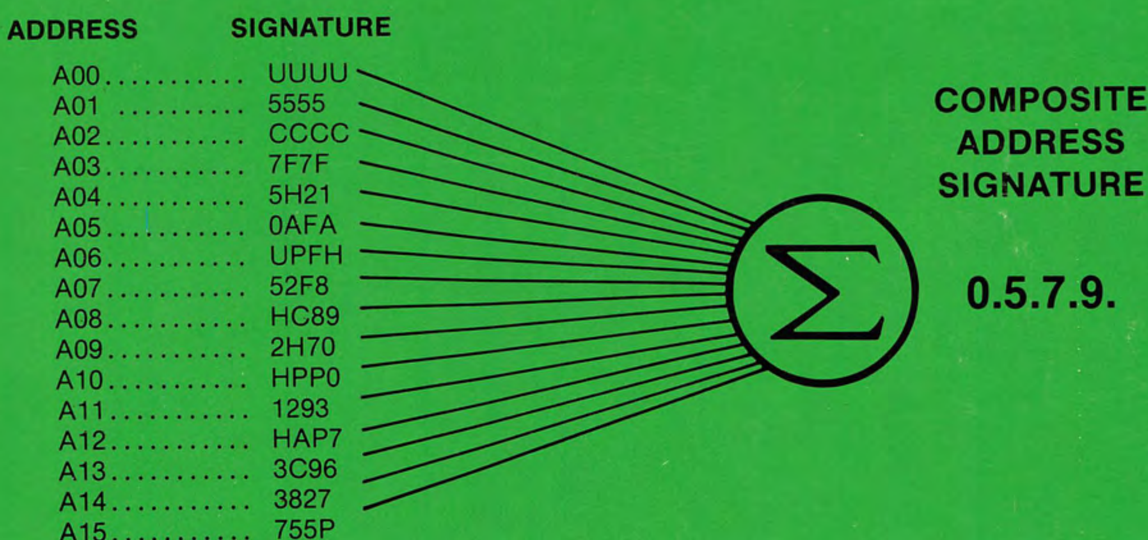
Application Note 222-6

Troubleshooting with Composite Signatures



HEWLETT PACKARD

Application Note 222-6

"Troubleshooting with Composite Signatures"

Composite Signature is the binary sum of individual signatures. Composite signature saves the troubleshooter time by reducing the amount of visual comparisons of the signature analyzer display to printed signature tables. Any grouping of digital signals can be chosen to form a composite signature. Composite IC or Bus signatures are good examples.

This application note explains how composite signature and the backtracing algorithm can be used to implement a structured troubleshooting procedure without a computer-aided system. The result is time savings for the logic troubleshooter.

FOREWORD

ABOUT DIGITAL TROUBLESHOOTING

Microprocessors have revolutionized your product line. Your products are smarter, faster, friendlier and more competitive because they take advantage of μP-based control and computation. They are also harder to build, harder to test and harder to fix when they fail. Complex bus structures and timing relationships have practically obsoleted the scope/voltmeter and signal tracing techniques so effective on analog products. The need to enhance the testability and serviceability of your digital products is acute. So is the need for specialized digital troubleshooting equipment.

ABOUT SIGNATURE ANALYSIS

To address these needs, Hewlett-Packard has developed the Signature Analysis technique, as well as a Signature Analyzer product line, for component-level troubleshooting of microprocessor-based products. A Signature Analyzer detects and displays the unique digital signatures associated with the data nodes in a circuit under test. By comparing these actual signatures to the correct ones, a troubleshooter can back-trace to a faulty node. By designing S.A. into digital products, or stimulating them externally, a manufacturer can provide manufacturing test and field service procedures for component-level repair, without dependence on expensive board-exchange programs.

ABOUT THIS PUBLICATION

This application note shows how composite signature can be used to implement a structured troubleshooting procedure without a computer-aided system. The backtracing algorithm is explained and flowcharted. Examples show how to measure and calculate composite signature. Potential time savings is estimated. Theory of operation and probability of error detection are derived in the appendices.

ABOUT OTHER PUBLICATIONS

Application Note 222-0, "An Index to Signature Analysis Publications" lists all other application notes currently available in the AN 222 series about Signature Analysis. They cover a wide range of interests, from how to design or retrofit Signature Analysis into digital systems, to the cost reductions that can be expected in production test and field service by doing so. It also lists all data sheets for the complete line of Hewlett-Packard Signature Analysis products, plus other related publications about digital troubleshooting.

TABLE OF CONTENTS

INTRODUCTION 1

A STRUCTURED APPROACH TO FINDING FAULTS 2

BACKTRACING 6

TIME SAVING ESTIMATES 8

USING A COMPOSITE SIGNATURE ANALYZER 9

CALCULATING COMPOSITE SIGNATURE 10

CONCLUSION 11

APPENDICES — THEORY OF OPERATION 12

INTRODUCTION

Composite signature **magnifies** the power of Signature Analysis by providing a single signature that verifies the correct operation of an IC, microprocessor bus or digital circuit. Rough estimates show that one can find the first bad signature ten times faster than by taking individual signatures. The time saved is realized when making manual comparisons of measured signatures to the expected ones recorded on paper. One simply probes the individual nodes and then only compares the composite signatures to detect the presence of individual faulty waveforms. Of course, with a computer-aided system there is no advantage because comparisons of signatures to memory are done automatically. Therefore, composite signature is primarily used in manual troubleshooting applications.

