

On the Bidi_Mirroring_Glyph of U+1DB10 CARTESIAN EQUALS SIGN

From: Robin Leroy
Date: 2026-07-24
To: UTC

Note: As the issue set out in this document, discovered after the end of the 18.0 β review period, pertains to possible security implications of the 18.0 property assignments, there is an urgent need for the UTC to consider it. The Properties and Algorithms briefly discussed the issue, but did not have the time to come to a conclusion. Instead of deliberating the issue further in the working group for recommendations to be made at UTC #189, too late to affect the Unicode 18.0 release, this proposal is therefore presented directly to UTC #188.

Background

In Unicode 18.0 β , BidiMirroring.txt has the following lines:

```
221D; 1DB10 # PROPORTIONAL TO  
1DB10; 221D # CARTESIAN EQUALS SIGN
```

The sign indeed looks like a mirrored ∞ , see [WG 2 N5334R2](#) pp. 2 & 34.

However, this is the first instance of Bidi_Mirroring_Glyph mapping a BMP character to a non-BMP character, and vice versa. After 18.0 β integration, this caused a flurry of serious bugs (including two buffer overflows) in the ICU bidi implementation, which has an option to perform the mirroring¹, and assumed this did not change the UTF-16 size; see [ICU-23454](#), [ICU-23455](#), [ICU-23456](#), [ICU-23457](#).

The ICU bugs have been resolved. However, it is expected that there are other implementations that use Bidi_Mirroring_Glyph, and they may be making the same assumptions that ICU was. If so, the mapping could create vulnerabilities in these implementations, which may well go unnoticed: the ICU bugs were not immediately caught by regular test suites, but instead were detected after weeks of fuzzing following β integration.

The primary non-legacy use of these mappings is to provide documentation for font designers; however, some font designers use them through tooling that checks for font features, so they would only benefit from an actual mapping, not from documentation that there should be one. Notably, the new character, U+1DB10 CARTESIAN EQUALS SIGN, is unlikely to occur in right-to-left text since it is a historical mathematical character used in publications in Latin script, so the practical implications may be minor even if designers do not have the mapping.

Proposal

Two options were discussed by the Properties and Algorithms group.

¹ This is used by older text rendering implementations that do not do their mirroring via OpenType.

Alternative 1

Comment out these lines in BidiMirroring.txt for 18.0, adding an explanation in the file. Issue a PRI stating that they will be uncommented in 19.0, and warning implementers that, in general, they should ensure their usage of code point valued properties does assume that they preserve UTF-16 size, calling out in particular the simple case mappings and foldings which currently preserve UTF-16 size.

This gives implementers as much advance notice as possible, and gives us an opportunity to warn them about future issues: once we run out of room in the BMP, any uppercase counterparts of BMP characters that are found will require simple case mappings that change UTF-16 size.

Alternative 2

Keep the mapping as in 18.0β, and warn implementers about the potential issue in the [Migration](#) section of the 18.0 release notes.

This avoids delaying the mapping for an issue that should only affect implementations that rely on legacy text rendering techniques.