Proposal for C2x
WG14 2603

Title: Qualifier-preserving standard library functions
Author, affiliation:
Alex Gilding, Perforce
Jens Gustedt, INRIA
Date: 2020-10-29
Proposal category: Feature enhancement
Target audience: Library developers, library users

Abstract

Proposal to improve type safety of existing C Standard library functions by preventing the ability to silently remove `const`-qualification without a cast. This introduces a suggested new notation for qualifier-generic functions, and aims to slightly reduce the difference between the C and C++ Standard libraries.

Qualifier-preserving standard library functions

Reply-to: Alex Gilding (agilding@perforce.com)
Document No: N2603
Revises Document No: N/A
Date: 2020-10-29

Summary of Changes

N2603

- original proposal

Introduction

The C Standard Library contains twelve "qualifier-losing" search functions:

```
bsearch
bsearch_s
memchr
strchr
strpbrk
strrchr
strstr
wcschr
wcspbrk
wcsrchr
wcsstr
wmemchr
```

These functions accept a `const`-qualified pointer to a buffer to be searched, but return the pointer to the found element without `const`-qualification.

This proposal suggests that the library should specify that these functions return a found result element with the same qualification as the input buffer, as provided by the user. This avoids the risk of inadvertently "casting away" constness on an input buffer when this is not desired.

This proposal is extracted from n2522, "a common C/C++ core specification", by Jens Gustedt.

Rationale

The existing APIs were designed and added to the library before C11 introduced the ability to define generic and overloaded functions. Therefore the existing signatures are by-design, so that they can be used to search both `const` and mutable buffers - since `const`-qualification can be added implicitly, the input parameter is able to accept both kinds of buffer. If the functions are used correctly, the missing qualification on the return will be restored in the same way on assignment to an appropriately-qualified result pointer. This makes the search functions provide a primitive form of genericity.

Unfortunately this relies on the user to manually check that the variable for the returned pointer to the found element is of the correct type. If the user searches a `const`-qualified buffer but assigns

the result to a pointer to a mutable object, the API has no way to directly communicate that this is a type error. An implementation may be able to warn anyway but this would require a hardcoded knowledge of the library functions and their contracts beyond what is communicated in-language.

For example:

```
wchar_t const buf[] = L"Hwæt! wē Gār-Dena in gēar-dagum þēod-cyningaþrym
gefrūnon";

wchar_t const * thr = wcschr (buf, L'þ'); // const implicitly restored
wchar_t       * ans = wcschr (buf, L'æ'); // currently assignment not wrong;
const lost

// ...

*thr = L't'; // constraint violation
*ans = L'a'; // currently no error, runtime undefined behaviour
```

The `const`-loss is purely an API-accommodation for the fact that in C99 and earlier revisions, it was not possible to express qualifier-generic functions in-language. There is no valid use case for this lossiness (intentionally passing a `const`-qualified buffer and receiving the element without restoring the qualification), because casting away `const`-qualification explicitly is already a feature of the language. If the user really needs a non-`const`-qualified pointer into a `const`-qualified array, they can still communicate that this is an intentional decision, by casting the `const`-qualification from the pointer to the buffer *before* passing it as an input argument to the search API.

```
wchar_t * ans = wcschr ((wchart *)buf, L'æ'); // explicitly strip constness
```

Unlike the `strerror` function and others discussed in n2526, there is no scope for a library implementation to provide additional mutability features, because the returned pointer is into a buffer controlled and provided completely by the user, not to some piece of library-internal state which may have other uses, or access points elsewhere in an extended API.

This vulnerability has already been fixed in C++, which is able to resolve an overloaded version of each function with the appropriate returned pointer type, based on the `const`-qualification of the buffer passed as the argument. This therefore reduces the footprint of differences between the two langauges' Standard libraries.

Proposal

We propose that each of these 12 functions be defined as a *generic function*, parameterized so that the qualification of the buffer pointed to by the first argument is the same as the qualification of the pointed to the found element.

This can be expressed with three choices of notation. Their relative merits, or lack thereof, may provide input to a related discussion about standarizing C's notation for generic library functions.

Parameterizing only the qualifier:

```
char Q * strchr (char Q * s, int c);
void Q * memchr (void Q * s, int c, size_t n);
```

(following existing convention, `Q` would be italicized or otherwise marked)

The advantage of this notation is that it limits the scope of the constraint to the qualification and leaves the object type either explicitly typed, or `void`. This retains the explicit typing of those functions that examine characters, and does not place additional restrictions on how objects found in opaque buffers should be interpreted.

