INTERNATIONAL ORGANISATION FOR STANDARDIZATION

ORGANISATION INTERNATIONALE DE NORMALIZATION

ISO/IEC JTC 1/SC 29/WG 3

CODING OF MOTING PICTURES AND AUDIO

ISO/IEC JTC 1/SC 29/WG 3 mNNNN

Online — November 1, 2024

Title: Allow CFF2 VariationStore lengths greater than 65,535

Author: Skef Iterum

Introduction

The current CFF2 specification limits the size of its VariationStore to 65,535 bytes, due to the `uint16` used to indicate its length. The thought was probably that because there are no deltas stored in that IVS then sixteen bits would be fine. Behdad Esfahbod has noted that this limit has already been reached in some of Google's test scenarios.

The suggestion is to allow the length of the IVS to exceed 65,535 bytes when needed, in which case the length field should be set to 65,535. If some client needs to determine the length it can do so by parsing the entire IVS structure and tracking the offsets it reads.

While this change is not strictly editorial, it is unlikely to affect any client that *reads* and *interprets* a font. The length field is likely ignored except by programs that need to *manipulate* the font.

Additionally, even those cases are unlikely to include a subsetting program, as those will more likely parse and write the IVS back out. Therefore we feel this change is relatively low-risk.

Changes

In section 5.3.3.11.2 (VariationStore)

In second column of the `length` row of the table, "data[length]" becomes "data[length] or (varies)".

After the table this note is added:

> Note: When the ItemVariationStore data length is less than 65,535 bytes the length field should match that length. When it is 65,535 bytes or longer, which is permitted, the length field should be set to 65535. An application needing to know its actual length can determine it by parsing all of its data and tracking the maximum offset reached.