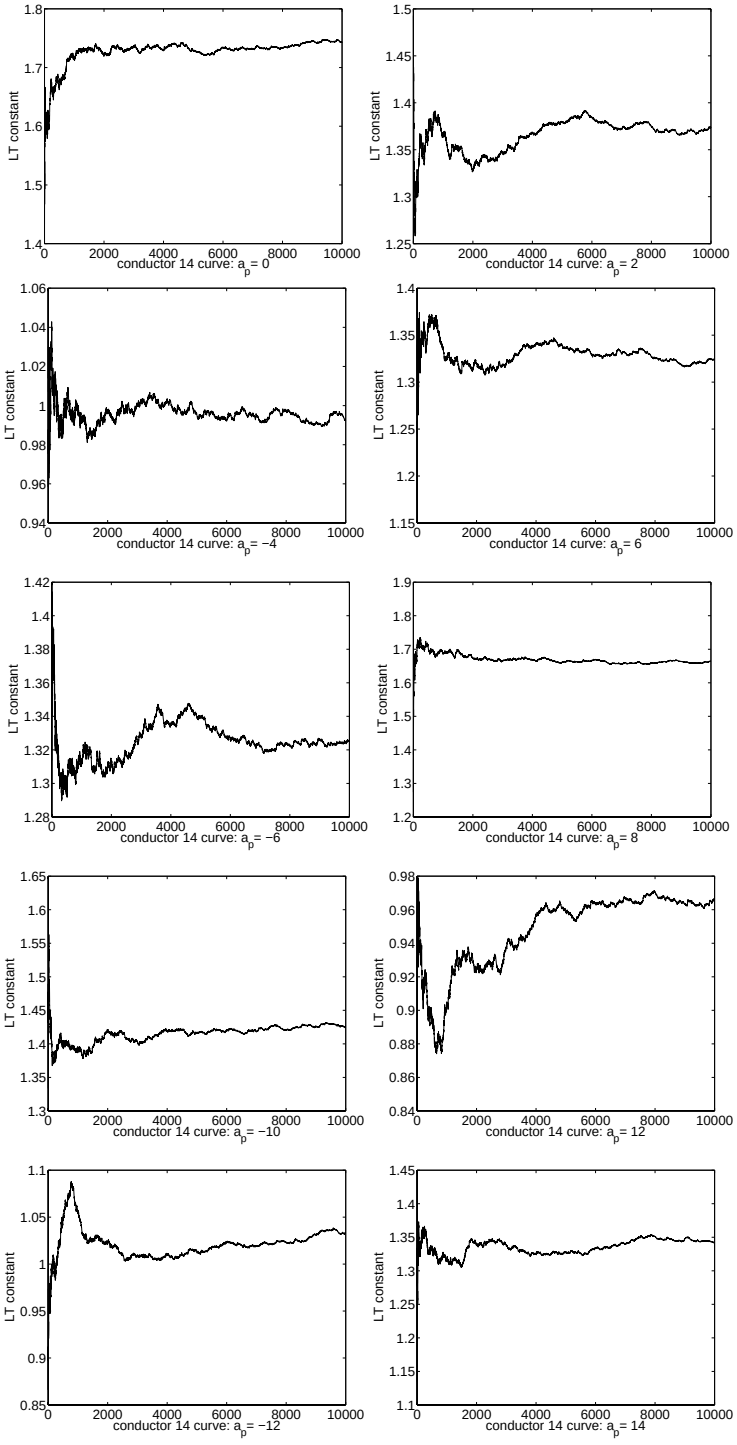
By lemma 5.4, $p \equiv r - 1 \pmod{m}$ for all $p \in A$ and $p \equiv -r - 1 \pmod{m}$ for all $p \in B$. So, if $r - 1$ or $-r - 1$ is a square modulo m, then $A = A_0$ or $B = B_0$ respectively. If $r - 1$ or $-r - 1$ is not a square modulo m, then $A = \emptyset$ or $B = \emptyset$ respectively.

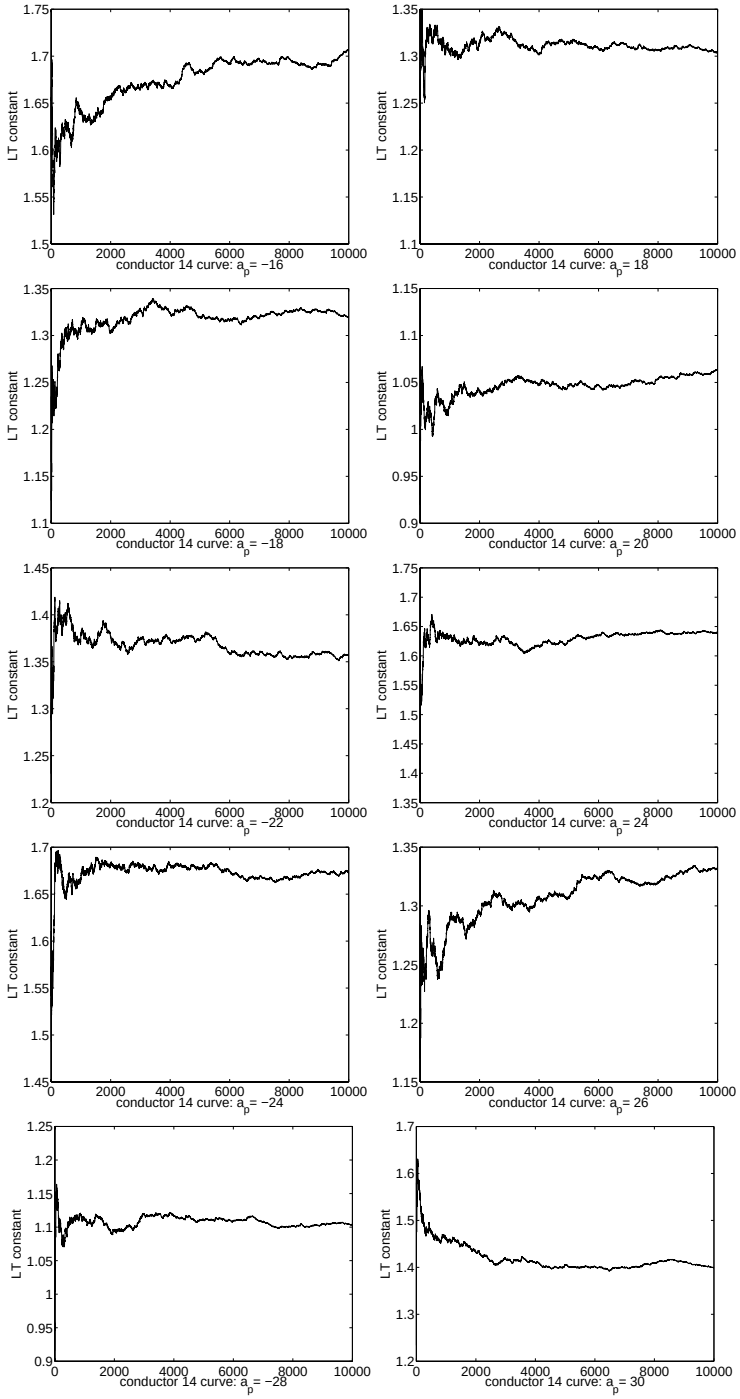
Thus, $H = \emptyset$, $H = A$, $H = B$, or $H = A \cup B$. Since the L-T conjecture holds for E, it also holds for E_D in the first three cases. So assume $H = A \cup B$. Then $\#\{p < x : p \in H\} = \#\{p < x : p \in A\} + \#\{p < x : p \in B\}$. Since $\#\{p < x : p \in A\} \sim c_1\sqrt{x}/\log x$ and $\#\{p < x : p \in B\} \sim c_2\sqrt{x}/\log x$ for some c_1 and c_2, $\#\{p < x : p \in H\} \sim (c_1 + c_2)\sqrt{x}/\log x$. Thus, the L-T Conjecture holds for E_D. □

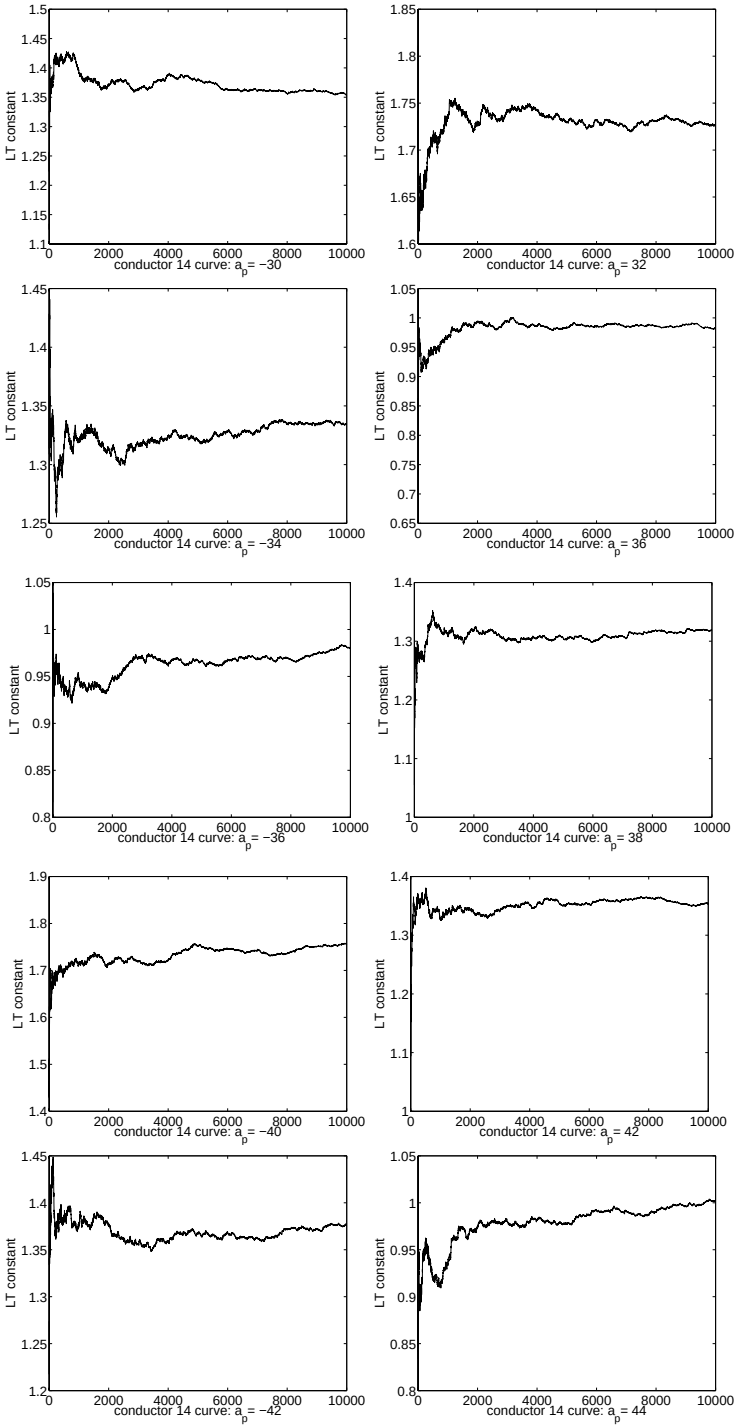
It would be beneficial to show that when any curve satisfies the L-T conjecture, its twist does as well. However, in the absence of such a proof, lemma 5.2 provides a mechanism for quickly calculating a_p for twists. After calculating a_p for all $p < n$ for an elliptic curve E, the a_p for all $p < n$ for E_D can be computed by calculating $\left(\frac{D}{p}\right)$ for all $p < n$. This has running time $O(n)$. While this is an improvement upon the $O(n^{5/4})$ running time of the Mestre-Shanks algorithm, the constant is much smaller because no elliptic curve arithmetic is needed.

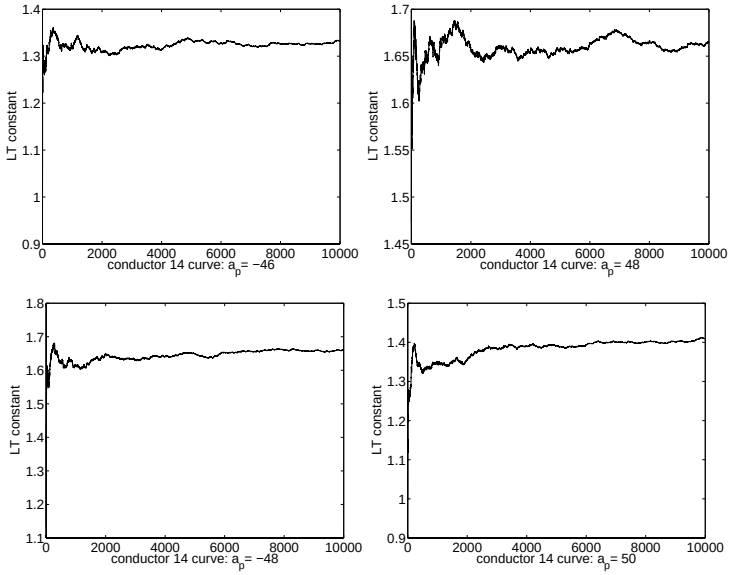
6. Data

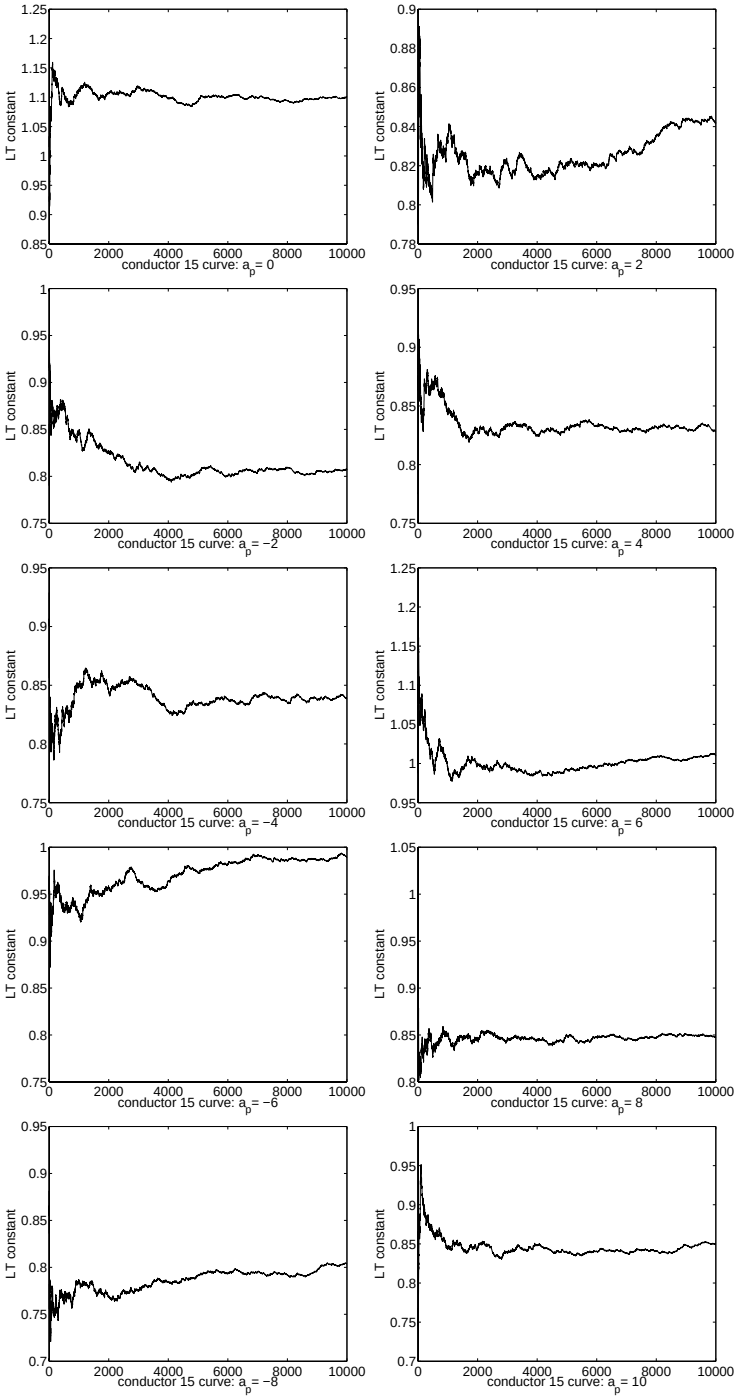
After compiling a vast number of a_p for each conductor ≤ 50, we recorded the value of $c\sqrt{x}/\log x$ once every $100,000$ primes. We then divided these values by $\pi_{1/2}(X) := \sum_{p<X} \frac{1}{2\sqrt{p}}$ to isolate c and graphed the results. In this section, we exhibit a series of these graphs.

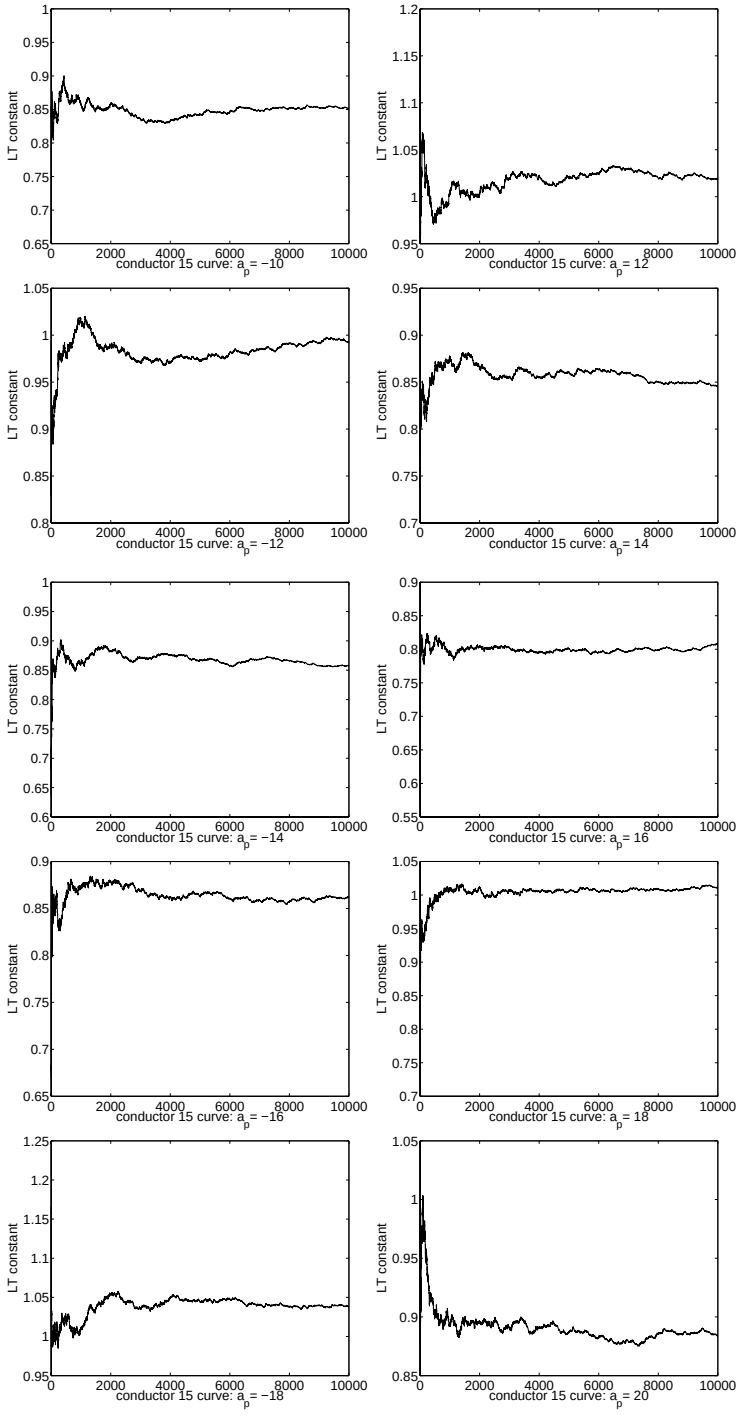

LT constant
conductor 14 curve: $a_p = 0$
conductor 14 curve: $a_p = 2$
conductor 14 curve: $a_p = -4$
conductor 14 curve: $a_p = 6$
conductor 14 curve: $a_p = -6$
conductor 14 curve: $a_p = 8$
conductor 14 curve: $a_p = -10$
conductor 14 curve: $a_p = 12$
conductor 14 curve: $a_p = -12$
conductor 14 curve: $a_p = 14$

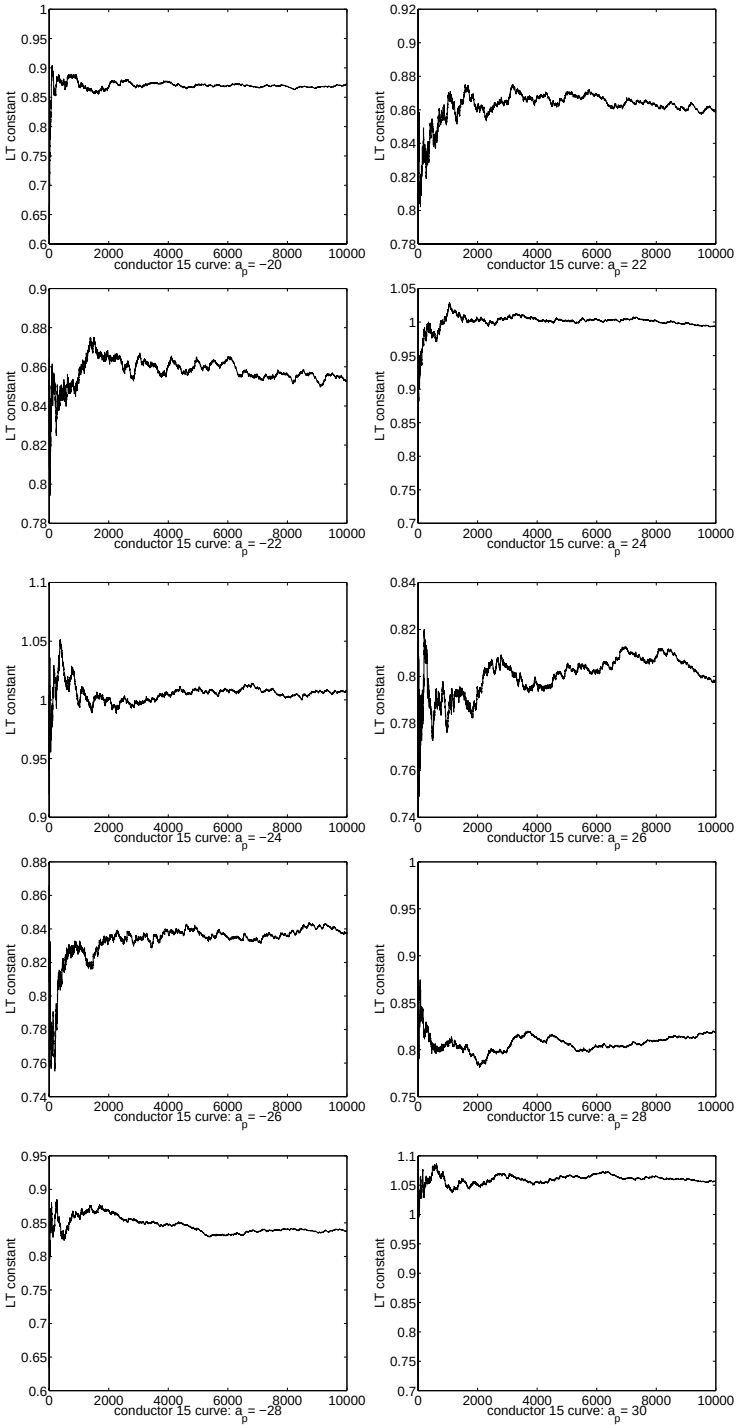

LT constant
conductor 14 curve: $a_p = -16$
conductor 14 curve: $a_p = 18$
conductor 14 curve: $a_p = -18$
conductor 14 curve: $a_p = 20$
conductor 14 curve: $a_p = -22$
conductor 14 curve: $a_p = 24$
conductor 14 curve: $a_p = -24$
conductor 14 curve: $a_p = 26$
conductor 14 curve: $a_p = -28$
conductor 14 curve: $a_p = 30$

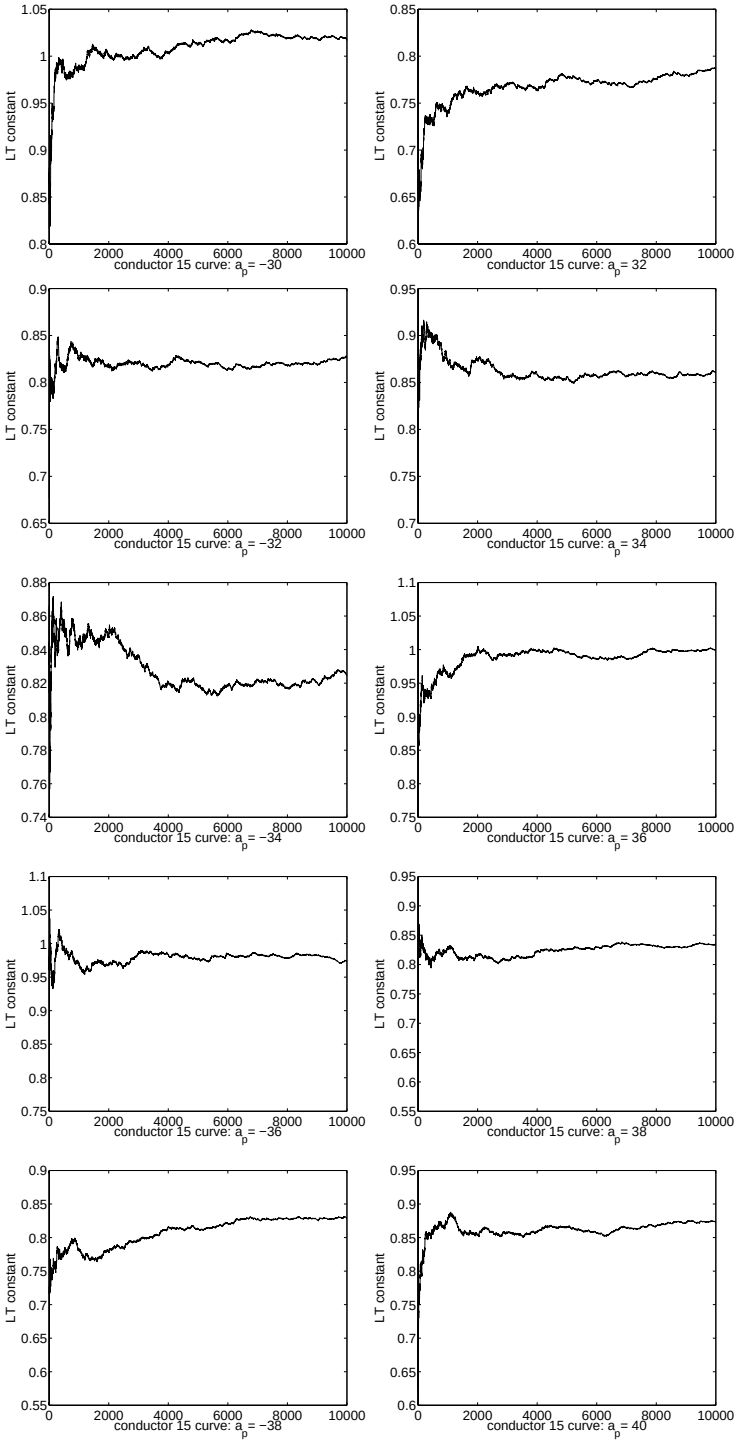

LT constant
conductor 14 curve: $a_p = -30$
conductor 14 curve: $a_p = 32$
conductor 14 curve: $a_p = -34$
conductor 14 curve: $a_p = 36$
conductor 14 curve: $a_p = -36$
conductor 14 curve: $a_p = 38$
conductor 14 curve: $a_p = -40$
conductor 14 curve: $a_p = 42$
conductor 14 curve: $a_p = -42$
conductor 14 curve: $a_p = 44$

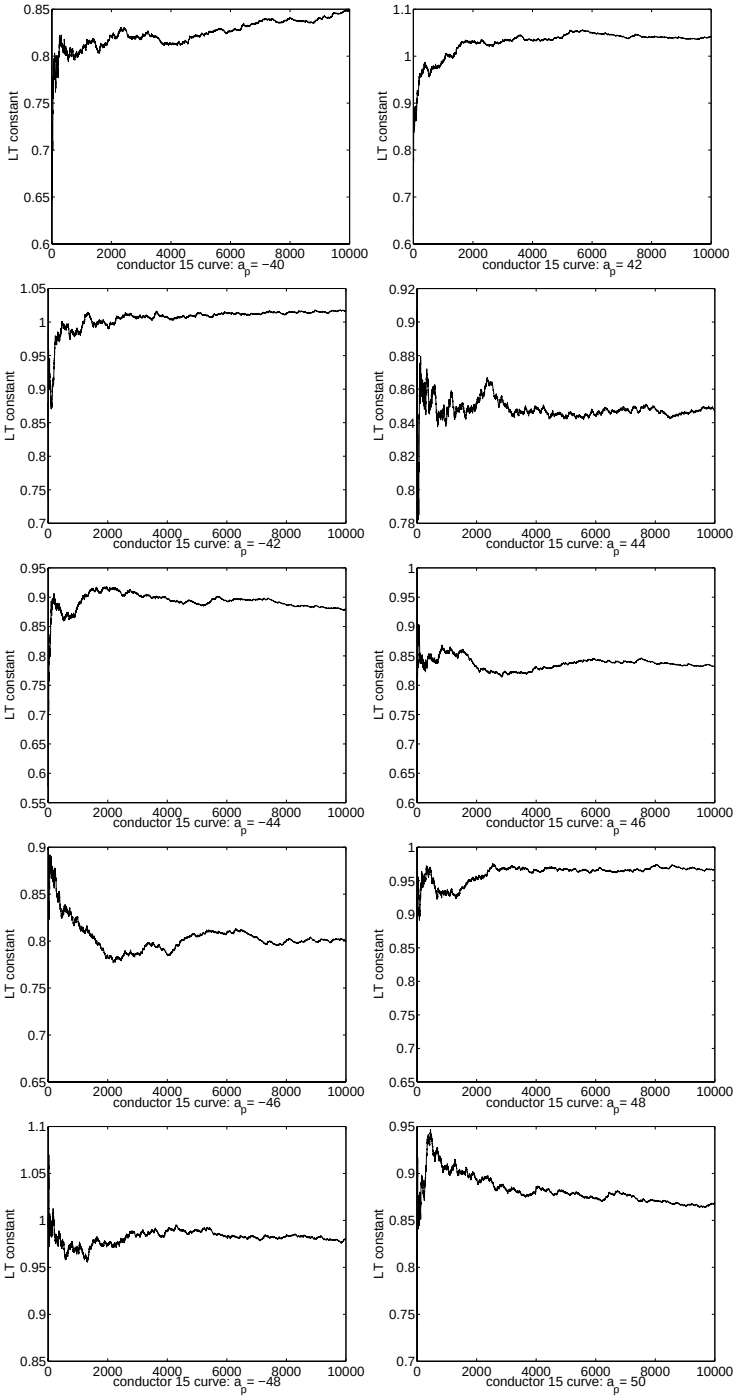

LT constant
conductor 14 curve: $a_p = -46$
conductor 14 curve: $a_p = 48$
conductor 14 curve: $a_p = -48$
conductor 14 curve: $a_p = 50$

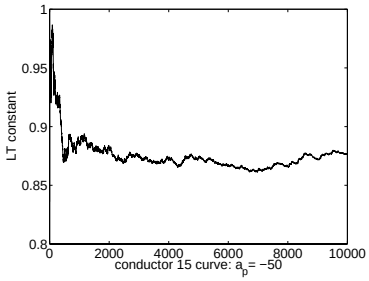

LT constant
conductor 15 curve: $a_p = 0$
conductor 15 curve: $a_p = 2$
conductor 15 curve: $a_p = -2$
conductor 15 curve: $a_p = 4$
conductor 15 curve: $a_p = -4$
conductor 15 curve: $a_p = 6$
conductor 15 curve: $a_p = -6$
conductor 15 curve: $a_p = 8$
conductor 15 curve: $a_p = -8$
conductor 15 curve: $a_p = 10$

