16p-A14-8

乱数検定による位相揺らぎの乱雑度評価

Characterizing Phase Fluctuations by Random Number Test

日立中研　○戸丸 辰也

Hitachi, Central Research Laboratory, ○Tatsuya Tomaru

E-mail: tatsuya.tomaru.yq@hitachi.com

はじめに：安全な光通信法として位相揺らぎを利用した方法を提案してきた[1,2]。この方法では位相揺らぎの予測不能性を安全性の根拠にしているため、実際の揺らぎが十分に乱雑であることを示すことが重要になる。信号重畳法としては DPSK (Differential Phase-Shift Keying)を想定しており、揺らぎ源として LD の位相揺らぎを利用できる[3]。その周波数特性は概ねフラットである[4]。本報告では時間軸上で評価した結果を述べる。

実験：位相揺らぎを２値乱数に変換し、乱数評価用の NIST SP800-22 で評価した。揺らぎ源は cw 動作の LD であり、出力光を 400 ps の非対称干渉計(2.5 Gbps 用 DPSK demodulator)に通すことにより位相揺らぎを強度揺らぎに変換し、平衡型検出器で受光後、デジタルオシロスコープ（帯域 1 GHz）により 8 ビットでサンプリングした。位相揺らぎの頻度分布はガウス分布的であり、情報量 $I = -\Sigma_i p_i \log_2 p_i$ を見積もれば 4.5 bit 程度であった。そこで、２値乱数化では８ビットデータを 4 ビットにした。その際 2.5×10^8 or 5×10^8 点の頻度分布を使って各ビット値の分布を均等化した。

結果：SP800-22 では 15 種類 188 項目に関して単位乱数（10^6 個）ごとの乱雑度（種類ごとに定義式あり）を算出し、その乱雑度（1000 or 2000 個）の統計分布を一様性と裾部の比率の観点から評価する。SP800-22 の Default の判定基準を 188 項目全体で見ると、一様性検定に対して有意水準 1.9%、比率検定に対して有意水準 40%の検定になっている。その基準における結果を表 1 に示す。一様性検定ではすべて“pass”したが、比率検定に関して“pass”しなかった項目がある。仮に有意水準を 2.5%に設定すればすべて“pass”になる。

I_d, f_r	1000 units		2000 units
12 mA 100 MHz	pass	pass	pass
	pass	978/1000	pass
12 mA 1 GHz	pass	pass	pass
	pass	pass	pass
	pass	pass	pass
	pass	pass	1964/2000
70 mA 100 MHz	pass	pass	pass
	pass	979/1000 979/1000	pass
70 mA 1 GHz	pass	pass	pass
	pass	979/1000	pass
	pass	pass	pass
	979/1000	pass	pass

Table I. Test results by SP800-22, where significance level is 1.9% for uniformity test (upper line) and 40% for proportion test (lower line, colored). I_d is an injection current to an LD. f_r is a sampling rate. A concrete value indicates a result that was “false” in the test of this significance level. Criteria of “pass” are more than 980/1000 and 1966/2000 in proportion test of each units.

結論：LD の位相揺らぎを、一様性検定に関して有意水準 1.9%で、比率検定に関して有意水準 2.5%で評価すれば、SP800-22 の検定で“pass”になる。

謝辞：本研究の一部は文部科学省 イノベーションシステム整備事業の支援により遂行された。

[1] T. Tomaru, JJAP **49**, 074401 (2010).

[2] 戸丸, 2012 年秋季応物学会 13aB1-5.

[3] 戸丸, 2013 年春季応物学会 30pD1-2.

[4] T. Tomaru, JOSAB 28, 1502 (2011).