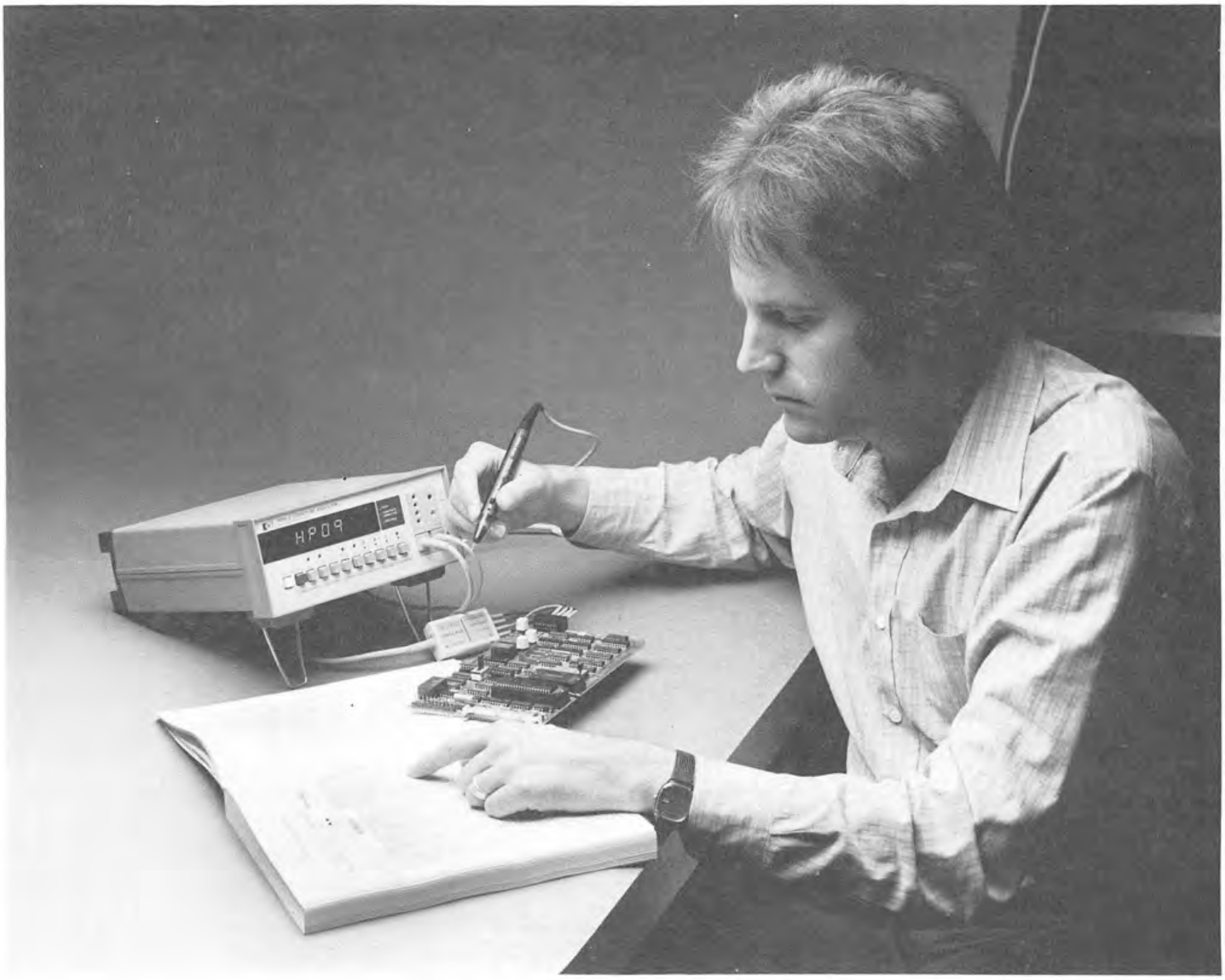


Figure 1. Composite signature saves time by reducing the amount of visual comparisons the troubleshooter must make to printed documentation. The HP 5006A Signature Analyzer is the first signature measurement instrument to offer this capability.

A STRUCTURED APPROACH TO FINDING FAULTS

The composite signature function now gives digital troubleshooting a **structured approach**. The objective of digital troubleshooting is to find the **source** of the faulty signals being propagated in a circuit. A fault source could be a bad integrated circuit, component, solder bridge of faulty trace. Figure 2 summarizes the steps taken to find the source of faulty signals on a digital circuit board. Composite signature aids the troubleshooter who does not have access to a computer-aided troubleshooting system by making the process faster and easier. The instrument used as an example in this note is the HP 5006A Signature Analyzer, the first signature measurement instrument to offer composite signature.

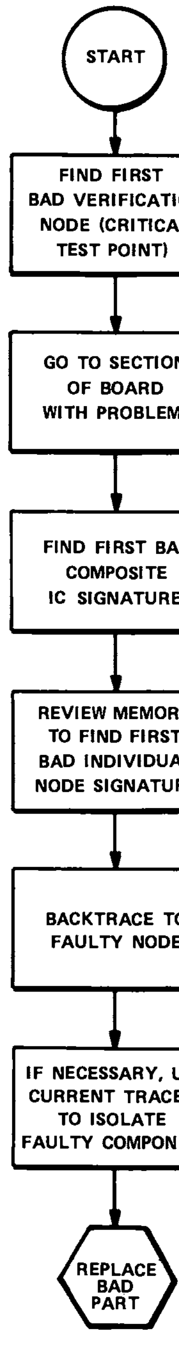


Figure 2. Identifying a Fault Source in a Digital Circuit

Composite signature is a sum of all triggered signatures since the last CLEAR. A signature is triggered when the probe button is pushed. This causes the signature to be added to the composite. The triggered signature is also stored in the memory stack.

First, when troubleshooting by hand, the correct operation of a circuit board can be tested by taking a composite signature on key test points or "verification nodes". A good composite at this point means the circuit board is operating correctly with high confidence. This assumes the designer has created verification nodes that will not leave undetected faults.

If the composite does not match the signature table, there is a fault somewhere in the circuit. The divide and conquer strategy is now used. Perhaps a bad signature at an individual verification node indicates a certain part of the circuit is the source of the fault. Thus, the next step is to measure individual signatures on verification nodes. Figure 3 details the process used to verify correctly operating circuit boards or find the subsection of the board with the failure if a faulty verification node is found.