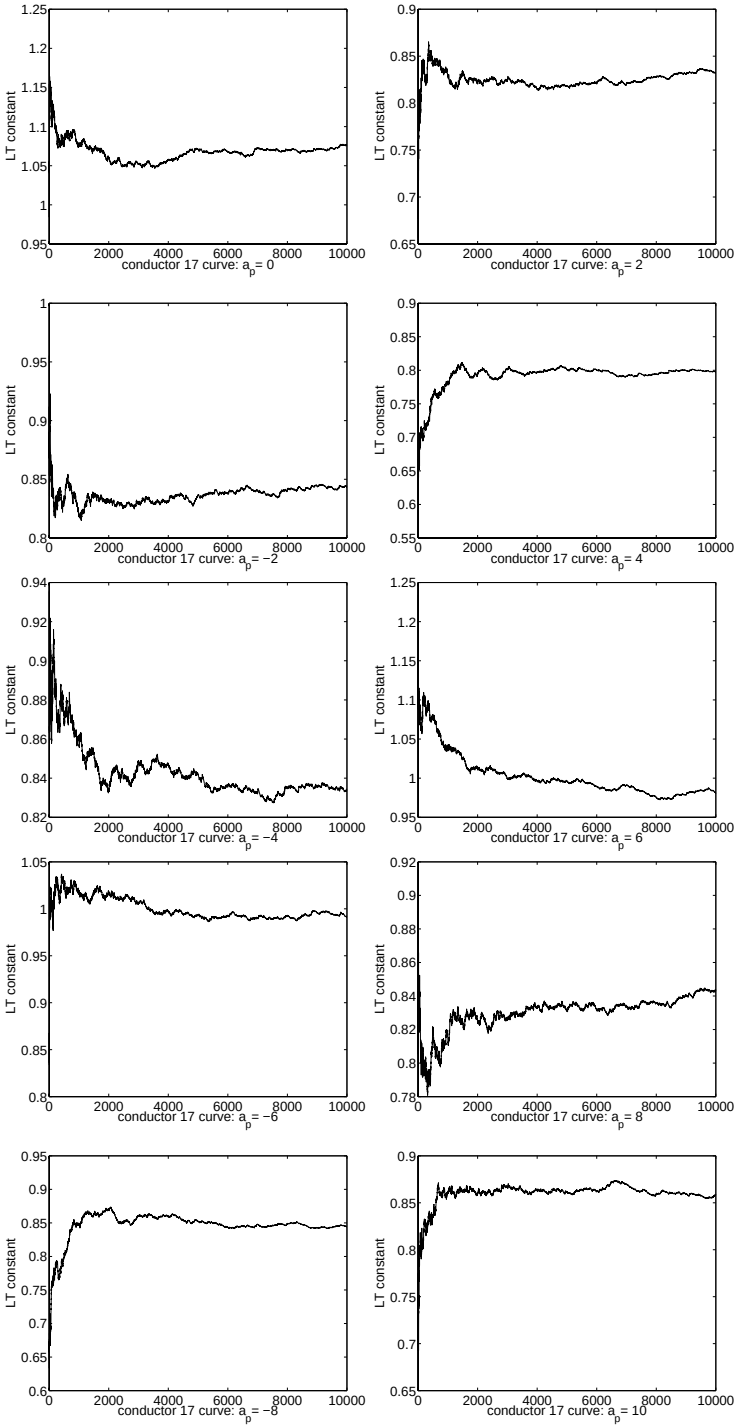

LT constant
conductor 15 curve: $a_p = -10$
conductor 15 curve: $a_p = 12$
conductor 15 curve: $a_p = -12$
conductor 15 curve: $a_p = 14$
conductor 15 curve: $a_p = -14$
conductor 15 curve: $a_p = 16$
conductor 15 curve: $a_p = -16$
conductor 15 curve: $a_p = 18$
conductor 15 curve: $a_p = -18$
conductor 15 curve: $a_p = 20$

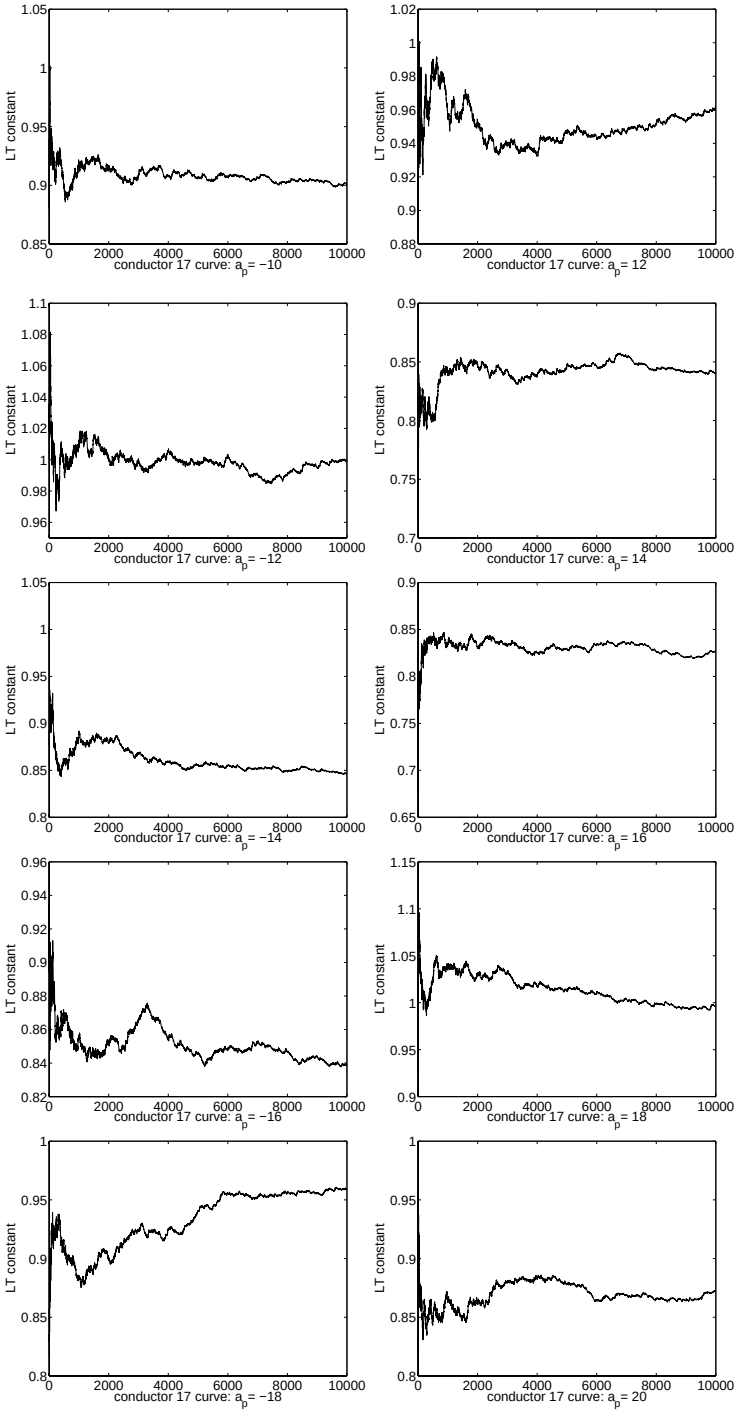

LT constant
conductor 15 curve: $a_p = -20$
conductor 15 curve: $a_p = 22$
conductor 15 curve: $a_p = -22$
conductor 15 curve: $a_p = 24$
conductor 15 curve: $a_p = -24$
conductor 15 curve: $a_p = 26$
conductor 15 curve: $a_p = -26$
conductor 15 curve: $a_p = 28$
conductor 15 curve: $a_p = -28$
conductor 15 curve: $a_p = 30$

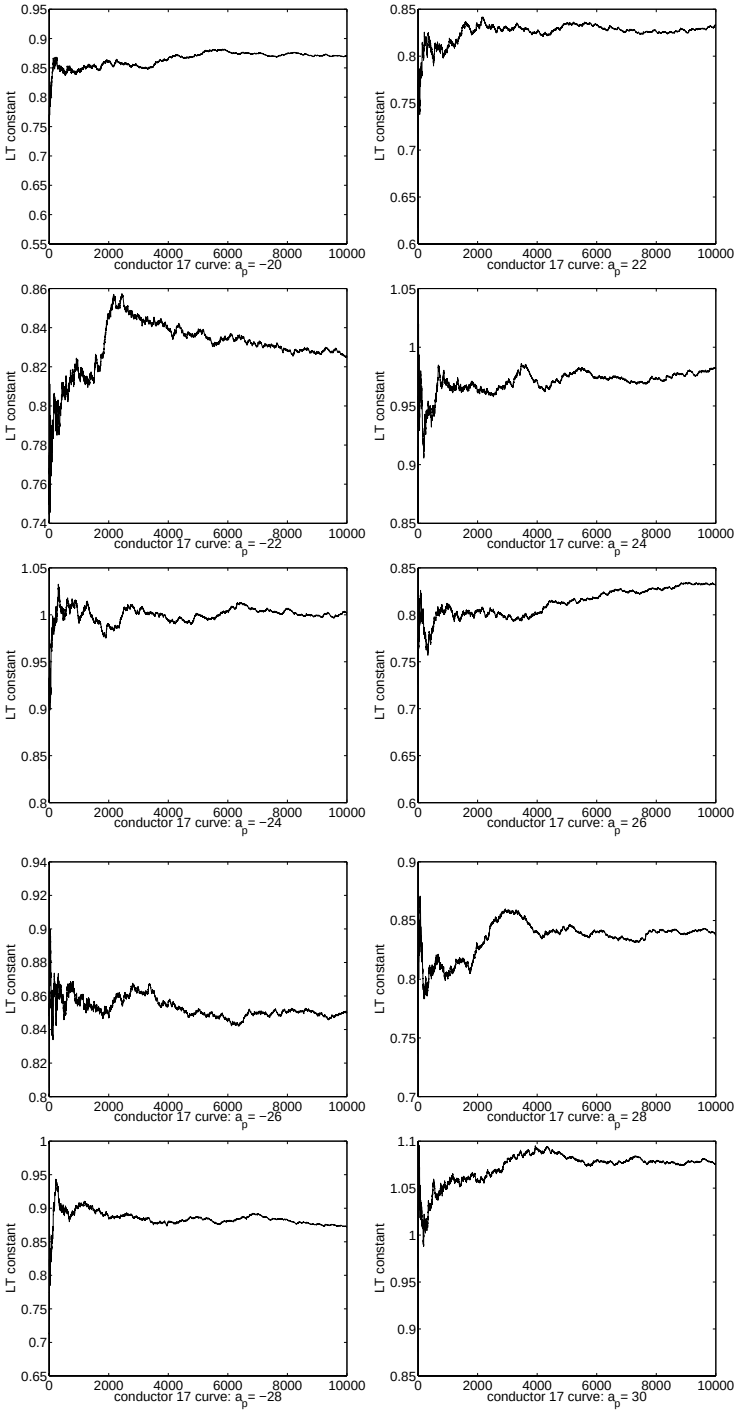

LT constant
conductor 15 curve: $a_p = -30$
conductor 15 curve: $a_p = 32$
conductor 15 curve: $a_p = -32$
conductor 15 curve: $a_p = 34$
conductor 15 curve: $a_p = -34$
conductor 15 curve: $a_p = 36$
conductor 15 curve: $a_p = -36$
conductor 15 curve: $a_p = 38$
conductor 15 curve: $a_p = -38$
conductor 15 curve: $a_p = 40$

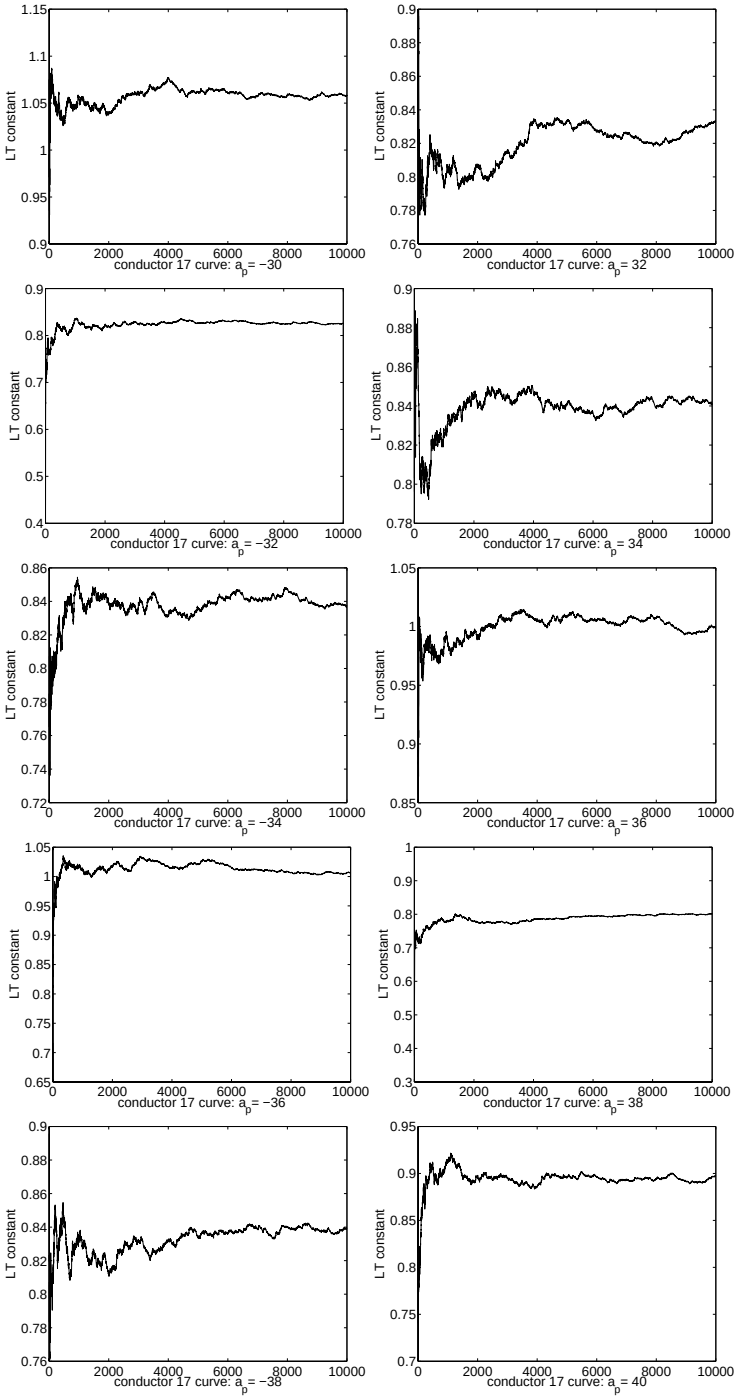

LT constant
conductor 15 curve: $a_p = -40$
conductor 15 curve: $a_p = 42$
conductor 15 curve: $a_p = -42$
conductor 15 curve: $a_p = 44$
conductor 15 curve: $a_p = -44$
conductor 15 curve: $a_p = 46$
conductor 15 curve: $a_p = -46$
conductor 15 curve: $a_p = 48$
conductor 15 curve: $a_p = -48$
conductor 15 curve: $a_p = 50$

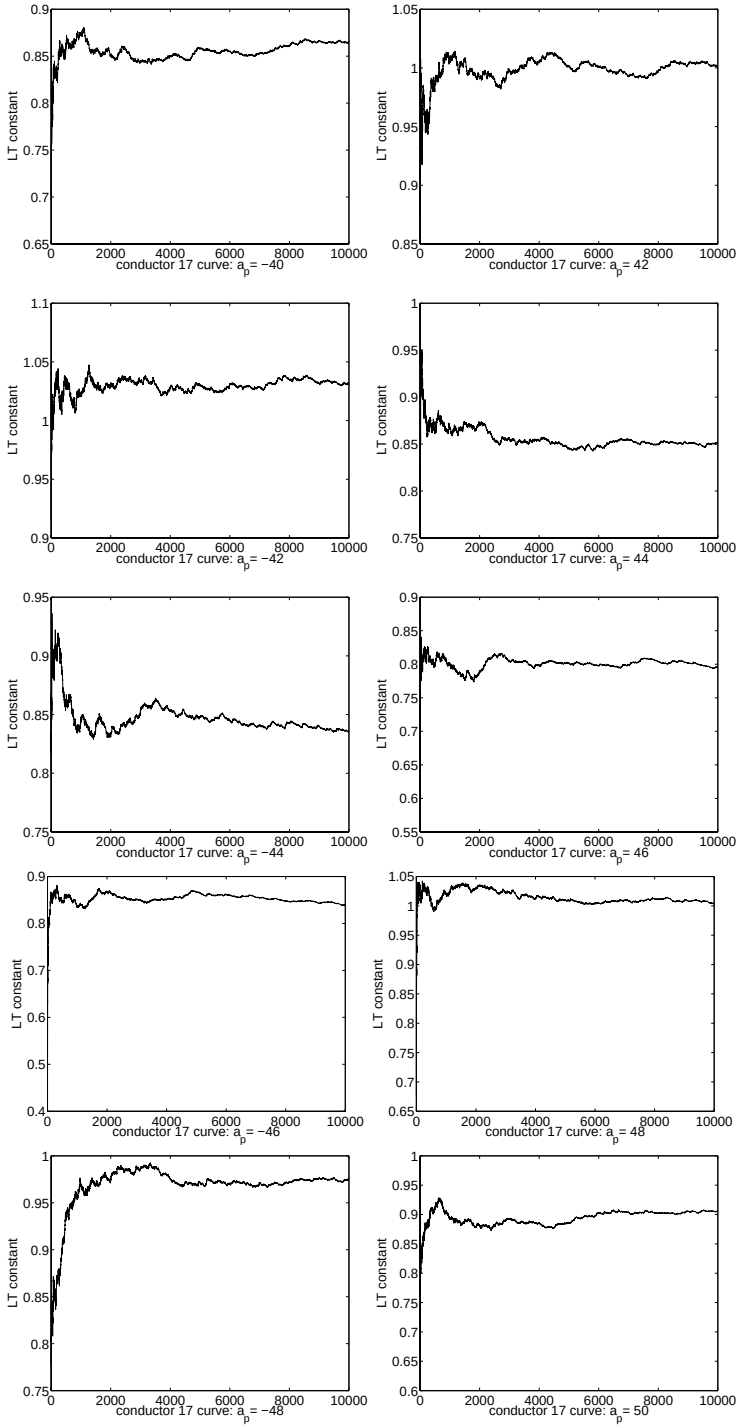

1
0.95
0.9
0.85
0.8
LT constant
0
2000
4000
6000
8000
10000
conductor 15 curve: a_p = −50

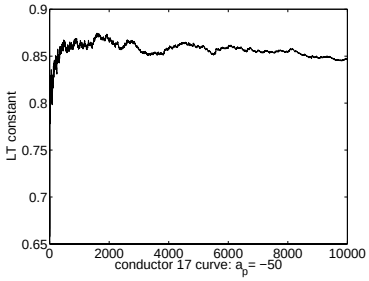

LT constant
conductor 17 curve: $a_p = 0$
conductor 17 curve: $a_p = 2$
conductor 17 curve: $a_p = -2$
conductor 17 curve: $a_p = 4$
conductor 17 curve: $a_p = -4$
conductor 17 curve: $a_p = 6$
conductor 17 curve: $a_p = -6$
conductor 17 curve: $a_p = 8$
conductor 17 curve: $a_p = -8$
conductor 17 curve: $a_p = 10$

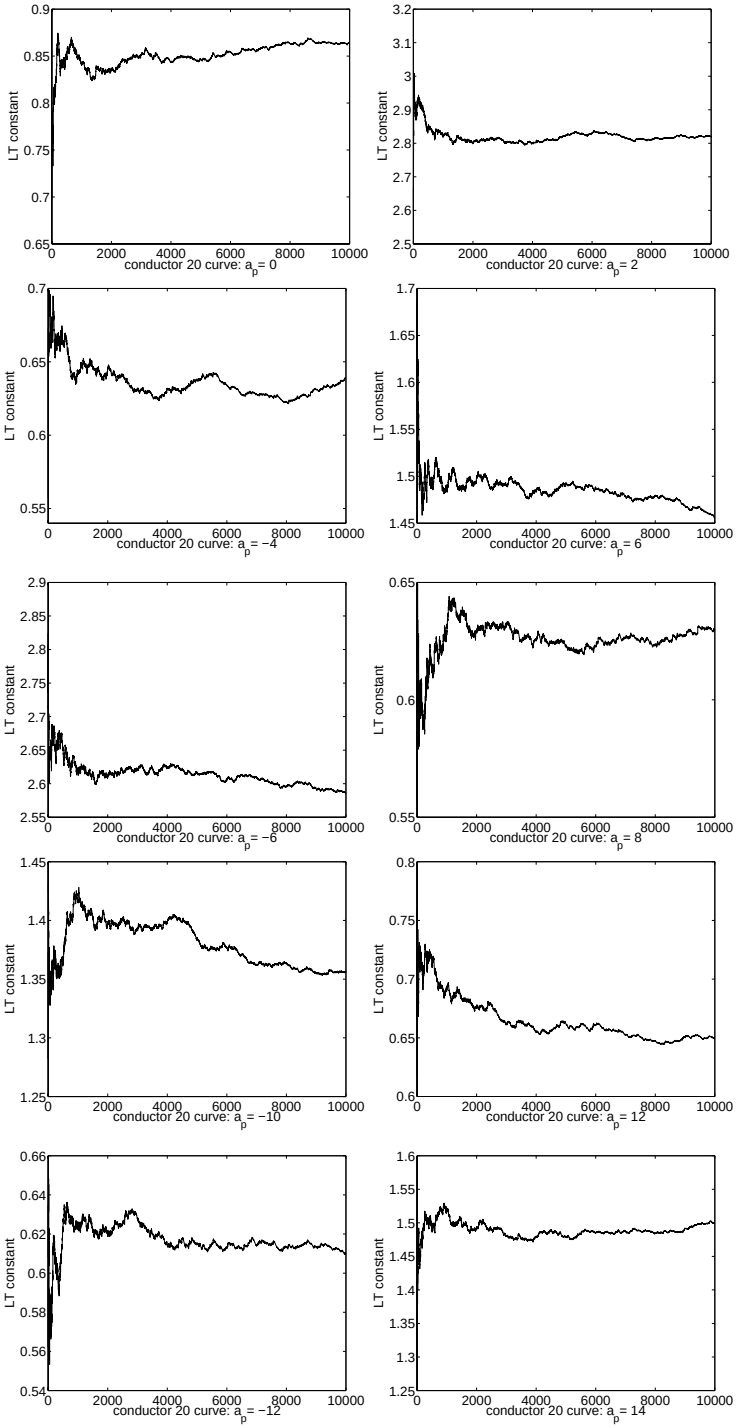

LT constant
conductor 17 curve: $a_p = -10$
conductor 17 curve: $a_p = 12$
conductor 17 curve: $a_p = -12$
conductor 17 curve: $a_p = 14$
conductor 17 curve: $a_p = -14$
conductor 17 curve: $a_p = 16$
conductor 17 curve: $a_p = -16$
conductor 17 curve: $a_p = 18$
conductor 17 curve: $a_p = -18$
conductor 17 curve: $a_p = 20$

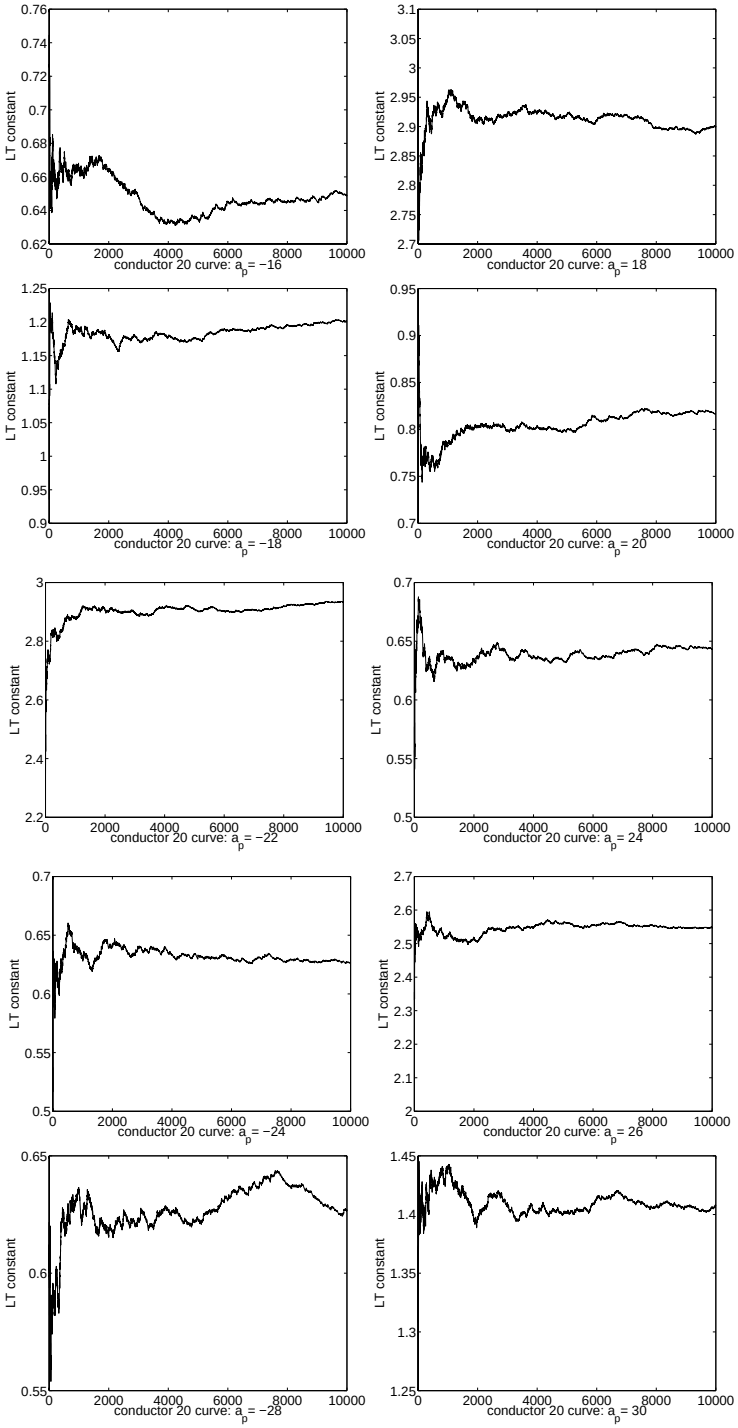

LT constant
conductor 17 curve: $a_p = -20$
conductor 17 curve: $a_p = 22$
conductor 17 curve: $a_p = -22$
conductor 17 curve: $a_p = 24$
conductor 17 curve: $a_p = -24$
conductor 17 curve: $a_p = 26$
conductor 17 curve: $a_p = -26$
conductor 17 curve: $a_p = 28$
conductor 17 curve: $a_p = -28$
conductor 17 curve: $a_p = 30$

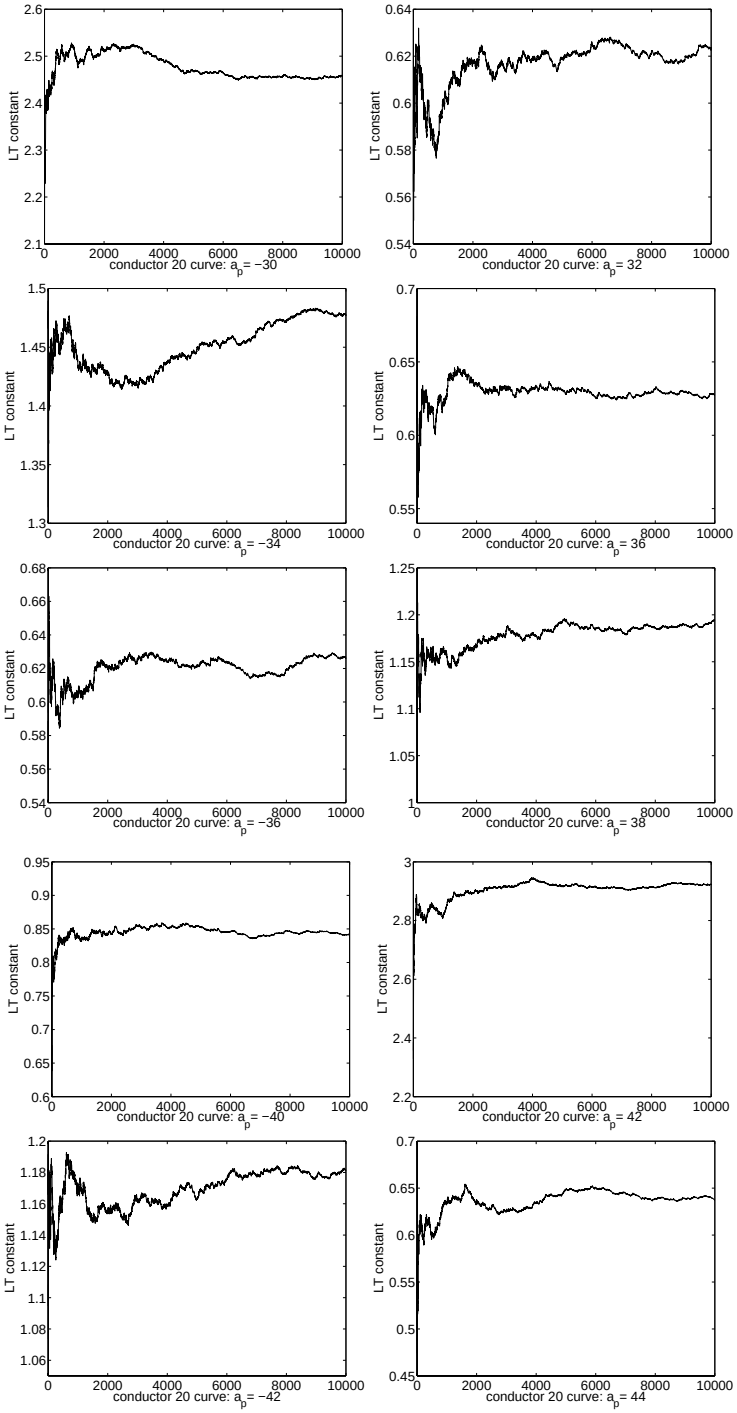

LT constant
conductor 17 curve: $a_p = -30$
conductor 17 curve: $a_p = 32$
conductor 17 curve: $a_p = -32$
conductor 17 curve: $a_p = 34$
conductor 17 curve: $a_p = -34$
conductor 17 curve: $a_p = 36$
conductor 17 curve: $a_p = -36$
conductor 17 curve: $a_p = 38$
conductor 17 curve: $a_p = -38$
conductor 17 curve: $a_p = 40$

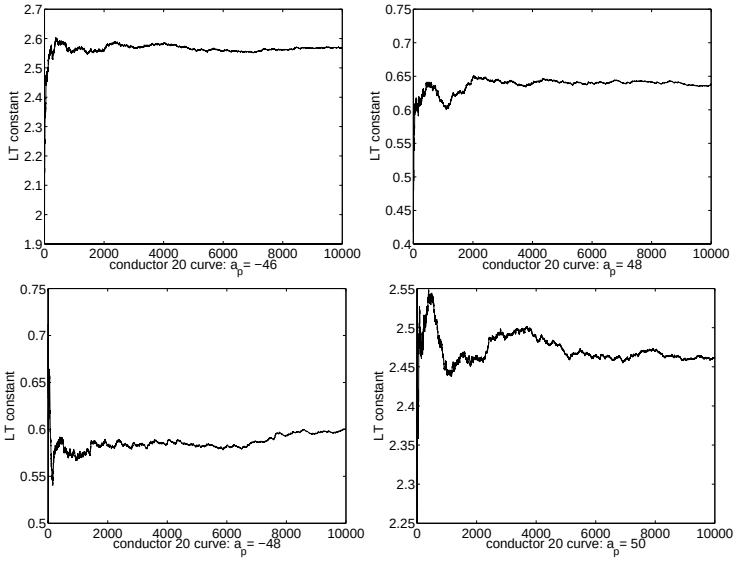

LT constant
conductor 17 curve: $a_p = -40$
conductor 17 curve: $a_p = 42$
conductor 17 curve: $a_p = -42$
conductor 17 curve: $a_p = 44$
conductor 17 curve: $a_p = -44$
conductor 17 curve: $a_p = 46$
conductor 17 curve: $a_p = -46$
conductor 17 curve: $a_p = 48$
conductor 17 curve: $a_p = -48$
conductor 17 curve: $a_p = 50$