Parameterizing the entire pointed-to type, including qualifier and object components:

```
C * strrchr (C * s, int c);
W * wcsrchr (W * s, wchar_t c);
C * strpbrk (C * s1, char const * s2);
```

The advantage of this convention is that the entire pointed-to type is parameterized, which may be visually clearer by communicating that the qualification is a preserved part of the complete derived type. It also does not imply that there is necessarily any qualification at all (i.e. `Q` can be empty / missing). However, by removing the explicit mention of the qualifier it also removes the focus on the fact that it is preserved.

This highlights an advantage: other pseudo-generic parameters (such as the `int` or `wint_t` second parameters) can be marked as sharing the parameterized type. This indicates that the search key and the array of elements to examine are expected to be the same type of object. For `bsearch`, this might look like:

```
E * bsearch (E const * key, E * ptr, size_t count, size_t size
           , int (*comp) (void const *, void const *));
```

However, this highlights several problems: the notation now makes it visually ambiguous whether the parameter is supposed to include the qualification (the redundant qualification in `E const * ptr` is consistent with `typedef` rules, but not necessarily *clear*), and the fact that the `comp` parameter actually does need to be strongly-typed to accept `void` pointers means it cannot be written using the parameters. In addition, in the case of the `strchr` group, the key parameter does *not* have the same object representation, using `int` as a generic character key instead.

For the string search functions, this does show the possibility for further modification to the API, to unify the wide and narrow character searches into a single non-prefixed API. This would be a more intrusive change than proposed here. (see Future Directions, Generic functions)

For `bsearch`, this shows that simple parameterization in the signature is not sufficient to combine with `void` pointers used by higher-order function types. A more powerful mechanism for describing strongly-typed `void` pointers in generic higher-order functions is required. (see Future Directions, *void-which-binds*)

Overload lists:

```
char const * strstr (char const * s1, char const * s2);
char       * strstr (char       * s1, char const * s2);

wchar_t const * wmemchr (wchar_t const * s, wchar_t c, size_t n);
wchar_t       * wmemchr (wchar_t       * s, wchar_t c, size_t n);
```

This is consistent with C++, which actually does provide separate overloads.

However, this is misleading: this is not how overloading works or is implemented in C, and has no connection at all to the declarations that would exist in the library.

In C++, each overload is also a completely separate function - this declaration communicates that fact. In C, there is only ever one callable with a given name. If it exists as a non-macro entity, it has a singular type and it has a single exported external symbol. The C++ syntax is therefore not appropriate as it communicates a completely different set of assumptions about how the library makes names visible.

The rest of this document will use the first syntax option, parameterizing only the qualifier, as it is the smallest and least intrusive change. The second syntax option provides grounds for future discussion about the evolving role of generic functions and a direction for more aggressive API changes.

Alternatives

An alternative would be to deprecate all twelve functions and to add new APIs with the qualifier-preserving property. This has three major drawbacks:

- the new APIs would likely only be used by conscientious users who are less likely to make the underlying error in the first place.
- new APIs do not fix existing erroneous uses of the unsafe APIs; any errors will still be present and not elicit warnings.
- because C++ has already closed this loophole using its own in-language tools for these APIs, introducing new function names would widen rather than narrow the divergence between the two languages.

A potential heavier-weight alternative relying on future language directions would be to convert all APIs to use typed `void` pointers, i.e. the *void-which-binds*. This would also allow the compiler to enforce that the object type of the element is preserved and not just its qualification. This has the significant disadvantage of not yet existing in-language.

However, this may demonstrate an initial use case for such a feature.

Impact

ABI

None. The existing functions already work correctly when used with the appropriate operands. All this proposal does is alter the interpretation of the signature types to enable stricter checking of the invocations. The Standard guarantees that the object representation of a pointer to `T` and a pointer to `T const` are compatible, so the ABI *must* not change to accommodate the proposed change (limited to qualifiers). A single underlying function body remains sufficient to implement the search feature itself, without changes.

C++ already provides two overloads which correctly propagate qualification. This means that the ABI problem would already be addressed in external linkage if two names are needed, and also that any existing code which compiles as both C and C++ has already been checked for qualifier-correctness by C++'s stricter library signatures. Therefore, user code in this category will be unaffected by the change as it must already be qualifier-correct.