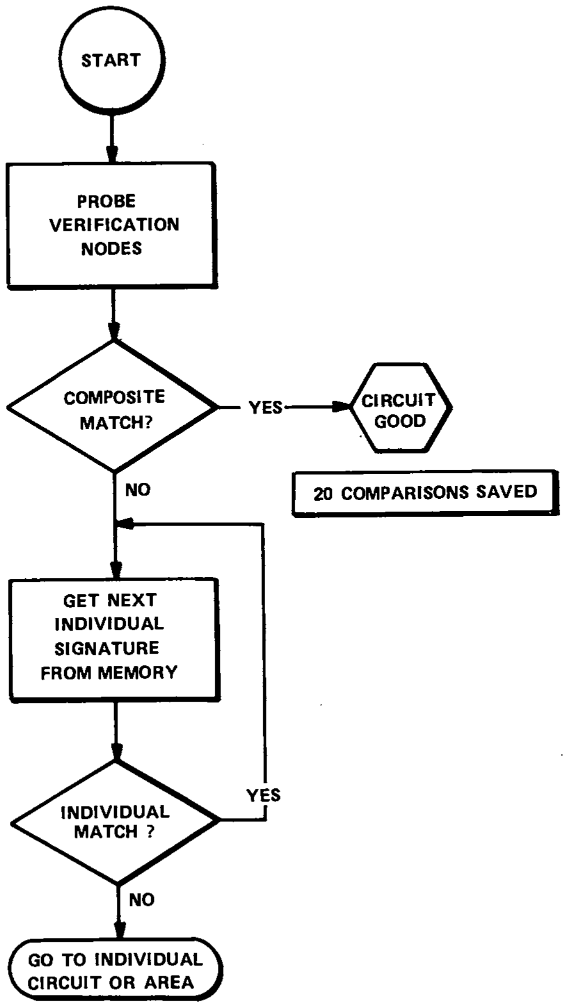


Figure 3. Board Verification — Finding the Subsection of Board with the Fault Source

Composite signature is again used in the faulty part of a circuit to do high level testing and quickly identify a bad signal with only minimal comparisons to documentation. Figure 4 shows the process of finding the first individual signature that does not match. This is necessary to begin backtracing. Composites can be taken on logical groupings of signals. For example, since it is easy to lose your place and tedious to count pins, a composite signature for a single IC saves the troubleshooter time and frustration when probing.

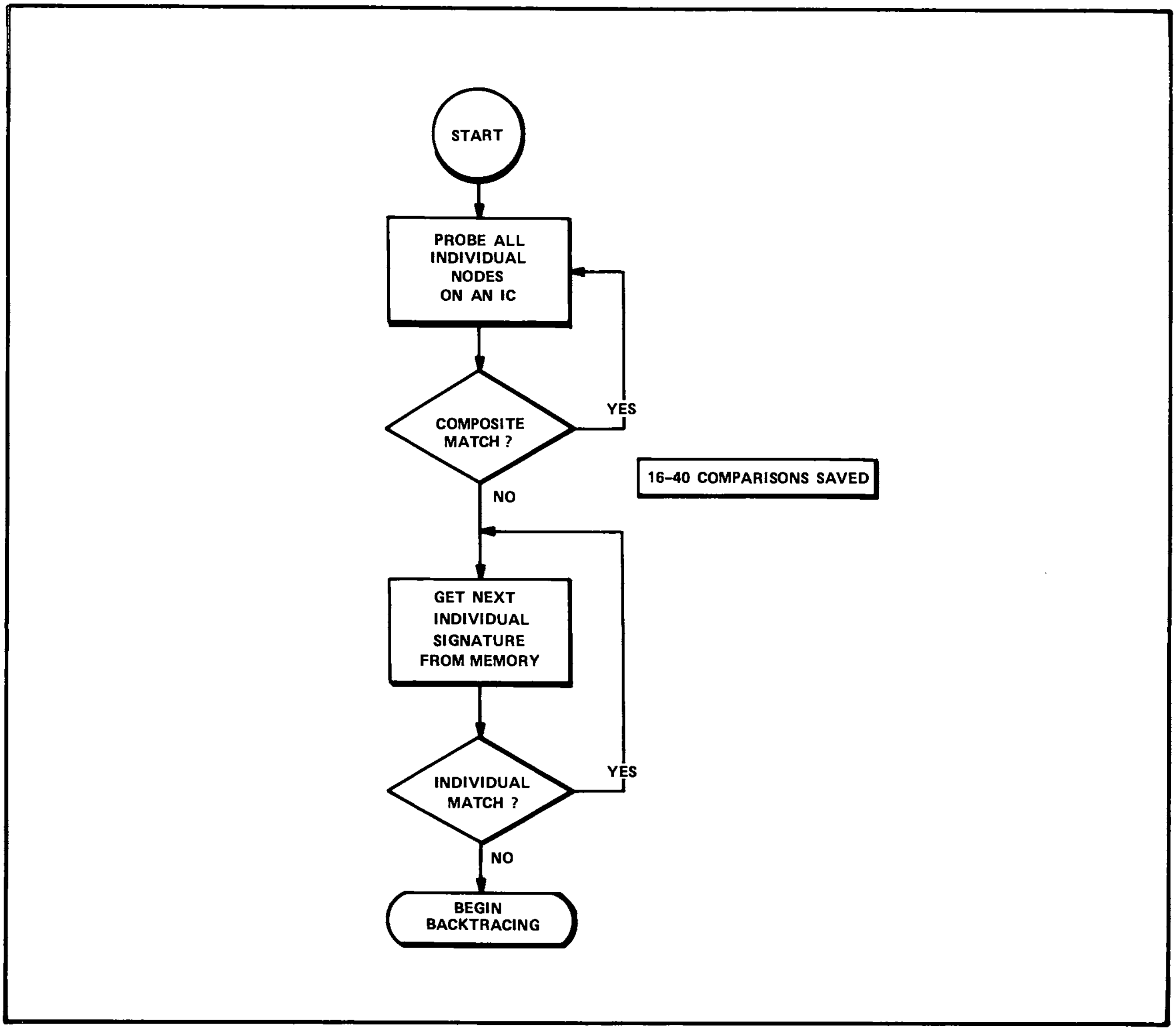


Figure 4. Finding a place to start backtracing by comparing Composite Signature for an Integrated Circuit.