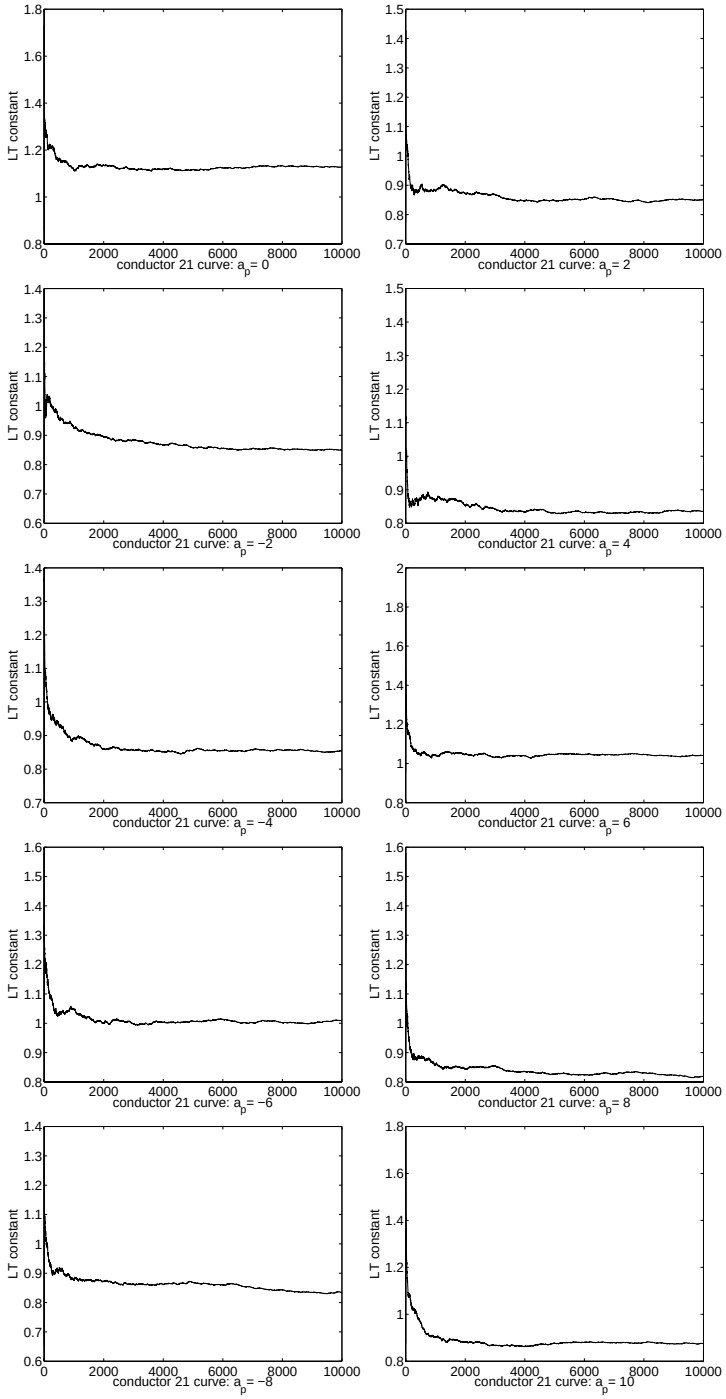

0.9
0.85
0.8
0.75
0.7
0.65
LT constant
0
2000
4000
6000
8000
10000
conductor 17 curve: a_p = −50

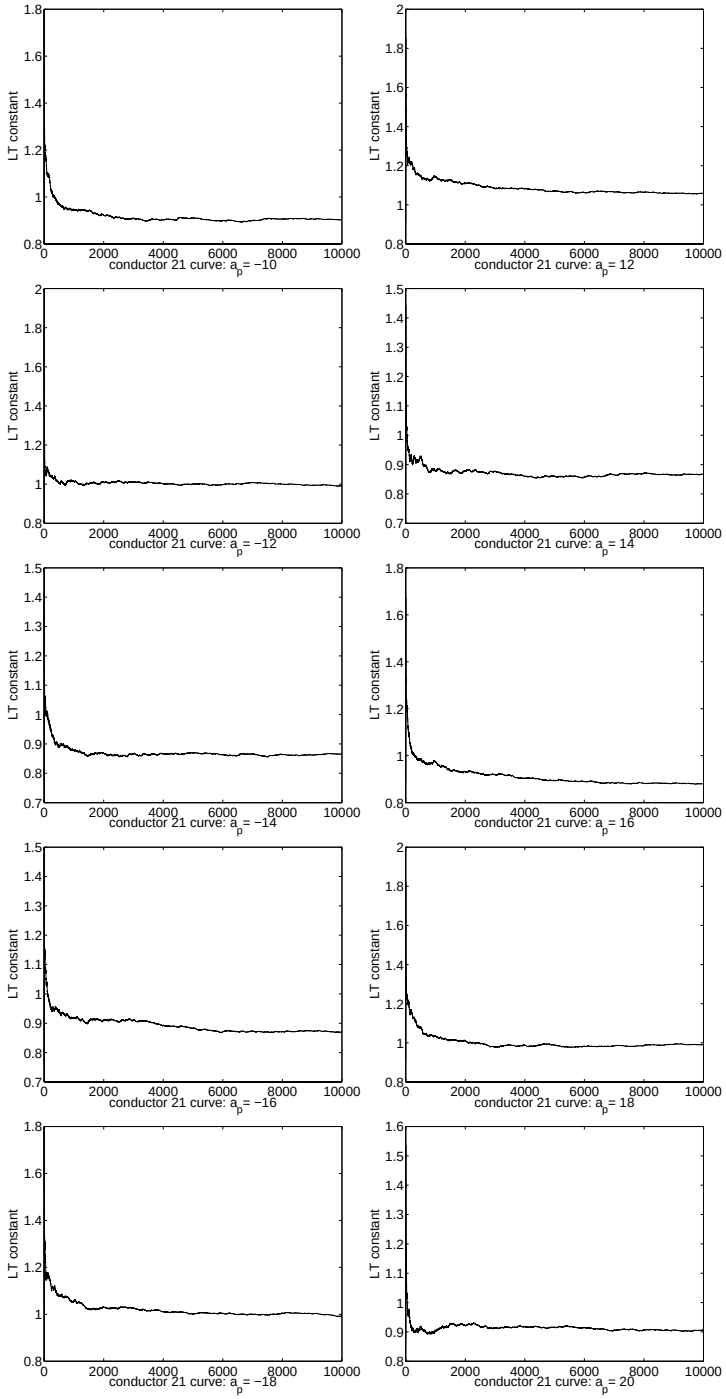

LT constant
conductor 20 curve: $a_p = 0$
conductor 20 curve: $a_p = 2$
conductor 20 curve: $a_p = -4$
conductor 20 curve: $a_p = 6$
conductor 20 curve: $a_p = -6$
conductor 20 curve: $a_p = 8$
conductor 20 curve: $a_p = -10$
conductor 20 curve: $a_p = 12$
conductor 20 curve: $a_p = -12$
conductor 20 curve: $a_p = 14$

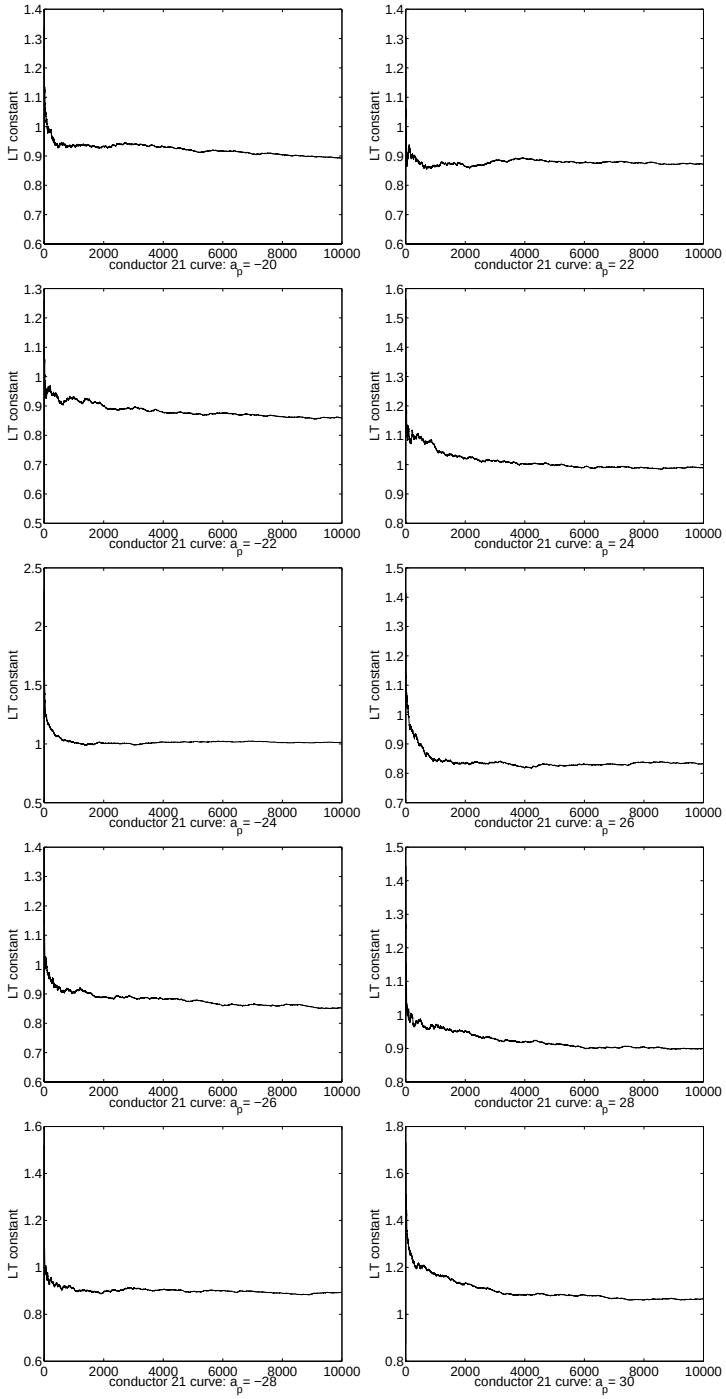

LT constant
conductor 20 curve: $a_p = -16$
conductor 20 curve: $a_p = 18$
conductor 20 curve: $a_p = -18$
conductor 20 curve: $a_p = 20$
conductor 20 curve: $a_p = -22$
conductor 20 curve: $a_p = 24$
conductor 20 curve: $a_p = -24$
conductor 20 curve: $a_p = 26$
conductor 20 curve: $a_p = -28$
conductor 20 curve: $a_p = 30$

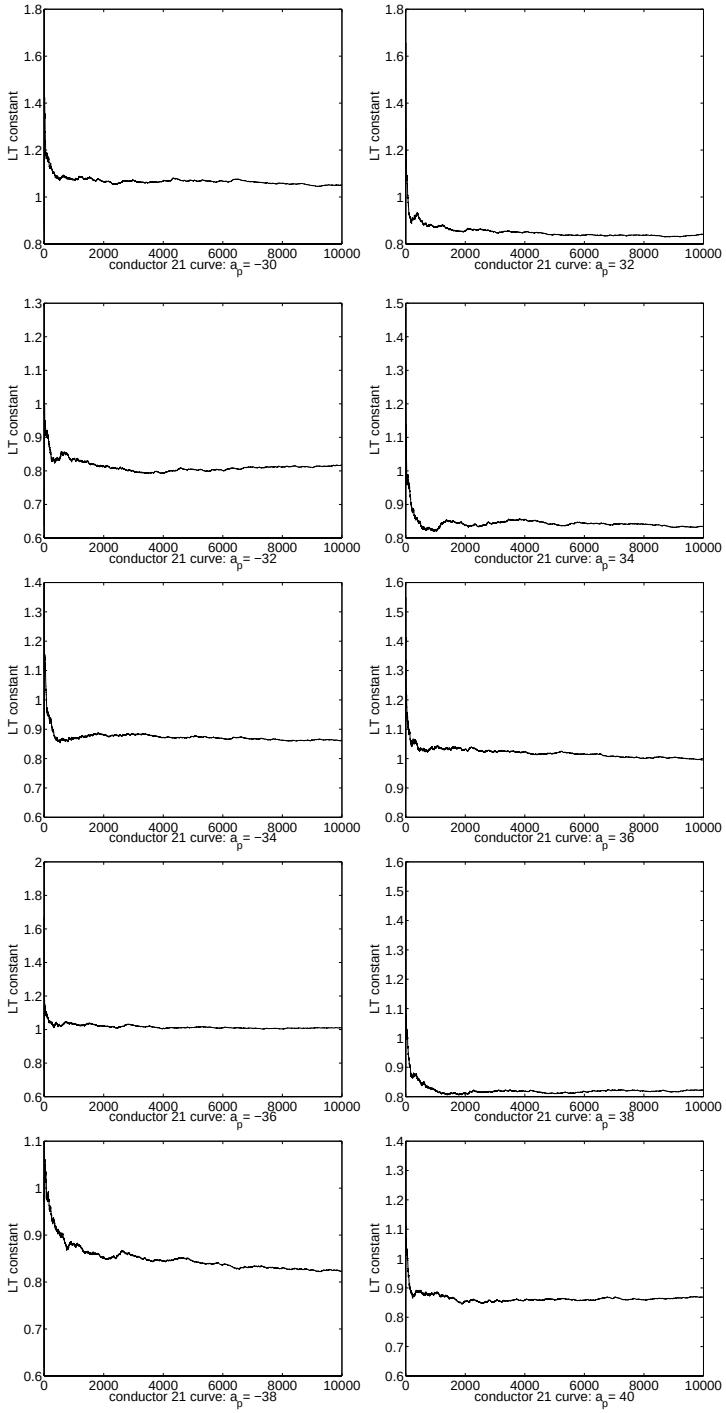

LT constant
conductor 20 curve: $a_p = -30$
conductor 20 curve: $a_p = 32$
conductor 20 curve: $a_p = -34$
conductor 20 curve: $a_p = 36$
conductor 20 curve: $a_p = -36$
conductor 20 curve: $a_p = 38$
conductor 20 curve: $a_p = -40$
conductor 20 curve: $a_p = 42$
conductor 20 curve: $a_p = -42$
conductor 20 curve: $a_p = 44$

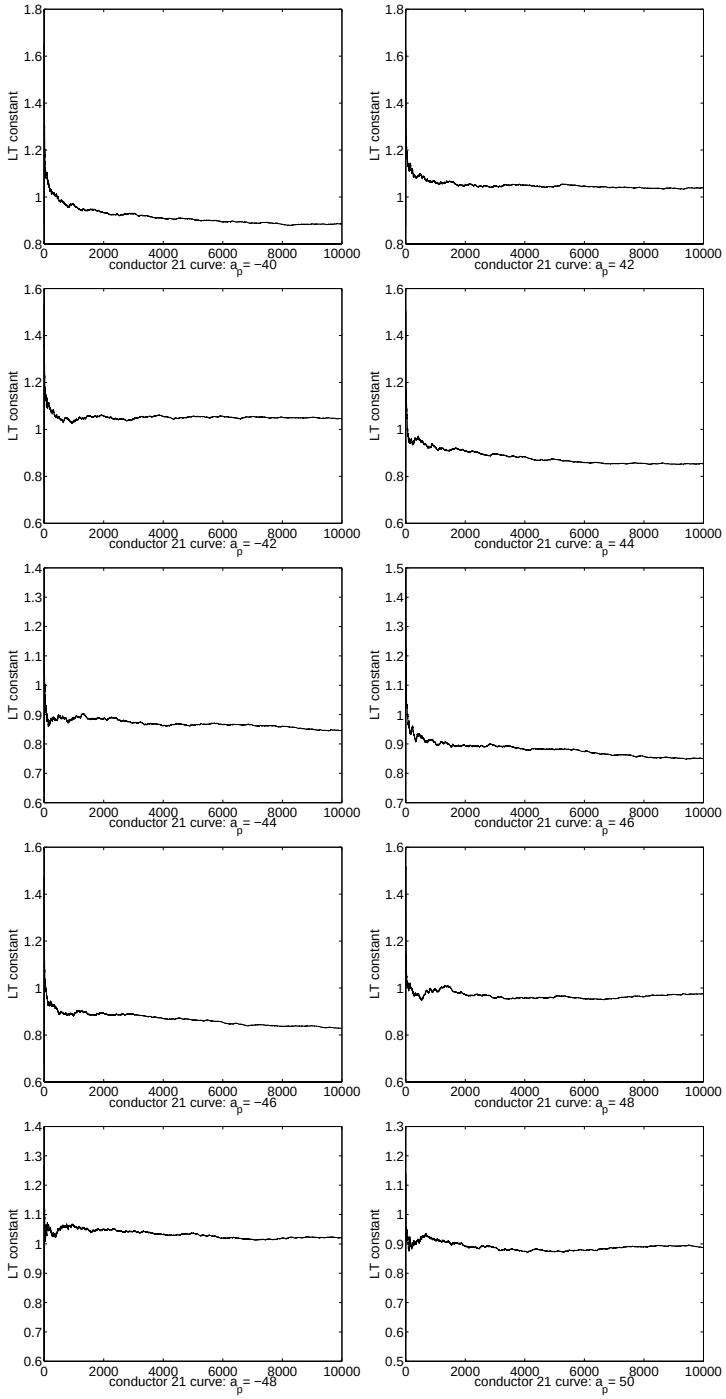

LT constant
conductor 20 curve: a_p = −46
LT constant
conductor 20 curve: a_p = 48
LT constant
conductor 20 curve: a_p = −48
LT constant
conductor 20 curve: a_p = 50

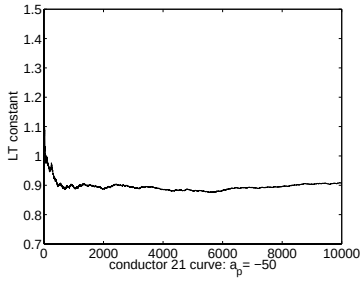

LT constant
conductor 21 curve: a_p= 0
conductor 21 curve: a_p= 2
conductor 21 curve: a_p= −2
conductor 21 curve: a_p= 4
conductor 21 curve: a_p= −4
conductor 21 curve: a_p= 6
conductor 21 curve: a_p= −6
conductor 21 curve: a_p= 8
conductor 21 curve: a_p= −8
conductor 21 curve: a_p= 10

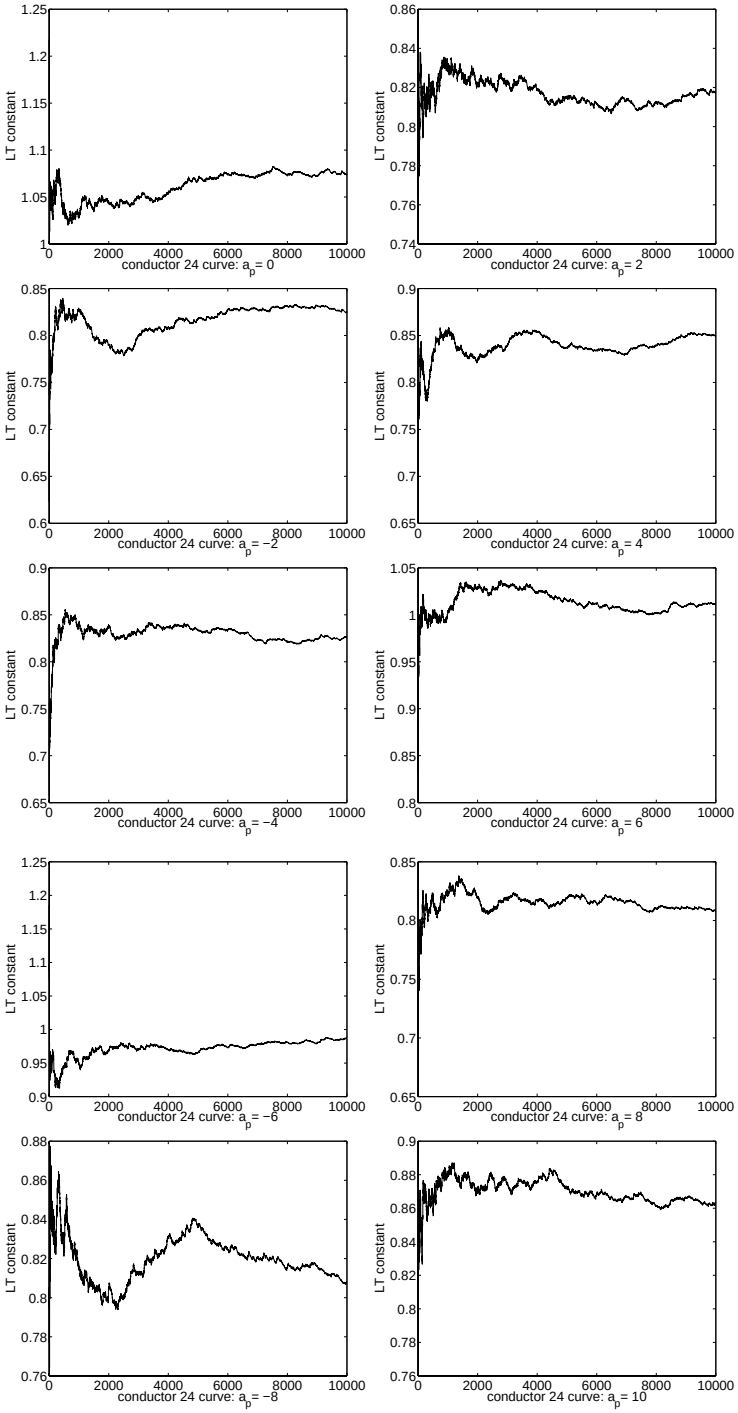

LT constant
conductor 21 curve: $a_p = -10$
conductor 21 curve: $a_p = 12$
conductor 21 curve: $a_p = -12$
conductor 21 curve: $a_p = 14$
conductor 21 curve: $a_p = -14$
conductor 21 curve: $a_p = 16$
conductor 21 curve: $a_p = -16$
conductor 21 curve: $a_p = 18$
conductor 21 curve: $a_p = -18$
conductor 21 curve: $a_p = 20$

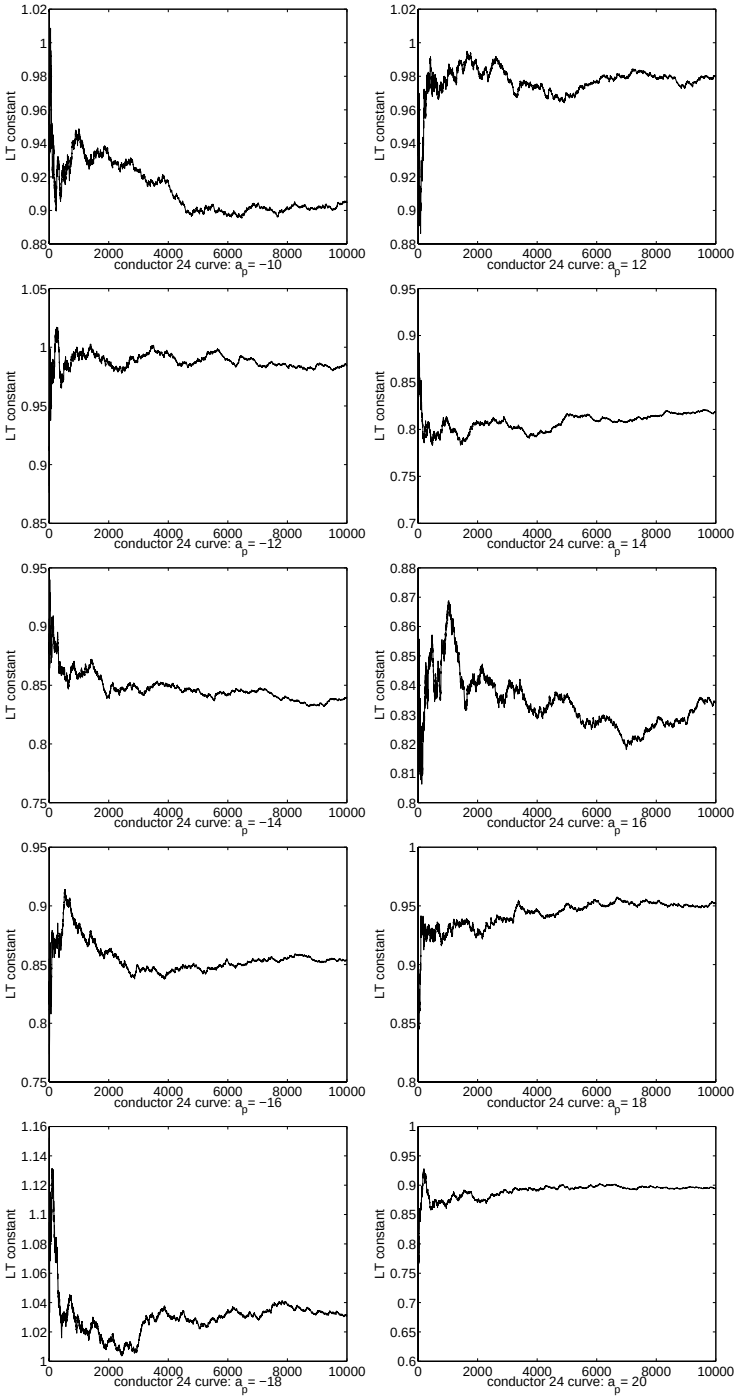

LT constant
conductor 21 curve: $a_p = -20$
conductor 21 curve: $a_p = 22$
conductor 21 curve: $a_p = -22$
conductor 21 curve: $a_p = 24$
conductor 21 curve: $a_p = -24$
conductor 21 curve: $a_p = 26$
conductor 21 curve: $a_p = -26$
conductor 21 curve: $a_p = 28$
conductor 21 curve: $a_p = -28$
conductor 21 curve: $a_p = 30$

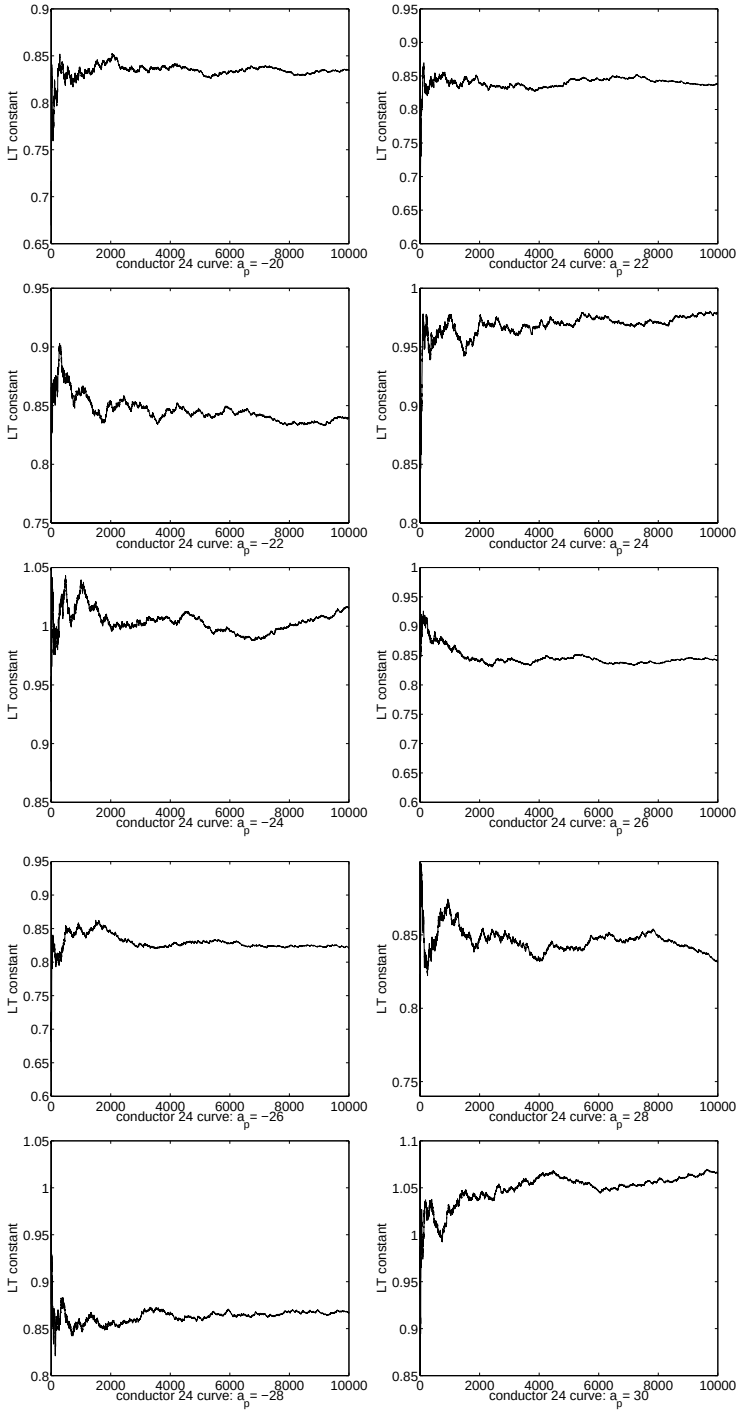

LT constant
conductor 21 curve: $a_p = -30$
conductor 21 curve: $a_p = 32$
conductor 21 curve: $a_p = -32$
conductor 21 curve: $a_p = 34$
conductor 21 curve: $a_p = -34$
conductor 21 curve: $a_p = 36$
conductor 21 curve: $a_p = -36$
conductor 21 curve: $a_p = 38$
conductor 21 curve: $a_p = -38$
conductor 21 curve: $a_p = 40$

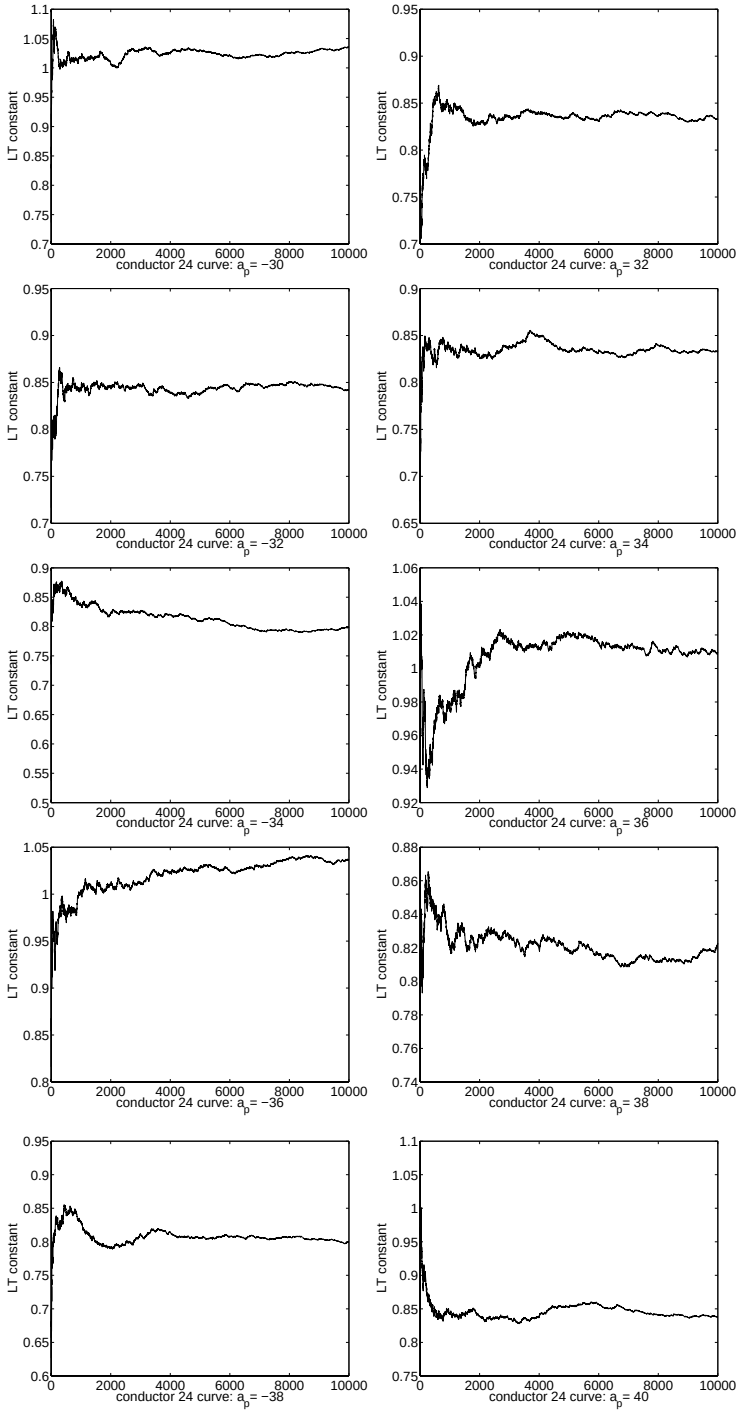

LT constant
conductor 21 curve: $a_p = -40$
conductor 21 curve: $a_p = 42$
conductor 21 curve: $a_p = -42$
conductor 21 curve: $a_p = 44$
conductor 21 curve: $a_p = -44$
conductor 21 curve: $a_p = 46$
conductor 21 curve: $a_p = -46$
conductor 21 curve: $a_p = 48$
conductor 21 curve: $a_p = -48$
conductor 21 curve: $a_p = 50$

