Paid work has recently led me into the realm of barcodes. I had not thought that this is an area offering much in the way of intellectual interest. However looking at it a bit closer shows that there is more to it than meets the eye...

What it comes down to is that a barcode is designed to be severely maltreated, but still remain readable. This is not as simple as one might think. Designers work hard to make the barcodes robust, firstly through the optical quality of the encoding - i.e. how unambiguous the patterns are - and secondly through the use of sophisticated error checking/correction codes, e.g. Reed Solomon.

Another factor is the rise of 2D Barcodes such as DataMatrix or Aztec. With these codes one can store a considerable amount of data - not just a reference to a database entry held somewhere else. This makes offline applications possible, for example, the internet ticketing used by the deutsche Bahn (Aztec), or the postal stamps that one can buy over the internet & print out yourself (DataMatrix for the US Post).

One negative aspect of this is the sheer mass of different formats, including sub-formats - for example Code128, a one dimensional barcode, has three separate supported subsets of characters that it can represent, effectively making it into 3 separate formats. Relying on documentation that claims to "support Code 128" is not enough.

This has all led to very little work being done on cryptoleague recently. I will get back to it though.