Notice that as long as the composite consists of less than 32 signatures, it will not be necessary to **reprobe** the individual nodes, test points, or pins. The HP 5006 A remembers the last 32 signatures probed. It numbers them in the order probed. Number one is thus the first signature probed. When reviewing the stack in RECALL mode, the HP 5006 first displays the number and then the signature. The first signature displayed is the composite. The individual signatures are displayed in reverse order when the probe button is pushed (RECALL mode). Address and data buses can have composite signatures. Checking each line with the HP 5006A signature memory can be done quickly if there is no match of composite signature.

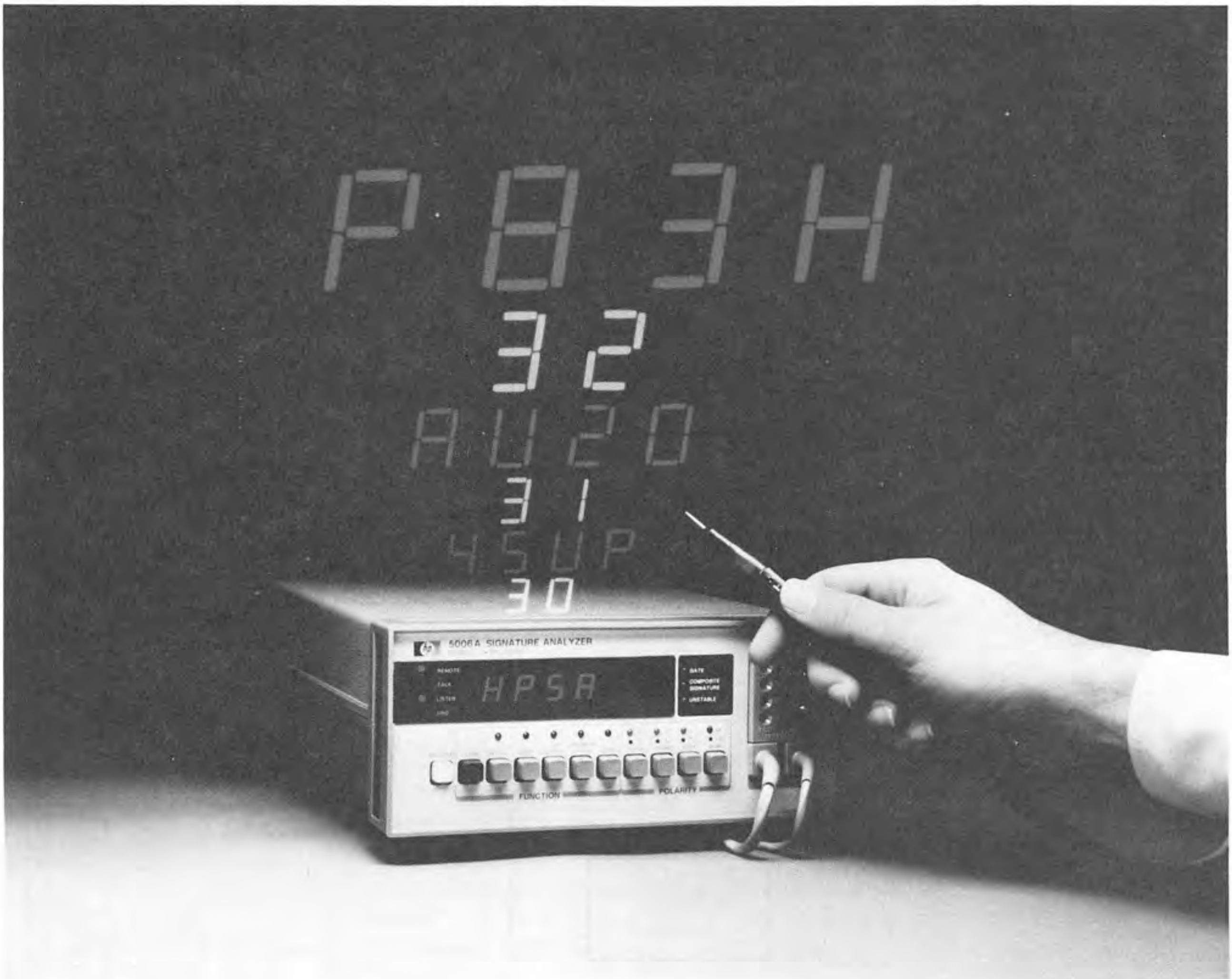


Figure 5. The operator can concentrate on probing without referring to the display using the signature memory in the HP 5006A. This makes misprobes and miscounts less likely. Time is saved when composite signature does not match because individual signatures do not need to be reprobed. The memory can be reviewed in the RECALL mode by pressing the probe switch and then compared to printed tables.

BACKTRACING

Once a bad signal is identified, the backtracing process begins. Backtracing is defined as tracing faulty signals upstream in a circuit to isolate the source of bit stream errors. Because signature analysis is highly accurate, it is well suited for detecting even the most subtle errors downstream from the source. See Figure 6 for a detailed graphical explanation of backtracing. Because a good part will pass faulty waveforms, inputs are checked first. If a faulty waveform is detected at an input, there is no reason to check an output. The troubleshooter uses the schematic and signature table to trace his way back to the source of errors, checking only inputs as he probes. The stopping rule in backtracing is:

"When all inputs on a device are ***good****, stop backtracing."*

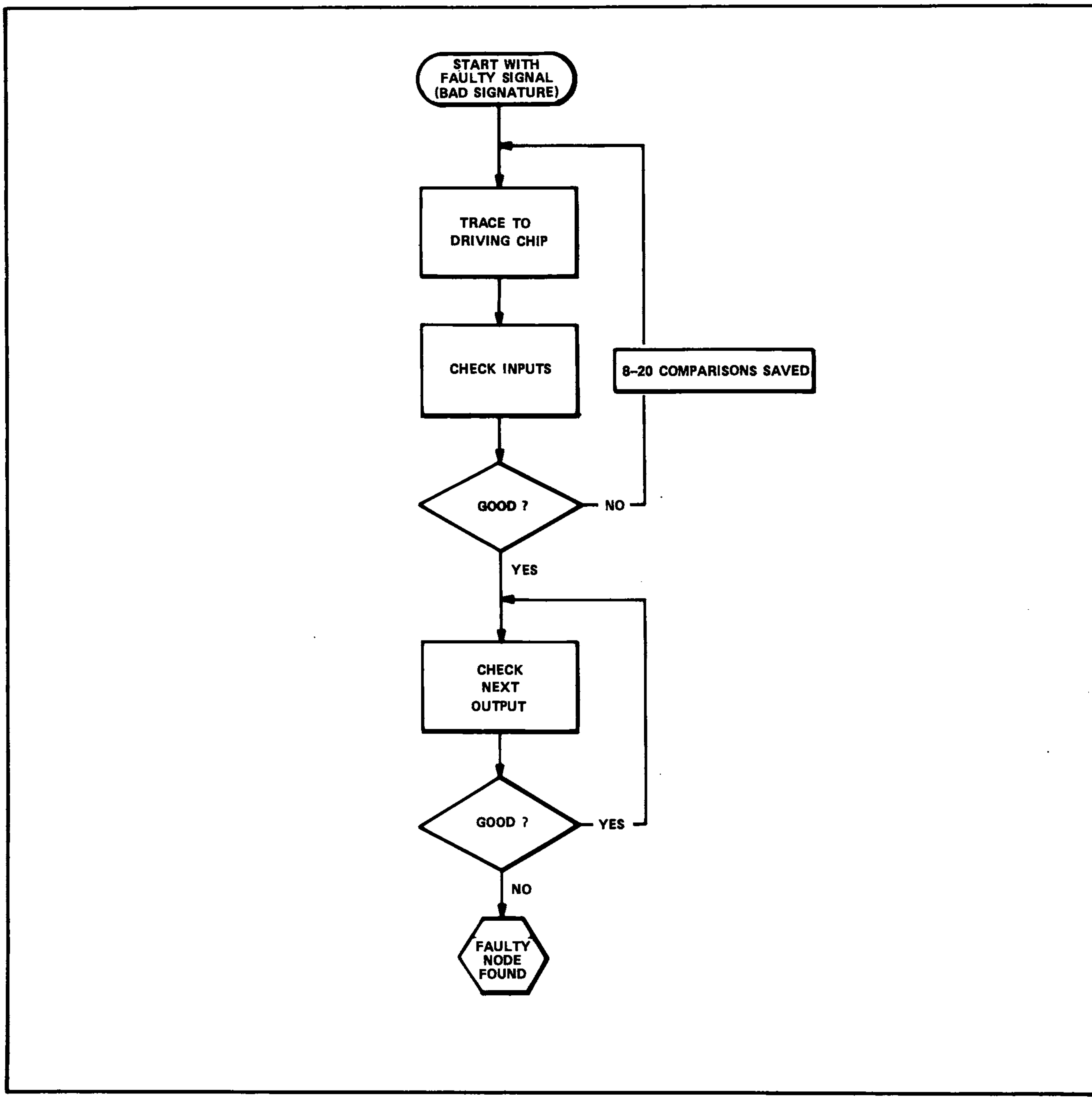


Figure 6. Backtracing

In most cases, the source of waveform errors is generated inside a faulty device. Most likely one of the output signatures will not match the recorded good ones. In all cases, a bad node has been found. Figure 7 shows the conclusions made after all inputs have been found good. If all outputs (and inputs) are good, the fault must be between this **good** chip and the last faulty input probed. Hence, we conclude the problem is a bad trace, in this case.

It is possible to speed up the backtracing process by generating composite signatures for inputs. The troubleshooter then probes all inputs on a device and only compares the composite signature to the expected one. Thus, when a good composite signature is found for inputs, the backtracing process can stop.