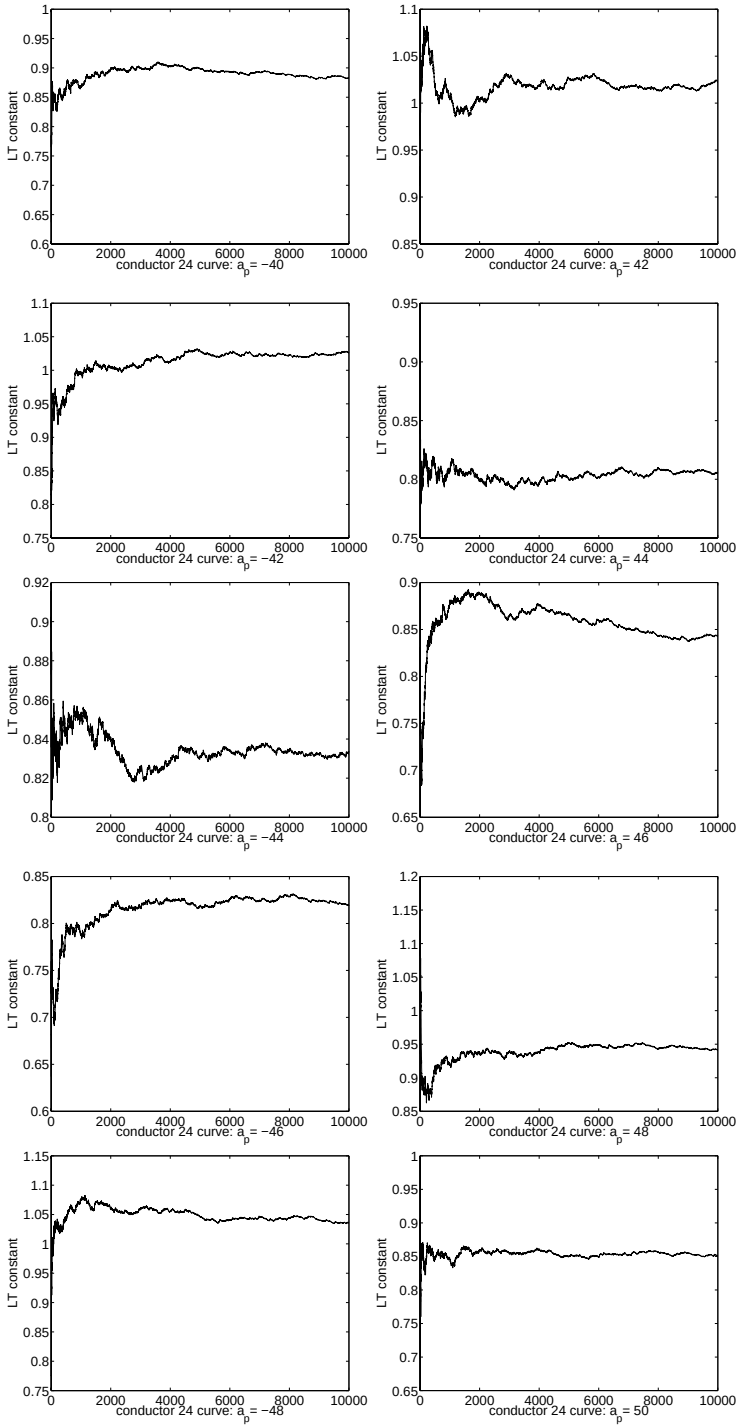

1.5
1.4
1.3
1.2
1.1
1
0.9
0.8
0.7
LT constant
0
2000
4000
6000
8000
10000
conductor 21 curve: $a_p = -50$

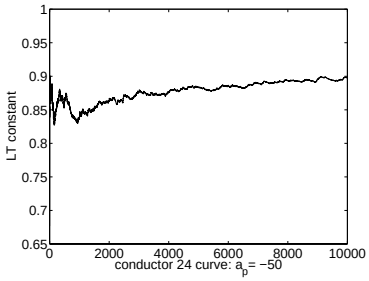

LT constant
conductor 24 curve: $a_p = 0$
conductor 24 curve: $a_p = 2$
conductor 24 curve: $a_p = -2$
conductor 24 curve: $a_p = 4$
conductor 24 curve: $a_p = -4$
conductor 24 curve: $a_p = 6$
conductor 24 curve: $a_p = -6$
conductor 24 curve: $a_p = 8$
conductor 24 curve: $a_p = -8$
conductor 24 curve: $a_p = 10$

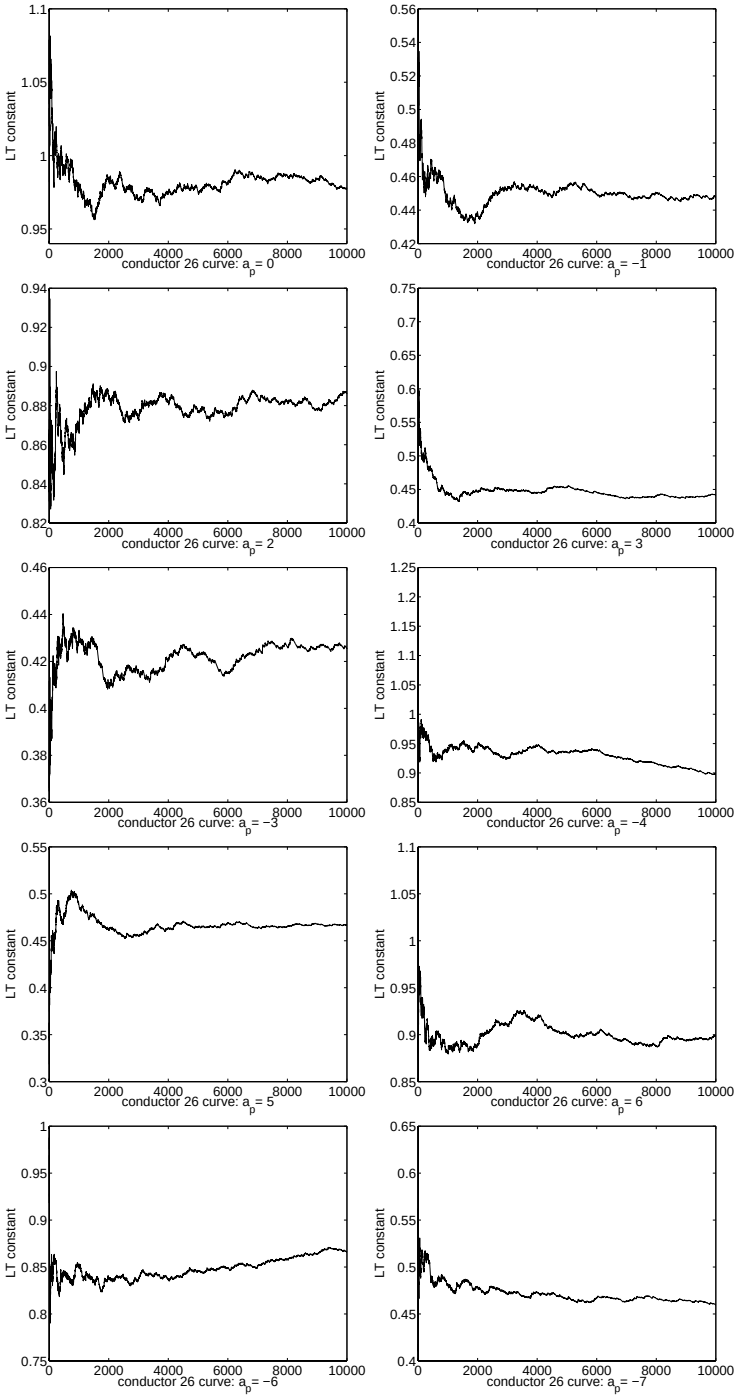

LT constant
conductor 24 curve: $a_p = -10$
conductor 24 curve: $a_p = 12$
conductor 24 curve: $a_p = -12$
conductor 24 curve: $a_p = 14$
conductor 24 curve: $a_p = -14$
conductor 24 curve: $a_p = 16$
conductor 24 curve: $a_p = -16$
conductor 24 curve: $a_p = 18$
conductor 24 curve: $a_p = -18$
conductor 24 curve: $a_p = 20$

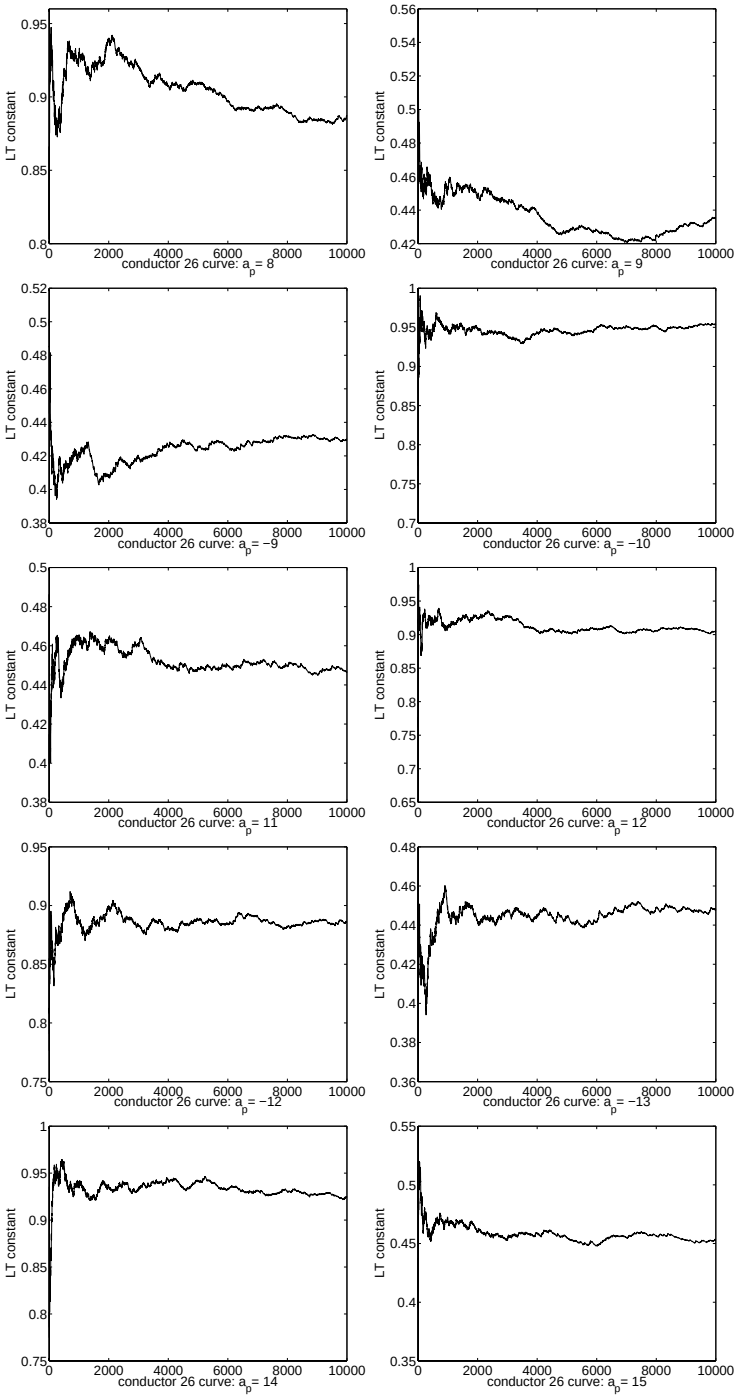

LT constant
conductor 24 curve: $a_p = -20$
conductor 24 curve: $a_p = 22$
conductor 24 curve: $a_p = -22$
conductor 24 curve: $a_p = 24$
conductor 24 curve: $a_p = -24$
conductor 24 curve: $a_p = 26$
conductor 24 curve: $a_p = -26$
conductor 24 curve: $a_p = 28$
conductor 24 curve: $a_p = -28$
conductor 24 curve: $a_p = 30$

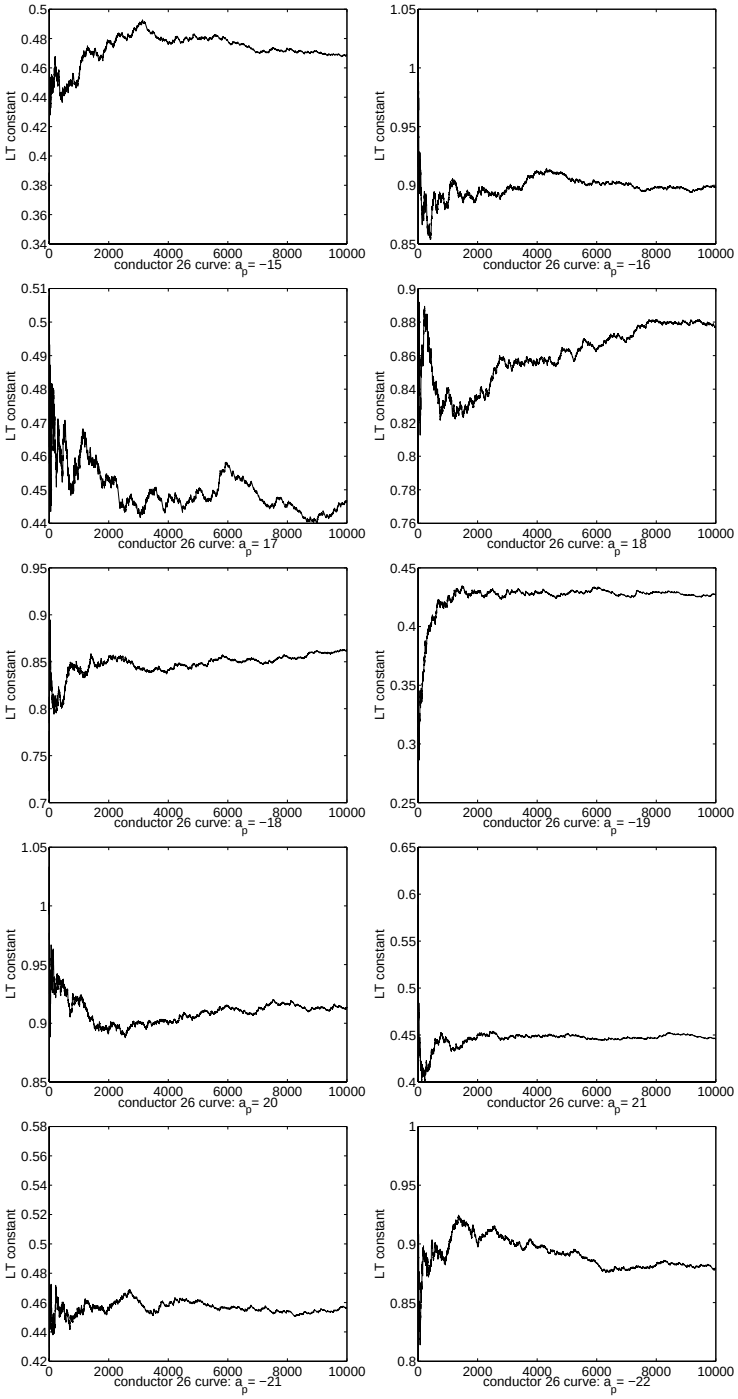

LT constant
conductor 24 curve: $a_p = -30$
conductor 24 curve: $a_p = 32$
conductor 24 curve: $a_p = -32$
conductor 24 curve: $a_p = 34$
conductor 24 curve: $a_p = -34$
conductor 24 curve: $a_p = 36$
conductor 24 curve: $a_p = -36$
conductor 24 curve: $a_p = 38$
conductor 24 curve: $a_p = -38$
conductor 24 curve: $a_p = 40$

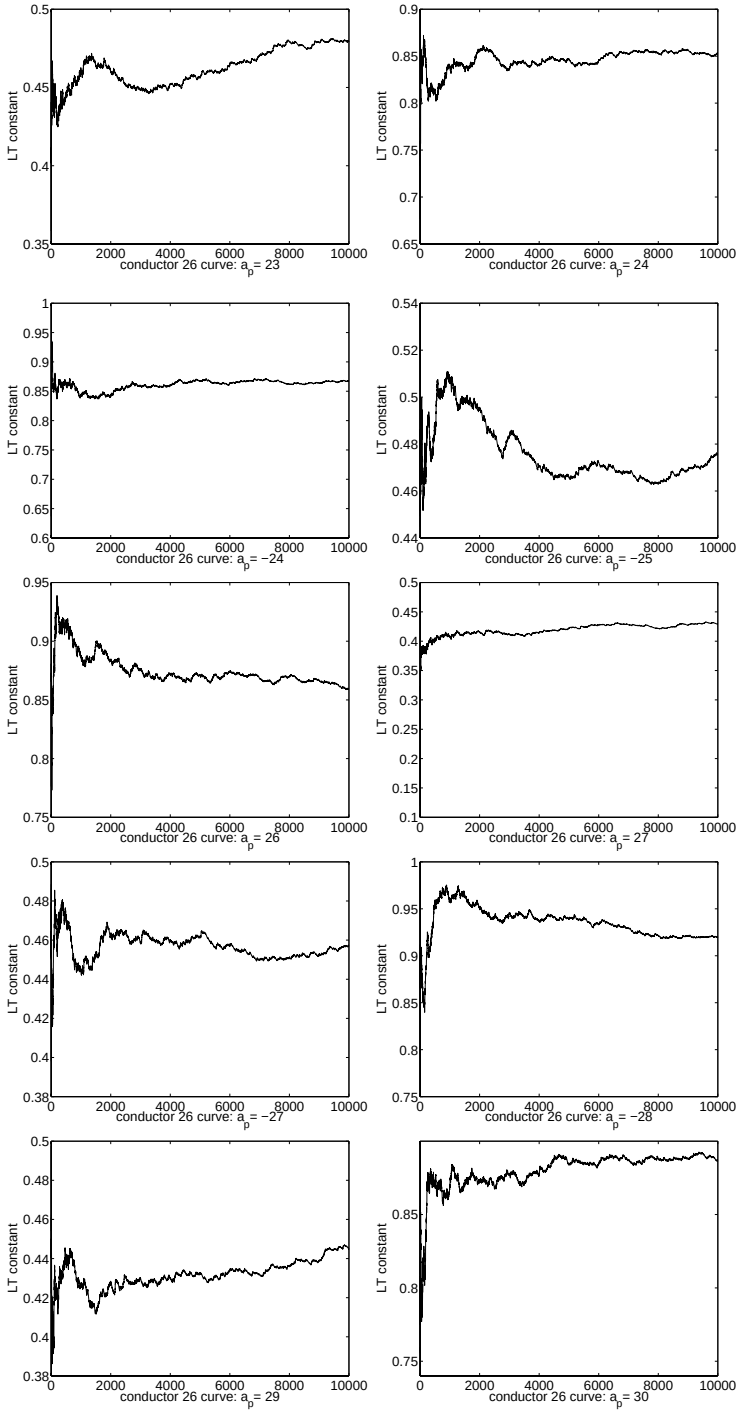

LT constant
conductor 24 curve: $a_p = -40$
conductor 24 curve: $a_p = 42$
conductor 24 curve: $a_p = -42$
conductor 24 curve: $a_p = 44$
conductor 24 curve: $a_p = -44$
conductor 24 curve: $a_p = 46$
conductor 24 curve: $a_p = -46$
conductor 24 curve: $a_p = 48$
conductor 24 curve: $a_p = -48$
conductor 24 curve: $a_p = 50$

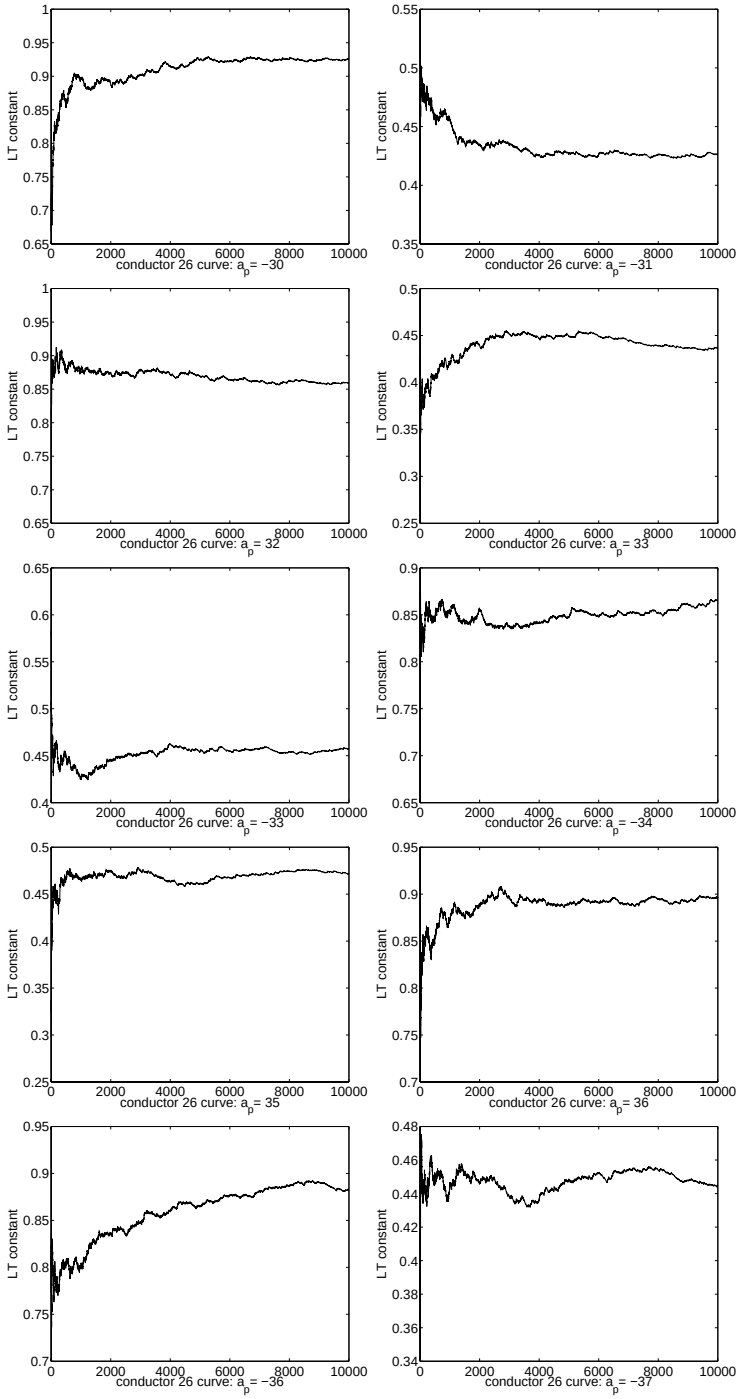

1
0.95
0.9
0.85
0.8
0.75
0.7
0.65
LT constant
0
2000
4000
6000
8000
10000
conductor 24 curve: a_p = −50

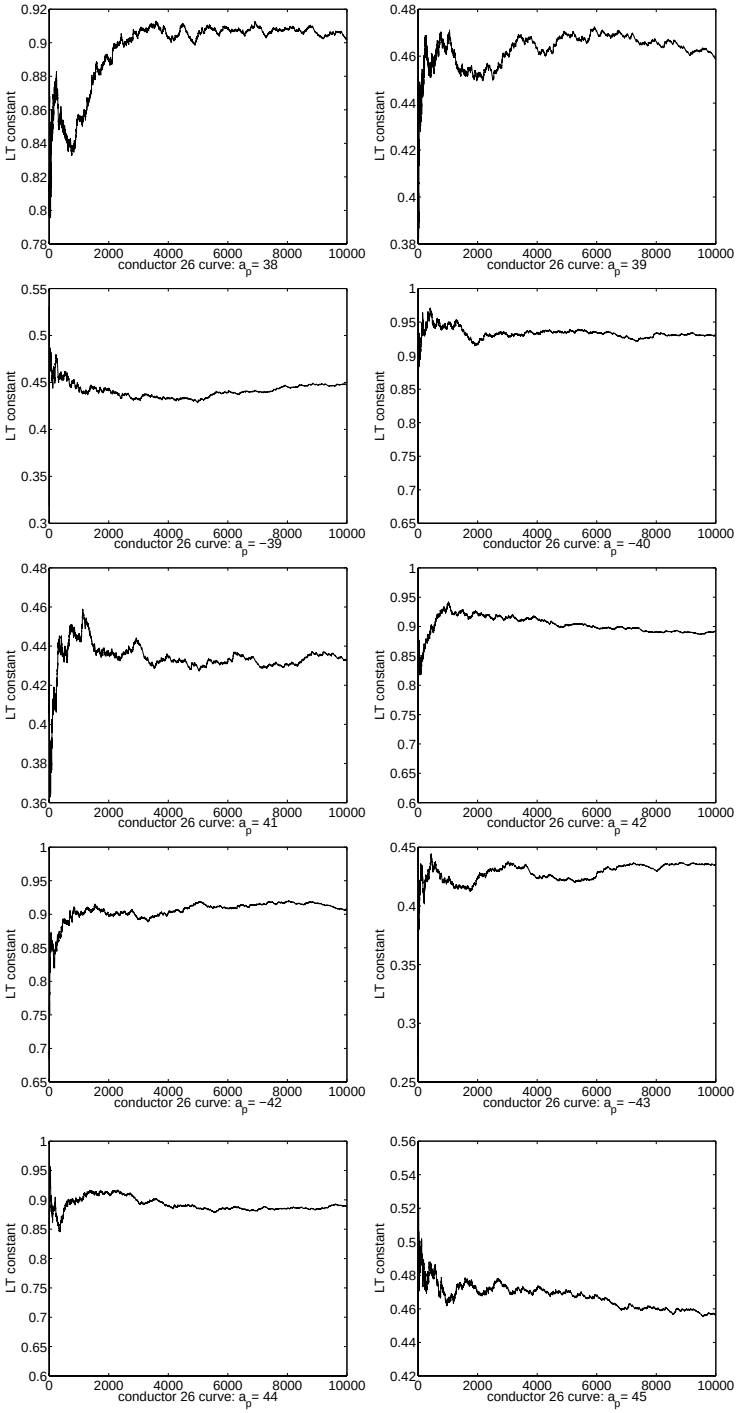

LT constant
conductor 26 curve: $a_p = 0$
conductor 26 curve: $a_p = -1$
conductor 26 curve: $a_p = 2$
conductor 26 curve: $a_p = 3$
conductor 26 curve: $a_p = -3$
conductor 26 curve: $a_p = -4$
conductor 26 curve: $a_p = 5$
conductor 26 curve: $a_p = 6$
conductor 26 curve: $a_p = -6$
conductor 26 curve: $a_p = -7$

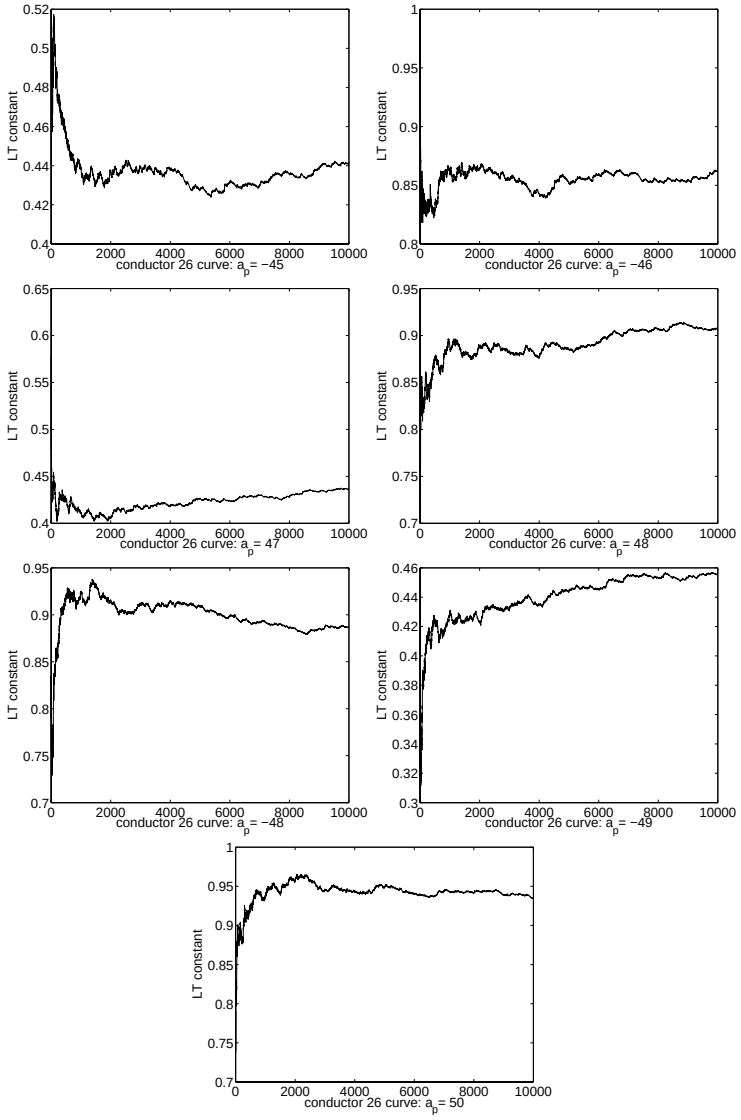

LT constant
conductor 26 curve: $a_p = 8$
conductor 26 curve: $a_p = 9$
conductor 26 curve: $a_p = -9$
conductor 26 curve: $a_p = -10$
conductor 26 curve: $a_p = 11$
conductor 26 curve: $a_p = 12$
conductor 26 curve: $a_p = -12$
conductor 26 curve: $a_p = -13$
conductor 26 curve: $a_p = 14$
conductor 26 curve: $a_p = 15$

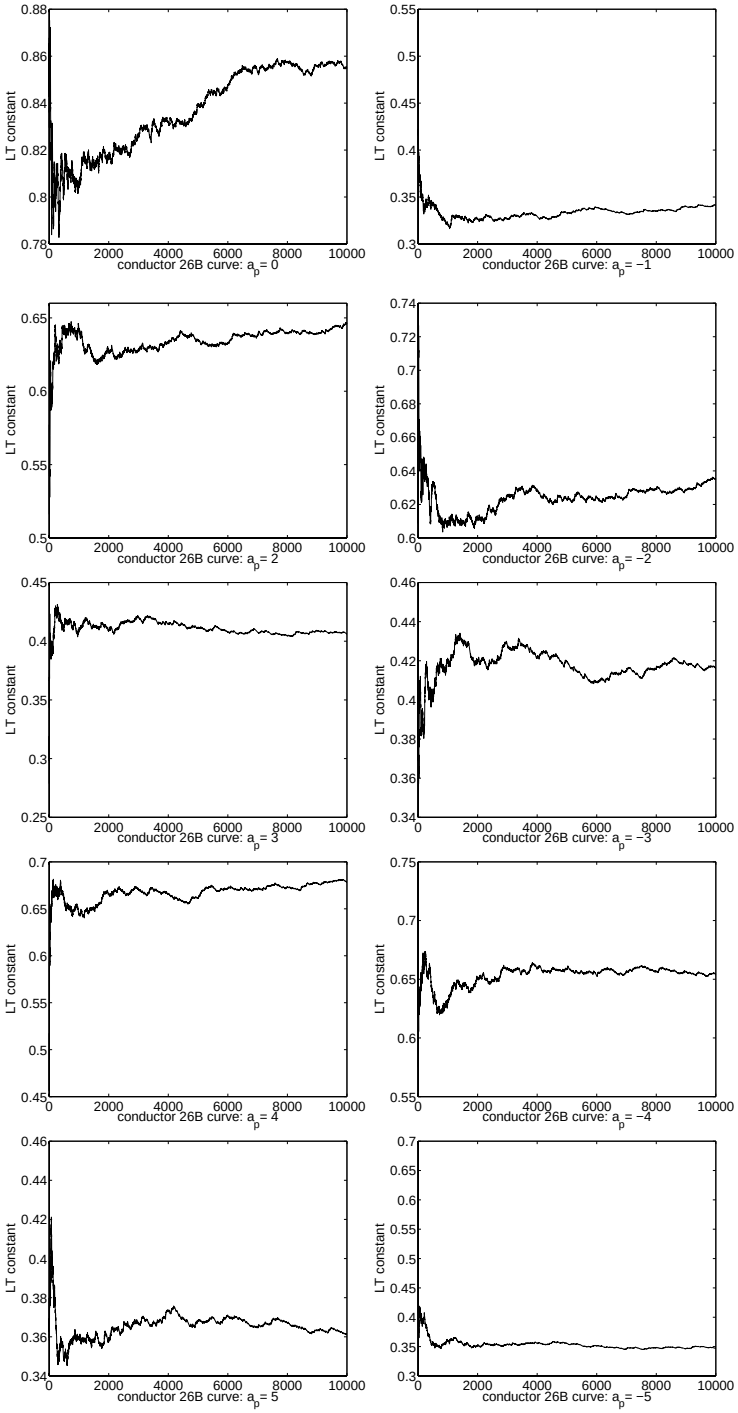

LT constant
conductor 26 curve: $a_p = -15$
conductor 26 curve: $a_p = -16$
conductor 26 curve: $a_p = 17$
conductor 26 curve: $a_p = 18$
conductor 26 curve: $a_p = -18$
conductor 26 curve: $a_p = -19$
conductor 26 curve: $a_p = 20$
conductor 26 curve: $a_p = 21$
conductor 26 curve: $a_p = -21$
conductor 26 curve: $a_p = -22$