Some existing user code should be expected to raise an error when it compiled cleanly before. However, it seems that all such new warnings would indicate a legitimate design error - unlike the `strerror` case, there is no valid use case for implicitly removing `const`-qualification from a buffer that the user *has* ownership of. If they meant to do so, they can still strip the qualification explicitly themselves, and communicate that intent. Therefore, this should be considered an API safety improvement and the new errors would be desirable.

Implementation

A high-quality implementation should provide a macro wrapper around the calls to the implementation function that re-applies correct qualification to the result type. The only impact of this would be to introduce a compile-time implicit pointer type conversion between two compatible pointer types, meaning that there is guaranteed to be no run-time cost.

An example of this implementation wrapper might be:

```
// string.h
// ...

#define _COMBINE_PTR(T, P) (false ? (T*)1 : (P))

#define _STRING_SEARCH_QP(T, F, S, ...)  \
  (false ? _COMBINE_PTR (T, (S)) : (F) ((S), __VA_ARGS__))

#define memchr(S, C, N)  _STRING_SEARCH_QP(void, memchr, (S), (C), (N))
#define strchr(S, C)     _STRING_SEARCH_QP(char, strchr, (S), (C))
#define strpbrk(S1, S2)  _STRING_SEARCH_QP(char, strpbrk, (S1), (S2))
#define strrchr(S, C)    _STRING_SEARCH_QP(char, strrchr, (S), (C))
#define strstr(S1, S2)   _STRING_SEARCH_QP(char, strstr, (S1), (S2))
```

This takes advantage of the type conversion rules used to convert both results of a ternary operator to the same pointer type. The qualifiers of the input argument are combined with the basic object type of the result pointer so that the returned result has the same qualification as the argument. This has no runtime cost, as guaranteed by the Standard.

A check for specific qualifiers is not required, as if the argument is more heavily qualified than the signature of the underlying search function allows, it will fail to type check after expansion. (If user-defined qualifiers are added to a later language version, an explicit exclusion check and cast become necessary to e.g. prevent `volatile` or an address-space qualifier from being used.)

A simpler implementation could continue to provide the APIs as they are and merely document that the constraint now applies. This might introduce some inconsistencies if the result of a search function is used with `_Generic`, but this is unlikely (the type is already one the user would not expect to match).

Future directions

This proposal introduces a number of ideas for further library development:

- in n2522, the wide and narrow versions of the string searches are all unified under the narrow-string names, and made generic in the character type. This would be a more intrusive change.

    - this would introduce the option for additional character types to be searchable by the same set of function names.
    - this significantly simplifies user-side type-generic string processing. However, this does not have precedent from C++, and would imply an ABI change. It is also unclear which headers would provide the APIs, and how completely (for instance, should the wide character searches be available from `string.h`, or should those "overloads" only become visible when both `string.h` and `wchar.h` are included? Should `wchar.h` still provide the explicit wide APIs?)
- The Embedded C TR 18037 introduces additional qualifiers to represent *named address spaces*. Pointers to objects in these address spaces can round-trip through `void`, but may have a different representation and can therefore not be examined by a generic pointer readthrough.
    - the `_Atomic` qualifier is already permitted to indicate different object layout requirements, and is similarly inappropriate to use with these APIs. This is therefore consistent with the idea that the overloads may restrict the set of qualifiers abstracted; currently only to `const`.
    - strongly-typed `void` pointers would be able to accommodate this when the read is only achieved through a provided access callback, so this restriction could be lifted from `bsearch` and `bsearch_s` in the presence of *void-which-binds*.
- Embedded C specifies that an implementation should provide some mechanism to declare the new qualifiers. This could exist separately as a way to tag opaque types with user-side meaningful data, without indicating an incompatible object representation (similar to `const`).
    - If such "tag qualifiers" were added to the language, it would be useful to allow them to qualify the operands to these search functions and to be preserved as well. They should be distinguished from qualifiers that may affect layout (address space, `_Atomic`) or the nature of access (`_Atomic` and `volatile`), which are not appropriate to abstract.
- ideally, the object type should also be preserved, rather than allowing the result pointer to a found element to be implicitly converted to a correctly- qualified pointer to an unrelated object layout.