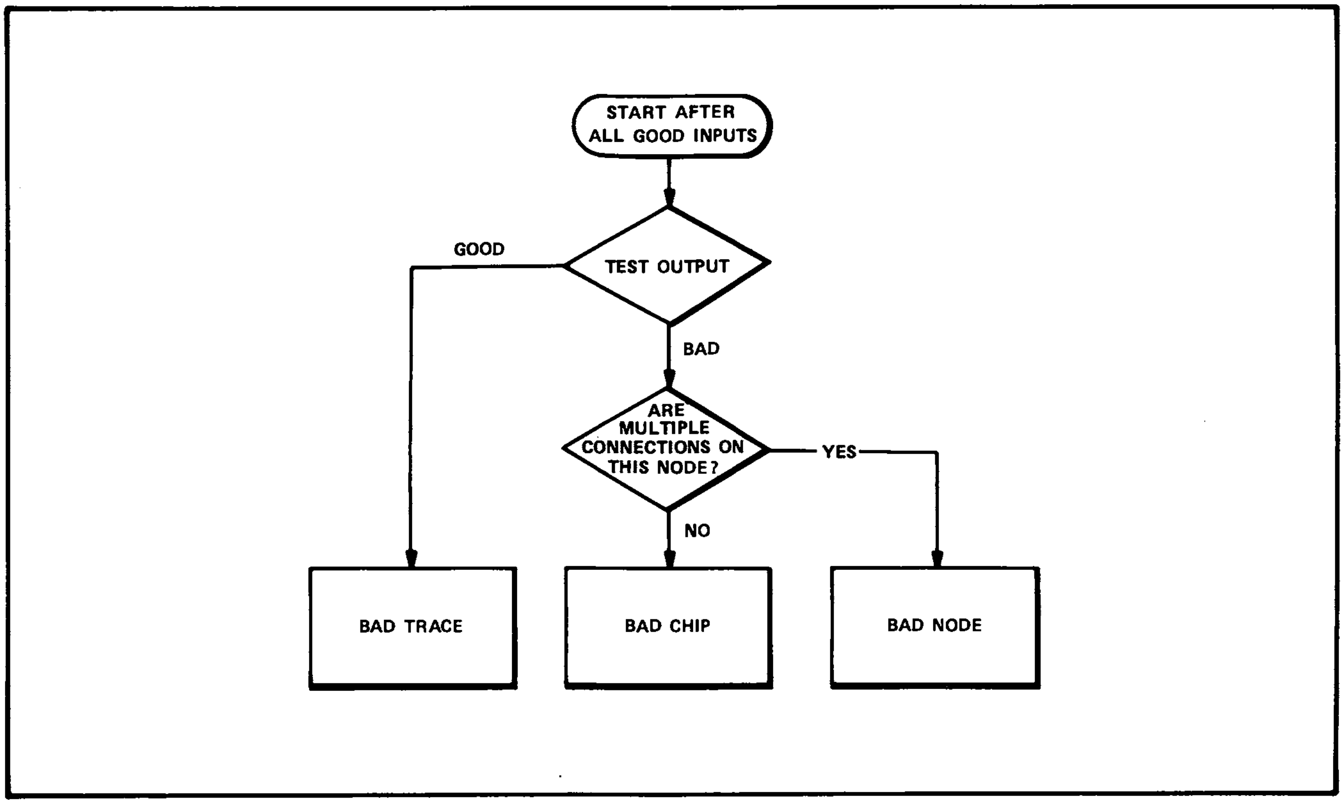


Figure 7. Resolving outputs after finding a part with all good inputs.

TIME SAVING ESTIMATES

It has been estimated that 5 to 35 minutes can be saved per circuit board using composite signatures when troubleshooting by hand without the aid of a computer to do matching of the individual signatures. These estimates are based on a number of assumptions:

1. The average number of nodes which need to be probed to find the bad parts.
2. The amount of time saved by not having to read the display and make a visual comparison to a signature table or schematic, for each individual signature.

Table 1 details these estimates for the three steps in troubleshooting where signature comparisons occur: probing verification nodes, finding the first bad signal and backtracing. These estimates do not take into consideration the additional advantage of not having to hold the probe on the node while reading the display and comparing to documentation. The benefit is that the probe is less likely to slip off the pin. Thus, the user will not have to recount the pins and the chances of a misprobe are much lower.

TABLE 1 — **Summary of time saved per circuit board using composite signature**

TROUBLESHOOTING STEP	NUMBER OF COMPARISONS			AVERAGE TIME SAVED PER CIRCUIT BOARD @ 5 SEC / COMPARISON
	Min.	Avg.	Max.	
Verification Nodes	5	15	25	1¼ Min.
First Bad IC (Pins x IC's)	80 (16 x 5)	100 (20 x 5)	200 (40 x 5)	8⅓ Min.
Backtracing (Inputs x IC's)	80 (8 x 10)	100 (10 x 10)	200 (20 x 10)	8⅓ Min.
Total	165	215	425	∽ 18 Min. Average 5 — 35 Min. Range

USING A COMPOSITE SIGNATURE ANALYZER

The HP 5006A automatically generates a unique "composite signature" after each triggered signature measurement. The composite signature is a computed signature, representative of the sum of all the triggered signatures accumulated since the last CLEAR or power-up. Only triggered signatures (those preceded by pressing the Data Probe Switch) can affect the composite signature. In operation, the composite signature is automatically recalculated and updated with each new measurement, based on two factors; the previous composite signature and the new signature. In this manner, the composite signature remains representative of all signatures taken, even after signatures have dropped off the bottom of the memory stack.

A composite signature can be used to represent as many signatures as you like, from a set of two pins to an entire circuit board. You should be aware that the larger the number of pins involved, the greater the chance of a duplication, misprobe or forgery. Approximately twenty measurements per composite signature is generally a safe and convenient number.

The composite signature can be reviewed at any time by pressing the front panel RECALL key. In the RECALL function, the composite signature is identified in two ways; the front panel COMPOSITE SIGNATURE LED annunciator lights and all four decimal points in the display light (the latter is advantageous during remote operation). To return to normal operation press RECALL a second time to turn the function off.

Figure 8. Troubleshooting is easier and faster with composite signature for those who do not have a computer-aided system. Composite signature is indicated in the RECALL mode with decimal points in the display and a lit LED between the gate and unstable LEDs just to the right of the display.

Editing the Signature Memory Stack

If a composite signature comes up bad for an IC or bus, it may be because the user has probed the same pin twice, for example. The user does **not** have to reprobe every pin in the group. Single signatures can be changed in the stack in the EDIT mode. Composite signature will be automatically corrected when the individual signature is remeasured. The remeasured signature will be written over the old entry in the stack. The new composite and individual signature can be reviewed by going back to the RECALL mode.

CALCULATING COMPOSITE SIGNATURE

One may wish to calculate composite signatures for existing products rather than measuring them with the HP 5006A. Calculating composite signature is straightforward. It is simply the sum of the individual signatures. However, since signatures are represented in a unique character set (see Table 2), they must first be converted to hexidecimal and then reconverted after they are summed. Carries beyond 16 bits are simply discarded.

TABLE 2 — Hex to Signature Conversion Chart

HEX	SIGNATURE
A	A
B	C
C	F
D	H
E	P
F	U

Figure 9 shows an example for the composite address signature of the 8085 microprocessor when free-running. A microprocessor can be made to freerun by forcing a NOP on its data bus with hardware. The processor will cycle through its address space continuously searching for an instruction only to find another NOP. Freerun is useful for checking out the microprocessor, ROM's, address bus and data bus.

ADDRESS	SIGNATURE		HEX
0	UUUU		FFFF
1	5555		5555
2	CCCC		BBBB
3	7F7F		7C7C
4	5H21		5D21
5	0AFA		0ACA
6	UPFH		FECD
7	52F8		52C8
8	HC89		DB89
9	2J70		2D70
10	HPP0		DEE0
11	1293		1293
12	HAP7		DAE7
13	3C96		3B96
14	3827	+	3827
15	755P		755E
Total			0579

Composite Address Signature = 0579 (8085 FREERUN)

Figure 9. Example — Free Run Address Composite Signature for the 8085

CONCLUSION

Composite signature is the sum of individual signatures. The individual signatures can be from IC's, buses or any other logical grouping of signals. Composite signature saves troubleshooters time when making comparisons of the display to printed documentation. Preliminary estimates show from 5 to 35 minutes can be saved per circuit board tested.