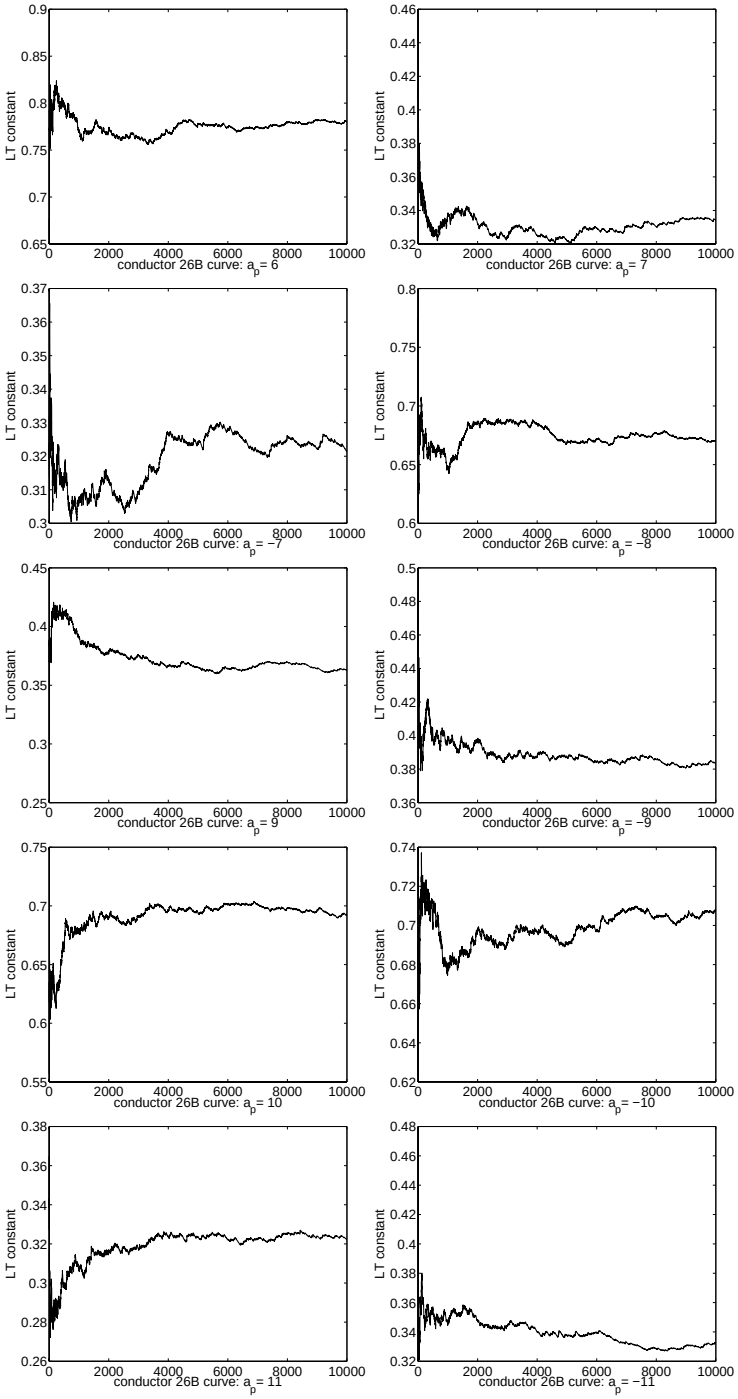

LT constant
conductor 26 curve: a_p= 23
conductor 26 curve: a_p= 24
conductor 26 curve: a_p= −24
conductor 26 curve: a_p= −25
conductor 26 curve: a_p= 26
conductor 26 curve: a_p= 27
conductor 26 curve: a_p= −27
conductor 26 curve: a_p= −28
conductor 26 curve: a_p= 29
conductor 26 curve: a_p= 30

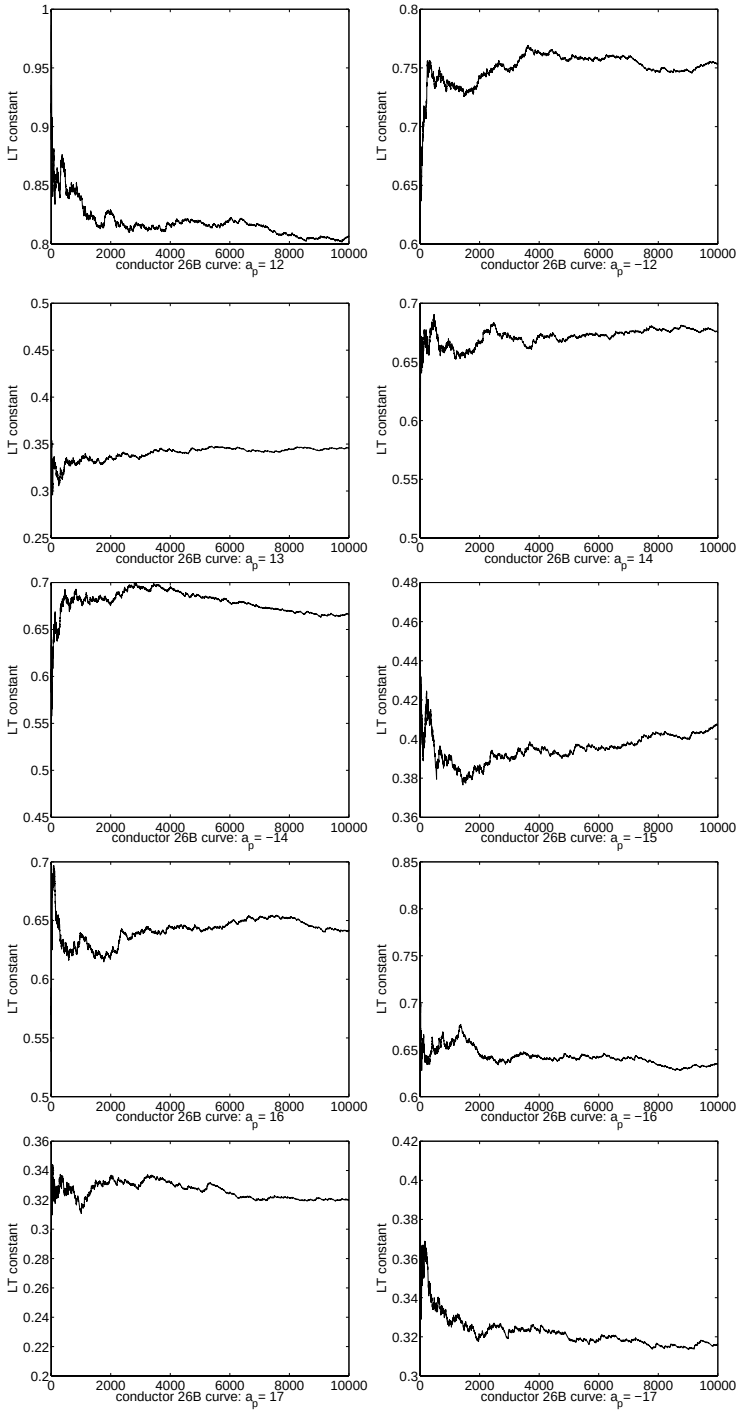

LT constant
conductor 26 curve: $a_p = -30$
conductor 26 curve: $a_p = -31$
conductor 26 curve: $a_p = 32$
conductor 26 curve: $a_p = 33$
conductor 26 curve: $a_p = -33$
conductor 26 curve: $a_p = -34$
conductor 26 curve: $a_p = 35$
conductor 26 curve: $a_p = 36$
conductor 26 curve: $a_p = -36$
conductor 26 curve: $a_p = -37$

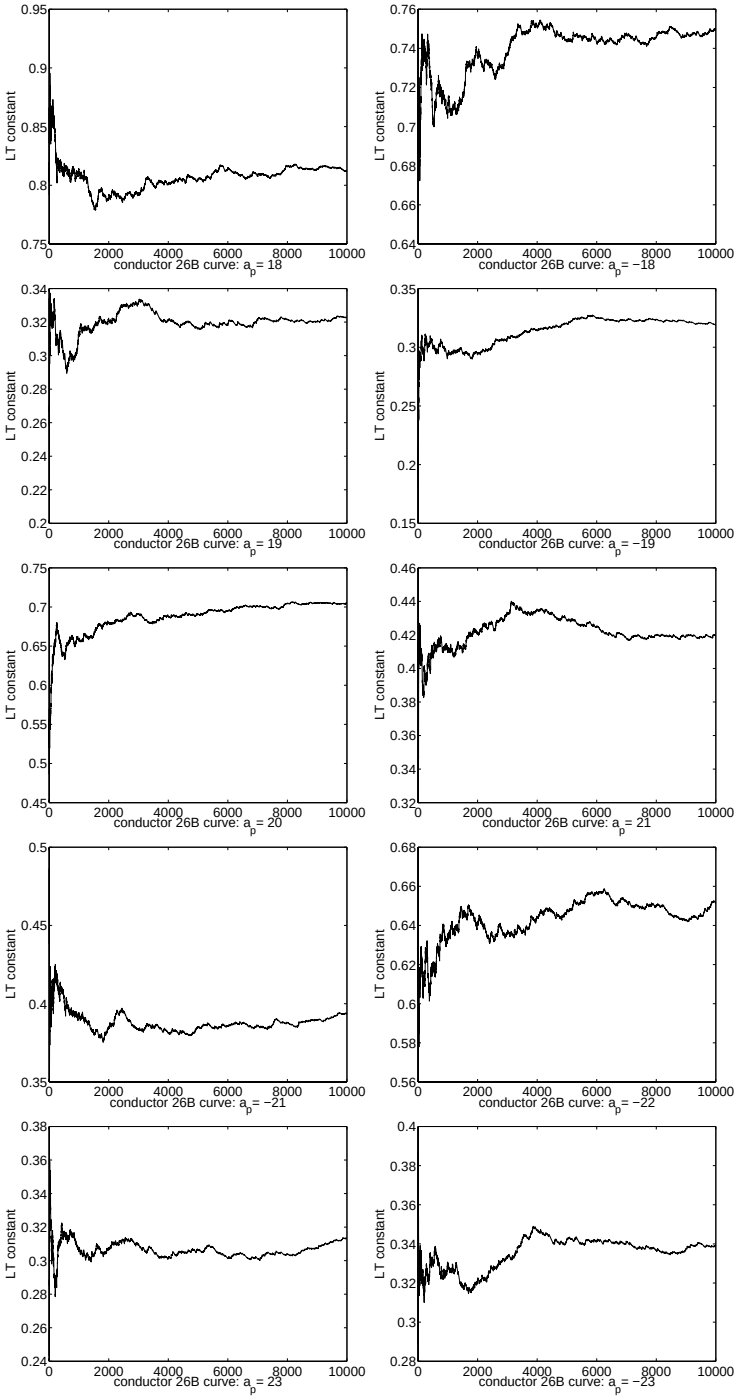

LT constant
conductor 26 curve: $a_p = 38$
conductor 26 curve: $a_p = 39$
conductor 26 curve: $a_p = -39$
conductor 26 curve: $a_p = -40$
conductor 26 curve: $a_p = 41$
conductor 26 curve: $a_p = 42$
conductor 26 curve: $a_p = -42$
conductor 26 curve: $a_p = -43$
conductor 26 curve: $a_p = 44$
conductor 26 curve: $a_p = 45$

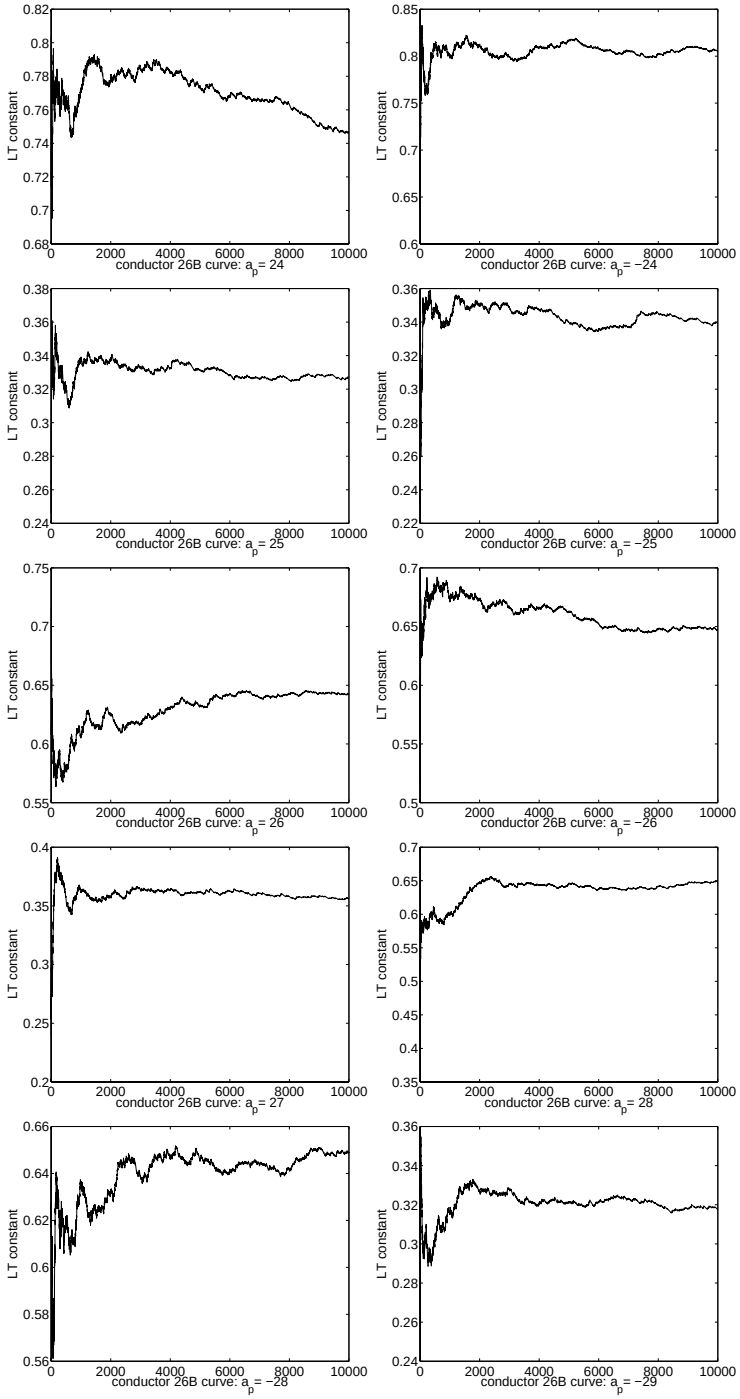

LT constant
conductor 26 curve: $a_p = -45$
conductor 26 curve: $a_p = -46$
conductor 26 curve: $a_p = 47$
conductor 26 curve: $a_p = 48$
conductor 26 curve: $a_p = -48$
conductor 26 curve: $a_p = -49$
conductor 26 curve: $a_p = 50$

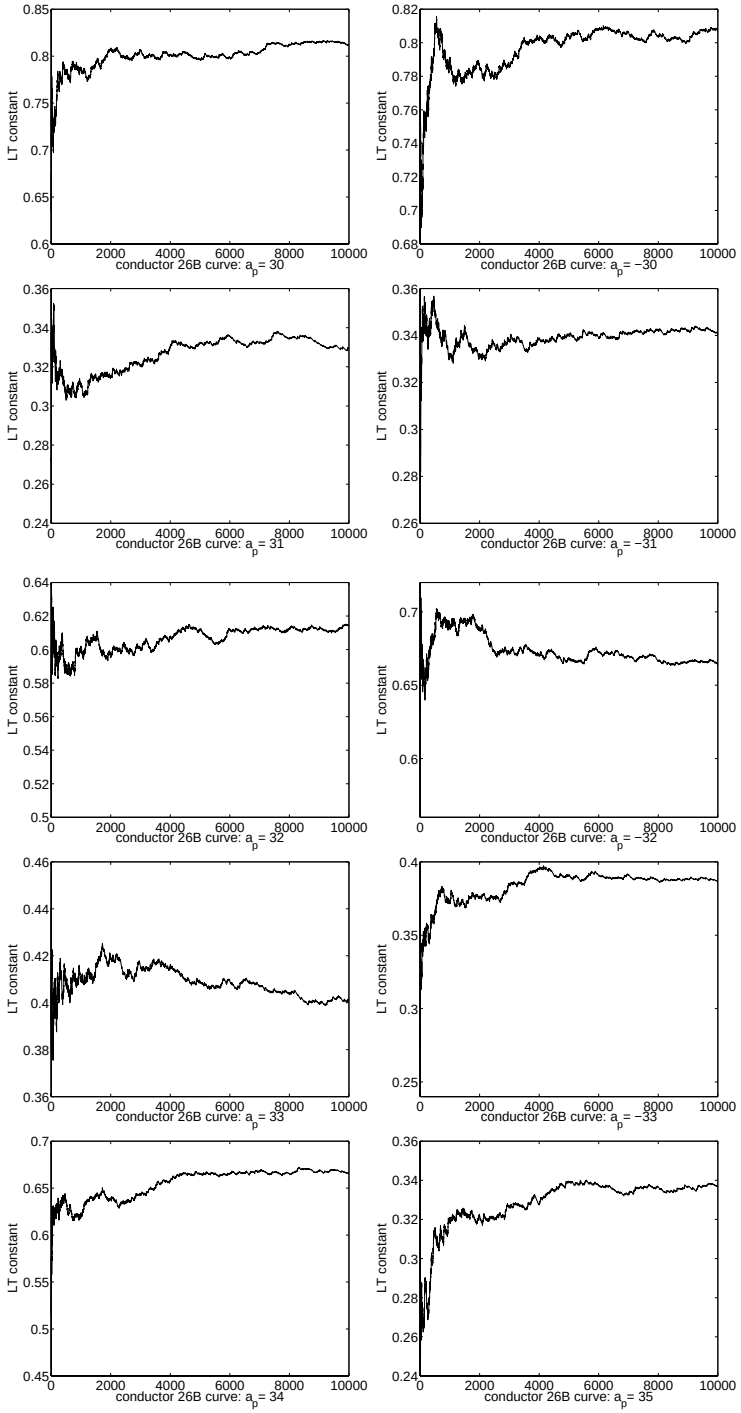

LT constant
conductor 26B curve: $a_p = 0$
conductor 26B curve: $a_p = -1$
conductor 26B curve: $a_p = 2$
conductor 26B curve: $a_p = -2$
conductor 26B curve: $a_p = 3$
conductor 26B curve: $a_p = -3$
conductor 26B curve: $a_p = 4$
conductor 26B curve: $a_p = -4$
conductor 26B curve: $a_p = 5$
conductor 26B curve: $a_p = -5$

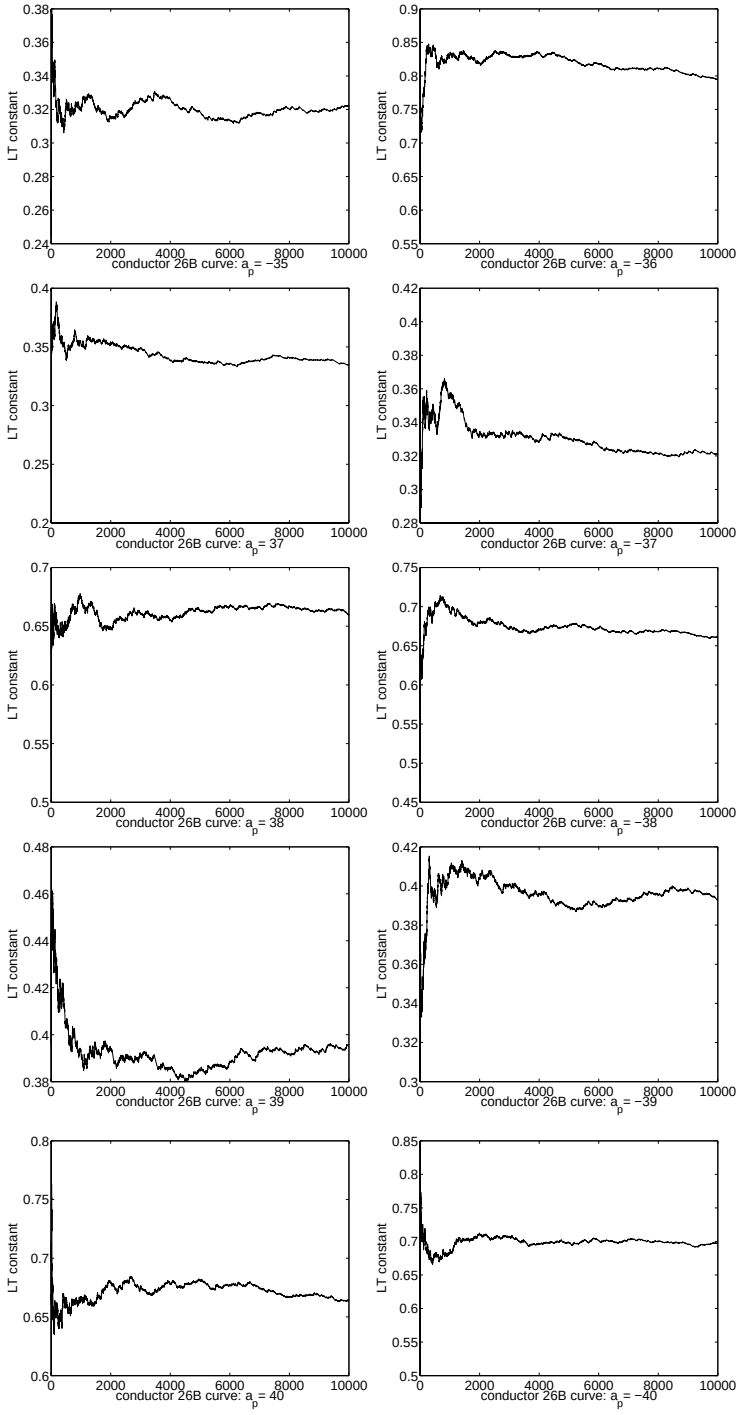

LT constant
conductor 26B curve: $a_p = 6$
conductor 26B curve: $a_p = 7$
conductor 26B curve: $a_p = -7$
conductor 26B curve: $a_p = -8$
conductor 26B curve: $a_p = 9$
conductor 26B curve: $a_p = -9$
conductor 26B curve: $a_p = 10$
conductor 26B curve: $a_p = -10$
conductor 26B curve: $a_p = 11$
conductor 26B curve: $a_p = -11$

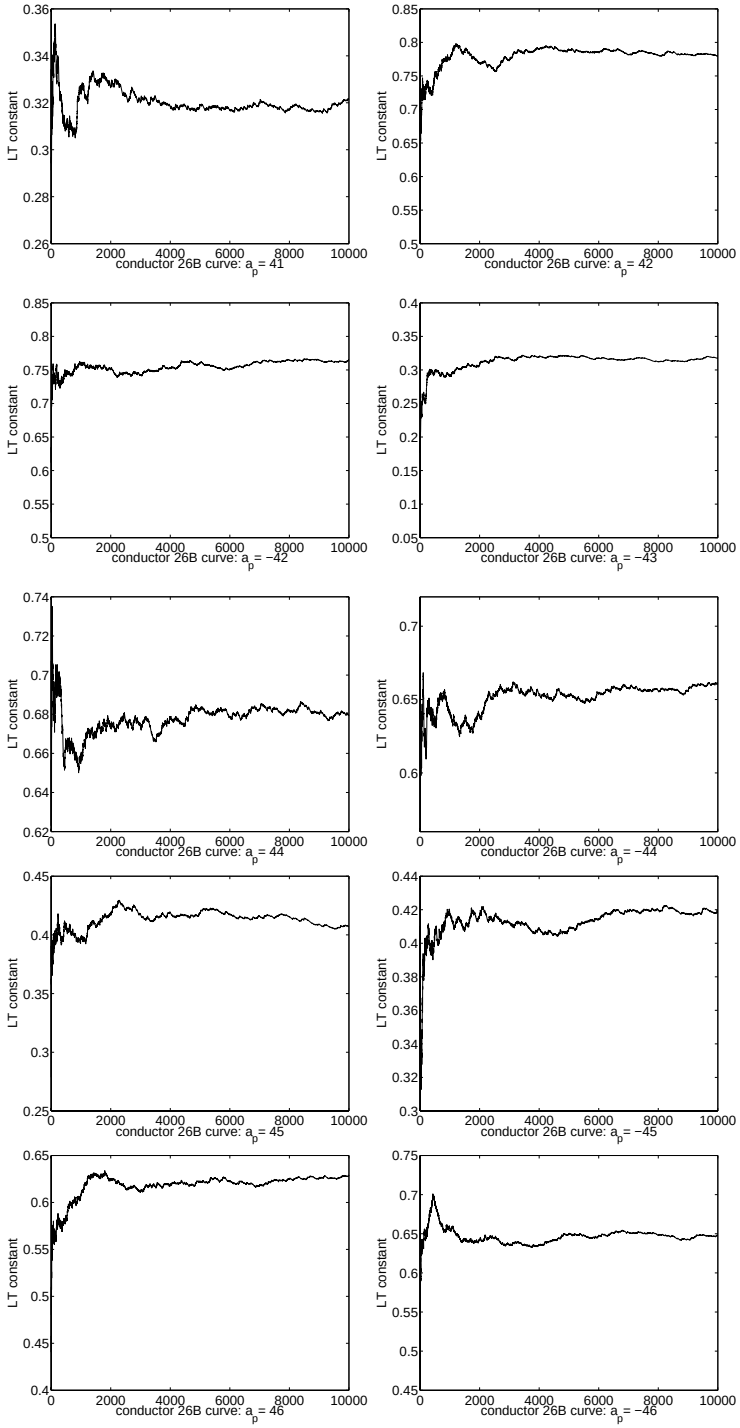

LT constant
conductor 26B curve: $a_p = 12$
conductor 26B curve: $a_p = -12$
conductor 26B curve: $a_p = 13$
conductor 26B curve: $a_p = 14$
conductor 26B curve: $a_p = -14$
conductor 26B curve: $a_p = -15$
conductor 26B curve: $a_p = 16$
conductor 26B curve: $a_p = -16$
conductor 26B curve: $a_p = 17$
conductor 26B curve: $a_p = -17$

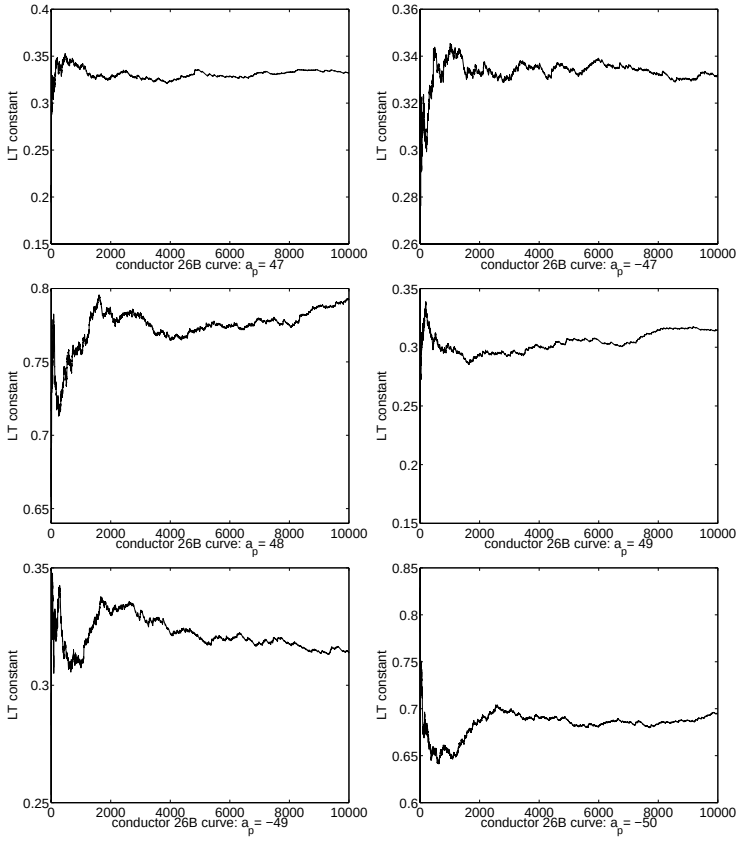

LT constant
conductor 26B curve: $a_p = 18$
conductor 26B curve: $a_p = -18$
conductor 26B curve: $a_p = 19$
conductor 26B curve: $a_p = -19$
conductor 26B curve: $a_p = 20$
conductor 26B curve: $a_p = 21$
conductor 26B curve: $a_p = -21$
conductor 26B curve: $a_p = -22$
conductor 26B curve: $a_p = 23$
conductor 26B curve: $a_p = -23$

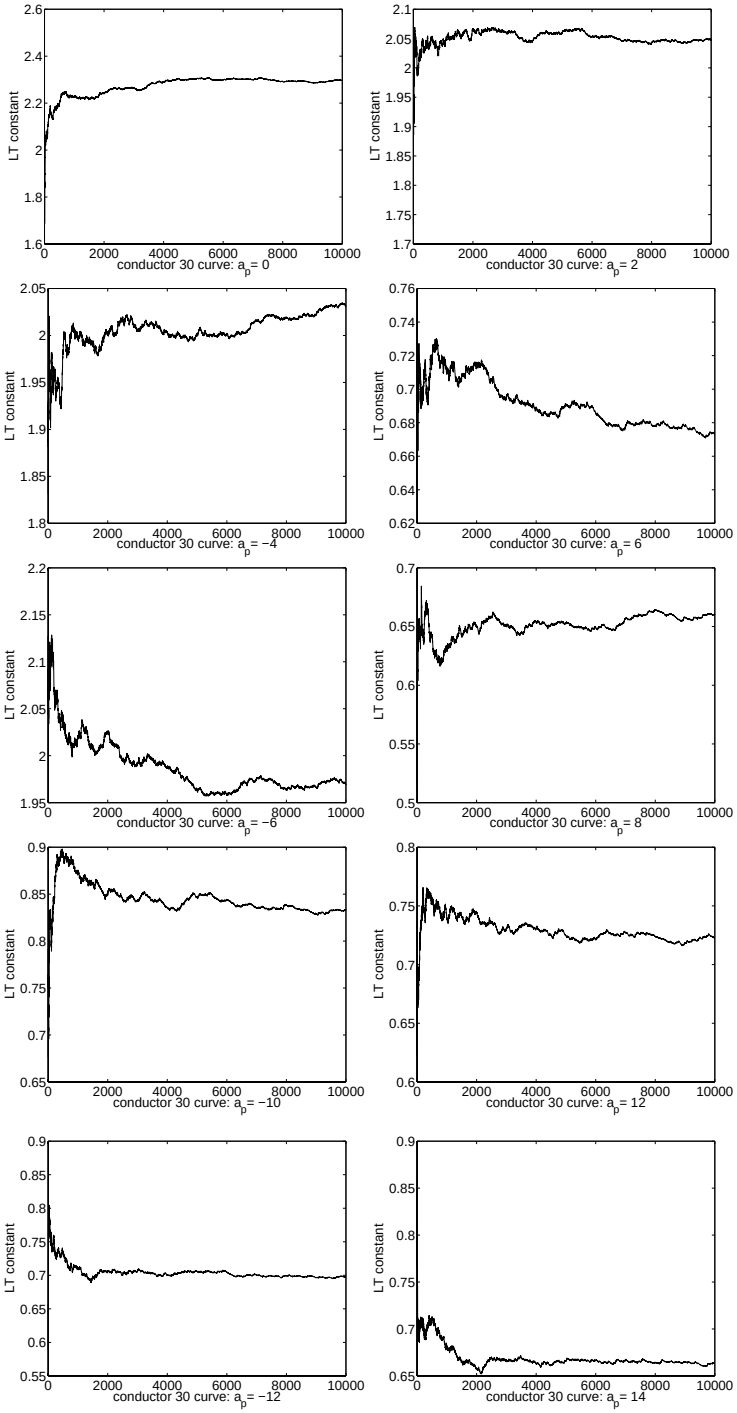

LT constant
conductor 26B curve: $a_p = 24$
conductor 26B curve: $a_p = -24$
conductor 26B curve: $a_p = 25$
conductor 26B curve: $a_p = -25$
conductor 26B curve: $a_p = 26$
conductor 26B curve: $a_p = -26$
conductor 26B curve: $a_p = 27$
conductor 26B curve: $a_p = 28$
conductor 26B curve: $a_p = -28$
conductor 26B curve: $a_p = -29$