  One future proposal which would allow this to be communicated is *void-which-binds*, introducing the concept of "strongly-typed `void`" to function declarations via attributes:

```
#define Void(A) void [[bind_type (A)]]

Void(T) * memchr (Void(T) * s, int c, size_t n);
```

  This future proposal would require that all implicit conversions to or from a `void` pointer component of a signature that are annotated with the same parameter name, bind to or from the same object type. Therefore,

```
char const buf[] = "o menel aglar elenath";

char const * mp = memchr (buf, 'm', 21); // OK
int  const * ip = memchr (buf, 'm', 21); // not OK if [[type(A)]] is
enforced
```

This would allow typed parameterization of `bsearch`'s key/buffer/result type without losing the connection to the `comp` function:

```
Void(T) * bsearch (Void(T) const * key, Void(T) * ptr
    , size_t count, size_t size
    , int (*comp) (Void(T) const *, Void(T) const *));
```

The ABI is not changed at all because the parameters are still `void` pointers, but their connection to a single element type is communicated.

- a unified notational convention for generic function signatures should be established for use throughout the Standard library. This will build consensus for whether it is better to abstract type components or whole pointed-to types, and will ensure that the signatures are easier to understand because they follow a coherent pattern. At the moment there is no formal convention because the needs of each library section are relatively distinct.

  The proposal in this document suggests a convention for abstracting the qualifier component of a type and leaving the object type component concrete; both approaches (vs. abstracting the whole pointed-to type) may be weighed against each other for clarity.

Proposed wording

The wording proposed is a diff from the ISO/IEC 9899-2018 archived public draft, n2176. Bolded text is new text.

`bsearch`

Modify 7.22.5.1 p1:

```
#include <stdlib.h>
Q void *bsearch (const void *key, Q void *base,
        size_t nmemb, size_t size,
        int (*compar)(const void *, const void *));
```

(`Q`-qualify the return type and change the `const` qualifier of `base` to `Q`)

Modify the first sentence of 7.22.5.1 p2:

> The `bsearch` **generic** function searches an array of ...

Modify the first sentence of 7.22.5.1 p4:

> The `bsearch` **generic** function returns a pointer to ...

Add a new paragraph after 7.22.5.1 p4:

> The `bsearch` function is generic in the qualification of the type pointed to by the argument to `base`. If this argument is a pointer to a `const`-qualified array, the returned pointer will also be to a `const`-qualified type.

7.24.5

Add an introductory paragraph before the individual function descriptions, 7.24.5 p1:

> The stateless search functions in this section (`memchr`, `strchr`, `strpbrk`, `strrchr`, `strstr`) are *generic functions*. These functions are generic in the

qualification of the array to be searched and will return a result pointer to an element with the same qualification as the passed array. If the array to be searched is `const`-qualified, the result pointer will be to a `const` -qualified element. If the array to be searched is not `const`-qualified, the result pointer will be to an unqualified element. The `volatile` and `_Atomic` qualifiers are not accepted on the elements of the array to search.

`memchr`

Modify 7.24.5.1 p1:

```
#include <string.h>
Q void *memchr (Q void *s, int c, size_t n);
```

(`Q`-qualify the return type and change the `const` qualifier of `s` to `Q`)

Modify the first sentence of 7.24.5.1 p2:

> The `memchr` **generic** function locates the first occurence of ...

Modify 7.24.5.1 p3:

> The `memchr` **generic** function returns a pointer to ...

`strchr`

Modify 7.24.5.2 p1:

```
#include <string.h>
Q char *strchr (Q char *s, int c);
```

(`Q`-qualify the return type and change the `const` qualifier of `s` to `Q`)

Modify the first sentence of 7.24.5.2 p2:

> The `strchr` **generic** function locates the first occurence of ...

Modify 7.24.5.2 p3:

> The `strchr` **generic** function returns a pointer to ...

`strpbrk`

Modify 7.24.5.4 p1:

```
#include <string.h>
Q char *strpbrk (Q char *s1, const char *s2);
```

(`Q`-qualify the return type and change the `const` qualifier of `s1` to `Q`)

Modify the first sentence of 7.24.5.4 p2:

> The `strpbrk` **generic** function locates the first occurence in ...

Modify 7.24.5.4 p3:

> The `strpbrk` **generic** function returns a pointer to ...

`strrchr`

Modify 7.24.5.5 p1:

```
#include <string.h>
Q char *strrchr (Q char *s, int c);
```

(`Q`-qualify the return type and change the `const` qualifier of `s` to `Q`)

Modify the first sentence of 7.24.5.5 p2:

> The `strrchr` **generic** function locates the last occurence of ...

Modify 7.24.5.5 p3:

> The `strrchr` **generic** function returns a pointer to ...