With the HP 5006A, signature gathering and comparing to documentation can be done separately and in groups. The signature memory has allowed probing to be done without having to look at the display. The benefit is that the operator can concentrate on probing, making miscounts and misprobes less likely. Individual signatures do not have to be RECALLED if the measured composite matches the documentation, saving time.

APPENDICES — THEORY OF OPERATION

The two appendices show why composite signature works. The linearity property of signature analysis allows us to add signatures to form a composite signature. The section on "probability of error detection" shows that the chance a composite signature will **not** detect an altered waveform (forgery) is only slightly less than that for individual signatures (for composites made up of moderate amounts of individual signatures).

APPENDIX A

LINEARITY

Signature Analysis is linear. Because of this property, composite Signature Analysis is possible. Linearity means signatures can be summed. Composite signature should possess the normal properties of addition such as commutativity and associativity

The idea was generated from a ROM testing technique. A ROM can be tested by reading each address in a loop and then taking signatures on the data bus. Another technique serializes the individual data bus lines and generates a single signature for all the data. Thus, one signature represents whether the ROM was working or not. There is then no need to test the individual signatures of each bus line.

Figure 10 shows the probability of not detecting a waveform bit error as a function of waveform bit sequence length. This phenomenon has been called a forgery. The signature appears good although the waveform is different. The probability of forgery approaches 2^{-16} asymptotically as bit sequences get long. It is effectively 2^{-16} for bit sequences longer than 25.

With microprocessor clocks typically 1 MHz or greater, it is easy to get waveforms with thousands of bits. Intuitively the probability of forgery (not detecting a waveform error) is less for individual signatures than composite signatures. It only becomes significant when the number of individual signatures making up the composite becomes large. Composite signatures can be used to structure digital testing and provide a "top-down" approach to troubleshooters.

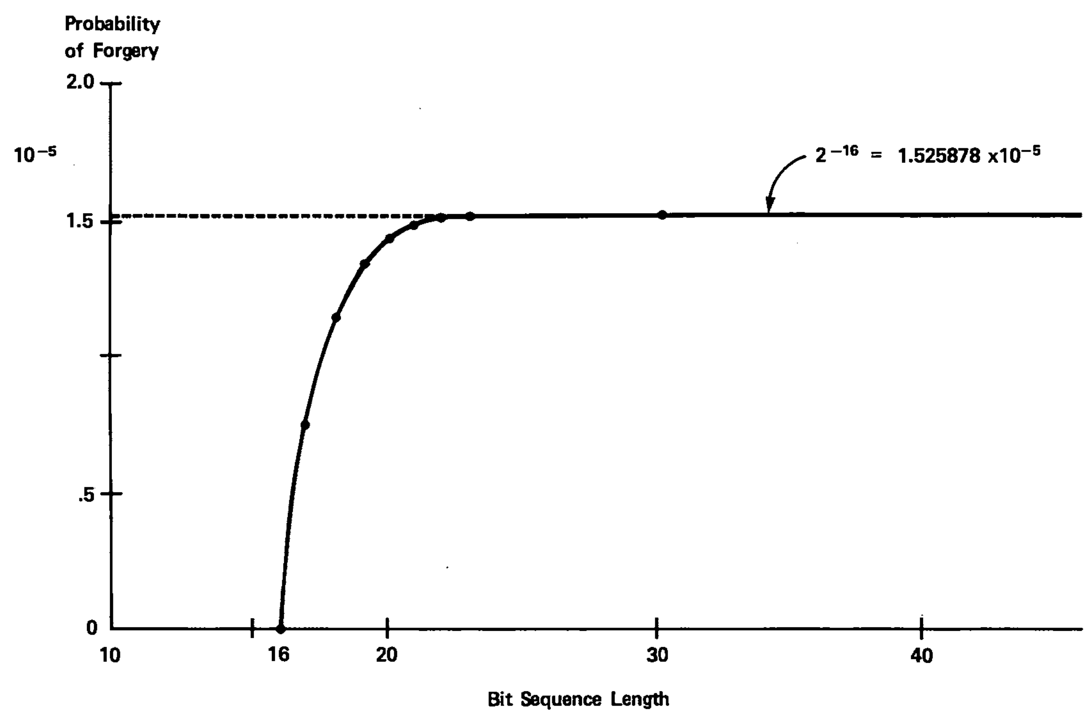


Figure 10. Probability of forgery as a function of bit sequence length.

APPENDIX B

PROBABILITY OF ERROR DETECTION

There are two ways a composite signature will not catch a bit error. A forgery of one or more of its individual signatures is one way. A signature is forged when a bit error occurs, but the signature remains unchanged. A sum of forgeries is a forgery. The second way is when two or more bad signatures cancel in the sum. The probabilities are addressed by the following questions:

1. What is the chance all individual signatures are good and the composite is bad? ANS: 0. i.e., A bad composite always indicates a bad individual.
2. What is the chance one individual is bad but composite is good? ANS: 0. Because of linearity, the one altered individual will produce an altered sum.
3. What is the chance two or more individual signatures are bad and cancel out when summed in the composite? ANS: 2^{-16}.
4. What is the chance one or more individual signatures are forged, and thus, the composite is forged?

   ANS: $1-(1-p)^n$

   where n = number of individual signatures in the sum.

   p = probability of individual forgery ($\sim 2^{-16}$ for 25 bits or more).

Proof of 3:

Suppose individual bit errors occur to alter 2 individual signatures.

A —> A' = A + a   a not = 0
B —> B' = B + b   b not = 0

If the composite is to remain unaltered then:

A + B = A' + B'

Substituting gives

A + B = A + a + B + b
0 = a + b for unaltered composite

Thus, for every "a" there is only one "b" out of 2^{16} possibilities that give a sum equal to zero.

For three or more signatures, the argument would be similar.

Please see Figure 11 for a graphical explanation.

Stated simply: A sum of signatures will be in the set of all signatures. It will be equally likely that a sum will be zero as any other signature. Thus, the chance that two or more signatures are bad and cancel in the composite is $1/2^{16}$.