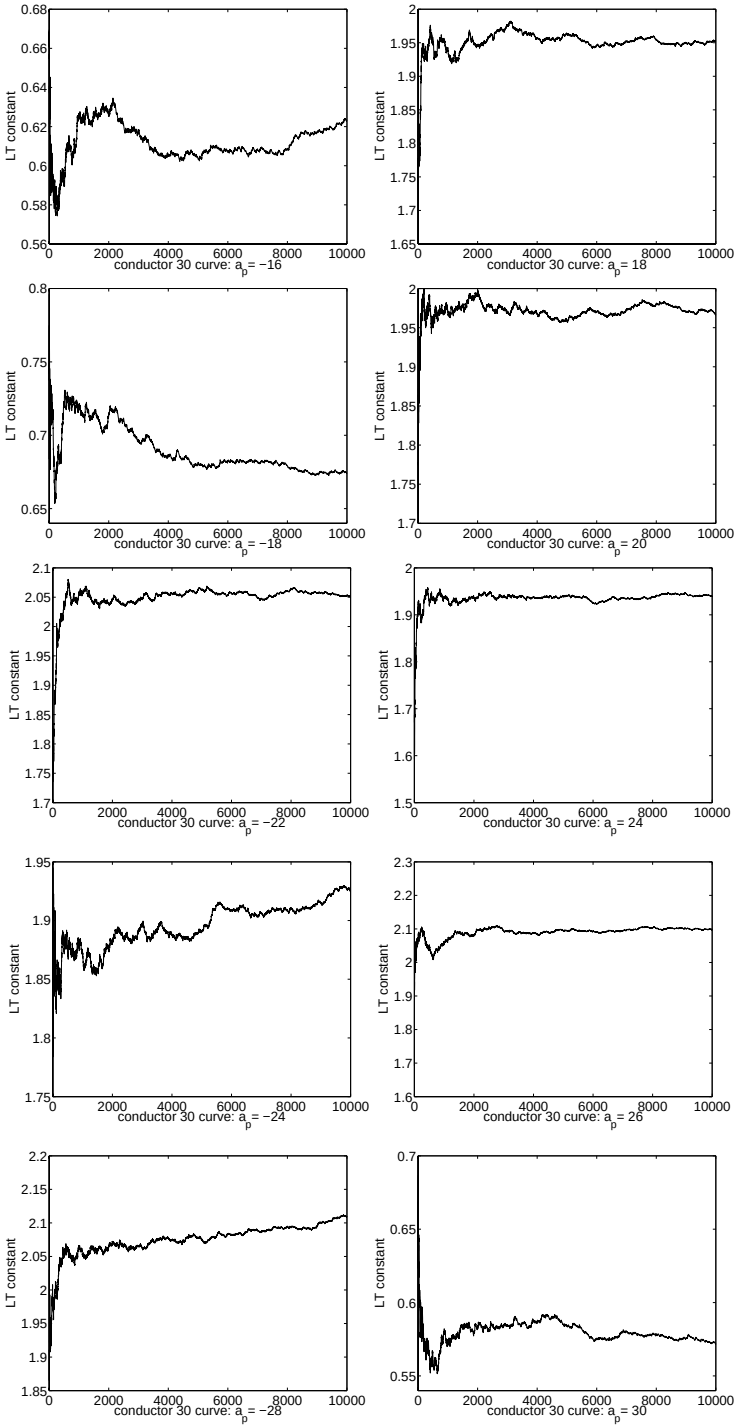

LT constant
conductor 26B curve: $a_p = 30$
conductor 26B curve: $a_p = -30$
conductor 26B curve: $a_p = 31$
conductor 26B curve: $a_p = -31$
conductor 26B curve: $a_p = 32$
conductor 26B curve: $a_p = -32$
conductor 26B curve: $a_p = 33$
conductor 26B curve: $a_p = -33$
conductor 26B curve: $a_p = 34$
conductor 26B curve: $a_p = 35$

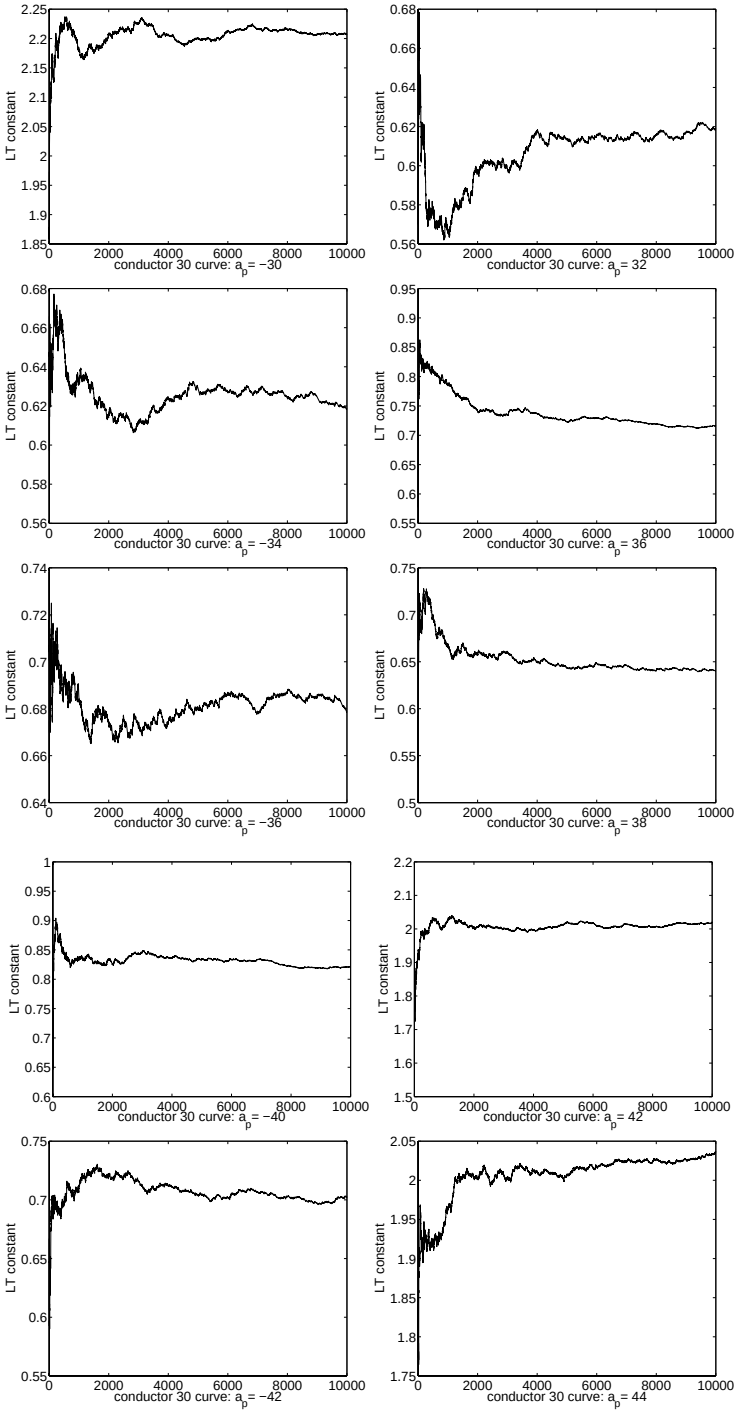

LT constant
conductor 26B curve: $a_p = -35$
conductor 26B curve: $a_p = -36$
conductor 26B curve: $a_p = 37$
conductor 26B curve: $a_p = -37$
conductor 26B curve: $a_p = 38$
conductor 26B curve: $a_p = -38$
conductor 26B curve: $a_p = 39$
conductor 26B curve: $a_p = -39$
conductor 26B curve: $a_p = 40$
conductor 26B curve: $a_p = -40$

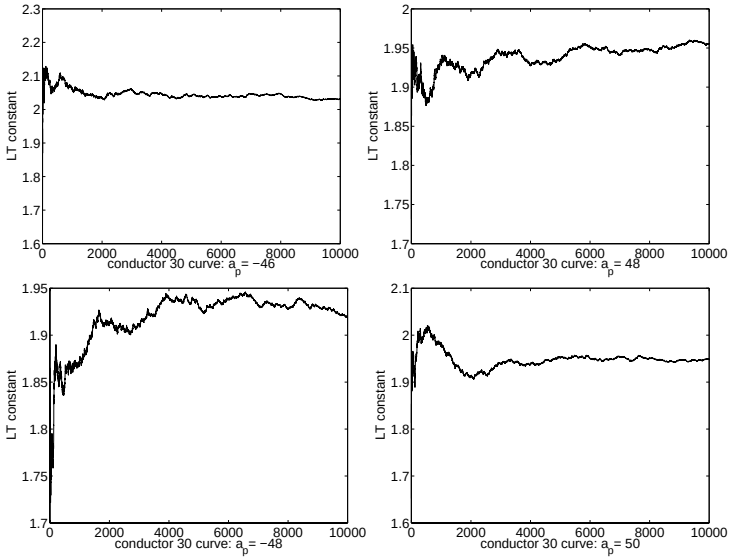

LT constant
conductor 26B curve: $a_p = 41$
conductor 26B curve: $a_p = 42$
conductor 26B curve: $a_p = -42$
conductor 26B curve: $a_p = -43$
conductor 26B curve: $a_p = 44$
conductor 26B curve: $a_p = -44$
conductor 26B curve: $a_p = 45$
conductor 26B curve: $a_p = -45$
conductor 26B curve: $a_p = 46$
conductor 26B curve: $a_p = -46$

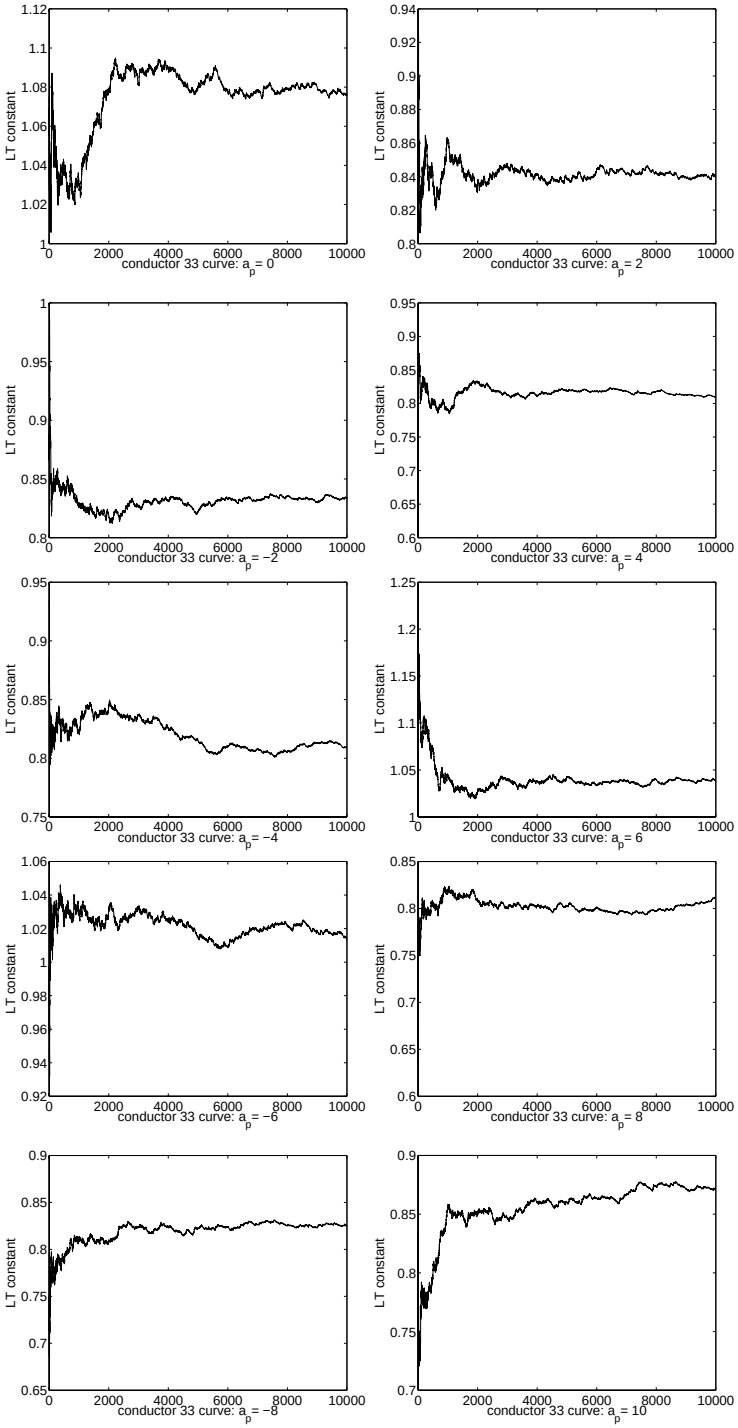

LT constant
conductor 26B curve: $a_p = 47$
LT constant
conductor 26B curve: $a_p = -47$
LT constant
conductor 26B curve: $a_p = 48$
LT constant
conductor 26B curve: $a_p = 49$
LT constant
conductor 26B curve: $a_p = -49$
LT constant
conductor 26B curve: $a_p = -50$

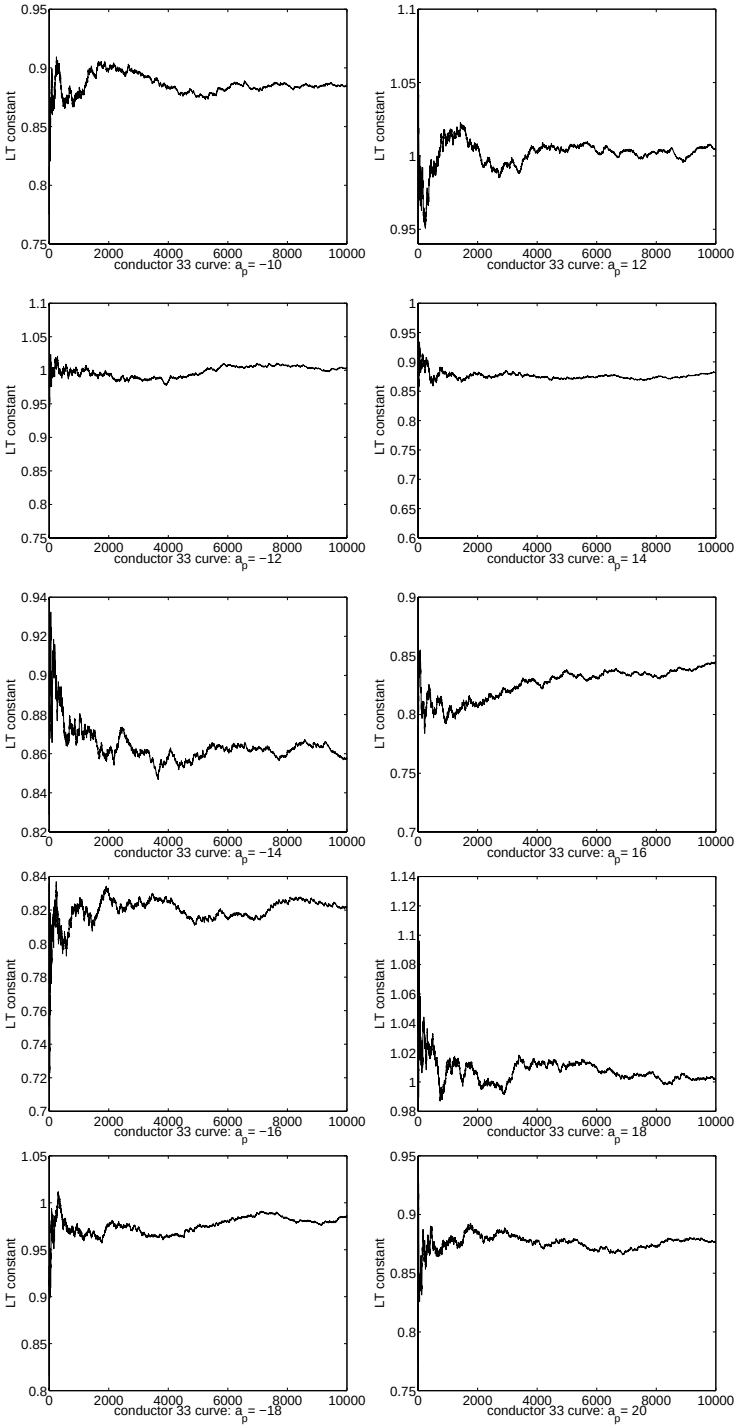

LT constant
conductor 30 curve: $a_p = 0$
conductor 30 curve: $a_p = 2$
conductor 30 curve: $a_p = -4$
conductor 30 curve: $a_p = 6$
conductor 30 curve: $a_p = -6$
conductor 30 curve: $a_p = 8$
conductor 30 curve: $a_p = -10$
conductor 30 curve: $a_p = 12$
conductor 30 curve: $a_p = -12$
conductor 30 curve: $a_p = 14$

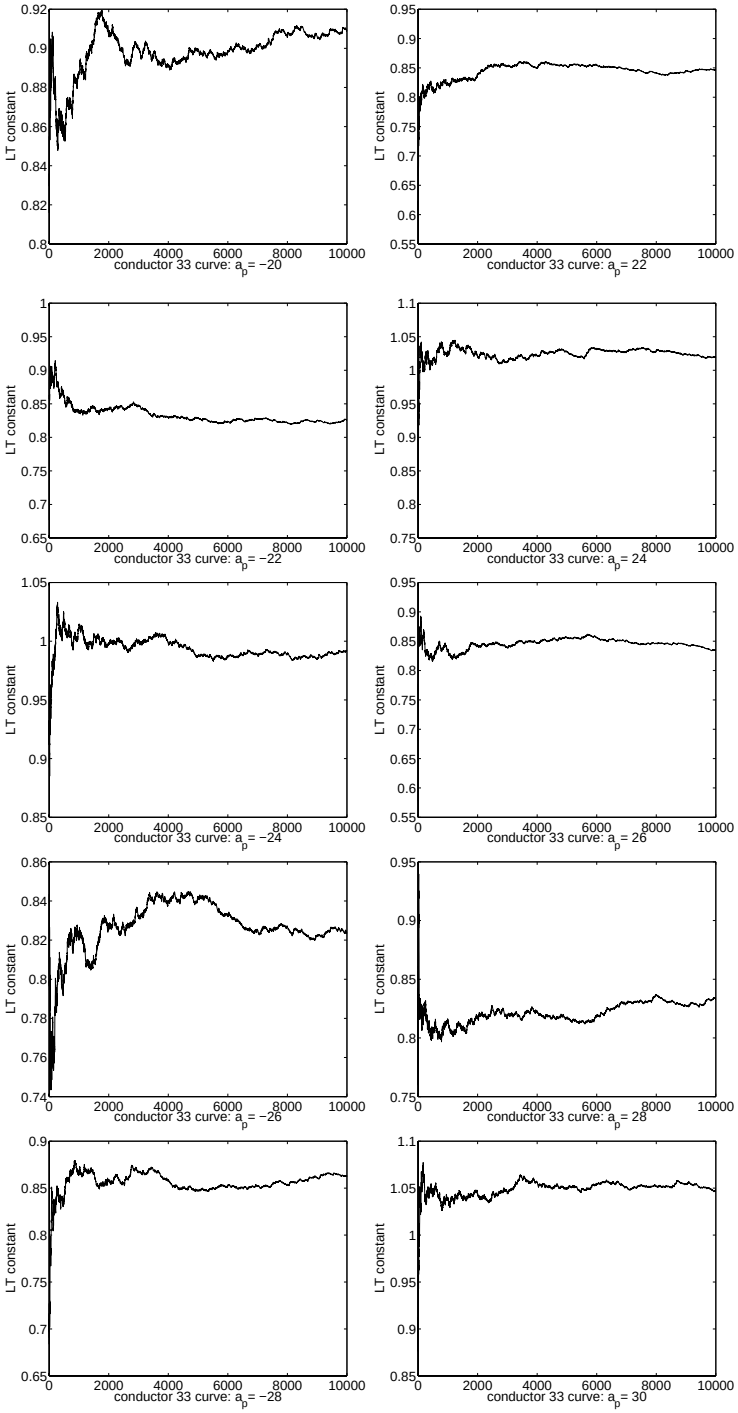

LT constant
conductor 30 curve: $a_p = -16$
conductor 30 curve: $a_p = 18$
conductor 30 curve: $a_p = -18$
conductor 30 curve: $a_p = 20$
conductor 30 curve: $a_p = -22$
conductor 30 curve: $a_p = 24$
conductor 30 curve: $a_p = -24$
conductor 30 curve: $a_p = 26$
conductor 30 curve: $a_p = -28$
conductor 30 curve: $a_p = 30$

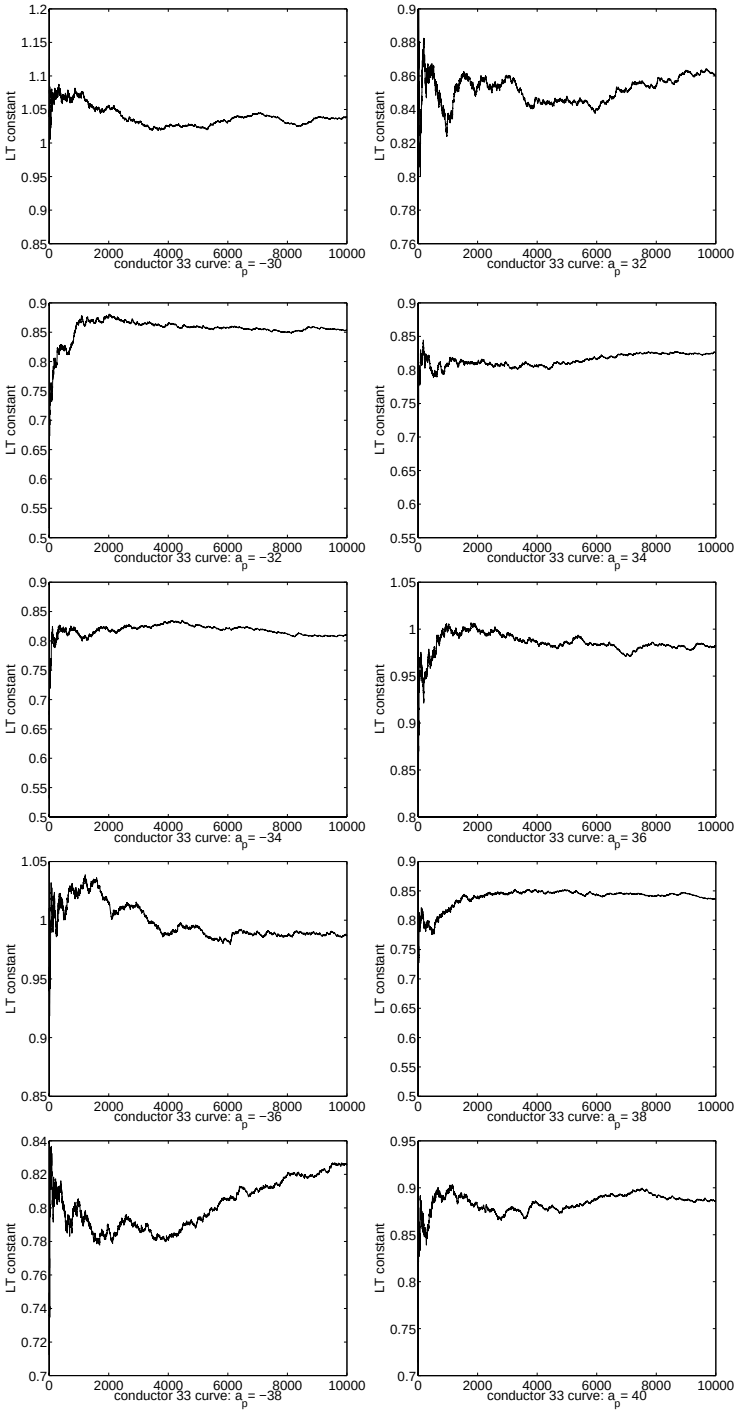

LT constant
conductor 30 curve: $a_p = -30$
conductor 30 curve: $a_p = 32$
conductor 30 curve: $a_p = -34$
conductor 30 curve: $a_p = 36$
conductor 30 curve: $a_p = -36$
conductor 30 curve: $a_p = 38$
conductor 30 curve: $a_p = -40$
conductor 30 curve: $a_p = 42$
conductor 30 curve: $a_p = -42$
conductor 30 curve: $a_p = 44$

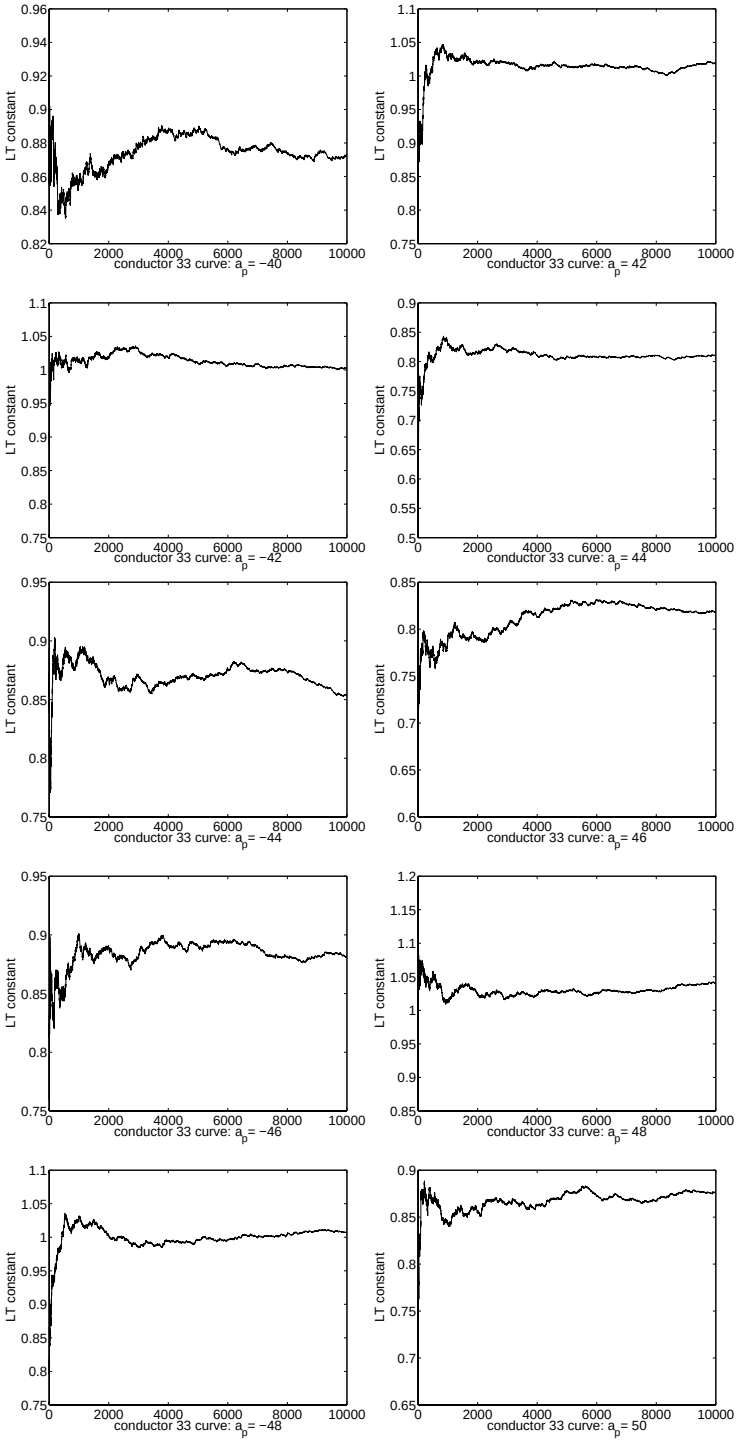

LT constant
conductor 30 curve: a_p = −46
LT constant
conductor 30 curve: a_p = 48
LT constant
conductor 30 curve: a_p = −48
LT constant
conductor 30 curve: a_p = 50

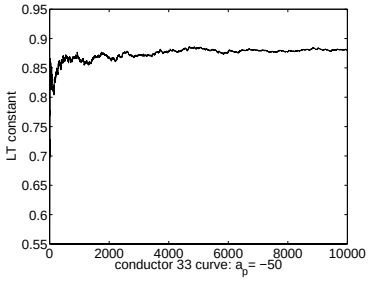

LT constant
conductor 33 curve: $a_p = 0$
conductor 33 curve: $a_p = 2$
conductor 33 curve: $a_p = -2$
conductor 33 curve: $a_p = 4$
conductor 33 curve: $a_p = -4$
conductor 33 curve: $a_p = 6$
conductor 33 curve: $a_p = -6$
conductor 33 curve: $a_p = 8$
conductor 33 curve: $a_p = -8$
conductor 33 curve: $a_p = 10$

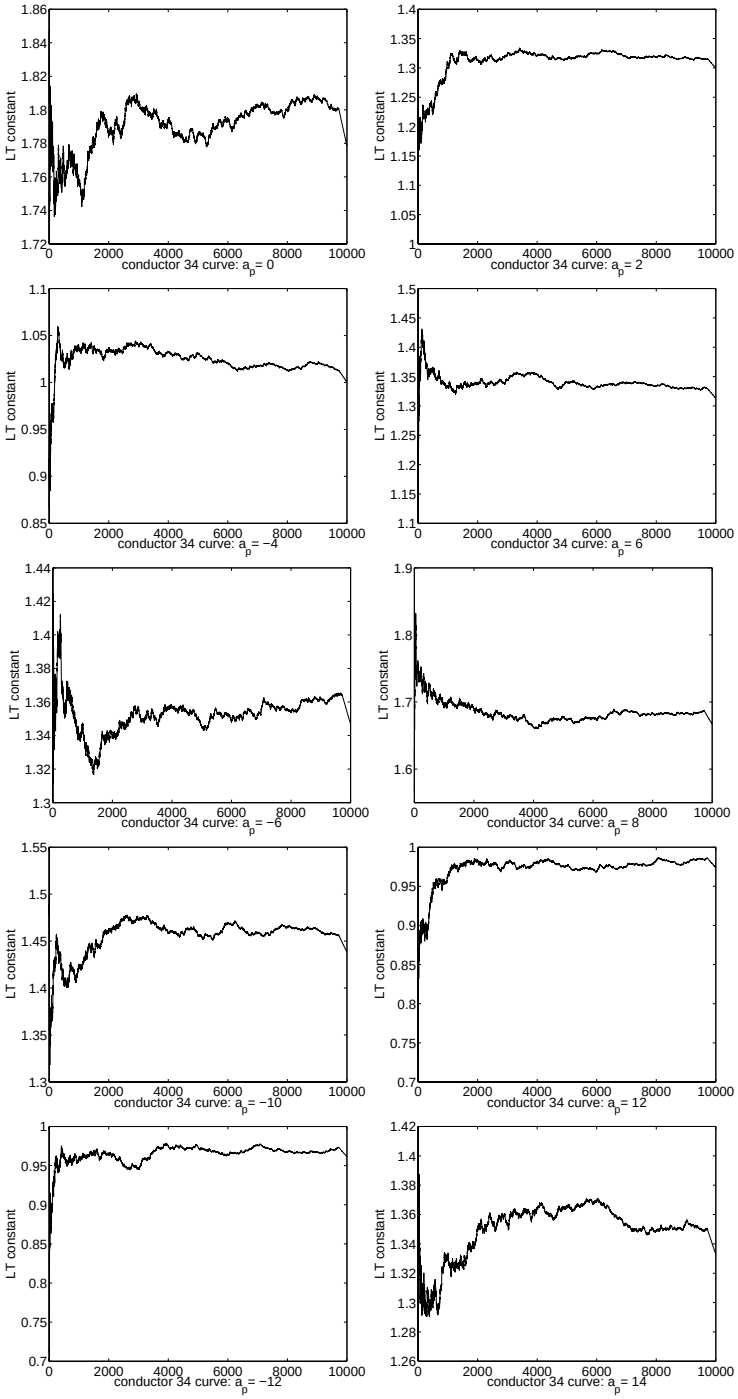

LT constant
conductor 33 curve: $a_p = -10$
conductor 33 curve: $a_p = 12$
conductor 33 curve: $a_p = -12$
conductor 33 curve: $a_p = 14$
conductor 33 curve: $a_p = -14$
conductor 33 curve: $a_p = 16$
conductor 33 curve: $a_p = -16$
conductor 33 curve: $a_p = 18$
conductor 33 curve: $a_p = -18$
conductor 33 curve: $a_p = 20$