`strstr`

Modify 7.24.5.7 p1:

```
#include <string.h>
Q char *strstr (Q char *s1, const char *s2);
```

(`Q`-qualify the return type and change the `const` qualifier of `s1` to `Q`)

Modify the first sentence of 7.24.5.7 p2:

> The `strstr` **generic** function locates the first occurence in ...

Modify the first sentence of 7.24.5.7 p3:

> The `strstr` **generic** function returns a pointer to ...

7.29.4.5

Add an introductory paragraph before the individual function descriptions, 7.29.4.5 p1:

> The stateless search functions in this section (`wcschr`, `wcspbrk`, `wcsrchr`, `wmemchr`, `wcsstr`) are *generic functions*. These functions are generic in the qualification of the array to be searched and will return a result pointer to an element with the same qualification as the passed array. If the array to be searched is `const`-qualified, the result pointer will be to a `const` -qualified element. If the array to be searched is not `const`-qualified, the result pointer will be to an unqualified element. The `volatile` and `_Atomic` qualifiers are not accepted on the elements of the array to search.

`wcschr`

Modify 7.29.4.5.1 p1:

```
#include <string.h>
Q wchar_t *wcschr (Q wchar_t *s, wchar_t c);
```

(`Q`-qualify the return type and change the `const` qualifier of `s` to `Q`)

Modify the first sentence of 7.29.4.5.1 p2:

The `wcschr` **generic** function locates the first occurence of ...

Modify 7.29.4.5.1 p3:

The `wcschr` **generic** function returns a pointer to ...

wcspbrk

Modify 7.29.4.5.3 p1:

```
#include <wchar.h>
Q wchar_t *wcspbrk (Q wchar_t *s1, const wchar_t *s2);
```

(`Q`-qualify the return type and change the `const` qualifier of `s1` to `Q`)

Modify the first sentence of 7.29.4.5.3 p2:

The `wcspbrk` **generic** function locates the first occurence in ...

Modify 7.29.4.5.3 p3:

The `wcspbrk` **generic** function returns a pointer to ...

wcsrchr

Modify 7.29.4.5.4 p1:

```
#include <wchar.h>
Q wchar_t *wcsrchr (Q wchar_t *s, wchar_t c);
```

(`Q`-qualify the return type and change the `const` qualifier of `s` to `Q`)

Modify the first sentence of 7.29.4.5.4 p2:

The `wcsrchr` **generic** function locates the last occurence of ...

Modify 7.29.4.5.4 p3:

The `wcsrchr` **generic** function returns a pointer to ...

wcsstr

Modify 7.29.4.5.6 p1:

```
#include <wchar.h>
Q wchar_t *wcsstr (Q wchar_t *s1, const wchar_t *s2);
```

(`Q`-qualify the return type and change the `const` qualifier of `s1` to `Q`)

Modify the first sentence of 7.29.4.5.6 p2:

The `wcsstr` **generic** function locates the first occurence in ...

Modify the first sentence of 7.29.4.5.6 p3:

The `wcsstr` **generic** function returns a pointer to ...

wmemchr

Modify 7.29.4.5.8 p1:

```
#include <wchar.h>
Q wchar_t *wmemchr (Q wchar_t *s, wchar_t c, size_t n);
```

(Q-qualify the return type and change the `const` qualifier of `s` to `Q`)

Modify the first sentence of 7.29.4.5.8 p2:

> The `wmemchr` **generic** function locates the first occurence of ...

Modify 7.29.4.5.8 p3:

> The `wmemchr` **generic** function returns a pointer to ...

bsearch_s

Modify K.3.6.3.1 p1:

```
#define __STDC_WANT_LIB_EXT1__ 1
#include <stdlib.h>
Q void *bsearch_s(const void *key, Q void *base, rsize_t nmemb,
rsize_t size,
        int (*compar)(const void *k, const void *y, void *context),
        void *context);
```

(Q-qualify the return type and change the `const` qualifier of `base` to `Q`)

Modify the first sentence of K.3.6.3.1 p4:

> The `bsearch_s` **generic** function searches an array of ...

Modify the first sentence of K.3.6.3.1 p6:

> The `bsearch_s` **generic** function returns a pointer to ...

Add a new paragraph after K.3.6.3.1 p6:

> The `bsearch_s` function is generic in the qualification of the type pointed to by the argument to `base`. If this argument is a pointer to a `const`-qualified array, the returned pointer will also be to a `const`-qualified type.

References

C17

Core

C++

Embedded C

n2526

Future references

nXXXX: Generic functions notation

nXXXX: Void Which Binds