SIGNATURE		HEX		CHANGE
S_1	$\longrightarrow$	H_1	$+$	Δ_1
S_2	$\longrightarrow$	H_2	$+$	Δ_2
⋮	⋮	⋮	⋮	⋮
S_n	$\longrightarrow$	H_n	$+$	Δ_n

$$S_c \longleftarrow \sum_{i=1}^{n} H_i + \sum_{i=1}^{n} \Delta_i$$

$$P\left(\sum_{i=1}^{n} \Delta_i = 0\right) = \frac{1}{2^{16}}$$

Figure 11. Probability of two or more individual signatures cancelling in the sum (composite signature).

Derivation of 4:

Because it is a sum, the probability that a composite signature has not been forged is the probability that no individual signature has been forged.

Let n = number of individual signatures.
f_c = composite forgery
f_i = individual forgery

$$\text{not } f_c = \Omega_{i=1}^{n} \text{ not } f_i$$

Assuming forgeries occur independently:

$$p(\text{not } f_c) = \prod_{i=1}^{n} \left\{1 - p(f_i)\right\}$$

$$\approx (1 - 2^{-16})^n \text{ for bits sequences longer than 25 bits.}$$

Figure 12 graphs the probability of composite forgery as a function of individual nodes (n).

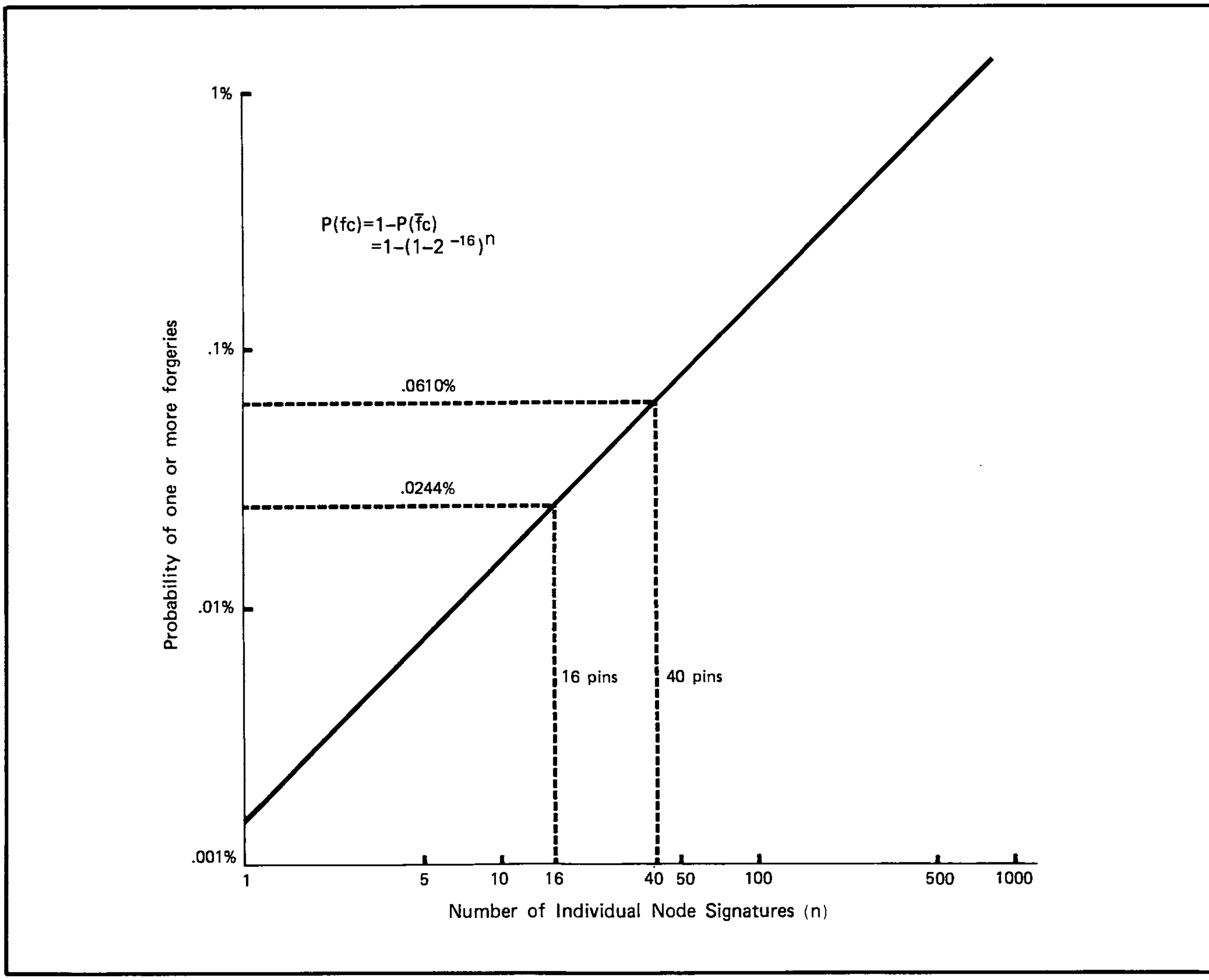


Figure 12. Probability of composite forgery as a result of one or more individual forgeries.

HEWLETT PACKARD

For more information, call your local HP Sales Office or nearest Regional Office: **Eastern** (201) 265-5000; **Midwestern** (312) 255-9800; **Southern** (404) 955-1500; **Western** (213) 970-7500; **Canadian** (416) 678-9430. Ask the operator for instrument sales. Or write Hewlett-Packard, 1501 Page Mill Road, Palo Alto, CA 94304. **In Europe**: Hewlett-Packard S.A., 7, rue du Bois-du-Lan, P.O. Box, CH 1217 Meyrin 2, Geneva, Switzerland. **In Japan**: Yokogawa-Hewlett-Packard Ltd., 29-21, Takaido-Higashi 3-chome, Suginami-ku, Tokyo 168.

02-5952-7684 **APRIL 1983** **PRINTED IN U.S.A.**