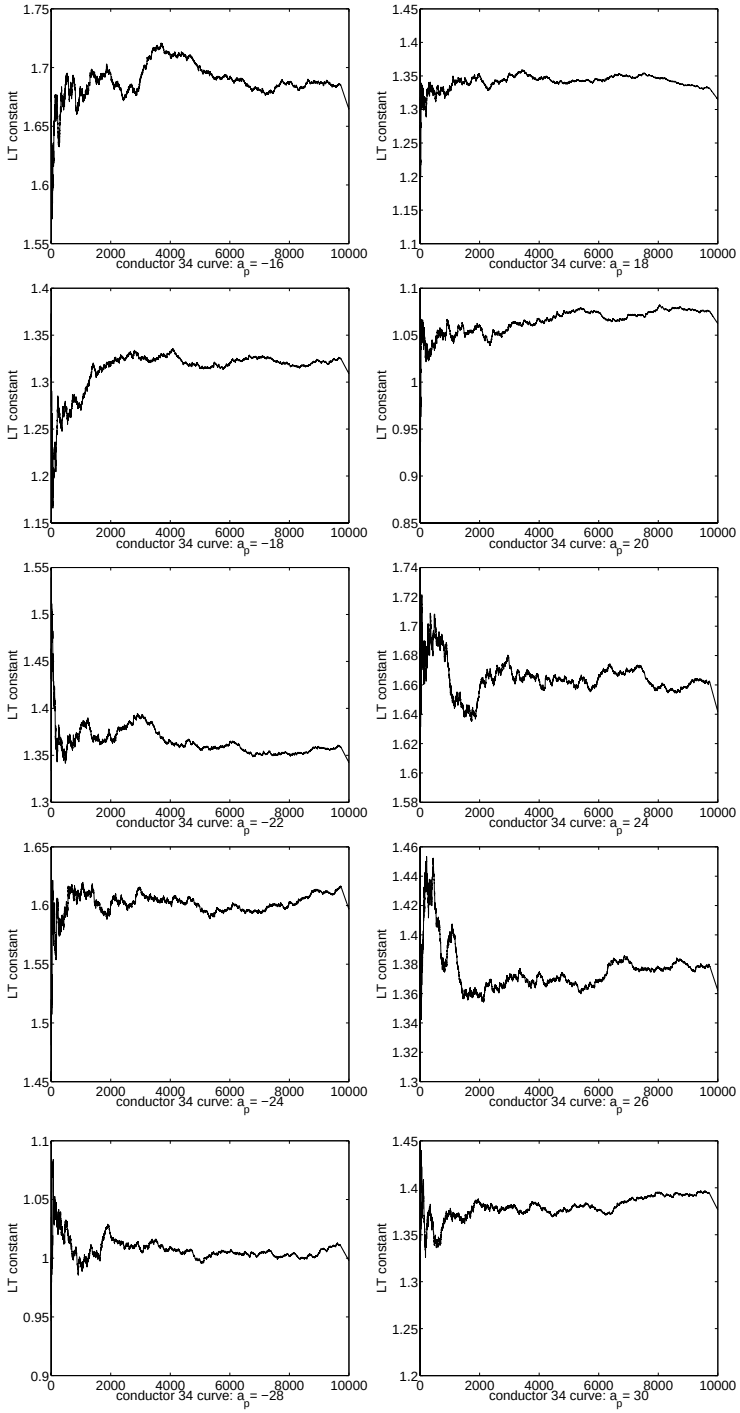

LT constant
conductor 33 curve: $a_p = -20$
conductor 33 curve: $a_p = 22$
conductor 33 curve: $a_p = -22$
conductor 33 curve: $a_p = 24$
conductor 33 curve: $a_p = -24$
conductor 33 curve: $a_p = 26$
conductor 33 curve: $a_p = -26$
conductor 33 curve: $a_p = 28$
conductor 33 curve: $a_p = -28$
conductor 33 curve: $a_p = 30$

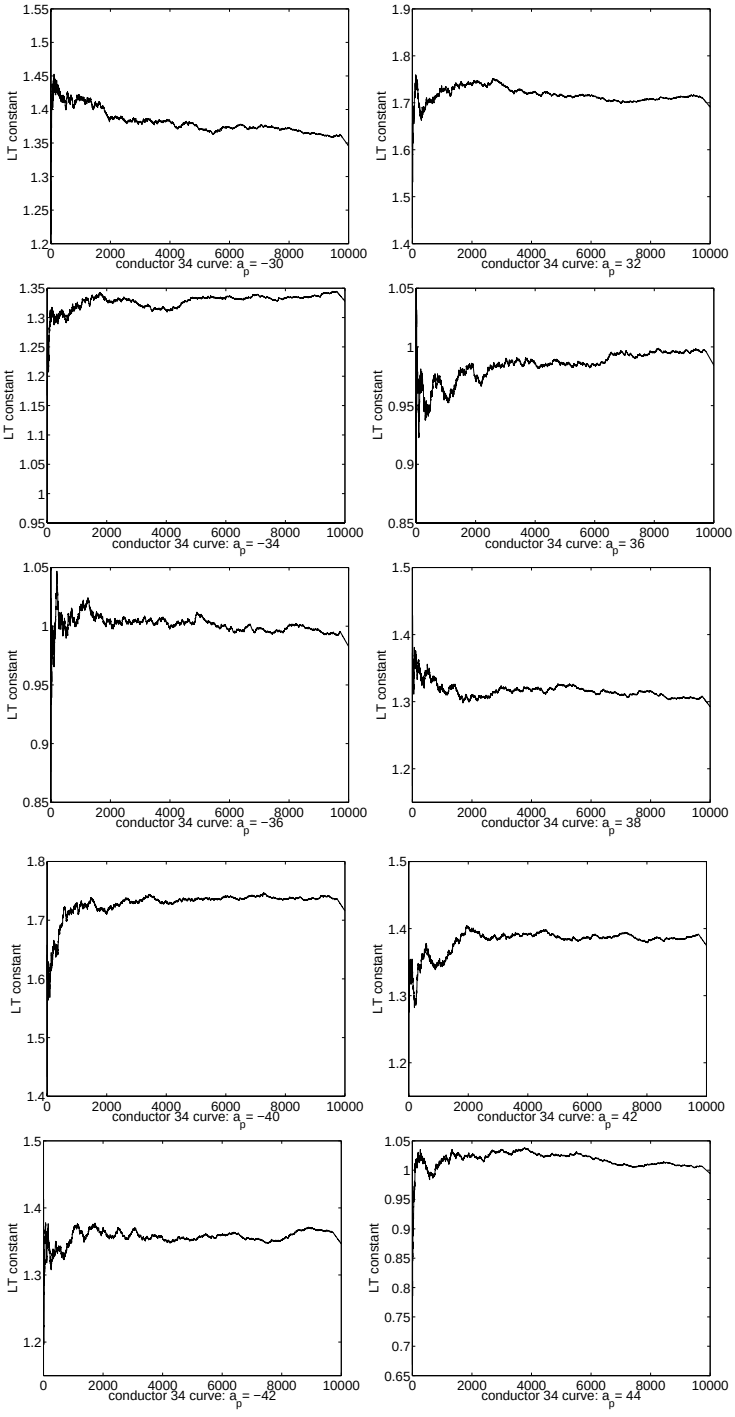

LT constant
conductor 33 curve: $a_p = -30$
conductor 33 curve: $a_p = 32$
conductor 33 curve: $a_p = -32$
conductor 33 curve: $a_p = 34$
conductor 33 curve: $a_p = -34$
conductor 33 curve: $a_p = 36$
conductor 33 curve: $a_p = -36$
conductor 33 curve: $a_p = 38$
conductor 33 curve: $a_p = -38$
conductor 33 curve: $a_p = 40$

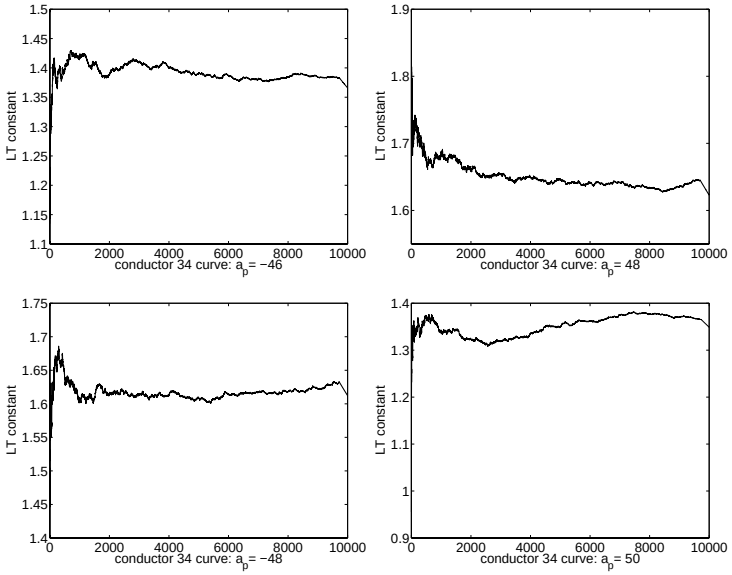

LT constant
conductor 33 curve: $a_p = -40$
conductor 33 curve: $a_p = 42$
conductor 33 curve: $a_p = -42$
conductor 33 curve: $a_p = 44$
conductor 33 curve: $a_p = -44$
conductor 33 curve: $a_p = 46$
conductor 33 curve: $a_p = -46$
conductor 33 curve: $a_p = 48$
conductor 33 curve: $a_p = -48$
conductor 33 curve: $a_p = 50$

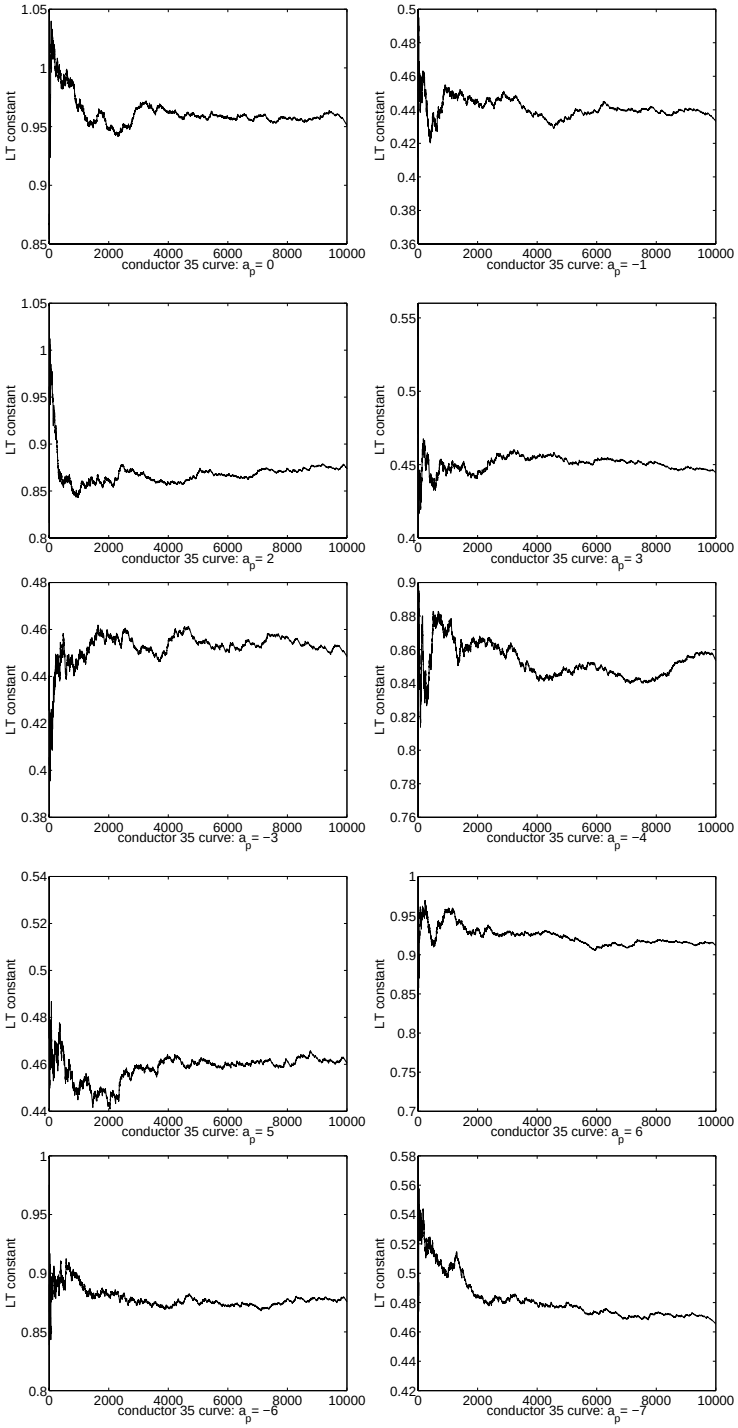

0.95
0.9
0.85
0.8
0.75
0.7
0.65
0.6
0.55
LT constant
0
2000
4000
6000
8000
10000
conductor 33 curve: a_p = −50

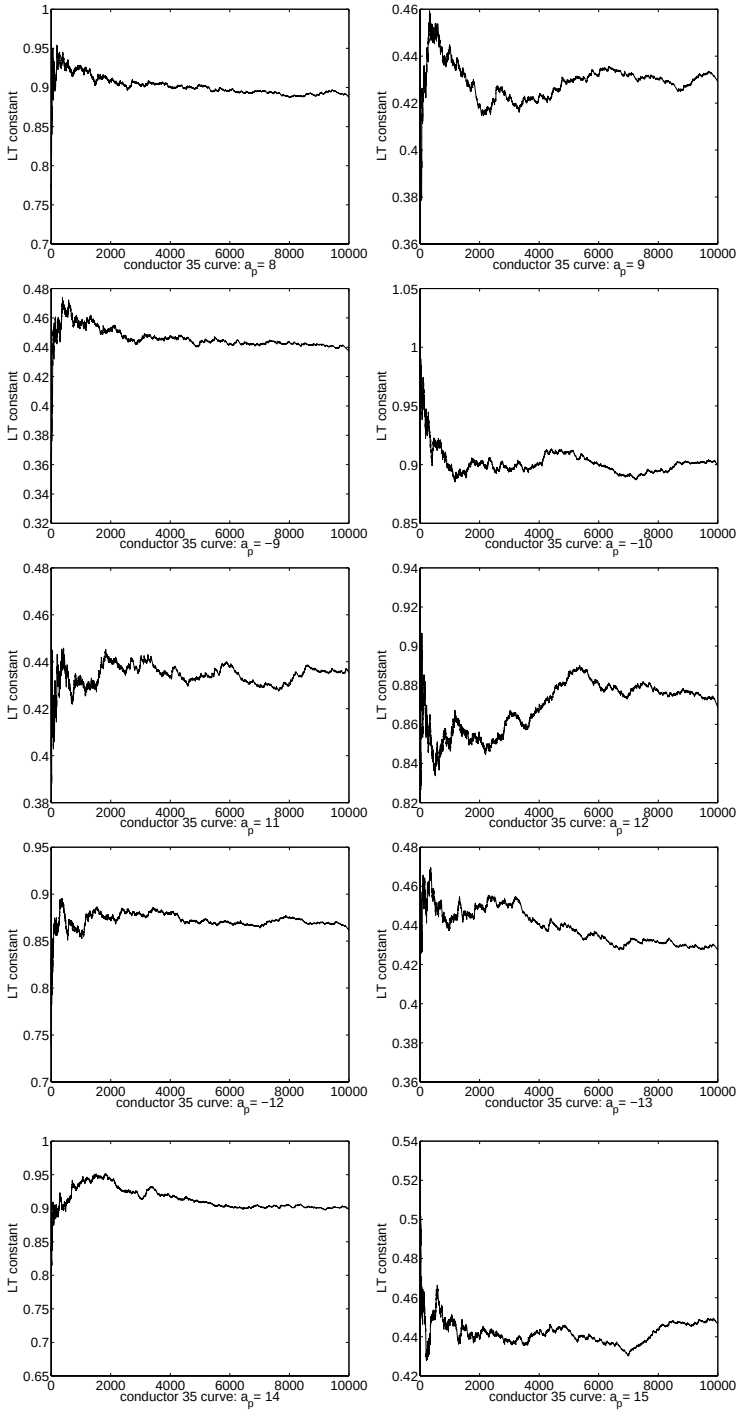

LT constant
conductor 34 curve: $a_p = 0$
conductor 34 curve: $a_p = 2$
conductor 34 curve: $a_p = -4$
conductor 34 curve: $a_p = 6$
conductor 34 curve: $a_p = -6$
conductor 34 curve: $a_p = 8$
conductor 34 curve: $a_p = -10$
conductor 34 curve: $a_p = 12$
conductor 34 curve: $a_p = -12$
conductor 34 curve: $a_p = 14$

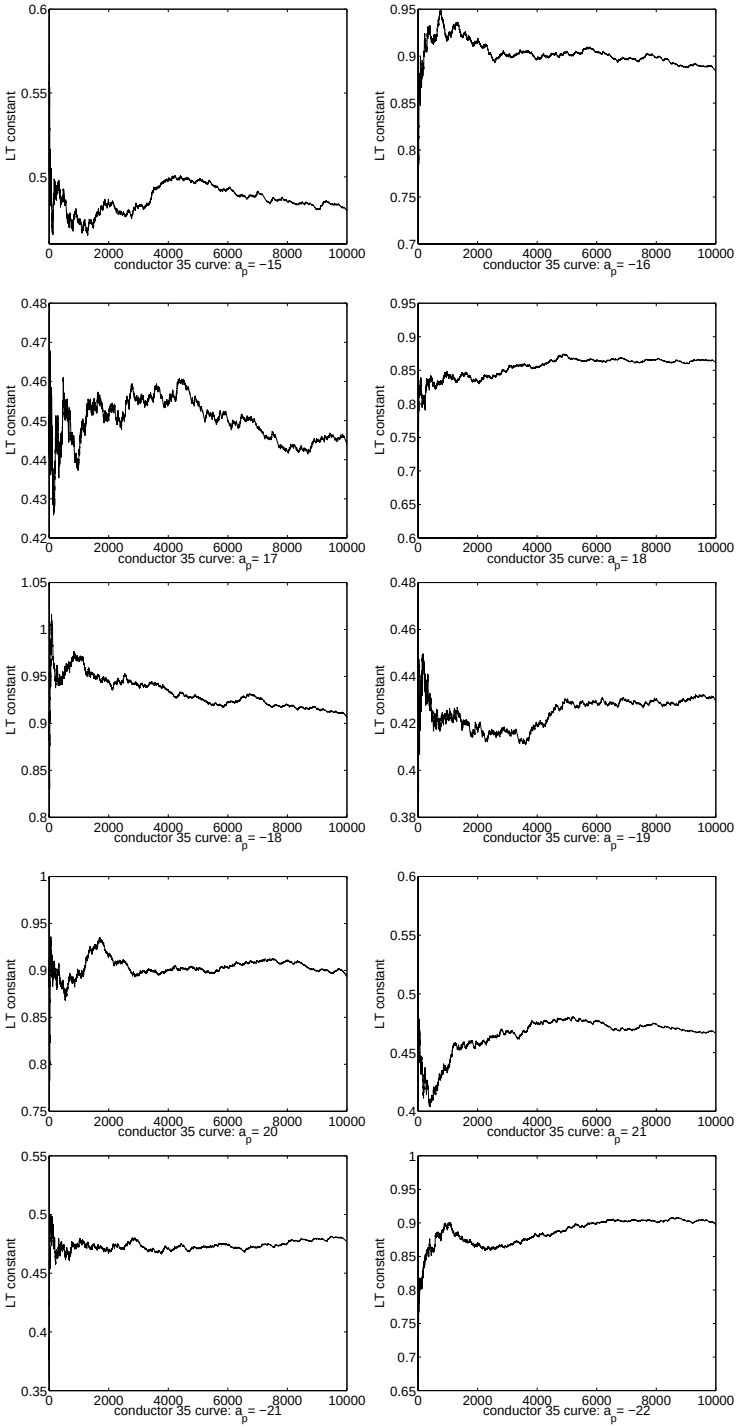

LT constant
conductor 34 curve: $a_p = -16$
conductor 34 curve: $a_p = 18$
conductor 34 curve: $a_p = -18$
conductor 34 curve: $a_p = 20$
conductor 34 curve: $a_p = -22$
conductor 34 curve: $a_p = 24$
conductor 34 curve: $a_p = -24$
conductor 34 curve: $a_p = 26$
conductor 34 curve: $a_p = -28$
conductor 34 curve: $a_p = 30$

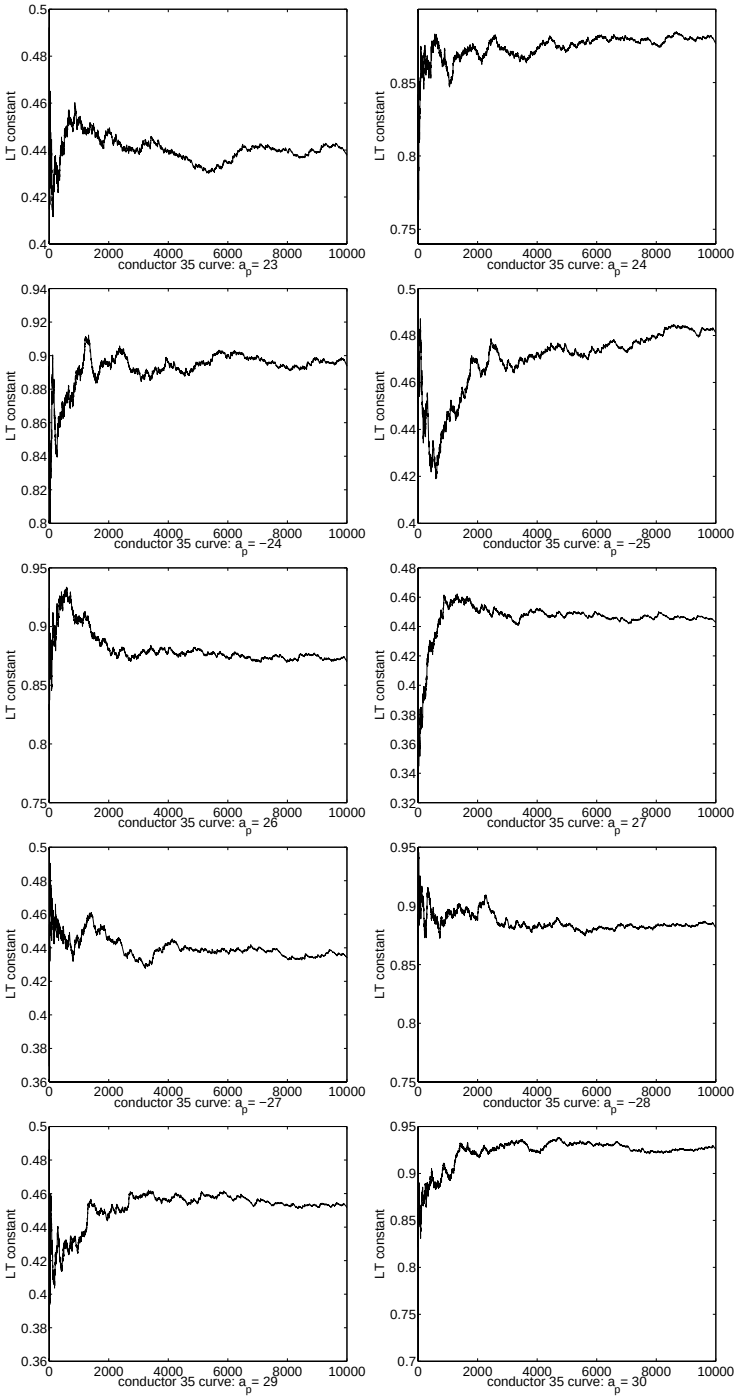

LT constant
conductor 34 curve: $a_p = -30$
conductor 34 curve: $a_p = 32$
conductor 34 curve: $a_p = -34$
conductor 34 curve: $a_p = 36$
conductor 34 curve: $a_p = -36$
conductor 34 curve: $a_p = 38$
conductor 34 curve: $a_p = -40$
conductor 34 curve: $a_p = 42$
conductor 34 curve: $a_p = -42$
conductor 34 curve: $a_p = 44$

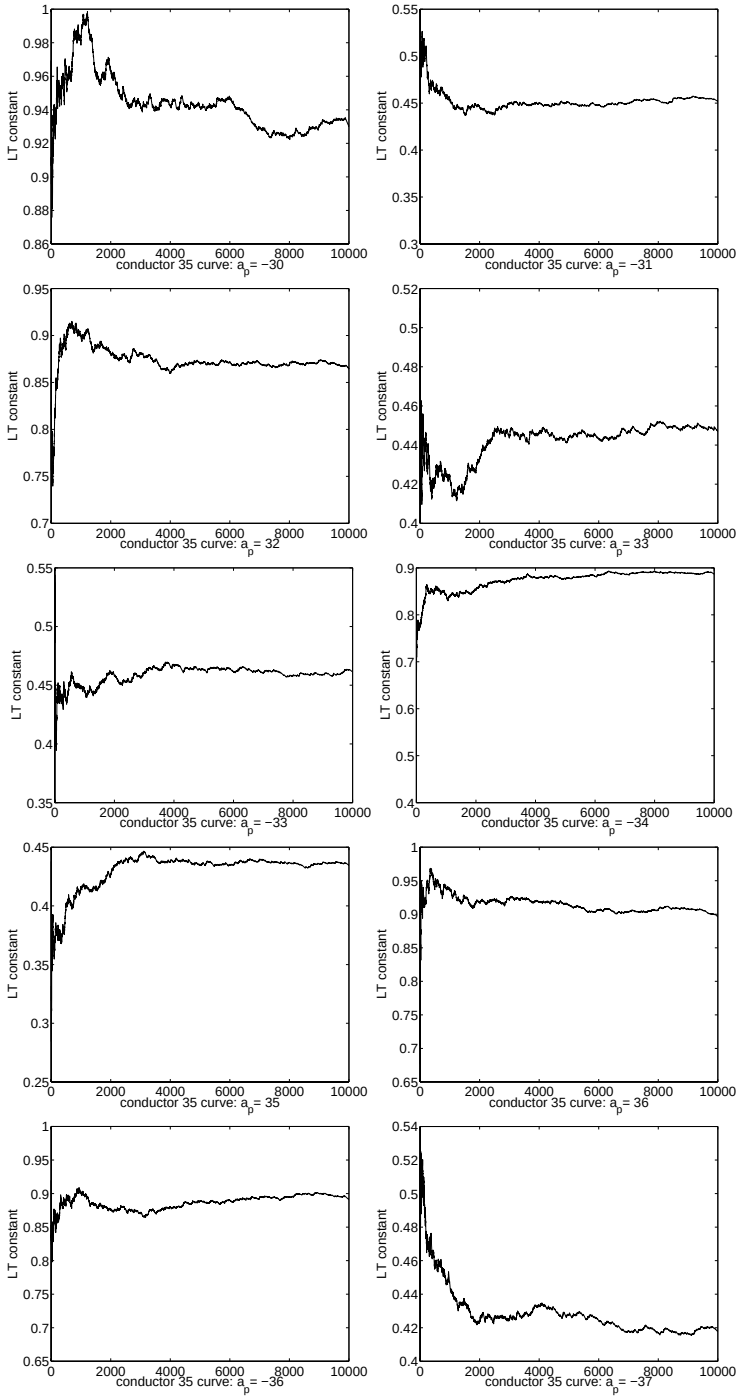

LT constant
conductor 34 curve: $a_p = -46$
conductor 34 curve: $a_p = 48$
conductor 34 curve: $a_p = -48$
conductor 34 curve: $a_p = 50$

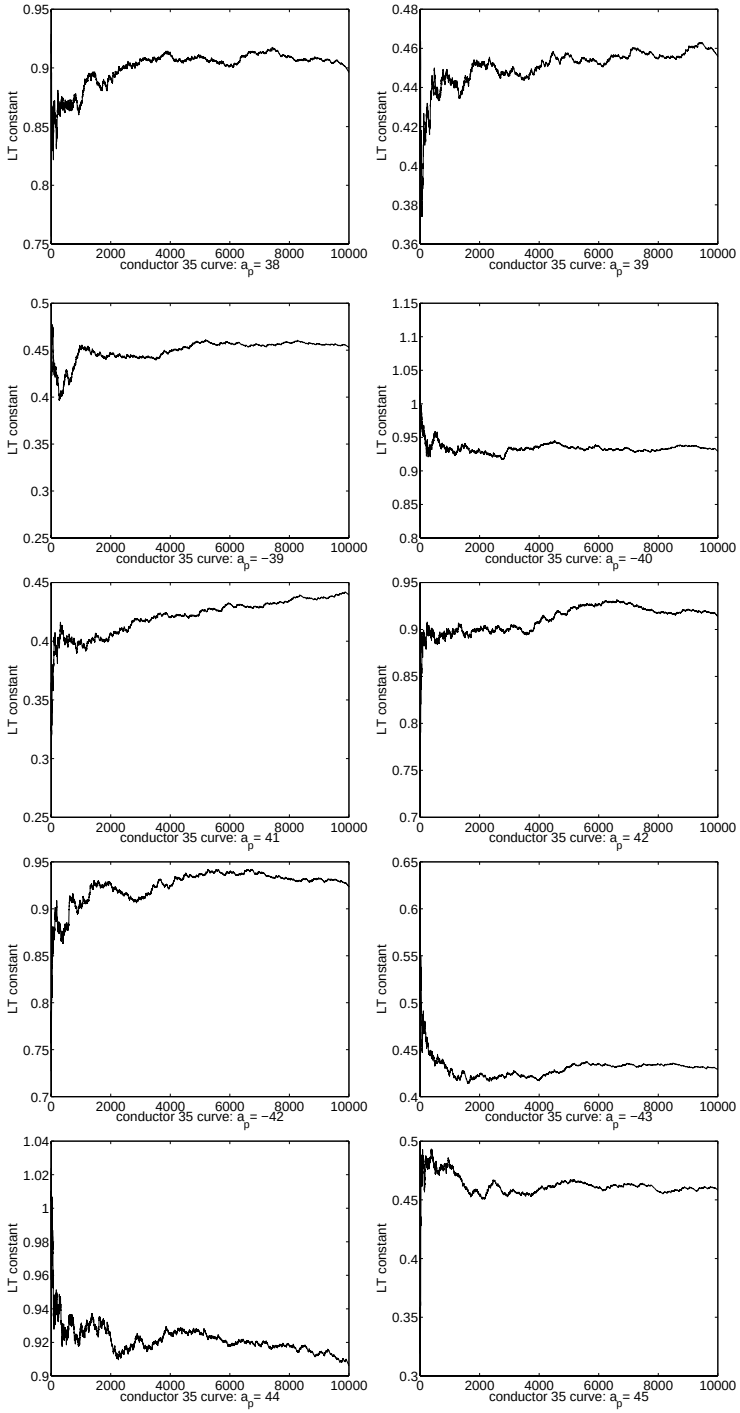

LT constant
conductor 35 curve: $a_p = 0$
conductor 35 curve: $a_p = -1$
conductor 35 curve: $a_p = 2$
conductor 35 curve: $a_p = 3$
conductor 35 curve: $a_p = -3$
conductor 35 curve: $a_p = -4$
conductor 35 curve: $a_p = 5$
conductor 35 curve: $a_p = 6$
conductor 35 curve: $a_p = -6$
conductor 35 curve: $a_p = -7$

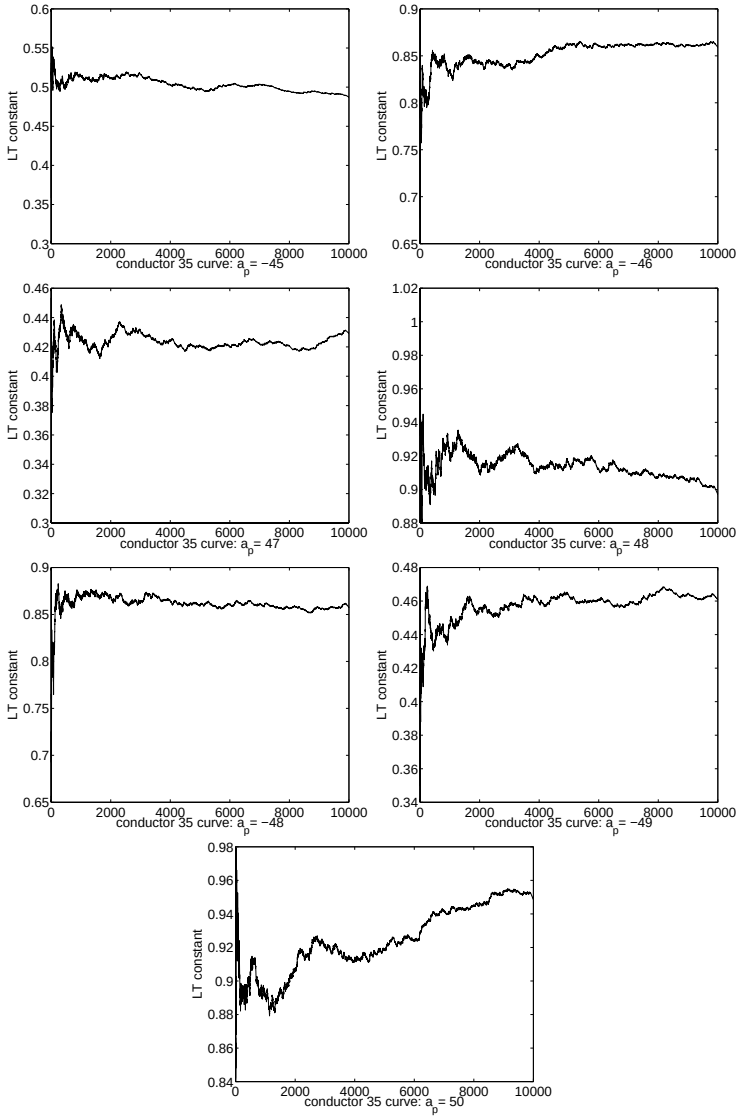

LT constant
conductor 35 curve: $a_p = 8$
conductor 35 curve: $a_p = 9$
conductor 35 curve: $a_p = -9$
conductor 35 curve: $a_p = -10$
conductor 35 curve: $a_p = 11$
conductor 35 curve: $a_p = 12$
conductor 35 curve: $a_p = -12$
conductor 35 curve: $a_p = -13$
conductor 35 curve: $a_p = 14$
conductor 35 curve: $a_p = 15$

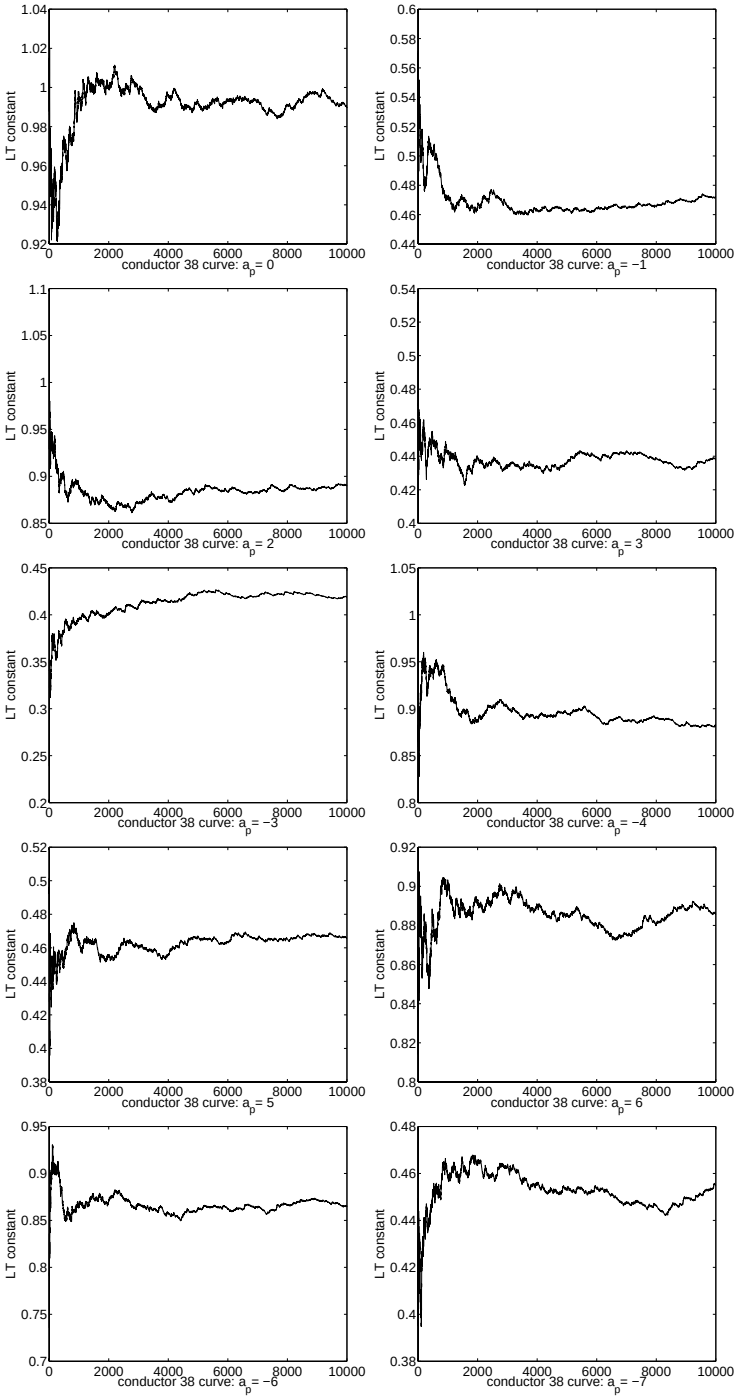

LT constant
conductor 35 curve: $a_p = -15$
conductor 35 curve: $a_p = -16$
conductor 35 curve: $a_p = 17$
conductor 35 curve: $a_p = 18$
conductor 35 curve: $a_p = -18$
conductor 35 curve: $a_p = -19$
conductor 35 curve: $a_p = 20$
conductor 35 curve: $a_p = 21$
conductor 35 curve: $a_p = -21$
conductor 35 curve: $a_p = -22$

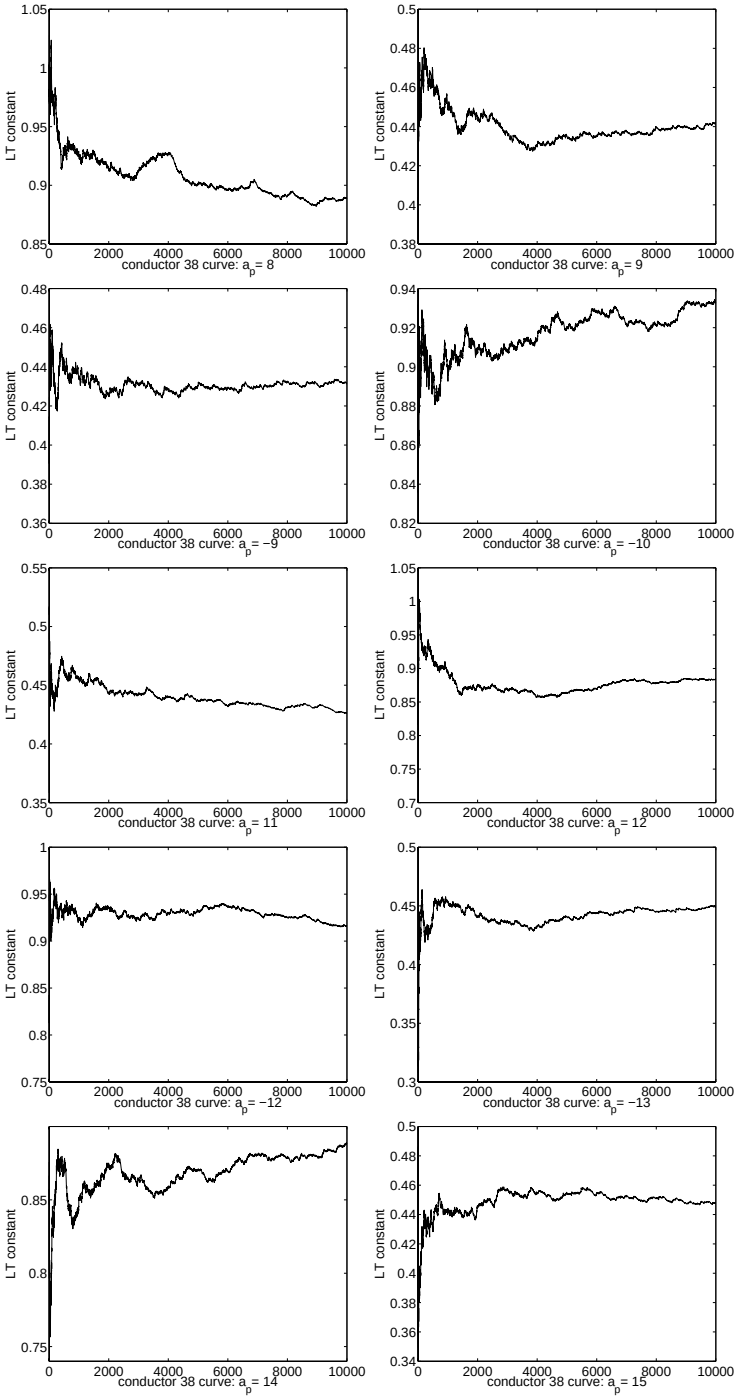

LT constant
conductor 35 curve: $a_p = 23$
conductor 35 curve: $a_p = 24$
conductor 35 curve: $a_p = -24$
conductor 35 curve: $a_p = -25$
conductor 35 curve: $a_p = 26$
conductor 35 curve: $a_p = 27$
conductor 35 curve: $a_p = -27$
conductor 35 curve: $a_p = -28$
conductor 35 curve: $a_p = 29$
conductor 35 curve: $a_p = 30$

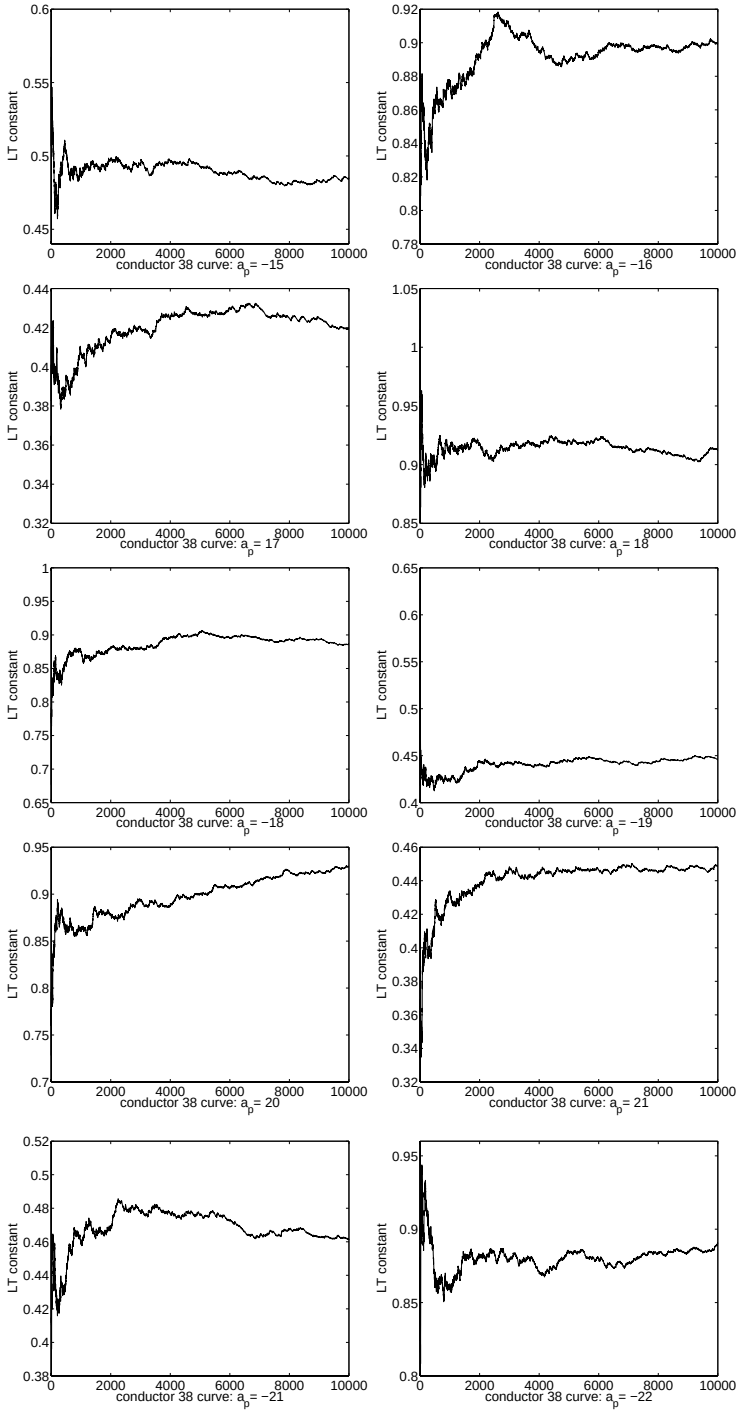

LT constant
conductor 35 curve: $a_p = -30$
conductor 35 curve: $a_p = -31$
conductor 35 curve: $a_p = 32$
conductor 35 curve: $a_p = 33$
conductor 35 curve: $a_p = -33$
conductor 35 curve: $a_p = -34$
conductor 35 curve: $a_p = 35$
conductor 35 curve: $a_p = 36$
conductor 35 curve: $a_p = -36$
conductor 35 curve: $a_p = -37$

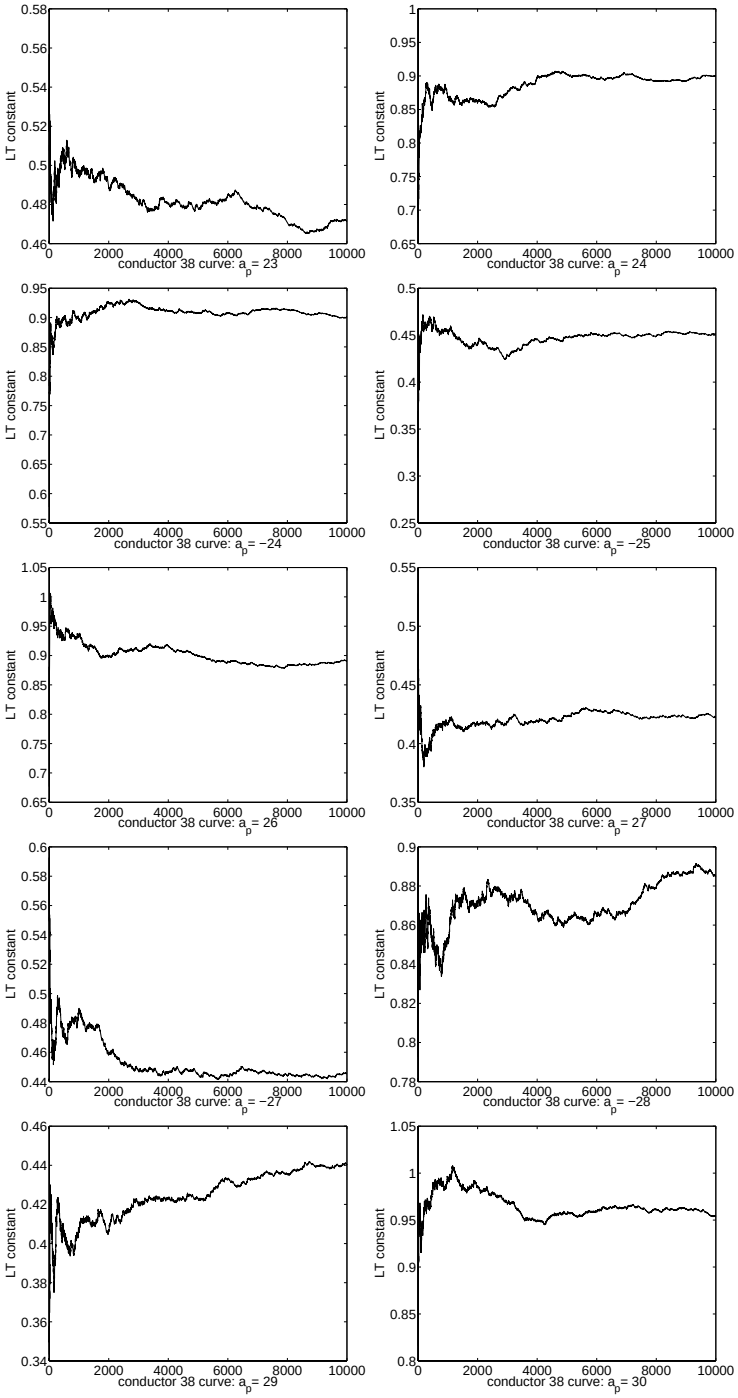

LT constant
conductor 35 curve: $a_p = 38$
conductor 35 curve: $a_p = 39$
conductor 35 curve: $a_p = -39$
conductor 35 curve: $a_p = -40$
conductor 35 curve: $a_p = 41$
conductor 35 curve: $a_p = 42$
conductor 35 curve: $a_p = -42$
conductor 35 curve: $a_p = -43$
conductor 35 curve: $a_p = 44$
conductor 35 curve: $a_p = 45$

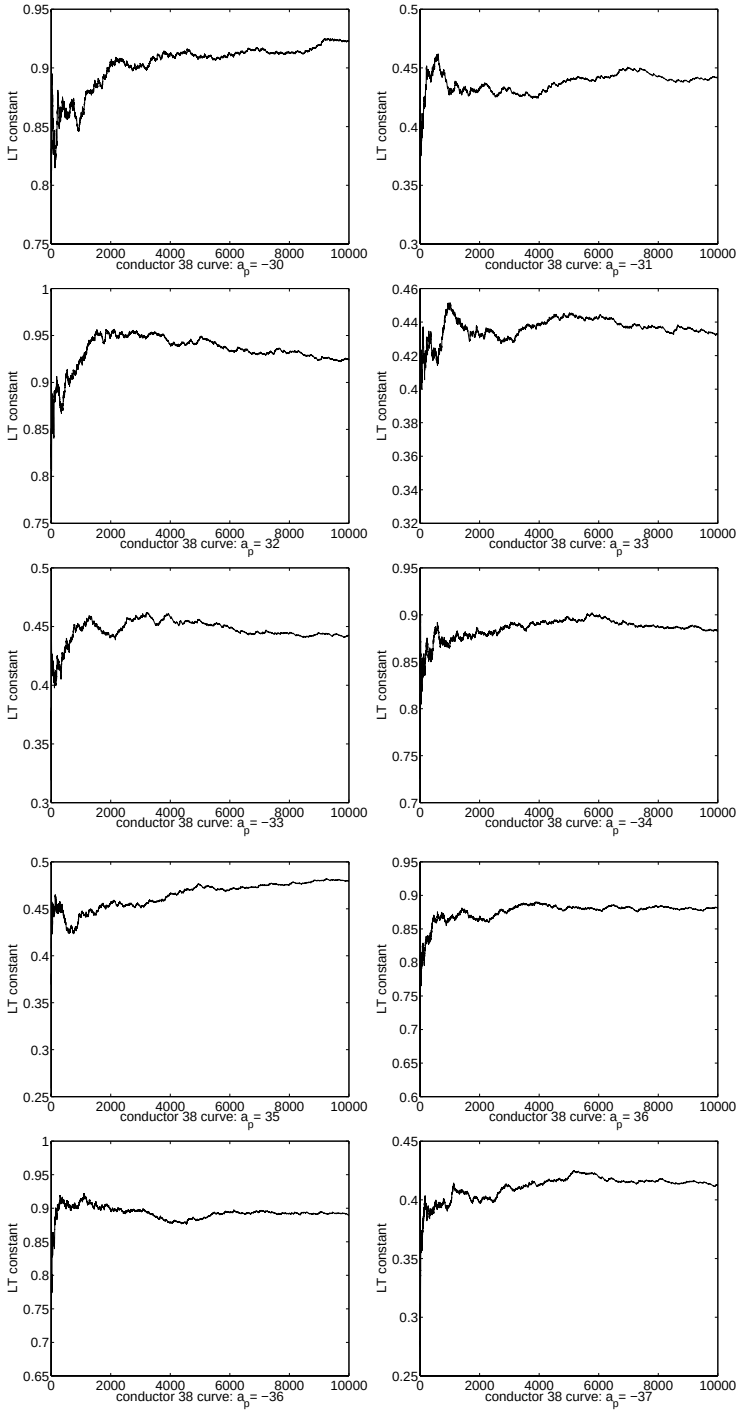

LT constant
conductor 35 curve: $a_p = -45$
conductor 35 curve: $a_p = -46$
conductor 35 curve: $a_p = 47$
conductor 35 curve: $a_p = 48$
conductor 35 curve: $a_p = -48$
conductor 35 curve: $a_p = -49$
conductor 35 curve: $a_p = 50$

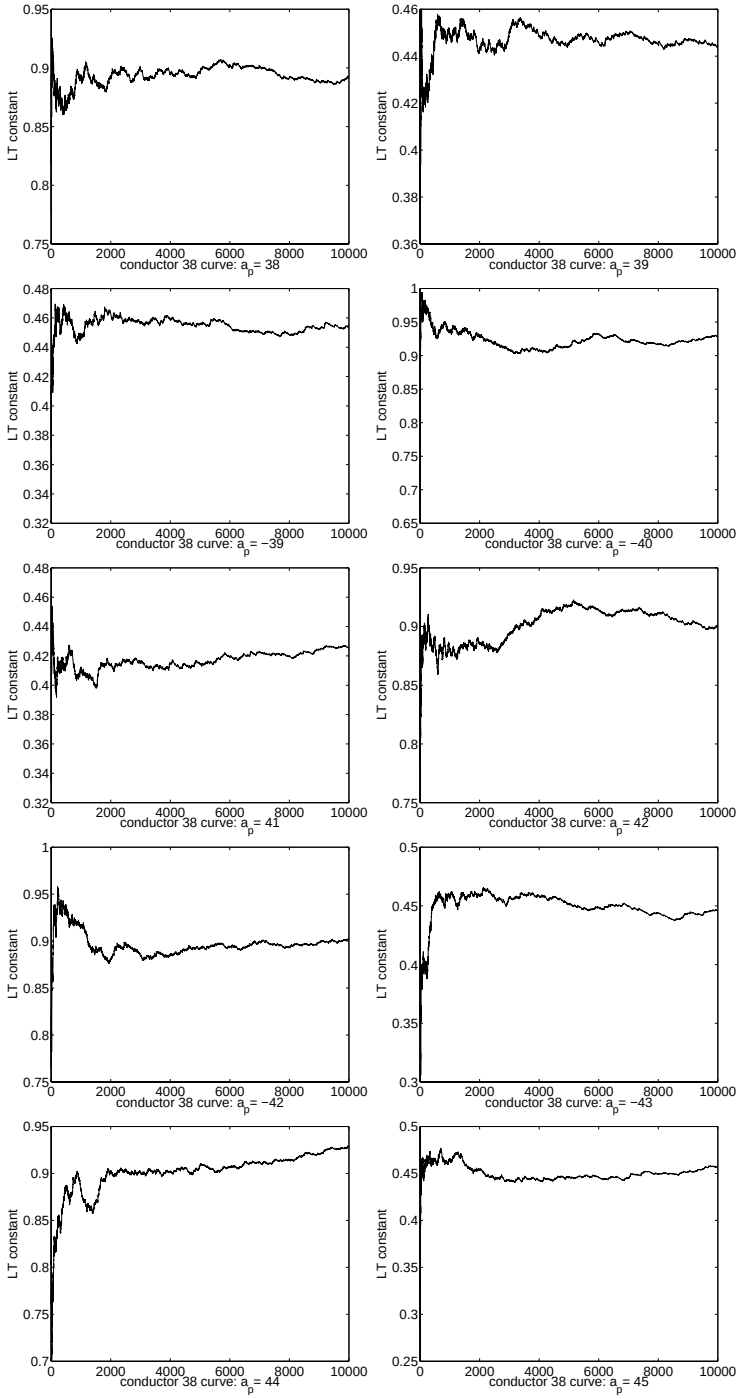

LT constant
conductor 38 curve: $a_p = 0$
conductor 38 curve: $a_p = -1$
conductor 38 curve: $a_p = 2$
conductor 38 curve: $a_p = 3$
conductor 38 curve: $a_p = -3$
conductor 38 curve: $a_p = -4$
conductor 38 curve: $a_p = 5$
conductor 38 curve: $a_p = 6$
conductor 38 curve: $a_p = -6$
conductor 38 curve: $a_p = -7$

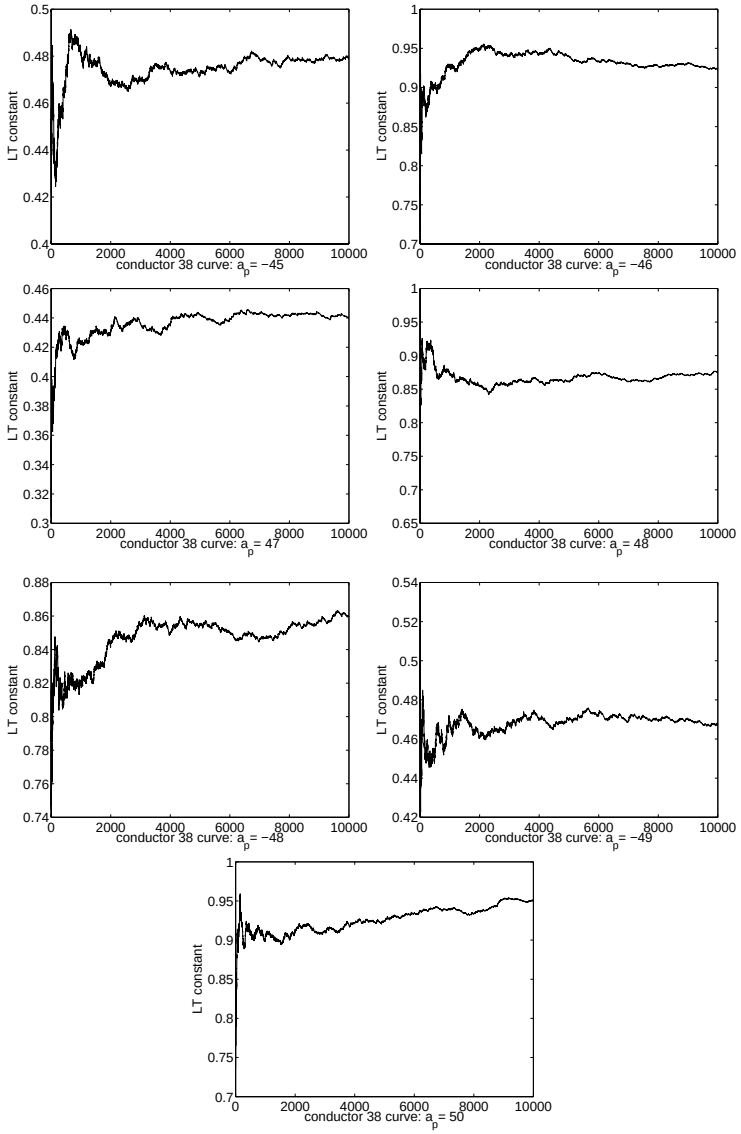

LT constant
conductor 38 curve: $a_p = 8$
conductor 38 curve: $a_p = 9$
conductor 38 curve: $a_p = -9$
conductor 38 curve: $a_p = -10$
conductor 38 curve: $a_p = 11$
conductor 38 curve: $a_p = 12$
conductor 38 curve: $a_p = -12$
conductor 38 curve: $a_p = -13$
conductor 38 curve: $a_p = 14$
conductor 38 curve: $a_p = 15$


LT constant
conductor 38 curve: $a_p = -15$
conductor 38 curve: $a_p = -16$
conductor 38 curve: $a_p = 17$
conductor 38 curve: $a_p = 18$
conductor 38 curve: $a_p = -18$
conductor 38 curve: $a_p = -19$
conductor 38 curve: $a_p = 20$
conductor 38 curve: $a_p = 21$
conductor 38 curve: $a_p = -21$
conductor 38 curve: $a_p = -22$


LT constant
conductor 38 curve: $a_p = 23$
conductor 38 curve: $a_p = 24$
conductor 38 curve: $a_p = -24$
conductor 38 curve: $a_p = -25$
conductor 38 curve: $a_p = 26$
conductor 38 curve: $a_p = 27$
conductor 38 curve: $a_p = -27$
conductor 38 curve: $a_p = -28$
conductor 38 curve: $a_p = 29$
conductor 38 curve: $a_p = 30$


LT constant
conductor 38 curve: $a_p = -30$
conductor 38 curve: $a_p = -31$
conductor 38 curve: $a_p = 32$
conductor 38 curve: $a_p = 33$
conductor 38 curve: $a_p = -33$
conductor 38 curve: $a_p = -34$
conductor 38 curve: $a_p = 35$
conductor 38 curve: $a_p = 36$
conductor 38 curve: $a_p = -36$
conductor 38 curve: $a_p = -37$


LT constant
conductor 38 curve: $a_p = 38$
conductor 38 curve: $a_p = 39$
conductor 38 curve: $a_p = -39$
conductor 38 curve: $a_p = -40$
conductor 38 curve: $a_p = 41$
conductor 38 curve: $a_p = 42$
conductor 38 curve: $a_p = -42$
conductor 38 curve: $a_p = -43$
conductor 38 curve: $a_p = 44$
conductor 38 curve: $a_p = 45$


LT constant
conductor 38 curve: $a_p = -45$
conductor 38 curve: $a_p = -46$
conductor 38 curve: $a_p = 47$
conductor 38 curve: $a_p = 48$
conductor 38 curve: $a_p = -48$
conductor 38 curve: $a_p = -49$
conductor 38 curve: $a_p = 50$

References

[1] Crandall, R., and Pomerance, C. *Prime numbers*. Springer-Verlag, New York, 2001. A computational perspective.

[2] David, C., and Pappalardi, F. Average Frobenius distributions of elliptic curves. *Internat. Math. Res. Notices*, 4 (1999), 165–183.

[3] Elkies, N. D. The existence of infinitely many supersingular primes for every elliptic curve over $\mathbf{Q}$. *Invent. Math. 89*, 3 (1987), 561–567.

[4] Fouvry, E., and Murty, M. R. On the distribution of supersingular primes. *Canad. J. Math. 48*, 1 (1996), 81–104.

[5] Lang, S., and Trotter, H. *Frobenius distributions in* GL_2*-extensions*. Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers, Lecture Notes in Mathematics, Vol. 504.

[6] Schoof, R. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp. 44*, 170 (1985), 483–494.

[7] Serre, J.-P. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math. 15*, 4 (1972), 259–331.

[8] Tate, J. T. Algebraic cycles and poles of zeta functions. In *Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963)*. Harper & Row, New York, 1965, pp. 93–110.